Discrete random variables

Teo Banica

Department of Mathematics, University of Cergy-Pontoise, F-95000 Cergy-Pontoise, France. teo.banica@gmail.com

2010 *Mathematics Subject Classification.* 60C05

Key words and phrases. Probability, Discrete variable

Abstract. This is an introduction to probability and discrete random variables. We first discuss games, counting and basic probability, with the mathematics of the binomials and factorials recalled, and with everything explained with numerous illustrations. Then we get into the theory of discrete random variables, with the basic theory explained, with illustrations, notably with results about the binomial and Poisson laws. Then we discuss more advanced distributions, such as the Bessel, hypergeometric and beta binomial ones, with methods from both algebra and analysis. We end with an introduction to continuous phenomena, advanced combinatorics, random matrices and freeness.

Preface

Does standard, foundational mathematics produce probability, or vice versa? Traditionally, the answer to this question is that standard mathematics comes first, and probability, which is something more specialized, comes after. However, never underestimate the egg, who can strike back the chicken, at least philosophically, as follows:

(1) As a first observation, which is of course something quite subjective, standard mathematics is developed via abstract theorems coming with abstract proofs, and as always with abstractions, there is a great deal of possible mistakes involved, in all this. So, after all, standard mathematics is something rather probabilistic in nature.

(2) More scientifically, theoretical physics, and more specifically statistical and quantum mechanics, tell us that everything, when examined with a good microscope, is probabilistic in nature. And the continuum that we are so used to, from basic calculus and mathematics, comes as a sort of limiting miracle, from this underlying randomness.

(3) Academically now, countless generations of modern scientists, in branches like biology or economics, have been trained with emphasis on probability, not to say with zero or almost knowledge in more standard undergraduate mathematics, and survived that training, and did good biology or economics afterwards. So, this approach works.

(4) Finally, from a purely mathematical perspective, discrete probability is truly a wonderland, with so many interesting things that can be said, based or nothing or almost. So, this can count as foundations, and everything else, including continuity, probabilistic or pure mathematical, can be potentially considered as coming on top of this.

But are we here for talking philosophy. The present book will be a down-to-earth introduction to probability and discrete random variables, with all the needed preliminaries included, based somehow on the belief that all this material is quite foundational, as suggested by (1,2,3,4) above. As for the author, which is myself, I really adhere to this, because as a scientist, mainly doing quantum physics, I certainly agree with (1,2), while as mathematics teacher, I have some familiarity with (3,4) too.

Getting now to the organization of the book, we will have 400 pages, which is quite long, for talking about all this, and on every topic, once the basics explained, we will not

hesitate to go into more advanced aspects, or discuss extensive illustrations, or alternative proofs, and so on. The book is organized in 4 parts, as follows:

I. We first discuss games, counting and basic probability, with the mathematics of the binomials recalled, and with everything explained with numerous illustrations.

II. Then we get into the theory of discrete random variables, with the basic theory explained, with illustrations, and with results about the binomial and Poisson laws.

III. Then we discuss some more advanced distributions, such as the Bessel, hypergeometric and beta binomial ones, with methods from both algebra and analysis.

IV. We end with an introduction to continuous phenomena, via random walks and central limits, and advanced combinatorics, random matrices and freeness.

The book is quite self-contained, or at least that is its aim, but we will need from time to time, usually for various specialized purposes, certain formulae from calculus. The problem indeed comes from the fact that, even when dealing with discrete probability, as we do here, for formulating your results in a final, truly usable form, you might need for instance the Stirling formula, for approximating the various factorials that you found. And the proof of this Stirling formula is certainly no easy business.

So, this is the situation, in short, enjoy this book as such, advertised as being self-contained, and for some help with the calculus and other things that are sometimes needed, you have my general book on mathematics [10]. Also, for more calculus you have my book [11], and for more about the material at the end, you have my book [12].

Many thanks to my cats, for their various probabilistic teachings. When it comes to quickly count, and process the count results, they are the kings of this world.

Cergy, July 2026
Teo Banica

Contents

Part I

Games, counting

Que mi pueblo
No derrame tanta sangre
Y se levante mi gente
A Dios le pido

CHAPTER 1

Binomials, factorials

1a. Binomial formula

Welcome to probability, and question for the two of us, how to start this book, and our learning? Normally we will be talking here about lots of things, touching many of the aspects of mathematics, and its applications. And so, as a starting point for this book, we should have the starting theorem of mathematics, taken in a large sense.

But, what is this theorem? When thinking about mathematics at large, the first thought goes to numbers and counting, which are needed pretty much everywhere, no matter what you want to do. And, regarding numbers and counting, if there is something which is extremely useful in practice, and at the same time easy enough to be understood, and hard enough to deserve the name Theorem, this is the following result:

THEOREM 1.1. *The number of possibilities of choosing k objects among n objects is*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

called binomial number, where $n! = 1 \cdot 2 \cdot 3 \ldots (n-2)(n-1)n$, called "factorial n".

PROOF. This is something quite tricky, when met for the first time, as follows:

(1) Imagine a set consisting of n objects. We have then n possibilities for choosing our 1st object, then $n-1$ possibilities for choosing our 2nd object, out of the $n-1$ objects left, and so on up to $n-k+1$ possibilities for choosing our k-th object, out of the $n-k+1$ objects left. Since the possibilities multiply, the total number of choices is:

$$\begin{aligned} N &= n(n-1)\ldots(n-k+1) \\ &= n(n-1)\ldots(n-k+1) \cdot \frac{(n-k)(n-k-1)\ldots 2 \cdot 1}{(n-k)(n-k-1)\ldots 2 \cdot 1} \\ &= \frac{n(n-1)\ldots 2 \cdot 1}{(n-k)(n-k-1)\ldots 2 \cdot 1} \\ &= \frac{n!}{(n-k)!} \end{aligned}$$

(2) But, is this correct. Normally a mathematical formula coming with mathematical proof is guaranteed to be 100% correct, or at least that's what mathematicians say. This

being said, who knows, so let us doublecheck our formula, by taking for instance:

$$n = 3 \quad , \quad k = 2$$

Here we have to choose 2 objects among 3 objects, and this is something easily done, because what we have to do is to dismiss one of the objects, and $N = 3$ choices here, and keep the 2 objects left. Thus, the total number of choices for our problem is $N = 3$. On the other hand, our computation in (1) gives a wrong answer, namely:

$$N = \frac{3!}{1!} = 6$$

(3) So, where is the mistake? Thinking a bit, the number N that we computed is in fact the number of possibilities of choosing k ordered objects among n objects. Thus, we must divide everything by the number M of orderings of the k objects that we chose:

$$\binom{n}{k} = \frac{N}{M}$$

(4) In order to compute now the missing number M, imagine a set consisting of k objects. There are k choices for the object to be designated #1, then $k - 1$ choices for the object to be designated #2, and so on up to 1 choice for the object to be designated $\#k$. We conclude that the missing number M is given by the following formula:

$$M = k(k-1)\ldots 2 \cdot 1 = k!$$

(5) Now by getting back to what we wanted to compute, we are led to:

$$\binom{n}{k} = \frac{N}{M} = \frac{n!/(n-k)!}{k!} = \frac{n!}{k!(n-k)!}$$

And this is the correct answer, because, well, that is how things are. In case you doubt, at $n = 3, k = 2$ for instance we obtain $3!/2!1! = 3$, which is correct. □

Quite interesting all the above, we have some nice mathematics going on, and more on this in a moment, and in addition, we have learned that producing correct theorems with correct proofs is not an easy business. Actually, Theorem 1.1 as stated is not exactly in final form, because as an important adding to it, which must be made, we have:

CONVENTION 1.2. *By definition,* $0! = 1$*, and this in order for the computation*

$$\binom{n}{n} = \frac{n!}{n!0!} = \frac{n!}{n! \times 1} = 1$$

based on Theorem 1.1 to work, yielding the correct value of $\binom{n}{n}$*, which is* 1*.*

Going ahead now with more mathematics and less philosophy, with Theorem 1.1 complemented by Convention 1.2 being in final form (trust me), we have:

THEOREM 1.3. *We have the binomial formula*

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$$

valid for any two numbers $a,b\in\mathbb{R}$.

PROOF. We have to compute the following quantity, with n terms in the product:

$$(a+b)^n=(a+b)(a+b)\ldots(a+b)$$

When expanding, we obtain a certain sum of products of a,b variables, with each such product being a quantity of type a^kb^{n-k}. Thus, we have a formula as follows:

$$(a+b)^n=\sum_{k=0}^{n}C_ka^kb^{n-k}$$

In order to finish, it remains to compute the above coefficients C_k. But, according to our product formula, C_k is the number of choices for the k needed a variables among the n available a variables. Thus, according to Theorem 1.1, we have:

$$C_k=\binom{n}{k}$$

We are therefore led to the formula in the statement. □

Theorem 1.3 is something quite interesting, so let us doublecheck it with some numerics. At small values of n we obtain the following formulae, which are all correct:

$$(a+b)^0=1$$

$$(a+b)^1=a+b$$

$$(a+b)^2=a^2+2ab+b^2$$

$$(a+b)^3=a^3+3a^2b+3ab^2+b^3$$

$$(a+b)^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$$

$$(a+b)^5=a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5$$

$$\vdots$$

Now observe that in these formulae, say for memorization purposes, the powers of the a,b variables are something very simple, that can be recovered right away. What matters are the coefficients, which are the binomial coefficients $\binom{n}{k}$, which form a triangle. So, it is enough to memorize this triangle, and this can be done by using:

THEOREM 1.4. *The Pascal triangle, formed by the binomial coefficients* $\binom{n}{k}$,

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & , & 1 & & & & \\
 & & & 1 & , & 2 & , & 1 & & & \\
 & & 1 & , & 3 & , & 3 & , & 1 & & \\
 & 1 & , & 4 & , & 6 & , & 4 & , & 1 & \\
1 & , & 5 & , & 10 & , & 10 & , & 5 & , & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

has the property that each entry is the sum of the two entries above it.

PROOF. In practice, the theorem states that the following formula holds:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

There are many ways of proving this formula, all instructive, as follows:

(1) Brute-force computation. We have indeed, as desired:

$$\begin{aligned}
\binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!}\left(\frac{1}{n-k} + \frac{1}{k}\right) \\
&= \frac{(n-1)!}{(k-1)!(n-k-1)!} \cdot \frac{n}{k(n-k)} \\
&= \binom{n}{k}
\end{aligned}$$

(2) Algebraic proof. We have the following formula, to start with:

$$(a+b)^n = (a+b)^{n-1}(a+b)$$

By using the binomial formula, this formula becomes:

$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \left[\sum_{r=0}^{n-1} \binom{n-1}{r} a^r b^{n-1-r}\right](a+b)$$

Now let us perform the multiplication on the right. We obtain a certain sum of terms of type $a^k b^{n-k}$, and to be more precise, each such $a^k b^{n-k}$ term can either come from the $\binom{n-1}{k-1}$ terms $a^{k-1}b^{n-k}$ multiplied by a, or from the $\binom{n-1}{k}$ terms $a^k b^{n-1-k}$ multiplied by b. Thus, the coefficient of $a^k b^{n-k}$ on the right is $\binom{n-1}{k-1} + \binom{n-1}{k}$, as desired.

(3) Combinatorics. Let us count k objects among n objects, with one of the n objects having a hat on top. Obviously, the hat has nothing to do with the count, and we obtain

$\binom{n}{k}$. On the other hand, we can say that there are two possibilities. Either the object with hat is counted, and we have $\binom{n-1}{k-1}$ possibilities here, or the object with hat is not counted, and we have $\binom{n-1}{k}$ possibilities here. Thus $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, as desired. □

There are many more things that can be said about binomial coefficients, with all sorts of interesting formulae, and more on this in a moment, but the idea is always the same, namely that in order to find such formulae you have a choice between algebra and combinatorics, and that when it comes to proofs, the brute-force computation method is useful too. In practice, the best is to master all 3 techniques. Among others, you will have in this way 3 different methods, for making sure that your formulae are correct indeed.

1b. Binomial coefficients

The binomial numbers, as constructed above, are quite fascinating objects, and the more you know about them, the better your mathematics will be. Trust me here. To start with, here are the first few factorials, that you should definitely memorize:

$$1! = 1 \quad , \quad 2! = 2 \quad , \quad 3! = 6 \quad , \quad 4! = 24 \quad , \quad 5! = 120 \quad , \quad 6! = 720$$

Next, here are some basic formulae for binomial coefficients, that you should definitely memorize too, and pull right away, when needed in your computations:

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6}$$

$$\binom{n}{4} = \frac{n(n-1)(n-2)(n-3)}{24}$$

Here are as well some numerics, with $n = k, k+1, k+2, \ldots$ in each case, that you should know well too, and pull out instantly, when needed in your computations:

$$\binom{n}{2} = 1, 3, 6, 10, 15, 21, 28, \ldots$$

$$\binom{n}{3} = 1, 4, 10, 20, 35, 56, \ldots$$

$$\binom{n}{4} = 1, 5, 15, 35, 70, \ldots$$

Still talking basics, there are as well a number of useful general formulae relating the binomial coefficients, that you should know too. Let us start with a simple fact:

PROPOSITION 1.5. *We have the following formula,*

$$\binom{n}{k} = \binom{n}{n-k}$$

valid for any integers $n \in \mathbb{N}$ and $k \leq n$.

PROOF. This is pretty much obvious, but as an illustration for the advice in the previous section, let us try to prove this by as many methods as we can:

(1) Combinatorics. We know that $\binom{n}{k}$ is the number of possibilities of choosing k objects among n objects. But, by looking at the $n-k$ objects which are dismissed, this is the same as the number $\binom{n}{n-k}$ of possibilities of choosing $n-k$ objects among n.

(2) Computation. Here is the computation, using the formula from Theorem 1.1:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = \binom{n}{n-k}$$

(3) Algebra. Let us have a look at the binomial formula from Theorem 1.3:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

With the replacement $k \to n-k$, this formula takes the following form:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{n-k} a^{n-k} b^k$$

Next, by interchanging $a \leftrightarrow b$, this latter formula takes the following form:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{n-k} a^k b^{n-k}$$

Now by comparing with the original formula above, we obtain the result.

(4) Pascal triangle. We can argue here that the Pascal triangle from Theorem 1.4 is symmetric with respect to vertical, and with this being formally provable for instance by recurrence on n. And I will leave the details here to you, have fun with this. □

Next, here are two more useful formulae, relating the binomial coefficients:

PROPOSITION 1.6. *The binomial coefficients are subject to the formulae*

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \quad , \quad \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

both coming from the binomial formula.

PROOF. The above formulae come indeed from the binomial formula from Theorem 1.3. Indeed, at $a = b = 1$ that formula gives the first formula in the statement:

$$(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k}$$

Also, with $a = 1$ and $b = -1$ we obtain the second formula in the statement:

$$(1-1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k (-1)^{n-k}$$

Alternatively, we can use $a = -1$ and $b = 1$, which gives right away that formula:

$$(-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k}$$

Thus, we are led to the above conclusions. Of course, there are many other such formulae, look up and learn some, that can only improve your mathematics. □

Getting now to more advanced things regarding the binomial coefficients, let us formulate, as a complement to the various particular cases discussed before:

DEFINITION 1.7. *The central binomial coefficients are the following numbers,*

$$D_n = \binom{2n}{n}$$

which are not to be confused with the middle binomial coefficients,

$$E_n = \binom{n}{[n/2]}$$

with [.] *standing as usual for the integer part.*

Observe that we can recover the central binomial coefficients as particular cases of the middle binomial coefficients, due to the following formula:

$$D_n = E_{2n}$$

However, in practice, the central binomial coefficients D_n are the truly interesting quantities, and the middle binomial coefficients E_n remain something secondary. Regarding now the numerics for the central binomial coefficients, these are as follows:

$$D_n = 1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620, \ldots$$

This sequence is actually something quite fascinating, and if you are a number theory nerd, and hope so are you, one of the first things that you will discover, by playing with it, is that these central binomial coefficients factorize as follows:

$$\begin{aligned} D_n &= 1 \times 1, 2 \times 1, 3 \times 2, 4 \times 5, 5 \times 14, 6 \times 42, \\ &\quad 7 \times 132, 8 \times 429, 9 \times 1430, 10 \times 4862, \ldots \end{aligned}$$

Thus, we are led in this way to the following conjecture:

CONJECTURE 1.8. *The central binomial coefficients factorize as*

$$D_n = (n+1)C_n$$

with $C_n = 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, \ldots$ *being certain integers.*

However, this is something which is not trivial to prove, with bare hands, and we will leave it for later in this chapter, once we will know more things.

More modestly now, but along the same lines, let us attempt to work out some basic arithmetic properties of the general binomial coefficients. We first have:

PROPOSITION 1.9. *Given a prime number* $p \geq 2$*, we have*

$$p \,|\, \binom{p}{k} \quad , \quad p^2 \not| \binom{p}{k}$$

for any integer $1 < k < p$*.*

PROOF. This is something that you can come upon by examining the Pascal triangle, and in what regards the formal proof, this comes from the following formula:

$$\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$$

Indeed, due to our assumption $1 < k < p$, the numerator is divisible by p, and not by p^2, while the denominator is not divisible by p, and this gives the result. □

Along the same lines, at a more advanced level, we have the following result, which is something very useful, in practice, for various arithmetic purposes:

THEOREM 1.10. *Given a prime number* $p \geq 2$*, the exponent of* p *inside* $n!$ *is*

$$a_n = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

and so the exponent of p *inside* $\binom{n}{k}$ *is given by the formula*

$$b_{n,k} = a_n - a_k - a_{n-k}$$

with $[.]$ *standing as usual for the integer part.*

PROOF. This is indeed something quite self-explanatory, the idea being as follows:

(1) Regarding the first assertion, about factorials, which is the main one, we must compute the exponent of p inside the following product:

$$n! = 1 \cdot 2 \cdot 3 \cdot 4 \ldots n$$

But here, as a first contribution to the exponent, we have a 1 factor for each of the multiples of p of type $0 < pa \leq n$, and so this first contribution is given by:

$$c_1 = \left[\frac{n}{p}\right]$$

Next, as a second contribution, we must add a supplementary 1 factor for each of the multiples of p^2 of type $0 < p^2a \leq n$, and this second contribution is given by:

$$c_2 = \left[\frac{n}{p^2}\right]$$

But then, we have as well a third contribution, coming by adding a supplementary 1 factor for each of the multiples of p^3 of type $0 < p^3a \leq n$, which is given by:

$$c_3 = \left[\frac{n}{p^3}\right]$$

And so on, and we are led in this way to the formula in the statement, namely:

$$a_n = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

By the way, observe that this sum is finite, stopping where $p^k > n$.

(2) In what regards now the second assertion, we must compute the exponent of p inside the binomial coefficients, which are given by the following formula:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

But this gives right away $b_{n,k} = a_n - a_k - a_{n-k}$, as claimed.

(3) Finally, as an illustration for this, for any number $s \leq p$ we have:

$$\begin{aligned} a_s &= \left[\frac{s}{p}\right] + \left[\frac{s}{p^2}\right] + \left[\frac{s}{p^3}\right] + \ldots \\ &= \delta_{sp} + 0 + 0 + \ldots \\ &= \delta_{sp} \end{aligned}$$

We conclude that for $n = p$ and $1 < k < p$ we have the following formula:

$$\begin{aligned} b_{p,k} &= a_p - a_k - a_{p-k} \\ &= 1 - 0 - 0 \\ &= 1 \end{aligned}$$

Thus, the present result generalizes what we previously had, in Proposition 1.9. □

As a basic application now of our binomial formula technology, we have:

THEOREM 1.11. *We have the following congruence, for any prime p,*

$$a^p = a(p)$$

called Fermat's little theorem.

PROOF. We can prove this by recurrence on $a \in \mathbb{N}$, by using Proposition 1.9:

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p}\binom{p}{k}a^k\\ &= a^p + 1(p)\\ &= a + 1(p)\end{aligned}$$

Thus, we have the result for any $a \in \mathbb{N}$, and with the case $p = 2$ being trivial, we can assume $p \geq 3$, and here by using $a \to -a$ we get it for any $a \in \mathbb{Z}$, as desired. □

1c. Analysis, estimates

In practice, in order to get some applications out of our counting results, we will need some estimates for the binomials. Let us start with something very basic, namely:

THEOREM 1.12. *We have the following estimates for the binomial coefficients,*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \frac{n^k}{k!}$$

both coming from definitions.

PROOF. We have two estimates to be proved, the idea being as follows:

(1) Regarding the first estimate, this can be established as follows:

$$\begin{aligned}\binom{n}{k} &= \frac{n}{k}\cdot\frac{n-1}{k-1}\cdots\frac{n-k+1}{1}\\ &\geq \frac{n}{k}\cdot\frac{n}{k}\cdots\frac{n}{k}\\ &= \left(\frac{n}{k}\right)^k\end{aligned}$$

(2) The proof of the second estimate is similar, as follows:

$$\begin{aligned}\binom{n}{k} &= \frac{n}{k}\cdot\frac{n-1}{k-1}\cdots\frac{n-k+1}{1}\\ &\leq \frac{n}{k}\cdot\frac{n}{k-1}\cdots\frac{n}{1}\\ &= \frac{n^k}{k!}\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

The problem is now, how to do better? Leaving aside the fact that both our estimates were quite rough, so job for us later to improve our method, what is quite bothering is the upper bound $n^k/k!$, and more specifically, the number $k!$ appearing there.

In order to deal with this latter problem, we can use the number e. We have:

THEOREM 1.13. *We can define a number $e = 2.71828\ldots$ as the following limit:*

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Alternatively, we have the following formula, equivalent to the above one:

$$e = \sum_{n=0}^{\infty}\frac{1}{n!}$$

More generally, the exponential of any number x can be computed as follows:

$$e^x = \lim_{n\to\infty}\left(1+\frac{x}{n}\right)^n$$

Alternatively, we have the following formula, equivalent to the above one:

$$e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}$$

Also, e is irrational, that is, impossible to write as $e = a/b$, with $a, b \in \mathbb{N}$.

PROOF. All this is well-known, first class mathematics, the idea being as follows:

(1) The fact that $(1+1/n)^n$ increases, and converges towards a certain limit $e \in [2, 3]$, follows by using the binomial formula, and the arithmetic-geometric inequality.

(2) The fact that $\sum_n 1/n!$ converges is elementary, and some estimates show that the limit must be e. Moreover, this can be used for reaching to the figure $e = 2.71828\ldots$

(3) Regarding the first formula for the exponential, namely $(1 + x/n)^n \to e^x$, this follows from the first formula for e, from (1), in a straightforward way.

(4) Regarding $e^x = \sum_n x^n/n!$, the idea is that the function $f(x) = \sum_n x^n/n!$ satisfies $f(x + y) = f(x)f(y)$, so we must have $f(x) = a^x$, with $a = f(1) = e$.

(5) Assuming $e = a/b$ with $a, b \in \mathbb{N}$, set $x = b!(e - \sum_{n=0}^{b} 1/n!)$. Obviously, $x > 0$ and $x \in \mathbb{N}$. On the other hand $x < 1/(b + 1) + 1/(b + 1)^2 + \ldots = 1/b < 1$, contradiction. □

Quite interesting all this, hope you agree with me. As a conclusion, e is something quite subtle, and this will be our mathematical weapon of choice, in what follows.

Although calculus is not really on the menu, in this book doing discrete probability, let us record as well some calculus results regarding e, which are good to know:

THEOREM 1.14 (continuation). *More conceptually, regarding the number e:*

(1) *e is the unique number satisfying $e^x \simeq 1 + x$ for $x \simeq 0$.*
(2) *$x \to e^x$ is the unique power function satisfying $(e^x)' = e^x$.*
(3) *In fact, e^x is the unique function satisfying $f(0) = 1$ and $f' = f$.*

PROOF. As mentioned, this is something more advanced, that we will not really need, in what follows, but this being important, and good to know, here is the story with it:

(1) We certainly have $e^x \simeq 1 + x$ for $x \simeq 0$, coming from $e^x = \sum_n x^n/n!$, by keeping the first two terms, and ignoring the rest. So good, at least we know one thing.

(2) In what regards the converse, if we denote by log the inverse of $x \to e^x$ we have $a^x = e^{x \log a} \simeq 1 + x \log a$ for $x \simeq 0$, so $a^x \simeq 1 + x$ requires indeed $a = e$, as desired.

(3) Next, we can talk about the derivatives of functions $f : \mathbb{R} \to \mathbb{R}$, with $f(x)$ being the slope of f at x, that is, according to $f(x + t) \simeq f(x) + f'(x)t$ with $t \simeq 0$.

(4) Now consider the function $f(x) = e^x$. Then (1) tells us that $f'(0) = 1 = f(0)$. More generally, from $e^{x+t} = e^x e^t \simeq e^x(1 + t)$ we obtain $f'(x) = e^x = f(x)$, for any x.

(5) Alternatively, it follows from the binomial formula that we have $(x^n)' = nx^{n-1}$, and by using $e^x = \sum_n x^n/n!$ we obtain right away $(e^x)' = e^x$, as desired.

(6) Regarding the converse, completing the proof of the assertion (2) in the statement, this simply follows from the uniqueness in the assertion (1) in the statement.

(7) As for the last assertion, when looking for $f(x) = \sum_n c_n x^n$ satisfying $f(0) = 1$ and $f' = f$, by using the rule $(x^n)' = nx^{n-1}$ from (5) we get $f(x) = \sum_n x^n/n! = e^x$.

(8) However, not done with this, because we must prove that $f(x) = e^x$ is the unique abstract function satisfying $f(0) = 1$ and $f' = f$. Thus, we have to work some more.

(9) So, let us develop some more calculus. Following Leibnitz, we have the differentiation rule $(fg)' = f'g + fg'$, coming straight from the definitions in (3).

(10) We will need as well the fact, which is quite intuitive, and formally comes by looking at the minima and maxima, that $f' = 0$ implies that f is constant.

(11) Good news, we can now finish. Indeed, assuming $f(0) = 1$ and $f' = f$ we have $(e^{-x}f)' = -e^{-x}f + e^{-x}f' = 0$, which gives $e^{-x}f = 1$, and so $f(x) = e^x$, as desired.

(12) And with this, end of our calculus excursion. Do not hesitate of course to learn more about all this, and trust me here, learning calculus is an excellent investment. □

Good news, we can go back now to our previous estimates from Theorem 1.12, for the binomials, and improve them into something truly useful, as follows:

THEOREM 1.15. *We have the following estimates for the binomials,*

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} < \left(\frac{ne}{k}\right)^k$$

with $e = 2.71828\ldots$ being the usual constant from analysis.

PROOF. We have indeed the following estimate, based on Theorem 1.13:

$$\frac{k^k}{k!} < \sum_{n=0}^{\infty} \frac{k^n}{n!} = e^k$$

But with this, we can go back to the upper bound in Theorem 1.12, and we have:

$$\frac{n^k}{k!} < \frac{n^k}{k^k/e^k} = \left(\frac{ne}{k}\right)^k$$

Thus, we are led to the conclusions in the statement. □

The problem is now, how to improve Theorem 1.15? In order to solve this question, which is something non-trivial, let us start with the following key result:

THEOREM 1.16. *We have the following estimate,*

$$\left(\frac{N}{e}\right)^N e < N! < \left(\frac{N}{e}\right)^N e(N+1)$$

valid for any $N \in \mathbb{N}$.

PROOF. This is something quite tricky, the idea being as follows:

(1) To start with, yes I know that calculus is not on the menu for this book, dealing with discrete probability, but still, we can learn some interesting things on the way, and prove the present theorem. So, have a second look at Theorem 1.14, and stay with me.

(2) In order to get our estimate, the idea is to integrate the logarithm. Indeed, we can talk about the integral $\int_a^b f(x)dx$ of any continuous function $f : [a, b] \to \mathbb{R}$, as being the signed area below its graph. By drawing rectangles, the relevant formula is:

$$\int_a^b f(x)dx = \lim_{n\to\infty} \sum_{k=0}^{n-1} \frac{b-a}{n} \cdot f\left(a + k \cdot \frac{b-a}{n}\right)$$

(3) Now let us do this for $\log : [1, \infty) \to [0, \infty)$, inverse of $\exp : [0, \infty) \to [1, \infty)$. Since exp is increasing, log is increasing too, and by drawing rectangles, we obtain:

$$\log 1 + \ldots + \log(N-1) < \int_1^N \log x \, dx < \log 2 + \ldots + \log N$$

(4) Which is good news, because we get the following estimate, involving factorials:

$$\log((N-1)!) < \int_1^N \log x\, dx < \log(N!)$$

Equivalently, by exponentiating, we have the following estimate:

$$(N-1)! < \exp\left(\int_1^N \log x\, dx\right) < N!$$

(5) The problem is now, how to integrate log? For this purpose, let us go back to the differentiation theory developed in the proof of Theorem 1.14. As a continuation, we have the following straightforward formula, called fundamental theorem of calculus:

$$\int_a^b F'(x)dx = F(b) - F(a)$$

(6) So, in the end it all comes to finding a function F satisfying $F' = \log$. Now for this purpose, let us start with a formula that we know from Theorem 1.14, namely:

$$\exp' = \exp$$

It is easy to see that we have $(f \circ g)'(x) = f'(g(x))g'(x)$, and this gives:

$$(\log x)' = \frac{1}{x}$$

(7) In order to make now appear log on the right, the idea is quite clear, namely multiplying on the left by x. We obtain in this way the following formula:

$$(x \log x)' = 1 \cdot \log x + x \cdot \frac{1}{x} = \log x + 1$$

We are almost there, all we have to do is to substract x from the left, as to get:

$$(x \log x - x)' = \log x$$

(8) Summarizing, integration problem solved, and by using this, we have:

$$\begin{aligned} \int_1^N \log x\, dx &= (N \log N - N) - (1 \log 1 - 1) \\ &= N \log N - N + 1 \end{aligned}$$

(9) But with this, by going back to the estimate found in (4), we obtain:

$$(N-1)! < \left(\frac{N}{e}\right)^N e < N!$$

Equivalently, with $N \to N+1$ on the left, we have the following estimate:

$$\left(\frac{N}{e}\right)^N e < N! < \left(\frac{N+1}{e}\right)^{N+1} e$$

(10) Now observe that the upper bound on the right satisfies:

$$\left(\frac{N+1}{e}\right)^{N+1} e = \left(\frac{N+1}{N}\right)^{N} \left(\frac{N}{e}\right)^{N} (N+1) < \left(\frac{N}{e}\right)^{N} e(N+1)$$

Thus, we are led to the formula in the statement. □

Still with me I hope, after all these computations. Actually, although this book was advertised to be about discrete mathematics, not based on calculus, we ended up in learning a massive number of calculus things. Nevermind. That's how mathematics is.

Coming next, as a consequence of Theorem 1.16, let us formulate:

THEOREM 1.17. *We have the following estimate, in the $N \to \infty$ limit,*

$$N! \approx \left(\frac{N}{e}\right)^{N} e$$

with the $\approx$ sign meaning that the quotient is much smaller than both factors.

PROOF. This is clear from what we have in Theorem 1.16, which tells us that the quotient of the functions in the statement satisfies the following estimate:

$$N! \Big/ \left(\frac{N}{e}\right)^{N} e \in [1, N+1]$$

Thus, with the above convention for $\approx$, we are led to the formula in the statement. □

Good news, we can now approximate the binomial coefficients, as follows:

THEOREM 1.18. *We have the following estimate for the binomial coefficients,*

$$\binom{N}{K} \approx \left(\frac{1}{t^t(1-t)^{1-t}}\right)^{N}$$

in the $K \simeq tN \to \infty$ limit, with $t \in (0, 1]$. In particular we have

$$\binom{2N}{N} \approx 4^N$$

in the $N \to \infty$ limit, for the central binomial coefficients.

PROOF. We know from Theorem 1.17 that we have $N! \approx \left(\frac{N}{e}\right)^{N} e$, and in practice, with our convention for $\approx$, this can be replaced by $N! \approx \left(\frac{N}{e}\right)^{N}$. Now by using this:

(1) The first estimate follows from the definition of the binomial coefficients:

$$\begin{aligned}\binom{N}{K} &= \frac{N!}{K!(N-K)!}\\ &\approx \left(\frac{N}{e}\right)^N\left(\frac{e}{K}\right)^K\left(\frac{e}{N-K}\right)^{N-K}\\ &= \frac{N^N}{K^K(N-K)^{N-K}}\\ &= \frac{N^N}{(tN)^{tN}((1-t)N)^{(1-t)N}}\\ &= \left(\frac{1}{t^t(1-t)^{1-t}}\right)^N\end{aligned}$$

(2) The second estimate follows from a similar computation, as follows:

$$\begin{aligned}\binom{2N}{N} &= \frac{(2N)!}{N!N!}\\ &\approx \left(\frac{2N}{e}\right)^{2N}\left(\frac{e}{N}\right)^{2N}\\ &= 4^N\end{aligned}$$

Alternatively, we can take $t=1/2$ in (1), then rescale via $N\to 2N$. □

Shall we stop here? You must be kidding. The $\approx$ sign that we have in Theorems 1.17 and 1.18 is quite annoying, but we can improve that, in the following way:

THEOREM 1.19. *We have the Stirling formula*

$$N!\simeq\left(\frac{N}{e}\right)^N\sqrt{2\pi N}$$

valid in the $N\to\infty$ limit.

PROOF. This is something quite tricky, the idea being as follows:

(1) We recall, from the proof of Theorem 1.16, that with rectangles we get:

$$\log(N!)\approx\int_1^N\log x\,dx=N\log N-N+1$$

By exponentiating, this gives the following estimate, which is not bad:

$$N!\approx\left(\frac{N}{e}\right)^N\cdot e$$

(2) We can improve this by replacing the rectangles with trapezoids. We get:

$$\begin{aligned}\log(N!) &\approx \int_1^N \log x\,dx + \frac{\log 1 + \log N}{2}\\ &= N\log N - N + 1 + \frac{\log N}{2}\end{aligned}$$

By exponentiating, this gives the following estimate, which gets us closer:

$$N! \approx \left(\frac{N}{e}\right)^N \cdot e \cdot \sqrt{N}$$

(3) In order to conclude, we must take some kind of mathematical magnifier, and carefully estimate the error made in (2). Fortunately, this mathematical magnifier exists, called Euler-Maclaurin formula, and after some computations, this leads to Stirling.

(4) Alternatively, we have the following computation, which is non-trivial either:

$$\begin{aligned}N! &= \int_0^\infty x^N e^{-x} dx\\ &\simeq \int_{-N}^N \left(\frac{N}{e}\right)^N e^{-y^2/2N}\,dy\\ &\simeq \left(\frac{N}{e}\right)^N \int_{\mathbb{R}} e^{-y^2/2N}\,dy\\ &= \left(\frac{N}{e}\right)^N \sqrt{2N}\int_{\mathbb{R}} e^{-z^2}\,dz\\ &= \left(\frac{N}{e}\right)^N \sqrt{2\pi N}\end{aligned}$$

(5) In short, quite complicated, all this. We will be back to this, later in this book. □

Good news, we can now professionally estimate the binomials, as follows:

THEOREM 1.20. *We have the following estimate for binomial coefficients,*

$$\binom{N}{K} \simeq \left(\frac{1}{t^t(1-t)^{1-t}}\right)^N \frac{1}{\sqrt{2\pi t(1-t)N}}$$

in the $K \simeq tN \to \infty$ limit, with $t \in (0,1]$. In particular we have

$$\binom{2N}{N} \simeq \frac{4^N}{\sqrt{\pi N}}$$

in the $N \to \infty$ limit, for the central binomial coefficients.

PROOF. All this is very standard, by using the Stirling formula, as follows:

(1) This follows from the definition of the binomial coefficients, namely:

$$\begin{aligned}\binom{N}{K} &= \frac{N!}{K!(N-K)!}\\ &\simeq \left(\frac{N}{e}\right)^N\sqrt{2\pi N}\left(\frac{e}{K}\right)^K\frac{1}{\sqrt{2\pi K}}\left(\frac{e}{N-K}\right)^{N-K}\frac{1}{\sqrt{2\pi(N-K)}}\\ &= \frac{N^N}{K^K(N-K)^{N-K}}\sqrt{\frac{N}{2\pi K(N-K)}}\\ &\simeq \frac{N^N}{(tN)^{tN}((1-t)N)^{(1-t)N}}\sqrt{\frac{N}{2\pi tN(1-t)N}}\\ &= \left(\frac{1}{t^t(1-t)^{1-t}}\right)^N\frac{1}{\sqrt{2\pi t(1-t)N}}\end{aligned}$$

Thus, we are led to the conclusion in the statement.

(2) This estimate follows from a similar computation, as follows:

$$\begin{aligned}\binom{2N}{N} &= \frac{(2N)!}{N!N!}\\ &\simeq \left(\frac{2N}{e}\right)^{2N}\sqrt{4\pi N}\left(\frac{e}{N}\right)^{2N}\frac{1}{2\pi N}\\ &= \frac{4^N}{\sqrt{\pi N}}\end{aligned}$$

Alternatively, we can take $t=1/2$ in (1), then rescale via $N\to 2N$. □

And with this, good news, we have all the needed tools in our bag for converting the past, present and future counting results into something useful, in practice.

1d. Catalan numbers

With the above discussed, done with the binomials? Certainly not. There are far more things that can be said, about them, and as a most pressing task, we would like to prove Conjecture 1.8, which states that the following numbers are integers:

$$C_k=\frac{1}{k+1}\binom{2k}{k}$$

Aa explained earlier in this chapter, numerically this seems to hold indeed, with the sequence $\{C_k|k \geq 0\}$ consisting indeed of integers only, as follows:

$$C_k = 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, \ldots$$

But, how to prove this? In answer, this is undoable with bare hands, and we will have to trick. Obviously, we need to know what the above numbers C_k count, and for this purpose, we can use the following fact, which fits with the above numerics:

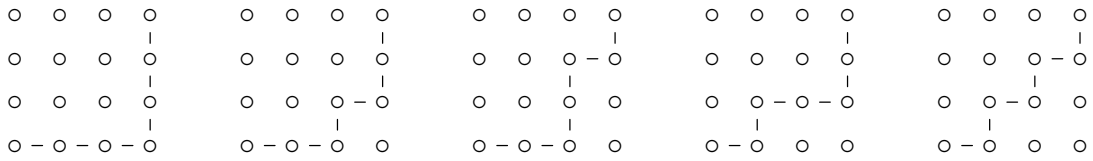
THEOREM 1.21. *The following objects are counted by the same numbers C_k, called Catalan numbers, given by $C_0 = C_1 = 1$ and $C_{k+1} = \sum_{a+b=k} C_a C_b$:*

(1) *The length $2k$ loops on $\mathbb{N}$, based at 0.*
(2) *The noncrossing pairings of $1, \ldots, 2k$.*
(3) *The noncrossing partitions of $1, \ldots, k$.*
(4) *The length $2k$ Dyck paths in the plane.*

PROOF. All this is standard combinatorics, the idea being as follows:

(1) To start with, in what regards the various objects involved, the length $2k$ loops on $\mathbb{N}$ are the usual length $2k$ loops on $\mathbb{N}$, and the same goes for the noncrossing pairings of $1, \ldots, 2k$, and for the noncrossing partitions of $1, \ldots, k$, the idea here being that you must be able to draw the pairing or partition in a noncrossing way.

(2) Regarding now the length $2k$ Dyck paths in the plane, these are by definition the paths from $(0, 0)$ to (k, k), marching North-East over the integer lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$, by staying inside the square $[0, k] \times [0, k]$, and staying as well under the diagonal of this square. As an example, here are the 5 possible Dyck paths at $n = 3$:



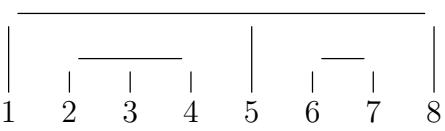
(3) Thus, we have definitions for all objects involved, and in each case, if you start counting them, you end up with the same sequence, namely that in Conjecture 1.8:

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, \ldots$$

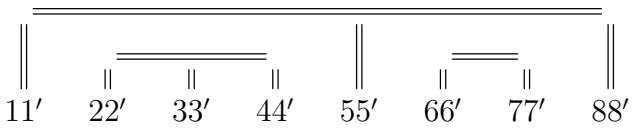
(4) In order to prove now that (1-4) produce indeed the same numbers, many things can be said. The idea is that, leaving aside mathematical brevity, and more specifically abstract reasonings of type $a = b, b = c \implies a = c$, what we have to do, in order to fully understand what is going on, is to etablish $\binom{4}{2} = 6$ equalities, via bijective proofs.

(5) But this can be done, indeed. As an example here, the noncrossing pairings of $1, \ldots, 2k$ from (2) are in bijection with the noncrossing partitions of $1, \ldots, k$ from (3), via

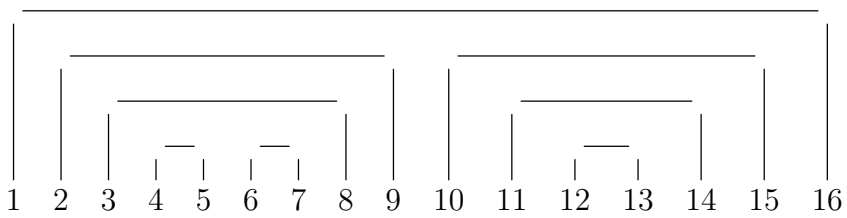
fattening the pairings and shrinking the partitions. Consider a noncrossing partition:



Now let us "fatten" this partition, by doubling everything, as follows:



We can see emerging here a noncrossing pairing, and by relabeling the points $1, \ldots, 16$, and properly redrawing the picture, what we have is indeed a noncrossing pairing:



As for the reverse operation, that is obviously obtained by "shrinking" our pairing, by collapsing pairs of consecutive neighbors, that is, by identifying $1 = 2$, then $3 = 4$, then $5 = 6$, and so on. We will leave the details here as an instructive exercise, and exercise as well, to add the loops in (1) and the Dyck paths in (4) to the bijective picture.

(6) This being said, as a matter of having our theorem formally proved, I mean by me professor and not by you student, here is a less elegant argument, which is however quick, and does the job. The point is that, in each of the cases (1-4) under consideration, the numbers C_k that we get are easily seen to be subject to the following recurrence:

$$C_{k+1} = \sum_{a+b=k} C_a C_b$$

Now the initial data being the same, namely $C_0 = C_1 = 1$, in each of the cases (1-4) under consideration, we get indeed the same numbers, as desired. □

Now we can pass to the second step, namely selecting in the above list the objects that we find the most convenient to count, and count them. This leads to:

THEOREM 1.22. *The Catalan numbers are given by the formula*

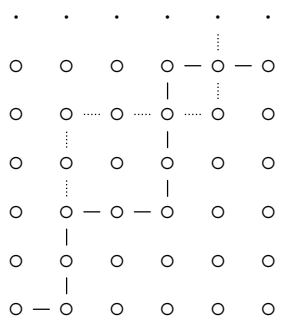
$$C_k = \frac{1}{k+1}\binom{2k}{k}$$

with this being best seen by counting the length $2k$ Dyck paths in the plane.

PROOF. This is something quite tricky, the idea being as follows:

(1) Let us count indeed the Dyck paths in the plane. For this purpose, we use a trick. Indeed, if we ignore the assumption that our path must stay under the diagonal of the square, we have $\binom{2k}{k}$ such paths. And among these, we have the "good" ones, those that we want to count, and then the "bad" ones, those that we want to ignore.

(2) So, let us count the bad paths, those crossing the diagonal of the square, and reaching the higher diagonal next to it, the one joining $(0,1)$ and $(k,k+1)$. In order to count these, the trick is to "flip" their bad part over that higher diagonal, as follows:



(3) Now observe that, as it is obvious on the above picture, due to the flipping, the flipped bad path will no longer end in (k,k), but rather in $(k-1,k+1)$. Moreover, more is true, in the sense that, by thinking a bit, we see that the flipped bad paths are precisely those ending in $(k-1,k+1)$. Thus, we can count these flipped bad paths, and so the bad paths, and so the good paths too, and so good news, we are done.

(4) To finish now, by putting everything together, we have:

$$\begin{aligned} C_k &= \binom{2k}{k} - \binom{2k}{k-1} \\ &= \binom{2k}{k} - \frac{k}{k+1}\binom{2k}{k} \\ &= \frac{1}{k+1}\binom{2k}{k} \end{aligned}$$

Thus, we are led to the formula in the statement. And good work that we did, among others with Conjecture 1.8 being now proved. Nothing can resist us. □

Quite interesting all this, but you might wonder, after all, is there any simpler proof for Conjecture 1.8? I mean, do we really need all the combinatorics above.

In answer, not clear, so I guess I'll have to catch a cat, and ask. And with now as I type being Summer, during a heat wave, with all the cats lying dormant around the

house, on the grass, nothing easier for a slow animal like me, which however lacks fur, than quickly catching one, and asking my mathematical questions. And cat answers:

CAT 1.23. *Calculus, baby, using* $f(z) = \sum_k C_k z^k$.

Thanks cat, this sounds like a good idea. So, thinking a bit at all this, we are led to the following new approach to the Catalan numbers, based this time on calculus:

THEOREM 1.24. *The Catalan numbers have the following properties:*

(1) *They satisfy* $C_{k+1} = \sum_{a+b=k} C_a C_b$.
(2) *The series* $f(z) = \sum_{k\geq 0} C_k z^k$ *satisfies* $zf^2 - f + 1 = 0$.
(3) *This series is given by* $f(z) = \frac{1-\sqrt{1-4z}}{2z}$.
(4) *We have the formula* $C_k = \frac{1}{k+1}\binom{2k}{k}$.

PROOF. Here (1) is something that we know from Theorem 1.21, then (2) comes from (1), then (3) comes from (2), and finally (4) can only come from (3), right, I mean if there is a tricky formula for $\sqrt{1-x}$, that certainly must be known, and coming via calculus. We will be back to this later in this book, when knowing more calculus. □

1e. Exercises

This chapter was a standard introduction to counting, and as exercises, we have:

EXERCISE 1.25. *Further meditate on* $0! = 1$*, but not too much.*

EXERCISE 1.26. *Memorize as many binomials and factorials you can.*

EXERCISE 1.27. *Look up and learn other interesting formulae relating binomials.*

EXERCISE 1.28. *Learn some more, about the arithmetic of the binomials.*

EXERCISE 1.29. *Review if needed the full theory of the number* e.

EXERCISE 1.30. *Review also the basics of derivatives and integrals.*

EXERCISE 1.31. *Learn the various proofs of the Stirling formula.*

EXERCISE 1.32. *Learn more about the Catalan numbers, and their properties.*

As bonus exercise, learn some programming too. You will need this, later.

CHAPTER 2

Games, counting

2a. Flipping coins

We learned many interesting things so far, about binomials and factorials, sometimes a bit crazy, coming without complete proofs, and that was certainly good learning. Time now to get to a more normal pace, and slowly develop what we want to do in this book, with definitions, examples, and proofs for everything, namely discrete probability.

Needless to say, all this will not use that crazy approximation stuff from chapter 1. However, as mentioned there, that approximation results are very useful, in order to convert our future probabilistic findings into truly usable results. Good to know.

Getting started now, the entry point to discrete probability are basic activities from the real life, such as playing with coins, dice or cards. Many things can be said here, of various levels of abstraction and difficulty, and our plan will be as follows:

(1) We will do a lot of computations in this chapter, and in the next one too, in relation with coins, dice and cards, as to get familiar with the subject. And with doing such computations, we insist, being something key, for understanding probability.

(2) And then afterwards, in chapter 4, we will talk about abstract probability theory, with definitions, theorems and everything, inspired from what we found. And with this being, we insist too, something that comes only when familiar with coins, dice, cards.

Let us start with the coins. We will use here a coin designated as follows:

heads *tails*

At the beginning of everything, when talking coins, we have the following fact:

FACT 2.1. *The probability for a coin to land as heads is* $1/2$. *Thus*

$$\otimes \to \frac{1}{2} \quad , \quad \odot \to \frac{1}{2}$$

with the numbers standing for the probabilities of the situations to happen.

But the problem now is, is this just a fact, undoubtedly true, or a mathematical theorem? And with the answer here being a bit unclear, due to the extremely simple nature of our problem. So, in order to further comment on this, and eventually reach to an answer to our question, let us do something more complicated, as follows:

PROPOSITION 2.2. *When throwing a coin twice, the probabilities are as follows:*

$$\otimes\otimes \to \frac{1}{4} \quad , \quad \otimes\odot \to \frac{1}{4}$$

$$\odot\otimes \to \frac{1}{4} \quad , \quad \odot\odot \to \frac{1}{4}$$

Alternatively, we have the following probabilities for what happens,

$$\otimes \text{ only } \to \frac{1}{4} \quad , \quad \otimes \text{ and } \odot \to \frac{1}{2} \quad , \quad \odot \text{ only } \to \frac{1}{4}$$

when interested only in the final count of heads and tails.

PROOF. This is indeed something obvious, with the only math involved being as follows, with P standing for the probability for something to happen:

$$\begin{aligned} P\left(\otimes \text{ and } \odot\right) &= P\left(\otimes\odot\right) + P\left(\odot\otimes\right) \\ &= \frac{1}{4} + \frac{1}{4} \\ &= \frac{1}{2} \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Along the same lines, regarding now 3 throws, we have the following result:

PROPOSITION 2.3. *When throwing a coin three times, the probabilities are*

$$\otimes\otimes\otimes \to \frac{1}{8}\,, \quad \otimes\otimes\odot \to \frac{1}{8}\,, \quad \otimes\odot\otimes \to \frac{1}{8}\,, \quad \otimes\odot\odot \to \frac{1}{8}$$

$$\odot\otimes\otimes \to \frac{1}{8}\,, \quad \odot\otimes\odot \to \frac{1}{8}\,, \quad \odot\odot\otimes \to \frac{1}{8}\,, \quad \odot\odot\odot \to \frac{1}{8}$$

Alternatively, we have the following probabilities for what happens,

$$3\otimes \to \frac{1}{8} \quad , \quad 2\otimes, 1\odot \to \frac{3}{8} \quad , \quad 2\odot, 1\otimes \to \frac{3}{8} \quad , \quad 3\odot \to \frac{1}{8}$$

when interested only in the final count of heads and tails.

PROOF. This is again something obvious, with the first piece of math involved being as follows, with P standing as usual for the probability for something to happen:

$$\begin{aligned} P\left(2\otimes, 1\odot\right) &= P\left(\otimes\otimes\odot\right) + P\left(\otimes\odot\otimes\right) + P\left(\odot\otimes\otimes\right) \\ &= \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \\ &= \frac{3}{8} \end{aligned}$$

As for the second piece of math involved, this is similar, as follows:

$$\begin{aligned} P\left(1\otimes, 2\odot\right) &= P\left(\otimes\odot\odot\right) + P\left(\odot\otimes\odot\right) + P\left(\odot\odot\otimes\right) \\ &= \frac{1}{8} + \frac{1}{8} + \frac{1}{8} \\ &= \frac{3}{8} \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Let us work out as well what happens for 4 throws. The result here is as follows:

PROPOSITION 2.4. *When throwing a coin four times, the probabilities are*

$$\otimes\otimes\otimes\otimes \to \frac{1}{16}\,, \quad \otimes\otimes\otimes\odot \to \frac{1}{16}\,, \quad \ldots \quad, \odot\odot\odot\odot \to \frac{1}{16}$$

Alternatively, we have the following probabilities for what happens,

$$4\otimes \to \frac{1}{16}\,,\ 3\otimes 1\odot \to \frac{1}{4}\,,\ 2\otimes 2\odot \to \frac{3}{8}\,,\ 1\otimes 3\odot \to \frac{1}{4}\,,\ 4\otimes \to \frac{1}{16}$$

when interested only in the final count of heads and tails.

PROOF. As before, the first assertion is clear, with the complete table of the possibilities being as follows, each of them coming with probability 1/16:

$$\begin{array}{cccc} \otimes\otimes\otimes\otimes & \otimes\otimes\otimes\odot & \otimes\otimes\odot\otimes & \otimes\otimes\odot\odot \\ \otimes\odot\otimes\otimes & \otimes\odot\otimes\odot & \otimes\odot\odot\otimes & \otimes\odot\odot\odot \\ \odot\otimes\otimes\otimes & \odot\otimes\otimes\odot & \odot\otimes\odot\otimes & \odot\otimes\odot\odot \\ \odot\odot\otimes\otimes & \odot\odot\otimes\odot & \odot\odot\odot\otimes & \odot\odot\odot\odot \end{array}$$

Regarding now the second assertion, we first have the following computation:

$$\begin{aligned}
P\left(3\otimes, 1\odot\right) &= P\left(\otimes\otimes\otimes\odot\right)+P\left(\otimes\otimes\odot\otimes\right)\\
&\quad +P\left(\otimes\odot\otimes\otimes\right)+P\left(\odot\otimes\otimes\otimes\right)\\
&= \frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}\\
&= \frac{1}{4}
\end{aligned}$$

Similarly, we have the following computation, for the balanced situation:

$$\begin{aligned}
&P\left(2\otimes, 2\odot\right)\\
= \;& P\left(\otimes\otimes\odot\odot\right)+P\left(\otimes\odot\otimes\odot\right)+P\left(\otimes\odot\odot\otimes\right)\\
&+P\left(\odot\otimes\otimes\odot\right)+P\left(\odot\otimes\odot\otimes\right)+P\left(\odot\odot\otimes\otimes\right)\\
= \;& \frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}\\
= \;& \frac{3}{8}
\end{aligned}$$

And then, for finishing our study, we have the following computation:

$$\begin{aligned}
P\left(1\otimes, 3\odot\right) &= P\left(\otimes\odot\odot\odot\right)+P\left(\odot\otimes\odot\odot\right)\\
&\quad +P\left(\odot\odot\otimes\odot\right)+P\left(\odot\odot\odot\otimes\right)\\
&= \frac{1}{16}+\frac{1}{16}+\frac{1}{16}+\frac{1}{16}\\
&= \frac{1}{4}
\end{aligned}$$

Finally, as a matter of making sure that we didn't mess with the various cases, let us make a doublecheck. The probability P for something to happen must be 1, and the sum of the numbers that we computed is indeed 1, as shown by the following computation:

$$\begin{aligned}
P &= P\left(4\otimes\right)+P\left(3\otimes, 1\odot\right)+P\left(2\otimes, 2\odot\right)\\
&\quad +P\left(1\otimes, 3\odot\right)+P\left(4\odot\right)\\
&= \frac{1}{16}+\frac{1}{4}+\frac{3}{8}+\frac{1}{4}+\frac{1}{16}\\
&= 1
\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

With a bit more work, we can solve the problem for n throws, as follows:

THEOREM 2.5. *When throwing a coin n times, the probabilities are*

$$\begin{array}{ccc}
\otimes\otimes\ldots\otimes\otimes \to \frac{1}{2^n} & , & \otimes\otimes\ldots\otimes\odot \to \frac{1}{2^n} \\
\otimes\otimes\ldots\odot\otimes \to \frac{1}{2^n} & , & \otimes\otimes\ldots\odot\odot \to \frac{1}{2^n} \\
\vdots & & \\
\odot\odot\ldots\otimes\otimes \to \frac{1}{2^n} & , & \odot\odot\ldots\otimes\odot \to \frac{1}{2^n} \\
\odot\odot\ldots\odot\otimes \to \frac{1}{2^n} & , & \odot\odot\ldots\odot\odot \to \frac{1}{2^n}
\end{array}$$

Alternatively, we have the following probabilities for what happens,

$$a\otimes b\odot \to \frac{1}{2^n}\binom{n}{a}$$

with $a+b=n$, when interested only in the final count of heads and tails.

PROOF. Observe first that this generalizes Propositions 2.2, 2.3 and 2.4, and in view of all the computations that we did there, you might probably expect something quite complicated, as a proof for this. However, by some magic, which is the magic of the binomial coefficients themselves, the whole thing is in fact trivial:

(1) Indeed, assuming $a+b=n$, in order to reach to the situation in the statement, namely a heads and b tails, we must select the a occurrences of heads, among the n total throws, and there are $\binom{n}{a}$ choices here, and then sum over these $\binom{n}{a}$ choices the common quantity $1/2^n$. Thus, formula in the statement proved, just like that.

(2) Next, observe that all this generalizes indeed the various computations in Propositions 2.2, 2.3 and 2.4, corresponding to the cases $n=2,3,4$, as follows:

$$n=2 \quad : \quad P\left(a\otimes\right)=\frac{1}{4}\binom{2}{a} \quad \to \quad \frac{1}{4},\frac{1}{2},\frac{1}{4}$$

$$n=3 \quad : \quad P\left(a\otimes\right)=\frac{1}{8}\binom{3}{a} \quad \to \quad \frac{1}{8},\frac{3}{8},\frac{3}{8},\frac{1}{8}$$

$$n=4 \quad : \quad P\left(a\otimes\right)=\frac{1}{16}\binom{4}{a} \quad \to \quad \frac{1}{16},\frac{1}{4},\frac{3}{8},\frac{1}{4},\frac{1}{16}$$

Here, for simplicity of notation, we chose not to record the number of tail occurrences, which is uniquely determined, given by the formula $b=n-a$, in each case.

(3) As a continuation of this, let us work out as well what happens at $n = 5, 6, 7$. We need here formulae for the binomial coefficients, and for this purpose, we can use the Pascal triangle from chapter 1, extended with two more rows, which looks as follows:

$$\begin{array}{c}
1\\
1\ ,\ 1\\
1\ ,\ 2\ ,\ 1\\
1\ ,\ 3\ ,\ 3\ ,\ 1\\
1\ ,\ 4\ ,\ 6\ ,\ 4\ ,\ 1\\
1\ ,\ 5\ ,\ 10\ ,\ 10\ ,\ 5\ ,\ 1\\
1\ ,\ 6\ ,\ 15\ ,\ 20\ ,\ 15\ ,\ 6\ ,\ 1\\
1\ ,\ 7\ ,\ 21\ ,\ 35\ ,\ 35\ ,\ 21\ ,\ 7\ ,\ 1\\
\vdots
\end{array}$$

We obtain the following probabilities, in relation with our coin game:

$$n = 5 \quad : \quad \frac{1}{32}\binom{5}{a} \quad \to \quad \frac{1}{32}\ ,\ \frac{5}{32}\ ,\ \frac{5}{16}\ ,\ \frac{5}{16}\ ,\ \frac{5}{32}\ ,\ \frac{1}{32}$$

$$n = 6 \quad : \quad \frac{1}{64}\binom{6}{a} \quad \to \quad \frac{1}{64}\ ,\ \frac{3}{32}\ ,\ \frac{15}{64}\ ,\ \frac{5}{16}\ ,\ \frac{15}{64}\ ,\ \frac{3}{32}\ ,\ \frac{1}{64}$$

$$n = 7 \ : \ \frac{1}{128}\binom{7}{a} \ \to \ \frac{1}{128}\ ,\ \frac{7}{128}\ ,\ \frac{21}{128}\ ,\ \frac{35}{128}\ ,\ \frac{35}{128}\ ,\ \frac{21}{128}\ ,\ \frac{7}{128}\ ,\ \frac{1}{128}$$

(4) Let us see as well what happens at $n = 8, 9, 10$. The next 3 rows of the Pascal triangle above, computed as usual by making sums, are as follows:

$$\begin{array}{c}
\vdots\\
1\ ,\ 8\ ,\ 28\ ,\ 56\ ,\ 70\ ,\ 56\ ,\ 28\ ,\ 8\ ,\ 1\\
1\ ,\ 9\ ,\ 36\ ,\ 84\ ,\ 126\ ,\ 126\ ,\ 84\ ,\ 36\ ,\ 9\ ,\ 1\\
1\ ,\ 10\ ,\ 45\ ,\ 120\ ,\ 210\ ,\ 252\ ,\ 210\ ,\ 120\ ,\ 45\ ,\ 10\ ,\ 1\\
\vdots
\end{array}$$

We obtain the following probabilities, in relation with our coin game:

$$n = 8 \quad : \quad \frac{1}{256}\ ,\ \frac{1}{32}\ ,\ \frac{7}{64}\ ,\ \frac{7}{32}\ ,\ \frac{35}{128}\ ,\ \frac{7}{32}\ ,\ \frac{7}{64}\ ,\ \frac{1}{32}\ ,\ \frac{1}{256}$$

$$n = 9 \quad : \quad \frac{1}{512}\ ,\ \frac{9}{512}\ ,\ \frac{9}{128}\ ,\ \frac{21}{128}\ ,\ \frac{63}{256}\ ,\ \frac{63}{256}\ ,\ \frac{21}{128}\ ,\ \frac{9}{128}\ ,\ \frac{9}{512}\ ,\ \frac{1}{512}$$

$$n = 10 \ : \ \frac{1}{1024}\ ,\ \frac{5}{512}\ ,\ \frac{45}{1024}\ ,\ \frac{15}{128}\ ,\ \frac{105}{512}\ ,\ \frac{63}{256}\ ,\ \frac{105}{512}\ ,\ \frac{15}{128}\ ,\ \frac{45}{1024}\ ,\ \frac{5}{512}\ ,\ \frac{1}{1024}$$

(5) Finally, for making sure that we have not messed up anything, let us check as well, as we did at the end of the proof of Proposition 2.4, that the total probability P, for something to happen, is 1. But this comes indeed from the binomial formula:

$$\begin{aligned}
P &= \sum_{a=0}^{n} P\left(a\bigotimes\right)\\
&= \sum_{a=0}^{n} \frac{1}{2^n}\binom{n}{a}\\
&= \frac{1}{2^n}\sum_{a=0}^{n} \binom{n}{a}1^a1^{n-a}\\
&= \frac{1}{2^n}(1+1)^n\\
&= 1
\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Very nice all this, we have here some good knowledge for dealing with coin throws. However, this is not the end of the story, because by can further build on the formula that we found in Theorem 2.5, with all sorts of more specialized formulae, and with some estimates too, then we can talk as well about biased coins, and finally we can, again based on what we have in Theorem 2.5, have an economics discussion, about this.

Thus, many things to be done. So, be patient, this will take some time.

Going first with what happens when throwing biased coins, we have the following straightforward generalization of Theorem 2.5, in this setting:

THEOREM 2.6. *Consider a biased coin, landing on heads and tails according to*

$$\bigotimes \to p \quad , \quad \bigodot \to 1-p$$

for some $p \in (0,1)$. When throwing this coin n times, the probabilities are

$$\mathrm{C} \to p^{\#(\bigotimes\in C)}(1-p)^{\#(\bigodot\in C)}$$

for any given configuration $C \in \{\bigotimes\ldots\bigotimes,\ldots,\bigodot\ldots\bigodot\}$. Alternatively, we have

$$a\bigotimes b\bigodot \to \binom{n}{a}p^a(1-p)^b$$

with $a+b=n$, when interested only in the final count of heads and tails.

PROOF. As mentioned above, this is a straightforward generalization of Theorem 2.5, which corresponds to the case $p = 1/2$, the details being as follows:

(1) The first assertion is clear. As for the second assertion, assuming $a+b=n$, in order to reach to the situation in the statement, namely a heads and b tails, we must select the a occurrences of heads, among the n total throws, and there are $\binom{n}{a}$ choices here, and then sum over these $\binom{n}{a}$ choices the common quantities $p^a(1-p)^b$.

(2) Thus, we are led to the formula in the statement, and as an illustration here, in the case $p=1/2$ we recover the formula from Theorem 2.5, as follows:

$$a\bigotimes b\bigodot\ \to\ \binom{n}{a}\frac{1}{2^a}\cdot\frac{1}{2^b}=\binom{n}{a}\frac{1}{2^n}$$

(3) Finally, for making sure that we have not messed up anything, let us check as well, as we did at the end of the proof of Theorem 2.5, that the total probability P, for something to happen, is 1. But this comes indeed from the binomial formula:

$$\begin{aligned}P&=\sum_{a=0}^{n}P\left(a\bigotimes\right)\\&=\sum_{a=0}^{n}\binom{n}{a}p^a(1-p)^{n-a}\\&=(p+1-p)^n\\&=1\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

And with the above result, discussion over, regarding the biased coins? Not really, because we can further complicate our game by throwing, one after another, n different biased coins. This leads to the following theoretical generalization of Theorem 2.6:

THEOREM 2.7. *Consider a sequence of n biased coins, landing according to*

$$\text{coin } i\quad :\quad \bigotimes\ \to\ p_i\quad ,\quad \bigodot\ \to\ 1-p_i$$

for some numbers $p_i\in(0,1)$. When throwing these n coins, the probabilities are

$$\text{C}\ \to\ \prod_{C_i=\bigotimes}p_i\prod_{C_i=\bigodot}(1-p_i)$$

for any given configuration $C\in\{\bigotimes\ldots\bigotimes,\ldots,\bigodot\ldots\bigodot\}$. Alternatively, we have

$$a\bigotimes b\bigodot\ \to\ \sum_{\#(\bigotimes\in C)=a}\left(\prod_{C_i=\bigotimes}p_i\prod_{C_i=\bigodot}(1-p_i)\right)$$

with $a+b=n$, when interested only in the final count of heads and tails.

PROOF. Obviously, this is something far too general and abstract, but on the bottom line, all this remains quite instructive, in order to get familiar with mathematical notation. Getting now to what the statement says, this is plainly trivial, once the notations understood, and end of the story. Finally, for pure mathematical pleasure, let us formally check as well that the total probability P, for something to happen, is 1. With some summing know-how, and familiarity with algebra, this can be done as follows:

$$\begin{aligned}
P &= \sum_{a=0}^{n} P\left(a\bigotimes\right)\\
&= \sum_{a=0}^{n}\sum_{\#(\bigotimes\in C)=a}\left(\prod_{C_i=\bigotimes}p_i\prod_{C_i=\bigodot}(1-p_i)\right)\\
&= \sum_{C}\left(\prod_{C_i=\bigotimes}p_i\prod_{C_i=\bigodot}(1-p_i)\right)\\
&= \sum_{C}\prod_{i}\left(p_i\delta_{C_i\bigotimes}+(1-p_i)\delta_{C_i\bigodot}\right)\\
&= (p_1+1-p_1)\ldots(p_n+1-p_n)\\
&= 1\times\ldots\times 1\\
&= 1
\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Summarizing, coins reasonably understood. As mentioned before, this is not the end of the story with them, and will be back to them on several occasions, in what follows.

2b. Rolling dice

Getting now to more formal work, based on this, we can answer our philosophical questions, in relation with Fact 2.1, and with probability in general, as follows:

DEFINITION 2.8. *The probability for an event E to happen is*

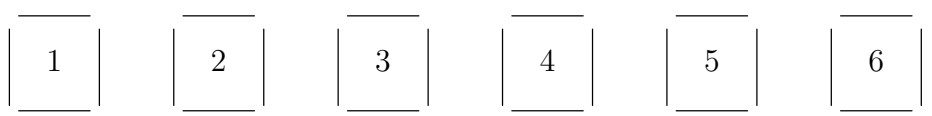
$$P(E)=\frac{\text{number of times } E \text{ happens}}{\text{total number of possibilities}}$$

and with this making Fact 2.1 into a mathematical theorem.

To be more precise, in what regards the above formula for $P(E)$, this is something which comes from Fact 2.1, Propositions 2.2, 2.3, 2.4 and Theorems 2.5, 2.6, 2.7, and from many other things that can be said, along these lines. And, with this definition $P(E)$ in hand, Fact 2.1 becomes a mathematical fact, or Theorem if you prefer.

We will be back to such things in chapter 4, with an even better axiomatization of probability theory, based on the above. For the moment, what we have will do.

Moving on, coming as a second class of examples of what we can do, which is more complicated than flipping coins, we can roll dice. Consider a usual, 6-faced die:



When throwing the die, the probabilities are obviously all equal, as follows:

$$P(1) = P(2) = P(3) = P(4) = P(5) = P(6) = \frac{1}{6}$$

Next, when throwing it twice, the probabilities are again equal, as follows:

$$P(1,1) = P(1,2) = \ldots = P(6,5) = P(6,6) = \frac{1}{36}$$

When throwing the die three times, the probabilities are again equal, as follows:

$$P(1,1,1) = P(1,1,2) = \ldots = P(6,6,5) = P(6,6,6) = \frac{1}{216}$$

And so on. In order now to have some mathematics going, let us look at the possible patterns that can occur. When throwing the die twice, the result is as follows:

PROPOSITION 2.9. *When throwing the die twice, the probabilities are*

$$P(11) = \ldots = P(66) = \frac{1}{36}$$

$$P(12) = \ldots = P(56) = \frac{1}{18}$$

with the first formula dealing with 6 *cases, and the second formula, with* 15 *cases.*

PROOF. This is standard counting, based on Definition 2.8. Indeed:

(1) There are 6 possible configurations of type aa, namely those coming from $a = 1, \ldots, 6$, and for each of these, the probability of getting it is obviously $1/36$.

(2) As for the other configurations, of type ab with $a \neq b$, there are $\binom{6}{2} = 15$ of them, and for each of these, the probability of getting it is $2/36 = 1/18$.

(3) Finally, in order to make sure that we didn't mess up anything, let us ckeck, as usual, that the total probability is indeed 1. But this comes from:

$$P = \frac{6}{36} + \frac{15}{18} = \frac{1}{6} + \frac{5}{6} = 1$$

Thus, our computations are indeed correct, and doublechecked, as desired. □

Next, when throwing the die three times, the result is as follows:

PROPOSITION 2.10. *When throwing the die three times, the probabilities are*

$$P(111) = \ldots = P(666) = \frac{1}{216}$$

$$P(112) = \ldots = P(566) = \frac{1}{72}$$

$$P(123) = \ldots = P(456) = \frac{1}{36}$$

with these formulae dealing respectively with 6 *cases,* 30 *cases,* 20 *cases.*

PROOF. This is again standard counting, based on Definition 2.8. Indeed:

(1) There are 6 possible configurations of type aaa, namely those coming from $a = 1, \ldots, 6$, and for each of these, the probability of getting it is obviously $1/216$.

(2) Next, we have the configurations of type aab, with $a \neq b$. There are $6 \cdot 5 = 30$ of these, and for each of them, the probability of getting it is $3/216 = 1/72$.

(3) And finally, we have the configurations of type abc, with a, b, c distinct. There are $\binom{6}{3} = 20$ of these, and for each of them, the probability of getting it is $6/216 = 1/36$.

(4) As usual in such situations, in order to make sure that we didn't mess up anything, let us ckeck that the total probability is indeed 1. But this comes from:

$$P = \frac{6}{216} + \frac{30}{72} + \frac{20}{36} = \frac{1}{36} + \frac{15}{36} + \frac{20}{36} = 1$$

Thus, our computations are indeed correct, and doublechecked, as desired. □

Shall we do one more computation, for four throws? Here the result is as follows:

PROPOSITION 2.11. *When throwing the die four times, the probabilities are*

$$P(1111) = \ldots = P(6666) = \frac{1}{1296}$$

$$P(1112) = \ldots = P(5666) = \frac{1}{324}$$

$$P(1122) = \ldots = P(5566) = \frac{1}{216}$$

$$P(1123) = \ldots = P(4566) = \frac{1}{108}$$

$$P(1234) = \ldots = P(3456) = \frac{1}{54}$$

with these formulae dealing with 6 *cases,* 30 *cases,* 15 *cases,* 60 *cases,* 15 *cases.*

PROOF. This is again standard counting, based on Definition 2.8. Indeed:

(1) There are 6 possible configurations of type $aaaa$, namely those coming from $a = 1, \ldots, 6$, and for each of these, the probability of getting it is obviously $1/1296$.

(2) Next, we have the configurations of type $aaab$, with $a \neq b$. There are $6 \cdot 5 = 30$ of these, and for each of them, the probability of getting it is $4/1296 = 1/324$.

(3) Then, we have the configurations of type $aabb$, with $a \neq b$. There are $\binom{6}{2} = 15$ of these, and for each of them, the probability of getting it is $6/1296 = 1/216$.

(4) Then, we have the configurations of type $aabc$, with a, b, c distinct. There are $6\binom{5}{2} = 60$ of these, and for each of them, the probability of getting it is $12/1296 = 1/108$.

(5) Finally, we have the configurations of type $abcd$, with a, b, c, d distinct. There are $\binom{6}{4} = 15$ of these, and for each of them, the probability of getting it is $24/1296 = 1/54$.

(6) As usual in such situations, in order to make sure that we didn't mess up anything, let us ckeck that the total probability is indeed 1. But this comes from:

$$\begin{aligned} P &= \frac{6}{1296} + \frac{30}{324} + \frac{15}{216} + \frac{60}{108} + \frac{15}{54} \\ &= \frac{1}{216} + \frac{20}{216} + \frac{15}{216} + \frac{120}{216} + \frac{60}{216} \\ &= 1 \end{aligned}$$

Thus, our computations are indeed correct, and doublechecked, as desired. □

The problem is now, what to do with the above data. Which is not clear, so time I guess to disturb again the cat. And cat, after a big yawn, answers:

CAT 2.12. *Sir, you are most likely here into things of type*

$$\binom{n}{a_1 \ldots a_k} = \frac{n!}{a_1! \ldots a_k!}$$

with $a_1 + \ldots + a_k = n$, called multinomial coefficients.

Humm, quite interesting, so let us see if this works. And it looks like yes indeed, because in relation with our question we can now formulate, in the general case:

THEOREM 2.13. *When throwing a die n times, the probabilities are*

$$P(a_1 \times 1, \ldots, a_6 \times 6) = \frac{1}{6^n}\binom{n}{a_1 \ldots a_6}$$

with $a_1 + \ldots + a_6 = n$, with this generalizing our previous computations.

PROOF. Many things can be said here, the idea being as follows:

(1) To start with, the result as stated is quite clear, because the number of situations for getting $a_1 \times 1, \ldots, a_6 \times 6$ after throwing our die n times is:

$$\begin{aligned} N &= \binom{n}{a_1}\binom{n-a_1}{a_2}\binom{n-a_1-a_2}{a_3}\ldots\ldots \\ &= \frac{n!}{a_1!(n-a_1)!}\cdot\frac{(n-a_1)!}{a_2!(n-a_1-a_2)!}\cdot\frac{(n-a_1-a_2)!}{a_3!(n-a_1-a_2-a_3)!}\ldots\ldots \\ &= \frac{n!}{a_1!\ldots a_6!} \\ &= \binom{n}{a_1\ldots a_6} \end{aligned}$$

Thus, when dividing by the total number of possibilities, 6^n, we get our formula.

(2) Next, as a routine doublecheck, the total probability is indeed 1, as shown by:

$$\begin{aligned} P &= \sum_{a_1+\ldots+a_6=n}\frac{1}{6^n}\binom{n}{a_1\ldots a_6} \\ &= \frac{1}{6^n}\sum_{a_1+\ldots+a_6=n}\binom{n}{a_1\ldots a_6}1^{a_1}\ldots 1^{a_6} \\ &= \frac{1}{6^n}(1+1+1+1+1+1)^n \\ &= \frac{1}{6^n}\cdot 6^n \\ &= 1 \end{aligned}$$

Here I used the multinomial formula, coming as a generalization of the binomial formula from chapter 1, and whose proof is straightforward, based on that, namely:

$$(x_1+\ldots+x_k)^n=\sum_{a_1+\ldots+a_k=n}\binom{n}{a_1\ldots a_k}x_1^{a_1}\ldots x_k^{a_k}$$

(3) Finally, in relation with what we had in Propositions 2.9, 2.10 and 2.11, the probabilities there coincide with those here. Indeed, at $n=2$ the present result reads:

$$P(11)=\frac{1}{36}\binom{2}{2\ 0\ 0\ 0\ 0\ 0}=\frac{1}{36}\cdot 1=\frac{1}{36}$$

$$P(12)=\frac{1}{36}\binom{2}{1\ 1\ 0\ 0\ 0\ 0}=\frac{1}{36}\cdot 2=\frac{1}{18}$$

Next, at $n = 3$ the present result gives the formulae in Proposition 2.10:

$$P(111) = \frac{1}{216}\binom{3}{3\ 0\ 0\ 0\ 0\ 0} = \frac{1}{216} \cdot 1 = \frac{1}{216}$$

$$P(112) = \frac{1}{216}\binom{3}{2\ 1\ 0\ 0\ 0\ 0} = \frac{1}{216} \cdot 3 = \frac{1}{72}$$

$$P(123) = \frac{1}{216}\binom{3}{1\ 1\ 1\ 0\ 0\ 0} = \frac{1}{216} \cdot 6 = \frac{1}{36}$$

And finally, at $n = 4$ the present result gives the formulae in Proposition 2.11:

$$P(1111) = \frac{1}{1296}\binom{4}{4\ 0\ 0\ 0\ 0\ 0} = \frac{1}{1296} \cdot 1 = \frac{1}{1296}$$

$$P(1112) = \frac{1}{1296}\binom{4}{3\ 1\ 0\ 0\ 0\ 0} = \frac{1}{1296} \cdot 4 = \frac{1}{324}$$

$$P(1122) = \frac{1}{1296}\binom{4}{2\ 2\ 0\ 0\ 0\ 0} = \frac{1}{1296} \cdot 6 = \frac{1}{216}$$

$$P(1123) = \frac{1}{1296}\binom{4}{2\ 1\ 1\ 0\ 0\ 0} = \frac{1}{1296} \cdot 12 = \frac{1}{108}$$

$$P(1234) = \frac{1}{1296}\binom{4}{1\ 1\ 1\ 1\ 0\ 0} = \frac{1}{1296} \cdot 24 = \frac{1}{54}$$

Summarizing, everything on this subject fully understood. Thanks cat. □

2c. Further games

At a more advanced level, in order to find some work to do, for us mathematicians, we need to think of all this, as for the coins before, as being a game. When playing dice, it is customary to throw the die several times, and compute the sum, with of course the bigger the sum, the better. So, let us study this question. For two throws, we have:

PROPOSITION 2.14. *When throwing the die twice*

S	2	3	4	5	6	7	8	9	10	11	12
P	1/36	1/18	1/12	1/9	5/36	1/6	5/36	1/9	1/12	1/18	1/36

is your sum distribution.

PROOF. Since we have only two throws, we can draw the following self-explanatory table, for the outcome of these two throws, and the resulting sum:

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

At the level of possibilities for the various sums, this gives us the following table:

S	2	3	4	5	6	7	8	9	10	11	12
N	1	2	3	4	5	6	5	4	3	2	1

Now by dividing everything by 36, we are led to the table in the statement. □

When throwing the die three times, the result is more complicated, as follows:

THEOREM 2.15. *When throwing the die three times*

S	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
P	$\frac{1}{216}$	$\frac{1}{72}$	$\frac{1}{36}$	$\frac{5}{108}$	$\frac{5}{72}$	$\frac{7}{72}$	$\frac{25}{216}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{25}{216}$	$\frac{7}{72}$	$\frac{5}{72}$	$\frac{5}{108}$	$\frac{1}{36}$	$\frac{1}{72}$	$\frac{1}{216}$

is your sum distribution.

PROOF. We can use here Proposition 2.14, and more specifically, the S/N table from its proof. Indeed, when throwing the die a 3rd time, some of the possibilities appearing there will sum up, and we are led in this way to the following table:

S	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
N	1	1	1	1	1	1	2	3	4	5	6	5	4	3	2	1
		+2	+2	+2	+2	+2	+3	+4	+5	+6	+5	+4	+3	+2	+1	
			+3	+3	+3	+3	+4	+5	+6	+5	+4	+3	+2	+1		
				+4	+4	+4	+5	+6	+5	+4	+3	+2	+1			
					+5	+5	+6	+5	+4	+3	+2	+1				
						+6	+5	+4	+3	+2	+1					

And with this, almost done. By computing the sums, this S/N table is as follows:

S	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
N	1	3	6	10	15	21	25	27	27	25	21	15	10	6	3	1

Observe that we have not messed up anything, with our computations, because according to our table above, the total number of possibilities is, as it should:

$$2(1+3+6+10+15+21+25+27)=2\times 108=216$$

Now by dividing everything by 216, we are led to the table in the statement. □

For four and more throws, things looks quite complicated, and in the hope that we agree on this. In addition, bad luck, cat is gone, so I will have to ask instead the rat.

Speaking rat, this fellow is doing quite well these days, wearing a suit and tie, wondering where that money comes from. When asked about math, here is his take:

RAT 2.16. *When no longer in control, change the rule of the game. Most folks won't even notice, and cash will keep flowing.*

Humm, quite interesting all this, thanks rat. So, let us forget about the sum question above, maybe for later in this book, once we will know more things, and convene for the following new rules, for our die game, involving this time two partners:

RULES 2.17. *Rolling the die is played with the following rules:*

(1) *Every time it is* $1,2,3,4,5$*, your partner wins* \$1 *from you.*
(2) *And every time it is* 6*, you win* \$5 *from your partner.*

Which sounds like a nice game, and with the audience approving, unanimously, let us get now into this. We have the following result, regarding the outcome of the game:

THEOREM 2.18. *When rolling a die n times what you can win are quantities of type $6w-n$, with $w=0,1,\ldots,n$, with the probability for this to happen being:*

$$P(6w-n)=\frac{5^{n-w}}{6^n}\binom{n}{w}$$

Geometrically, your winning curve starts with probability $(5/6)^n$ of losing n, then increases, up to some point, and then decreases, up to probability $1/6^n$ of winning $5n$.

PROOF. There are several things going on here, the idea being as follows:

(1) When rolling the die n times, what will happen is that you will win w times and lose l times, with $n=w+l$. And in this situation, your profit will be, as stated:

$$\begin{aligned}\$ &= 5w-l\\ &= 5w-(n-w)\\ &= 6w-n\end{aligned}$$

(2) As for the probability for this to happen, this is the total number of possibilities for you to win w times, which is $5^{n-w}\binom{n}{w}$, because this amounts in choosing the w times when you will win, among n, then multiplying by 5^{n-w} possibilities, at places where your partner wins, and finally dividing by the total number of possibilities, which is 6^n:

$$P(6w-n)=\frac{5^{n-w}}{6^n}\binom{n}{w}$$

(3) Let us doublecheck all this. The sum of all probabilities involved is indeed 1:

$$\begin{aligned}\sum_{w=0}^{n}P(6w-n)&=\sum_{w=0}^{n}\frac{5^{n-w}}{6^n}\binom{n}{w}5^{n-w}\\&=\frac{1}{6^n}\sum_{w=0}^{n}\binom{n}{w}\\&=\frac{1}{6^n}\sum_{w=0}^{n}\binom{n}{w}1^w5^{n-w}\\&=\frac{1}{6^n}(1+5)^n\\&=\frac{1}{6^n}\times 6^n\\&=1\end{aligned}$$

(4) Let us triplecheck this as well. Obviously, Rules 2.17 do not favor you, nor your partner, so on average, you should win 0. And this is the case indeed, because:

$$\begin{aligned}\sum_{w=0}^{n}P(6w-n)\times(6w-n)&=\frac{1}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n}{w}(6w-n)\\&=\frac{1}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n}{w}5w-\frac{1}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n}{w}(n-w)\\&=\frac{5}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n}{w}w-\frac{1}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n}{w}(n-w)\\&=\frac{5n}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n-1}{w-1}-\frac{n}{6^n}\sum_{w=0}^{n}5^{n-w}\binom{n-1}{w}\\&=\frac{5n}{6^n}(1+5)^{n-1}-\frac{5n}{6^n}(1+5)^{n-1}\\&=0\end{aligned}$$

This last computation was hot, wasn't it, but in math, triplechecks are mandatory. In any case theorem proved, and the final conclusions in the statement are clear too. □

Quite interestingly, Theorem 2.18 is best seen, both at the level of the statement, and of the proof, from the viewpoint of your partner. Let us record this, as follows:

THEOREM 2.19. *When rolling a die n times what you can win are quantities of type $5n-6l$, with $l=0,1,\ldots,n$, with the probability for this to happen being:*

$$P(5n-6l)=\frac{5^l}{6^n}\binom{n}{l}$$

Geometrically, your winning curve starts with probability $(5/6)^n$ of losing n, then increases, up to some point, and then decreases, up to probability $1/6^n$ of winning $5n$.

PROOF. As before, when rolling the die n times, you will win w times and lose l times, with $n=w+l$. And in this situation, your profit will be, as stated:

$$\begin{aligned}\$ &= 5w-l\\ &= 5(n-l)-l\\ &= 5n-6l\end{aligned}$$

As for the rest, we already know all this from Theorem 2.18, but the point is that the proof of Theorem 2.18 becomes slightly simpler when using l instead of w. □

Summarizing, the mathematics of dice is quite similar to the mathematics of coins. We will be back to this, on a more systematic basis, in chapter 4 and afterwards.

2d. Strategy, outcome

As a continuation of the above material, we would like to end this chapter with some more games and philosophy, or perhaps with an introduction to economics. Let us start with something very basic, in relation with the coin game, as follows:

FACT 2.20. *The probability of winning when flipping a coin is $1/2$.*

Obvious you would say, but there are some subtleties here, even in this simplest possible probability question. The first thing is that I said "winning", like everyone says when it comes to flipping coins, but winning against whom?

So, this is a first subtlety. Flipping a coin is best regarded as being a game, with you choosing between heads and tails, let us say heads, then flipping the coin, and winning if heads. But now, that we talked about a game, you need a partner for your game. That is, you are not playing a game alone, but with someone else, who wins when it's tails.

Which brings us into a second question, winning what?

Many things can be said here, and with the ultimate answer being money, because this is what money is made for, for simplifying such things, transactions between humans. With this discussed, let us record now our findings, as follows:

CONCLUSION 2.21. *Flipping a coin is best regarded as being a game, between you and a partner, the rules being:*

(1) *Every time it is heads, you win* \$1 *from your partner.*
(2) *Every time it is tails, your partner wins* \$1 *from you.*

With this conclusion recorded, we can see now more clearly what is behind coin flipping. Obviously, all sorts of interesting things that we can explore, and we will do that, and with the main question, which is surely on everyone's mind, being:

QUESTION 2.22. *Who wins?*

So, let us study now this question. Thus is a matter of understanding how the game axiomatized in Conclusion 2.21 evolves over the time, taking into account the $1/2$ mathematics from Fact 2.20, and here are a few preliminary observations, about this:

PROPOSITION 2.23. *When flipping a coin k times, the following happen,*

(1) *The probability of you winning* $\$k$ *is* $1/2^k$.
(2) *The probability of you winning* $\$k-1$ *is* 0.
(3) *The probability of you winning* $\$k-2$ *is* $k/2^k$.
(4) *The probability of you winning* $\$k-3$ *is again* 0.
(5) *The probability of you winning* $\$k-4$ *is* $k(k-1)/2^{k+1}$.

and so on, with the probability increasing, up to the tie situation, and then decreasing.

PROOF. This follows indeed from some simple mathematics, as follows:

(1) You winning $\$k$ means you winning every time, over k attempts, so your probability here is $P=(1/2)\times\ldots\times(1/2)$, with k terms in the product, which reads $P=1/2^k$.

(2) The point here is that you cannot win $\$k-1$, exactly. Indeed, you must lose at least once, and so you profit will be $\leq(k-1)-1=k-2$.

(3) Here we have a similar computation as in (1). For winning $\$k-2$ you need to lose exactly once, and since there are k possibilities of losing exactly once, $P=k/2^k$.

(4) Here the situation is similar to that in (2). Indeed, for winning exactly $\$k-3$ you would certainly need to lose twice, so you profit will be $\leq(k-2)-2=k-4$.

(5) With the same reasoning as in (3), here you need to lose exactly twice, and since there are $k(k-1)/2$ possibilities of losing exactly twice, $P=k(k-1)/2^{k+1}$.

(6) Finally, regarding the last assertion, which is a bit informal, we will leave the clarification here, both statement and proof, to you, as an instructive exercise. □

Obviously, some interesting mathematics is going on here, that needs to be better understood. We have the following result, generalizing Proposition 2.23:

THEOREM 2.24. *When flipping a coin k times what you can win are quantities of type $\$k-2s$, with $s=0,1,\ldots,k$, with the probability for this to happen being:*

$$P(k-2s)=\frac{1}{2^k}\binom{k}{s}$$

Geometrically, your winning curve starts with probability $1/2^k$ of winning $-\$k$, then increases up to the tie situation, and then decreases, up to probability $1/2^k$ of winning $\$k$.

PROOF. All this is quite clear, by fine-tuning our various observations from Proposition 2.23 and its proof, the idea with this being as follows:

(1) To start with, the point is that, in order for you to win $k-s$ times and lose s times, over your k attempts, the number of possibilities is:

$$\binom{k}{s}=\frac{k!}{s!(k-s)!}$$

Thus, by dividing now by 2^k, which is the total number of possibilities, for the whole game, we are led to the probability in the statement, namely:

$$P(k-2s)=\frac{1}{2^k}\binom{k}{s}$$

(2) Shall we doublecheck this? Sure yes, doublecheking is the first thing to be done, when you come across a theorem, in your mathematics. As a first check, the sum of probabilities that we found should be 1, and 1 that is, as shown by:

$$\begin{aligned}\sum_{s=0}^{k}P(k-2s)&=\frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}\\&=\frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}1^s1^{k-s}\\&=\frac{1}{2^k}(1+1)^k\\&=\frac{1}{2^k}\times 2^k\\&=1\end{aligned}$$

(3) But shall we really trust this. Imagine for instance that you play your game for \$1000 instead of \$1 as basic gain, your life is obviously at stake, so all this is worth a second doublecheck, before being used in practice. So, as second doublecheck, let us verify that, on average, what you win is exactly \$0, which is something very intuitive, the game

itself obviously not favoring you, nor your partner. But this can be checked as follows:

$$\begin{aligned}
\sum_{s=0}^{k} P(k-2s)\times(k-2s) &= \frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}(k-2s)\\
&= \frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}s\\
&= \frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{t=0}^{k}\binom{k}{k-t}(k-t)\\
&= \frac{1}{2^k}\sum_{s=0}^{k}\binom{k}{s}(k-s)-\frac{1}{2^k}\sum_{t=0}^{k}\binom{k}{t}(k-t)\\
&= 0
\end{aligned}$$

Summarizing, we have a good theorem here, proved, doublechecked and triplechecked, as per the highest scientific standards, ready to be used in practice. □

With Theorem 2.24 in hand, we are somehow done with math, and time now to turn to Question 2.22. Let us first examine a more concrete question, namely:

QUESTION 2.25. *What and how do you win, depending on your strategy?*

However, this appears to be a bit of a bad question, at least in the context of our very simple flipping game, because you have not so many options for developing a strategy. To be more precise, the only thing that you can do, as strategy, is that of pulling off the game, once you won enough money. And even this is something debatable, because you pulling off at the moment of your choice assumes that the rules are biased, favoring you. So, well, let us do this, and reformulate our strategy question as follows:

QUESTION 2.26. *Assuming that the rules are biased, favoring you, by allowing you to pull off at any moment of your choice, what is your best strategy?*

And with this, we are now straight into popular mathematics, because everyone in a casino, or buying lottery tickets, or doing stocks or crypto in front of a computer, thinks about such things, and at a highest possible seriousness level. You won't mess up things with your own money, hardly won via hard daily labor, won't you.

In relation with this, the legend has it that what you have to do is to play and play, until you reached a sum of money that you fixed as objective in advance, say $100. Then you pull off, with the money in your pocket. Simple like that.

So, let us see how this works. To start with, this can only work, I mean just play and play, as indicated above, and you will certainly end up with $100 in your pocket, no

question about it. However, this might take some precious time t, and the mathematics, based on our formula in Theorem 2.24, shows that this time t is as follows:

Time spent playing	Probability to win
$t = 100$	$1/2^{100} = 0.000$
$t = 102$	$102/2^{102} = 0.000$
$t = 104$	$\binom{104}{2}/2^{104} = 0.000$
$t = 106$	$\binom{106}{3}/2^{106} = 0.000$
$t = 108$	$\binom{108}{4}/2^{108} = 0.000$
$t = 110$	$\binom{110}{5}/2^{110} = 0.000$
$\vdots$	$\vdots$

Which does not loook very good, hope you agree with me. Obviously, we are here into some sort of very abstract math, not corresponding to anything in the real life. So, in order to reach to something more reasonable, good moment to remember that:

FACT 2.27. *Time is money.*

In view of this, let us downgrade our ambitions, and only wish to win a modest \$10. Here we reach to a more reasonable winning scheme, as follows:

Time spent playing	Probability to win
$t = 10$	$1/2^{10} = 0.001$
$t = 12$	$12/2^{12} = 0.003$
$t = 14$	$\binom{14}{2}/2^{14} = 0.006$
$t = 16$	$\binom{16}{3}/2^{16} = 0.009$
$t = 18$	$\binom{18}{4}/2^{18} = 0.012$
$t = 20$	$\binom{20}{5}/2^{20} = 0.015$
$\vdots$	$\vdots$

However, this is still not interesting, financially speaking, so in order to reach to something more viable, let us further downgrade our ambitions, and only wish to win a very modest \$5. And here, we reach to something more attractive, as follows:

Time spent playing	Probability to win
$t = 5$	$1/2^5 = 0.031$
$t = 7$	$7/2^7 = 0.055$
$t = 9$	$\binom{9}{2}/2^9 = 0.070$
$t = 11$	$\binom{11}{3}/2^{11} = 0.081$
$t = 13$	$\binom{13}{4}/2^{13} = 0.087$
$t = 15$	$\binom{15}{5}/2^{15} = 0.092$
$\vdots$	$\vdots$

But this still does not look very good, so going now for the true way of reason, let us simply wish to win a tiny \$3. And here, the situation becomes as follows:

Time spent playing	Probability to win
$t = 3$	$1/2^3 = 0.125$
$t = 5$	$5/2^5 = 0.156$
$t = 7$	$\binom{7}{2}/2^7 = 0.164$
$t = 9$	$\binom{9}{3}/2^9 = 0.164$
$t = 11$	$\binom{11}{4}/2^{11} = 0.163$
$t = 13$	$\binom{13}{5}/2^{13} = 0.157$
$\vdots$	$\vdots$

Which is sort of reasonable, but not really, observe for instance that the probabilities on the right start decreasing, and before putting this scheme into practice, we must probably do some more math, make sure that these probabilities won't start to decrease very sharply, which might complicate our business, and so on.

Moving ahead now, we talked in the above about "time is money", which is something that must be taken into account, but thinking well, what really matters in all this is the maximum amount of money that you can afford to lose.

Which is something quite subtle, not included in our modeling above. So, let us further reformulate our strategy question, by making it more realistic, in touch with what happens in the real life, as follows:

QUESTION 2.28. *What is your best strategy, assuming that the game is asymmetric:*

(1) *With the rules being biased, favoring you, by allowing you to pull off from the game, at any moment of your choice.*
(2) *With the capital being unequal, favoring your partner, who has N money that he can afford to lose, compared to your $n < N$ money.*
(3) *And perhaps with a fee for playing the game too, again favoring your partner, to be paid by you, and this because N, n are normally secret.*

And good news, this is the good, final question, which perfectly makes sense, and is fully realistic. There is some math to be done here, and getting started with this, we can solve a simple case right away, namely that when your partner has endless money:

$$N = \infty$$

A player having this feature is called "the bank", and with this convention made, the answer to our various questions, and notably to Question 2.22 that we started with, is:

ANSWER 2.29. *The bank wins.*

To be more precise here, as already mentioned, we can certainly do some math here, and we will do this later. But, for our purposes now, the simplest is to argue that, in your situation, when you have $\$n$ and you lose $\$n$, say with $n = 1,000,000$ for having a precise figure, you are dead, say with this coming from drug overdose, after reaching the street, after your bankruptcy. So, your strategy of pulling off once you won a precise sum of money, say \$100, is certainly flawed, because you can meet death on the way:

Time spent playing	Probability to win	Other outcomes
$t = 100$	small	losing
$t = 102$	small	losing
$t = 104$	small	losing
$\vdots$	$\vdots$	$\vdots$
$t = 1,000,000$	attractive	death
$t = 1,000,002$	attractive	death
$t = 1,000,004$	attractive	death
$\vdots$	$\vdots$	$\vdots$

As for the variations of this strategy, these can be certainly investigated too, but it is quite clear that all this will not lead to anything good, because originally you were there happy, looking for a strategy for winning the game, but all of the sudden, the rule (2) from Question 2.28 puts you in a very defensive situation, more caring about your life, than of winning the game. So, it is pretty much clear that we are led to Answer 2.29.

2e. Exercises

This was a basic introduction to probability, and as exercises, we have:

EXERCISE 2.30. *Do more computations for biased coins.*

EXERCISE 2.31. *Do some computations for biased dice too.*

EXERCISE 2.32. *Do more computations for dice thrown several times.*

EXERCISE 2.33. *Do some computations for biased dice thrown several times.*

EXERCISE 2.34. *Do some computations as well for the Russian roulette.*

EXERCISE 2.35. *Do some computations for some basic card games too.*

EXERCISE 2.36. *Further meditate on what we said, about money and banks.*

EXERCISE 2.37. *Find around you and do some other basic probability computations.*

As bonus exercise, complementary to our math, start reading some social science too.

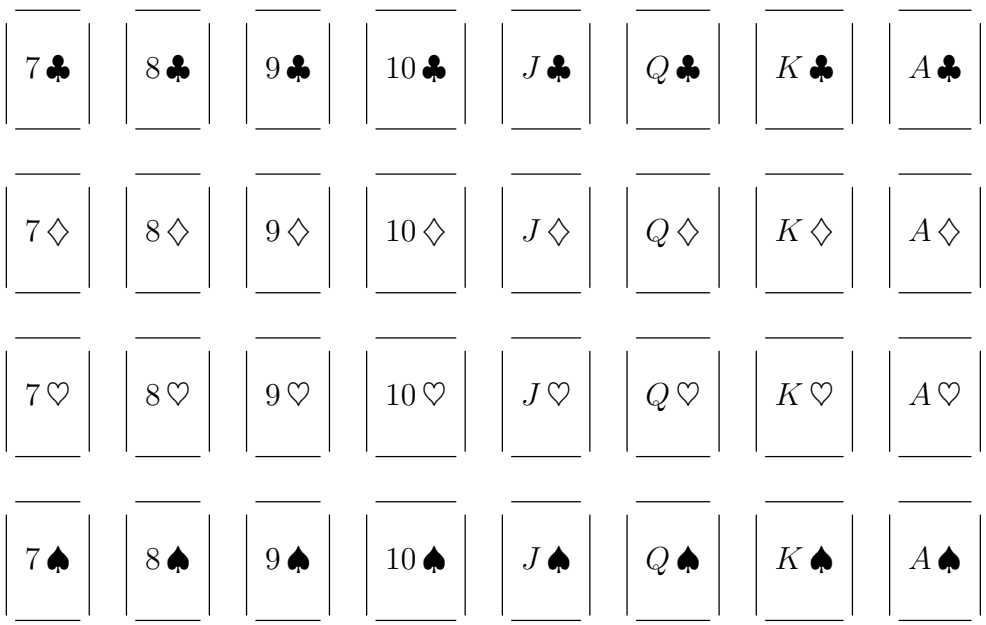
CHAPTER 3

Cards, poker

3a. Playing poker

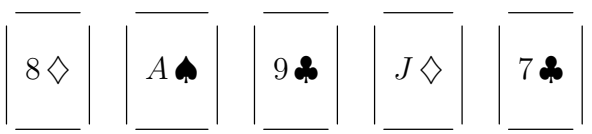
At a more advanced level now, getting to really serious stuff, which really matters in real life, we can play cards. We will be interested in the game of poker, played with the old rules. In order to explain the conventions of the game, let us start with:

DEFINITION 3.1. *We play poker with a deck of* 32 *cards, Wild West style*



with everything else being ruled out, as being modernity.

And make sure that you bring a loaded gun too, for dealing with the cheaters. Getting now to the game itself, at the beginning you get 5 cards from the deck, randomly drawn. Typically, with your hand will be something like this, just 5 random cards:



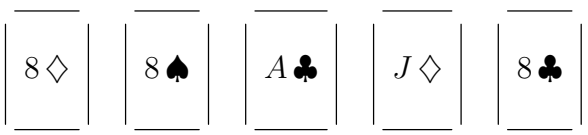
This particular hand does not look very good, with no coincidences or other interesting patterns appearing. However, if you are a bit lucky, you might have a pair:

$\leftarrow$ *one pair*

If you are even luckier, you might have two pairs, say as follows:

$\leftarrow$ *two pairs*

Another interesting thing that can happen is to have three of a kind:

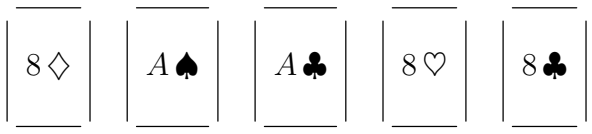


$\leftarrow$ *three of a kind*

Next, you can have a straight, which is something of the following type:

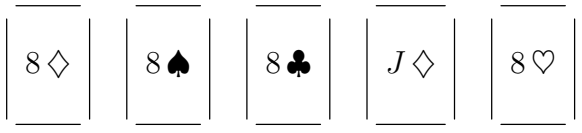
$\leftarrow$ *straight*

Even more remarkably, you can have a full house, with this meaning:



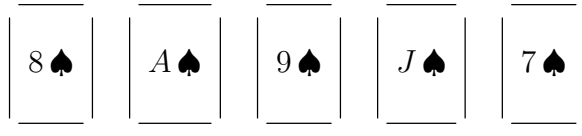
$\leftarrow$ *full house*

Next, and you might know this from movies, you can have four of a kind:



$\leftarrow$ *four of a kind*

But then, and you might know this from movies too, you might have a flush:



$\leftarrow$ *flush*

And finally, very rarely, even if you play much, you can have a straight flush:

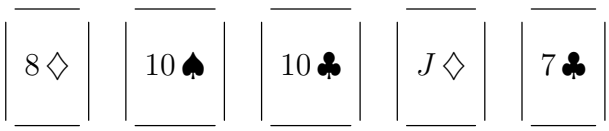
To summarize, the various coincidences and patterns in your hand can vary, and the convention is that these are valued according to the ordering above, as follows:

CONVENTION 3.2. *The various coincidences and patterns in your hand are valued as follows, in increasing order,*

(1) *One pair.*
(2) *Two pairs.*
(3) *Three of a kind.*
(4) *Straight.*
(5) *Full house.*
(6) *Four of a kind.*
(7) *Flush.*
(8) *Straight flush.*

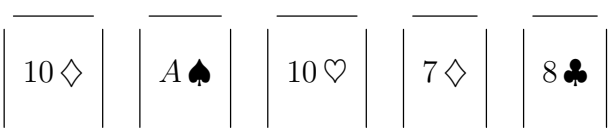
and with the precise figures and suits breaking the tie, in case that happens.

To be more precise here, in what regards the last rule, which is something more technical, assume for instance that you have a pair, as follows:



Now let us assume that one of your partners has a pair too, as follows:

Then you partner wins of course, because $A > 10$. However, the story is not over here with the pairs, because your partner can have the same pair as you, say as follows:



In this case the rule is that the suits take over, with the usual convention here being $\clubsuit < \diamondsuit < \heartsuit < \spadesuit$. Thus, in the above situation, you win, because you have the $10\spadesuit$.

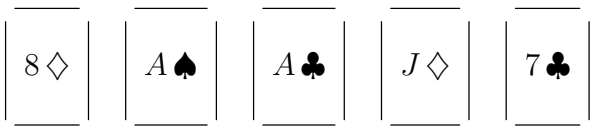
As for the comparison of the other things that can happen, again by using the convention $\clubsuit < \diamondsuit < \heartsuit < \spadesuit$, this can certainly be done, with some common sense, in a unique reasonable way, and I will leave it to you, to figure out the exact details here.

We are now ready to formulate the precise rules of the game, as follows:

RULES 3.3. *The game of poker is played as follows:*

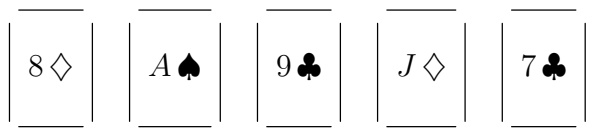
(1) *There are* 4 *players, and at the beginning, each one gets* 5 *cards.*
(2) *Then they bet, in cyclic order, each one putting some money on the table.*
(3) *Then they can exchange some cards, in the same cyclic order as before.*
(4) *Then they bet again, in the same cyclic order, until no one bets anymore.*
(5) *And then they show the cards, and the one having the best cards takes the money.*

As you can see, there are two things going on here, namely betting, and exchanging of cards. Leaving the betting for later, let us try to understand the exchanging of cards. Assume for instance that your initial hand was a pair, say as follows:



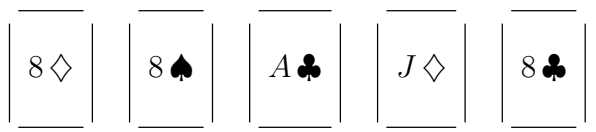
It is then a no-brainer to keep the aces, and exchange the other 3 cards, with the hope in mind of reaching to two pairs, or three of a kind, or a full house, or four of a kind.

As another common situation that can appear, assume that you have nothing:



In this case the standard thing is to keep the ace and the jack, and exchange the other 3 cards, again in the hope of something better. Of course you can exchange if you want the jack too, and even the ace, but this won't be very clever, because your partners will know in this way that you had nothing, to start with, and as always, silence is golden.

Finally, in case your intial hand is something interesting, you will certainly have to exchange < 3 cards, not to destroy that configuration, and in this process, unfortunately, communicate information about you hand. However, you can trick a bit here. Assume for instance that what you have initially are three of a kind, as follows:



Common sense would dictate to exchange the ace and the jack, in hope for a full house, or four of the kind. However, reaching to a full house, or to four of the kind, remains something rare, so instead, you can simply keep your hand, and this in order to fool you partners, making them believe that you have a straight, or a full house. Up to you.

In short, you get it, Rules 3.3 allow for a lot of tricks, and strategy.

With this discussed, time now for some math? As a first job, let us try to understand what happens when drawing the initial 5 cards, out of the deck of 32 cards. The result here, which is certainly within our reach, coming by counting, is as follows:

THEOREM 3.4. *The probabilities at poker are as follows:*

(1) *One pair:* 0.53392.
(2) *Two pairs:* 0.12013.
(3) *Three of a kind:* 0.05339.
(4) *Straight:* 0.02026.
(5) *Full house:* 0.00667.
(6) *Four of a kind:* 0.00111.
(7) *Flush:* 0.00103.
(8) *Straight flush:* 0.00007.

PROOF. Let us consider indeed our deck of 32 cards:

$$\{7,8,9,10,J,Q,K,A\}\times\{\clubsuit,\diamondsuit,\heartsuit,\spadesuit\}$$

The total number of possibilities for a poker hand is:

$$\binom{32}{5}=\frac{32\cdot 31\cdot 30\cdot 29\cdot 28}{2\cdot 3\cdot 4\cdot 5}=32\cdot 31\cdot 29\cdot 7$$

(1) For having a pair, we first have to choose the figure of that pair, and there are $\binom{8}{1}=8$ choices here. Then we have to choose the colors of that pair, and there are $\binom{4}{2}=6$ choices here. Next, we have to choose the figures of the remaining 3 cards, and there are $\binom{7}{3}=35$ choices here. And finally, we have to choose the colors of that remaining 3 cards, and there are $\binom{4}{1}^3=64$ choices here. Thus, the total number of possibilities is:

$$N=\binom{8}{1}\binom{4}{2}\times\binom{7}{3}\binom{4}{1}^3=8\cdot 6\cdot 35\cdot 64$$

Thus, the probability of having a pair is:

$$P=\frac{8\cdot 6\cdot 35\cdot 64}{32\cdot 31\cdot 29\cdot 7}=\frac{6\cdot 5\cdot 16}{31\cdot 29}=\frac{480}{899}=0.53392$$

(2) For having two pairs, we first have to choose the figures of that two pairs, and there are $\binom{8}{2}=28$ choices here. Then we have to choose the colors of that two pairs, and

there are $\binom{4}{2}^2 = 36$ choices here. And finally, we have to choose the remaining card, and there are $\binom{24}{1} = 24$ choices here. Thus, the total number of possibilities is:

$$N = \binom{8}{2}\binom{4}{2}^2 \times \binom{24}{1} = 28 \cdot 36 \cdot 24$$

Thus, the probability of having two pairs is:

$$P = \frac{28 \cdot 36 \cdot 24}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{36 \cdot 3}{31 \cdot 29} = \frac{108}{899} = 0.12013$$

(3) For having three of a kind, first have to choose the figure of that three of a kind cards, and there are $\binom{8}{1} = 8$ choices here. Then we have to choose the colors of that three of a kind cards, and there are $\binom{4}{3} = 4$ choices here. Next, we have to choose the figures of the remaining 2 cards, and there are $\binom{7}{2} = 21$ choices here. And finally, we have to choose the colors of that remaining 2 cards, and there are $\binom{4}{1}^2 = 16$ choices here. Thus, the total number of possibilities is:

$$N = \binom{8}{1}\binom{4}{3} \times \binom{7}{2}\binom{4}{1}^2 = 8 \cdot 4 \cdot 21 \cdot 16$$

Thus, the probability of having three of a kind is:

$$P = \frac{8 \cdot 4 \cdot 21 \cdot 16}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{3 \cdot 16}{31 \cdot 29} = \frac{48}{899} = 0.05339$$

(4) For having a straight, we first have to choose the type of straight that we get, and with the lowest card being one of $7, 8, 9, 10$, we have 4 choices here. Then, we have to choose the colors of our 5 cards, and there are $\binom{4}{1}^5 = 1024$ choices here, but with 4 of these, namely $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$ everywhere, leading to a straight flush, we have in fact only $\binom{4}{1}^5 - 4 = 1020$ choices. Thus, the total number of possibilities is:

$$N = 4\left[\binom{4}{1}^5 - 4\right] = 4 \cdot 1020$$

Thus, the probability of having a straight is:

$$P = \frac{4 \cdot 1020}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{255}{2 \cdot 31 \cdot 29 \cdot 7} = \frac{255}{12586} = 0.02026$$

(5) For having full house, that is, three of a kind plus a pair, first have to choose the figure of the three of a kind cards, and there are $\binom{8}{1} = 8$ choices here. Then we have to choose the colors of that three of a kind cards, and there are $\binom{4}{3} = 4$ choices here. Next, we have to choose the figure of the remaining pair, and there are $\binom{7}{1} = 7$ choices here.

And finally, we have to choose the colors of that remaining pair, and there are $\binom{4}{2} = 6$ choices here. Thus, the total number of possibilities is:

$$N = \binom{8}{1}\binom{4}{3} \times \binom{7}{1}\binom{4}{2} = 8 \cdot 4 \cdot 7 \cdot 6$$

Thus, the probability of having full house is:

$$P = \frac{8 \cdot 4 \cdot 7 \cdot 6}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{6}{31 \cdot 29} = \frac{6}{899} = 0.00667$$

(6) For having four of a kind, we first have to choose the figure of that four of a kind cards, and there are $\binom{8}{1} = 8$ choices here. And then we have to choose the remaining card, and there are 28 choices here. Thus, the total number of possibilities is:

$$N = \binom{8}{1} \times 28 = 8 \cdot 28$$

Thus, the probability of having four of a kind is:

$$P = \frac{8 \cdot 28}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{31 \cdot 29} = \frac{1}{899} = 0.00111$$

(7) For having a flush, we first have to choose the type of flush that we get, namely $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$, and there are 4 choices here. Then we have to choose the figures of the 5 cards, and there are $\binom{8}{5} = 56$ choices here, but with 4 of these leading to a straight flush, we have in fact only $\binom{8}{5} - 4 = 52$ choices. Thus, the total number of possibilities is:

$$N = 4\left[\binom{8}{5} - 4\right] = 4 \cdot 52$$

Thus, the probability of having a flush is:

$$P = \frac{4 \cdot 52}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{13}{2 \cdot 31 \cdot 29 \cdot 7} = \frac{13}{12586} = 0.00103$$

(8) For having a straight flush, we first have to choose the type of straight that we get, starting at $7, 8, 9, 10$, and there are 4 choices here, and then the color of our cards, namely $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$, and 4 choices here too. Thus, the total number of possibilities is:

$$N = 4 \cdot 4$$

Thus, the probability of having a straight flush is:

$$P = \frac{4 \cdot 4}{32 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{2 \cdot 31 \cdot 29 \cdot 7} = \frac{1}{12586} = 0.00007$$

Thus, we have obtained the numbers in the statement. □

3b. Ordered hands

So far, so good, but you might argue, what if we model our problem as for our poker hand to be ordered, do we still get the same answer? In answer, sure yes, as shown by:

THEOREM 3.5. *The probabilities at poker, computed using ordered hands, are:*

(1) *One pair:* 0.53392.
(2) *Two pairs:* 0.12013.
(3) *Three of a kind:* 0.05339.
(4) *Straight:* 0.02026.
(5) *Full house:* 0.00667.
(6) *Four of a kind:* 0.00111.
(7) *Flush:* 0.00103.
(8) *Straight flush:* 0.00007.

PROOF. We already know all this, from Theorem 3.4, but it is instructive to do all these computations in detail, with this standing among others as a verification for Theorem 3.4. So, let us consider the deck of 32 cards:

$$\{7, 8, 9, 10, J, Q, K, A\} \times \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$$

The total number of possibilities for an ordered poker hand is then:

$$32 \cdot 31 \cdot 30 \cdot 29 \cdot 28$$

(1) For having a pair, we first have to choose the position of that pair, inside our ordered hand, and there are $\binom{5}{2} = 10$ choices here. Then we have to choose the cards of our hand, and ignoring the second card of the pair, this amounts in choosing 4 cards having different figures, and there are $32 \cdot 28 \cdot 24 \cdot 20$ choices. As for the second card of the pair, there are 3 choices for it. Thus, the total number of possibilities is:

$$N = 10 \cdot 32 \cdot 28 \cdot 24 \cdot 20 \cdot 3$$

Thus, the probability of having a pair is:

$$P = \frac{10 \cdot 32 \cdot 28 \cdot 24 \cdot 20 \cdot 3}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{24 \cdot 20}{31 \cdot 29} = \frac{480}{899} = 0.53392$$

(2) For having two pairs, we first have to choose the position of that two pairs, inside our ordered hand, and there are $5 \times 3 = 15$ choices here, coming from 5 choices for the position of the extra card, not belonging to the two pairs, and then 3 choices for the second card of the first pair. Then we have to choose the cards of our hand, and ignoring the second card of each pair, this amounts in choosing 3 cards having different figures, and there are $32 \cdot 28 \cdot 24$ choices. As for the second card of each pair, there are 3 choices for it, which makes it for $3 \times 3 = 9$ more choices. Thus, the number of possibilities is:

$$N = 15 \cdot 32 \cdot 28 \cdot 24 \cdot 9$$

Thus, the probability of having two pairs is:

$$P = \frac{15 \cdot 32 \cdot 28 \cdot 24 \cdot 9}{32 \cdot 31 \cdot 30 \cdot 29\dot{2}8} = \frac{12 \cdot 9}{31 \cdot 29} = \frac{108}{899} = 0.12013$$

(3) For having three of a kind, we first have to choose the position of that three of a kind cards, inside our ordered hand, and there are $\binom{5}{3} = 10$ choices here. Then we have to choose the cards of our hand, and ignoring the second and third cards of our three of a kind cards, this amounts in choosing 3 cards having different figures, and there are $32 \cdot 28 \cdot 24$ choices. As for the second and third cards of our three of a kind cards, there are $3 \times 2 = 6$ choices here. Thus, the total number of possibilities is:

$$N = 10 \cdot 32 \cdot 28 \cdot 24 \cdot 6$$

Thus, the probability of having three of a kind is:

$$P = \frac{10 \cdot 32 \cdot 28 \cdot 24 \cdot 6}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{8 \cdot 6}{31 \cdot 29} = \frac{48}{899} = 0.05339$$

(4) For having a straight, we first have to choose the type of straight that we get, and with the lowest card being one of $7, 8, 9, 10$, we have 4 choices here. Then, we have to choose our cards, realizing this straight, and there are 20 choices for the 1st card, then 16 choices for the 2nd card, 12 choices for the 3rd card, 8 choices for the 4th card, and 4 choices for the 5th card, which leads to the following total number of possibilities:

$$N = 4 \cdot 20 \cdot 16 \cdot 12 \cdot 8 \cdot 4$$

However, some of these possibilities will lead to a straight flush. To be more precise, in order to have a straight flush, we must choose as before the type of straight that we get, and with the lowest card being one of $7, 8, 9, 10$, we have 4 choices here. Then we must choose the color of our cards, among $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$, and there are 4 choices here. And finally, we must choose the cards realizing our straight flush, and there are $5 \cdot 4 \cdot 3 \cdot 2$ choices here. Thus, the total number of possibilities for a straight flush is:

$$N' = 4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2$$

We conclude that the number of possibilities for a usual straight is:

$$\begin{aligned} N'' &= N - N' \\ &= 4 \cdot 20 \cdot 16 \cdot 12 \cdot 8 \cdot 4 - 4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 16 \cdot 20 \cdot 6(16 \cdot 2 \cdot 8 - 1) \\ &= 16 \cdot 20 \cdot 6 \cdot 255 \end{aligned}$$

Thus, the probability of having a usual straight is:

$$P = \frac{16 \cdot 20 \cdot 6 \cdot 255}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{255}{31 \cdot 29 \cdot 14} = \frac{255}{12586} = 0.02026$$

(5) For having full house, we first have to choose the position of the pair, inside our ordered hand, and there are $\binom{5}{2} = 10$ choices here. Then we have to choose the cards of

our hand, and ignoring the second card the pair, and the second and third cards of the three of a kind cards, there are $32 \cdot 28$ choices here. As for the remaining cards, there are 3 choices for the second card of the pair, and then $3 \times 2 = 6$ choices for the second and third cards of the three of a kind cards, which makes it for a total of $3 \times 6 = 18$ more choices. Thus, the number of possibilities for having full house is:

$$N = 10 \cdot 32 \cdot 28 \cdot 18$$

Thus, the probability of having full house is:

$$P = \frac{10 \cdot 32 \cdot 28 \cdot 18}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{6}{31 \cdot 29} = \frac{6}{899} = 0.00667$$

(6) For having four of a kind, we first have to choose the position of the extra card, inside our ordered hand, and there are $\binom{5}{1} = 5$ choices here. Then we have to choose the cards of our hand, and ignoring the second, the third and the fourth cards of our four of a kind cards, we have $32 \cdot 28$ choices here. As for the remaining cards, there are $3 \times 2 \times 1 = 6$ choices here. Thus, the number of possibilities for having four of a kind is:

$$N = 5 \cdot 32 \cdot 28 \cdot 6$$

Thus, the probability of having four of a kind is:

$$P = \frac{5 \cdot 32 \cdot 28 \cdot 6}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{1}{31 \cdot 29} = \frac{1}{899} = 0.00111$$

(7) For having a flush, we first have to choose the type of flush that we get, namely $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$, and there are 4 choices here. Then we have to choose our 5 cards, realizing the flush, and there are $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$ choices here. Thus, the number of possibilities is:

$$N = 4 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4$$

However, some some of these will lead to a straight flush. To be more precise, as computed in the proof of (4), the number of possibilities for a straight flush is:

$$N' = 4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2$$

We conclude that the number of possibilities for a usual flush is:

$$\begin{aligned} N'' &= N - N' \\ &= 4 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 - 4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 16 \cdot 40(42 - 3) \\ &= 16 \cdot 40 \cdot 39 \end{aligned}$$

Thus, the probability of having a usual flush is:

$$P = \frac{16 \cdot 40 \cdot 39}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{13}{2 \cdot 31 \cdot 29 \cdot 7} = \frac{13}{12586} = 0.00103$$

(8) Finally, for having a straight flush, as explained in the proof of (4), we must choose the type of straight that we get, and with the lowest card being $7, 8, 9, 10$, we have

4 choices. Then we must choose the color of our cards, among $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$, and there are 4 choices here. And finally, we must choose the cards realizing our straight flush, and there are $5 \cdot 4 \cdot 3 \cdot 2$ choices here. Thus, the number of possibilities for a straight flush is:

$$N' = 4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2$$

We conclude that the probability of having a straight flush is:

$$P = \frac{4 \cdot 4 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{32 \cdot 31 \cdot 30 \cdot 29 \cdot 28} = \frac{1}{31 \cdot 29 \cdot 14} = \frac{1}{12586} = 0.00007$$

Thus, we have obtained the numbers in the statement. □

As a comment here, Theorem 3.4 is the same thing as Theorem 3.5, scientifically speaking, because the probabilities at poker are unique, corresponding to something happening in the real life, and our theorems compute these unique probabilities. Mathematically however, are Theorems 3.4 and 3.5 the same thing? This is something which is not very clear, and I will leave it to you, some further thinking at all this.

As a second comment, our computations above are just the beginning, in the mathematical study of the game of poker. As a continuation of this, we have:

QUESTIONS 3.6. *In relation with the mathematics of the game of poker:*

(1) *What are the probabilities after having nothing, and exchanging* 3 *cards?*
(2) *What about probabilities after having a pair, and exchanging* 3 *cards?*
(3) *What about more specialized probabilities, when aiming for a straight or flush?*
(4) *What are your final probabilities, after working out the best exchange strategy?*
(5) *And then, what about playing usually, with* 3 *partners, including betting issues?*

And good questions these are. Regarding (1), this is normally some standard mathematics, along the lines of what we did in the above, and with the figures being very close to those from Theorems 3.4 and 3.5, but not identical to these, for a variety of reasons. And, up to you to do some computations here, as an instructive exercise.

Regarding (2), this is something quite interesting, again standard mathematics, and with the figures being quite different from those from Theorem 3.4 and 3.5, for instance with the probability of ending up with three of a kind being substantially higher, and with the same going for full house. Again, good exercise that we have here.

Regarding (3), many things can be said here, and with this being again standard mathematics, and assuming all this discussed, with all computations done, having a nice list for (4) is certainly possible. And with this, you are ready to perfectly play poker alone, I mean getting the best out of original hand, via mathematics, and enjoying.

In what regards now (5), which gets us to the whole point, well, quite different business going on here. Indeed, while the poker game can be perfectly played alone, as explained

above, via some reasonably simple mathematics, when playing with a partner, or 2 partners, or 3 partners as the game is traditionally played, the mathematics obviously becomes far more complicated. And on top of this comes betting, which is again a complicated business. So, no way to really master such things, only via mathematics, and if you want to be good at it, practice, and practice again, that is the only possible advice.

3c. Exchanging cards

We would like to solve now Questions 3.6. Let us start with the first question there, namely, what are the probabilities after having nothing, and exchanging 3 cards?

As a first comment here, normally you can exchange as many cards as you want to, including all 5, but with a bit of strategy in mind, if you have nothing, it is better, and very standard, to exchange 3 cards only, in order to make believe your partners that you already have a pair, and with this not affecting much your final percentages.

As a second comment, assuming that you have nothing, and want to exchange 3 cards, you still have to choose what 2 cards to keep. A standard choice here is keeping two cards of the same color, with a flush attempt in mind, although keeping for instance A, K, regardless of the colors, which are certainly good cards, among others in view of a strong straight attempt, makes sense too. Thus, things a bit complicated here, and in view of this, we will not comment on this problem, at least for now, and also, we will do the various computations below by ignoring the straight and flush situations.

With these comments made, the answer to Question 3.6 (1) is as follows:

THEOREM 3.7. *The probabilities at poker, after having nothing, and exchanging* 3 *cards, and ignoring the straight and flush situations, are as follows:*

(1) *One pair:* 0.53538.
(2) *Two pairs:* 0.12000.
(3) *Three of a kind:* 0.04820.
(4) *Full house:* 0.00615.
(5) *Four of a kind:* 0.00068.
(6) *None of these:* 0.28957.

PROOF. Assume indeed that you have nothing, meaning that you have a hand of type $ABxyz$, with A, B, x, y, z distinct. You decide then to keep A, B, and exchange x, y, z, for 3 other cards from the remaining pack, which looks as follows:

$$AAA \quad , \quad BBB$$

$$xxx \quad , \quad yyy \quad , \quad zzz$$

$$aaaa \quad , \quad bbbb \quad , \quad cccc$$

The total number of possibilities for this exchange of 3 cards is then:

$$\binom{27}{3} = \frac{27 \cdot 26 \cdot 25}{6} = 9 \cdot 13 \cdot 25 = 2925$$

(1) For having a pair, several situations appear. The first situation is that of a pair of type AA, and so of a final hand of type $AB|A**$. In this case, we have 3 choices for the extra A card to be drawn, and then $\binom{21}{2} = 210$ choices for the extra cards $**$, but with $3\binom{3}{2} + 3\binom{4}{2} = 9 + 18$ of these latter choices corresponding to $* = *$, and so removed. Thus, the total number of situations for having a pair of type AA is:

$$\begin{aligned} N_{AA} &= 3\left[\binom{21}{2} - 3\binom{3}{2} - 3\binom{4}{2}\right] \\ &= 3(210 - 9 - 18) \\ &= 3 \cdot 183 \\ &= 549 \end{aligned}$$

Similarly, the total number of situations for having a pair of type BB is:

$$N_{BB} = 549$$

Next, the total number of situations for having pairs of type xx, yy, zz are as follows, with the 3 figure coming from selecting that pair, out of xxx, yyy, zzz available, and with $18 = 21 - 3$ being the number of possibilities for the remaining card:

$$N_{xx} = N_{yy} = N_{zz} = 3 \cdot 18 = 54$$

Finally, the total number of situations for having pairs of type aa, bb, cc are as follows, with the 6 figure coming from selecting that pair, out of $aaaa$, $bbbb$, $cccc$ available, and with $17 = 21 - 4$ being the number of possibilities for the remaining card:

$$N_{aa} = N_{bb} = N_{cc} = 6 \cdot 17 = 102$$

We can now finish. The number of total possibilities for having a pair is:

$$\begin{aligned} N &= N_{AA} + N_{BB} + N_{xx} + N_{yy} + N_{zz} + N_{aa} + N_{bb} + N_{cc} \\ &= 2 \cdot 549 + 3 \cdot 54 + 3 \cdot 102 \\ &= 1098 + 162 + 306 \\ &= 1566 \end{aligned}$$

We conclude that the probability of having a pair is:

$$P = \frac{1566}{2925} = 0.53538$$

(2) For having two pairs, again we have several situations. First we have the case of a hand of type $AB|AB*$, and the number of possibilities here is as follows, with the two

3 values coming from the choices of A, B, and with 21 coming from the choice of $*$:

$$N_{AB|AB*} = 3 \cdot 3 \cdot 21 = 189$$

Then, we have the case of a hand of type $AB|A**$, and the number of possibilities here is as follows, with the 3 value coming from the choice of the extra A card, and with $9 + 18 = 3 + 3 + 3 + 6 + 6 + 6$ coming from the choice of the extra $**$ cards:

$$N_{AB|A**} = 3(9 + 18) = 3 \cdot 27 = 81$$

Finally, we have hands of type $AB|B**$, and the number of possibilities here is:

$$N_{AB|B**} = 81$$

We can now finish. The number of total possibilities for having two pairs is:

$$N = 189 + 81 + 81 = 351$$

We conclude that the probability of having two pairs is:

$$P = \frac{351}{2925} = 0.12000$$

(3) For having three of a kind, the first situation that can appear is that of a final hand of type $AB|AA*$, with the number of possibilities here being as follows:

$$N_{AB|AA*} = 3 \cdot 21 = 63$$

Next, we can have hands of type $AB|BB*$, the number of possibilities here being:

$$N_{AB|AA*} = 63$$

Finally, we can have hands of type $AB|***$, the number of possibilities here being:

$$N_{AB|***} = 1 + 1 + 1 + 4 + 4 + 4 = 15$$

We can now finish. The number of total possibilities for having three of a kind is:

$$N = 63 + 63 + 15 = 141$$

We conclude that the probability of having three of a kind is:

$$P = \frac{141}{2925} = 0.04820$$

(4) For having full house, the first situation that can appear is that of a final hand of type $AB|AAB$, with the number of possibilities here being as follows:

$$N_{AB|AAB} = 3 \cdot 3 = 9$$

We can have as well hands of type $AB|ABB$, the number of possibilities here being:

$$N_{AB|ABB} = 9$$

Thus, the number of total possibilities for having full house is:

$$N = 9 + 9 = 18$$

We conclude that the probability of having full house is:

$$P = \frac{18}{2925} = 0.00615$$

(5) For having four of a kind, the first situation that can appear is that of a final hand of type $AB|AAA$, with the number of possibilities here being as follows:

$$N_{AB|AAA} = 1$$

We can have as well hands of type $AB|BBB$, the number of possibilities here being:

$$N_{AB|BBB} = 1$$

Thus, the number of total possibilities for having four of a kind is:

$$N = 1 + 1 = 2$$

We conclude that the probability of having four of a kind is:

$$P = \frac{2}{2925} = 0.00068$$

(6) Summarizing, done with our computations, but as a matter of having a doublecheck for all this, via the standard fact that all probabilities must sum up to 1, let us compute as well the probability at the end, that of having nothing at all. This situation corresponds to a final hand of type $AB|pqr$, with p, q, r distinct, chosen among:

$$xxx \quad , \quad yyy \quad , \quad zzz$$

$$aaaa \quad , \quad bbbb \quad , \quad cccc$$

So, let us count these latter situations. First comes the case where the 3 cards drawn p, q, r are x, y, z, with the number of possibilities here being as follows:

$$N_{xyz} = 3 \cdot 3 \cdot 3 = 27$$

Next comes the case where the 3 cards drawn p, q, r are of type xya, with xy standing for xy, xz, yz, and a standing for a, b, c, with the number of possibilities here being:

$$N_{xya} = 3 \cdot 3 \cdot 3 \cdot 12 = 324$$

Next comes the case where the 3 cards drawn p, q, r are of type xab, with x standing for x, y, z, and ab standing for ab, ac, bc, with the number of possibilities here being:

$$N_{xab} = 9 \cdot 3 \cdot 4 \cdot 4 = 432$$

Finally, as a last situation, we have the case where the 3 cards drawn p, q, r are a, b, c, with the number of possibilities here being as follows:

$$N_{abc} = 4 \cdot 4 \cdot 4 = 64$$

Thus, the number of total possibilities for having nothing is:

$$N = 27 + 324 + 432 + 64 = 847$$

Observe that this makes it for our doublecheck, because the various possibilities counted in (1-5) above, plus this one, sum up to $\binom{27}{3} = 2925$, as they should:

$$1566 + 351 + 141 + 18 + 2 + 847 = 2925$$

Finally, in what concerns the probability of having nothing, this follows to be:

$$P = \frac{847}{2925} = 0.28957$$

Thus, we have obtained the numbers in the statement, as desired. □

As a next task, let us compare now what we found with the figures computed before. For this purpose, we must do one more computation, namely that of the probability of having nothing at all, in the context of the original draw, from before. The number of possibilities here can be computed by using the numbers found there, and is:

$$\begin{aligned} N &= N_{total} - N_{pair} - N_{pairs} - N_{three} - N_{full} - N_{four} \\ &= 201376 - 107520 - 24192 - 10752 - 1344 - 224 \\ &= 201376 - 144032 \\ &= 57344 \end{aligned}$$

Thus, the probability of having nothing, in the context of the original hand, is:

$$P = \frac{57344}{201376} = 0.28476$$

We can now do the comparison. We can see that, with respect to what we had before, most of the probabilities decrease, the situation being as follows:

$$\begin{aligned} \text{pair} &: 0.53392 < 0.53538 \\ \text{pairs} &: 0.12013 > 0.12000 \\ \text{three} &: 0.05339 > 0.04820 \\ \text{full} &: 0.00667 > 0.00615 \\ \text{four} &: 0.00111 > 0.00068 \\ \text{nothing} &: 0.28476 < 0.28957 \end{aligned}$$

And is this plausible, let us try now to quickly think at this. In answer, we can intuitively expect the probabilities to decrease, in what regards the two pairs, the three of a kind, the full house, and the four of a kind. Also, the probability of having nothing at all is intuitively supposed to increase. Thus, everything fine, expect for the situation with the pairs, where the probability, intuitively, is rather supposed to decrease.

However, this is wrong, because thinking well, what intuitively decreases, quite clearly, is rather the probability for having at least a pair. And with the probabilities for the two pairs, three of a kind, full house and four of a kind being all decreasing, by some magic

of the numbers, the probability of having exactly one pair might well increase, after all. And this is indeed the case, as shown by the above computations.

Summarizing, good work that we did. However, things are far from being over.

3d. More strategy

With this discussed, let us turn now to our next problem to be solved, namely Question 3.6 (2), asking for the probabilities after having a pair, and exchanging 3 cards.

We have here the following answer, which this time is complete, covering as well what happens in relation with the straight and flush situations, due to the fact that these two situations cannot appear, since we assumed that we have a pair:

THEOREM 3.8. *The probabilities at poker, after having a pair, and exchanging* 3 *cards, are as follows:*

(1) *One pair:* 0.53982.
(2) *Two pairs:* 0.24000.
(3) *Three of a kind:* 0.18256.
(4) *Full house:* 0.02905.
(5) *Four of a kind:* 0.00854.

PROOF. Assume indeed that you have a pair, meaning that you have a hand of type $AAxyz$, with A, x, y, z distinct. You decide then to keep the pair AA, and exchange x, y, z, for 3 other cards from the remaining pack, which looks as follows:

$$AA$$

$$xxx \quad , \quad yyy \quad , \quad zzz$$

$$aaaa \quad , \quad bbbb \quad , \quad cccc \quad , \quad dddd$$

The total number of possibilities for this exchange of 3 cards is then:

$$\binom{27}{3} = \frac{27 \cdot 26 \cdot 25}{6} = 9 \cdot 13 \cdot 25 = 2925$$

(1) For ending up with a pair, your final hand must be $AA|pqr$, with p, q, r chosen distinct, among the cards of type x, y, z and a, b, c, d. The first situation is that where the 3 cards drawn p, q, r are x, y, z, with the number of possibilities here being as follows:

$$N_{xyz} = 3 \cdot 3 \cdot 3 = 27$$

Next comes the case where the 3 cards drawn p, q, r are of type xya, with xy standing for xy, xz, yz, and a standing for a, b, c, d, with the number of possibilities here being:

$$N_{xya} = 3 \cdot 3 \cdot 3 \cdot 16 = 432$$

Next comes the case where p, q, r are of type xab, with x standing for x, y, z, and ab standing for ab, ac, ad, bc, bd, cd, with the number of possibilities here being:

$$N_{xab} = 9 \cdot \binom{4}{2} \cdot 4 \cdot 4 = 9 \cdot 6 \cdot 4 \cdot 4 = 864$$

Finally, as a last situation, we have the case where the 3 cards drawn p, q, r are distinct, among a, b, c, d, with the number of possibilities here being as follows:

$$N_{abc} = 4 \cdot 4 \cdot 4 \cdot 4 = 256$$

Thus, the number of total possibilities for ending up with a pair is:

$$N = 27 + 432 + 864 + 256 = 1579$$

We conclude that the probability for ending up with a pair is:

$$P = \frac{1579}{2925} = 0.53982$$

(2) For ending up with two pairs, again we have several situations. First we have the case of a final hand of type $AA|xxy$, with xy standing here for xy, yx, xz, zx, yz, zy, with the number of possibilities here being as follows:

$$N_{AA|xxy} = 6 \cdot 3 \cdot 3 = 54$$

Next, we have the case of a final hand of type $AA|xxa$, with x standing here for x, y, z, and a standing for a, b, c, d, with the number of possibilities here being as follows:

$$N_{AA|xxa} = 3 \cdot 3 \cdot 16 = 144$$

Then, we have the case of a hand of type $AA|xaa$, with x standing again for x, y, z, and a standing for a, b, c, d, with the number of possibilities here being as follows:

$$N_{AA|xaa} = 9 \cdot 4 \cdot \binom{4}{2} = 9 \cdot 4 \cdot 6 = 216$$

And finally, we have the case of a final hand of type $AA|aab$, with ab standing here for $ab, ba, ac, ca, ad, da, bc, cb, bd, db, cd, dc$, with the number of possibilities here being:

$$N_{AA|aab} = 12 \cdot \binom{4}{2} \cdot 4 = 12 \cdot 6 \cdot 4 = 288$$

Thus, the number of total possibilities for having two pairs is:

$$N = 54 + 144 + 216 + 288 = 702$$

We conclude that the probability of having two pairs is:

$$P = \frac{702}{2925} = 0.24000$$

(3) For having three of a kind, the only situation that can appear is that of a final hand of type $AA|A**$, with the number of possibilities here being as follows:

$$\begin{aligned} N &= 2\left[\binom{25}{2} - 3\binom{3}{2} - 4\binom{4}{2}\right] \\ &= 2(25 \cdot 12 - 3 \cdot 3 - 4 \cdot 6) \\ &= 2(300 - 9 - 24) \\ &= 2 \cdot 267 \\ &= 534 \end{aligned}$$

Thus, the probability of having three of a kind is:

$$P = \frac{534}{2925} = 0.18256$$

(4) For having full house, the first situation that can appear is that of a final hand of type $AA|A**$, with the number of possibilities here being as follows:

$$\begin{aligned} N_{AA|A**} &= 2(3 + 3 + 3 + 6 + 6 + 6 + 6) \\ &= 2(9 + 24) \\ &= 2 \cdot 33 \\ &= 66 \end{aligned}$$

We can have as well hands of type $AA|***$, the number of possibilities here being:

$$N_{AA|***} = 1 + 1 + 1 + 4 + 4 + 4 + 4 = 19$$

Thus, the number of total possibilities for having full house is:

$$N = 66 + 19 = 85$$

We conclude that the probability of having full house is:

$$P = \frac{85}{2925} = 0.02905$$

(5) For having four of a kind, the only situation that can appear is that of a final hand of type $AA|AA*$, with the number of possibilities here being as follows:

$$N = 25$$

We conclude that the probability of having four of a kind is:

$$P = \frac{25}{2925} = 0.00854$$

(6) Finally, as a doublecheck, our figures sum indeed up to $\binom{27}{3} = 2925$:

$$1579 + 702 + 534 + 85 + 25 = 2925$$

Thus, we are led to the conclusions in the statement. □

Getting now towards Question 3.6 (3), before getting to problems regarding the straight and flush configurations, we have something more basic to be done, namely:

PROPOSITION 3.9. *The probabilities at poker, after having two pairs, and exchanging* 1 *card, are as follows:*

(1) *Two pairs:* 0.85185.
(2) *Full house:* 0.14814.

PROOF. Assume indeed that you have two pairs, meaning that you have a hand of type $AABBx$, with A, B, x distinct. You decide then to keep the two pairs $AABB$, and exchange x, for a remaining card in the pack. The winning situation is then that when that card is A, B, so you get a full house, and the number of possibilities here is:

$$N = 4$$

As for the total number of possibilities for this exchange of 1 card, this is 27. Thus, the probability for ending up with a full house is:

$$P = \frac{4}{27} = 0.14814$$

As for the losing probability, that of staying with two pairs, this is:

$$P = \frac{23}{27} = 0.85185$$

Thus, we are led to the conclusions in the statement. □

Along the same lines, we have as well the following result:

PROPOSITION 3.10. *The probabilities at poker, after having three of a kind, and exchanging* 2 *cards, are as follows:*

(1) *Three of a kind:* 0.82336.
(2) *Full house:* 0.10256.
(3) *Four of a kind:* 0.07407.

PROOF. Assume indeed that you have three of a kind, meaning that you have a hand of type $AAAxy$, with A, x, y distinct. You decide then to keep the cards AAA, and exchange x, y, for two remaining cards in the pack, which looks as follows:

$$A$$

$$xxx \quad , \quad yyy$$

$$aaaa \quad , \quad bbbb \quad , \quad cccc \quad , \quad dddd \quad , \quad eeee$$

The total number of possibilities for this exchange of 2 cards is then:

$$\binom{27}{2} = 27 \cdot 13 = 351$$

(1) For ending up with your initial three of a kind, the cards p, q that you receive must be distinct, and distinct from A. The total number of possibilities here is:

$$\begin{aligned} N &= \binom{26}{2} - 3 - 3 - 6 - 6 - 6 - 6 - 6 \\ &= 13 \cdot 25 - 6 - 30 \\ &= 325 - 36 \\ &= 289 \end{aligned}$$

Thus, the probability for ending up with your initial three of a kind is:

$$P = \frac{289}{351} = 0.82336$$

(2) For reaching to a full house, the cards p, q that you receive must be equal, and distinct from A. The total number of possibilities here is:

$$N = 3 + 3 + 6 + 6 + 6 + 6 + 6 = 36$$

Thus, the probability for ending up with a full house is:

$$P = \frac{36}{351} = 0.10256$$

(2) For reaching to four of the kind, the condition is that one of the cards p, q that you receive must be A. The total number of possibilities here is:

$$N = 26$$

Thus, the probability for ending up with four of a kind is:

$$P = \frac{26}{351} = 0.07407$$

Note in passing, as a verification for all this, now that we did the final computation, that the numbers that we computed sum up to $\binom{27}{2} = 351$, as they should:

$$289 + 36 + 26 = 351$$

Thus, we are led to the conclusions in the statement. □

Still with me I hope, after all these computations. It is of course possible to do some more, but thinking a bit, what we have is not that bad, and it is perhaps time to put everything together. Not that we will obtain our final result in this way, but at least we will have something interesting and 99% accurate to say, which can be used in practice.

So, by putting everything together, we obtain the following result, which basically teaches you how to perfectly play poker alone, and with the slight uncertainties coming from the straight and flush situations, which require some tricky choices when it comes to exchanging cards, that we have not analysed in depth, in the above:

THEOREM 3.11. *The probabilities at poker, after suitably exchanging cards, are approximately as follows:*

(1) *One pair:* 0.44067.
(2) *Two pairs:* 0.26464.
(3) *Three of a kind:* 0.05767.
(4) *Full house:* 0.02786.
(5) *Straight:* 0.02248.
(6) *Four of a kind:* 0.00961.
(7) *Flush:* 0.00114.
(8) *Straight flush:* 0.00007.

PROOF. This follows indeed from the various results that we have, from before and from here, via the usual rule "probabilities multiply", the details being as follows:

(1) A pair can come either by itself, and staying a pair after exchanging 3 cards, or by initially having nothing, exchanging 3 cards, and reaching in this way to a pair. Thus, with the probabilities multiplying, the corresponding probability is given by:

$$\begin{aligned} P &= 0.53392 \times 0.53982 + 0.28476 \times 0.53538 \\ &= 0.28822 + 0.15245 \\ &= 0.44067 \end{aligned}$$

(2) Two pairs can come either by themselves, and staying two pairs after exchanging 1 card, or by initially having nothing, exchanging 3 cards, and reaching in this way to two pairs, or by initially having one pair, exchanging 3 cards, and reaching in this way to two pairs. With probabilities multiplying, the corresponding probability is given by:

$$\begin{aligned} P &= 0.12013 \times 0.85185 + 0.28476 \times 0.12000 + 0.53392 \times 0.24000 \\ &= 0.10233 + 0.03417 + 0.12814 \\ &= 0.26464 \end{aligned}$$

(3) Three of a kind can come either by themselves, and staying three of a kind after exchanging 2 cards, or by initially having nothing, exchanging 3 cards, and reaching in this way to three of a kind, or by initially having one pair, exchanging 3 cards, and reaching in this way to three of a kind. The corresponding probability is given by:

$$\begin{aligned} P &= 0.05339 \times 0.82336 + 0.28476 \times 0.04820 + 0.53392 \times 0.18256 \\ &= 0.04395 + 0.01372 + 0.09747 \\ &= 0.05767 \end{aligned}$$

(4) A full house can come either by itself, or by initially having a pair, exchanging 3 cards, and reaching to a full house, or by initially having three of a kind, exchanging 2

cards, and reaching to a full house. The corresponding probability is given by:

$$\begin{aligned} P &= 0.00667 + 0.53392 \times 0.02905 + 0.05339 \times 0.10256 \\ &= 0.00667 + 0.01551 + 0.00568 \\ &= 0.02786 \end{aligned}$$

(5) Regarding the straight, we can expect here to have a slight increase in the figure from before, which was 0.02026. We will leave the study here for later.

(6) Four of a kind can come either by themselves, or by initially having a pair, exchanging 3 cards, and reaching to four of a kind, or by initially having three of a kind, exchanging 2 cards, and reaching to four of a kind. The corresponding probability is:

$$\begin{aligned} P &= 0.00111 + 0.53392 \times 0.00854 + 0.05339 \times 0.07407 \\ &= 0.00111 + 0.00455 + 0.00395 \\ &= 0.00961 \end{aligned}$$

(7) It remains to discuss the straight, the flush, and the straight flush, based on what we have. For this purpose, recall that the figures from before were as follows:

$$\begin{aligned} \text{straight} &: 0.02026 \\ \text{flush} &: 0.00103 \\ \text{straight flush} &: 0.00007 \end{aligned}$$

By adding these three figures, we obtain the following straight/flush total:

$$\text{total} : 0.02136$$

Our method in what follows, in the lack of a detailed study of the straight and flush situations, when exchanging cards, will be that of rescaling linearly all these quantities.

(8) For this purpose, let us first compare what we obtained in the above, with what we previously had from before. The situation here is as follows, very reasonable, with a decrease for the pair, a more than doubling for the two pairs, an increase for the three of a kind, and a substantial increases for the full house and four of a kind:

$$\begin{aligned} \text{pair} &: 0.53392 > 0.44067 \\ \text{pairs} &: 0.12013 < 0.26464 \\ \text{three} &: 0.05339 < 0.05767 \\ \text{full} &: 0.00667 < 0.02786 \\ \text{four} &: 0.00111 < 0.00961 \end{aligned}$$

At the level of the totals, and negated totals, the situation is as follows:

$$\begin{aligned} \text{total of these} &: 0.71522 < 0.80045 \\ \text{none of these} &: 0.28478 > 0.19955 \end{aligned}$$

Getting back now to our questions regarding the straight, the flush, and the straight flush, the above suggests, somehow, to perform a 11% increase to the figures from (7). Which is of course something very heuristic, but in the lack of anything better, we will just do this. We obtain in this way the following figures:

$$\begin{array}{rcl} \text{straight} & : & 0.02026 \to 0.02248 \\ \text{flush} & : & 0.00103 \to 0.00114 \\ \text{straight flush} & : & 0.00007 \to 0.00007 \end{array}$$

Thus, we are led to the conclusions in the statement. □

Many other things can be said about poker, as a continuation of the above. And with the remark of course that nothing can replace practicing. Lots of practicing.

3e. Exercises

Serious computations that we had in this chapter, and as exercises, we have:

EXERCISE 3.12. *Figure out the exact comparison rules, using* $\clubsuit < \diamondsuit < \heartsuit < \spadesuit$.

EXERCISE 3.13. *Further meditate on the relation between ordered and unordered.*

EXERCISE 3.14. *Does is make sense, statistically, to exchange* 4 *or* 5 *cards?*

EXERCISE 3.15. *What about exchanging* 4 *or* 5 *cards, with strategy in mind?*

EXERCISE 3.16. *Further meditate on that probability for pairs increasing.*

EXERCISE 3.17. *Clarify what happens for the straight and flush situations.*

EXERCISE 3.18. *Start doing some math, in relation with the initial betting.*

EXERCISE 3.19. *Then do as well some math, for the final betting.*

As bonus exercise, and no surprise here, find 3 fellows, and start playing.

CHAPTER 4

Basic probability

4a. Probability spaces

Welcome to probability, take two. Fun is over I guess, we played many interesting games, and learned many interesting things, but time now to get to more formal work, inspired from what we have so far, and mathematically axiomatize everything.

In answer, what we did so far suggests formulating the following definition:

DEFINITION 4.1. *A discrete probability space is a set X, usually finite or countable, whose elements $x \in X$ are called events, together with a function*

$$P : X \to [0, \infty)$$

called probability function, which is subject to the condition

$$\sum_{x \in X} P(x) = 1$$

telling us that the overall probability for something to happen is 1.

Which sounds quite neat, this is definitely a rigorous mathematical definition, that we can build our theory upon. Examples, making the link with the material from chapters 2-3, coming in a moment, but before that, two quick comments, in relation with this:

(1) As a first comment, our condition $\sum_{x \in X} P(x) = 1$ perfectly makes sense, and this even if X is uncountable, because the sum of positive numbers is always defined, as a number in $[0, \infty]$, and this no matter how many positive numbers we have.

(2) As a second comment, we have chosen in the above not to assume that X is finite or countable, and this for instance because we want to be able to regard any probability function on $\mathbb{N}$ as a probability function on $\mathbb{R}$, by setting $P(x) = 0$ for $x \notin \mathbb{N}$.

And more on such things, which can be a bit technical, at the end of the present section. Getting now to the material from chapters 2-3, as a first observation, our previous axiomatization of probability theory, from chapter 2, is compatible with Definition 4.1, and in fact gets fully rigorous, with Definition 4.1 added. Let us formulate indeed:

COMMENT 4.2. *Once we have a probability function $P : X \to [0, \infty)$ as above, we can compute what the probability for a set of events $Y \subset X$ to happen is, by setting*

$$P(Y) = \sum_{y \in Y} P(y)$$

and with this being compatible with what we have been doing before, namely "probability $P(Y)$ is the number of situations where Y happens, over total number of possibilities".

To be more precise here, what we have in the above is a formula for $P(Y)$, coming as a definition, based on Definition 4.1, and then a comment in relation with our previous work on probability, which remains to be justified, via examples and everything.

So, time now for examples? The basic examples will come of course from basic games, and at the beginning of everything, we certainly have the flipping of coins:

EXAMPLE 4.3. *Flipping coins.*

Here things are simple and clear, because when you flip a coin the corresponding discrete probability space, together with its probability measure, is as follows:

$$X = \big\{\text{heads, tails}\big\} \quad , \quad P(\text{heads}) = P(\text{tails}) = \frac{1}{2}$$

In the case where the coin is biased, as to land on heads with probability $2/3$, and on tails with probability $1/3$, the corresponding probability space is as follows:

$$X = \big\{\text{heads, tails}\big\} \quad , \quad P(\text{heads}) = \frac{2}{3} \quad , \quad P(\text{tails}) = \frac{1}{3}$$

More generally, given any number $p \in [0, 1]$, we have an abstract probability space as follows, where we have replaced heads and tails by win and lose:

$$X = \big\{\text{win, lose}\big\} \quad , \quad P(\text{win}) = p \quad , \quad P(\text{lose}) = 1 - p$$

Finally, things become more interesting when flipping a coin, biased or not, several times in a row. In the case of a biased coin, landing on heads with probability p_1 and on tails with probability $p_2 = 1 - p_2$, thrown n times, the probability space is:

$$X = \big\{1, 2\big\}^n \quad , \quad P(i_1 \ldots i_n) = p_{i_1} \ldots p_{i_n} \quad , \quad p_i \geq 0 \ , \ p_1 + p_2 = 1$$

Observe that, when formulating this, I changed my mind once again in what regards the exact designation of the elements of X. You might wonder why, and in answer, it is better to formulate things as above, using the familiar numbers 1,2, for a number of computations to be easier to write down. And, as an illustration here, let us check that the sum 1 condition in Definition 4.1 is indeed satisfied, and with this proving that our

coin modeling is bug-free. But this is the case indeed, as shown by:

$$\begin{aligned}\sum_{i\in X} P(i) &= \sum_{i_1,\ldots,i_n} P(i_1\ldots i_n)\\ &= \sum_{i_1,\ldots,i_n} p_{i_1}\ldots p_{i_n}\\ &= \sum_{i_1} p_{i_1}\ldots\sum_{i_n} p_{i_n}\\ &= 1\times\ldots\times 1\\ &= 1\end{aligned}$$

Summarizing, coins reasonably understood, or at least the mathematical formalism of the coin game, reasonably understood. However, in what regards the mathematics itself of the coin game, we have seen in chapter 2 that many interesting things can be said. We will be back to this, with more, by using the present formalism, in chapter 6 below.

Moving on, and still in relation with the material from chapter 2, we have:

EXAMPLE 4.4. *Rolling dice.*

Again, things here are simple and clear, because when you throw a die the corresponding probability space, together with its probability measure, is as follows:

$$X=\big\{1,\ldots,6\big\}\quad,\quad P(i)=\frac{1}{6}\ ,\ \forall i$$

As before with the coins, we can further complicate this by assuming that the die is biased, say landing on face i with probability $p_i\in[0,1]$. In this case the corresponding probability space, together with its probability measure, is as follows:

$$X=\big\{1,\ldots,6\big\}\quad,\quad P(i)=p_i\quad,\quad p_i\geq 0\ ,\ \sum_i p_i=1$$

Also as before with coins, things become more interesting when throwing a die several times in a row, or equivalently, when throwing several identical dice at the same time. In this latter case, with n identically biased dice, the probability space is as follows:

$$X=\big\{1,\ldots,6\big\}^n\quad,\quad P(i_1\ldots i_n)=p_{i_1}\ldots p_{i_n}\quad,\quad p_i\geq 0\ ,\ \sum_i p_i=1$$

Observe that the sum 1 condition in Definition 4.1 is indeed satisfied, and with this proving that our dice modeling is bug-free, due to the following computation:

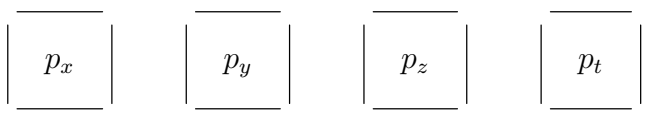
$$\begin{aligned}\sum_{i\in X}P(i) &= \sum_{i_1,\ldots,i_n}P(i_1\ldots i_n)\\ &= \sum_{i_1,\ldots,i_n}p_{i_1}\ldots p_{i_n}\\ &= \sum_{i_1}p_{i_1}\ldots\sum_{i_n}p_{i_n}\\ &= 1\times\ldots\times 1\\ &= 1\end{aligned}$$

In fact, this computation is identical to the one that we did before, for coins. And with this, we will end our preliminary discussion about dice. More on throwing dice, and on the mathematics of the die game, coming in chapter 6 below.

Getting back now to theory, in the general context of Definition 4.1, we can see that what we have there is very close to the biased die, from Example 4.4. Indeed, in the general context of Definition 4.1, we can say that what happens is that we have a die with $|X|$ faces, which is biased such that it lands on face i with probability $P(i)$.

Which is something quite interesting, theoretically speaking, in relation with the discrete probability theory that we want to develop in this book, because we have now some intuition on all this. So, as a conclusion to this, let us record this finding as follows:

PRINCIPLE 4.5. *Discrete probability can be understood as being about throwing a general die, having an arbitrary number of faces, and which is arbitrarily biased too:*



To be more precise, when writing our probability space as $X=\{x,y,z,t,\ldots\}$, with the corresponding probabilities being $p_x,p_y,p_z,p_t,\ldots$, the picture is the one above.

Which sounds like something quite conceptual, which is good to know. We will be back to this key principle, many times, on various occasions, later in this book.

Moving on, still talking theory, I owe you in fact some further explanations on Definition 4.1, in relation with the two comments that I made there, afterwards. So, let us review this, with more details. The first comment on Definition 4.1 was as follows:

COMMENT 4.6. *In Definition 4.1, the condition $\sum_{x\in X} P(x) = 1$ perfectly makes sense, and this even if X is uncountable, because the sum of positive numbers is always defined, as a number in $[0,\infty]$, and this no matter how many positive numbers we have.*

Which is of course something trivial, and self-explanatory, but as a side remark here, which is good to know, such things are not true if we allow negative numbers. Consider indeed the following series, which converges, as shown by our estimate below:

$$\begin{aligned}
1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\ldots &= \left(1-\frac{1}{2}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\left(\frac{1}{5}-\frac{1}{6}\right)+\ldots\\
&< \left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\left(\frac{1}{3}-\frac{1}{4}\right)+\ldots\\
&= 1-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\frac{1}{3}-\frac{1}{4}+\ldots\\
&= 1
\end{aligned}$$

Now let us look at the subseries formed by the odd, and the even terms. In order to do so, observe first that we have the following computation:

$$\begin{aligned}
1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots &= 1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)+\ldots\\
&\geq 1+\frac{1}{2}+\left(\frac{1}{4}+\frac{1}{4}\right)+\left(\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right)+\ldots\\
&= 1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\ldots\\
&= \infty
\end{aligned}$$

But with this, we have the following formulae, for the above-mentioned subseries:

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\frac{1}{8}+\ldots=\frac{1}{2}\left(1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots\right)=\infty$$

$$1+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\ldots\geq\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\frac{1}{8}+\ldots=\infty$$

Thus, both these series diverge. The point now is that, by using this, when rearranging terms in the original alternating series, we can arrange for the partial sums to go arbitrarily high, or arbitrarily low, and we can obtain any $x\in[-\infty,\infty]$ as limit. Good to know.

Next, the second comment that we made after Definition 4.1 was as follows:

COMMENT 4.7. *In Definition 4.1, we chose not to assume that the set X is finite or countable, and this for instance because we want to be able to regard any probability function on $\mathbb{N}$ as a probability function on $\mathbb{R}$, by setting $P(x)=0$ for $x\notin\mathbb{N}$.*

Again, this is something trivial, and self-explanatory, and more on this later, when discussing some further illustrations for Definition 4.1. This being said, since we talk here about countability, time to review that. We have indeed the following theorem, which is something good to know, and is the basis for everything, in relation with countability:

THEOREM 4.8. *The following happen, in relation with countability:*

(1) $\mathbb{Q}$ *is countable, while* $\mathbb{R}$ *is not countable.*
(2) $r \in \mathbb{R}$ *is rational precisely when its decimal writing is periodic.*
(3) *The probability for a randomly picked* $x \in \mathbb{R}$ *to be rational is* 0.

PROOF. We have several things to be proved, the idea being as follows:

(1) We can count the positive rationals, with some redundancies, as follows:

$$\begin{array}{ccccccc}
1/1 & \to & 1/2 & & 1/3 & \to & 1/4 & \ldots \\
& \swarrow & & \nearrow & & \swarrow & & \\
2/1 & & 2/2 & & 2/3 & & 2/4 & \ldots \\
\downarrow & \nearrow & & \swarrow & & & & \\
3/1 & & 3/2 & & 3/3 & & 3/4 & \ldots \\
& \swarrow & & & & & & \\
4/1 & & 4/2 & & 4/3 & & 4/4 & \ldots \\
\\
\vdots & & \vdots & & \vdots & & \vdots & \ddots
\end{array}$$

Now after eliminating the redundancies, and then adding the negatives, which must be countable too, say via an alternating $+/-$ scheme, countability of $\mathbb{Q}$ proved.

(2) Regarding now the reals, assume by contradiction that $[0,1]$ is countable, listed as follows, and with the convention that the writings of type $\ldots 999 \ldots$ are avoided:

$$x_1 = 0.a_1a_2a_3\ldots$$

$$x_2 = 0.b_1b_2b_3\ldots$$

$$x_3 = 0.c_1c_2c_3\ldots$$

$$\ldots$$

Now pick digits $\sigma_1 \neq a_1$, $\sigma_2 \neq b_2$, $\sigma_3 \neq c_3$ and so on, again with a technical convention here, that these are different from 9, and define $x \in \mathbb{R}$ as follows:

$$x = 0.\sigma_1\sigma_2\sigma_3\ldots$$

We have then $x \in [0,1]$, and since x is obviously not on the above list, this is a contradiction. Thus $[0,1]$ is not countable, and it follows that $\mathbb{R}$ is not countable either.

(3) Assuming that $r \in \mathbb{R}$ has periodic decimal writing, the following computation, based on $(10^p-1)(\sum_k 10^{-kp})=1$, obtained by multiplying, gives $r \in \mathbb{Q}$:

$$\begin{aligned} r &= \pm a_1 \ldots a_m . b_1 \ldots b_n c_1 \ldots c_p c_1 \ldots c_p \ldots \\ &= \pm \frac{1}{10^n}\left(a_1 \ldots a_m b_1 \ldots b_n + c_1 \ldots c_p \left(\frac{1}{10^p}+\frac{1}{10^{2p}}+\ldots\right)\right) \\ &= \pm \frac{1}{10^n}\left(a_1 \ldots a_m b_1 \ldots b_n + \frac{c_1 \ldots c_p}{10^p-1}\right) \end{aligned}$$

(4) Conversely, given a rational number $r=k/l$, we can find its decimal writing by performing the usual division algorithm, k divided by l. But this algorithm will be surely periodic, after some time, so the decimal writing of r is indeed periodic.

(5) Regarding now the probability assertion, we are a bit in trouble, because that is obviously about continuous probability, as opposed to discrete probability, that we are doing in this book. So, I will have to be a bit sloppy here, perhaps even cheat a bit, who knows. In any case, here is what I have to say, and you will have to trust me here:

(6) It is enough to prove that the probability for a real number $x \in [0,1]$ to be rational is 0, with this being stronger than the assertion in the statement. So, let us write the rational numbers $r \in [0,1]$ in the form of a sequence $r_1, r_2, r_3 \ldots$ as follows:

$$\mathbb{Q} \cap [0,1] = \left\{r_1, r_2, r_3, \ldots\right\}$$

Let us also pick a number $c>0$. Since the probability of having $x=r_1$ is certainly smaller than $c/2$, then the probability of having $x=r_2$ is certainly smaller than $c/4$, then the probability of having $x=r_3$ is certainly smaller than $c/8$ and so on, the probability for x to be rational satisfies the following inequality:

$$P \leq \frac{c}{2}+\frac{c}{4}+\frac{c}{8}+\ldots = c\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots\right) = c$$

Now since the number $c>0$ was arbitrary, we obtain $P=0$, as desired. □

And with this, end of our discussion regarding Definition 4.1, and its ramifications.

4b. Bayes formula

We have already learned some good probability, but we are not done yet with the basics. Here is for instance a simple question, that does not look easy to solve:

QUESTION 4.9. *What is the probability of getting* 12 *as total, when throwing* 3 *dice, knowing that none of the dice falls on* 1*?*

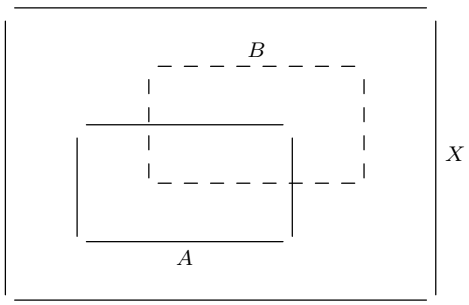
Fortunately, there is a systematic approach to such questions, called conditional probability. Indeed, by thinking a bit, we are led to the following basic fact:

THEOREM 4.10. *The probability for A to happen, knowing that B happens, is*

$$P(A|B)=\frac{P(A\cap B)}{P(B)}$$

with this being called conditional probability.

PROOF. This is something quite obvious, by drawing a Venn diagram, as follows:



Indeed, knowing that B happens means that our computation takes place inside B. Next, we are interested in the probability for A to happen, and since B happens, this means that we are interested in the probability for $A\cap B$ to happen. Thus, we have:

$$P(A|B)=\frac{P(A\cap B)}{P(B)}$$

Summarizing, we are led to the conclusion in the statement. □

As an illustration for the above formula, let us go back to Question 4.9. By using Theorem 4.10, can now answer that question, as follows:

ANSWER 4.11. *The probability of getting* 12*, with none of our* 3 *dice falling on* 1*, is*

$$P=\frac{19/216}{125/216}=\frac{19}{125}$$

according to our general formula above, for conditional probability.

To be more precise here, we have the following self-explanatory computation, based on the general formula from Theorem 4.10:

$$\begin{aligned}P&=\frac{P(246)+P(255)+P(336)+P(345)+P(444)}{P(\geq 2,\geq 2,\geq 2)}\\&=\frac{6/216+3/216+3/216+6/216+1/216}{125/216}\\&=\frac{19/216}{125/216}\\&=\frac{19}{125}\end{aligned}$$

As another illustration for the formula in Theorem 4.10, we have:

EXAMPLE 4.12. *Given a poker hand, out of a standard deck of* 32 *cards, namely*

$$\{7,8,9,10,J,Q,K,A\}\times\{\clubsuit,\diamondsuit,\heartsuit,\spadesuit\}$$

the probabilities of having a given card, knowing that we have a straight, are:

(1) $P(7)=1/4$.
(2) $P(8)=1/2$.
(3) $P(9)=3/4$.
(4) $P(10)=1$.
(5) $P(J)=1$.
(6) $P(Q)=3/4$.
(7) $P(K)=1/2$.
(8) $P(A)=1/4$.

To be more precise, in order to investigate such questions, we can use the general formula in Theorem 4.10, which in our situation takes the following form:

$$P(C|\text{straight})=\frac{P(C,\text{straight})}{P(\text{straight})}$$

Which suggests computing a lot of probabilities, but thinking a bit, we can do this without many computations. Indeed, there are 4 types of straight situations, namely:

$$7\ ,\ 8\ ,\ 9\ ,\ 10\ ,\ J$$
$$8\ ,\ 9\ ,\ 10\ ,\ J\ ,\ Q$$
$$9\ ,\ 10\ ,\ J\ ,\ Q\ ,\ K$$
$$10\ ,\ J\ ,\ Q\ ,\ K\ ,\ A$$

Obviously, these 4 types of straight situations are uniformly distributed, with this meaning that, knowing that we have a straight, each of these 4 situations will appear with probability 1/4. But with this remark in hand, we obtain right away the probabilities that we need, because having a 7 means that we must be in the first straight situation, so probability 1/4, then having a 8 means that we must be in the first of second straight situation, so probability $1/4+1/4=1/2$, and so on up the last case, where having an ace A means that we must be in the fourth straight situation, and so probability 1/4.

In relation with conditional probability questions, at a more theoretical level, we have the following well-known and useful formula, due to Bayes:

THEOREM 4.13. *We have the following formula,*

$$P(A|B)=\frac{P(B|A)P(A)}{P(B)}$$

involving conditional probabilities.

PROOF. This is something which might look quite difficult to establish, just by thinking at probabilities, but which follows easily by using our mathematical formalism for probability, and for conditional probability in particular. Recall indeed that we have:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}$$

Now observe that this equality can be written in the following way:

$$P(A|B)P(B) = P(A \cap B)$$

By symmetry reasons, the following formula must hold as well:

$$P(B|A)P(A) = P(A \cap B)$$

Now by forgetting about $P(A \cap B)$, we conclude that the following holds:

$$P(A|B)P(B) = P(B|A)P(A)$$

But this leads to the Bayes formula, as stated. □

In practice, there are many interesting applications of the Bayes formula. Here is a first illustration, which is quite hard to come upon, with bare hands:

EXAMPLE 4.14. *Assume that we have* 100 *dice,* 75 *of which are normal, and* 25 *of which are biased, with* $P(6) = 1/2$*. If we pick a die, throw it, and get* 6*, then this means that the probability of the die that we picked to be biased is* $1/2$*.*

Indeed, according to the Bayes formula, the probability that we are interested in, that of having a biased die, knowing that we got a 6 after throwing it, is:

$$P(\text{biased}|6) = \frac{P(6|\text{biased})P(\text{biased})}{P(6)}$$

Now in this formula, the numbers on top are already known to us, given by:

$$P(6|\text{biased}) = \frac{1}{2} \quad , \quad P(\text{biased}) = \frac{25}{100} = \frac{1}{4}$$

As for the number on the bottom, this can be computed as follows:

$$\begin{aligned} P(6) &= P(6, \text{normal}) + P(6, \text{biased}) \\ &= P(6|\text{normal})P(\text{normal}) + P(6|\text{biased})P(\text{biased}) \\ &= \frac{1}{6} \times \frac{3}{4} + \frac{1}{2} \times \frac{1}{4} \\ &= \frac{1}{8} + \frac{1}{8} \\ &= \frac{1}{4} \end{aligned}$$

Thus, we can finish our computation, and we obtain indeed probability $1/2$:

$$\begin{aligned} P(\text{biased}|6) &= \frac{P(6|\text{biased})P(\text{biased})}{P(6)} \\ &= \frac{1/2 \times 1/4}{1/4} \\ &= \frac{1}{2} \end{aligned}$$

Back now to theory, it is possible to come up with more complicated formulae, in the spirit of the one of Bayes, featuring 3 or more events. In order to discuss this, observe that we have the following formula, which is something self-explanatory:

$$P(B) = P(B|A)P(A) + P(B|A^c)P(A^c)$$

By using this, the Bayes formula from Theorem 4.13 can be rewitten as follows:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B|A)P(A) + P(B|A^c)P(A^c)}$$

Now the point is that this latter formula generalizes as follows:

THEOREM 4.15. *Assuming $X = \sqcup_i A_i$, we have the formula*

$$P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_j P(B|A_j)P(A_j)}$$

which generalizes the Bayes formula, obtained with $X = A \sqcup A^c$.

PROOF. Due to the fact that we have a partition, $X = \sqcup_i A_i$, we have:

$$P(B) = \sum_j P(B|A_j)P(A_j)$$

But with this, we have the following computation, using the Bayes formula:

$$\begin{aligned} P(A_i|B) &= \frac{P(B|A_i)P(A_i)}{P(B)} \\ &= \frac{P(B|A_i)P(A_i)}{\sum_j P(B|A_j)P(A_j)} \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

In relation with the above, there are also some further abstract aspects of conditional probability, to be worked out as well. But more on this later, when we will know more about probability, in general. For the moment, what we have in the above will do.

Getting back now to the applications of the basic Bayes formula, from Theorem 4.13, there are many of them, all in the spirit of Example 4.14. Here is a second one:

EXAMPLE 4.16. *Assume that a student has four ways of getting to school:*

(1) *He takes these four ways* A, B, C, D *with probabilities* $1/3, 1/4, 1/12, 1/3$.
(2) *And the probabilities for getting late, in these ways, are* $1/20, 1/10, 1/5, 0$.

Then, knowing that he got late, the probability of having chosed C *is* $2/7$.

Indeed, according to the Bayes formula, the probability that we are interested in, that of the student having chosed way C, knowing that he got late, is:

$$P(C|\text{late}) = \frac{P(\text{late}, C)P(C)}{P(\text{late})}$$

Now in this formula, the numbers on top are already known to us, given by:

$$P(\text{late}, C) = \frac{1}{5} \quad , \quad P(C) = \frac{1}{12}$$

As for the number on the bottom, this can be computed as follows:

$$\begin{aligned} & P(\text{late}) \\ = \ & P(\text{late}|A)P(A) + P(\text{late}|B)P(B) + P(\text{late}|C)P(C) + P(\text{late}|D)P(D) \\ = \ & \frac{1}{20} \times \frac{1}{3} + \frac{1}{10} \times \frac{1}{4} + \frac{1}{5} \times \frac{1}{12} + 0 \times \frac{1}{3} \\ = \ & \frac{1}{60} + \frac{1}{80} + \frac{1}{60} \\ = \ & \frac{7}{120} \end{aligned}$$

Thus, we can finish our computation, and we obtain indeed probability $2/7$:

$$\begin{aligned} P(C|\text{late}) &= \frac{P(\text{late}, C)P(C)}{P(\text{late})} \\ &= \frac{1/5 \times 1/12}{7/120} \\ &= \frac{2}{7} \end{aligned}$$

And with this, end of our discussion regarding conditional probability, and the Bayes formula. We will be back to such things later in this book, once we will know more.

4c. Pareto, iterations

Getting now into more applied probability, and more specifically economics, a well-known observation, due to Pareto, is that in pretty much any business, on this planet, 20% of the people do 80% of the work. To be more precise, this is certainly true, and I confirm, in the academia, and more generally in any public sector business.

As for the private businesses, of reasonable size of course, as for probability theory to properly apply, the Pareto principle holds there as well, and this no matter what the respective CEO tell their shareholders, about the high reliability of their thing, and hard work done by 100% of their empolyees. Humans will be humans, no matter the job.

In short, we have the following principle, encapsulating some deep things:

PRINCIPLE 4.17 (Pareto law). 20% *of the people do* 80% *of the work.*

More generally, by some kind of miracle, the Pareto law applies to many other situations, where humans and their activities are involved. For instance, when comparing the wealth of people, working or not, 20% of the people earn 80% of the money. And so on.

With this discussed, the question is now, can we have some interesting mathematics going, out of this? And the answer here is yes, because we can iterate the Pareto law, and we are lead to some interesting mathematics, involving the binomial laws.

Indeed, if we iterate the Pareto law once, among the 20% of the people doing 80% of the work, 20% will do 80% of that work, and 80% will do 20% of that work. As for the 80% of the people doing 20% of the work, 20% will do 80% of that work, and 80% will do 20% of that work. And so, in the end, we are led to the conclusion that:

(1) 4% of people do 64% of the work.

(2) 32% of people do 32% of the work.

(3) 64% of people do 4% of the work.

Next, if we iterate the Pareto law once more, among the 4% of the people doing 64% of the work, 20% will do 80% of that work, and 80% will do 20% of that work. Next, in what regards the 32% of the people doing 32% of the work, 20% will do 80% of that work, and 80% will do 20% of that work. As for the remaining 64% of the people, doing 4% of the work, 20% will do 80% of that work, and 80% will do 20% of that work. And so, in the end, we are led to the conclusion that, when iterating the Pareto law twice:

(1) 0.8% of people do 51.2% of the work.

(2) 9.6% of people do 38.4% of the work.

(3) 38.4% of people do 9.6% of the work.

(4) 51.2% of people do 0.8% of the work.

And so on, and it is pretty much clear that we obtain in this way binomial laws. To be more precise, we have the following general result, in relation with this:

THEOREM 4.18. *When iterating n times a generalized Pareto law, namely*

$$p \text{ people do } 1-p \text{ of the work}$$

with $p \in (0,1)$, we obtain a binomial law, as follows,

$$\binom{n}{s}p^{n-s}(1-p)^s \text{ people do } \binom{n}{s}p^s(1-p)^{n-s} \text{ of the work}$$

for $s = 0, 1, \ldots, n$.

PROOF. This is indeed something self-explanatory, and with the case $p = 1/5$ and $n = 2, 3$ corresponding to our computations above, for the usual Pareto law. □

Finally, observe that the $n >> 0$ iterations of the Pareto law lead to singularities, because with $p < 1/2$ the heaviest workers, the p^n ones doing $(1-p)^n$ of the work, are each supposed to do $((1-p)/p)^n$ work, which is impossible with $n \to \infty$.

Thus, as a conclusion to all this, while iterating a bit the Pareto law makes some sense, iterating it too much leads to contradictions. Which is something good to know.

4d. Models for e, pi

We would like to end this chapter, and the present Part I, with some interesting applications of probability theory to fundamental mathematics, and more specifically, with some remarkable probabilistic models for the numbers e, π. Let us start with:

THEOREM 4.19. *The number e from analysis, given by*

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}$$

which numerically means $e = 2.7182818284\ldots$, is irrational.

PROOF. We know this since chapter 1, but always good to talk about it again, with more details. Following Fourier, we will prove this by contradiction. So, assume by contradiction that $e = m/n$, with $m, n \in \mathbb{N}$, and let us look at the following number:

$$x = n!\left(e - \sum_{k=0}^{n} \frac{1}{k!}\right)$$

As a first observation, x is an integer, as shown by the following computation:

$$\begin{aligned} x &= n!\left(\frac{m}{n} - \sum_{k=0}^{n} \frac{1}{k!}\right) \\ &= m(n-1)! - \sum_{k=0}^{n} n(n-1)\ldots(n-k+1) \\ &\in \mathbb{Z} \end{aligned}$$

On the other hand $x > 0$, and we have as well the following estimate:

$$\begin{aligned} x &= n! \sum_{k=n+1}^{\infty} \frac{1}{k!} \\ &= \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \ldots \\ &< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \ldots \\ &= \frac{1}{n} \end{aligned}$$

Thus $x \in (0, 1)$, which contradicts our previous finding $x \in \mathbb{Z}$, as desired. □

Quite interesting all this, philosophically speaking, telling us that our beloved e constant, and so our mathematics itself, is something a bit alien. Moreover, it is possible to prove that e is in fact transcendental, meaning it is not something of type $\sqrt{2}$ or $1 + \sqrt[3]{3}$, that is, it is not a root of a polynomial with rational coefficients, $P \in \mathbb{Q}[X]$. For more on such things, which are quite fascinating, check any standard introduction to arithmetic.

In relation now with what we know how to do, in this book, probability, the question is, can we come up with a nice probabilistic model for e? In answer, let us start with:

PROPOSITION 4.20. *We have the following formula,*

$$\left(\bigcup_i A_i \right)^c = \bigcap_i A_i^c$$

as well as the following formula,

$$\left(\bigcap_i A_i \right)^c = \bigcup_i A_i^c$$

with c standing as usual for the complements.

PROOF. This is something elementary, the idea being as follows:

(1) In what regards the first assertion, this is the mathematical formulation of the obvious fact that "x does not belong to any of the A_i precisely when x does not belong to any of the A_i". Or at least, this is how I personally view this formula.

(2) Similar story for the second assertion, with this being the mathematical formulation of the fact that "x does not belong to at least one of the A_i precisely when x does not belong at least to one of the A_i". With this being, again, something trivial.

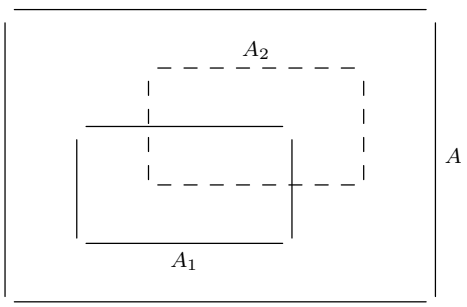
(3) Finally, in case where you ever find one of (1,2) more difficult than the other, here are some equivalences that might be of interest for you, with $B_i = A_i^c$:

$$\left(\bigcup_i A_i\right)^c = \bigcap_i A_i^c \iff \left(\bigcup_i A_i\right)^{cc} = \left(\bigcap_i A_i^c\right)^c$$
$$\iff \bigcup_i A_i = \left(\bigcap_i A_i^c\right)^c$$
$$\iff \bigcup_i B_i^c = \left(\bigcap_i B_i\right)^c$$

Thus, (1) and (2) are in fact equivalent, so if one is easy, so is the other. □

Getting now to counting unions or intersections as above, we have here the inclusion-exclusion principle, that we would like to explain now. Let us start with:

PROPOSITION 4.21. *Two subsets of a given set $A_1, A_2 \subset A$ are best represented by the corresponding Venn diagram,*



and we have the following counting formula regarding them,

$$|(A_1 \cup A_2)^c| = |A| - |A_1| - |A_2| + |A_1 \cap A_2|$$

called inclusion-exclusion principle for two sets.

PROOF. This is something quite self-explanatory, the idea being as follows:

(1) To start with, we can draw indeed a Venn diagram as above, and with this Venn diagram in hand, the inclusion-exclusion principle is something clear.

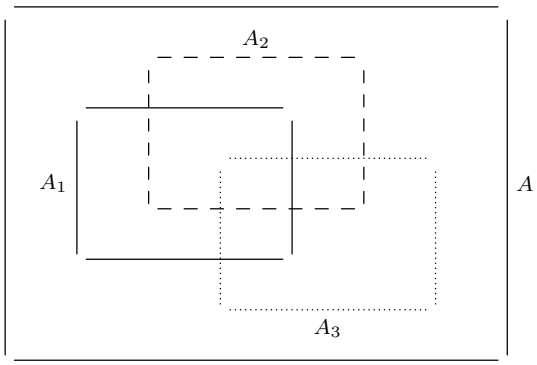
(2) However, shall we really trust diagrams. So, here is as well an abstract proof for the inclusion-exclusion principle, not using diagrams of any kind:

– In order to count $(A_1 \cup A_2)^c$, we certainly have to start with $|A|$, and then remove both $|A_1|$, $|A_2|$, because the elements of A_1, A_2 do not belong to $(A_1 \cup A_2)^c$.

– But then, thinking well, we have to put back $|A_1 \cap A_2|$, because we removed twice the elements of $A_1 \cap A_2$. Thus, we are led to the above formula. □

In the case of three subsets $A_1, A_2, A_3 \subset A$ we have a similar result, as follows:

PROPOSITION 4.22. *Three subsets of a given set $A_1, A_2, A_3 \subset A$ are best represented by the corresponding Venn diagram,*



and we have the following counting formula regarding them,

$$\begin{aligned} |(A_1 \cup A_2 \cup A_3)^c| &= |A| - |A_1| - |A_2| - |A_3| \\ &\quad + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| \\ &\quad - |A_1 \cap A_2 \cap A_3| \end{aligned}$$

called inclusion-exclusion principle for three sets.

PROOF. This is again something quite self-explanatory, the idea being as follows:

(1) To start with, we can draw indeed a Venn diagram as above, and with this Venn diagram in hand, the inclusion-exclusion principle is something clear.

(2) However, as before, shall we really trust diagrams. So, here is as well an abstract proof for the inclusion-exclusion principle, not using diagrams of any kind:

– In order to count $(A_1 \cup A_2 \cup A_3)^c$, we have to start with $|A|$, and then remove $|A_1|$, $|A_2|$, $|A_3|$, because the elements of A_1, A_2, A_3 do not belong to $(A_1 \cup A_2 \cup A_3)^c$.

– But then, thinking well, we have to put back $|A_1 \cap A_2|$, $|A_1 \cap A_3|$, $|A_2 \cap A_3|$, because we removed twice the elements of $A_1 \cap A_2$, $A_1 \cap A_3$, $A_2 \cap A_3$.

– And then, thinking some more, we have to remove $|A_1 \cap A_2 \cap A_3|$, because with our various manipulations above, the elements of $A_1 \cap A_2 \cap A_3$ were counted once, then removed 3 times, and then put back 3 times, which overall amounts in counting them once. And since these elements do not belong to the set $(A_1 \cup A_2 \cup A_3)^c$ that we are counting, we have to remove them, and we are led to the above formula. □

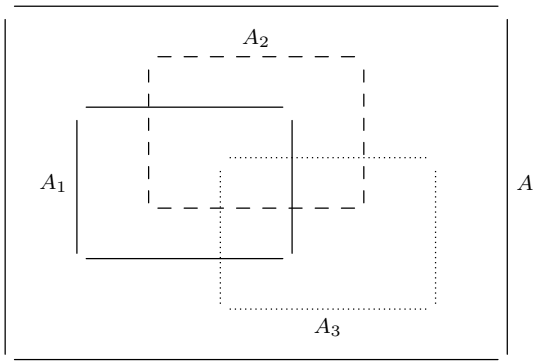
Quite boring all this, you would say, but getting now to the next case, that of four subsets $A_1, A_2, A_3, A_4 \subset A$, something interesting happens here, as follows:

PROPOSITION 4.23. *Four subsets of a given set $A_1, A_2, A_3, A_4 \subset A$ are quite difficult to represent on a Venn diagram, but we still have the following formula regarding them,*

$$\begin{aligned} & |(A_1 \cup A_2 \cup A_3 \cup A_4)^c| \\ = \ & |A| - |A_1| - |A_2| - |A_3| - |A_4| \\ & + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4| \\ & - |A_1 \cap A_2 \cap A_3| - |A_1 \cap A_2 \cap A_4| - |A_1 \cap A_3 \cap A_4| - |A_2 \cap A_3 \cap A_4| \\ & + |A_1 \cap A_2 \cap A_3 \cap A_4| \end{aligned}$$

called inclusion-exclusion principle for four sets.

PROOF. In what regards the first assertion, this is obviously something subjective, and I challenge you to find on the following diagram some sort of nice room for an extra set A_4, and with a Nobel Prize in Economics being offered for solving this question:



Regarding now the second assertion, we can use here the same method as in the proof of Proposition 4.21 and Proposition 4.22, and with the comment here that, retrospectively, it was indeed a good idea to work out that proofs, without using Venn diagrams:

– In order to count $(A_1 \cup A_2 \cup A_3 \cup A_4)^c$, we have to start with $|A|$, and then remove each $|A_i|$, because the elements of each A_i do not belong to $(A_1 \cup A_2 \cup A_3 \cup A_4)^c$.

– But then, thinking well, we have to put back each $|A_i \cap A_j|$, because in our count so far, we removed twice the elements of each $A_i \cap A_j$.

– And then, thinking some more, we have to remove each $|A_i \cap A_j \cap A_k|$, because with our various manipulations above, the elements of $A_i \cap A_j \cap A_k$ were counted once, then removed 4 times, and then put back 4 times, which overall amounts in counting them once. And since these elements do not belong to the set $(A_1 \cup A_2 \cup A_3 \cap A_4)^c$ that we are counting, we have to remove them, and we are led to the above formula.

– And then, we are in fact still not done, because in what regards the elements of $A_1 \cap A_2 \cap A_3 \cap A_4$, we counted them once, then removed them 4 times, then added them

6 times, then removed them 4 times, which amounts in counting them $1-4+6-4=-1$ times. Thus, we have to put them back, as to have them counted 0 times, as needed. □

Lots of fun that we are having here, obviously, set theory is something more exciting than what we expected. In general, the inclusion-exclusion principle is as follows:

THEOREM 4.24. *We have the following formula,*

$$\left|\left(\bigcup_i A_i\right)^c\right| = |A| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \ldots$$

called inclusion-exclusion principle.

PROOF. This is indeed quite clear, by thinking a bit, as before, as follows:

(1) In order to count $(\cup_i A_i)^c$, we certainly have to start with $|A|$.

(2) Then, we obviously have to remove each $|A_i|$, and so remove $\sum_i |A_i|$.

(3) But then, we have to put back each $|A_i \cap A_j|$, and so put back $\sum_{i<j} |A_i \cap A_j|$.

(4) Then, we must remove each $|A_i \cap A_j \cap A_k|$, so remove $\sum_{i<j<k} |A_i \cap A_j \cap A_k|$.

$\vdots$

(5) And so on, which leads to the formula in the statement. □

Observe that, for various practical purposes, the inclusion-exclusion principle can be written in a more compact form, by using a double sum, as follows:

$$\left|\left(\bigcup_i A_i\right)^c\right| = \sum_{s\geq 0} (-1)^s \sum_{i_1<\ldots<i_s} |A_{i_1} \cap \ldots \cap A_{i_s}|$$

As an interesting application of the theory of the binomial coefficients, we can now present a useful application of the inclusion-exclusion principle. Let us start with something well-known, and quite intiutive, often met in the real life, as follows:

DEFINITION 4.25. *A permutation of $\{1,\ldots,N\}$ is a bijection, as follows:*

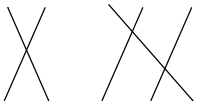
$$\sigma : \{1,\ldots,N\} \to \{1,\ldots,N\}$$

The set of such permutations is denoted S_N.

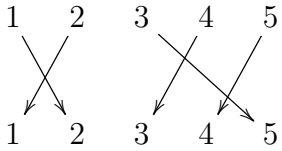
There are many possible notations for the permutations, the basic one consisting in writing the numbers $1,\ldots,N$, and below them, their permuted versions:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Another method, which is certainly faster, and which is actually my personal favorite, is by denoting the permutations as diagrams, acting from top to bottom:

$\sigma =$ 

To be more precise, this diagram stands as a shorthand for the following diagram:

$\sigma =$ 

Here are now some basic properties of the permutations, which are all quite intuitive, coming from definitions, and which are good to know:

PROPOSITION 4.26. *The permutations have the following properties:*

(1) *There are $N!$ of them.*
(2) *They are stable by composition and inversion.*

PROOF. This is something elementary, the idea being as follows:

(1) In order to construct a permutation $\sigma \in S_N$, we have:

– N choices for the value of $\sigma(N)$.
– $(N-1)$ choices for the value of $\sigma(N-1)$.
– $(N-2)$ choices for the value of $\sigma(N-2)$.
$\vdots$
– and so on, up to 1 choice for the value of $\sigma(1)$.

Thus, we have $N!$ choices for any element $\sigma \in S_N$, as claimed in (1).

(2) This is clear, because composing or inverting bijections gives you a bijection. □

With this discussed, here is now the application of the inclusion-exclusion principle that we were having in mind, making appear e, in a nice combinatorial way:

THEOREM 4.27. *The probability for a random permutation $\sigma \in S_N$ to be a derangement, that is, to have no fixed points, is given by the following formula:*

$$P = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^N \frac{1}{N!}$$

Thus we have the following asymptotic formula, in the $N \to \infty$ limit,

$$P \simeq \frac{1}{e}$$

with $e = 2.71828\ldots$ being the usual constant from analysis.

PROOF. This is something very classical, which is best viewed by using the inclusion-exclusion principle. Consider indeed the following sets of permutations:

$$S_N^i = \left\{\sigma \in S_N \middle| \sigma(i) = i\right\}$$

The set of permutations having no fixed points, or derangements, is then:

$$X_N = \left(\bigcup_i S_N^i\right)^c$$

By inclusion-exclusion, the probability that we are interested in is given by:

$$\begin{aligned}
& P(\sigma \in X_N) \\
= \ & \frac{1}{N!}\left(|S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^i \cap S_N^j| - \ldots + (-1)^N \sum_{i_1<\ldots<i_N} |S_N^{i_1} \cap \ldots \cap S_N^{i_N}|\right) \\
= \ & \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \sum_{i_1<\ldots<i_k} (N-k)! \\
= \ & \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \binom{N}{k}(N-k)! \\
= \ & \frac{1}{N!}\sum_{k=0}^{N}(-1)^k \frac{N!}{k!(N-k)!}(N-k)! \\
= \ & \sum_{k=0}^{N}\frac{(-1)^k}{k!}
\end{aligned}$$

Since at the end we have the expansion of $1/e$, we obtain the result. □

The above result is something quite interesting, and many other things can be said, about this. We will be back to this, on a more systematic basis, later in this book.

Getting now to the theory of π, let us try to do something similar to what we did for e, namely basics, and then probabilistic modeling. We first have the following result:

THEOREM 4.28. *The number $\pi = 3.14159\ldots$ is irrational.*

PROOF. This is something more complicated than for e, as follows:

(1) The idea is to use calculus. So, getting back to the calculus that we already learned, in this chapter, we talked about the Leibnitz formula $(fg)' = f'g + fg'$, and about the

fundamental theorem of calculus too, $\int_a^b F'(x)dx = F(b) - F(a)$. But now, the point is that we can combine these two formulae, and we obtain in this way:

$$\int_a^b f'(x)g(x)dx = [f(b)g(b) - f(a)g(a)] - \int_a^b f(x)g'(x)dx$$

This latter formula is called integration by parts. Of particular importance is the case where fg vanishes at both endpoints a, b, in which case our formula simply reads:

$$\int_a^b f'(x)g(x)dx = -\int_a^b f(x)g'(x)dx$$

(2) We will need as well, coming as a complement to $(x^n) = nx^{n-1}$, the following two formulae, coming from the usual formulae for the sines and cosines of sums:

$$\sin' = \cos \quad , \quad \cos' = -\sin$$

(3) Getting now started, following Hermite, consider the following quantities:

$$I_n(t) = \int_{-1}^1 (1 - x^2)^n \cos(xt)dx$$

By double partial integration we obtain the following formula:

$$\begin{aligned}
I_n(t) &= \int_{-1}^1 (1 - x^2)^n \cos(xt)dx \\
&= \int_{-1}^1 2nx(1 - x^2)^{n-1} \frac{\sin(xt)}{t}\, dx \\
&= \frac{2n}{t} \int_{-1}^1 x(1 - x^2)^{n-1} \sin(xt)dx \\
&= \frac{2n}{t} \int_{-1}^1 \left[(1 - x^2)^{n-1} - 2(n-1)x^2(1 - x^2)^{n-2}\right] \frac{\cos(xt)}{t}\, dx \\
&= \frac{2n}{t^2} \int_{-1}^1 (1 - x^2)^{n-2} \left[1 - x^2 - 2(n-1)x^2\right] \cos(xt)dx \\
&= \frac{2n}{t^2} \int_{-1}^1 (1 - x^2)^{n-2} \left[1 - (2n-1)x^2\right] \cos(xt)dx \\
&= \frac{2n}{t^2} \int_{-1}^1 (1 - x^2)^{n-2} \left[(2n-1)(1 - x^2) - (2n-2)\right] \cos(xt)dx \\
&= \frac{2n}{t^2} \left[(2n-1)I_{n-1}(t) - (2n-2)I_{n-2}(t)\right]
\end{aligned}$$

(4) Thus, we have the following recurrence relation for our quantities:

$$t^2 I_n(t) = 2n(2n-1)I_{n-1}(t) - 4n(n-1)I_{n-2}(t)$$

In terms of $J_n(t) = t^{2n+1}I_n(t)$, this recurrence formula becomes:

$$J_n(t) = 2n(2n-1)J_{n-1}(t) - 4n(n-1)t^2J_{n-2}(t)$$

Regarding now the initial data, for this latter recurrence, this is as follows:

$$J_0(t) = 2\sin t \quad , \quad J_1(t) = -4t\cos t + 4\sin t$$

We conclude from this that we must have a formula as follows, with P_n, Q_n being certain polynomials of degree $\leq n$, with integer coefficients:

$$J_n(t) = n!(P_n(t)\sin t + Q_n(t)\cos t)$$

(5) Now observe that with $t = \pi/2$, we obtain from this the following formula:

$$\left(\frac{\pi}{2}\right)^{2n+1} I_n\left(\frac{\pi}{2}\right) = n!P_n\left(\frac{\pi}{2}\right)$$

Assume now by contradiction that π is rational, so that $\pi/2 = a/b$ with $a, b \in \mathbb{N}$. We can rewrite the formula found above in the following more convenient way:

$$\frac{a^{2n+1}}{n!} I_n\left(\frac{a}{b}\right) = b^{2n+1}P_n\left(\frac{a}{b}\right)$$

But, by definition of the integrals I_n, we know that we have:

$$I_n\left(\frac{a}{b}\right) = I_n\left(\frac{\pi}{2}\right) \in (0, 2)$$

Thus with $n >> 0$ the number on the left belongs to $(0, 1)$, which is contradictory, because the number on the right is an integer. And so π is irrational, as claimed. □

Getting now to probability, we would like to have a model for π, a bit as before with our model for e. And here, we have the following remarkable result, due to Buffon:

THEOREM 4.29. *The probability for a needle of length* 1*, when trown on a grid of parallel* 1*-spaced lines, to intersect one line, is:*

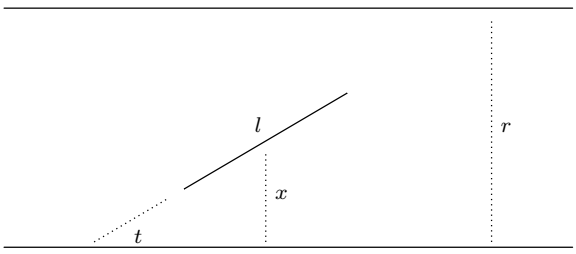
$$P = \frac{2}{\pi}$$

Moreover, we have generalizations of this result, with needles of arbitrary length, thrown over a grid of parallel lines, with arbitrary spacing.

PROOF. We are obviously into continuous probability here, and of rather complicated type, 2-dimensional, so here is the idea of the proof, for what this is worth, and for fully understanding, come back later here, say after reading the present book:

(1) Let us examine, right from the beginning, the general question involving throwing a needle of length l on a grid of parallel r-spaced lines. We denote by $x \in [0, r/2]$ the

distance from the middle of the needle to the closest line, and by $t \in [0, \pi/2]$ the acute angle formed by the needle and that line, according to the following picture:



(2) Now since $x \in [0, r/2]$ varies uniformly, and $t \in [0, \pi/2]$ varies uniformly too, in the case $l \leq r$ the probability for our needle to cross a line is given by:

$$\begin{aligned} P\left(x \leq \frac{l \sin t}{2}\right) &= \int_0^{\pi/2} \int_0^{l \sin t/2} \frac{4}{\pi r}\, dxdt \\ &= \frac{4}{\pi r} \int_0^{\pi/2} \frac{l \sin t}{2}\, dt \\ &= \frac{2l}{\pi r} \end{aligned}$$

(3) In particular, with $l = r = 1$ the crossing probability is $P = 2/\pi$, as stated. □

4e. Exercises

We have seen many interesting things in this chapter, and as exercises, we have:

EXERCISE 4.30. *Work out the general die model, for a coin thrown n times.*

EXERCISE 4.31. *Work out the general die model, for a usual die thrown n times.*

EXERCISE 4.32. *Learn more about sets and countability, including some logic.*

EXERCISE 4.33. *Learn more about the Bayes formula, its versions and applications.*

EXERCISE 4.34. *Experiment some more with the iterations of the Pareto law.*

EXERCISE 4.35. *Find and read the proof of the fact that e is transcendental.*

EXERCISE 4.36. *Then, find and read the proof of the fact that π is transcendental.*

EXERCISE 4.37. *Clarify what we said above in relation with the Buffon needle.*

As bonus exercise, find some interesting probability spaces, which are infinite.

Part II

Variables, laws

Cuantas veces he intentado
Enterrarte en mi memoria
Y aunque diga ya no mas
Es otra vez la misma historia

CHAPTER 5

Random variables

5a. Random variables

Welcome again to probability theory. In the present Part II we will take things very seriously, axiomatize the various phenomena that we met in Part I, which are all quite interesting, and make a mathematical theory, called discrete probability, out of this.

We have seen a first axiomatization of probability in chapter 2, which was something quite intuitive, and then a second axiomatization, more formal, in chapter 4. So, let us begin with a quick review of that material. As explained in chapter 4, we have:

DEFINITION 5.1. *A discrete probability space is a set X, usually finite or countable, whose elements $x \in X$ are called events, together with a function*

$$P : X \to [0, \infty)$$

called probability function, which is subject to the condition

$$\sum_{x \in X} P(x) = 1$$

telling us that the overall probability for something to happen is 1.

Also as explained in chapter 4, this definition comes with 3 comments, as follows:

(1) Our condition $\sum_{x \in X} P(x) = 1$ perfectly makes sense, even if X is uncountable, because the sum of positive numbers is always defined, as a number in $[0, \infty]$.

(2) We have chosen not to assume that X is finite or countable, for instance as for any probability function on $\mathbb{N}$ to be extendable to $\mathbb{R}$, by setting $P(x) = 0$ for $x \notin \mathbb{N}$.

(3) Once we have $P : X \to [0, \infty)$ as above, we can compute what the probability for a set of events $Y \subset X$ to happen is, by setting $P(Y) = \sum_{y \in Y} P(y)$.

And more on such things, abstract aspects of probability theory, once we will get deeper into all this. For the moment, what we have in the above will do.

Regarding now the basic examples, these come from usual games, from the real life, such as flipping coins, or rolling dice. To be more precise, regarding coins, we have:

EXAMPLE 5.2. *When flipping a coin, the probability space is as follows:*

$$X = \big\{\text{heads, tails}\big\} \quad , \quad P(\text{heads}) = P(\text{tails}) = \frac{1}{2}$$

When our coin is biased, the probability space is as follows, with $p \in [0,1]$*:*

$$X = \big\{\text{heads, tails}\big\} \quad , \quad P(\text{heads}) = p \quad , \quad P(\text{tails}) = 1 - p$$

Also, when flipping such a biased coin n *times, the probability space is*

$$X = \big\{\text{heads, tails}\big\}^n \quad , \quad P(i_1 \ldots i_n) = p_{i_1} \ldots p_{i_n}$$

with the constants involved being $p_{heads} = p \in [0,1]$*, and* $p_{tails} = 1 - p$*.*

All this is self-explanatory, I hope, and for more about coins and their mathematics, which can be something quite interesting, we refer to the material in chapter 2. In particular, let us record the main formula found there, for the probability when flipping a $p - (1-p)$ biased coin as above n times, which was as follows:

$$P(a \text{ heads},\ b \text{ tails}) = \binom{n}{a} p^a (1-p)^b$$

Regarding now the dice, their modeling is quite similar, as follows:

EXAMPLE 5.3. *When rolling a die, the probability space is as follows:*

$$X = \big\{1, \ldots, 6\big\} \quad , \quad P(i) = \frac{1}{6} \ , \ \forall i$$

In the case where our die is biased, the probability space is as follows:

$$X = \big\{1, \ldots, 6\big\} \quad , \quad P(i) = p_i \quad , \quad p_i \geq 0 \ , \ \sum_i p_i = 1$$

When rolling such a biased die n *times, the probability space is as follows:*

$$X = \big\{1, \ldots, 6\big\}^n \quad , \quad P(i_1 \ldots i_n) = p_{i_1} \ldots p_{i_n} \quad , \quad p_i \geq 0 \ , \ \sum_i p_i = 1$$

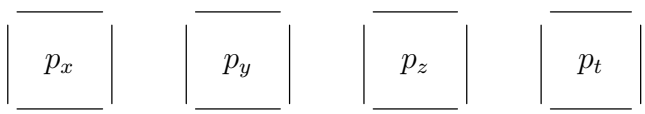
More generally, we can talk, in the obvious way, of k*-faced dice, for any* k*.*

Once again, all this is self-explanatory, I hope, and for more about dice and their mathematics, both open and closed problems, we refer to the material in chapter 2. In particular, let us record the main formula coming from there, for the probability when flipping a $p_1, \ldots, p_6$ biased die as above n times, which was as follows:

$$P(a_1 \times 1, \ldots, a_6 \times 6) = \binom{n}{a_1 \ldots a_6} p_1^{a_1} \ldots p_6^{a_6}$$

As a last thing about coins and dice, observe that a coin is a 2-faced die. Thus, Example 5.2 is a particular case of Example 5.3. In fact, more generally, we have:

PRINCIPLE 5.4. *Discrete probability can be understood as being about throwing a general die, having an arbitrary number of faces, and which is arbitrarily biased too:*



To be more precise, when writing our probability space as $X = \{x, y, z, t, \ldots\}$, with the corresponding probabilities being $p_x, p_y, p_z, p_t, \ldots$, the picture is the one above.

And with this, end of our quick review of the material from Part I. Of course, we did many other things there, but for our purposes now, what we have above will do.

Getting now to what we want to do in this chapter, namely further building on Definition 5.1, let us formulate an intuitive and down-to-earth question, as follows:

QUESTION 5.5. *As usual when doing probability computations, we are mainly interested in winning. But, winning what?*

And good question this is, because Definition 5.1 as stated does not provide an answer to it. So, let us look first at the examples. In case we are dealing with a die, what we win is what the die says. Thus, on average, what we win is the following quantity:

$$E = \frac{1 + 2 + 3 + 4 + 5 + 6}{6} = 3.5$$

In case we are dealing with a biased die, again as in Example 5.3, once again what we win is what the die says, and on average, what we win is the following quantity:

$$E = \sum_i i \times p_i$$

Let us record these findings, which are of course both trivial, but interesting for us, because providing a beginning of answer to Question 5.5, as follows:

PROPOSITION 5.6. *When dealing with a die, what we win on the average is*

$$E = \sum_i i \times p_i$$

which for a usual die reads $E = 3.5$. More generally, when $X \subset \mathbb{R}$, what we win is

$$E = \sum_i i \times P(i)$$

with the sum being over all the elements $i \in X$ of our probability space.

PROOF. All this is very intuitive, coming from the above, and with the last assertion being something theoretical, straightforward generalization of the biased die formula. □

With this understood, what about coins? Here, before doing any computation, we have to assign some numbers to our events, and a standard choice here is as follows:

$$f : \{\text{heads, tails}\} \to \mathbb{R} \quad , \quad f(\text{heads}) = 1 \quad , \quad f(\text{tails}) = 0$$

With this choice made, what we can expect to win is the following quantity:

$$\begin{aligned} E(f) &= f(\text{heads}) \times P(\text{heads}) + f(\text{tails}) \times P(\text{tails}) \\ &= 1 \times \frac{1}{2} + 0 \times \frac{1}{2} \\ &= \frac{1}{2} \end{aligned}$$

When dealing with a biased coin, as in Example 5.2, the computation becomes:

$$\begin{aligned} E(f) &= f(\text{heads}) \times P(\text{heads}) + f(\text{tails}) \times P(\text{tails}) \\ &= 1 \times p + 0 \times (1-p) \\ &= p \end{aligned}$$

However, the story with coins is not over here, because with a different convention for f, we will reach to a different outcome. So, let us try to understand this. We have:

PROPOSITION 5.7. *When flipping a coin, and with our winning function being*

$$f : \{\text{heads, tails}\} \to \mathbb{R} \quad , \quad f(\text{heads}) = a \quad , \quad f(\text{tails}) = b$$

with $a, b \in \mathbb{R}$, what we can expect to win, on average, is the quantity

$$E(f) = ap + b(1-p)$$

in the case of a biased coin. For a normal coin, this reads $E(f) = (a+b)/2$.

PROOF. With the above convention for the winning function, we have indeed:

$$\begin{aligned} E(f) &= f(\text{heads}) \times P(\text{heads}) + f(\text{tails}) \times P(\text{tails}) \\ &= a \times p + b \times (1-p) \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Quite interesting all this, and in hope that you get the point, which is made clear by our latest example, involving coins. In order to do some math, in the context of Definition 5.1, we need a random variable $f : X \to \mathbb{R}$, and the math will consist in computing the expectation of this variable, $E(f) \in \mathbb{R}$. Alternatively, in order to do some business in the context of Definition 5.1, we need some form of "money", and our random variable $f : X \to \mathbb{R}$ will stand for that money, and then $E(f) \in \mathbb{R}$, for the average gain.

Let us axiomatize this situation, in the general context of Definition 5.1, as follows:

DEFINITION 5.8. *A random variable on a probability space X is a function*

$$f : X \to \mathbb{R}$$

and the expectation of such a random variable is the quantity

$$E(f) = \sum_{x \in X} f(x)P(x)$$

which is best thought as being the average gain, when the game is played.

Here the word "game" refers to the probability space interpretation from Principle 5.4. Indeed, in that context, with our discrete set of events X being thought of as corresponding to a generalized die, and by thinking of f as representing some sort of money, the above quantity $E(f)$ is what we win, on average, when playing the game.

Quite nice, all this. As a philosophical conclusion to what we did, in relation with Principle 5.4 and our latest remarks above, coming from it, let us formulate:

CONCLUSION 5.9. *Random variables are money.*

And with this, not only we will better understand what is to come, in this book, but, interestingly, we have yet one more definition for money, with this being, believe me, something quite complicated, economically speaking. Moreover, with Floyd Mayweather being currently broke, now as I type this first edition, 2026, we can even convene to call ourselves, me writer and you reader, The Money Team (TMT). Very good.

5b. Expectations

Getting now to the examples, we already computed the expectations for coins and dice, biased or not, in the above. As a next task, let us try to understand what happens when flipping coins or rolling dice, n times in a row. To start with, we have:

THEOREM 5.10. *When flipping a usual coin n times in a row:*

(1) $E(\text{heads}) = n/2$.
(2) $E(\text{tails}) = n/2$.
(3) $E(a \times \text{heads} + b \times \text{tails}) = n(a+b)/2$.

PROOF. We have several possible proofs here, the idea being as follows:

(1) Let us first fix some mathematical notation, in the spirit of what we have in Definition 5.8. Consider the variables in the statement, namely:

$$f : \big\{\text{heads, tails}\big\}^n \to \mathbb{R} \quad , \quad f = \text{number of heads}$$

$$g : \big\{\text{heads, tails}\big\}^n \to \mathbb{R} \quad , \quad g = \text{number of tails}$$

$$h : \big\{\text{heads, tails}\big\}^n \to \mathbb{R} \quad , \quad h = a \times \text{heads} + b \times \text{tails}$$

(2) According to Definition 5.8, the expectations of these variables are given by the following formulae, which might look of course a bit scary, at a first glance:

$$E(f)=\sum_{x\in\{\text{heads, tails}\}^n}\#(\text{heads}\in x)\times\frac{1}{2^n}$$

$$E(g)=\sum_{x\in\{\text{heads, tails}\}^n}\#(\text{tails}\in x)\times\frac{1}{2^n}$$

$$E(h)=\sum_{x\in\{\text{heads, tails}\}^n}[a\#(\text{heads}\in x)+b\#(\text{tails}\in x)]\times\frac{1}{2^n}$$

However, no fear, and with a bit of probabilistic know-how, we can compute these quantities, by using several methods, which are all instructive, as follows:

(3) Symmetry proof. Observe that, by using the obvious symmetry between heads and tails, at the level of the expectation formulae given above, we have:

$$E(f)=E(g)$$

On the other hand, we also have $f+g=n$, which gives the following formula:

$$E(f)+E(g)=E(f+g)=E(n)=n$$

Thus, we reach to the following conclusion, which is the one in the statement:

$$E(f)=E(g)=\frac{n}{2}$$

As for the general variable h, no need here for new computations, because we have:

$$\begin{aligned}E(h)&=E(af+bg)\\&=aE(f)+bE(g)\\&=an/2+bn/2\\&=n(a+b)/2\end{aligned}$$

Thus, we are led to the conclusions in the statement.

(4) Additive proof. We can argue here that the formulae in the statement are all obvious, by using the fact that, when flipping our coin several times in a row, the expectations will sum up. That is, if we denote by f_n,g_n,h_n our variables, we have:

$$E(f_n)=nE(f_1)\quad,\quad E(g_n)=nE(g_1)\quad,\quad E(h_n)=nE(h_1)$$

Indeed, by using these formulae, along with our computations before at $n=1$, telling us that we have $E(f_1)=E(g_1)=1/2$ and $E(h_1)=(a+b)/2$, we obtain, as desired:

$$E(f_n)=E(g_n)=\frac{n}{2}\quad,\quad E(h_n)=\frac{n(a+b)}{2}$$

(5) Algebraic proof. Here is as well a third proof, which is certainly more complicated, but has the advantage of using 0 thinking and neurons, or almost. We have:

$$\begin{aligned}
E(f) &= \sum_{x\in\{\text{heads, tails}\}^n} \#(\text{heads}\in x)\times\frac{1}{2^n}\\
&= \sum_{s=1}^{n}\sum_{\#(\text{heads}\in x)=s} \#(\text{heads}\in x)\times\frac{1}{2^n}\\
&= \sum_{s=1}^{n}\binom{n}{s}\times s\times\frac{1}{2^n}\\
&= \frac{1}{2^n}\sum_{s=1}^{n}\frac{n!}{(s-1)!(n-s)!}\\
&= \frac{n}{2^n}\sum_{t=0}^{n-1}\binom{n-1}{t}\\
&= \frac{n}{2^n}\times 2^{n-1}\\
&= \frac{n}{2}
\end{aligned}$$

Similarly, $E(g)=n/2$, and then $E(h)=n(a+b)/2$ comes by linearity, as in (3). □

Getting now to the more general case of a biased coin, the result here is as follows:

THEOREM 5.11. *When flipping a biased coin n times in a row:*

(1) $E(\text{heads})=np$.
(2) $E(\text{tails})=n(1-p)$.
(3) $E(a\times\text{heads}+b\times\text{tails})=n(ap+b(1-p))$.

PROOF. This is a matter of generalizing Theorem 5.10, the idea being as follows:

(1) As before, we denote by f,g,h our random variables. According to Definition 5.8, the expectations of these variables are given by the following formulae:

$$E(f)=\sum_{x\in\{\text{heads, tails}\}^n}\#(\text{heads}\in x)\times p^{\#(\text{heads}\in x)}\times(1-p)^{\#(\text{tails}\in x)}$$

$$E(g)=\sum_{x\in\{\text{heads, tails}\}^n}\#(\text{tails}\in x)\times p^{\#(\text{heads}\in x)}\times(1-p)^{\#(\text{tails}\in x)}$$

$$E(h)=\sum_{x\in\{\text{heads, tails}\}^n}[a\#(\text{heads}\in x)+b\#(\text{tails}\in x)]\times p^{\#(\text{heads}\in x)}\times(1-p)^{\#(\text{tails}\in x)}$$

(2) As a first observation, as before for the unbiased coins, the formulae in the statement for $E(f)$ and $E(g)$ give the formula for $E(h)$, by linearity, as follows:

$$\begin{aligned} E(h) &= E(af+bg)\\ &= aE(f)+bE(g)\\ &= anp+bn(1-p)\\ &= n(ap+b(1-p)) \end{aligned}$$

Thus, we are left with computing $E(f)$ and $E(g)$, and regarding the 3 possible approaches here, from the proof of Theorem 5.10, the situation with them is as follows:

(3) Symmetry proof. Normally, the idea here would be to exploit the symmetry between heads and tails, with the goal of reaching to the following formula:

$$(1-p)E(f)=pE(g)$$

Indeed, on the other hand, we have $f+g=n$, which gives the following formula:

$$E(f)+E(g)=E(f+g)=E(n)=n$$

Thus, we would reach to the following conclusion, which is the one in the statement:

$$E(f)=np \quad , \quad E(g)=n(1-p)$$

The problem, however, is that the symmetry study, leading to $(1-p)E(f)=pE(g)$, is not obvious when $p\neq 1/2$. So, relax, and we should better run away from this.

(4) Additive proof. As before, we can argue that the formulae in the statement are all obvious, by using the fact that, when flipping our coin several times in a row, the expectations will sum up. That is, if we denote by f_n, g_n, h_n our variables, we have:

$$E(f_n)=nE(f_1) \quad , \quad E(g_n)=nE(g_1) \quad , \quad E(h_n)=nE(h_1)$$

Indeed, using these formulae, along with our computations before at $n=1$, telling us that we have $E(f_1)=p$, $E(g_1)=1-p$, $E(h_1)=ap+b(1-p)$, we obtain, as desired:

$$E(f_n)=np \quad , \quad E(g_n)=n(1-p) \quad , \quad E(h_n)=n(ap+b(1-p))$$

(5) Algebraic proof. And here is as well the algebraic proof, certainly more complicated, but having the advantage of using 0 thinking, or almost:

$$\begin{aligned}
E(f) &= \sum_{x\in\{\text{heads, tails}\}^n} \#(\text{heads} \in x) \times p^{\#(\text{heads}\in x)} \times (1-p)^{\#(\text{tails}\in x)} \\
&= \sum_{s=1}^{n} \sum_{\#(\text{heads}\in x)=s} \#(\text{heads} \in x) \times p^{\#(\text{heads}\in x)} \times (1-p)^{\#(\text{tails}\in x)} \\
&= \sum_{s=1}^{n} \binom{n}{s} sp^s(1-p)^{n-s} \\
&= \sum_{s=1}^{n} \frac{n!}{(s-1)!(n-s)!}\, p^s(1-p)^{n-s} \\
&= np\sum_{s=1}^{n} \frac{(n-1)!}{(s-1)!(n-s)!}\, p^{s-1}(1-p)^{n-s} \\
&= np\sum_{t=0}^{n-1} \binom{n-1}{t} p^t(1-p)^{n-t-1} \\
&= np(p+1-p)^{n-1} \\
&= np
\end{aligned}$$

Indeed, a similar computation gives $E(g) = n(1-p)$, and then the general formula, $E(h) = n(ap + b(1-p))$, comes from this, by linearity, as explained in (2). □

Next, come the dice. Here there are several natural choices for our random variable, as explained in chapter 2, and regarding the essentials, in the unbiased case, we have:

THEOREM 5.12. *When rolling a usual die n times in a row:*

(1) *For $f_i = \#i$, we have $E(f_i) = n/6$.*
(2) *For $g_i = i\#i$, we have $E(g_i) = ni/6$.*
(3) *For $h = \text{sum}$, we have $E(h) = 3.5n$.*

PROOF. The story here is quite similar to that of a usual coin, and skipping some straightforward details, and going directly to the three possible methods for proving such things, from the proof of Theorem 5.10, the situation is as follows:

(1) Symmetry proof. The variables $f_i = \#i$, counting the number of occurrences of $i \in \{1, \ldots, 6\}$ during our n throws, obviously satisfy the following condition:

$$E(f_1) = \ldots = E(f_6)$$

On the other hand, we have as well the following trivial computation:

$$f_1 + \ldots + f_6 = n \implies E(f_1) + \ldots + E(f_6) = n$$

Thus we have $E(f_i) = n/6$ for any i, as stated. Then, by multiplying by i, we have $E(g_i) = ni/6$. And finally, by summing over i we obtain $E(h) = 3.5n$.

(2) Additive proof. We can argue here that the formulae in the statement are all obvious, using the intuitive fact that, when rolling our die several times in a row, the expectations will sum up. That is, if we denote by f_i^n, g_i^n, h^n our variables, we have:

$$E(f_i^n) = nE(f_i^1) \quad , \quad E(g_i^n) = nE(g_i^1) \quad , \quad E(h^n) = nE(h^1)$$

Indeed, by using these formulae, along with our computations before at $n = 1$, telling us that we have $E(f_i^1) = 1/6$, $E(g_i^1) = i/6$, $E(h^1) = 3.5$, we obtain, as desired:

$$E(f_i^n) = \frac{n}{6} \quad , \quad E(g_i^n) = \frac{ni}{6} \quad , \quad E(h^n) = 3.5n$$

(3) Algebraic proof. Things are a bit more tricky here, depending on the exact variables that we have in mind, the situation being as follows:

– Normally, we can compute indeed $E(f_i)$ algebrically, a bit as before for the coins, by using binomial coefficients and some summing, and I will leave this as an exercise for you, and then pass to $E(g_i)$, and then to $E(h)$, as explained in (1), by linearity.

– However, if we want to compute for instance $E(h)$ directly, algebrically, we are a bit in trouble, because as explained in chapter 2, computing the distribution of the sum h is a quite delicate question, that we do not know yet how to solve.

– So, as a conclusion to this, some algebraic computations definitely work, with our present knowledge, but not all of them. Of course, this is something temporary, and we will be hopefully back to this later in this book, once we will know more things. □

Finally, in the case of a biased die, the result is as follows:

THEOREM 5.13. *When rolling a biased die n times in a row:*

(1) *For $f_i = \#i$, we have $E(f_i) = np_i$.*
(2) *For $g_i = i\#i$, we have $E(g_i) = nip_i$.*
(3) *For $h = \text{sum}$, we have $E(h) = n\sum_i ip_i$.*

PROOF. This is something hybrid between Theorem 5.11 and Theorem 5.12, and skipping the various straightforward details here, the situation is as follows:

(1) Symmetry proof. This won't quite work for a biased die, for the technical reasons explained in the proof of Theorem 5.11, dealing with a biased coin.

(2) Additive proof. Good news here, this works, as usual, because if we denote by f_i^n, g_i^n, h^n our variables, it is clear that we have the following formulae:

$$E(f_i^n) = nE(f_i^1) \quad , \quad E(g_i^n) = nE(g_i^1) \quad , \quad E(h^n) = nE(h^1)$$

Indeed, by using these formulae, along with our computations before at $n = 1$, telling us that we have $E(f_i^1) = p_i$, $E(g_i^1) = ip_i$, $E(h^1) = \sum_i ip_i$, we obtain, as desired:

$$E(f_i^n) = np_i \quad , \quad E(g_i^n) = nip_i \quad , \quad E(h^n) = n\sum_i ip_i$$

(3) Algebraic proof. This won't work well for a biased die, for the technical reasons explained in the proof of Theorem 5.12, dealing with a usual die. □

Many other computations can be performed, along the above lines, and we will certainly get back to this in what follows, in chapter 6, and afterwards.

5c. The variance

We have already seen some good illustrations for Definition 5.8, so time now to get into more delicate aspects. Imagine that you want to set up some sort of business, with your variable $f : X \to \mathbb{R}$. You are of course mostly interested in the expectation $E(f) \in \mathbb{R}$, but passed that, the way this expectation comes in matters too. For instance:

(1) When your variable is constant, $f = c$, you certainly have $E(f) = c$, and your business will run smoothly, with not so many surprises on the way.

(2) On the opposite, for a complicated variable satisfying $E(f) = c$, your business will be more bumpy, with wins and loses on the way, depending on your skills.

In short, and extrapolating now from business to mathematics, physics, chemistry and everything else, we must complement Definition 5.8 with something finer, regarding the "quality" of the expectation $E(f) \in \mathbb{R}$ appearing there. And the first thought here, which is the correct one, goes to the following definition, of the variance of our variable:

DEFINITION 5.14. *The variance of a variable $f : X \to \mathbb{R}$ is the quantity*

$$V(f) = E\left((f - E(f))^2\right)$$

intuitively measuring how far is f from a constant variable.

As a first observation, which is in tune with what we were saying in the above, the variance is 0 precisely when the variable is constant, equal to its expectation:

$$\begin{aligned} V(f) = 0 &\iff f = \text{constant} \\ &\iff f = E(f) \end{aligned}$$

Many other things, more specialized, can be said, as a continuation of this. In general now, the variance is best computed by using the following result:

THEOREM 5.15. *The variance of a variable $f : X \to \mathbb{R}$ is given by*

$$V(f) = E(f^2) - E(f)^2$$

with E denoting as usual the expectation.

PROOF. This is something straightforward, the idea being as follows:

(1) To start with, our formula holds indeed, as shown by the following computation:

$$\begin{aligned} V(f) &= E\left((f-E(f))^2\right) \\ &= E\left(f^2-2E(f)f+E(f)^2\right) \\ &= E(f^2)-2E(f)^2+E(f)^2 \\ &= E(f^2)-E(f)^2 \end{aligned}$$

(2) However, as an interesting consequence, we have the following inequality, and the question is whether we can prove directly this inequality, with bare hands:

$$E(f^2)\geq E(f)^2$$

In practice, using Definition 5.8, this amounts in proving an inequality as follows, for any numbers $p_i\in[0,1]$ satisfying $\sum_i p_i=1$, and any real numbers $f_i\in\mathbb{R}$:

$$\sum_i f_i^2p_i\geq\left(\sum_i f_ip_i\right)^2$$

Now in order to prove this, let us write this inequality as follows:

$$\sum_i f_i^2p_i\sum_i p_i\geq\left(\sum_i f_ip_i\right)^2$$

(3) Our claim now is that this latter inequality, which might look a bit mysterious, is in fact the very familiar Cauchy-Schwarz inequality, which is as follows:

$$\sum_i a_i^2\sum_i b_i^2\geq\left(\sum_i a_ib_i\right)^2$$

Indeed, the passage from this to the inequality in (3) can be done by setting:

$$a_i=f_i\sqrt{p_i}\quad,\quad b_i=\sqrt{p_i}$$

As for the passage from (3) to Cauchy-Schwarz, this can be done too, as follows:

$$f_i=\frac{a_i}{b_i}\quad,\quad p_i=b_i^2$$

(4) Summarizing, saved by Cauchy-Schwarz, we can say now that we have a good understanding of $V(f)\geq 0$. However, for finishing this discussion, actually, where does

Cauchy-Schwarz come from? In answer, consider the following function:

$$\begin{aligned}\varphi(t) &= ||at+b||^2\\ &= <at+b, at+b>\\ &= <a,a>t^2+2<a,b>t+<b,b>\\ &= ||a||^2t^2+2<a,b>t+||b||^2\end{aligned}$$

Since we have $\varphi \geq 0$, the discriminant must be negative, $\Delta \leq 0$, which reads:

$$4<a,b>^2-4||a||^2||b||^2 \leq 0$$

Thus, we have the following inequality, which is the Cauchy-Schwarz one above:

$$||a|| \cdot ||b|| \geq |<a,b>|$$

And with this, we have now a truly good understanding of $V(f) \geq 0$. □

As a complement to Definition 5.14, let us formulate as well:

DEFINITION 5.16. *The standard deviation of a variable $f : X \to \mathbb{R}$ is the quantity*

$$\sigma(f) = \sqrt{E\left((f-E(f))^2\right)}$$

so that $V(f) = \sigma(f)^2$, intuitively measuring how far is f from a constant variable.

And we will leave some thinking here, on whether the variance $V(f)$ or the standard deviation $\sigma(f)$ is the best way of measuring how far is f from a constant variable, as an instructive exercise. With the comment that this is, ultimately, a matter of taste.

Moving on, but still about expectations and variances of variables, as constructed above, at the abstract level, following Markov, we have the following result:

THEOREM 5.17. *We have the following Markov inequality,*

$$P\big(|f| \geq a\big) \leq \frac{E(f)}{a}$$

valid for any random variable $f : X \to \mathbb{R}$, and any $a > 0$.

PROOF. This is something trivial, coming from definitions. Indeed, we have:

$$\begin{aligned} E(f) &= \sum_{x\in X} f(x)P(x) \\ &\geq \sum_{|f(x)|\geq a} f(x)P(x) \\ &\geq \sum_{|f(x)|\geq a} aP(x) \\ &= a\sum_{|f(x)|\geq a} P(x) \\ &= aP\big(|f|\geq a\big) \end{aligned}$$

Thus, we are led to the Markov inequality in the statement. □

Next, following Chebycheff, we have the following key estimate:

THEOREM 5.18. *We have the following Chebycheff inequality,*

$$P\big(|g-E|\geq b\big)=\frac{V}{b^2}$$

valid for any random variable $g:X\to\mathbb{R}$, having mean E and variance V.

PROOF. Given a random variable $g:X\to\mathbb{R}$, having mean E and variance V, we can use the Markov inequality above with $f=(g-E)^2$, and we obtain in this way:

$$\begin{aligned} P\big(|g-E|\geq b\big) &= P\big((g-E)^2\geq b^2\big) \\ &\leq \frac{E((g-E)^2)}{b^2} \\ &= \frac{V}{b^2} \end{aligned}$$

Thus, we are led to the Chebycheff inequality in the statement. □

Getting back now to the real-life considerations from the beginning of this section, good that we have the notion of variance, for understanding how to run our business, but let us not stop here. For a total control of your business, be that of financial, mathematical, physical or chemical type, you will certainly want to know more about your variable $f:X\to\mathbb{R}$. Which leads us into general moments, constructed as follows:

DEFINITION 5.19. *The moments of a variable $f:X\to\mathbb{R}$ are the numbers*

$$M_k=E(f^k)$$

which satisfy $M_0=1$, then $M_1=E(f)$, and then $V(f)=M_2-M_1^2$.

And with this, good news, we have now all the needed tools in our bag for doing some good business, in what follows. To put things in a very compacted way:

– M_0 is about foundations.

– M_1 is about running some business.

– M_2 is about running that business well.

– M_3 and higher are advanced level, about ruining all the competing businesses.

Which is something quite intuitive, and good to know, and this will be our favorite picture of the moments, in what follows, for the remainder of this book.

As a last piece of discussion, still regarding the moments, we can formulate the following version of Definition 5.19, making a more clear link with the variance:

DEFINITION 5.20. *The central moments of a variable $f : X \to \mathbb{R}$ are the numbers*

$$M'_k = E((f - E)^k)$$

with $E = E(f)$, which satisfy $M'_0 = 1$, $M'_1 = 0$, $M'_2 = V(f)$.

In other words, the central moments of a variable $f : X \to \mathbb{R}$ are the moments of the shifted variable $f - E : X \to \mathbb{R}$, with the shift being there for having 0 mean. Which is something quite nice, and we will sometimes use this, instead of Definition 5.19.

Along the same lines, we can do in fact a bit better, as follows:

DEFINITION 5.21. *The normalized central moments of $f : X \to \mathbb{R}$ are the numbers*

$$M''_k = E\left(\left(\frac{f - E}{\sigma}\right)^k\right)$$

with $\sigma = \sigma(f)$, which satisfy $M''_0 = 1$, $M''_1 = 0$, $M''_2 = 1$.

To be more precise here, we can define indeed the normalized central moments by the above formula, assuming of course $\sigma > 0$, and we have then $M''_0 = 1$, $M''_1 = 0$. As for the second normalized central moment, this follows to be 1 indeed, according to:

$$M''_2 = E\left(\left(\frac{f - E}{\sigma}\right)^2\right) = \frac{V(f)}{V(f)} = 1$$

The normalization made in Definition 5.21 is something quite clever, and of particular interest are the cases $k = 3, 4$, where we can formulate:

DEFINITION 5.22. *Given $f : X \to \mathbb{R}$, its third normalized central moment*

$$\gamma = E\left(\left(\frac{f-E}{\sigma}\right)^3\right)$$

is called skewness, and its fourth normalized central moment

$$\kappa = E\left(\left(\frac{f-E}{\sigma}\right)^4\right)$$

is called kurtosis.

And we will end our discussion regarding the moments with this. As a conclusion, a random variable $f : X \to \mathbb{R}$ is quite reasonably described by the data $(E, \sigma, \gamma, \kappa)$ consisting of the expectation, standard deviation, skewness and kurtosis, which are all quite intuitive quantities, whose knowledge is the same as that of M_1, M_2, M_3, M_4. And for more delicate questions, we still have the higher moments, M_k with $k \geq 5$.

5d. Variable laws

Done with the theory? Not really, because we still have to formulate one more key result, which is perhaps the most important one, in probability, as follows:

THEOREM 5.23. *Each random variable $f : X \to \mathbb{R}$ has a law,*

$$\mu = \sum_{x \in X} P(x)\delta_{f(x)}$$

linear combination of Dirac masses, regarded as probability measure on $\mathbb{R}$.

PROOF. Given a random variable $f : X \to \mathbb{R}$, we can certainly talk about its law μ, as being the formal linear combination of Dirac masses in the statement. Our claim is that this is a probability measure on $\mathbb{R}$, in the sense of Definition 5.1:

(1) Indeed, according to our conventions above, the weight of each point $y \in \mathbb{R}$ is the following quantity, which is positive, as it should:

$$d\mu(y) = \sum_{f(x)=y} P(x)$$

(2) Moreover, the total mass of this measure is 1, as it should, due to:

$$\begin{aligned}\sum_{y \in \mathbb{R}} d\mu(y) &= \sum_{y \in \mathbb{R}} \sum_{f(x)=y} P(x)\\ &= \sum_{x \in X} P(x)\\ &= 1\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Still talking basics, let us record as well the following alternative formula for the law, which is clear from definitions, and that we will often use, in what follows:

$$\mu = \sum_{y\in\mathbb{R}} P(f = y)\delta_y$$

But you might probably ask, what is the law good for? In answer, many things, and as a first illustration here, the law encodes the sequence of moments, as shown by:

THEOREM 5.24. *The expectation of a random variable $f : X \to \mathbb{R}$ is given by*

$$E(f) = \int_{\mathbb{R}} y\, d\mu(y)$$

where μ is the law. More generally, we have the following formula, for any $k \in \mathbb{N}$,

$$E(f^k) = \int_{\mathbb{R}} y^k d\mu(y)$$

with the usual convention that each Dirac mass integrates up to 1.

PROOF. This is something straightforward, the idea being as follows:

(1) Let us first compute the expectation of f. With the usual convention that each Dirac mass integrates up to 1, as mentioned in the statement, we have:

$$\begin{aligned} E(f) &= \sum_{x\in X} P(x)f(x) \\ &= \sum_{y\in\mathbb{R}} y \sum_{f(x)=y} P(x) \\ &= \int_{\mathbb{R}} y d\mu(y) \end{aligned}$$

(2) More generally, we have the following computation, for the moments:

$$\begin{aligned} E(f^k) &= \sum_{x\in X} P(x)f(x)^k \\ &= \sum_{y\in\mathbb{R}} y^k \sum_{f(x)=y} P(x) \\ &= \int_{\mathbb{R}} y^k d\mu(y) \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Along the same lines, we have as well the following straightforward generalization of Theorem 5.24, dealing with other functions that can be applied to our variables:

THEOREM 5.25. *Given a random variable $f : X \to \mathbb{R}$ having law μ, we have*

$$E(\phi(f)) = \int_{\mathbb{R}} \phi(y) d\mu(y)$$

with the usual convention that each Dirac mass integrates up to 1.

PROOF. We have indeed the following straighforward computation:

$$\begin{aligned} E(\phi(f)) &= \sum_{x \in X} P(x)\phi(f(x)) \\ &= \sum_{y \in \mathbb{R}} \phi(y) \sum_{f(x)=y} P(x) \\ &= \int_{\mathbb{R}} \phi(y) d\mu(y) \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

Getting now to more abstract aspects, the above results are quite interesting, theoretically speaking, and in view of them, it is tempting to formulate:

DEFINITION 5.26. *Given a set X, which can be finite, countable, or even uncountable, a discrete probability measure on it is a linear combination as follows,*

$$\mu = \sum_{x \in X} \lambda_x \delta_x$$

with the coefficients $\lambda_i \in \mathbb{R}$ satisfying $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. For $f : X \to \mathbb{R}$ we set

$$\int_X f(x) d\mu(x) = \sum_{x \in X} \lambda_x f(x)$$

with the convention that each Dirac mass integrates up to 1.

Observe that, with this, we are now into pure mathematics. However, and we insist on this, it is basic probability, as developed before, which is behind all this.

Now by staying abstract a bit more, with Definition 5.26 in hand, we can recover our previous basic notions, from Definition 5.1 and from Theorem 5.23, as follows:

THEOREM 5.27. *With the above notion of discrete probability measure in hand:*

(1) *A discrete probability space is simply a space X, with a discrete probability measure on it ν. In this picture, the probability function is $P(x) = d\nu(x)$.*
(2) *Each random variable $f : X \to \mathbb{R}$ has a law, which is a discrete probability measure on $\mathbb{R}$. This law is given by $\mu = f_*\nu$, push-forward of ν by f.*

PROOF. This might look a bit scary, but is in fact a collection of trivialities, coming straight from definitions, the details being as follows:

(1) Nothing much to say in relation with the first assertion, with this being something which is plainly clear, just by comparing Definition 5.1 and Definition 5.26.

(2) As a interesting comment, however, in the general context of Definition 5.26, observe that a probability measure $\mu = \sum_{x\in X} \lambda_x \delta_x$ as there depends only on the following function, called density of our probability measure:

$$\varphi : X \to \mathbb{R} \quad , \quad \varphi(x) = \lambda_x$$

And, with this notion in hand, our equation $P(x) = d\nu(x)$ simply says that the probability function P is the density of ν. Which is something which is good to know.

(3) Pretty much the same story with the first assertion in (2), which this being something clear, just by comparing Theorem 5.23 and Definition 5.26.

(4) As for the very last assertion in (2), consider more generally a probability space (X, ν), and a function $f : X \to Y$. We can construct then a probability measure $\mu = f_*\nu$ on Y, called push-forward of ν by f, according to the following formula:

$$\nu = \sum_{x\in X} \lambda_x \delta_x \implies \mu = \sum_{y\in Y} \left(\sum_{f(x)=y} \lambda_x \right) \delta_y$$

Alternatively, at the level of the corresponding measures of the parts $Z \subset Y$, we have the following abstract formula, which looks more conceptual:

$$\mu(Z) = \nu(f^{-1}(Z))$$

In any case, one way or another we can talk about push-forward measures $\mu = f_*\nu$, and in the case of a random variable $f : X \to \mathbb{R}$, we obtain in this way the law of f. □

Getting back to more concrete things, and to Theorems 5.23 and 5.24 as stated, quite remarkably, the sequence of moments uniquely determines the law, as shown by:

THEOREM 5.28. *The sequence of moments of a variable $f : X \to \mathbb{R}$,*

$$M_k = E(f^k)$$

uniquely determines the law of the variable.

PROOF. This is something very standard, using a bit of analysis, as follows:

(1) Assume indeed that the law of our variable $f : X \to \mathbb{R}$ is as follows:

$$\mu = \sum_i \lambda_i \delta_{x_i}$$

(2) The sequence of moments is then given by the following formula:

$$M_k = \sum_i \lambda_i x_i^k$$

(3) But it is then standard calculus to recover the numbers $\lambda_i, x_i \in \mathbb{R}$, and so the measure μ, out of the sequence of numbers M_k. Indeed, assuming that the numbers x_i are $0 < x_1 < \ldots < x_n$ for simplifying, with $k \to \infty$ we have the following estimate:

$$M_k \sim \lambda_n x_n^k$$

(4) Thus, we got the parameters $\lambda_n, x_n \in \mathbb{R}$ of our measure μ, and then by substracting them and doing an obvious recurrence, we get the other parameters $\lambda_i, x_i \in \mathbb{R}$ as well.

(5) So, this was for the proof of the present theorem, and more regarding this, which is something quite interesting, called "moment problem", later in this book. □

Moving on, the law of a variable $f : X \to \mathbb{R}$ is not the only main quantity related to f that we can talk about. As a rival to this notion, we have:

DEFINITION 5.29. *Given a random variable $f : X \to \mathbb{R}$, the function*

$$F(x) = P(f \leq x)$$

is called its cumulative distribution function (CDF).

Observe that the cumulative distribution function $F : \mathbb{R} \to [0, 1]$ must be by definition increasing, and also, that it must have the following limiting properties:

$$F(-\infty) = 0 \quad , \quad F(\infty) = 1$$

As an important comment now, pretty much everything that we have been doing lately, including Definition 5.29, makes sense as well for the continuous variables $f : X \to \mathbb{R}$. So, allowing us a bit of slopiness in regards with the formalism, let us formulate the following result, regarding the CDF of the general random variables $f : X \to \mathbb{R}$:

THEOREM 5.30. *The cumulative distribution function $F : \mathbb{R} \to [0, 1]$ must be*

(1) *Increasing.*
(2) *Right continuous.*
(3) *Such that $F(-\infty) = 0$.*
(4) *Such that $F(\infty) = 1$.*

and conversely, any function satisfying these properties appears as a CDF.

PROOF. Here the first assertion is quite clear, and I will leave it to you to check the right continuity property, after remembering what that property exactly is. As for the second assertion, this is something which is clear too, good exercise for you. □

Getting back now to our usual, discrete variables $f : X \to \mathbb{R}$, in relation with the law of the variable, as previously axiomatized, we have the following result:

THEOREM 5.31. *Assuming that a random variable $f : X \to \mathbb{R}$ has as law*

$$\mu = \sum_i \lambda_i \delta_{x_i} \quad , \quad x_1 < \ldots < x_N \quad , \quad \lambda_i > 0, \ \sum_i \lambda_i = 1$$

its cumulative distribution function is the following step function:

$$F(x) = \begin{cases} 0 & : \ x \in (-\infty, x_1] \\ \lambda_1 & : \ x \in (x_1, x_2] \\ \lambda_1 + \lambda_2 & : \ x \in (x_2, x_3] \\ \vdots & \\ \lambda_1 + \ldots + \lambda_{N-1} & : \ x \in (x_{N-1}, x_N] \\ 1 & : \ x \in (x_N, \infty) \end{cases}$$

Conversely, any such step function F produces a law μ, in the obvious way.

PROOF. This is something self-explanatory, coming from definitions:

(1) The first assertion is indeed clear, coming from definitions.

(2) Regarding the second assertion, consider an arbitrary step function, assumed to be as in Theorem 5.30, namely right continuous, and increasing from 0 to 1. Thus, this step function must be as follows, for certain numbers $0 < \mu_1 < \ldots < \mu_{N-1} < 1$:

$$F(x) = \begin{cases} 0 & : \ x \in (-\infty, x_1] \\ \mu_1 & : \ x \in (x_1, x_2] \\ \mu_2 & : \ x \in (x_2, x_3] \\ \vdots & \\ \mu_{N-1} & : \ x \in (x_{N-1}, x_N] \\ 1 & : \ x \in (x_N, \infty) \end{cases}$$

If we set then $\lambda_i = \mu_i - \mu_{i-1}$, with the convention $\mu_0 = 0$, we have:

$$\lambda_i > 0, \ \sum_i \lambda_i = 1$$

Thus, the following linear combination is a probability measure:

$$\mu = \sum_i \lambda_i \delta_{x_i}$$

But this latter law μ has F as cumulative distribution function, as desired. □

Alternatively, in terms of the density, we have the following result:

THEOREM 5.32. *Assuming that $f : X \to \mathbb{R}$ has density φ, its CDF is:*

$$F(x) = \int_{-\infty}^{x} \varphi(t)dt$$

Conversely, the density appears in terms of the CDF according to

$$\varphi(x) = F'(x)$$

with the convention that the derivative at each step produces a Dirac mass.

PROOF. Again, this is something self-explanatory, coming from definitions, with the above convention for the derivatives of the step functions. □

The above convention regarding the derivatives of step functions, although fully motivated by our probabilistic theory, might of course remain quite mysterious. In answer, functional analysis has an explanation for this, in terms of the notion of distribution. However, we will not get into this in what follows. What we have in the above will do.

5e. Exercises

This was a quite crowded theoretical chapter, and as exercises, we have:

EXERCISE 5.33. *Further develop the symmetry approach, for coins and dice.*

EXERCISE 5.34. *Further develop the additive approach, for coins and dice.*

EXERCISE 5.35. *Further develop the algebraic approach, for coins and dice.*

EXERCISE 5.36. *Work out some further examples of expectations.*

EXERCISE 5.37. *Work out some further examples of variances.*

EXERCISE 5.38. *Learn the various versions of the Cauchy-Schwarz inequality.*

EXERCISE 5.39. *Clarify what we said, in relation with push-forward measures.*

EXERCISE 5.40. *Compute some higher moments too, for variables of your choice.*

As bonus exercise, have a look at measure theory, which is related to all this.

CHAPTER 6

Binomial laws

6a. Binomial laws

Now that we have some abstract knowledge of probability theory, notably in relation with the notions of law, expectation and variance, time to systematically study the variables appearing in the real life. And, as our first variables here, which are the most fundamental ones in discrete probability, we have, and no surprise, the binomial ones.

We already talked about binomial laws on several occasions, with actually most of chapters 2 and 5 dealing with them. So, let us begin with a quick review of that material. There will be some redundancy, of course, but this is for the good cause, always a good idea to talk about the binomial laws, which are foundational for discrete probability.

At the level of the very basics, coming as a start for everything, we have:

PROPOSITION 6.1. *When flipping a coin, the probabilities are:*

$$P(\text{heads}) = P(\text{tails}) = \frac{1}{2}$$

Thus, the number of wins, meaning heads, can be $0, 1$*, with the probabilities being:*

$$P(0) = \frac{1}{2} \quad , \quad P(1) = \frac{1}{2}$$

Your winning law is therefore the following probability measure,

$$b_{1/2} = \frac{1}{2}\left(\delta_0 + \delta_1\right)$$

called Bernoulli law of parameter $1/2$*.*

PROOF. This is indeed something self-explanatory, and quite trivial:

(1) The first assertion, which might look at the first glance as a physics fact, is in fact a mathematical result, coming by computing the probabilities according to:

$$P(E) = \frac{\text{number of times } E \text{ happens}}{\text{total number of possibilities}}$$

(2) Be said in passing, as an interesting twist to the story, the physics fact is actually wrong, with the probability of the coin of landing in the same way as it was launched being around 51%. But are we here for talking physics, let's better ignore this.

(3) The second assertion, regarding the number of wins, comes from the first one.

(4) As for the third assertion, regarding the law, this comes from the second one. □

Coming next, according to our study from chapter 2, we have the following fundamental result, coming as a generalization of Proposition 6.1:

THEOREM 6.2. *When flipping a coin n times in a row, the probabilities are:*

$$P(s \text{ heads}, n-s \text{ tails}) = \frac{1}{2^n}\binom{n}{s}$$

Thus, the number of wins, meaning heads, can be $s = 0, \ldots, n$, the probabilities being:

$$P(s) = \frac{1}{2^n}\binom{n}{s}$$

Your winning law is therefore the following probability measure,

$$b_{n,1/2} = \frac{1}{2^n}\sum_{s=0}^{n}\binom{n}{s}\delta_s$$

called binomial law of parameter $1/2$.

PROOF. This is again self-explanatory, because in order to reach to the situation in the statement, namely s heads and $n-s$ tails, we must select the s occurrences of heads, among the n total throws, and there are $\binom{n}{s}$ choices here, and then sum over these $\binom{n}{s}$ choices the common quantity $1/2^n$. Thus, we are led to the formulae in the statement. □

Let us record as well some numerics, up to $n = 10$. For this purpose, we can use the Pascal triangle from chapter 1, extended with 5 more rows, which looks as follows:

$$\begin{array}{c}
1\\
1\ ,\ 1\\
1\ ,\ 2\ ,\ 1\\
1\ ,\ 3\ ,\ 3\ ,\ 1\\
1\ ,\ 4\ ,\ 6\ ,\ 4\ ,\ 1\\
1\ ,\ 5\ ,\ 10\ ,\ 10\ ,\ 5\ ,\ 1\\
1\ ,\ 6\ ,\ 15\ ,\ 20\ ,\ 15\ ,\ 6\ ,\ 1\\
1\ ,\ 7\ ,\ 21\ ,\ 35\ ,\ 35\ ,\ 21\ ,\ 7\ ,\ 1\\
1\ ,\ 8\ ,\ 28\ ,\ 56\ ,\ 70\ ,\ 56\ ,\ 28\ ,\ 8\ ,\ 1\\
1\ ,\ 9\ ,\ 36\ ,\ 84\ ,\ 126\ ,\ 126\ ,\ 84\ ,\ 36\ ,\ 9\ ,\ 1\\
1\ ,\ 10\ ,\ 45\ ,\ 120\ ,\ 210\ ,\ 252\ ,\ 210\ ,\ 120\ ,\ 45\ ,\ 10\ ,\ 1\\
\vdots
\end{array}$$

Now by dividing the rows by $1/2^n$, and simplifying the fractions, we are led to the following table, for the binomial laws of parameter $1/2$, going up to $n = 10$:

$n\backslash s$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	$\frac{1}{2}$	$\frac{1}{2}$									
2	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$								
3	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$							
4	$\frac{1}{16}$	$\frac{1}{4}$	$\frac{3}{8}$	$\frac{1}{4}$	$\frac{1}{16}$						
5	$\frac{1}{32}$	$\frac{5}{32}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{5}{32}$	$\frac{1}{32}$					
6	$\frac{1}{64}$	$\frac{3}{32}$	$\frac{15}{64}$	$\frac{5}{16}$	$\frac{15}{64}$	$\frac{3}{32}$	$\frac{1}{64}$				
7	$\frac{1}{128}$	$\frac{7}{128}$	$\frac{21}{128}$	$\frac{35}{128}$	$\frac{35}{128}$	$\frac{21}{128}$	$\frac{7}{128}$	$\frac{1}{128}$			
8	$\frac{1}{256}$	$\frac{1}{32}$	$\frac{7}{64}$	$\frac{7}{32}$	$\frac{35}{128}$	$\frac{7}{32}$	$\frac{7}{64}$	$\frac{1}{32}$	$\frac{1}{256}$		
9	$\frac{1}{512}$	$\frac{9}{512}$	$\frac{9}{128}$	$\frac{21}{128}$	$\frac{63}{256}$	$\frac{63}{256}$	$\frac{21}{128}$	$\frac{9}{128}$	$\frac{9}{512}$	$\frac{1}{512}$	
10	$\frac{1}{1024}$	$\frac{5}{512}$	$\frac{45}{1024}$	$\frac{15}{128}$	$\frac{105}{512}$	$\frac{63}{256}$	$\frac{105}{512}$	$\frac{15}{128}$	$\frac{45}{1024}$	$\frac{5}{512}$	$\frac{1}{1024}$

Observe that at $n = 0$ the binomial law is δ_0, that is, Dirac mass at 0, with this corresponding to the fact that if you don't play the game, you will certainly not win. Also, at $n = 1$ we obtain the Bernoulli law $\frac{1}{2}(\delta_0 + \delta_1)$, from Proposition 6.1.

Finally, and importantly, for making sure that we have not messed up anything, let us check the total probability is 1. But this comes indeed from the binomial formula:

$$\begin{aligned} P &= \sum_{s=0}^{n} \frac{1}{2^n} \binom{n}{s} \\ &= \frac{1}{2^n} \sum_{s=0}^{n} \binom{n}{s} 1^s 1^{n-s} \\ &= \frac{1}{2^n}(1+1)^n \\ &= 1 \end{aligned}$$

Next, and more generally, again by following the material from chapter 2, let us do the same for a biased coin, landing on heads with probability $p \in [0, 1]$, and on tails with probability $1 - p$. We first have the following result, generalizing Proposition 6.1:

PROPOSITION 6.3. *When flipping a biased coin, with the probabilities being*

$$P(\text{heads}) = p \quad , \quad P(\text{tails}) = 1 - p$$

with $p \in [0, 1]$, the number of wins, meaning heads, can be $0, 1$, the probabilities being:

$$P(0) = 1 - p \quad , \quad P(1) = p$$

Your winning law is therefore the following probability measure,

$$b_p = (1 - p)\delta_0 + p\delta_1$$

called Bernoulli law of parameter $p \in [0, 1]$.

PROOF. This is indeed something self-explanatory, and trivial. □

Coming next, according to our study from chapter 2, we have the following fundamental result, coming as a joint generalization of Theorem 6.2 and Proposition 6.3:

THEOREM 6.4. *When flipping a biased coin n times in a row, the probabilities are:*

$$P(s \text{ heads}, n - s \text{ tails}) = \binom{n}{s} p^s (1 - p)^{n-s}$$

Thus, the number of wins, meaning heads, can be $s = 0, \ldots, n$, the probabilities being:

$$P(s) = \binom{n}{s} p^s (1 - p)^{n-s}$$

Your winning law is therefore the following probability measure,

$$b_{np} = \sum_{s=0}^{n} \binom{n}{s} p^s (1 - p)^{n-s} \delta_s$$

called binomial law of parameter $p \in [0, 1]$.

PROOF. This is again clear, because in order to reach to the situation in the statement, namely s heads and $n - s$ tails, we must select the s occurrences of heads, among the n total throws, and there are $\binom{n}{s}$ choices here, and then sum over these $\binom{n}{s}$ choices the common quantity $p^s(1 - p)^{n-s}$. Thus, we are led to the formulae in the statement. □

At the level of the numerics, if we can call these numerics, because we still have a parameter $p \in [0, 1]$ involved, the table is as follows, with the convention $q = 1 - p$:

$n\backslash s$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	q	p									
2	q^2	$2pq$	p^2								
3	q^3	$3pq^2$	$3p^2q$	p^3							
4	q^4	$4pq^3$	$6p^2q^2$	$4p^3q$	p^4						
5	q^5	$5pq^4$	$10p^2q^3$	$10p^3q^2$	$5p^4q$	p^5					
6	q^6	$6pq^5$	$15p^2q^4$	$20p^3q^3$	$15p^4q^2$	$6p^5q$	p^6				
7	q^7	$7pq^6$	$21p^2q^5$	$35p^3q^4$	$35p^4q^3$	$21p^5q^2$	$7p^6q$	p^7			
8	q^8	$8pq^7$	$28p^2q^6$	$56p^3q^5$	$70p^4q^4$	$56p^5q^3$	$28p^6q^2$	$8p^7q$	p^8		
9	q^9	$9pq^8$	$36p^2q^7$	$84p^3q^6$	$126p^4q^5$	$126p^5q^4$	$84p^6q^3$	$36p^7q^2$	$9p^8q$	p^9	
10	q^{10}	$10pq^9$	$45p^2q^8$	$120p^3q^7$	$210p^4q^6$	$252p^5q^5$	$210p^6q^4$	$120p^7q^3$	$45p^8q^2$	$10p^9q$	p^{10}

Observe that at $n = 0$ the binomial law is δ_0, that is, Dirac mass at 0, with this corresponding to the fact that if you don't play the game, you will certainly not win. Also, at $n = 1$ we obtain the Bernoulli law $(1-p)\delta_0 + p\delta_1$, from Proposition 6.3.

Finally, as usual, for making sure that we have not messed up anything, let us check the total probability is 1. But this comes indeed from the binomial formula:

$$\begin{aligned} P &= \sum_{s=0}^{n} \binom{n}{s} p^s (1-p)^{n-s} \\ &= (p + 1 - p)^n \\ &= 1 \end{aligned}$$

Time now for a conclusion, to all this? Good work that we did, in chapter 2, then in chapter 5, and then here, and as a very compact version of what we found, we have:

THEOREM 6.5. *When playing with a biased coin, your winning law is*

$$b_p = (1-p)\delta_0 + p\delta_1$$

the Bernoulli law of parameter $p \in [0, 1]$. When playing n times, your winning law is

$$b_{np} = \sum_{s=0}^{n} \binom{n}{s} p^s (1-p)^{n-s} \delta_s$$

called binomial law of parameter $p \in [0, 1]$.

PROOF. This is indeed a summary of what we did in chapter 2, in chapter 5, and then here, and perhaps even a summary of what we did so far in this book, the essentials of our study, I mean. As for the proof, this is trivial, but for the pleasure, let us recall it:

(1) In order to have s wins, meaning s heads and $n-s$ tails, we must select the s occurrences of heads, among the n throws, and there are $\binom{n}{s}$ choices here.

(2) And then, we must sum over these $\binom{n}{s}$ choices the common probability $p^s(1-p)^{n-s}$, for having s heads and $n-s$ tails. Thus, we are led to the formulae in the statement.

(3) So, this is for the story of our result, the conclusion being that, after 100+ pages of mathematics, that's all we have. Not bad, mathematics is trivial, believe me. □

Let us do now some computations. As a first concrete result about the binomial laws, regarding the mean and the variance, as introduced in chapter 5, we have:

THEOREM 6.6. *The binomial law b_{np} has the following properties:*

(1) *The mean is $E=np$.*
(2) *The variance is $V=np(1-p)$.*

PROOF. This is very standard, by using the binomial formula, as follows:

(1) We recall that the binomial law b_{np} is given by the following formula:

$$b_{np}=\sum_{s=0}^{n}\binom{n}{s}p^s(1-p)^{n-s}\delta_s$$

(2) Regarding the mean of a binomial variable $f:X\to\mathbb{R}$, the computation, based on a suitable application of the binomial formula, is as follows:

$$\begin{aligned}
E(f) &= \sum_{s=1}^{n}s\binom{n}{s}p^s(1-p)^{n-s}\\
&= \sum_{s=1}^{n}\frac{n!}{(s-1)!(n-s)!}p^s(1-p)^{n-s}\\
&= np\sum_{s=1}^{n}\frac{(n-1)!}{(s-1)!(n-s)!}p^{s-1}(1-p)^{n-s}\\
&= np\sum_{t=0}^{n-1}\binom{n-1}{t}p^t(1-p)^{n-t-1}\\
&= np(p+1-p)^{n-1}\\
&= np
\end{aligned}$$

(3) Coming next, with the same trick, we can compute the following quantity:

$$\begin{aligned}
E(f^2)-E(f) &= \sum_{s=2}^{n}(s^2-s)\binom{n}{s}p^s(1-p)^{n-s}\\
&= \sum_{s=2}^{n}\frac{k!}{(s-2)!(n-s)!}p^s(1-p)^{n-s}\\
&= n(n-1)p^2\sum_{s=2}^{n}\frac{(n-2)!}{(s-2)!(n-s)!}p^{s-2}(1-p)^{n-s}\\
&= n(n-1)p^2\sum_{t=0}^{n-2}\binom{n-2}{t}p^t(1-p)^{n-t-2}\\
&= n(n-1)p^2(p+1-p)^{n-2}\\
&= n(n-1)p^2
\end{aligned}$$

(4) Now by using the above formulae, we conclude that the variance of a binomial variable $V(f)=E(f^2)-E(f)^2$ is given by the following formula:

$$\begin{aligned}
V(f) &= [E(f^2)-E(f)]+E(f)-E(f)^2\\
&= n(n-1)p^2+np-(np)^2\\
&= np(1-p)
\end{aligned}$$

We are therefore led to the conclusions in the statement. □

Very nice all this, and we will be back to moment computations, with more results, regarding the higher moments and their versions, later in this chapter.

Finally, a word about dice, that we certainly spent some time with, in chapter 2, and then in chapter 5 too. Here things are a bit more complicated, for several reasons:

(1) As explained in chapters 2 and 5, there are several possible choices for the relevant random variable $f:X\to\mathbb{R}$, depending on the type of game that we are playing. You can for instance look for occurrences of 6, or look at the total sum, and so on.

(2) And then, unfortunately, for the most common type of game, which consists in looking at the sum $S:X\to\mathbb{R}$, we do not have yet the formula of the law. For more on this, we refer to the material from chapter 2, and to my discussion with rat there.

(3) In addition, an extra problem comes from the fact that dice can be biased or not, and with k faces instead of 6, and the most general case, that of an arbitrary k-faced biased die, corresponds to a generic discrete random variable. Which is too much.

In short, patience, and no worries, we will come back to this, once we will know more.

6b. Independence

Let us try now to understand, more systematically, the relation between the Bernoulli and binomial laws. Indeed, we know from the above that the Bernoulli laws produce the binomial laws, simply by iterating the game, from 1 throw to $n \in \mathbb{N}$ throws.

Obviously, what matters in all this is the "independence" of our coin throws. So let us record this finding, in the form of a rather informal statement, as follows:

THEOREM 6.7. *The following happen, in the context of the biased coin game:*

(1) *The Bernoulli laws b_p produce the binomial laws b_{np}, by iterating the coin game $n \in \mathbb{N}$ times, via the independence of the throws.*
(2) *We have in fact $b_{np} = b_p^{*n}$, with $*$ being the convolution operation for the real probability measures, given by $\delta_x * \delta_y = \delta_{x+y}$, and linearity.*

PROOF. Obviously, this is something a bit informal, but let us prove this as stated, and we will come back later to it, with precise definitions, theorems and everything. By using the binomial formula, with numbers formally replaced by Dirac masses, we have:

$$\begin{aligned} b_p^{*n} &= \big((1-p)\delta_0 + p\delta_1\big)^{*n} \\ &= \sum_{s=0}^{n} p^s(1-p)^{n-s}\binom{n}{s}\delta_0^{*(n-s)} * \delta_1^{*s} \\ &= \sum_{s=0}^{n} p^s(1-p)^{n-s}\binom{n}{s}\delta_s \\ &= b_{np} \end{aligned}$$

Thus, good news, save for some uncertainties regarding what independence exactly means, mathematically speaking, and more on this in a moment, theorem proved. □

Getting now to more formal mathematical work, let us start with the following straightforward definition, inspired by what happens for coins, dice and cards:

DEFINITION 6.8. *We say that two variables $f, g : X \to \mathbb{R}$ are independent when*

$$P(f = x, g = y) = P(f = x)P(g = y)$$

happens, for any $x, y \in \mathbb{R}$.

As already mentioned, this notion is something very intuitive, inspired by what happens for coins, dice and cards. There are of course many other examples available. However, more on this later, once we will fully understand what happens to the coins, with having Theorem 6.7 understood, both statement and proof, being our main objective.

As a first result now regarding independence, we have:

THEOREM 6.9. *Assuming that $f, g : X \to \mathbb{R}$ are independent, we have:*

$$E(fg) = E(f)E(g)$$

More generally, we have the following formula, for the mixed moments,

$$E(f^k g^l) = E(f^k)E(g^l)$$

and the converse holds, in the sense that this implies the independence of f, g.

PROOF. This is something straightforward, the idea being as follows:

(1) Regarding the first assertion, we have indeed the following computation:

$$\begin{aligned} E(fg) &= \sum_{xy} xyP(f = x, g = y) \\ &= \sum_{xy} xyP(f = x)P(g = y) \\ &= \sum_{x} xP(f = x) \sum_{y} yP(g = y) \\ &= E(f)E(g) \end{aligned}$$

(2) Regarding now the middle assertion, the computation is similar, as follows:

$$\begin{aligned} E(f^k g^l) &= \sum_{xy} x^k y^l P(f = x, g = y) \\ &= \sum_{xy} x^k y^l P(f = x)P(g = y) \\ &= \sum_{x} x^k P(f = x) \sum_{y} y^l P(g = y) \\ &= E(f^k)E(g^l) \end{aligned}$$

(3) As for the last assertion, we know from the computation in (2) that our mixed moment formula $E(f^k g^l) = E(f^k)E(g^l)$ is equivalent to the following formula:

$$\sum_{xy} x^k y^l P(f = x)P(g = y) = \sum_{xy} x^k y^l P(f = x, g = y)$$

But this amounts in saying that we must have, for any x, y:

$$P(f = x, g = y) = P(f = x)P(g = y)$$

Thus, our variables $f, g : X \to \mathbb{R}$ must be independent, as stated. □

Regarding now the convolution operation, motivated by what we found before, in relation with games, let us start with the following abstract definition:

DEFINITION 6.10. *Given a space X with a sum operation $+$, we can define the convolution of any two discrete probability measures on it,*

$$\mu = \sum_i a_i \delta_{x_i} \quad , \quad \nu = \sum_j b_j \delta_{y_j}$$

as being the discrete probability measure given by the following formula:

$$\mu * \nu = \sum_{ij} a_i b_j \delta_{x_i + y_j}$$

That is, the convolution operation $*$ is defined by $\delta_x * \delta_y = \delta_{x+y}$, and linearity.

As a first observation, our operation is well-defined, with $\mu * \nu$ being indeed a discrete probability measure, because the weights are positive, $a_i b_j \geq 0$, and their sum is:

$$\sum_{ij} a_i b_j = \sum_i a_i \sum_j b_j = 1 \times 1 = 1$$

Also, the above definition agrees with what we did before with coins, and Bernoulli and binomial laws. We have in fact the following general result:

THEOREM 6.11. *Assuming that $f, g : X \to \mathbb{R}$ are independent, we have*

$$\mu_{f+g} = \mu_f * \mu_g$$

where $*$ is the convolution of real probability measures.

PROOF. We have two possible proofs here, both instructive, as follows:

(1) We have indeed the following straightforward computation, based on the independence formula from Definition 6.8, and on Definition 6.10:

$$\begin{aligned}
\mu_{f+g} &= \sum_{x \in \mathbb{R}} P(f + g = x) \delta_x \\
&= \sum_{y,z \in \mathbb{R}} P(f = y, g = z) \delta_{y+z} \\
&= \sum_{y,z \in \mathbb{R}} P(f = y) P(g = z) \delta_y * \delta_z \\
&= \left(\sum_{y \in \mathbb{R}} P(f = y) \delta_y \right) * \left(\sum_{z \in \mathbb{R}} P(g = z) \delta_z \right) \\
&= \mu_f * \mu_g
\end{aligned}$$

(2) Alternatively, we have the following computation, again using independence:

$$\begin{aligned} M_k(f+g) &= E((f+g)^k) \\ &= \sum_r \binom{k}{r} E(f^r g^{k-r}) \\ &= \sum_r \binom{k}{r} M_r(f) M_{k-r}(g) \end{aligned}$$

On the other hand, we have as well the following computation:

$$\begin{aligned} \int_X x^k d(\mu_f * \mu_g)(x) &= \int_{X\times X} (x+y)^k d\mu_f(x) d\mu_g(y) \\ &= \sum_r \binom{k}{r} \int_X x^r d\mu_f(x) \int_X y^{k-r} d\mu_g(y) \\ &= \sum_r \binom{k}{r} M_r(f) M_{k-r}(g) \end{aligned}$$

Thus our measures have the same moments, so they coincide, as stated. □

Still in relation with the basic theory of independence, here is now a second result, coming as a continuation of Theorem 6.11, which is something more advanced:

THEOREM 6.12. *Assuming that $f, g : X \to \mathbb{R}$ are independent, we have*

$$F_{f+g} = F_f F_g$$

where $F_f(x) = E(e^{ixf})$ is the Fourier transform.

PROOF. We have the following computation, using Theorem 6.11:

$$\begin{aligned} F_{f+g}(x) &= \int_X e^{ixz} d\mu_{f+g}(z) \\ &= \int_X e^{ixz} d(\mu_f * \mu_g)(z) \\ &= \int_{X\times X} e^{ix(z+t)} d\mu_f(z) d\mu_g(t) \\ &= \int_X e^{ixz} d\mu_f(z) \int_X e^{ixt} d\mu_g(t) \\ &= F_f(x) F_g(x) \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Of course, you might wonder what $i \in \mathbb{C}$ has to do with all this. Good point, this is something quite subtle, and more on this later, trust me in the meantime.

And with this, end of our preliminary study of abstract independence. As a first application, we can now prove a theorem that we announced before, namely:

THEOREM 6.13. *The following happen, in the context of the biased coin game:*

(1) *The Bernoulli laws b_p produce the binomial laws b_{np}, by iterating the coin game $n \in \mathbb{N}$ times, via the independence of the throws.*
(2) *We have in fact $b_{np} = b_p^{*n}$, with $*$ being the convolution operation for the real probability measures, given by $\delta_x * \delta_y = \delta_{x+y}$, and linearity.*

PROOF. By using the binomial formula, with numbers formally replaced by Dirac masses, which is something that we can do, we have indeed the following computation:

$$\begin{aligned} b_p^{*n} &= \big((1-p)\delta_0 + p\delta_1\big)^{*n} \\ &= \sum_{s=0}^{n} p^s(1-p)^{n-s}\binom{n}{s}\delta_0^{*(n-s)} * \delta_1^{*s} \\ &= \sum_{s=0}^{n} p^s(1-p)^{n-s}\binom{n}{s}\delta_s \\ &= b_{np} \end{aligned}$$

Thus, up to the general the independence theory developed above, and with everything here doing well, as desired, we are led to the various conclusions in the statement. □

Moving on, as a second application of our independence technology, which is this time something new, partly solving some problems that we were having before, we have:

THEOREM 6.14. *When rolling a die n times, the measure*

$$\mu_n = \frac{1}{6^n}(\delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6)^{*n}$$

is the law of the sum $S : X \to \mathbb{R}$.

PROOF. Many things can be said here, the idea being as follows:

(1) To start with, the result is plainly clear, by using our independence theory above. Thus, we have our result, and with this answering some questions raised in chapter 2.

(2) Let us do as well some verifications, with the aim of recovering the formulae from chapter 2. At $n = 1$ we have indeed the measure in the statement, namely:

$$\mu_1 = \frac{1}{6}(\delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6)$$

(3) At $n = 2$ we have the following computation, giving the law from chapter 2:

$$\begin{aligned}
&\mu_2\\
=\ &\frac{1}{36}(\delta_1+\delta_2+\delta_3+\delta_4+\delta_5+\delta_6)*(\delta_1+\delta_2+\delta_3+\delta_4+\delta_5+\delta_6)\\
=\ &\frac{1}{36}(\delta_2+2\delta_3+3\delta_4+4\delta_5+5\delta_6+6\delta_7+5\delta_8+4\delta_9+3\delta_{10}+2\delta_{11}+\delta_{12})\\
=\ &\frac{1}{36}\delta_2+\frac{1}{18}\delta_3+\frac{1}{12}\delta_4+\frac{1}{9}\delta_5+\frac{5}{36}\delta_6+\frac{1}{6}\delta_7+\frac{5}{36}\delta_8+\frac{1}{9}\delta_9+\frac{1}{12}\delta_{10}+\frac{1}{18}\delta_{11}+\frac{1}{36}\delta_{12}
\end{aligned}$$

(4) At $n = 3$ the computation is as follows, again giving the law from chapter 3:

$$\begin{aligned}
&\mu_3\\
=\ &\mu_2*\mu_1\\
=\ &\frac{1}{216}(\delta_2+2\delta_3+3\delta_4+\ldots+3\delta_{10}+2\delta_{11}+\delta_{12})*(\delta_1+\ldots+\delta_6)\\
=\ &\frac{1}{216}(\delta_3+3\delta_4+6\delta_5+10\delta_6+15\delta_7+21\delta_8+25\delta_9+27\delta_{10}\\
&+27\delta_{11}+25\delta_{12}+21\delta_{13}+15\delta_{14}+10\delta_{15}+6\delta_{16}+3\delta_{17}+\delta_{18})\\
=\ &\frac{1}{216}\delta_3+\frac{1}{72}\delta_4+\frac{1}{36}\delta_5+\frac{5}{108}\delta_6+\frac{5}{72}\delta_7+\frac{7}{72}\delta_8+\frac{25}{216}\delta_9+\frac{1}{8}\delta_{10}\\
&+\frac{1}{8}\delta_{11}+\frac{25}{216}\delta_{12}+\frac{7}{72}\delta_{13}+\frac{5}{72}\delta_{14}+\frac{5}{108}\delta_{15}+\frac{1}{36}\delta_{16}+\frac{1}{72}\delta_{17}+\frac{1}{216}\delta_{18}
\end{aligned}$$

(5) At $n = 4$ now, where we are into uncharted territory, we have:

$$\begin{aligned}
&\mu_4\\
=\ &\mu_3*\mu_1\\
=\ &\frac{1}{1296}(\delta_3+3\delta_4+6\delta_5+\ldots+6\delta_{16}+3\delta_{17}+\delta_{18})*(\delta_1+\ldots+\delta_6)\\
=\ &\frac{1}{1296}(\delta_4+4\delta_5+10\delta_6+20\delta_7+35\delta_8+56\delta_9+80\delta_{10}+104\delta_{11}\\
&+125\delta_{12}+140\delta_{13}+146\delta_{14}+140\delta_{15}+125\delta_{16}\\
&+104\delta_{17}+80\delta_{18}+56\delta_{19}+35\delta_{20}+20\delta_{21}+10\delta_{22}+4\delta_{23}+\delta_{24})\\
=\ &\frac{1}{1296}\delta_4+\frac{1}{324}\delta_5+\frac{5}{648}\delta_6+\frac{5}{324}\delta_7+\frac{35}{1296}\delta_8+\frac{7}{162}\delta_9+\frac{5}{81}\delta_{10}+\frac{13}{162}\delta_{11}\\
&+\frac{125}{196}\delta_{12}+\frac{35}{324}\delta_{13}+\frac{73}{648}\delta_{14}+\frac{35}{324}\delta_{15}+\frac{125}{1296}\delta_{16}\\
&+\frac{13}{162}\delta_{17}+\frac{5}{81}\delta_{18}+\frac{7}{162}\delta_{19}+\frac{35}{1296}\delta_{20}+\frac{5}{324}\delta_{21}+\frac{5}{648}\delta_{22}+\frac{1}{324}\delta_{23}+\frac{1}{1296}\delta_{24}
\end{aligned}$$

(6) And so on, the idea being that what we have here, although not explicitly computing μ_n, is certainly better than our method using tables from chapter 2.

(7) As a comment now, you would certainly say here, yes quite nice all this, but this cannot be the end of the story, we would like to have the formula of the distribution. To which, I agree, and we will come back to this later, once we will know more things.

(8) Finally, for our discussion to be complete, let us discuss as well what happens for a biased die. Here the formula, generalizing the one in the statement, is as follows:

$$\mu_n = (p_1\delta_1 + p_2\delta_2 + p_3\delta_3 + p_4\delta_4 + p_5\delta_5 + p_6\delta_6)^{*n}$$

In the more general case of a k-faced biased die, the formula is as follows:

$$\mu_n = \left(\sum_i p_i\delta_i\right)^{*n}$$

As for the most general case, that of a k-faced biased die, with the faces of the die marked with arbitrary numbers $x_1, \ldots, x_k$, the formula here is as follows:

$$\mu_n = \left(\sum_i p_i\delta_{x_i}\right)^{*n}$$

And with this, end of mathematics I guess, this being far too general. So, as a conclusion, good to have the present theorem proved, and more about this later. □

Many other things can be done with independence, and we have for instance:

THEOREM 6.15. *When rolling a usual die n times in a row,*

$$E = 3.5^n$$

is the expectation of the product of the numbers that you get.

PROOF. This is something quite interesting, the idea being as follows:

(1) To start with, we can kill this with our independence technology. Indeed, this comes by using the multiplicativity formula for expectations in Theorem 6.9.

(2) Next, observe that, contrary to the study of the sum, where we have $E = 3.5n$, which is something quite trivial, available via several simple methods, as explained in chapter 5, in what regards the product our proof above, using the general independence theory and Theorem 6.9, seems to be pretty much the only one available.

(3) In short, the challenge is to find an elementary proof of the present theorem, without using independence. You can try here for instance the various simple methods from chapter 5, or a trick using a logarithmic die, or many more. Have fun with this. □

As a last thing to be discussed, in relation with independence, we have:

THEOREM 6.16. *Given variables $f, g : X \to \mathbb{R}$, we can talk about their covariance*

$$\begin{aligned} cov(f,g) &= E[(f-E(f))(g-E(g))] \\ &= E(fg)-E(f)E(g) \end{aligned}$$

with this quantity having the following properties:

(1) $cov(f,f) = V(f)$.

(2) *If f, g are independent, $cov(f,g) = 0$.*

(3) *The converse of this latter fact is, unfortunately, not true.*

PROOF. This is something very standard. To start with, we have the following computation, which shows that our two definitions for the covariance are equivalent:

$$\begin{aligned} E[(f-E(f))(g-E(g))] &= E[fg-E(f)g-fE(g)+E(f)E(g)] \\ &= E(fg)-E(f)E(g)-E(f)E(g)+E(f)E(g) \\ &= E(fg)-E(f)E(g) \end{aligned}$$

As for the various assertions in the statement, their proof goes as follows:

(1) This is indeed clear, with either of the definitions for the variance $V(f)$.

(2) This is clear too, coming from the multiplicativity formula from Theorem 6.9.

(3) To start with, the converse of (2) has obviously zero chances to hold, because we perfectly know from Theorem 6.9 that the independence of $f, g : X \to \mathbb{R}$ amounts in having the following formula, for the mixed moments, meaning for any $k, l \in \mathbb{N}$:

$$E(f^k g^l) = E(f^k)E(g^l)$$

(4) This being said, an explicit counterexample will certainly not hurt. Consider two Bernoulli variables $f, g : X \to \mathbb{R}$, taking their values according to the following table:

$g \backslash f$	a	b	
c	$pq+x$	$(1-p)q-x$	q
d	$p(1-q)-x$	$(1-p)(1-q)+x$	$1-q$
	p	$1-p$	

The covariance of f, g can be then computed as follows:

$$\begin{aligned} & cov(f,g) \\ = \;& E(fg)-E(f)E(g) \\ = \;& [ac(pq+x)+ad(p(1-q)-x)+bc((1-p)q-x)+bd((1-p)(1-q)+x)] \\ & -[ap+b(1-p)][cq+d(1-q)] \\ = \;& acx-adx-bcx+bdx \\ = \;& (a-b)(c-d)x \end{aligned}$$

Which is bad news, because $cov(f,g)=0$ means $x=0$, which in turn means that f,g must be independent. Damn, so instead of our counterexample, we have a theorem here, stating that the converse of (2) holds for the Bernoulli variables. Good to know.

(5) Counterexample, take two. In view of the above, consider the simplest possible situation which is not (Bernoulli, Bernoulli), which is as follows, with f following a uniform trivalent distribution on $[-1,1]$, and with g being taken to be its square, $g=f^2$:

$g\backslash f$	-1	0	1	
0	0	$1/3$	0	$1/3$
1	$1/3$	0	$1/3$	$2/3$
	$1/3$	$1/3$	$1/3$	

Our variables are then not independent, because the upper left 0 does not come as $0=1/3\cdot 1/3$. On the other hand we have $E(f)=0$, $E(g)=1/3$, $E(fg)=0$, so the covariance is $cov(f,g)=0-0=0$, and we have our counterexample, as desired. □

So long for independence, and related topics. Although exercises are not the strong feature of this book, we highly recommend finding and doing some, say on the internet, as to get familiar with tables as above, and their use in relation with independence.

6c. Higher moments

Getting back now to the binomial laws, let us discuss now the computation of their higher moments, as a continuation of Theorem 6.6. We first have here:

THEOREM 6.17. *The moments of the binomial law $P(s)=p^s(1-p)^{n-s}\binom{n}{s}$ are*

$$M_1=np$$
$$M_2=n(n-1)p^2+np$$
$$M_3=n(n-1)(n-2)p^3+3n(n-1)p^2+np$$
$$M_4=n(n-1)(n-2)(n-3)p^4+6n(n-1)(n-2)p^3+7n(n-1)p^2+np$$
$$\vdots$$

with the computation in general being possible by recurrence.

PROOF. The moments of the binomial law b_{np} of parameters $n\in\mathbb{N}$ and $p\in[0,1]$ are by definition given by the following formula:

$$M_k=\sum_{s=1}^{n}s^k\binom{n}{s}p^s(1-p)^{n-s}$$

We already know the first two formulae from Theorem 6.6 and its proof, and the continuation is by using the same trick as there, as follows:

(1) Regarding the third moment, we can use here the following formula, that you can come upon by some sort of reverse engineering, and I will leave this as an exercise:

$$\begin{aligned} s(s-1)(s-2)+3s(s-1)+s &= s(s^2-3s+2+3s-3+1)\\ &= s^3 \end{aligned}$$

Indeed, this gives the following formula for the third moment:

$$\begin{aligned} M_3 &= \sum_{s=1}^{n} s^3\binom{n}{s}p^s(1-p)^{n-s}\\ &= \sum_{s=1}^{n}\left[s(s-1)(s-2)+3s(s-1)+s\right]\binom{n}{s}p^s(1-p)^{n-s}\\ &= \sum_{s=3}^{n} s(s-1)(s-2)\binom{n}{s}p^s(1-p)^{n-s}\\ &\quad +3\sum_{s=2}^{n} s(s-1)\binom{n}{s}p^s(1-p)^{n-s}\\ &\quad +\sum_{s=1}^{n} s\binom{n}{s}p^s(1-p)^{n-s}\\ &= n(n-1)(n-2)\sum_{s=3}^{n}\binom{n-3}{s-3}p^s(1-p)^{n-s}\\ &\quad +3n(n-1)\sum_{s=2}^{n}\binom{n-2}{s-2}p^s(1-p)^{n-s}\\ &\quad +n\sum_{s=1}^{n}\binom{n-1}{s-1}p^s(1-p)^{n-s}\\ &= n(n-1)(n-2)p^3+3n(n-1)p^2+np \end{aligned}$$

(2) Regarding the fourth moment, we can use here the following formula, which again can be discovered via some routine work, say good exercise for you:

$$\begin{aligned} & s(s-1)(s-2)(s-3)+6s(s-1)(s-2)+7s(s-1)+s\\ = \;& s[(s-1)(s^2-5s+6+6s-12+7)+1]\\ = \;& s[(s-1)(s^2+s+1)+1]\\ = \;& s[s^3-1+1]\\ = \;& s^4 \end{aligned}$$

Indeed, this gives the following formula for the fourth moment:

$$\begin{aligned}
M_4 &= \sum_{s=4}^{n} s(s-1)(s-2)(s-3)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad +6\sum_{s=3}^{n} s(s-1)(s-2)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad +7\sum_{s=2}^{n} s(s-1)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad +\sum_{s=1}^{n} s\binom{n}{s}p^s(1-p)^{n-s}\\
&= n(n-1)(n-2)(n-3)\sum_{s=4}^{n}\binom{n-4}{s-4}p^s(1-p)^{n-s}\\
&\quad +6n(n-1)(n-2)\sum_{s=3}^{n}\binom{n-3}{s-3}p^s(1-p)^{n-s}\\
&\quad +7n(n-1)\sum_{s=2}^{n}\binom{n-2}{s-2}p^s(1-p)^{n-s}\\
&\quad +n\sum_{s=1}^{n}\binom{n-1}{s-1}p^s(1-p)^{n-s}\\
&= n(n-1)(n-2)(n-3)p^4+6n(n-1)(n-2)p^3+7n(n-1)p^2+np
\end{aligned}$$

(3) As a continuation of this, it is quite clear that we can compute M_k by recurrence. We will be back to this later, with more results on the subject. □

Let us record as well a result about the corresponding central moments:

THEOREM 6.18. *The central moments of the binomial law are*

$$M_1' = 0$$

$$M_2' = np(1-p)$$

$$M_3' = np(1-p)(1-2p)$$

$$M_4' = np(1-p)(1+(3n-6)p(1-p))$$

$$\vdots$$

with the computation in general being possible by recurrence.

PROOF. We recall from chapter 5 that the central moments of a variable $f : X \to \mathbb{R}$, designed for having $M_1' = 0$, $M_2' = V$, are the following numbers, with $E = E(f)$:

$$M_k' = E((f - E)^k)$$

Thus $M_1' = 0$, and the formula in the statement for $M_2' = V$ is the one from Theorem 6.6. Regarding now the higher moments, by the binomial formula, we have:

$$\begin{aligned} M_k' &= E\left(\sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r f^{k-r}\right) \\ &= \sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r M_{k-r} \\ &= \sum_{r=0}^{k-2}(-1)^r\binom{k}{r}E^r M_{k-r} + (-1)^{k-1}(k-1)E^k \end{aligned}$$

Now with $k = 3$, by using the formulae from Theorem 6.17, we obtain:

$$\begin{aligned} M_3' &= M_3 - 3EM_2 + 2E^3 \\ &= [n(n-1)(n-2)p^3 + 3n(n-1)p^2 + np] - 3np(n(n-1)p^2 + np) + 2(np)^3 \\ &= np(1-p)(1-2p) \end{aligned}$$

Similarly, at $k = 4$, again by using the formulae from Theorem 6.17, we have:

$$\begin{aligned} & M_4' \\ = \ & M_4 - 4EM_3 + 6E^2M_2 - 3E^4 \\ = \ & n(n-1)(n-2)(n-3)p^4 + 6n(n-1)(n-2)p^3 + 7n(n-1)p^2 + np \\ & -4np[n(n-1)(n-2)p^3 + 3n(n-1)p^2 + np] + 6(np)^2(n(n-1)p^2 + np) - 3(np)^4 \\ = \ & np(1-p)(1 + (3n-6)p(1-p)) \end{aligned}$$

As for the last assertion, we will be back to it later, with details. □

Let us end this discussion with the following result, capturing the essentials:

THEOREM 6.19. *The mean, variance, skewness and kurtosis of b_{np} are*

$$E = np \quad , \quad V = npq \quad , \quad \gamma = \frac{q-p}{\sqrt{npq}} \quad , \quad \kappa = 3 + \frac{1-6pq}{npq}$$

with the convention $q = 1 - p$.

PROOF. We know the first two formulae, from Theorem 6.6. Regarding the last two formulae, we recall from chapter 5 that the skewness γ and kurtosis κ of a variable $f : X \to \mathbb{R}$ are its third and fourth normalized central moments, with these latter

moments, designed for having $M_0''=1$, $M_1''=0$, $M_2''=1$, being the following numbers, with $E=E(f)$ as usual, and with $\sigma=\sqrt{V}$ being the standard deviation:

$$M_k''=E\left(\left(\frac{f-E}{\sigma}\right)^k\right)$$

Thus, we can use the central moment formulae from Theorem 6.18. Observe first that with the convention $q=1-p$, our formulae for M_3',M_4' there read:

$$M_3'=npq(q-p)\quad,\quad M_4'=npq(1+(3n-6)pq)$$

Now by dividing respectively by $\sigma^3=V\sqrt{V}$ and $\sigma^4=V^2$, we obtain the formulae in the statement for γ and κ. Needless to say, the higher normalized central moments can be computed too, and we will back to this later, with some explicit results. □

Finally, let us record as well a result regarding the Fourier transform:

THEOREM 6.20. *The Fourier transform of the binomial law is given by:*

$$F_f(x)=(1-p+pe^{ix})^n$$

In particular, we can see that $\log F$ *is linear in* n*, as it should.*

PROOF. We have indeed the following straightforward computation:

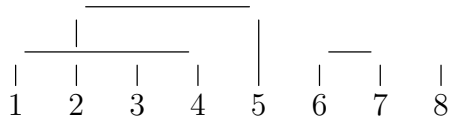
$$\begin{aligned}
F_f(x)&=E(e^{ixf})\\
&=\sum_{s=0}^n\binom{n}{s}p^s(1-p)^{n-s}e^{ixs}\\
&=(1-p)^n\sum_{s=0}^n\binom{n}{s}p^s(1-p)^{-s}e^{ixs}\\
&=(1-p)^n\sum_{s=0}^n\binom{n}{s}\left(\frac{p}{1-p}\,e^{ix}\right)^s\\
&=(1-p)^n\left(1+\frac{p}{1-p}\,e^{ix}\right)^n\\
&=(1-p+pe^{ix})^n
\end{aligned}$$

As for the last assertion, this is just an observation, to be related to Theorem 6.12. □

6d. Partitions, blocks

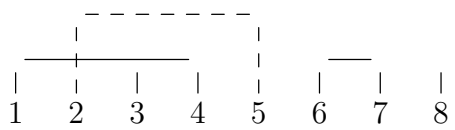
We would like to discuss, as a last topic for this chapter, a more conceptual and powerful approach to the computation of the moments of the binomial laws. Let us start with something nice, fundamental, and seemingly unrelated, namely:

DEFINITION 6.21. *We denote by $P(k)$ the set of partitions of $\{1,\ldots,k\}$, with these partitions $\pi\in P(k)$ being most conveniently being drawn as diagrams,*



with the strings joining the numbers belonging to the same block of π. That is, the above diagram represents the partition $\{1,\ldots,8\}=\{1,3,4\}\cup\{2,5\}\cup\{6,7\}\cup\{8\}$.

Observe that there is a bit of care to be taken with this convention, with respect to the crossings. We can either proceed as above, with the $\{2,5\}$ block being respresented "under" the block $\{1,3,4\}$, or use different types of strings, as for instance:



Both conventions are good, and we will be mostly using here the first one, that from Definition 6.21, which in practice leads to quicker drawings.

Now let us go back to the binomial laws. We have the following result, about them:

THEOREM 6.22. *The moments of the binomial law b_{np} are given by*

$$M_k=\sum_{\pi\in P(k)}\frac{n!}{(n-|\pi|)!}\,p^{|\pi|}$$

with $|.|$ being the number of blocks.

PROOF. This is something very standard, the idea being as follows:

(1) Some numerics first. At $k=1$ we only have one partition, namely $|$, and the formula in the statement holds indeed, as shown by the following computation:

$$\begin{aligned}\sum_{\pi\in P(1)}\frac{n!}{(n-|\pi|)!}\,p^{|\pi|}&=\frac{n!}{(n-|\,|\,|)!}\,p^{|\,|\,|}\\&=\frac{n!}{(n-1)!}\,p^1\\&=np\end{aligned}$$

(2) At $k=2$ now, we have two partitions, namely $||$ and $\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}\sum_{\pi\in P(2)}\frac{n!}{(n-|\pi|)!}p^{|\pi|} &= \frac{n!}{(n-|\ ||\ |)!}p^{|\ ||\ |}+\frac{n!}{(n-|\sqcap|)!}p^{|\sqcap|}\\ &= \frac{n!}{(n-2)!}p^2+\frac{n!}{(n-1)!}p^1\\ &= n(n-1)p^2+np\end{aligned}$$

(3) At $k=3$ we have 5 partitions, namely $|\,|\,|$, $\sqcap\,|$, $|\sqcap$, $|\sqcap$, $\sqcap\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}\sum_{\pi\in P(3)}\frac{n!}{(n-|\pi|)!}p^{|\pi|} &= \frac{n!}{(n-|\ |||\ |)!}p^{|\ |||\ |}+\ldots+\frac{n!}{(n-|\sqcap\sqcap|)!}p^{|\sqcap\sqcap|}\\ &= \frac{n!}{(n-3)!}p^3+3\cdot\frac{n!}{(n-2)!}p^2+\frac{n!}{(n-1)!}p^1\\ &= n(n-1)(n-2)p^3+3n(n-1)p^2+np\end{aligned}$$

(4) At $k=4$ we have 15 partitions, with the list of relevant partitions, and their multiplicities up to permutations, which is self-explanatory, being as follows:

$$|\,|\,|\,|\times 1\quad,\quad \sqcap\,|\,|\times 6\quad,\quad \sqcap\sqcap\times 3\quad,\quad \sqcap\sqcap\,|\times 4\quad,\quad \sqcap\sqcap\sqcap\times 1$$

Now by doing the computation, as before, the formula in the statement holds again:

$$\begin{aligned}&\sum_{\pi\in P(4)}\frac{n!}{(n-|\pi|)!}p^{|\pi|}\\ =\ &\frac{n!}{(n-|\ ||||\ |)!}p^{|\ ||||\ |}+\ldots\ldots+\frac{n!}{(n-|\sqcap\sqcap\sqcap|)!}p^{|\sqcap\sqcap\sqcap|}\\ =\ &\frac{n!}{(n-4)!}p^4+6\cdot\frac{n!}{(n-3)!}p^3+(3+4)\cdot\frac{n!}{(n-2)!}p^2+\frac{n!}{(n-1)!}p^1\\ =\ &n(n-1)(n-2)(n-3)p^4+6n(n-1)(n-2)p^3+7n(n-1)p^2+np\end{aligned}$$

(5) In general now, in order to prove the result, let us go back to our computations from the proof of Theorem 6.17. The idea there was that of using a formula as follows:

$$\begin{aligned}s^k &= s(s-1)\ldots(s-k+1)\\ &\quad +c_1s(s-1)\ldots(s-k+2)\\ &\quad \vdots\\ &\quad +c_{k-2}s(s-1)\\ &\quad +s\end{aligned}$$

(6) Indeed, assuming that we have such a magic formula, we obtain:

$$\begin{aligned}
M_k &= \sum_{s=k}^{n} s(s-1)\ldots(s-k+1)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad +c_1\sum_{s=k-1}^{n} s(s-1)\ldots(s-k+2)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad \vdots\\
&\quad +c_{k-2}\sum_{s=2}^{n} s(s-1)\binom{n}{s}p^s(1-p)^{n-s}\\
&\quad +\sum_{s=1}^{n} s\binom{n}{s}p^s(1-p)^{n-s}\\
&= n(n-1)\ldots(n-k+1)\sum_{s=k}^{n}\binom{n-k}{s-k}p^s(1-p)^{n-s}\\
&\quad +c_1n(n-1)\ldots(n-k+2)\sum_{s=k-1}^{n}\binom{n-k+1}{s-k+1}p^s(1-p)^{n-s}\\
&\quad \vdots\\
&\quad +c_{k-2}n(n-1)\sum_{s=2}^{n}\binom{n-2}{s-2}p^s(1-p)^{n-s}\\
&\quad +n\sum_{s=1}^{n}\binom{n-1}{s-1}p^s(1-p)^{n-s}
\end{aligned}$$

(7) Thus, we are led to the following formula, for the k-th moment:

$$\begin{aligned}
M_k &= n(n-1)\ldots(n-k+1)p^k\\
&\quad +c_1n(n-1)\ldots(n-k+2)p^{k-1}\\
&\quad \vdots\\
&\quad +c_{k-2}n(n-1)p^2\\
&\quad +np
\end{aligned}$$

(8) The problem is now, how to find that magic formula from (5)? And the answer here comes from partitions. Indeed, with the standard convention that for a multi-index

$i=(i_1,\ldots,i_k)$, its kernel is the partition $\ker i\in P(k)$ joining equal indices, we have:

$$\begin{aligned}s^k&=\sum_{i_1=1}^{s}\ldots\sum_{i_k=1}^{s}1\\&=\sum_{\pi\in P(k)}\#\left\{(i_1,\ldots,i_k)\in\{1,\ldots,s\}^k\,\middle|\,\ker i=\pi\right\}\\&=\sum_{\pi\in P(k)}\frac{s!}{(s-|\pi|)!}\end{aligned}$$

(9) Thus, good news, we have the magic formula that we need as data in (5), and according now to (7), we are led to the following formula, for the moment:

$$M_k=\sum_{\pi\in P(k)}\frac{n!}{(n-|\pi|)!}\,p^{|\pi|}$$

Thus, we have indeed the formula in the statement. □

We will be back to this, moments and partitions, many times in what follows. In fact, doing such combinatorics will be a main theme of discussion, in this book.

6e. Exercises

This was our first truly advanced chapter, and as exercises, we have:

EXERCISE 6.23. *Work out various asymptotics for the binomial laws.*

EXERCISE 6.24. *Find some interesting probability spaces X, having a sum $+$.*

EXERCISE 6.25. *Learn, from a calculus book, about the convolution of functions.*

EXERCISE 6.26. *Have a look as well at the convolution of abstract measures.*

EXERCISE 6.27. *Meditate about the need, or not, for $i\in\mathbb{C}$, at Fourier.*

EXERCISE 6.28. *Compute the law of the sum, when rolling a die 5 times.*

EXERCISE 6.29. *Compute the law of the sum, when rolling a die n times.*

EXERCISE 6.30. *Learn more about partitions, and Bell and Stirling numbers.*

As bonus exercise, learn about the $51-49$ law. Theory is not everything.

CHAPTER 7

Pascal distributions

7a. Negative binomials

We have seen so far the basics of probability theory, mainly illustrated by the binomial laws, and with these laws coming from the binomial formula, namely:

$$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k}$$

End of the story with the binomial laws, you would say? Not so quick, because the binomial formula has a number of generalizations, involving exponents $n\in\mathbb{R}$, which can be used in order to construct certain useful versions of the binomial laws.

Let us start our discussion here with the following key result:

THEOREM 7.1. *We have the generalized binomial formula*

$$(1+x)^n=\sum_{k=0}^{\infty}\binom{n}{k}x^k$$

with the generalized binomial coefficients being given by

$$\binom{n}{k}=\frac{n(n-1)\ldots(n-k+1)}{k!}$$

valid for any exponent $n\in\mathbb{Z}$, and any $|x|<1$.

PROOF. This is something very standard, the idea being as follows:

(1) For exponents $n\in\mathbb{N}$, this is something that we know well from chapter 1, and which is valid for any $x\in\mathbb{R}$, coming from the usual binomial formula, namely:

$$(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k$$

(2) For the exponent $n=-1$ this is something that we know from chapter 1 too, coming from the following formula, valid for any $|x|<1$:

$$\frac{1}{1+x}=1-x+x^2-x^3+\ldots$$

Indeed, this is exactly our generalized binomial formula at $n = -1$, because:

$$\binom{-1}{k} = \frac{(-1)(-2)\dots(-k)}{k!} = (-1)^k$$

(3) Let us discuss now the general case $n \in -\mathbb{N}$. With $n = -m$ and $m \in \mathbb{N}$, the generalized binomial coefficients are given by the following formula:

$$\begin{aligned}\binom{-m}{k} &= \frac{(-m)(-m-1)\dots(-m-k+1)}{k!}\\ &= (-1)^k\frac{m(m+1)\dots(m+k-1)}{k!}\\ &= (-1)^k\frac{(m+k-1)!}{(m-1)!k!}\\ &= (-1)^k\binom{m+k-1}{m-1}\end{aligned}$$

Thus, our generalized binomial formula at $n = -m$ and $m \in \mathbb{N}$ reads:

$$\frac{1}{(1+t)^m} = \sum_{k=0}^{\infty}(-1)^k\binom{m+k-1}{m-1}t^k$$

(4) In order to prove this formula, it is convenient to write it with $-t$ instead of t, in order to get rid of signs. The formula to be proved becomes:

$$\frac{1}{(1-t)^m} = \sum_{k=0}^{\infty}\binom{m+k-1}{m-1}t^k$$

(5) We prove this by recurrence on m. At $m = 1$ this formula definitely holds, as explained in (2) above. So, assume that the formula holds at $m \in \mathbb{N}$. We have then:

$$\begin{aligned}\frac{1}{(1-t)^{m+1}} &= \frac{1}{1-t}\cdot\frac{1}{(1-t)^m}\\ &= \sum_{k=0}^{\infty}t^k\sum_{l=0}^{\infty}\binom{m+l-1}{m-1}t^l\\ &= \sum_{s=0}^{\infty}t^s\sum_{l=0}^{s}\binom{m+l-1}{m-1}\end{aligned}$$

On the other hand, the formula that we want to prove is:

$$\frac{1}{(1-t)^{m+1}} = \sum_{s=0}^{\infty}\binom{m+s}{m}t^k$$

Thus, in order to finish, we must prove the following formula:

$$\sum_{l=0}^{s}\binom{m+l-1}{m-1}=\binom{m+s}{m}$$

(6) In order to prove this latter formula, we proceed by recurrence on $s\in\mathbb{N}$. At $s=0$ the formula is trivial, $1=1$. So, assume that the formula holds at $s\in\mathbb{N}$. In order to prove the formula at $s+1$, we are in need of the following formula:

$$\binom{m+s}{m}+\binom{m+s}{m-1}=\binom{m+s+1}{n}$$

But this is the Pascal formula, that we know from chapter 1, and we are done. □

We will see later in this chapter that the generalized binomial formula from Theorem 7.1 holds in fact for any exponent $n\in\mathbb{R}$. For the moment, what we have will do.

By the way, talking about what will do, let us record the following more digest formulation of Theorem 7.1, corresponding to the formula (4) in its proof:

THEOREM 7.2. *We have the following inversion formula,*

$$\frac{1}{(1-t)^m}=\sum_{k=0}^{\infty}\binom{m+k-1}{m-1}t^k$$

valid for any $|t|<1$.

PROOF. As mentioned, this is indeed what we proved, in the proof of Theorem 7.1, and with this being equivalent to Theorem 7.1, for the exponents $n\in-\mathbb{N}$. □

Going ahead now with some probability, with the idea in mind of encoding the above binomials into a "negative" version of the binomial law.. excuse me, but cat, that we haven't met since chapter 2, is here, meowing something. What is it, cat?

CAT 7.3. *Congratulations boss, with your new binomial formula, you are good for some complex analysis.*

Thanks cat, and indeed, our formula is something quite subtle, which can be useful for many other purposes, including complex analysis. So, with us never being in a hurry, a bit like cats, let us explore this first, who knows when we will need such things.

Let us start our discussion with some real analysis. The most basic functions are the polynomials, $P\in\mathbb{R}[X]$, and although many other interesting functions exist in this world, such as sin, cos, exp, log and so on, when studying functions, in order to really take off from the polynomial level, the wisest way is by looking at the rational functions:

DEFINITION 7.4. *A rational function is a formal quotient of polynomials:*

$$f = \frac{P}{Q}$$

When assuming $(P, Q) = 1$, we can view f as a usual, continuous function

$$f : \mathbb{R} - P_f \to \mathbb{R} \quad , \quad x \to \frac{P(x)}{Q(x)}$$

with $P_f \subset \mathbb{R}$ being the set of zeroes Q, also called poles of f.

The rational functions are quite interesting objects, with their algebra and analysis generalizing that of the polynomials, quite often in a straightforward way. To start with, the rational functions add, multiply and divide according to the following formulae:

$$\frac{P}{Q} + \frac{R}{S} = \frac{PS + QR}{QS} \quad , \quad \frac{P}{Q} \cdot \frac{R}{S} = \frac{PR}{QS} \quad , \quad \frac{P}{Q} : \frac{R}{S} = \frac{PS}{QR}$$

The rational functions are stable as well by composition, according to the following computation, m, n being the degrees of P, Q, and P', Q' being certain polynomials:

$$\frac{P}{Q} \circ \frac{R}{S} = \frac{P(R/S)}{Q(R/S)} = \frac{P'/S^m}{Q'/S^n} = \frac{P'S^n}{Q'S^m}$$

We know from Definition 7.4 that given a rational function $f = P/Q$, it is best to assume that the polynomials P, Q are prime to each other, $(P, Q) = 1$, as for the zeroes of Q to be exactly the poles of f. We can further build on this, as follows:

PROPOSITION 7.5. *Any rational function can be written as*

$$f(x) = \frac{A_1(x)}{(x - r_1)^{m_1}} + \ldots + \frac{A_s(x)}{(x - r_s)^{m_s}} + \frac{B(x)}{C(x)}$$

with $r_1, \ldots, r_s \in \mathbb{R}$ being the poles, and with C having no roots.

PROOF. This comes via some standard algebra, the idea being as follows:

(1) To start with, any rational function, $f = P/Q$ with $(P, Q) = 1$, can be written as follows, with $r_1, \ldots, r_s \in \mathbb{R}$ being the poles, $P(r_i) \neq 0$, and with C having no roots:

$$f(x) = \frac{P(x)}{(x - r_1)^{m_1} \ldots (x - r_s)^{m_s} C(x)}$$

(2) Next, we will need the standard fact that given two polynomials which are prime to each other, $(E, F) = 1$, we can always find two polynomials A, B such that:

$$AF + BE = 1$$

Indeed, this is something very standard, exactly as the similar result for numbers, that you surely know. So, consider the following d polynomials, with $d = \deg E$:

$$F, xF, x^2F, \ldots, x^{d-1}F$$

These polynomials are then, modulo scalars, the various remainders modulo E, so we conclude that, again modulo E and modulo scalars, we have the following equality:

$$\{F, xF, x^2F, \ldots, x^{d-1}F\} = \{1, x, x^2, \ldots, x^{d-1}\}$$

In particular $AF = 1(E)$ modulo scalars, for some $A = x^k$, which means $AF + BE = 1$ modulo scalars, for some A, B, and by dividing by the scalar, $AF + BE = 1$.

(3) Now observe that the formula $AF + BE = 1$ found above can be written as:

$$\frac{1}{EF} = \frac{A}{E} + \frac{B}{F}$$

Thus, we can apply this trick in the context of (1), and we obtain the result. □

Getting now to complex scalars, we can improve Proposition 7.5, as follows:

THEOREM 7.6. *Any complex rational function can be written as*

$$f(x) = \frac{A_1(x)}{(x - r_1)^{m_1}} + \ldots + \frac{A_k(x)}{(x - r_s)^{m_s}}$$

with $r_1, \ldots, r_s \in \mathbb{C}$ being the poles.

PROOF. What we did in the above extends to the case of complex rational functions, in the obvious way, and the point is that, since any complex polynomial has roots, in the context of the formula from Proposition 7.5, the last term there, B/C, dissapears. □

Getting now to where we wanted to get, the point is that by using Theorem 7.1, or rather its more digest form, Theorem 7.2, we can complement Theorem 7.6 with:

THEOREM 7.7 (addendum). *We have the following formula, for $|x| < r$,*

$$\frac{1}{(r - x)^m} = \frac{1}{r^m} \sum_{k=0}^{\infty} \binom{m + k - 1}{m - 1} \left(\frac{x}{r}\right)^k$$

which computes the rational functions, written as $f(x) = \sum_i A_i(x)/(r_i - x)^{m_i}$.

PROOF. This comes indeed from the negative binomial formula in Theorem 7.2, or rather from its more digest formulation, Theorem 7.2, by setting $t = x/r$ there. □

Which sounds very good, we are now experts in complex analysis. This being said, before going ahead with probability, let us listen as well to what rat has to say.

We haven't met rat in a while either, also since chapter 2, and some strange things happened, in the meantime. For unknown reasons, rat has traded his business suits for colorful clothes, also ditched his trademark cigars, although I can see that he's still a smoker, and he's driving now an old VW van. And, stopping by, he says:

RAT 7.8. *Mate, sorry for that wrong gaming advice I gave you in chapter 2. You should go for the dice sum, that is luminous. Peace upon you.*

Okay, thanks rat, and good to see that you enjoy your new life. By the way, careful with cat, although peaceful as usual, he's still not vegetarian, as far as I know.

Getting now to what rat says, it makes sense indeed, now that we have new binomial technology coming from Theorem 7.2, to have a new look at the dice sum problem. And, remarkably, we can now fully solve that problem, the result being as follows:

THEOREM 7.9. *When rolling a die n times, the distribution of the sum is*

$$P(s)=\frac{1}{6^n}\sum_{k=0}^{[\frac{s-n}{6}]}(-1)^k\binom{n}{k}\binom{s-6k-1}{n-1}$$

with this coming from the binomial formula with negative exponents.

PROOF. This is something quite tricky, the idea being as follows:

(1) To start with, as explained in chapter 6, the law of the sum is:

$$\mu_n=\frac{1}{6^n}(\delta_1+\delta_2+\delta_3+\delta_4+\delta_5+\delta_6)^{*n}$$

(2) Equivalently, when thinking a bit, we have the following formula for the law of the sum, and I will leave it to you, to clarify the details here:

$$\sum_{s=n}^{6n}P(s)x^s=\frac{1}{6^n}(x+x^2+x^3+x^4+x^5+x^6)^n$$

(3) So, let us compute the function on the right. This is given by:

$$\begin{aligned}f(x)&=\frac{1}{6^n}(x+x^2+x^3+x^4+x^5+x^6)^n\\&=\frac{x^n}{6^n}(1+x+x^2+x^3+x^4+x^5)^n\\&=\frac{x^n}{6^n}\cdot\frac{(1-x^6)^n}{(1-x)^n}\end{aligned}$$

(4) By using the usual binomial formula for the numerator $(1-x^6)^n$, and the formula from Theorem 7.2 for the fraction $1/(1-x)^n$, we obtain the following formula:

$$\begin{aligned}f(x)&=\frac{x^n}{6^n}\sum_{k=0}^{n}(-1)^k\binom{n}{k}x^{6k}\sum_{l=0}^{\infty}\binom{n+l-1}{n-1}x^l\\&=\frac{1}{6^n}\sum_{k=0}^{n}\sum_{l=0}^{\infty}(-1)^k\binom{n}{k}\binom{n+l-1}{n-1}x^{n+6k+l}\\&=\frac{1}{6^n}\sum_{s=0}^{\infty}\sum_{k=0}^{n}(-1)^k\binom{n}{k}\binom{s-6k-1}{n-1}x^s\end{aligned}$$

(5) Now remember that f was a polynomial of degree $6n$, divisible by x^n. Thus, the true range of the first summing index is $s=n,\ldots,6n$. Also, from $s=n+6k+l$ in the above computation, we get $s\geq n+6k$, and so $k\leq[(s-n)/6]$, integer part. Thus, our formula in (4), written by ignoring zero coefficients appearing from cancellation, is:

$$f(x)=\frac{1}{6^n}\sum_{s=n}^{6n}\sum_{k=0}^{[\frac{s-n}{6}]}(-1)^k\binom{n}{k}\binom{s-6k-1}{n-1}x^s$$

But with this, we are led via (2) to the formula in the statement.

(6) Finally, let us doublecheck this. At $n=1$ our formula is as follows, correct:

$$P(s)=\frac{1}{6}\sum_{k=0}^{[\frac{s-1}{6}]}(-1)^k\binom{1}{k}\binom{s-6k-1}{0}=\frac{1}{6}(-1)^0\binom{1}{0}\binom{s-1}{0}=\frac{1}{6}$$

At $n=2$ the formula that we found is as follows, which is correct too:

$$\begin{aligned}P(s)&=\frac{1}{36}\sum_{k=0}^{[\frac{s-2}{6}]}(-1)^k\binom{1}{k}\binom{s-6k-1}{1}\\&=\frac{1}{36}\sum_{k=0}^{[\frac{s-2}{6}]}(-1)^k(s-6k-1)\\&=\frac{1}{36}\times(1,2,3,4,5,6,5,4,3,2,1)\end{aligned}$$

(7) And so on, and I will leave the next verifications, at $n=3,4$, which fit indeed with what we previously found in chapter 6, to you, as an exercise. □

And with this, end of our preliminary discussion on Theorem 7.1, and its various ramifications. Good learning that was, and thanks to everyone involved.

7b. Pascal distributions

Getting back now to our regular business, based on the generalized binomial formula established above, at negative integer values of the exponent, or rather on Theorem 7.2, which was the digest version of it, we can formulate the following definition:

DEFINITION 7.10. *The negative binomial law c_{mp}, with $m\in\mathbb{N}$ and $p\in[0,1]$, is:*

$$P(s)=\binom{s+m-1}{s}(1-p)^sp^m$$

We also call this Pascal law of parameters $m\in\mathbb{N}$ and $p\in[0,1]$.

The relation with the negative binomial coefficients comes from:

$$\binom{s+m-1}{s} = (-1)^s\binom{-m}{s}$$

Indeed, by using this formula, we can write our law as follows:

$$P(s) = (-1)^s\binom{-m}{s}(1-p)^s p^m = \binom{-m}{s}(p-1)^s p^m$$

As a consequence of this, we have indeed a probability measure, as shown by:

$$\begin{aligned}\sum_{s\geq 0} P(s) &= \sum_{s\geq 0}\binom{-m}{s}(p-1)^s p^m\\ &= p^m\sum_{s\geq 0}\binom{-m}{s}(p-1)^s\\ &= p^m[1+(p-1)]^{-m}\\ &= p^m p^{-m}\\ &= 1\end{aligned}$$

Let us record this finding, which is something quite interesting, as follows:

PROPOSITION 7.11. *The negative binomial law c_{mp} is given by*

$$P(s) = \binom{-m}{s}(p-1)^s p^m$$

with $\binom{-m}{s}$ being a generalized binomial coefficient.

PROOF. This follows indeed from the above discussion, and with the remark that, in view of our mass 1 computation above, the present interpretation of the negative binomial law, with a generalized binomial coefficient as above, is the one that we will prefer. □

Before going further with our mathematics, you might certainly have this question, what are the negative binomial laws good for? In answer, many things, and as a very standard result here, which is similar to the one for usual binomial laws, we have:

THEOREM 7.12. *When flipping a biased coin until reaching to m heads,*

$$P(s \text{ tails}) = \binom{s+m-1}{s}(1-p)^s p^m$$

and so, c_{mp} is the law of the number of failures, when playing this game.

PROOF. When computing $P(s \text{ tails})$, we certainly have the $(1-p)^s p^m$ factor, coming from the m heads and s tails. As for the multiplicity, this is the binomial coefficient in the statement, coming from choosing the positions of the s tails, among the total of $s+m-1$ attempts, up to the last one, which does not count, because it must be heads. □

Summarizing, what we have is a useful generalization of the usual binomial laws. The negative binomial laws appear in many other concrete situations, quite often in relation with variations of Theorem 7.12, and I will leave some further learning here to you.

Regarding now the basic properties of these laws, these are as follows:

THEOREM 7.13. *The negative binomial law c_{mp} has the following properties:*

(1) *The mean is $E = \frac{m(1-p)}{p}$.*
(2) *The variance is $V = \frac{m(1-p)}{p^2}$.*

PROOF. This is indeed very standard, a bit as before for the binomial laws:

(1) Regarding the mean, this can be computed as follows:

$$\begin{aligned}
E &= \sum_{s\geq 1} sP(s)\\
&= \sum_{s\geq 1} s\binom{-m}{s}(p-1)^s p^m\\
&= \sum_{s\geq 1} -m\binom{-m-1}{s-1}(p-1)^s p^m\\
&= -mp^m(p-1)\sum_{s\geq 1}\binom{-m-1}{s-1}(p-1)^{s-1}\\
&= mp^m(1-p)[1+(p-1)]^{-m-1}\\
&= mp^m(1-p)p^{-m-1}\\
&= \frac{m(1-p)}{p}
\end{aligned}$$

To be more precise, we have used in the beginning the following formula:

$$\begin{aligned}
s\binom{-m}{s} &= s\,\frac{(-m)(-m-1)\ldots(-m-s+1)}{s!}\\
&= \frac{(-m)(-m-1)\ldots(-m-s+1)}{(s-1)!}\\
&= -m\,\frac{(-m-1)\ldots(-m-s+1)}{(s-1)!}\\
&= -m\binom{-m-1}{s-1}
\end{aligned}$$

(2) In order to compute now the second moment and the variance, we can use a similar trick. To start with, we have the following computation:

$$\begin{aligned} s(s-1)\binom{-m}{s} &= s(s-1)\,\frac{(-m)(-m-1)\dots(-m-s+1)}{s!} \\ &= \frac{(-m)(-m-1)\dots(-m-s+1)}{(s-2)!} \\ &= -m(-m-1)\,\frac{(-m-2)\dots(-m-s+1)}{(s-2)!} \\ &= m(m-1)\binom{-m-2}{s-2} \end{aligned}$$

Now by using this formula, we can compute the difference $M_2 - M_1$, as follows:

$$\begin{aligned} M_2 - M_1 &= \sum_{s\geq 2}(s^2-s)P(s) \\ &= \sum_{s\geq 2} s(s-1)\binom{-m}{s}(p-1)^s p^m \\ &= \sum_{s\geq 2} m(m+1)\binom{-m-2}{s-2}(p-1)^s p^m \\ &= m(m+1)p^m(p-1)^2\sum_{s\geq 2}\binom{-m-2}{s-2}(p-1)^{s-2} \\ &= m(m+1)p^m(1-p)^2[1+(p-1)]^{-m-2} \\ &= m(m+1)p^m(1-p)^2p^{-m-2} \\ &= m(m+1)\,\frac{(1-p)^2}{p^2} \end{aligned}$$

We conclude that the second moment is given by the following formula:

$$\begin{aligned} M_2 &= m(m+1)\,\frac{(1-p)^2}{p^2} + m\,\frac{1-p}{p} \\ &= m\,\frac{1-p}{p^2}[(m+1)(1-p)+p] \\ &= m\,\frac{1-p}{p^2}(1+m-mp) \end{aligned}$$

Thus, the variance is given by the following formula:

$$\begin{aligned} V &= M_2 - M_1^2 \\ &= m\frac{1-p}{p^2}(1+m-mp) - m^2\frac{(1-p)^2}{p^2} \\ &= m\frac{1-p}{p^2}[1+m-mp-m+mp] \\ &= m\frac{1-p}{p^2} \end{aligned}$$

We are therefore led to the conclusions in the statement. □

Moving on, of particular interest is the exponent $m = 1$, where we have:

PROPOSITION 7.14. *The negative binomial laws $c_p = c_{1p}$ of exponent $m = 1$ are*

$$P(s) = (1-p)^s p$$

with these being called geometric laws.

PROOF. This is indeed clear from definitions, and with the name of these laws coming from the geometric series which produces them. Indeed, we have:

$$\sum_{s\geq 0} P(s) = \sum_{s\geq 0}(1-p)^s p = p\cdot\frac{1}{1-(1-p)} = 1$$

Thus, we are led to the conclusions in the statement. □

In practice now, the above geometric laws appear in many concrete situations, in the real life, in various contexts involving iterated Bernoulli trials, as before in Theorem 7.12, and its variations, and I will leave some further learning here to you.

Regarding now the basic properties of the geometric laws, these are as follows:

PROPOSITION 7.15. *The geometric law c_p has the following properties:*

(1) *The mean is $E = \frac{(1-p)}{p}$.*
(2) *The variance is $V = \frac{(1-p)}{p^2}$.*

PROOF. This comes indeed as a consequence of Theorem 7.13, at $m = 1$. □

Finally, we have the following result, which is something quite conceptual, similar to our previous formula $b_{np} = b_p^{*n}$, from chapter 6, for the usual binomial laws:

THEOREM 7.16. *We have the following formula, for any $m \in \mathbb{N}$,*

$$c_{mp} = c_p^{*m}$$

relating the geometric laws and the negative binomial laws.

PROOF. This is something very standard, the idea being as follows:

(1) To start with, the result certainly holds at $m = 1$, by definition of c_p.

(2) The result holds as well at $m = 2$, as shown by the following computation:

$$\begin{aligned}
c_p * c_p &= \left(\sum_{a\geq 0}(1-p)^a p\delta_a\right) * \left(\sum_{b\geq 0}(1-p)^b p\delta_b\right)\\
&= \sum_{a,b\geq 0}(1-p)^{a+b}p^2\delta_{a+b}\\
&= \sum_{s\geq 0}\#\left\{a,b\geq 0\Big|a+b=s\right\}(1-p)^s p^2\delta_s\\
&= \sum_{s\geq 0}(s+1)(1-p)^s p^2\delta_s\\
&= \sum_{s\geq 0}\binom{s+1}{s}(1-p)^s p^2\delta_s\\
&= c_{2p}
\end{aligned}$$

(3) At $m = 3$ now, the computation is quite similar, as follows:

$$\begin{aligned}
c_p^{*3} &= \left(\sum_{a\geq 0}(1-p)^a p\delta_a\right) * \left(\sum_{b\geq 0}(1-p)^b p\delta_b\right) * \left(\sum_{c\geq 0}(1-p)^c p\delta_c\right)\\
&= \sum_{a,b,c\geq 0}(1-p)^{a+b+c}p^3\delta_{a+b+c}\\
&= \sum_{s\geq 0}\#\left\{a,b,c\geq 0\Big|a+b+c=s\right\}(1-p)^s p^3\delta_s\\
&= \sum_{s\geq 0}\sum_{c=0}^{s}\#\left\{a,b\geq 0\Big|a+b=s-c\right\}(1-p)^s p^3\delta_s\\
&= \sum_{s\geq 0}(1+2+\ldots+(s+1))(1-p)^s p^3\delta_s\\
&= \sum_{s\geq 0}\frac{(s+1)(s+2)}{2}(1-p)^s p^3\delta_s\\
&= \sum_{s\geq 0}\binom{s+2}{s}(1-p)^s p^3\delta_s\\
&= c_{3p}
\end{aligned}$$

(4) In the general case, where $m \in \mathbb{N}$ is arbitrary, we have, a bit as before:

$$\begin{aligned}
c_p^{*m} &= \left(\sum_{a_1\geq 0}(1-p)^{a_1}p\delta_{a_1}\right) * \ldots * \left(\sum_{a_m\geq 0}(1-p)^{a_m}p\delta_{a_m}\right)\\
&= \sum_{a_1,\ldots,a_m\geq 0}(1-p)^{a_1+\ldots+a_m}p^m\delta_{a_1+\ldots+a_m}\\
&= \sum_{s\geq 0}\#\left\{a_1,\ldots,a_m\geq 0\Big|a_1+\ldots+a_m=s\right\}(1-p)^s p^m\delta_s\\
&= \sum_{s\geq 0}\#\left\{b_1,\ldots,b_m\geq 1\Big|b_1+\ldots+b_m=s+m\right\}(1-p)^s p^m\delta_s\\
&= \sum_{s\geq 0}\binom{s+m-1}{m-1}(1-p)^s p^m\delta_s\\
&= \sum_{s\geq 0}\binom{s+m-1}{s}(1-p)^s p^m\delta_s\\
&= c_{mp}
\end{aligned}$$

(5) To be more precise here, the count at the end comes from the fact that, in order to partition $s+m$, best thought as a sequence of $s+m$ boxes, as $s+m=b_1+\ldots+b_m$, we have to insert $m-1$ markers between these boxes, at different locations, at the $s+m-1$ positions available. Thus, we are led to the conclusion in the statement. □

7c. Higher moments

Let us discuss now the computation of the higher moments of the negative binomial laws. We will be mostly interested in the computation of M_3, M_4, allowing the computation of the skewness and kurtosis, and the study here leads to the following result:

THEOREM 7.17. *The moments of the negative binomial law c_{mp} are*

$$M_1 = \frac{m(1-p)}{p}$$

$$M_2 = m\,\frac{1-p}{p^2}(1+m-mp)$$

$$M_3 = m\,\frac{1-p}{p^3}[(m+1)(m+2)(1-p)^2+3(m+1)(1-p)p+p^2]$$

$$M_4 = m\,\frac{1-p}{p^4}[(m+1)(m+2)(m+3)(1-p)^3+6(m+1)(m+2)(1-p)^2p+7(m+1)(1-p)p^2+p^3]$$

$$\vdots$$

with the computation in general being possible by recurrence.

PROOF. We already know the first two formulae from Theorem 7.13 and its proof, and the continuation is by using the same trick, as follows:

(1) Regarding the third moment, we can use here the following formula:

$$s^3 = s(s-1)(s-2) + 3s(s-1) + s$$

Indeed, this gives the following formula for the third moment:

$$\begin{aligned}
M_3 &= \sum_{s\geq 1} s^3 \binom{-m}{s}(p-1)^s p^m \\
&= \sum_{s\geq 1} \left[s(s-1)(s-2) + 3s(s-1) + s\right]\binom{-m}{s}(p-1)^s p^m \\
&= \sum_{s\geq 3} s(s-1)(s-2)\binom{-m}{s}(p-1)^s p^m \\
&\quad +3\sum_{s\geq 2} s(s-1)\binom{-m}{s}(p-1)^s p^m \\
&\quad +\sum_{s\geq 1} s\binom{-m}{s}(p-1)^s p^m \\
&= -m(m+1)(m+2)\sum_{s\geq 3}\binom{-m-3}{s-3}(p-1)^s p^m \\
&\quad +3m(m+1)\sum_{s\geq 2}\binom{-m-2}{s-2}(p-1)^s p^m \\
&\quad -m\sum_{s\geq 1}\binom{-m-1}{s-1}(p-1)^s p^m \\
&= m(m+1)(m+2)p^m(1-p)^3[1+(p-1)]^{-m-3} \\
&\quad +3r(m+1)p^m(1-p)^2[1+(p-1)]^{-m-2} \\
&\quad +mp^m(1-p)[1+(p-1)]^{-m-1} \\
&= m(m+1)(m+2)(1-p)^3p^{-3} \\
&\quad +3m(m+1)(1-p)^2p^{-2} \\
&\quad +m(1-p)p^{-1} \\
&= m\,\frac{1-p}{p^3}[(m+1)(m+2)(1-p)^2 + 3(m+1)(1-p)p + p^2]
\end{aligned}$$

(2) Regarding the fourth moment, we can use here the following formula:

$$s^4 = s(s-1)(s-2)(s-3) + 6s(s-1)(s-2) + 7s(s-1) + s$$

Indeed, this gives the following formula for the fourth moment:

$$\begin{aligned}
M_4 &= \sum_{s\geq 4} s(s-1)(s-2)(s-3)\binom{-m}{s}(p-1)^s p^m\\
&\quad +6\sum_{s\geq 3} s(s-1)(s-2)\binom{-m}{s}(p-1)^s p^m\\
&\quad +7\sum_{s\geq 2} s(s-1)\binom{-m}{s}(p-1)^s p^m\\
&\quad +\sum_{s\geq 1} s\binom{-m}{s}(p-1)^s p^m\\
&= m(m+1)(m+2)(m+3)\sum_{s\geq 4}\binom{-m-4}{s-4}(p-1)^s p^m\\
&\quad -6m(m+1)(m+2)\sum_{s\geq 3}\binom{-m-3}{s-3}(p-1)^s p^m\\
&\quad +7m(m+1)\sum_{s\geq 2}\binom{-m-2}{s-2}(p-1)^s p^m\\
&\quad -m\sum_{s\geq 1}\binom{-m-1}{s-1}(p-1)^s p^m\\
&= m(m+1)(m+2)(m+3)p^m(1-p)^4[1+(p-1)]^{-m-4}\\
&\quad +6m(m+1)(m+2)p^m(1-p)^3[1+(p-1)]^{-m-3}\\
&\quad +7r(m+1)p^m(1-p)^2[1+(p-1)]^{-m-2}\\
&\quad +mp^m(1-p)[1+(p-1)]^{-m-1}\\
&= m(m+1)(m+2)(m+3)(1-p)^4p^{-4}\\
&\quad +6m(m+1)(m+2)(1-p)^3p^{-3}\\
&\quad +7m(m+1)(1-p)^2p^{-2}\\
&\quad +m(1-p)p^{-1}\\
&= m\,\frac{1-p}{p^4}[(m+1)(m+2)(m+3)(1-p)^3\\
&\quad +6(m+1)(m+2)(1-p)^2p+7(m+1)(1-p)p^2+p^3]
\end{aligned}$$

(3) As a continuation of this, it is quite clear that we can compute M_k by recurrence. We will be back to this later, with more results on the subject. □

Let us record as well a result about the corresponding central moments:

THEOREM 7.18. *The central moments of c_{mp} are given by the formulae*

$$M_1' = 0$$

$$M_2' = \frac{m(1-p)}{p^2}$$

$$M_3' = \frac{m(1-p)(2-p)}{p^3}$$

$$M_4' = \frac{m(1-p)((3m+6)(1-p)+p^2)}{p^4}$$

$$\vdots$$

with the computation in general being possible by recurrence.

PROOF. The first central moments are $M_1' = 0$, and then $M_2' = V$, whose formula we know from Theorem 7.13. Regarding the higher central moments, we recall from chapter 6 that these appear from the usual moments via the following formula:

$$\begin{aligned} M_k' &= E\left(\sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r f^{k-r}\right) \\ &= \sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r M_{k-r} \\ &= \sum_{r=0}^{k-2}(-1)^r\binom{k}{r}E^r M_{k-r} + (-1)^{k-1}(k-1)E^k \end{aligned}$$

Now with $k = 3$, by using the formulae from Theorem 7.17, we obtain:

$$\begin{aligned} M_3' &= M_3 - 3EM_2 + 2E^3 \\ &= m\,\frac{1-p}{p^3}[(m+1)(m+2)(1-p)^2 + 3(m+1)(1-p)p + p^2] \\ &\quad -3\,\frac{m(1-p)}{p}\cdot m\,\frac{1-p}{p^2}(1+m-mp) + 2\,\frac{m^3(1-p)^3}{p^3} \\ &= \frac{m(1-p)(2-p)}{p^3} \end{aligned}$$

Similarly, at $k=4$, again by using the formulae from Theorem 7.17, we have:

$$\begin{aligned}
M_4' &= M_4 - 4EM_3 + 6E^2M_2 - 3E^4\\
&= m\,\frac{1-p}{p^4}[(m+1)(m+2)(m+3)(1-p)^3\\
&\quad +6(m+1)(m+2)(1-p)^2p + 7(m+1)(1-p)p^2 + p^3]\\
&\quad -4\,\frac{m^2(1-p)^2}{p^4}\cdot[(m+1)(m+2)(1-p)^2 + 3(m+1)(1-p)p + p^2]\\
&\quad +6\,\frac{m^2(1-p)^2}{p^2}\cdot m\,\frac{1-p}{p^2}(1+m-mp) - 3\,\frac{m^4(1-p)^4}{p^4}\\
&= \frac{m(1-p)((3m+6)(1-p)+p^2)}{p^4}
\end{aligned}$$

As for the last assertion, we will be back to it later, with details. □

Let us end this discussion with the following result, capturing the essentials:

THEOREM 7.19. *For the negative binomial law c_{mp},*

$$E=\frac{m(1-p)}{p}\ ,\ V=\frac{m(1-p)}{p^2}\ ,\ \gamma=\frac{2-p}{\sqrt{m(1-p)}}\ ,\ \kappa=3+\frac{6}{m}+\frac{p^2}{m(1-p)}$$

are the mean, variance, skewness and kurtosis.

PROOF. Regarding the formulae of E,V, we know these from Theorem 7.13. Next, by using the formula of M_3' from Theorem 7.18, the skewness is given by:

$$\begin{aligned}
\gamma &= M_3'/V\sqrt{V}\\
&= \frac{m(1-p)(2-p)}{p^3}\cdot\frac{p^2}{m(1-p)}\cdot\frac{p}{\sqrt{m(1-p)}}\\
&= \frac{2-p}{\sqrt{m(1-p)}}
\end{aligned}$$

As for the kurtosis, by using the formula of M_3' from Theorem 7.18, this given by:

$$\begin{aligned}
\kappa &= M_4'/V^2\\
&= \frac{m(1-p)((3m+6)(1-p)+p^2)}{p^4}\cdot\frac{p^4}{m^2(1-p)^2}\\
&= 3+\frac{6}{m}+\frac{p^2}{m(1-p)}
\end{aligned}$$

Thus, we are led to the formulae in the statement. Needless to say, the higher normalized central moments can be computed too, by recurrence. □

The Fourier transform can be computed as well, and the formula is quite similar to what we had before, in chapter 6, for the usual binomial laws:

THEOREM 7.20. *The Fourier transform of the negative binomial law is given by:*

$$F_f(x) = \left(\frac{p}{1+(p-1)e^{ix}}\right)^m$$

In particular, we can see that $\log F$ *is linear in* n*, as it should.*

PROOF. We have indeed the following computation, for the Fourier transform:

$$\begin{aligned} F_f(x) &= E(e^{ixf}) \\ &= \sum_{s\geq 0}\binom{-m}{s}(p-1)^s p^m e^{ixs} \\ &= p^m\sum_{s\geq 0}\binom{-m}{s}[(p-1)e^{ix}]^s \\ &= p^m(1+(p-1)e^{ix})^{-m} \\ &= \left(\frac{p}{1+(p-1)e^{ix}}\right)^m \end{aligned}$$

As for the last assertion, this is just an observation, to be related to Theorem 7.16. □

Again inspired from what we did before for the usual binomial laws, we have:

THEOREM 7.21. *The moments of* c_{mp} *are given by the following formula,*

$$M_k = \sum_{\pi\in P(k)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|}$$

with $|.|$ *standing as usual for the number of blocks.*

PROOF. Many things can be said here, the idea being as follows:

(1) Some numerics first. At $k=1$ we only have one partition, namely $|$, and the formula in the statement holds indeed, as shown by the following computation:

$$\begin{aligned} \sum_{\pi\in P(1)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|} &= \frac{m!}{(m-1)!}\left(\frac{1-p}{p}\right)^1 \\ &= m\cdot\frac{1-p}{p} \end{aligned}$$

(2) At $k=2$ now, we have two partitions, namely $||$ and $\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}\sum_{\pi\in P(2)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|} &= \frac{(m+1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^2+\frac{m!}{(m-1)!}\left(\frac{1-p}{p}\right)^1\\ &= m(m+1)\left(\frac{1-p}{p}\right)^2+m\cdot\frac{1-p}{p}\end{aligned}$$

(3) At $k=3$ we have 5 partitions, namely $|||$, $\sqcap|$, $\sqcap\!\!|$, $|\sqcap$, $\sqcap\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}&\sum_{\pi\in P(3)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|}\\ =\ &\frac{(m+2)!}{(m-1)!}\left(\frac{1-p}{p}\right)^3+3\cdot\frac{(m+1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^2+\frac{m!}{(m-1)!}\left(\frac{1-p}{p}\right)^1\\ =\ &m(m+1)(m+2)\left(\frac{1-p}{p}\right)^3+3m(m+1)\left(\frac{1-p}{p}\right)^2+m\cdot\frac{1-p}{p}\end{aligned}$$

(4) At $k=4$ we have 15 partitions, with the list of relevant partitions, and their multiplicities up to permutations, which is self-explanatory, being as follows:

$$|||\,|\times 1\quad,\quad \sqcap\,|\,|\times 6\quad,\quad \sqcap\sqcap\times 3\quad,\quad \sqcap\sqcap\,|\times 4\quad,\quad \sqcap\sqcap\sqcap\times 1$$

Now by doing the computation, as before, the formula in the statement holds again:

$$\begin{aligned}&\sum_{\pi\in P(4)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|}\\ =\ &\frac{(m+3)!}{(m-1)!}\left(\frac{1-p}{p}\right)^4+6\cdot\frac{(m+2)!}{(m-1)!}\left(\frac{1-p}{p}\right)^3\\ &+(3+4)\cdot\frac{(m+1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^2+\frac{m!}{(m-1)!}\left(\frac{1-p}{p}\right)^1\\ =\ &m(m+1)(m+2)(m+3)\left(\frac{1-p}{p}\right)^4+6m(m+1)(m+2)\left(\frac{1-p}{p}\right)^3\\ &+7m(m+1)\left(\frac{1-p}{p}\right)^2+m\cdot\frac{1-p}{p}\end{aligned}$$

(5) In general now, in order to prove the result, let us go back to our computations from the proof of Theorem 7.17. The idea there was that of using a formula as follows:

$$\begin{aligned} s^k &= s(s-1)\dots(s-k+1)\\ &\quad +c_1s(s-1)\dots(s-k+2)\\ &\quad \vdots\\ &\quad +c_{k-2}s(s-1)\\ &\quad +s \end{aligned}$$

(6) Indeed, assuming that we have such a formula, we obtain:

$$\begin{aligned} M_k &= \sum_{s\geq k}s(s-1)\dots(s-k+1)\binom{-m}{s}(p-1)^sp^m\\ &\quad +c_1\sum_{s\geq k-1}s(s-1)\dots(s-k+2)\binom{-m}{s}(p-1)^sp^m\\ &\quad \vdots\\ &\quad +c_{k-2}\sum_{s\geq 2}s(s-1)\binom{-m}{s}(p-1)^sp^m\\ &\quad +\sum_{s\geq 1}s\binom{-m}{s}(p-1)^sp^m\\ &= (-1)^km(m+1)\dots(m+k-1)\sum_{s\geq k}\binom{-m-k}{s-k}(p-1)^sp^m\\ &\quad +(-1)^{k+1}c_1m(m+1)\dots(m+k-2)\sum_{s\geq k-1}\binom{-m-k+1}{s-k+1}(p-1)^sp^m\\ &\quad \vdots\\ &\quad +c_{k-2}m(m+1)\sum_{s\geq 2}\binom{-m-2}{s-2}(p-1)^sp^m\\ &\quad -m\sum_{s\geq 1}\binom{-m-1}{s-1}(p-1)^sp^m \end{aligned}$$

(7) Thus, we are led to the following formula, for the k-th moment:

$$\begin{aligned}
M_k &= m(m+1)\ldots(m-k+1)p^m(1-p)^k[1+(p-1)]^{-m-k}\\
&\quad +c_1m(m+1)\ldots(m+k-2)p^m(1-p)^{k-1}[1+(p-1)]^{-m-k+1}\\
&\quad \vdots\\
&\quad +c_{k-2}m(m+1)p^m(1-p)^2[1+(p-1)]^{-m-2}\\
&\quad +mp^m(1-p)[1+(p-1)]^{-m-1}\\
&= m(m+1)\ldots(m+k-1)\left(\frac{1-p}{p}\right)^k\\
&\quad +c_1m(m+1)\ldots(m+k-2)\left(\frac{1-p}{p}\right)^{k-1}\\
&\quad \vdots\\
&\quad +c_{k-2}m(m+1)\left(\frac{1-p}{p}\right)^2+m\left(\frac{1-p}{p}\right)
\end{aligned}$$

(8) The point now is that, as explained in chapter 6, we have the following formula:

$$s^k=\sum_{\pi\in P(k)}\frac{s!}{(s-|\pi|)!}$$

Thus, we have the formula needed in (5), and according now to (7), we obtain:

$$M_k=\sum_{\pi\in P(k)}\frac{(m+|\pi|-1)!}{(m-1)!}\left(\frac{1-p}{p}\right)^{|\pi|}$$

And with this, good news, we have reached to the formula in the statement. □

7d. Further exponents

We would like to end this chapter with some pure mathematics. The point indeed is that, quite interestingly, the formula in Theorem 7.1 holds in fact at any $n\in\mathbb{R}$:

THEOREM 7.22. *We have the following generalized binomial formula, with $n\in\mathbb{R}$,*

$$(1+x)^n=\sum_{k=0}^{\infty}\binom{n}{k}x^k$$

with the generalized binomial coefficients being given by the formula

$$\binom{n}{k}=\frac{n(n-1)\ldots(n-k+1)}{k!}$$

valid for any $|x|<1$. With $n\in\mathbb{N}$, we recover the usual binomial formula.

PROOF. This does not look obvious to prove, with bare hands, but we can kill it with calculus. Indeed, the series in the statement f converges at $|x| < 1$, and we have:

$$(1+x)f'(x) = nf(x)$$

Now by using this formula, we have the following derivative computation:

$$\big((1+x)^{-n}f(x)\big)' = -n(1+x)^{-n-1}f(x) + (1+x)^{-n}f'(x) = 0$$

Thus we have $f(x) = c(1+x)^n$, with $c = f(0) = 1$, as desired. Just like that. □

As a main application of our generalized binomial formula above, which is something very useful in practice, we can now professionally extract square roots, as follows:

THEOREM 7.23. *We have the following formula,*

$$\sqrt{1+t} = 1 - 2\sum_{k=1}^{\infty} C_{k-1}\left(\frac{-t}{4}\right)^k$$

with $C_k = \frac{1}{k+1}\binom{2k}{k}$ *being the Catalan numbers. Also, we have*

$$\frac{1}{\sqrt{1+t}} = \sum_{k=0}^{\infty} D_k\left(\frac{-t}{4}\right)^k$$

with $D_k = \binom{2k}{k}$ *being the central binomial coefficients.*

PROOF. At $n = 1/2$, the generalized binomial coefficients are:

$$\begin{aligned}\binom{1/2}{k} &= \frac{1/2(-1/2)\ldots(3/2-k)}{k!}\\ &= (-1)^{k-1}\frac{(2k-2)!}{2^{k-1}(k-1)!2^k k!}\\ &= -2\left(\frac{-1}{4}\right)^k C_{k-1}\end{aligned}$$

Also, at $n = -1/2$, the generalized binomial coefficients are:

$$\begin{aligned}\binom{-1/2}{k} &= \frac{-1/2(-3/2)\ldots(1/2-k)}{k!}\\ &= (-1)^k\frac{(2k)!}{2^k k!2^k k!}\\ &= \left(\frac{-1}{4}\right)^k D_k\end{aligned}$$

Thus, Theorem 7.22 at $n = \pm 1/2$ gives the formulae in the statement. □

Finally, we would like to use our recently acquired calculus knowledge in order to fully rewrite the theory of the Catalan numbers, starting from zero. So, with apologies for the mess, what we did at the end of chapter 1 can be in fact better seen as follows:

THEOREM 7.24. *The Catalan numbers have the following properties:*

(1) *They satisfy* $C_{k+1}=\sum_{a+b=k}C_aC_b$.
(2) *The series* $f(z)=\sum_{k\geq 0}C_kz^k$ *satisfies* $zf^2-f+1=0$.
(3) *This series is given by* $f(z)=\frac{1-\sqrt{1-4z}}{2z}$.
(4) *We have the formula* $C_k=\frac{1}{k+1}\binom{2k}{k}$.

PROOF. This is best viewed by using noncrossing pairings, as follows:

(1) Let us count the noncrossing pairings of $\{1,\ldots,2k+2\}$. Such a pairing appears by pairing 1 to an odd number, $2a+1$, and then inserting a noncrossing pairing of $\{2,\ldots,2a\}$, and a noncrossing pairing of $\{2a+2,\ldots,2k+2\}$. Thus we have, as claimed:

$$C_{k+1}=\sum_{a+b=k}C_aC_b$$

(2) Consider now the generating series of the Catalan numbers, $f(z)=\sum_{k\geq 0}C_kz^k$. In terms of this generating series, the above recurrence gives, as desired:

$$\begin{aligned}zf^2&=\sum_{a,b\geq 0}C_aC_bz^{a+b+1}\\&=\sum_{k\geq 1}\sum_{a+b=k-1}C_aC_bz^k\\&=\sum_{k\geq 1}C_kz^k\\&=f-1\end{aligned}$$

(3) By solving the equation $zf^2-f+1=0$ found above, and choosing the solution which is bounded at $z=0$, we obtain the following formula, as claimed:

$$f(z)=\frac{1-\sqrt{1-4z}}{2z}$$

(4) In order to compute f, we can use the generalized binomial formula at exponent $n=1/2$, which according to the computations in the proof of Theorem 7.23 reads:

$$\sqrt{1+t}=1-2\sum_{k=1}^{\infty}\frac{1}{k}\binom{2k-2}{k-1}\left(\frac{-t}{4}\right)^k$$

Indeed, with $t=-4z$ we obtain from this the following formula:

$$\sqrt{1-4z}=1-2\sum_{k=1}^{\infty}\frac{1}{k}\binom{2k-2}{k-1}z^k$$

Now back to our series f, we obtain the following formula for it:

$$\begin{aligned} f(z) &= \frac{1-\sqrt{1-4z}}{2z} \\ &= \sum_{k=1}^{\infty}\frac{1}{k}\binom{2k-2}{k-1}z^{k-1} \\ &= \sum_{k=0}^{\infty}\frac{1}{k+1}\binom{2k}{k}z^{k} \end{aligned}$$

Thus, the Catalan numbers are indeed given by $C_k=\frac{1}{k+1}\binom{2k}{k}$, as claimed. □

In relation now with probability, it is possible to construct some new discrete measures, based on all this. We will be back to such things, later in this book.

7e. Exercises

This was a quite technical chapter, and as exercises on all this, we have:

EXERCISE 7.25. *Learn more about rational functions, and their properties.*

EXERCISE 7.26. *Do the $n=3,4$ verifications for our formula for the dice sum.*

EXERCISE 7.27. *Learn more about the occurrences of the negative binomial laws.*

EXERCISE 7.28. *Learn also about the various occurrences of the geometric laws.*

EXERCISE 7.29. *Compute some higher moments of the negative binomial laws.*

EXERCISE 7.30. *Compute as well higher central moments, normalized or not.*

EXERCISE 7.31. *Learn about the Taylor formula, and analytic functions.*

EXERCISE 7.32. *Try other rational values of the exponent, in the binomial formula.*

As bonus exercise, fully read a one-variable calculus book. All useful mathematics.

CHAPTER 8

Poisson laws

8a. Convergence

We have seen so far the basics of probability theory, illustrated by the binomial laws, positive and negative, and with these laws appearing by flipping a biased coin n times. Time now to get into more advanced aspects, involving various $n \to \infty$ procedures, and making the link with all sorts of continuous phenomena, appearing in the real life.

Before anything, since we will be mixing discrete and continuous theory in this chapter, and our theoretical knowledge reduces to the discrete case, we are right away a bit in trouble. So, what to do? Instead of reworking the material from chapters 5-6 in the continuous case, which can be a quite tricky business, normally reserved for later learning, after reading this book, let us lower our mathematical ambitions, and formulate:

PRINCIPLE 8.1. *What we did so far in this book, namely probability spaces, random variables and independence, extends in a straightforward way to the continuous case.*

To be more precise, we will use this principle in what follows, for some of the things that we will be doing. And of course relax, and take this as some sort of physics class.

Getting started now, with $n \to \infty$ phenomena, given independent identically distributed (i.i.d.) variables $f_1, f_2, f_3, \ldots$, intuition tells us that we should have a convergence as follows, with $E(f) = E(f_i)$ being the common expectation of our variables:

$$\frac{f_1 + \ldots + f_n}{n} \to E(f)$$

In order to further comment on this, and formulate a precise theorem about this convergence, we must first talk, in general, about the convergence of random variables.

In general, the convergence of random variables is a quite interesting topic, and we have several possible notions here. As a first notion, which is quite natural, we have:

DEFINITION 8.2. *Given variables $f_1, f_2, f_3, \ldots$, we say that $f_n \to f$ in law when*

$$E(\varphi(f_n)) \to E(\varphi(f))$$

for any bounded continuous function $\varphi : \mathbb{R} \to \mathbb{R}$.

As a first observation, by linearity we can assume that we are dealing with the power functions $\varphi(x) = x^k$, so the following condition must be satisfied, for any $k \in \mathbb{N}$:

$$E(f_n^k) \to E(f^k)$$

In other words, with M_k denoting as usual the moments, we must have:

$$M_k(f_n) \to M_k(f)$$

Alternatively, again by linearity, and by using some standard analysis, we can assume that we are dealing with characteristic functions of intervals, which leads to:

PROPOSITION 8.3. *We have $f_n \to f$ in law precisely when*

$$P(f_n \leq x) \to P(f \leq x)$$

for all the continuity points of the function $x \to P(f \leq x)$.

PROOF. This is indeed something very standard, coming from definitions, as explained above, by using linearity, and approximation by step functions. □

Moving on, as a second notion of convergence for random variables, we have:

DEFINITION 8.4. *Given variables $f_1, f_2, f_3, \ldots$, we say that $f_n \to f$ in probability when*

$$P(|f_n - f| \geq \varepsilon) \to 0$$

for any $\varepsilon > 0$.

Again, there are many illustrations for this notion, and further things can be said. Before everything, however, let us state and prove the following key result:

THEOREM 8.5. *We have the following implication,*

$$\begin{pmatrix} f_n \to f \\ \text{in probability} \end{pmatrix} \implies \begin{pmatrix} f_n \to f \\ \text{in law} \end{pmatrix}$$

and the reverse implication does not necessarily hold.

PROOF. This is something very standard, the idea being as follows:

(1) As a technical ingredient, we will need the following estimate, valid for any two random variables $f, g : X \to \mathbb{R}$, and any two numbers $a \in \mathbb{R}$ and $\varepsilon > 0$:

$$\begin{aligned} P(g \leq a) &= P(g \leq a, f \leq a + \varepsilon) + P(g \leq a, f > a + \varepsilon) \\ &\leq P(f \leq a + \varepsilon) + P(g \leq a, f > a + \varepsilon) \\ &= P(f \leq a + \varepsilon) + P(g - f \leq a - f < -\varepsilon) \\ &\leq P(f \leq a + \varepsilon) + P(g - f < -\varepsilon) \\ &\leq P(f \leq a + \varepsilon) + P(|g - f| > \varepsilon) \end{aligned}$$

(2) In order to prove now the result, the most convenient is to use the criterion for convergence in law from Proposition 8.3. That is, given a continuity point $a \in \mathbb{R}$ of the function $x \to P(f \leq x)$, we would like to prove that the following happens:

$$P(f_n \leq a) \to P(f \leq a)$$

(3) So, let $\varepsilon > 0$. By using the estimate found in (1), we have:

$$P(f_n \leq a) \leq P(f \leq a + \varepsilon) + P(|f_n - f| > \varepsilon)$$

$$P(f \leq a - \varepsilon) \leq P(f_n \leq a) + P(|f_n - f| > \varepsilon)$$

We conclude from this that we have the following estimate:

$$\begin{aligned} & P(f \leq a + \varepsilon) - P(|f_n - f| > \varepsilon) \\ \leq\ & P(f_n \leq a) \\ \leq\ & P(f \leq a + \varepsilon) + P(|f_n - f| > \varepsilon) \end{aligned}$$

(4) Now with $n \to \infty$ we obtain from this, in terms of $F(a) = P(x \leq a)$:

$$F(a - \varepsilon) \leq \lim_{n \to \infty} P(f_n \leq a) \leq F(a + \varepsilon)$$

Since F was assumed to be continuous at a, with $\varepsilon \to 0$ this gives:

$$\lim_{n \to \infty} P(f_n \leq a) = P(f \leq a)$$

Thus we have indeed the convergence $f_n \to f$ in distribution, as stated. □

Moving on, as a third and final notion of convergence, we have:

DEFINITION 8.6. *Given variables $f_1, f_2, f_3, \ldots$, we say that $f_n \to f$ almost surely when*

$$f_n(x) \to f(x)$$

outside a measure zero set.

Again, there are many illustrations for this notion, and further things can be said, about this. At the theoretical level, we the following key result:

THEOREM 8.7. *We have the following implication*

$$\begin{pmatrix} f_n \to f \\ \text{almost surely} \end{pmatrix} \implies \begin{pmatrix} f_n \to f \\ \text{in probability} \end{pmatrix}$$

and the reverse implication does not necessarily hold.

PROOF. Assume that $f_n \to f$ in probability in our sense, namely $P(|f_n - f| \geq \varepsilon) \to 0$, for any $\varepsilon > 0$. Given a continuous function $\varphi : \mathbb{R} \to \mathbb{R}$, we can write:

$$|E(\varphi(f_n)) - E(\varphi(f))| \ = \ |E(\varphi(f_n) - \varphi(f))|$$

The point now is that we can decompose the expectation on the right over the sets where $|f_n - f| \geq \varepsilon$ and $|f_n - f| < \varepsilon$, and we obtain zero in the limit, as desired. □

As a conclusion to all this, we have the following result:

THEOREM 8.8. *We have the following implications,*

$$\begin{pmatrix} f_n \to f \\ \text{almost surely} \end{pmatrix} \implies \begin{pmatrix} f_n \to f \\ \text{in probability} \end{pmatrix} \implies \begin{pmatrix} f_n \to f \\ \text{in law} \end{pmatrix}$$

and the reverse implications do not necessarily hold.

PROOF. This comes indeed by putting together what we have, namely Theorem 8.5 and Theorem 8.7. As for the counterexamples at the end, regarding the converse implications, are both elementary, and we will leave them as exercises. □

Getting now to what we wanted to do, namely convergence of an average of i.i.d. variables towards their common mean, we have the following result, about this:

THEOREM 8.9 (Weak law of large numbers). *Given i.i.d. variables $f_1, f_2, f_3, \ldots$, with common mean $E(f) = E(f_i)$, we have the following formula, for any $\varepsilon > 0$:*

$$\lim_{n\to\infty} P\left(\left|\frac{f_1 + \ldots + f_n}{n} - E(f)\right| \geq \varepsilon\right) = 0$$

In other words, we have the convergence

$$\frac{f_1 + \ldots + f_n}{n} \to E(f)$$

in probability.

PROOF. This is something very standard, the idea being as follows:

(1) Let us first establish a weaker result, namely the convergence in law, for our averages. Consider the sequence of averages of our variables:

$$g_n = \frac{f_1 + \ldots + f_n}{n}$$

Now let us look at the Fourier transforms of our variables. We have, for any i, the following estimate, with $E = E(f_i)$ being the common expectation of our variables:

$$F_{f_i}(t) \simeq 1 + iEt$$

Now by using independence, we deduce from this that we have, with $n \to \infty$:

$$\begin{aligned} F_{g_n}(t) &= \left[F_{f_i}\left(\frac{t}{n}\right)\right]^n \\ &\simeq \left[1 + iE\,\frac{t}{n}\right]^n \\ &\simeq e^{iEt} \end{aligned}$$

Now since the limiting function that we found e^{iEt} is the Fourier transform of the constant variable E, we conclude from this that we have $g_n \to E$ in law.

(2) In order to establish now the convergence in probability, as stated, we recall from chapter 5 that given a random variable $h : X \to \mathbb{R}$, having mean E and variance V, the Chebycheff inequality states that we have, for any $a > 0$:

$$P\big(|h - E| \geq a\big) \leq \frac{V}{a^2}$$

In order to prove the result, consider the following sequence of variables:

$$h_n = \frac{f_1 + \ldots + f_n}{n} - E$$

The mean and variance of these variables are then as follows, with $v = V(f_i)$:

$$E(h_n) = 0 \quad , \quad V(h_n) = \frac{v}{n}$$

Indeed, the mean formula $E(h_n) = 0$ is clear, and by using this, we have as well:

$$\begin{aligned}
V(h_n) &= E(h_n^2)\\
&= E\left(\frac{\sum_{ij} f_i f_j}{n^2} - \frac{2E\sum_i f_i}{n} + E^2\right)\\
&= E\left(\frac{\sum_i f_i^2}{n^2} + \frac{\sum_{i\neq j} f_i f_j}{n^2} - \frac{2E\sum_i f_i}{n} + E^2\right)\\
&= \frac{\sum_i E(f_i^2)}{n^2} + \frac{\sum_{i\neq j} E(f_i)E(f_j)}{n^2} - \frac{2E\sum_i E(f_i)}{n} + E^2\\
&= \frac{v + E^2}{n} + n(n-1)\cdot\frac{E^2}{n^2} - 2E^2 + E^2\\
&= \frac{v}{n} + \big(n + n(n-1) - n^2\big)\frac{E^2}{n^2}\\
&= \frac{v}{n}
\end{aligned}$$

Now let us apply the Chebycheff inequality above, for the variable h_n. This gives:

$$P(|h_n| \geq \varepsilon) \leq \frac{v/n}{\varepsilon^2}$$

Thus, we have the following inequality, in terms of the original variables f_i:

$$P\left(\left|\frac{f_1 + \ldots + f_n}{n} - E\right| \geq \varepsilon\right) \leq \frac{v}{\varepsilon^2 n}$$

But this gives, as desired, the convergence in probability, namely:

$$\lim_{n\to\infty} P\left(\left|\frac{f_1 + \ldots + f_n}{n} - E(f)\right| \geq \varepsilon\right) = 0$$

Thus, we are led to the conclusion in the statement. □

The above result is not the end of the story with the law of large numbers, because, quite remarkably, the convergence there holds almost surely. In order to explain this, which is something quite technical, we will need some preliminaries. Let us start with:

DEFINITION 8.10. *Given a sequence of events $A_1, A_2, A_3, \ldots$, we set*

$$\limsup_n A_n = \bigcap_{m\in\mathbb{N}} \bigcup_{n=m}^{\infty} A_n$$

with the limit notation coming from the decreasing intersection. Equivalently, we set

$$\limsup_n A_n = \left\{ w \in X \middle| w \in A_n \text{ i.o.} \right\}$$

with i.o. standing for infinitely often.

To be more precise here, given a sequence of events $A_1, A_2, A_3, \ldots$ as above, we certainly have a decreasing sequence of events, as follows:

$$\bigcup_{n=1}^{\infty} A_n \supset \bigcup_{n=2}^{\infty} A_n \supset \bigcup_{n=3}^{\infty} A_n \supset \ldots$$

Thus, we can consider the intersection of this sequence, and in analogy with what we know about numbers and limits, it makes sense to denote this intersection as above:

$$\limsup_n A_n = \lim_{m\to\infty} \bigcup_{n=m}^{\infty} A_n$$

Finally, it is clear from definitions that we have the following equivalent formula for our intersection, with i.o. standing for infinitely often:

$$\limsup_n A_n = \left\{ w \in X \middle| w \in A_n \text{ i.o.} \right\}$$

We can now state a key technical result, the Borel-Cantelli lemma:

PROPOSITION 8.11 (Borel-Cantelli). *Given events $A_1, A_2, A_3, \ldots$, we have*

$$\sum_{n=1}^{\infty} P(A_n) < \infty \implies P(w \in A_n \text{ i.o.}) = 0$$

with i.o. standing as usual for infinitely often.

PROOF. We use the interpretation of $P(w \in A_n \text{ i.o.})$ coming from Definition 8.10. In the context there, since the intersection there is decreasing, we have, for any $m \in \mathbb{N}$:

$$\limsup_n A_n \subset \bigcup_{n=m}^{\infty} A_n$$

We conclude from this that we have the following estimate, for any $m \in \mathbb{N}$:

$$P(\limsup_n A_n) \leq \sum_{n=m}^{\infty} P(A_n)$$

On the other hand, the assumption in the statement is that the series $\sum_{n=1}^{\infty} P(A_n)$ converges, and this can be stated in the following way:

$$\lim_{m\to\infty} \sum_{n=m}^{\infty} P(A_n) = 0$$

Thus $P(\limsup_n A_n)$ is arbitrarily small, and we conclude that we have:

$$P(\limsup_n A_n) = 0$$

But this is the same as saying that $P(w \in A_n \text{ i.o.}) = 0$, as stated. □

As a second technical ingredient, we will need the following straightforward generalization of the Chebycheff inequality from chapter 5, featuring an exponent p:

PROPOSITION 8.12. *We have the following Chebycheff inequality,*

$$P\big(|g| \geq a\big) \leq \frac{E(g^p)}{a^p}$$

valid for any random variable $g : X \to \mathbb{R}$, and any $p \in \mathbb{N}$.

PROOF. We have indeed the following computation, φ being the density:

$$\begin{aligned} E(|g|^p) &= \int_{\mathbb{R}} |x|^p \varphi(x) dx \\ &= \int_{|x|\geq a} |x|^p \varphi(x) dx \\ &\geq a^p \int_{|x|\geq a} \varphi(x) dx \\ &= a^p P(|g| \geq a) \end{aligned}$$

Thus, we are led to the Chebycheff inequality in the statement. □

We can now improve the weak law of large numbers, into something final, as follows:

THEOREM 8.13 (Strong law of large numbers). *Given i.i.d. variables $f_1, f_2, f_3, \ldots$, with common mean $E(f) = E(f_i)$, we have the convergence*

$$\frac{f_1 + \ldots + f_n}{n} \to E(f)$$

happening almost surely.

PROOF. This is something quite technical, the idea being as follows:

(1) By replacing the variables f_i by their centered versions $f_i - E$, we can assume:

$$E = 0$$

Consider the sums of our variables, which have also mean zero:

$$g_n = f_1 + \ldots + f_n$$

We would like to prove that the following convergence is almost sure:

$$\frac{g_n}{n} \to 0$$

(2) In order to do this, consider an arbitrary event $w \in X$ such that:

$$\lim_{n\to\infty} \frac{g_n(w)}{n} \neq 0$$

In this situation, there exists $\varepsilon > 0$ such that, for infinitely many n:

$$\left| \frac{g_n(w)}{n} \right| > \varepsilon$$

Thus, in order to prove our theorem, we must show that we have, for any $\varepsilon > 0$:

$$P(|g_n| > \varepsilon n \text{ i.o.}) = 0$$

(3) But for this latter purpose, we can use the Borel-Cantelli lemma, applied to:

$$A_n = \left\{ w \in X \middle| |g_n(w)| \geq n\varepsilon \right\}$$

Indeed, let us first verify that the convergence assumption in the Borel-Cantelli lemma is indeed satisfied. For this purpose, we will use the generalized Chebycheff inequality from Proposition 8.12, with exponent $p = 4$. By using our assumption $E = 0$, we have the following computation, with M_2, M_4 being the second and fourth moments of f_i:

$$\begin{aligned} E(g_n^4) &= E\left(\sum_{ijkl} f_i f_j f_k f_k \right) \\ &= E\left(\sum_i f_i^4 \right) + 6E\left(\sum_{i<j} f_i^2 f_j^2 \right) \\ &= nM_4 + 6\binom{n}{2} M_2^2 \\ &= nM_4 + 3n(n-1)M_2^2 \end{aligned}$$

But this shows that for $n >> 0$, we have a constant C such that:

$$E(g_n^4) < Cn^2$$

(4) Thus, the generalized Chebycheff inequality from Proposition 8.12 applies to our situation, with exponent $p = 4$, and gives the following estimate:

$$P(|g_n| \geq n\varepsilon) \leq \frac{E(g_n^4)}{(n\varepsilon)^4} \leq \frac{C}{\varepsilon^4 n^2}$$

And with this, we are almost there. Indeed, if we denote by $N \in \mathbb{N}$ the smallest integer where the inequality found in (3) holds, we have:

$$\sum_{n \geq N} P(|g_n| \geq n\varepsilon) \leq \sum_{n \geq N} \frac{C}{\varepsilon^4 n^2} < \infty$$

Thus, the Borel-Cantelli lemma applies, and shows that we have:

$$P(|g_n| > \varepsilon n \text{ i.o.}) = 0$$

But this ends the proof of our theorem, as explained in (2) above. □

Many other interesting things can be said, about averages of i.i.d. variables. We will be back to this topic later, towards the end of this book, with an explanation for the fact that, with a suitable normalization, we obtain in the limit a bell-shaped curve.

8b. Poisson limits

We would like to discuss now some other limiting results, in discrete probability. The mathematics will involve the Poisson laws p_t, which appear via the Poisson Limit Theorem (PLT). Let us start with the following definition, which is something very standard:

DEFINITION 8.14. *The Poisson law of parameter* 1 *is the following measure,*

$$p_1 = \frac{1}{e} \sum_{k \geq 0} \frac{\delta_k}{k!}$$

and the Poisson law of parameter $t > 0$ *is the following measure,*

$$p_t = e^{-t} \sum_{k \geq 0} \frac{t^k}{k!} \delta_k$$

with the letter "p" standing for Poisson.

We are using here, as before, some simplified notations for these laws. Observe that our laws have indeed mass 1, as they should, due to the following key formula:

$$e^t = \sum_{k \geq 0} \frac{t^k}{k!}$$

We will see in the moment why these measures appear a bit everywhere, in discrete contexts, the reasons for this coming from the Poisson Limit Theorem (PLT). Let us first develop some general theory. We first have the following basic result:

PROPOSITION 8.15. *The mean and variance of p_t are given by:*

$$E = t \quad , \quad V = t$$

In particular for the Poisson law p_1 we have $E = 1, V = 1$.

PROOF. We have two computations to be performed, as follows:

(1) Regarding the mean, this can be computed as follows:

$$\begin{aligned} E &= e^{-t}\sum_{k\geq 0}\frac{t^k}{k!}\cdot k \\ &= e^{-t}\sum_{k\geq 1}\frac{t^k}{(k-1)!} \\ &= e^{-t}\sum_{l\geq 0}\frac{t^{l+1}}{l!} \\ &= te^{-t}\sum_{l\geq 0}\frac{t^l}{l!} \\ &= t \end{aligned}$$

(2) For the variance, we first compute the second moment, as follows:

$$\begin{aligned} M_2 &= e^{-t}\sum_{k\geq 0}\frac{t^k}{k!}\cdot k^2 \\ &= e^{-t}\sum_{k\geq 1}\frac{t^k k}{(k-1)!} \\ &= e^{-t}\sum_{l\geq 0}\frac{t^{l+1}(l+1)}{l!} \\ &= te^{-t}\sum_{l\geq 0}\frac{t^l l}{l!} + te^{-t}\sum_{l\geq 0}\frac{t^l}{l!} \\ &= te^{-t}\sum_{l\geq 1}\frac{t^l}{(l-1)!} + t \\ &= t^2e^{-t}\sum_{m\geq 0}\frac{t^m}{m!} + t \\ &= t^2 + t \end{aligned}$$

Thus the variance is given by $V = (t^2 + t) - t^2 = t$, as claimed. □

Next, we have the following quite conceptual result, in relation with convolution:

THEOREM 8.16. *We have the following formula, for any $s,t>0$,*

$$p_s*p_t=p_{s+t}$$

so the Poisson laws form a convolution semigroup.

PROOF. By using $\delta_k*\delta_l=\delta_{k+l}$ and the binomial formula, we obtain:

$$\begin{aligned}
p_s*p_t&=e^{-s}\sum_{k\geq0}\frac{s^k}{k!}\,\delta_k*e^{-t}\sum_{l\geq0}\frac{t^l}{l!}\,\delta_l\\
&=e^{-s-t}\sum_{n\geq0}\delta_n\sum_{k+l=n}\frac{s^kt^l}{k!l!}\\
&=e^{-s-t}\sum_{n\geq0}\frac{\delta_n}{n!}\sum_{k+l=n}\frac{n!}{k!l!}s^kt^l\\
&=e^{-s-t}\sum_{n\geq0}\frac{(s+t)^n}{n!}\,\delta_n\\
&=p_{s+t}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Next in line, we have the following result, which is fundamental as well:

THEOREM 8.17. *The Poisson laws appear as formal exponentials*

$$p_t=\sum_{k\geq0}\frac{t^k(\delta_1-\delta_0)^{*k}}{k!}$$

with respect to the convolution of measures $*$.

PROOF. By using the binomial formula, the measure on the right is:

$$\begin{aligned}
\mu&=\sum_{k\geq0}t^k\sum_{r+s=k}(-1)^s\frac{\delta_r}{r!s!}\\
&=\sum_{r\geq0}\frac{t^r\delta_r}{r!}\sum_{s\geq0}\frac{(-1)^s}{s!}\\
&=\frac{1}{e}\sum_{r\geq0}\frac{t^r\delta_r}{r!}\\
&=p_t
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Regarding now the Fourier transform computation, this is as follows:

THEOREM 8.18. *The Fourier transform of p_t is given by*

$$F_{p_t}(x) = \exp\left((e^{ix} - 1)t\right)$$

for any $t > 0$, with its logarithm being linear in t, as it should.

PROOF. We have indeed the following computation, which gives the result:

$$\begin{aligned} F_{p_t}(x) &= e^{-t} \sum_{k \geq 0} \frac{t^k}{k!} F_{\delta_k}(x) \\ &= e^{-t} \sum_{k \geq 0} \frac{t^k}{k!} e^{ikx} \\ &= e^{-t} \sum_{k \geq 0} \frac{(e^{ix}t)^k}{k!} \\ &= \exp(-t) \exp(e^{ix}t) \\ &= \exp\left((e^{ix} - 1)t\right) \end{aligned}$$

As for the last assertion, this is just a remark, to be related to Theorem 8.16. □

Good news, we can now establish the Poisson Limit Theorem, as follows:

THEOREM 8.19 (PLT). *We have the following convergence, in moments,*

$$\left(\left(1 - \frac{t}{n}\right)\delta_0 + \frac{t}{n}\,\delta_1\right)^{*n} \to p_t$$

for any $t > 0$. Equivalently, $b_{np} \to p_t$, when $p = t/n$ with $t > 0$ fixed.

PROOF. Let us denote by μ_n the Bernoulli law under the convolution sign:

$$\mu_n = \left(1 - \frac{t}{n}\right)\delta_0 + \frac{t}{n}\,\delta_1$$

We have the following computation, for the Fourier transform of the limit:

$$\begin{aligned} F_{\delta_r}(x) = e^{irx} &\implies F_{\mu_n}(x) = \left(1 - \frac{t}{n}\right) + \frac{t}{n}\,e^{ix} \\ &\implies F_{\mu_n^{*n}}(x) = \left(\left(1 - \frac{t}{n}\right) + \frac{t}{n}\,e^{ix}\right)^n \\ &\implies F_{\mu_n^{*n}}(x) = \left(1 + \frac{(e^{ix} - 1)t}{n}\right)^n \\ &\implies F(x) = \exp\left((e^{ix} - 1)t\right) \end{aligned}$$

Thus, we obtain indeed the Fourier transform of p_t, as desired. □

We have as well a negative Poisson Limit Theorem, as follows:

THEOREM 8.20 (negative PLT). *We have the following convergence, in moments,*

$$\left(\sum_{k\geq 0}\left(\frac{t}{m+t}\right)^k\frac{m}{m+t}\,\delta_k\right)^{*m}\to p_t$$

for any $t>0$. Equivalently, $c_{mp}\to p_t$, when $p=m/(m+t)$ with $t>0$ fixed.

PROOF. Let us denote by ν_m the geometric law under the convolution sign:

$$\nu_m=\sum_{k\geq 0}\left(\frac{t}{m+t}\right)^k\frac{m}{m+t}\,\delta_k$$

We have the following computation, for the Fourier transform of the limit:

$$\begin{aligned}
F_{\delta_k}(x)=e^{ikx}\quad&\implies\quad F_{\nu_m}(x)=\sum_{k\geq 0}\left(\frac{t}{m+t}\right)^k\frac{m}{m+t}\,e^{ikx}\\
&\implies\quad F_{\nu_m}(x)=\frac{m}{m+t-te^{ix}}\\
&\implies\quad F_{\nu_m^{*m}}(x)=\left(\frac{m}{m+t-te^{ix}}\right)^m\\
&\implies\quad F_{\nu_m^{*m}}(x)=\left(1+\frac{t(e^{ix}-1)}{m+t-te^{ix}}\right)^m\\
&\implies\quad F(x)=\exp\big(t(e^{ix}-1)\big)
\end{aligned}$$

Thus, we obtain indeed the Fourier transform of p_t, as desired. □

In practice, Theorems 8.19 and 8.20 lead to many occurrences of the Poisson laws, in relation with continuous phenomena from the real life. For instance, we have:

THEOREM 8.21. *The number of chewing gum pieces on a single tile of a sidewalk*

•		•	••		...
	•••		•	•••	...
••••		••	•	••	...

follows a Poisson law.

PROOF. This comes indeed from Theorem 8.19, and I will leave it to you, as an instructive exercise, to think some more at this, and clarify the details. □

8c. Algebraic aspects

What is next? You will be surprised, that is things that we already know. Indeed, we already met before a variable which might be Poisson, in our computations from chapter 4, in relation with permutations. So, let us recall from there that we have:

THEOREM 8.22. *The probability for a random permutation $\sigma \in S_N$ to be a derangement, that is, to have no fixed points, is given by the following formula:*

$$P = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots + (-1)^N \frac{1}{N!}$$

Thus we have the estimate $P \simeq 1/e$, in the $N \to \infty$ limit.

PROOF. This is something from chapter 4, but let us briefly recall the proof. With the notation $S_N^i = \{\sigma \in S_N | \sigma(i) = i\}$, the probability that we are interested in is:

$$\begin{aligned}
& P \\
= \ & \frac{1}{N!}\left(|S_N| - \sum_i |S_N^i| + \sum_{i<j} |S_N^i \cap S_N^j| - \ldots + (-1)^N \sum_{i_1<\ldots<i_N} |S_N^{i_1} \cap \ldots \cap S_N^{i_N}|\right) \\
= \ & \frac{1}{N!} \sum_{k=0}^{N} (-1)^k \sum_{i_1<\ldots<i_k} (N-k)! \\
= \ & \frac{1}{N!} \sum_{k=0}^{N} (-1)^k \binom{N}{k} (N-k)! \\
= \ & \frac{1}{N!} \sum_{k=0}^{N} (-1)^k \frac{N!}{k!(N-k)!} (N-k)! \\
= \ & \sum_{k=0}^{N} \frac{(-1)^k}{k!}
\end{aligned}$$

Since at the end we have the expansion of $1/e$, this finishes the proof. □

Let us discuss now, more generally, what happens when counting permutations having exactly k fixed points. The result here, extending Theorem 8.22, is as follows:

THEOREM 8.23. *The probability for a random permutation $\sigma \in S_N$ to have exactly k fixed points is given by the following formula:*

$$P = \frac{1}{k!}\left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^{N-1} \frac{1}{(N-1)!} + (-1)^N \frac{1}{N!}\right)$$

Thus we have the estimate $P \simeq 1/(ek!)$, in the $N \to \infty$ limit.

PROOF. We already know, from Theorem 8.22, that this formula holds at $k = 0$. In the general case now, we have to count the permutations $\sigma \in S_N$ having exactly k points. Since having such a permutation amounts in choosing k points among $1, \ldots, N$, and then permuting the $N - k$ points left, without fixed points allowed, we have:

$$\begin{aligned}
\#\left\{\sigma \in S_N \middle| \chi(\sigma) = k\right\} &= \binom{N}{k} \#\left\{\sigma \in S_{N-k} \middle| \chi(\sigma) = 0\right\} \\
&= \frac{N!}{k!(N-k)!} \#\left\{\sigma \in S_{N-k} \middle| \chi(\sigma) = 0\right\} \\
&= N! \times \frac{1}{k!} \times \frac{\#\left\{\sigma \in S_{N-k} \middle| \chi(\sigma) = 0\right\}}{(N-k)!}
\end{aligned}$$

Now by dividing everything by $N!$, we obtain from this the following formula:

$$\frac{\#\left\{\sigma \in S_N \middle| \chi(\sigma) = k\right\}}{N!} = \frac{1}{k!} \times \frac{\#\left\{\sigma \in S_{N-k} \middle| \chi(\sigma) = 0\right\}}{(N-k)!}$$

By using now the computation at $k = 0$, from Theorem 8.22, it follows that with $N \to \infty$ we have the following estimate, χ being the number of fixed points:

$$P(\chi = k) \simeq \frac{1}{k!} \cdot P(\chi = 0) \simeq \frac{1}{k!} \cdot \frac{1}{e}$$

Thus, we are led to the conclusion in the statement. □

Now observe that Theorem 8.23 reformulates into something very simple, namely:

THEOREM 8.24. *The number of fixed points of permutations,*

$$\chi(\sigma) = \#\left\{i \in \{1, \ldots, N\} \middle| \sigma(i) = i\right\}$$

when regarded as random variable $\chi : S_N \to \mathbb{N}$, satisfies the formula

$$\chi \sim p_1$$

that is, follows the Poisson law of parameter 1, in the $N \to \infty$ limit.

PROOF. This is a straightforward reformulation of Theorem 8.23, which tells us that with $N \to \infty$ we have the following estimate, for any $k \in \mathbb{N}$:

$$P(\chi = k) \simeq \frac{1}{ek!}$$

Indeed, according to our definition of the Poisson laws, this formula tells us precisely that the asymptotic law of the variable $\chi : S_N \to \mathbb{N}$ is Poisson (1), as stated. □

More generally now, and quite remarkably, we have in fact the following result:

THEOREM 8.25. *The number of partial fixed points of permutations,*

$$\chi_t(\sigma) = \#\left\{i \in \{1, \ldots, [tN]\} \middle| \sigma(i) = i\right\}$$

when regarded as random variable $\chi_t : S_N \to \mathbb{N}$, satisfies the formula

$$\chi_t \sim p_t$$

that is, follows the Poisson law of parameter $t \in (0, 1]$, in the $N \to \infty$ limit.

PROOF. We already know from Theorem 8.24 that the result holds at $t = 1$. In general, the proof is similar, the idea being as follows:

(1) Consider indeed the following sets, as in the proof of Theorem 8.24, or rather as in the proof of Theorem 8.22, leading to Theorem 8.24:

$$S_N^i = \left\{\sigma \in S_N \middle| \sigma(i) = i\right\}$$

The set of permutations having no fixed points among $1, \ldots, [tN]$ is then:

$$X_N = \left(\bigcup_{i \leq [tN]} S_N^i\right)^c$$

In order to compute now the cardinality $|X_N|$, consider as well the following sets, depending on indices $i_1 < \ldots < i_k$, obtained by taking intersections:

$$S_N^{i_1 \ldots i_k} = S_N^{i_1} \cap \ldots \cap S_N^{i_k}$$

As before in the proof of Theorem 8.22, we obtain by inclusion-exclusion that:

$$\begin{aligned}
P(\chi_t = 0) &= \frac{1}{N!} \sum_{k=0}^{[tN]} (-1)^k \sum_{i_1 < \ldots < i_k < [tN]} |S_N^{i_1 \ldots i_k}| \\
&= \frac{1}{N!} \sum_{k=0}^{[tN]} (-1)^k \sum_{i_1 < \ldots < i_k < [tN]} (N-k)! \\
&= \frac{1}{N!} \sum_{k=0}^{[tN]} (-1)^k \binom{[tN]}{k} (N-k)! \\
&= \sum_{k=0}^{[tN]} \frac{(-1)^k}{k!} \cdot \frac{[tN]!(N-k)!}{N!([tN]-k)!}
\end{aligned}$$

With $N\to\infty$, we obtain from this the following estimate:

$$\begin{aligned}P(\chi_t=0)&\simeq\sum_{k=0}^{[tN]}\frac{(-1)^k}{k!}\cdot t^k\\&=\sum_{k=0}^{[tN]}\frac{(-t)^k}{k!}\\&\simeq e^{-t}\end{aligned}$$

(2) More generally now, by counting the permutations $\sigma\in S_N$ having exactly k fixed points among $1,\ldots,[tN]$, as in the proof of Theorem 8.23, our claim is that we get:

$$P(\chi_t=k)\simeq\frac{t^k}{k!e^t}$$

We already know from (1) that this formula holds at $k=0$. In the general case now, we have to count the permutations $\sigma\in S_N$ having exactly k fixed points among $1,\ldots,[tN]$. Since having such a permutation amounts in choosing k points among $1,\ldots,[tN]$, and then permuting the $N-k$ points left, without fixed points among $1,\ldots,[tN]$ allowed, we obtain the following formula, where $s\in(0,1]$ is such that $[s(N-k)]=[tN]-k$:

$$\begin{aligned}\#\left\{\sigma\in S_N\Big|\chi_t(\sigma)=k\right\}&=\binom{[tN]}{k}\#\left\{\sigma\in S_{N-k}\Big|\chi_s(\sigma)=0\right\}\\&=\frac{[tN]!}{k!([tN]-k)!}\#\left\{\sigma\in S_{N-k}\Big|\chi_s(\sigma)=0\right\}\\&=\frac{1}{k!}\times\frac{[tN]!(N-k)!}{([tN]-k)!}\times\frac{\#\left\{\sigma\in S_{N-k}\Big|\chi_s(\sigma)=0\right\}}{(N-k)!}\end{aligned}$$

Now by dividing everything by $N!$, we obtain from this the following formula:

$$\frac{\#\left\{\sigma\in S_N\Big|\chi_t(\sigma)=k\right\}}{N!}=\frac{1}{k!}\times\frac{[tN]!(N-k)!}{N!([tN]-k)!}\times\frac{\#\left\{\sigma\in S_{N-k}\Big|\chi_s(\sigma)=0\right\}}{(N-k)!}$$

By using now the computation at $k=0$, that we already have, from (1) above, it follows that with $N\to\infty$ we have the following estimate:

$$\begin{aligned}P(\chi_t=k)&\simeq\frac{1}{k!}\times\frac{[tN]!(N-k)!}{N!([tN]-k)!}\cdot P(\chi_s=0)\\&\simeq\frac{t^k}{k!}\cdot P(\chi_s=0)\\&\simeq\frac{t^k}{k!}\cdot\frac{1}{e^s}\end{aligned}$$

Now recall that the parameter $s \in (0, 1]$ was chosen in the above such that:

$$[s(N - k)] = [tN] - k$$

Thus in the $N \to \infty$ limit we have $s = t$, and so we obtain, as claimed:

$$P(\chi_t = k) \simeq \frac{t^k}{k!} \cdot \frac{1}{e^t}$$

It follows that we obtain in the limit a Poisson law of parameter t, as stated. □

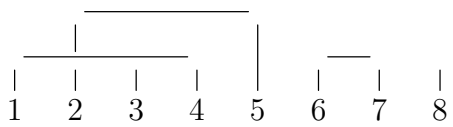
The above results are quite interesting, and are just the tip of the iceberg, with far more things, of interest for both algebra and probability, which can be said. We will be back to this, on a more systematic basis, a bit later, starting with chapter 9.

8d. Bell and Stirling

Getting back now to the basics of the Poisson laws, as a continuation of the above material, basically dealing with the mean and variance, let us discuss now the higher moments of these laws. As we will soon discover, things are quite tricky here, in relation with a lot of subtle mathematics, that will take us some time to understand.

Let us start with something that we are familiar with, from before, namely:

DEFINITION 8.26. *We denote by $P(k)$ the set of partitions of $\{1, \ldots, k\}$, with these partitions $\pi \in P(k)$ being most conveniently being drawn as diagrams,*



with the strings joining the numbers belonging to the same block of π. That is, the above diagram represents the partition $\{1, \ldots, 8\} = \{1, 3, 4\} \cup \{2, 5\} \cup \{6, 7\} \cup \{8\}$.

Now, let us study these partitions. And here, surprise, instead of pulling a theorem, as you would expect, we must formulate something quite modest, as follows:

PROPOSITION 8.27. *The Bell numbers $B_k = |P(k)|$ satisfy the recurrence relation*

$$B_{k+1} = \sum_s \binom{k}{s} B_{k-s}$$

with initial data $B_0 = 1$, $B_1 = 1$, and are numerically as follows:

$$1,\ 1,\ 2,\ 5,\ 15,\ 52,\ 203,\ 877,\ 4140,\ 21147,\ 115975,\ 678570,\ \ldots$$

However, there is no mathematical formula for B_k.

PROOF. There are several things going on here, the idea being as follows:

(1) Experiments first, before anything, let us compute a few Bell numbers. Obviously $B_1 = 1$, and then we have $B_2 = 2$, the partitions being as follows:

$$||\quad,\quad \sqcap$$

Next, we have $B_3 = 5$, the partitions at $k = 3$ being as follows:

$$|||\quad,\quad \sqcap|\quad,\quad \sqcap\!\!|\quad,\quad |\sqcap\quad,\quad \sqcap\!\sqcap$$

At $k = 4$ now, things become more complex, and it is better to trick. We can count the partitions up to permutations of the corresponding diagrams, and with this convention made, here are the relevant partitions and their multiplicities, leading to $B_4 = 15$:

$$||||\times 1\quad,\quad \sqcap||\times 6\quad,\quad \sqcap\sqcap\times 3\quad,\quad \sqcap\sqcap|\times 4\quad,\quad \sqcap\sqcap\sqcap\times 1$$

The same method works at $k = 5$, with the block distributions and multiplicities, which are simpler to draw than partitions, being as follows, leading to $B_5 = 52$:

$$11111 \to 1\ ,\ 2111 \to 10\ ,\ 221 \to 15\ ,\ 311 \to 10\ ,\ 32 \to 10\ ,\ 41 \to 5\ ,\ 5 \to 1$$

As for the case $k = 6$, where $B_6 = 203$, we will leave this as an instructive exercise.

(2) Let us try now to find a recurrence for these Bell numbers. Since a partition of $\{1, \ldots, k+1\}$ appears by choosing s partners for 1, among the k numbers available, and then partitioning the $k - s$ elements left, we have the following formula:

$$B_{k+1} = \sum_s \binom{k}{s} B_{k-s}$$

Observe that this formula forces us to talk about $B_0 = 1$, as done in the statement.

(3) As for the last assertion, regarding the non-computability of the Bell numbers, take this as a physics fact. Mankind has tried to find a formula for these numbers, had not found anything, and we are reporting here this finding, which is of course rock-solid. □

As a comment here, it is possible however to come up with several analytic results about the asymptotic behavior of the Bell numbers, by using the estimates from chapter 1. We will leave some work and learning here as an instructive exercise.

In relation now with the Poisson laws, and their higher moments, we first have the following result, dealing with the simplest case, where the parameter is $t = 1$:

THEOREM 8.28. *The moments of p_1 are the Bell numbers,*

$$M_k(p_1) = |P(k)|$$

where $P(k)$ is the set of partitions of $\{1, \ldots, k\}$.

PROOF. The moments of p_1 are given by the following formula:

$$M_k = \frac{1}{e}\sum_{n\geq 1}\frac{n^k}{n!}$$

We therefore have the following recurrence formula for these moments:

$$\begin{aligned}
M_{k+1} &= \frac{1}{e}\sum_{n\geq 1}\frac{n^{k+1}}{n!}\\
&= \frac{1}{e}\sum_{m\geq 0}\frac{(m+1)^k}{m!}\\
&= \frac{1}{e}\sum_{m\geq 0}\frac{m^k}{m!}\left(1+\frac{1}{m}\right)^k\\
&= \frac{1}{e}\sum_{m\geq 0}\frac{m^k}{m!}\sum_{s=0}^{k}\binom{k}{s}m^{-s}\\
&= \sum_{s=0}^{k}\binom{k}{s}\cdot\frac{1}{e}\sum_{m\geq 0}\frac{m^{k-s}}{m!}\\
&= \sum_{s=0}^{k}\binom{k}{s}M_{k-s}
\end{aligned}$$

With this done, let us try now to find a recurrence for the Bell numbers:

$$B_k = |P(k)|$$

A partition of $\{1,\ldots,k+1\}$ appears by choosing s neighbors for 1, among the k numbers available, and then partitioning the $k-s$ elements left. Thus, we have:

$$B_{k+1} = \sum_{s=0}^{k}\binom{k}{s}B_{k-s}$$

Thus, our moments M_k satisfy the same recurrence as the numbers B_k. Regarding now the initial values, in what concerns the first moment of p_1, we have:

$$M_1 = \frac{1}{e}\sum_{r}\frac{r}{r!} = 1$$

Also, by using the above recurrence for the numbers M_k, we obtain from this:

$$M_2 = \sum_{s}\binom{1}{s}M_{k-s} = 1+1 = 2$$

On the other hand, $B_1 = 1$ and $B_2 = 2$. Thus we obtain $M_k = B_k$, as claimed. □

Summarizing, the moments of the Poisson law p_1 are not computable. However, it is possible to say many theoretical things about them. We will be back to this.

As a continuation of the above study, more generally, we have the following result, dealing with the case of the arbitrary Poisson laws, p_t with $t > 0$:

THEOREM 8.29. *The moments of p_t with $t > 0$ are given by*

$$M_k(p_t) = \sum_{\pi \in P(k)} t^{|\pi|}$$

where $|.|$ is the number of blocks.

PROOF. The moments of the Poisson law p_t with $t > 0$ are given by:

$$M_k = e^{-t} \sum_{n \geq 1} \frac{t^n n^k}{n!}$$

We have the following recurrence formula for these moments:

$$\begin{aligned}
M_{k+1} &= e^{-t} \sum_{n \geq 1} \frac{t^n n^{k+1}}{n!} \\
&= e^{-t} \sum_{m \geq 0} \frac{t^{m+1} (m+1)^k}{m!} \\
&= e^{-t} \sum_{m \geq 0} \frac{t^{m+1} m^k}{m!} \left(1 + \frac{1}{m}\right)^k \\
&= e^{-t} \sum_{m \geq 0} \frac{t^{m+1} m^k}{m!} \sum_{s=0}^{k} \binom{k}{s} m^{-s} \\
&= \sum_{s=0}^{k} \binom{k}{s} \cdot e^{-t} \sum_{m \geq 0} \frac{t^{m+1} m^{k-s}}{m!} \\
&= t \sum_{s=0}^{k} \binom{k}{s} M_{k-s}
\end{aligned}$$

Regarding now the initial values, the first moment of p_t is given by:

$$\begin{aligned}
M_1 &= e^{-t} \sum_{r} \frac{t^r r}{r!} \\
&= e^{-t} \sum_{r} \frac{t^r}{(r-1)!} \\
&= t
\end{aligned}$$

Now by using the above recurrence we obtain from this:

$$\begin{aligned} M_2 &= t\sum_s \binom{1}{s} M_{k-s} \\ &= t(1+t) \\ &= t+t^2 \end{aligned}$$

On the other hand, consider the numbers in the statement, namely:

$$S_k = \sum_{\pi\in P(k)} t^{|\pi|}$$

Since a partition of $\{1,\ldots,k+1\}$ appears by choosing s neighbors for 1, among the k numbers available, and then partitioning the $k-s$ elements left, we have:

$$S_{k+1} = t\sum_s \binom{k}{s} S_{k-s}$$

As for the initial values of these numbers, these are as follows:

$$S_1 = t \quad , \quad S_2 = t+t^2$$

Thus the initial values coincide, and so by recurrence we obtain that these latter numbers are the moments of the Poisson law p_t, as stated. □

As an illustration now for the above result, numerically, we have:

THEOREM 8.30. *The low order moments of p_t are the numbers*

$$M_1 = t$$

$$M_2 = t+t^2$$

$$M_3 = t+3t^2+t^3$$

$$M_4 = t+7t^2+6t^3+t^4$$

$$M_5 = t+15t^2+25t^3+10t^4+t^5$$

$$\vdots$$

which at $t=1$ are the Bell numbers $1,2,5,15,52,\ldots$.

PROOF. We can use here input from the proof of Proposition 8.27, as follows:

(1) Obviously we have $B_1=1$, and $M_1=t$.

(2) Then $B_2=2$, the partitions being as follows, leading to $M_2=t+t^2$:

$$||\quad,\quad \sqcap$$

(3) Next, $B_3=5$, the partitions being as follows, leading to $M_3=t+3t^2+t^3$:

$$|||\quad,\quad \sqcap|\quad,\quad \sqcap\!\!\sqcap\quad,\quad |\sqcap\quad,\quad \sqcap\!\!\sqcap$$

(4) At $k = 4$ now, things become more complex, and it is better to trick. We can count the partitions up to permutations of the corresponding diagrams, and with this convention made, here are the relevant partitions and their multiplicities, leading to $B_4 = 15$:

$$|\,|\,|\,|\times 1 \quad , \quad \sqcap\,|\,|\times 6 \quad , \quad \sqcap\sqcap\times 3 \quad , \quad \sqcap\!\sqcap\,|\times 4 \quad , \quad \sqcap\!\sqcap\!\sqcap\times 1$$

But this leads to the formula in the statement for the fourth moment, namely:

$$M_4 = t + 7t^2 + 6t^3 + t^4$$

(5) The same method works at $k = 5$, with the block distributions and multiplicities, which are simpler to draw than partitions, being as follows, leading to $B_5 = 52$:

$$11111 \to 1\ ,\ 2111 \to 10\ ,\ 221 \to 15\ ,\ 311 \to 10\ ,\ 32 \to 10\ ,\ 41 \to 5\ ,\ 5 \to 1$$

But this leads to the formula in the statement for the fifth moment, namely:

$$M_5 = t + 15t^2 + 25t^3 + 10t^4 + t^5$$

(6) Next, in what regards the case $k = 6$, where $B_6 = 203$, or even higher, $k = 7, 8$ and so on, we will leave some computations here as an instructive exercise.

(7) Finally, let us mention that the coefficients appearing in the statement are called Stirling numbers. And exercise of course for you, to learn more about them. □

As a continuation of this, and as a last topic for this chapter let us discuss now the central moments of the Poisson laws. The result here is as follows:

THEOREM 8.31. *The low order central moments of p_t are the numbers*

$$M_1' = 0$$
$$M_2' = t$$
$$M_3' = t$$
$$M_4' = t + 3t^2$$
$$M_5' = t + 10t^2$$
$$\vdots$$

which at $t = 1$ are the numbers $0, 1, 1, 4, 11, \ldots$

PROOF. According to our formulae in chapters 5-6, and using $E = t$, we have:

$$M_k' = \sum_{s=0}^{k} (-1)^s \binom{k}{s} t^s M_{k-s}$$

In particular, at $t = 1$ we have the following formula, B_s being the Bell numbers:

$$M_k' = \sum_{s=0}^{k} (-1)^s \binom{k}{s} B_{k-s}$$

But with this, in practice, we are led to the formulae in the statement. □

Let us end this discussion with the following result, capturing the essentials:

THEOREM 8.32. *For the Poisson law p_t of parameter $t > 0$,*

$$E = t \quad , \quad V = t \quad , \quad \gamma = \frac{1}{\sqrt{t}} \quad , \quad \kappa = 3 + \frac{1}{t}$$

are the mean, variance, skewness and kurtosis.

PROOF. Regarding the formulae of E, V, we know these from Proposition 8.15. As for the formulae of γ, κ, these follow from Theorem 8.31. Indeed, we first have:

$$\gamma = \frac{M_2'}{V\sqrt{V}} = \frac{t}{t\sqrt{t}} = \frac{1}{\sqrt{t}}$$

As for the kurtosis, again by using Theorem 8.31, this is given by:

$$\kappa = \frac{M_3'}{V^2} = \frac{t + 3t^2}{t^2} = 3 + \frac{1}{t}$$

Thus, we are led to the conclusions in the statement. □

8e. Exercises

This was a key theoretical chapter, and as exercises on this, we have:

EXERCISE 8.33. *Read a bit of measure theory, or continuous probability theory.*

EXERCISE 8.34. *Find counterexamples, in relation with the 3 types of convergence.*

EXERCISE 8.35. *Learn a bit about bell-shaped curves, and central limits.*

EXERCISE 8.36. *Learn more about the precise convergence in the PLT.*

EXERCISE 8.37. *Try doing the algebra for various permutation groups $G \subset S_N$.*

EXERCISE 8.38. *Work out some asymptotics for the Bell numbers.*

EXERCISE 8.39. *Learn more about the Stirling numbers, and their properties.*

EXERCISE 8.40. *Do some further computations for the normalized central moments.*

As bonus exercise, do some real-life experiments, as to reach to the Poisson laws.

Part III

Further variables

Tengo la camisa negra
Hoy mi amor esta de luto
Hoy tengo en el alma una pena
Y es por culpa de tu embrujo

CHAPTER 9

Group theory

9a. Groups, examples

With the basics of probability theory learned, what is next? Many possible things, and we have at least 4 interesting directions to be explored, as follows:

(1) The discrete laws that we know so far, namely Bernoulli and binomial, then geometric and Pascal, and then Poisson, are related to each other, and certainly have some technical generalizations, worth exploring. Can we reach to some "big picture" here?

(2) Still talking laws that we have so far, we have seen that the mathematics of their moments leads to some interesting combinatorics and calculus, involving partitions, polynomials, and other functions. Again, can we reach to some "big picture" here?

(3) Talking now laws that we don't have yet, we certainly need to talk about central limits and bell-shaped curves, and perhaps some other continuous measures too. And then, speaking generalizations, why not having a look at quantum probability too?

(4) Finally, more modestly, I don't know about you, but in what concerns me, from what we learned so far, what I find most exciting are that permutation group models for the Poisson laws. So, why not working some more on this, probability on groups.

Well, this is the situation, and not clear what to do next. Not that this is a matter of life and death, we still have 200 pages in this book, and we will certainly have a look at all of (1-4), but what to start with, right, this is a legit question. And in the lack of a clear idea here, and with cats gone as usual, I guess I will have to ask the rat:

RAT 9.1. *You should go with groups, the big picture comes from there. And don't worry about physics and quantum, gauge theory rules there.*

Thanks rat, quite interesting all this, and certainly more advanced than what I was expecting. In fact, thinking well, that missing volumes of Feynman, and those of Weinberg too, in my personal library, must have been chewed by him, at night, while I was sleeping. So, too bad for the money, but now I have my answer, and this is what matters. By the way, with rat being now obviously more advanced than me, and than cats too, I will have to instruct the said cats that mice chasing inside the house is now forbidden.

So, group theory. The groups are something very simple, as follows:

DEFINITION 9.2. *A group is a set G endowed with a multiplication operation*

$$(g,h)\to gh$$

which must satisfy the following conditions:

(1) *Associativity: we have $(gh)k=g(hk)$, for any $g,h,k\in G$.*
(2) *Unit: there is an element $1\in G$ such that $g1=1g=g$, for any $g\in G$.*
(3) *Inverses: for any $g\in G$ there is $g^{-1}\in G$ such that $gg^{-1}=g^{-1}g=1$.*

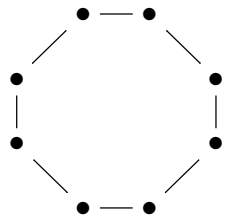
The multiplication law is not necessarily commutative. In the case where it is, in the sense that $gh=hg$, for any $g,h\in G$, we call G abelian, en hommage to Abel, and we usually denote its multiplication, unit and inverse operation as follows:

$$(g,h)\to g+h\quad,\quad 0\in G\quad,\quad g\to -g$$

However, this is not a general rule, and rather the converse is true, in the sense that if a group is denoted as above, this means that the group must be abelian.

Getting now to the finite group case, which is of particular interest for us, as a basic example here we have the cyclic group $\mathbb{Z}_N$, constructed as follows:

DEFINITION 9.3. *The cyclic group $\mathbb{Z}_N$ is the group formed by the N rotations of the regular N-gon, with the group operation being the composition of these rotations:*

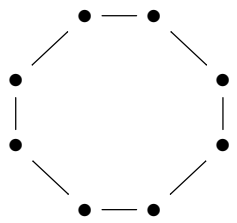


Alternatively, $\mathbb{Z}_N=\{0,1,2,\ldots,N-1\}$ is the group of remainders modulo N, with the usual addition operation for such remainders.

Here the fact that the above two definitions of $\mathbb{Z}_N$ are indeed equivalent comes from the fact that, with the first approach, if we set $\mathbb{Z}_N=\{R_0,R_1,R_2,\ldots,R_{N-1}\}$, with $R_0=id$, and with $R_1,R_2,\ldots$ being the other rotations, listed in increasing counterclockwise order, the group law is given by $R_kR_l=R_{k+l}$, with $k+l$ taken modulo N. Thus, we have $\mathbb{Z}_N=\{0,1,2,\ldots,N-1\}$, with the group operation being $(k,l)\to k+l$, modulo N.

Passed the cyclic group $\mathbb{Z}_N$, as a second basic example of a finite group, which is this time not abelian, we have the dihedral group D_N, which appears as follows:

DEFINITION 9.4. *The dihedral group D_N is the symmetry group of*



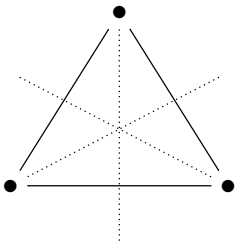
that is, of the regular polygon having N vertices.

In order to understand how this works, here are the basic examples of regular N-gons, at small values of the parameter $N \in \mathbb{N}$, along with their symmetry groups:

$\underline{N = 2}$. Here the N-gon is just a segment, and its symmetries are obviously the identity id, plus the symmetry τ with respect to the middle of the segment:

Thus we have $D_2 = \{id, \tau\}$, which in group theory terms means $D_2 = \mathbb{Z}_2$.

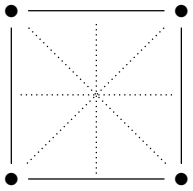
$\underline{N = 3}$. Here the N-gon is an equilateral triangle, and we have 6 symmetries, the rotations of angles $0°$, $120°$, $240°$, and the symmetries with respect to the altitudes:



Alternatively, we can say that the symmetries are all the $3! = 6$ possible permutations of the vertices, and so that in group theory terms, we have $D_3 = S_3$.

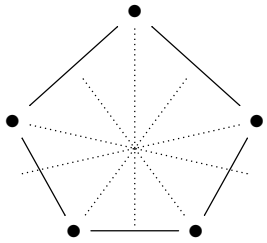
$\underline{N = 4}$. Here the N-gon is a square, and as symmetries we have 4 rotations, of angles $0°, 90°, 180°, 270°$, as well as 4 symmetries, with respect to the 4 symmetry axes, which

are the 2 diagonals, and the 2 segments joining the midpoints of opposite sides:

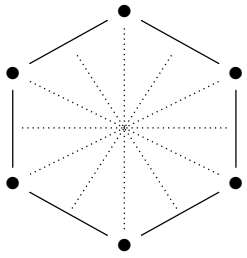


Thus, we obtain as symmetry group some sort of product between $\mathbb{Z}_4$ and $\mathbb{Z}_2$. Observe however that this product is not the usual one, our group being not abelian.

$\underline{N=5}$. Here the N-gon is a regular pentagon, and as symmetries we have 5 rotations, of angles $0°, 72°, 144°, 216°, 288°$, as well as 5 symmetries, with respect to the 5 symmetry axes, which join the vertices to the midpoints of the opposite sides:



$\underline{N=6}$. Here the N-gon is a regular hexagon, and we have 6 rotations, of angles $0°, 60°, 120°, 180°, 240°, 300°$, and 6 symmetries, with respect to the 6 symmetry axes, which are the 3 diagonals, and the 3 segments joining the midpoints of opposite sides:



In general now, let us start with the following basic fact, inspired by the above:

PROPOSITION 9.5. *The dihedral group D_N has $2N$ elements, as follows:*

1. *We have N rotations $R_1, \ldots, R_N$, with R_k being the rotation of angle $2k\pi/N$. When labeling the vertices of the N-gon $1, \ldots, N$, we have $R_k : i \to k + i$.*
2. *We have N symmetries $S_1, \ldots, S_N$, with S_k being the symmetry with respect to the Ox axis rotated by $k\pi/N$. The symmetry formula is $S_k : i \to k - i$.*

PROOF. This is clear, indeed. To be more precise, D_N consists of:

(1) The N rotations, those of angles $2k\pi/N$ with $k = 1, \ldots, N$. But these are exactly the rotations $R_1, \ldots, R_N$ from the statement.

(2) The N symmetries with respect to the N possible symmetry axes. But these are exactly the symmetries $S_1, \ldots, S_N$ from the statement. □

With the above description of D_N in hand, we can forget if we want about geometry and the regular N-gon, and talk about D_N abstractly, as follows:

THEOREM 9.6. *The dihedral group D_N is the group having $2N$ elements, $R_1, \ldots, R_N$ and $S_1, \ldots, S_N$, called rotations and symmetries, which multiply as follows,*

$$R_k R_l = R_{k+l} \quad , \quad R_k S_l = S_{k+l}$$

$$S_k R_l = S_{k-l} \quad , \quad S_k S_l = R_{k-l}$$

with all the indices being taken modulo N.

PROOF. With notations from Proposition 9.5, the various compositions between rotations and symmetries can be computed as follows:

$$R_k R_l \ : \ i \to l + i \to k + l + i$$

$$R_k S_l \ : \ i \to l - i \to k + l - i$$

$$S_k R_l \ : \ i \to l + i \to k - l - i$$

$$S_k S_l \ : \ i \to l - i \to k - l + i$$

But these are exactly the formulae for $R_{k+l}, S_{k+l}, S_{k-l}, R_{k-l}$, as stated. Now since a group is uniquely determined by its multiplication rules, this gives the result. □

The above is not the end of the story which the dihedral group D_N. Observe indeed that this group has the same cardinality as the following group:

$$E_N = \mathbb{Z}_N \times \mathbb{Z}_2$$

We obviously don't have $D_N \simeq E_N$, because D_N is not abelian, while E_N is. So, our next goal will be that of proving that D_N appears by "twisting" E_N. Let us start with:

PROPOSITION 9.7. *The group $E_N = \mathbb{Z}_N \times \mathbb{Z}_2$ is the group having $2N$ elements, $r_1, \ldots, r_N$ and $s_1, \ldots, s_N$, which multiply according to the following rules,*

$$r_k r_l = r_{k+l} \quad , \quad r_k s_l = s_{k+l}$$

$$s_k r_l = s_{k+l} \quad , \quad s_k s_l = r_{k+l}$$

with all the indices being taken modulo N.

PROOF. With the notation $\mathbb{Z}_2 = \{1, \tau\}$, the elements of the product group $E_N = \mathbb{Z}_N \times \mathbb{Z}_2$ can be labeled $r_1, \ldots, r_N$ and $s_1, \ldots, s_N$, as follows:

$$r_k = (k, 1) \quad , \quad s_k = (k, \tau)$$

These elements multiply then according to the formulae in the statement. Now since a group is uniquely determined by its multiplication rules, this gives the result. □

Let us compare now Theorem 9.6 and Proposition 9.7. In order to formally obtain D_N from E_N, we must twist some of the multiplication rules of E_N, namely:

$$s_k r_l = s_{k+l} \to s_{k-l}$$

$$s_k s_l = r_{k+l} \to r_{k-l}$$

Informally, this amounts in following the rule "τ switches the sign of what comes afterwards", and we are led in this way to the following definition:

DEFINITION 9.8. *Given groups H, K, with an action $K \curvearrowright H$, the crossed product*

$$G = H \rtimes K$$

is the set $H \times K$, with multiplication $(g, s)(h, t) = (gh^s, st)$.

It is routine to check that G is indeed a group. Observe that when the action is trivial, $h^s = h$ for any $h \in H$ and $s \in K$, we obtain the usual product $H \times K$.

Now with this technology in hand, by getting back to the dihedral group D_N, we can improve Theorem 9.6, into a final result on the subject, as follows:

THEOREM 9.9. *We have a crossed product decomposition as follows,*

$$D_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$$

with $\mathbb{Z}_2 = \{1, \tau\}$ acting on $\mathbb{Z}_N$ via switching signs, $k^\tau = -k$.

PROOF. We have an action $\mathbb{Z}_2 \curvearrowright \mathbb{Z}_N$ given by the formula in the statement, namely $k^\tau = -k$, so we can consider the corresponding crossed product group:

$$L_N = \mathbb{Z}_N \rtimes \mathbb{Z}_2$$

In order to understand the structure of L_N, we follow Proposition 9.7. The elements of L_N can indeed be labeled $\rho_1, \ldots, \rho_N$ and $\sigma_1, \ldots, \sigma_N$, as follows:

$$\rho_k = (k, 1) \quad , \quad \sigma_k = (k, \tau)$$

Now when computing the products of such elements, we basically obtain the formulae in Proposition 9.7, perturbed as in Definition 9.8. To be more precise, we have:

$$\rho_k \rho_l = \rho_{k+l} \quad , \quad \rho_k \sigma_l = \sigma_{k+l}$$

$$\sigma_k \rho_l = \sigma_{k+l} \quad , \quad \sigma_k \sigma_l = \rho_{k+l}$$

But these are exactly the multiplication formulae for D_N, from Theorem 9.6. Thus, we have an isomorphism $D_N \simeq L_N$ given by $R_k \to \rho_k$ and $S_k \to \sigma_k$, as desired. □

9b. Cayley embeddings

Let us go back now to the symmetric groups, which are fundamental objects in group theory, as we will soon discover. These groups are constructed as follows:

DEFINITION 9.10. *The symmetric group S_N is the group of permutations*

$$\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$$

of $\{1, \ldots, N\}$. This group has $N!$ elements, and is not abelian at $N \geq 3$.

To be more precise, these are things that we know since chapter 4, with the fact that S_N is indeed a group being clear, and with the last assertion being something clear too. In addition to this, we also know that at $N \leq 3$ we have the following formulae:

$$S_1 = \{1\} \quad , \quad S_2 = \mathbb{Z}_2 \quad , \quad S_3 = D_3$$

In practice, many interesting things can be said about S_N. At the level of the general theory, we have the following fundamental result, due to Cayley:

THEOREM 9.11. *Given a finite group G, we have an embedding as follows,*

$$G \subset S_N \quad , \quad g \to (h \to gh)$$

with $N = |G|$. Thus, any finite group is a permutation group.

PROOF. Given a group element $g \in G$, we can associate to it the following map:

$$\sigma_g : G \to G \quad , \quad h \to gh$$

Since $gh = gh'$ implies $h = h'$, this map is bijective, and so is a permutation of G, viewed as a set. Thus, with $N = |G|$, we can view this map as a usual permutation, $\sigma_G \in S_N$. Summarizing, we have constructed so far a map as follows:

$$G \to S_N \quad , \quad g \to \sigma_g$$

Our first claim is that this is a group morphism. Indeed, this follows from:

$$\sigma_g \sigma_h(k) = \sigma_g(hk) = ghk = \sigma_{gh}(k)$$

It remains to prove that this group morphism is injective. But this follows from:

$$\begin{aligned} g \neq h &\implies \sigma_g(1) \neq \sigma_h(1) \\ &\implies \sigma_g \neq \sigma_h \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Observe that in the above statement the embedding $G \subset S_N$ that we constructed depends on a particular writing $G = \{g_1, \ldots, g_N\}$, which is needed in order to identify the permutations of G with the elements of the symmetric group S_N. This is not very

good, in practice, and as an illustration, for the basic examples of groups that we know, the Cayley theorem provides us with embeddings as follows:

$$\mathbb{Z}_N \subset S_N \quad , \quad D_N \subset S_{2N} \quad , \quad S_N \subset S_{N!}$$

And here the first embedding is the good one, the second one is not the best possible one, but can be useful for certain purposes, and the third embedding is certainly useless. Thus, as a conclusion, the Cayley theorem remains something quite theoretical.

Nevermind. As a next twist to the story, we have the following key result:

THEOREM 9.12. *We have a group embedding as follows, obtained by regarding S_N as the permutation group of the N coordinate axes of $\mathbb{R}^N$,*

$$S_N \subset O_N$$

which makes $\sigma \in S_N$ correspond to the matrix having 1 on row $\sigma(j)$ and column j, for any j, and having 0 entries elsewhere.

PROOF. This is something quite fundamental, the idea being as follows:

(1) To start with, we can certainly regard S_N as being the permutation group of the N coordinate axes of $\mathbb{R}^N$. Now since these permutations of the N coordinate axes of $\mathbb{R}^N$ are isometries, this provides us with a group embedding $S_N \subset O_N$, as stated.

(2) Regarding now the formula of this embedding, we have by definition:

$$\sigma(e_j) = e_{\sigma(j)}$$

Thus, the permutation matrix corresponding to σ is given by:

$$\sigma_{ij} = \begin{cases} 1 & \text{if } \sigma(j) = i \\ 0 & \text{otherwise} \end{cases}$$

We are theferore led to the conclusion in the statement. □

In practice now, in order to get familiar with the permutation matrices, nothing beats working out some examples. For $S_2 = \{1, \tau\}$ the situation is very simple, as follows:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad , \quad \tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Regarding now S_3, with the standard (ijk) notation for its elements, we have:

$$(123) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad (213) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad (132) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$(321) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad , \quad (231) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad , \quad (312) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

And so on, you get the idea with this. The point now is that we can combine the above result with the Cayley theorem, and we obtain in this way:

THEOREM 9.13. *Given a finite group G, we have an embedding as follows,*

$$G \subset O_N \quad , \quad g \to (e_h \to e_{gh})$$

with $N = |G|$. Thus, any finite group is an orthogonal matrix group.

PROOF. The Cayley theorem gives an embedding as follows:

$$G \subset S_N \quad , \quad g \to (h \to gh)$$

On the other hand, Theorem 9.12 provides us with an embedding as follows:

$$S_N \subset O_N \quad , \quad \sigma \to (e_i \to e_{\sigma(i)})$$

Thus, we are led to the conclusion in the statement. □

The same remarks as for the Cayley theorem apply. First, the embedding $G \subset O_N$ that we constructed depends on a particular writing $G = \{g_1, \ldots, g_N\}$. And also, for the basic examples of groups that we know, the embeddings that we obtain are as follows:

$$\mathbb{Z}_N \subset O_N \quad , \quad D_N \subset O_{2N} \quad , \quad S_N \subset O_{N!}$$

And here, as before with Cayley, the first embedding is the good one, the second one is not the best possible one, but can be useful, and the third embedding is useless.

In any case, all this is not very good, and in order to advance, it is better to forget about the Cayley theorem, and build on Theorem 9.12 instead. So, let us start with the following result, standing as a useful complement to Theorem 9.12:

THEOREM 9.14. *The embedding $S_N \subset O_N$ is given by the formula*

$$\sigma_{ij} = \delta_{i\sigma(j)}$$

with a Kronecker symbol on the right, and has the following properties:

(1) *Products of permutation matrices correspond to compositions of permutations.*
(2) *Transposing permutation matrices corresponds to inverting permutations.*
(3) *The permutation matrices are diagonalizable, over $\mathbb{C}$.*
(4) *Their eigenvalues are roots of unity of order N.*
(5) *The trace $Tr(\sigma)$ equals the number of fixed points of σ.*
(6) *As for the determinant $\det(\sigma)$, this must be ± 1.*

PROOF. We know that $S_N \subset O_N$ is given by $\sigma(e_j) = e_{\sigma(j)}$, and this gives right away the formula in the statement, $\sigma_{ij} = \delta_{i\sigma(j)}$. As for the other assertions:

(1) This comes from the fact that $S_N \subset O_N$ is a group morphism.

(2) This comes too from our group morphism $S_N \subset O_N$, via the well-known inversion formula $U^t = U^{-1}$ for the orthogonal matrices.

(3) This is something heavier, coming from the spectral theorem in linear algebra, which tells us that any $U \in O_N$ is diagonalizable over $\mathbb{C}$. In case you wonder if $\mathbb{C}$ is really needed, here is a quick computation, for the permutation $\sigma = (231) \in S_3$:

$$\det(x - \sigma) = \begin{vmatrix} x & 0 & -1 \\ -1 & x & 0 \\ 0 & -1 & x \end{vmatrix} = x^3 - 1$$

(4) This comes again from linear algebra, and more specifically, from:

$$\sigma v = \lambda v \implies \sigma^N v = \lambda^N v \implies v = \lambda^N v \implies \lambda^N = 1$$

(5) This is something elementary, coming from the following computation:

$$Tr(\sigma) = \sum_i \sigma_{ii} = \sum_i \delta_{i\sigma(i)} = \#\left\{i \middle| \sigma(i) = i\right\}$$

(6) This is clear indeed from the definition of det, and more on this later. □

Getting back now to the various groups that we know, we have here:

THEOREM 9.15. *We have the following finite groups of matrices:*

(1) $\mathbb{Z}_N \subset O_N$, *the cyclic permutation matrices.*
(2) $D_N \subset O_N$, *the dihedral permutation matrices.*
(3) $S_N \subset O_N$, *the permutation matrices.*

PROOF. This is something self-explanatory, the idea being that Theorem 9.12 provides us with embeddings as follows, given by the permutation matrices:

$$\mathbb{Z}_N \subset D_N \subset S_N \subset O_N$$

In practice now, the groups in the statement appear as follows:

(1) The cyclic permutation matrices are by definition the matrices as follows, with 0 entries elsewhere, and form a group, which is isomorphic to the cyclic group $\mathbb{Z}_N$:

$$U = \begin{pmatrix} & & 1 & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \\ 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \end{pmatrix}$$

(2) The dihedral matrices are the above cyclic permutation matrices, plus some suitable symmetry permutation matrices, and form a group which is isomorphic to D_N.

(3) The permutation matrices, which by Theorem 9.12 form a group which is isomorphic to S_N, are the $0-1$ matrices having exactly one 1 on each row and column. □

9c. Characters, laws

We would like to develop in what follows some theory for the subgroups $G \subset U_N$, with our main example being the symmetric group $S_N \subset O_N$. Let us start with:

DEFINITION 9.16. *A representation of a finite group G is a group morphism*

$$u : G \to U_N$$

into a unitary group. The character of such a representation is the function

$$\chi : G \to \mathbb{C} \quad , \quad g \to Tr(u_g)$$

where Tr is the usual, unnormalized trace of the $N \times N$ matrices.

As a basic example here, for any finite group we always have available the trivial 1-dimensional representation, equal to its character, which is by definition as follows:

$$1 : G \to U_1 \quad , \quad g \to (1)$$

In the case where our group G naturally appears as a group of unitary matrices, the embedding $G \subset U_N$ is of course a representation, called fundamental representation:

$$u : G \subset U_N \quad , \quad g \to g$$

Finally, observe that this latter situation is in fact the generic one, at least theoretically, because available for any finite group G is its Cayley representation:

$$G \subset S_N \subset O_N \subset U_N \quad , \quad N = |G|$$

This being said, always careful with Cayley, as already pointed out in the above, and this is why we chose in Definition 9.16 to use the whole U_N, instead of just O_N.

In general now, let us first discuss the various operations on the representations. We have here the following elementary result, coming from definitions:

PROPOSITION 9.17. *The representations of a finite group G are subject to:*

(1) *Making sums. Given representations u, v, of dimensions N, M, their sum is the $N + M$-dimensional representation $u + v = diag(u, v)$.*
(2) *Making products. Given representations u, v, of dimensions N, M, their product is the NM-dimensional representation $(u \otimes v)_{ia,jb} = u_{ij} v_{ab}$.*
(3) *Taking conjugates. Given a N-dimensional representation u, its conjugate is the N-dimensional representation $(\bar{u})_{ij} = \bar{u}_{ij}$.*
(4) *Spinning by unitaries. Given a N-dimensional representation u, and a unitary $V \in U_N$, we can spin u by this unitary, $u \to VuV^*$.*

PROOF. The fact that the operations in the statement are indeed well-defined, among morphisms from G to unitary groups, is indeed clear from definitions. □

In relation now with characters, we have the following result:

PROPOSITION 9.18. *We have the following formulae, regarding characters*

$$\chi_{u+v}=\chi_u+\chi_v\quad,\quad\chi_{u\otimes v}=\chi_u\chi_v\quad,\quad\chi_{\bar{u}}=\bar{\chi}_u\quad,\quad\chi_{VuV^*}=\chi_u$$

in relation with the basic operations for the representations.

PROOF. All these assertions are elementary, by using the following formulae:

$$Tr(diag(U,V))=Tr(U)+Tr(V)\quad,\quad Tr(U\otimes V)=Tr(U)Tr(V)$$

$$Tr(\bar{U})=\overline{Tr(U)}\quad,\quad Tr(VUV^*)=Tr(U)$$

Thus, we are led to the character formulae in the statement. □

Assume now that we are given a finite group $G\subset U_N$. By using the above operations, we can construct a whole family of representations of G, as follows:

DEFINITION 9.19. *Given a finite group $G\subset U_N$, its Peter-Weyl representations are the tensor products between the fundamental representation and its conjugate:*

$$u:G\subset U_N\quad,\quad\bar{u}:G\subset U_N$$

We denote these tensor products $u^{\otimes k}$, with $k=\circ\bullet\bullet\circ\ldots$ being a colored integer, with the colored tensor powers being defined according to the rules

$$u^{\otimes\circ}=u\quad,\quad u^{\otimes\bullet}=\bar{u}\quad,\quad u^{\otimes kl}=u^{\otimes k}\otimes u^{\otimes l}$$

and with the convention that $u^{\otimes\emptyset}$ is the trivial representation $1:G\to U_1$.

Here are a few examples of such Peter-Weyl representations, namely those coming from the colored integers of length 2, to be often used in what follows:

$$u^{\otimes\circ\circ}=u\otimes u\quad,\quad u^{\otimes\circ\bullet}=u\otimes\bar{u}$$

$$u^{\otimes\bullet\circ}=\bar{u}\otimes u\quad,\quad u^{\otimes\bullet\bullet}=\bar{u}\otimes\bar{u}$$

In relation now with characters, we have the following result:

THEOREM 9.20. *The characters of Peter-Weyl representations are given by*

$$\chi_{u^{\otimes k}}=(\chi_u)^k$$

with the colored powers of a variable χ being by definition given by

$$\chi^\circ=\chi\quad,\quad\chi^\bullet=\bar{\chi}\quad,\quad\chi^{kl}=\chi^k\chi^l$$

and with the convention that $\chi^\emptyset$ equals by definition 1.

PROOF. This follows indeed from the additivity, multiplicativity and conjugation formulae established in Proposition 9.18, via the conventions in Definition 9.19. □

The above result is quite interesting, and as a main job for us now, which will eventually provide a link with the material from chapter 8, we would like to integrate the characters of Peter-Weyl representations. In order to discuss this, and directly in the more general case of the compact groups $G\subset U_N$, we first have:

PROPOSITION 9.21. *Given a unital positive linear form $\varphi : C(G) \to \mathbb{C}$, the limit*

$$\int_\varphi f = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f)$$

exists, and for a coefficient of a representation $f = (\tau \otimes id)v$ we have

$$\int_\varphi f = \tau(P)$$

where P is the orthogonal projection onto the 1-eigenspace of $(id \otimes \varphi)v$.

PROOF. By linearity, it is enough to prove the first assertion for functions of the following type, where v is a Peter-Weyl representation, and τ is a linear form:

$$f = (\tau \otimes id)v$$

Thus we are led into the second assertion, and more precisely, we can have the whole result proved if we can establish the following formula, with $f = (\tau \otimes id)v$:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f) = \tau(P)$$

In order to prove this latter formula, observe first that we have:

$$\varphi^{*k}(f) = (\tau \otimes \varphi^{*k})v = \tau((id \otimes \varphi^{*k})v)$$

Now let us set $M = (id \otimes \varphi)v$. In terms of this matrix, we have:

$$\begin{aligned}((id \otimes \varphi^{*k})v)_{i_0 i_{k+1}} &= \sum_{i_1 \ldots i_k} ((id \otimes \varphi)v)_{i_0 i_1} \ldots ((id \otimes \varphi)v)_{i_k i_{k+1}} \\ &= \sum_{i_1 \ldots i_k} M_{i_0 i_1} \ldots M_{i_k i_{k+1}} \\ &= (M^k)_{i_0 i_{k+1}}\end{aligned}$$

Thus $(id \otimes \varphi^{*k})v = M^k$, and it follows that our Cesàro limit is given by:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \tau(M^k) = \tau\left(\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} M^k\right)$$

Since v is unitary we have $||v|| = 1$, and from $M = (id \otimes \varphi)v$ we obtain $||M|| \leq 1$. We conclude that the last Cesàro limit appearing above converges, and equals the orthogonal projection onto the 1-eigenspace of M. That is, we conclude that we have:

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} M^k = P$$

Thus our initial Cesàro limit converges as well, to the quantity $\tau(P)$, as desired. □

The point now is that when the linear form $\varphi \in C(G)^*$ from the above result is chosen faithful, we obtain the following finer result, which is something very useful:

PROPOSITION 9.22. *Given a faithful unital linear form $\varphi \in C(G)^*$, the limit*

$$\int_\varphi f = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}(f)$$

exists, and is independent of φ, given on coefficients of representations by

$$\left(id \otimes \int_\varphi\right) v = P$$

where P is the orthogonal projection onto the space $Fix(v) = \left\{\xi \in \mathbb{C}^n \middle| v\xi = \xi\right\}$.

PROOF. In view of Proposition 9.21, it remains to prove that when φ is faithful, the 1-eigenspace of the matrix $M = (id \otimes \varphi)v$ equals the space $Fix(v)$.

"$\supset$" This is clear, and for any φ, because we have the following implication:

$$v\xi = \xi \implies M\xi = \xi$$

"$\subset$" Here we must prove that, when φ is faithful, we have:

$$M\xi = \xi \implies v\xi = \xi$$

For this purpose, assume that we have $M\xi = \xi$, and consider the following function:

$$f = \sum_i \left(\sum_j v_{ij}\xi_j - \xi_i\right)\left(\sum_k v_{ik}\xi_k - \xi_i\right)^*$$

We must prove that we have $f = 0$. Since v is unitary, we have:

$$\begin{aligned} f &= \sum_{ijk} v_{ij}v_{ik}^*\xi_j\bar{\xi}_k - \frac{1}{N}v_{ij}\xi_j\bar{\xi}_i - \frac{1}{N}v_{ik}^*\xi_i\bar{\xi}_k + \frac{1}{N^2}\xi_i\bar{\xi}_i \\ &= \sum_j |\xi_j|^2 - \sum_{ij} v_{ij}\xi_j\bar{\xi}_i - \sum_{ik} v_{ik}^*\xi_i\bar{\xi}_k + \sum_i |\xi_i|^2 \\ &= ||\xi||^2 - < v\xi, \xi > - \overline{< v\xi, \xi >} + ||\xi||^2 \\ &= 2(||\xi||^2 - Re(< v\xi, \xi >)) \end{aligned}$$

By using now our assumption $M\xi = \xi$, we obtain from this:

$$\begin{aligned} \varphi(f) &= 2\varphi(||\xi||^2 - Re(< v\xi, \xi >)) \\ &= 2(||\xi||^2 - Re(< M\xi, \xi >)) \\ &= 2(||\xi||^2 - ||\xi||^2) \\ &= 0 \end{aligned}$$

Now since φ is faithful, this gives $f = 0$, and so $v\xi = \xi$, as claimed. □

Good news, we can now formulate a main result about integration, as follows:

THEOREM 9.23. *The integration over a compact group $G \subset U_N$ can be constructed by starting with any faithful positive unital linear form $\varphi \in C(G)^*$, and setting:*

$$\int_G = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \varphi^{*k}$$

Moreover, for any representation v we have the following formula,

$$\left(id \otimes \int_G \right) v = P$$

where P is the orthogonal projection onto $Fix(v) = \left\{ \xi \in \mathbb{C}^n \middle| v\xi = \xi \right\}$.

PROOF. We can prove this from what we have, in several steps, as follows:

(1) Let us first go back to the general context of Proposition 9.21. Since convolving one more time with φ will not change the Cesàro limit appearing there, the functional $\int_\varphi \in C(G)^*$ constructed there has the following invariance property:

$$\int_\varphi * \varphi = \varphi * \int_\varphi = \int_\varphi$$

In the case where φ is assumed to be faithful, as in Proposition 9.22, our claim is that we have the following formula, valid this time for any $\psi \in C(G)^*$:

$$\int_\varphi * \psi = \psi * \int_\varphi = \psi(1) \int_\varphi$$

Moreover, it is enough to prove this formula on a coefficient of a representation:

$$f = (\tau \otimes id)v$$

(2) In order to do so, consider the following two matrices:

$$P = \left(id \otimes \int_\varphi \right) v \quad , \quad Q = (id \otimes \psi)v$$

We have then the following two computations, involving these matrices:

$$\left(\int_\varphi * \psi \right) f = \left(\tau \otimes \int_\varphi \otimes \psi \right) (v_{12}v_{13}) = \tau(PQ)$$

$$\left(\psi * \int_\varphi \right) f = \left(\tau \otimes \psi \otimes \int_\varphi \right) (v_{12}v_{13}) = \tau(QP)$$

Also, regarding the term on the right in our formula in (1), this is given by:

$$\psi(1) \int_\varphi f = \psi(1)\tau(P)$$

We conclude from all this that our claim is equivalent to the following equality:

$$PQ = QP = \psi(1)P$$

(3) But this latter equality holds indeed, coming from the fact, that we know from Proposition 9.22, that $P = (id \otimes \int_\varphi)v$ equals the orthogonal projection onto $Fix(v)$. Thus, we have proved our claim in (1), namely that the following formula holds:

$$\int_\varphi * \psi = \psi * \int_\varphi = \psi(1) \int_\varphi$$

(4) In order to finish now, it is convenient to introduce the following abstract operation, on the continuous functions $f, f' : C(G) \to \mathbb{C}$ on our group:

$$\Delta(f \otimes f')(g \otimes h) = f(g)f'(h)$$

With this convention, the formula that we established above can be written as:

$$\psi \left(\int_\varphi \otimes id \right) \Delta = \psi \left(id \otimes \int_\varphi \right) \Delta = \psi \int_\varphi (.)1$$

This formula being true for any $\psi \in C(G)^*$, we can simply delete ψ. We conclude that the following invariance formula holds indeed, with $\int_G = \int_\varphi$:

$$\left(\int_G \otimes id \right) \Delta = \left(id \otimes \int_G \right) \Delta = \int_G (.)1$$

But this is exactly the left and right invariance formula we were looking for.

(5) Finally, observe that we can recover the uniqueness as well, because assuming that we have two invariant integrals $\int_G, \int'_G$, we have, according to the invariance formula:

$$\left(\int_G \otimes \int'_G \right) \Delta = \left(\int'_G \otimes \int_G \right) \Delta = \int_G (.)1 = \int'_G (.)1$$

Thus we have $\int_G = \int'_G$, and this finishes the proof. □

Summarizing, we can now integrate over G. As a first application, we have:

THEOREM 9.24. *Given a compact subgroup $G \subset_u U_N$, we have the following formula, valid for any unitary group representation $v : G \to U_M$:*

$$\int_G \chi_v = \dim(Fix(v))$$

In particular, the moments of the main character $\chi = \chi_u$ are given by the formula

$$\int_G \chi^k = \dim(Fix(u^{\otimes k}))$$

so knowing the law of χ is the same as knowing the dimensions on the right.

PROOF. We have three assertions here, the idea being as follows:

(1) Given a unitary representation $v : G \to U_M$ as in the statement, its character χ_v is a coefficient, so we can use the integration formula for coefficients in Theorem 9.23. If we denote by P the projection onto $Fix(v)$, that formula gives, as desired:

$$\int_G \chi_v = Tr(P) = \dim(Im(P)) = \dim(Fix(v))$$

(2) This follows from (1), applied to the Peter-Weyl representations, as follows:

$$\int_G \chi^k = \int_G \chi_u^k = \int_G \chi_{u^{\otimes k}} = \dim(Fix(u^{\otimes k}))$$

(3) This follows from (2), and from the standard fact, which follows from definitions, that a probability measure is uniquely determined by its moments. □

9d. Poisson, revised

In order to discuss now some examples, let us get back to our main examples of finite groups, $\mathbb{Z}_N \subset D_N \subset S_N$. Let us start with the following simple fact:

PROPOSITION 9.25. *For the symmetric group, regarded as group of permutation matrices, $S_N \subset O_N$, the main character counts the number of fixed points:*

$$\chi(g) = \#\left\{i \in \{1, \ldots, N\} \middle| \sigma(i) = i\right\}$$

The same goes for any $G \subset S_N$, regarded as a matrix group via $G \subset S_N \subset O_N$.

PROOF. This is indeed clear from definitions, because the diagonal entries of the permutation matrices correspond to the fixed points of the permutation. □

Summarizing, we are left with counting fixed points. For the simplest possible group, namely the cyclic group $\mathbb{Z}_N \subset S_N$, the computation is as follows:

PROPOSITION 9.26. *The main character of $\mathbb{Z}_N \subset O_N$ is given by:*

$$\chi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ N & \text{if } g = 1 \end{cases}$$

Thus, at the probabilistic level, we have the following formula,

$$law(\chi) = \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\delta_N$$

telling us that the main character χ follows a Bernoulli law.

PROOF. The first formula is clear, because the cyclic permutation matrices have 0 on the diagonal, and so 0 as trace, unless the matrix is the identity, having trace N. As for the second formula, this is a probabilistic reformulation of the first one. □

Moving on, for the dihedral group D_N the computation is more interesting, but still not very exciting, with the final answer being no longer uniform in N, as follows:

PROPOSITION 9.27. *For the dihedral group $D_N \subset S_N$ we have*

$$law(\chi) = \begin{cases} \left(\frac{3}{4} - \frac{1}{2N}\right)\delta_0 + \frac{1}{4}\delta_2 + \frac{1}{2N}\delta_N & (N \text{ even}) \\ \left(\frac{1}{2} - \frac{1}{2N}\right)\delta_0 + \frac{1}{2}\delta_1 + \frac{1}{2N}\delta_N & (N \text{ odd}) \end{cases}$$

with this law being no longer uniform in N.

PROOF. The dihedral group D_N consists indeed of N symmetries, having each 1 fixed point when N is odd, and having 0 or 2 fixed points, distributed $50-50$, when N is even, and then of N rotations, each having 0 fixed points, except for the identity, which has N fixed points. Thus, we are led to the formula in the statement. □

Regarding now the symmetric group S_N itself, the result here is as follows:

THEOREM 9.28. *For the symmetric group $S_N \subset O_N$ we have*

$$\chi \sim p_1$$

in the $N \to \infty$ limit.

PROOF. This is indeed something that we know well from chapter 8, obtained there via inclusion-exclusion, and reformulated by using Proposition 9.25. □

An interesting question now is that of recovering all the Poisson laws p_t, by using group theory. In order to do this, let us formulate the following definition:

DEFINITION 9.29. *Given a closed subgroup $G \subset U_N$, the function*

$$\chi : G \to \mathbb{C} \quad , \quad \chi_t(g) = \sum_{i=1}^{[tN]} g_{ii}$$

is called main truncated character of G, of parameter $t \in (0, 1]$.

As before with the plain characters, there is some general theory behind this definition, and we will discuss this later. Getting back now to the symmetric groups, we have:

PROPOSITION 9.30. *For the symmetric group $S_N \subset O_N$ the coordinate functions are*

$$g_{ij} = \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

and in this picture, the truncated characters count the number of partial fixed points

$$\chi_t(\sigma) = \#\left\{i \in \{1, \ldots, [tN]\} \middle| \sigma(i) = i\right\}$$

with respect to the truncation parameter $t \in (0, 1]$.

PROOF. All this is clear indeed from definitions, with the formula for the coordinates being clear from the definition of the embedding $S_N \subset O_N$. □

Regarding now the asymptotic laws of the truncated characters, we have:

THEOREM 9.31. *For the symmetric group $S_N \subset O_N$ we have*

$$\chi_t \sim p_t$$

in the $N \to \infty$ limit, for any $t \in (0, 1]$.

PROOF. This is indeed something that we know well from chapter 8, obtained there via inclusion-exclusion, and reformulated by using Proposition 9.30. □

Quite nice all this, and worth I guess some more discussion. To start with, we can approach the above character problems directly, by using the following simple fact:

THEOREM 9.32. *Consider the symmetric group S_N, with its standard coordinates:*

$$g_{ij} = \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

The products of these coordinates span the algebra $C(S_N)$, and the arbitrary integrals over S_N are given, modulo linearity, by the formula

$$\int_{S_N} g_{i_1 j_1} \ldots g_{i_k j_k} = \begin{cases} \frac{(N - |\ker i|)!}{N!} & \text{if } \ker i = \ker j \\ 0 & \text{otherwise} \end{cases}$$

where $\ker i$ denotes as usual the partition of $\{1, \ldots, k\}$ whose blocks collect the equal indices of i, and where $|.|$ denotes the number of blocks.

PROOF. The first assertion follows from Stone-Weierstrass, because the standard coordinates g_{ij} separate the points of S_N. Regarding now the second assertion, according to the definition of the coordinates g_{ij}, the integrals in the statement are given by:

$$\int_{S_N} g_{i_1 j_1} \ldots g_{i_k j_k} = \frac{1}{N!} \# \left\{\sigma \in S_N \middle| \sigma(j_1) = i_1, \ldots, \sigma(j_k) = i_k\right\}$$

Now observe that the existence of $\sigma \in S_N$ as above requires:

$$i_m = i_n \iff j_m = j_n$$

Thus, the above integral vanishes when the following condition is satisfied:

$$\ker i \neq \ker j$$

Regarding now the case $\ker i = \ker j$, if we denote by $b \in \{1, \ldots, k\}$ the number of blocks of this partition $\ker i = \ker j$, we have $N - b$ points to be sent bijectively to $N - b$ points, and so $(N - b)!$ solutions, and the integral is $\frac{(N-b)!}{N!}$, as claimed. □

As an illustration for the above formula, we can recover the computation of the asymptotic laws of the truncated characters χ_t. We have indeed:

THEOREM 9.33 (again). *For the symmetric group $S_N \subset O_N$ we have*

$$\chi_t \sim p_t$$

in the $N \to \infty$ limit, for any $t \in (0, 1]$.

PROOF. We use Theorem 9.32. With S_{kb} being the Stirling numbers, counting the partitions of $\{1, \ldots, k\}$ having exactly b blocks, we have the following formula:

$$\begin{aligned}\int_{S_N} \chi_t^k &= \sum_{i_1,\ldots,i_k=1}^{[tN]} \int_{S_N} g_{i_1 i_1} \ldots g_{i_k i_k} \\ &= \sum_{\pi \in P(k)} \frac{[tN]!}{([tN] - |\pi|!)} \cdot \frac{(N - |\pi|!)}{N!} \\ &= \sum_{b=1}^{[tN]} \frac{[tN]!}{([tN] - b)!} \cdot \frac{(N-b)!}{N!} \cdot S_{kb}\end{aligned}$$

In particular with $N \to \infty$ we obtain the following formula:

$$\lim_{N\to\infty} \int_{S_N} \chi_t^k = \sum_{b=1}^{k} S_{kb} t^b$$

But this is the k-th moment of the Poisson law p_t, and so we are done. □

As another result now regarding S_N, here is a useful related formula:

THEOREM 9.34. *We have the law formula*

$$law(g_{11} + \ldots + g_{ss}) = \frac{s!}{N!} \sum_{p=0}^{s} \frac{(N-p)!}{(s-p)!} \cdot \frac{(\delta_1 - \delta_0)^{*p}}{p!}$$

where g_{ij} are the standard coordinates of $S_N \subset O_N$.

PROOF. We have the following moment formula, where m_f is the number of permutations of $\{1, \ldots, N\}$ having exactly f fixed points in the set $\{1, \ldots, s\}$:

$$\int_{S_N} (g_{11} + \ldots + g_{ss})^k = \frac{1}{N!} \sum_{f=0}^{s} m_f f^k$$

Thus the law in the statement, say ν_{sN}, is the following average of Dirac masses:

$$\nu_{sN} = \frac{1}{N!} \sum_{f=0}^{s} m_f \, \delta_f$$

Now observe that the permutations contributing to m_f are obtained by choosing f points in the set $\{1, \ldots, s\}$, then by permuting the remaining $N - f$ points in $\{1, \ldots, n\}$ in such a way that there is no fixed point in $\{1, \ldots, s\}$. But these latter permutations are

counted as follows: we start with all permutations, we substract those having one fixed point, we add those having two fixed points, and so on. We obtain in this way:

$$\begin{aligned}\nu_{sN} &= \frac{1}{N!}\sum_{f=0}^{s}\binom{s}{f}\left(\sum_{k=0}^{s-f}(-1)^k\binom{s-f}{k}(N-f-k)!\right)\delta_f\\ &= \sum_{f=0}^{s}\sum_{k=0}^{s-f}(-1)^k\frac{1}{N!}\cdot\frac{s!}{f!(s-f)!}\cdot\frac{(s-f)!(N-f-k)!}{k!(s-f-k)!}\,\delta_f\\ &= \frac{s!}{N!}\sum_{f=0}^{s}\sum_{k=0}^{s-f}\frac{(-1)^k(N-f-k)!}{f!k!(s-f-k)!}\,\delta_f\end{aligned}$$

We can proceed as follows, by using the new index $p=f+k$:

$$\begin{aligned}\nu_{sN} &= \frac{s!}{N!}\sum_{p=0}^{s}\sum_{k=0}^{p}\frac{(-1)^k(N-p)!}{(p-k)!k!(s-p)!}\,\delta_{p-k}\\ &= \frac{s!}{N!}\sum_{p=0}^{s}\frac{(N-p)!}{(s-p)!p!}\sum_{k=0}^{p}(-1)^k\binom{p}{k}\,\delta_{p-k}\\ &= \frac{s!}{N!}\sum_{p=0}^{s}\frac{(N-p)!}{(s-p)!}\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}\end{aligned}$$

Here $*$ is convolution of real measures, and the assertion follows. □

As an application, we can obtain yet another proof for our main result so far:

THEOREM 9.35. *Let g_{ij} be the standard coordinates of $C(S_N)$.*

(1) *$g_{11}+\ldots+g_{ss}$ with $s=o(N)$ is a projection of trace s/N.*
(2) *$g_{11}+\ldots+g_{ss}$ with $s=tN+o(N)$ is Poisson of parameter t.*

PROOF. We can use indeed the formula in Theorem 9.34, as follows:

(1) With s fixed and $N\to\infty$ we have the following estimate:

$$\begin{aligned}law(g_{11}+\ldots+g_{ss}) &= \sum_{p=0}^{s}\frac{(N-p)!}{N!}\cdot\frac{s!}{(s-p)!}\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}\\ &= \delta_0+\frac{s}{N}(\delta_1-\delta_0)+O(N^{-2})\end{aligned}$$

But the law on the right is that of a projection of trace s/N, as desired.

(2) We have a law formula of the following type:

$$law(g_{11}+\ldots+g_{ss})=\sum_{p=0}^{s}c_p\cdot\frac{(\delta_1-\delta_0)^{*p}}{p!}$$

The coefficients c_p can be estimated by using the Stirling formula, as follows:

$$\begin{aligned} c_p &= \frac{(tN)!}{N!}\cdot\frac{(N-p)!}{(tN-p)!}\\ &\simeq \frac{(tN)^{tN}}{N^N}\cdot\frac{(N-p)^{N-p}}{(tN-p)^{tN-p}}\\ &= \left(\frac{tN}{tN-p}\right)^{tN-p}\left(\frac{N-p}{N}\right)^{N-p}\left(\frac{tN}{N}\right)^{p}\\ &\simeq e^pe^{-p}t^p=t^p \end{aligned}$$

We can now compute the Fourier transform with respect to a variable x:

$$F(x)\simeq\sum_{p=0}^{s}t^p\cdot\frac{(e^{ix}-1)^p}{p!}=e^{t(e^{ix}-1)}$$

But this is the Fourier transform of p_t, and this gives the second assertion. □

9e. Exercises

This was a key algebraic chapter, and as exercises on this, we have:

EXERCISE 9.36. *Read a bit about group actions, and about orders of group elements.*

EXERCISE 9.37. *Learn about abelian groups, and the structure theorem for them.*

EXERCISE 9.38. *How many symmetries does the unit cube in* $3D$ *has?*

EXERCISE 9.39. *Learn more about permutation matrices, and their properties.*

EXERCISE 9.40. *What are the unitary group representations, in the* $1D$ *case?*

EXERCISE 9.41. *Learn about central functions, and their relation with characters.*

EXERCISE 9.42. *Learn about the signature, and the alternating group* $A_N\subset S_N$.

EXERCISE 9.43. *Do the character computations for the alternating group* $A_N\subset S_N$.

As bonus exercise, fully read representation theory, for the finite groups.

CHAPTER 10

Bessel laws

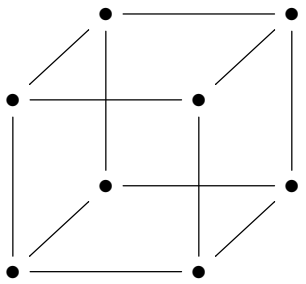
10a. Reflections, Bessel

What is next? More probability I guess, by computing character laws for suitably chosen groups of unitary matrices $G \subset U_N$. Or perhaps by computing character laws for suitably chosen subgroups $G \subset O_N$, for keeping things simple, to start with.

However, we are a bit in trouble here, because, although the results for the permutation group $S_N \subset O_N$ itself were truly remarkable, when looking at other basic groups, such as $\mathbb{Z}_N \subset O_N$, or $D_N \subset O_N$, the results that we had were not very interesting.

Nevermind, and relax. So, forgetting about probability, and going a bit philosophical, what is the most beautiful group $G \subset O_N$ of them all? And in answer here, we have:

DEFINITION 10.1. *The hyperoctahedral group $H_N \subset O_N$ is the group formed by the symmetries of the unit cube in $\mathbb{R}^N$,*



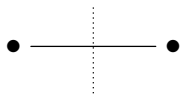
viewed as a graph, or equivalently, as a metric space.

Here the equivalence at the end is clear from definitions, because any symmetry of the cube graph must preserve the lengths of the edges, and so we have:

$$G(\square_{graph}) = G(\square_{metric})$$

The hyperoctahedral group is a quite interesting group, whose definition, as a symmetry group, reminds a bit that of the dihedral group D_N. So, let us start our study in the same way as we did for D_N, with a discussion at small values of $N \in \mathbb{N}$:

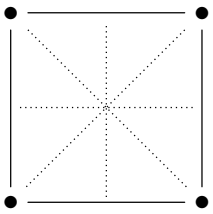
$\underline{N=1}$. Here the 1-cube is the segment, whose symmetries are the identity id, plus the symmetry τ with respect to the middle of the segment:



Thus, we obtain the group with 2 elements, which is a very familiar object:

$$H_1 = D_2 = S_2 = \mathbb{Z}_2$$

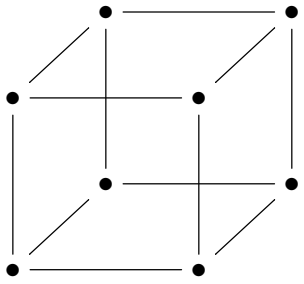
$\underline{N=2}$. Here the 2-cube is the square, whose symmetries are the 4 rotations, of angles $0°, 90°, 180°, 270°$, and the 4 symmetries with respect to the 4 symmetry axes, which are the 2 diagonals, and the 2 segments joining the midpoints of opposite sides:



Thus, we obtain a group with 8 elements, which again is a very familiar object:

$$H_2 = D_4 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$$

$\underline{N=3}$. Here the 3-cube is the usual cube in $\mathbb{R}^3$, pictured as follows:



However, in relation with the symmetries, the situation now is considerably more complicated, because, thinking well, this cube has no less than 48 symmetries. Indeed, if we look at the subgroup $SH_3 \subset H_3$ consisting of the orientation-preserving symmetries, this is the permutation group S_4 of the 4 main diagonals, and then, we have:

$$|H_3| = 2|SH_3| = 2|S_4| = 2 \times 24 = 48$$

Summarizing, all this looks quite complicated. Fortunately we can count H_N, at higher $N \in \mathbb{N}$ as well, by using a geometric trick, the result being as follows:

THEOREM 10.2. *We have the cardinality formula*

$$|H_N| = 2^N N!$$

coming from the fact that H_N is the symmetry group of the coordinate axes of $\mathbb{R}^N$.

PROOF. This follows from some geometric thinking, as follows:

(1) Consider the standard cube in $\mathbb{R}^N$, centered at 0, and having as vertices the points having coordinates ± 1. With this picture in hand, it is clear that the symmetries of the cube coincide with the symmetries of the N coordinate axes of $\mathbb{R}^N$.

(2) In order to count now these latter symmetries, a bit as we did for the dihedral group, observe first that we have $N!$ permutations of these N coordinate axes.

(3) But each of these permutations of the coordinate axes $\sigma \in S_N$ can be further "decorated" by a sign vector $e \in \{\pm 1\}^N$, consisting of the possible ± 1 flips which can be applied to each coordinate axis, at the arrival.

(4) And the point is that, obviously, we obtain in this way all the elements of H_N. Thus, we have the following formula, for the cardinality of H_N:

$$|H_N| = |S_N| \cdot |\mathbb{Z}_2^N| = N! \cdot 2^N$$

Thus, we are led to the conclusions in the statement. □

As before in the dihedral group case, it is possible to go beyond this, with a crossed product decomposition of H_N, of quite special type, called wreath product decomposition. To be more precise, further building on Theorem 10.2 leads to the following result:

THEOREM 10.3. *We have a wreath product decomposition as follows,*

$$H_N = \mathbb{Z}_2 \wr S_N$$

which means by definition that we have a crossed product decomposition

$$H_N = \mathbb{Z}_2^N \rtimes S_N$$

with the permutations $\sigma \in S_N$ acting on the elements $e \in \mathbb{Z}_2^N$ as follows:

$$\sigma(e_1, \ldots, e_k) = (e_{\sigma(1)}, \ldots, e_{\sigma(k)})$$

In particular we have, as found before, the cardinality formula $|H_N| = 2^N N!$.

PROOF. As explained in the proof of Theorem 10.2, the elements of H_N can be identified with the pairs $g = (e, \sigma)$ consisting of a permutation $\sigma \in S_N$, and a sign vector $e \in \mathbb{Z}_2^N$, so that at the level of the cardinalities, we have the following formula:

$$|H_N| = |\mathbb{Z}_2^N \times S_N|$$

To be more precise, given an element $g \in H_N$, the element $\sigma \in S_N$ is the corresponding permutation of the N coordinate axes, regarded as unoriented lines in $\mathbb{R}^N$, and $e \in \mathbb{Z}_2^N$ is the vector collecting the possible flips of these coordinate axes, at the arrival. Now

observe that the product formula for two such pairs $g = (e, \sigma)$ is as follows, with the permutations $\sigma \in S_N$ acting on the elements $f \in \mathbb{Z}_2^N$ as in the statement:

$$(e, \sigma)(f, \tau) = (ef^\sigma, \sigma\tau)$$

Thus, we are in the framework of the crossed products, as constructed in chapter 9, and we conclude that we have a crossed product decomposition, as follows:

$$H_N = \mathbb{Z}_2^N \rtimes S_N$$

Thus, we are led to the conclusion in the statement, with the formula $H_N = \mathbb{Z}_2 \wr S_N$ being just a shorthand for the decomposition $H_N = \mathbb{Z}_2^N \rtimes S_N$ that we found. □

Getting now to probability, we can compute the character laws by using the same method as for the symmetric group S_N, namely inclusion-exclusion, and we have:

THEOREM 10.4. *For the hyperoctahedral group $H_N \subset O_N$, the law of the variable*

$$\chi_t = \sum_{i=1}^{[tN]} u_{ii}$$

with u_{ij} being the standard coordinates, becomes in the $N \to \infty$ limit the measure

$$b_t^2 = e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \sum_{p=0}^{\infty} \frac{(t/2)^{|k|+2p}}{(|k|+p)!p!}$$

where δ_k is the Dirac mass at $k \in \mathbb{Z}$.

PROOF. We can regard the group H_N as being the symmetry group of the graph $I_N = \{I^1, \ldots, I^N\}$ formed by N segments. The diagonal coefficients are given by:

$$u_{ii}(g) = \begin{cases} 0 & \text{if } g \text{ moves } I^i \\ 1 & \text{if } g \text{ fixes } I^i \\ -1 & \text{if } g \text{ returns } I^i \end{cases}$$

We denote by $\uparrow g, \downarrow g$ the number of segments among $\{I^1, \ldots, I^s\}$ which are fixed, respectively returned by an element $g \in H_N$. With this notation, we have:

$$u_{11} + \ldots + u_{ss} = \uparrow g - \downarrow g$$

Let us denote by P_N probabilities computed over the group H_N. The density of the law of $u_{11} + \ldots + u_{ss}$ at a point $k \geq 0$ is then given by the following formula:

$$\begin{aligned} D(k) &= P_N(\uparrow g - \downarrow g = k) \\ &= \sum_{p=0}^{\infty} P_N(\uparrow g = k + p, \downarrow g = p) \end{aligned}$$

Assume first that we have $t = 1$. We use the fact, that we know well from chapter 4, that the probability of $\sigma \in S_N$ to have no fixed points is asymptotically given by:

$$P_0 = \frac{1}{e}$$

Thus the probability of $\sigma \in S_N$ to have m fixed points is asymptotically given by:

$$P_m = \frac{1}{em!}$$

In terms of probabilities over H_N, we obtain from this, as desired:

$$\begin{aligned}
\lim_{N\to\infty} D(k) &= \lim_{N\to\infty} \sum_{p=0}^{\infty} (1/2)^{k+2p} \binom{k+2p}{k+p} P_N(\uparrow g + \downarrow g = k+2p) \\
&= \sum_{p=0}^{\infty} (1/2)^{k+2p} \binom{k+2p}{k+p} \frac{1}{e(k+2p)!} \\
&= \frac{1}{e} \sum_{p=0}^{\infty} \frac{(1/2)^{k+2p}}{(k+p)!p!}
\end{aligned}$$

As for the general case $0 < t \leq 1$, here the result follows by performing some modifications in the above computation. The asymptotic density is computed as follows:

$$\begin{aligned}
\lim_{N\to\infty} D(k) &= \lim_{N\to\infty} \sum_{p=0}^{\infty} (1/2)^{k+2p} \binom{k+2p}{k+p} P_N(\uparrow g + \downarrow g = k+2p) \\
&= \sum_{p=0}^{\infty} (1/2)^{k+2p} \binom{k+2p}{k+p} \frac{t^{k+2p}}{e^t(k+2p)!} \\
&= e^{-t} \sum_{p=0}^{\infty} \frac{(t/2)^{k+2p}}{(k+p)!p!}
\end{aligned}$$

Together with $D(-k) = D(k)$, this gives the formula in the statement. □

The above result is quite interesting, and based on it, we can formulate:

DEFINITION 10.5. *The Bessel law of parameter $t > 0$ is the measure*

$$b_t^2 = e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \, f_k(t/2)$$

with the density being the following function, depending on $k \in \mathbb{Z}$,

$$f_k(t) = \sum_{p=0}^{\infty} \frac{t^{|k|+2p}}{(|k|+p)!p!}$$

which is the Bessel function of the first kind, from classical analysis.

Let us study now these Bessel laws that we found. In analogy with what we know about the Poisson laws p_t, from chapter 8, we first have the following result:

THEOREM 10.6. *The Bessel laws b_t^2 have the property*

$$b_s^2 * b_t^2 = b_{s+t}^2$$

so they form a truncated one-parameter semigroup with respect to convolution.

PROOF. We use the formula in Definition 10.5, namely:

$$b_t^2 = e^{-t} \sum_{k=-\infty}^{\infty} \delta_k \, f_k(t/2)$$

The Fourier transform of this measure is then given by:

$$F(x) = e^{-t} \sum_{k=-\infty}^{\infty} e^{ikx} \, f_k(t/2)$$

We can compute the derivative of F with respect to t, as follows:

$$\begin{aligned} F(x)' &= -e^{-t} \sum_{k=-\infty}^{\infty} e^{ikx} \, f_k(t/2) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{ikx} \, f_k'(t/2) \\ &= -F(x) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{ikx} \, f_k'(t/2) \end{aligned}$$

On the other hand, the derivative of f_k with $k \geq 1$ is given by:

$$\begin{aligned} f_k'(t) &= \sum_{p=0}^{\infty} \frac{(k+2p)t^{k+2p-1}}{(k+p)!p!} \\ &= \sum_{p=0}^{\infty} \frac{(k+p)t^{k+2p-1}}{(k+p)!p!} + \sum_{p=0}^{\infty} \frac{p\, t^{k+2p-1}}{(k+p)!p!} \\ &= \sum_{p=0}^{\infty} \frac{t^{k+2p-1}}{(k+p-1)!p!} + \sum_{p=1}^{\infty} \frac{t^{k+2p-1}}{(k+p)!(p-1)!} \\ &= \sum_{p=0}^{\infty} \frac{t^{(k-1)+2p}}{((k-1)+p)!p!} + \sum_{p=1}^{\infty} \frac{t^{(k+1)+2(p-1)}}{((k+1)+(p-1))!(p-1)!} \\ &= f_{k-1}(t) + f_{k+1}(t) \end{aligned}$$

This computation works in fact for any $k \in \mathbb{Z}$, so we get:

$$\begin{aligned} F(x)' &= -F(x) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{ikx}(f_{k-1}(t/2) + f_{k+1}(t/2)) \\ &= -F(x) + \frac{e^{-t}}{2} \sum_{k=-\infty}^{\infty} e^{i(k+1)x} f_k(t/2) + e^{i(k-1)x} f_k(t/2) \\ &= -F(x) + \frac{e^{ix} + e^{-ix}}{2} F(x) \\ &= \left(\frac{e^{ix} + e^{-ix}}{2} - 1 \right) F(x) \end{aligned}$$

Thus, the Fourier transform is subject to the following equation:

$$\frac{F(x)'}{F(x)} = \frac{e^{ix} + e^{-ix}}{2} - 1$$

Now by integrating, it follows that the Fourier transform is given by:

$$F(x) = \exp\left(\left(\frac{e^{ix} + e^{-ix}}{2} - 1 \right) t \right)$$

Thus the log of the Fourier transform is linear in t, and we get the result. □

As a conclusion to what we have so far, the Bessel laws b_t^2, appearing from the hyperoctahedral group $H_N \subset O_N$, are a bit similar to the Poisson laws p_t, appearing from the symmetric group $S_N \subset O_N$. We will further build on this analogy, in what follows.

10b. Compound Poisson

In order to further study the Bessel laws that we found, we will need a number of probabilistic preliminaries. We recall from chapter 8 that, conceptually speaking, the Poisson laws are the laws appearing via the Poisson Limit Theorem (PLT).

In order to generalize this construction of the Poisson laws, via the PLT, as to cover the Bessel laws that we found above, in connection with the hyperoctahedral group H_N, we have the following notion, extending the Poisson limit theory from chapter 8:

DEFINITION 10.7. *Associated to any compactly supported positive measure ν on $\mathbb{C}$ is the probability measure*

$$p_\nu = \lim_{n\to\infty} \left(\left(1 - \frac{c}{n} \right) \delta_0 + \frac{1}{n} \nu \right)^{*n}$$

where $c = mass(\nu)$, called compound Poisson law.

In other words, what we are doing here is to generalize the construction in the Poisson Limit Theorem, by allowing the only parameter there, which was the positive real number $t > 0$, to be replaced by a certain probability measure ν, of arbitrary mass $c > 0$.

In what follows we will be mostly interested in the case where ν is discrete, as is for instance the case for the measure $\nu = t\delta_1$ with $t > 0$, which produces the Poisson laws. To be more precise, the Poisson limit theorem from chapter 8 reformulates as:

THEOREM 10.8 (PLT). *The Poisson laws p_t are compound Poisson laws,*

$$p_t = p_{t\varepsilon}$$

with $\varepsilon = \delta_1$, Dirac mass at 1.

PROOF. We recall from chapter 8 that the PLT states that we have:

$$\lim_{n\to\infty} \left(\left(1 - \frac{t}{n} \right) \delta_0 + \frac{t}{n} \, \delta_1 \right)^{*n} = p_t$$

Thus, we are led to the conclusion in the statement. □

Getting back now to our comments on Definition 10.7, as stated, as mentioned in the above, we will be mostly interested here in the case where the measure ν is discrete. In fact, we will be mainly interested in the case where ν is a multiple of the uniform measure on the s-th roots of unity. But more on this later, once we will be more advanced.

Finally, as a last comment on Definition 10.7, we allow there the measure ν to be complex, instead of being real, and this precisely in order to have as examples, later, the multiples of the uniform measures on the s-th roots of unity. But, more on this later.

Getting now to some theory, for the compound Poisson laws as introduced in Definition 10.7, we first have the following result, allowing us to detect such laws:

PROPOSITION 10.9. *For a discrete measure, $\nu = \sum_{i=1}^{s} c_i \delta_{z_i}$ with $c_i > 0$ and $z_i \in \mathbb{C}$, we have the formula*

$$F_{p_\nu}(x) = \exp\left(\sum_{i=1}^{s} c_i (e^{ixz_i} - 1) \right)$$

where F denotes as usual the Fourier transform.

PROOF. In order to prove the formula in the statement, consider the measure μ_n appearing in Definition 10.7, under the convolution sign, namely:

$$\mu_n = \left(1 - \frac{c}{n} \right) \delta_0 + \frac{1}{n} \nu$$

We have the following computation, in the context of Definition 10.7:

$$F_{\mu_n}(x) = \left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^{s} c_i e^{ixz_i}$$

$$\implies \quad F_{\mu_n^{*n}}(x) = \left(\left(1 - \frac{c}{n}\right) + \frac{1}{n}\sum_{i=1}^{s} c_i e^{ixz_i}\right)^n$$

$$\implies \quad F_{p_\nu}(x) = \exp\left(\sum_{i=1}^{s} c_i(e^{ixz_i} - 1)\right)$$

Thus, we have obtained the formula in the statement. □

Next, we have the following key result, providing an alternative to Definition 10.7, and which will be our formulation here of the Compound Poisson Limit Theorem:

THEOREM 10.10 (CPLT). *For a discrete measure, $\nu = \sum_{i=1}^{s} c_i\delta_{z_i}$ with $c_i > 0$ and $z_i \in \mathbb{C}$, we have the following formula,*

$$p_\nu = \text{law}\left(\sum_{i=1}^{s} z_i\alpha_i\right)$$

with the variables α_i being Poisson (c_i), and independent.

PROOF. Let α be the sum of Poisson variables in the statement:

$$\alpha = \sum_{i=1}^{s} z_i\alpha_i$$

By using the Fourier transform formulae from chapter 8, we have:

$$F_{\alpha_i}(x) = \exp(c_i(e^{ix} - 1)) \quad \implies \quad F_{z_i\alpha_i}(x) = \exp(c_i(e^{ixz_i} - 1))$$

$$\implies \quad F_\alpha(x) = \exp\left(\sum_{i=1}^{s} c_i(e^{ixz_i} - 1)\right)$$

Thus we have the same formula as in Proposition 10.9, as desired. □

Getting back now to the Bessel laws, we have the following result:

THEOREM 10.11. *The Bessel laws b_t^2 are compound Poisson laws, given by*

$$b_t^2 = p_{t\varepsilon}$$

where $\varepsilon = \frac{1}{2}(\delta_{-1} + \delta_1)$ is the uniform measure on $\mathbb{Z}_2$.

PROOF. We recall from the proof of Theorem 10.6 that the Fourier transform of the Bessel law b_t^2, with respect to a variable x, is given by the following formula:

$$F(x) = \exp\left(\left(\frac{e^{ix}+e^{-ix}}{2}-1\right)t\right)$$

But, according to Proposition 10.9, this is exactly the Fourier transform of the compound Poisson law $p_{t\varepsilon}$ in the statement. Thus, we have $b_t^2 = p_{t\varepsilon}$, as claimed. □

As a conclusion to all this, when discussing the character laws for the basic finite subgroups $G \subset U_N$, such as $G = S_N, H_N$, it is all about compound Poisson laws.

10c. Complex Bessel

Our next task will be that of unifying and generalizing the results that we have for S_N, H_N. For this purpose, consider the following family of unitary groups:

DEFINITION 10.12. *The complex reflection group $H_N^s \subset U_N$, depending on parameters*

$$N \in \mathbb{N} \quad , \quad s \in \mathbb{N} \cup \{\infty\}$$

are the groups of permutation-type matrices with s-th roots of unity as entries,

$$H_N^s = M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N$$

with the convention $\mathbb{Z}_\infty = \mathbb{T}$, at $s = \infty$.

Observe that at $s = 1, 2$ we obtain the symmetric and hyperoctahedral groups:

$$H_N^1 = S_N \quad , \quad H_N^2 = H_N$$

Another important particular case is $s = \infty$, where we obtain a compact group which is actually not finite, but is of key importance, that we will denote as follows:

$$H_N^\infty = K_N$$

This latter group K_N is called full complex reflection group, and will appear many times, in what follows. In view of this, let us highlight its definition, as follows:

DEFINITION 10.13. *The full complex reflection group is given by:*

$$K_N = M_N(\mathbb{T} \cup \{0\}) \cap U_N$$

That is, K_N is the group of permutation-type matrices with entries from $\mathbb{T}$.

This group K_N seems to be a quite interesting object, with its precise potential remaining to be determined. So, let us first have a look at it at small values of N:

$\underline{N = 1}$. What we have is the unit circle, $K_1 = \mathbb{T}$.

$\underline{N = 2}$. Here K_2 consists of the matrices as follows, with nonzero entries in $\mathbb{T}$:

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}$$

$\underline{N=3}$. Here K_3 consists of the matrices as follows, with nonzero entries in $\mathbb{T}$:

$$\begin{pmatrix} x & 0 & 0\\ 0 & y & 0\\ 0 & 0 & z \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & x & 0\\ y & 0 & 0\\ 0 & 0 & z \end{pmatrix} \quad , \quad \begin{pmatrix} x & 0 & 0\\ 0 & 0 & y\\ 0 & z & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & x\\ 0 & y & 0\\ z & 0 & 0 \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & 0 & x\\ y & 0 & 0\\ 0 & z & 0 \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & x & 0\\ 0 & 0 & y\\ z & 0 & 0 \end{pmatrix}$$

$\underline{N\geq 4}$. And so on, you get the point, what we have is a bit like before for H_N, permutation matrices, but this time decorated by numbers in $\mathbb{T}$.

Generally speaking, K_N contains all the interesting finite groups $G\subset U_N$ that we know, including S_N, H_N, and more generally the groups H_N^s from Definition 10.12. Quite remarkably, the dihedral group D_N can be viewed as well as a subgroup, as follows:

THEOREM 10.14. *We have an embedding $D_N\subset K_2$, coming as follows,*

$$D_N=\left\{\begin{pmatrix} x & 0\\ 0 & y \end{pmatrix}\ ,\ \begin{pmatrix} 0 & x\\ y & 0 \end{pmatrix}\Big|x=y^{-1}\in\mathbb{Z}_N\right\}\subset K_2$$

obtained by augmenting the standard copy $\mathbb{Z}_N\subset K_2$ with a twisted copy of it.

PROOF. The matrices patterned as in the statement form indeed a group, and when adding the extra condition $xy=1$, this remains a group. In order now to establish the isomorphism with D_N, let us label our group elements as follows, with $xy=zt=1$:

$$R_x=\begin{pmatrix} x & 0\\ 0 & y \end{pmatrix} \quad , \quad S_z=\begin{pmatrix} 0 & z\\ t & 0 \end{pmatrix}$$

We have then the following computations, for the products of these elements:

$$R_xR_z=\begin{pmatrix} x & 0\\ 0 & y \end{pmatrix}\begin{pmatrix} z & 0\\ 0 & t \end{pmatrix}=\begin{pmatrix} xz & 0\\ 0 & yt \end{pmatrix}=R_{xz}$$

$$R_xS_z=\begin{pmatrix} x & 0\\ 0 & y \end{pmatrix}\begin{pmatrix} 0 & z\\ t & 0 \end{pmatrix}=\begin{pmatrix} 0 & xz\\ yt & 0 \end{pmatrix}=S_{xz}$$

$$S_xR_z=\begin{pmatrix} 0 & x\\ y & 0 \end{pmatrix}\begin{pmatrix} z & 0\\ 0 & t \end{pmatrix}=\begin{pmatrix} 0 & xt\\ yz & 0 \end{pmatrix}=S_{xz^{-1}}$$

$$S_xS_z=\begin{pmatrix} 0 & x\\ y & 0 \end{pmatrix}\begin{pmatrix} 0 & z\\ t & 0 \end{pmatrix}=\begin{pmatrix} xt & 0\\ 0 & yz \end{pmatrix}=R_{xz^{-1}}$$

But, we recognize here the table of multiplication of D_N, as desired. □

Summarizing, good idea to pass to complex numbers, and the complex reflection groups $H_N^s \subset U_N$ from Definition 10.12, with special attention to the group $H_N^\infty = K_N$ from Definition 10.13, which contains them all, will be our new objects of interest.

Let us start our study by summarizing some basic observations, as follows:

PROPOSITION 10.15. *The complex reflection groups $H_N^s \subset U_N$ are as follows:*

(1) *At $s = 1$ we have $H_N^1 = S_N$, having cardinality $|S_N| = N!$.*
(2) *At $s = 2$ we have $H_N^2 = H_N$, having cardinality $|H_N| = 2^N N!$.*
(3) *At $s = \infty$ we have $H_N^\infty = K_N$, having cardinality $|K_N| = \infty$.*

PROOF. This is clear indeed from the discussion made after Definition 10.12, and with the cardinality results at $s = 1$ and $s = 2$ being something that we know well. □

Let us record as well the following result, which is something elementary too:

PROPOSITION 10.16. *We have inclusions as follows, for any $r, s \in \mathbb{N} \cup \{\infty\}$:*

$$r|s \implies H_r \subset H_s$$

In particular, we have inclusions $S_N \subset H_N^s \subset K_N$, for any $s \in \mathbb{N} \cup \{\infty\}$.

PROOF. With the cyclic group $\mathbb{Z}_s$ being viewed as usual, as being the group of the s-th roots of unity in the complex plane, we have inclusions as follows:

$$r|s \implies \mathbb{Z}_r \subset \mathbb{Z}_s$$

Thus, with the group H_N^s constructed as in Definition 10.12, for $r|s$ we have:

$$\begin{aligned} H_N^r &= M_N(\mathbb{Z}_r \cup \{0\}) \cap U_N \\ &\subset M_N(\mathbb{Z}_s \cup \{0\}) \cap U_N \\ &= H_N^s \end{aligned}$$

Finally, the last assertion is clear, and comes also from this, via $1|s|\infty$, for any s. □

Coming next, in analogy with what we know about S_N, H_N, we first have:

PROPOSITION 10.17. *The number of elements of H_N^s with $s \in \mathbb{N}$ is:*

$$|H_N^s| = s^N N!$$

At $s = \infty$, the group $K_N = H_N^\infty$ that we obtain is infinite.

PROOF. This is indeed clear from our definition of H_N^s, as a matrix group, because there are $N!$ choices for a permutation-type matrix, and then s^N choices for the corresponding s-roots of unity, which must decorate the N nonzero entries. □

Once again in analogy with what we know at $s = 1, 2$, we have as well:

THEOREM 10.18. *We have a wreath product decomposition*

$$H_N^s = \mathbb{Z}_s^N \rtimes S_N = \mathbb{Z}_s \wr S_N$$

with the permutations $\sigma \in S_N$ acting on the elements $e \in \mathbb{Z}_s^N$ as follows:

$$\sigma(e_1, \ldots, e_N) = (e_{\sigma(1)}, \ldots, e_{\sigma(N)})$$

In particular we have, as found before, the cardinality formula $|H_N^s| = s^N N!$.

PROOF. As explained in the proof of Proposition 10.17, the elements of H_N^s can be identified with the pairs $g = (e, \sigma)$ consisting of a permutation $\sigma \in S_N$, and a decorating vector $e \in \mathbb{Z}_s^N$, so that at the level of the cardinalities, we have:

$$|H_N| = |\mathbb{Z}_s^N \times S_N|$$

Now observe that the product formula for two such pairs $g = (e, \sigma)$ is as follows, with the permutations $\sigma \in S_N$ acting on the elements $f \in \mathbb{Z}_s^N$ as in the statement:

$$(e, \sigma)(f, \tau) = (ef^\sigma, \sigma\tau)$$

Thus, we are in the framework of the crossed products, and we obtain $H_N^s = \mathbb{Z}_s^N \rtimes S_N$. But this can be written, by definition, as $H_N^s = \mathbb{Z}_s \wr S_N$, and we are done. □

Finally, in relation with geometric aspects, the above groups appear as follows:

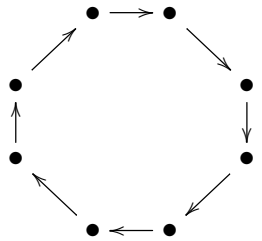
THEOREM 10.19. *The complex reflection group H_N^s appears as a symmetry group,*

$$H_N^s = G(C_s \ldots C_s)$$

with $C_s \ldots C_s$ consisting of N disjoint copies of the oriented cycle C_s.

PROOF. This is something elementary, the idea being as follows:

(1) Consider first the oriented cycle C_s, which looks as follows:



It is then clear that the symmetry group of this graph is the cyclic group $\mathbb{Z}_s$.

(2) In the general case now, where we have $N \in \mathbb{N}$ disjoint copies of the above cycle C_s, we must suitably combine the corresponding N copies of the cyclic group $\mathbb{Z}_s$. But this leads to the wreath product group $H_N^s = \mathbb{Z}_s \wr S_N$, as stated. □

Moving on, the story with the complex reflection groups is not over with the groups H_N^s constructed in Definition 10.12, because we can do more generally, as follows:

THEOREM 10.20. *We have subgroups of the basic complex reflection groups,*

$$H_N^{sd}=\left\{U\in H_N^s\Big|(\square U)^d=1\right\}$$

with $\square$ being the product of nonzero entries, covering all examples of reflection groups.

PROOF. This is something very standard, the idea as follows:

(1) To start with, with $\square$ being as above, we have a group morphism as follows:

$$\square:H_N^s\to\mathbb{Z}_s$$

Thus, for any $d|s$, we can define a subgroup $H_N^{sd}\subset H_N^s$ as in the statement.

(2) At the level of basic examples now, we certainly have the groups $H_N^s=H_N^{ss}$. Also, recall from Theorem 10.14 that we have an identification as follows:

$$D_N=\left\{\begin{pmatrix}x&0\\0&y\end{pmatrix}\ ,\ \begin{pmatrix}0&x\\y&0\end{pmatrix}\Big|x=y^{-1}\in\mathbb{Z}_N\right\}\subset K_2$$

But this translates into $D_N=H_2^{N1}$, so the dihedral group D_N is covered too. □

As a conclusion to all this, good work that we did, and we will stop here with our construction of complex reflection groups, due to a famous classification result of Shephard and Todd, that we would like to explain now. To start with, we can talk about complex reflections and about complex reflection groups abstractly, as follows:

DEFINITION 10.21. *We can talk about reflections and reflection groups, as follows:*

(1) *A reflection is a symmetry $S\in U_N$ with respect to a hyperplane $P\subset\mathbb{C}^N$.*
(2) *A reflection group is a group $G\subset U_N$ generated by reflections, $G=<S_i>$.*
(3) *Such a reflection group is called irreducible when it has no invariant subspaces.*

Observe that we have not assumed G to be finite, in the above, and with this making the above formalism quite broad, for instance with many continuous groups $G\subset U_N$ being reflection groups, in the above sense. Still in this setting, with no finiteness assumption on G, these reflection groups are best investigated by writing them as follows:

$$G=\left\langle S_1,\ldots,S_n\Big|(S_iS_j)^{m_{ij}}=1\right\rangle$$

And there has been a lot of work here, by Coxeter and others. Getting now to the finite group case, any reflection group appears as product of irreducible reflection groups, and in what regards these latter groups, we have the following classification result:

THEOREM 10.22. *The irreducible complex reflection groups are*

$$H_N^{sd}=\left\{U\in H_N^s\Big|(\square U)^d=1\right\}$$

along with 34 *exceptional examples.*

PROOF. This is something quite advanced, that we will not attempt to prove here, or even explain in detail, with the list of 34 exceptional cases, and we refer here to the paper of Shephard and Todd, and to the subsequent literature on the subject. □

Back now to probability, in order to do the character computations for H_N^s, and why not for H_N^{sd} too, we will need a number of further preliminaries. Let us start with:

DEFINITION 10.23. *The Bessel law of level $s \in \mathbb{N} \cup \{\infty\}$ and parameter $t > 0$ is*

$$b_t^s = p_{t\varepsilon_s}$$

with ε_s being the uniform measure on the s-th roots of unity.

Observe that at $s = 1, 2$ we obtain the Poisson and real Bessel laws:

$$b_t^1 = p_t \quad , \quad b_t^2 = b_t^2$$

Another important particular case is $s = \infty$, where we obtain a measure which is actually not discrete, that we will denote as follows:

$$b_t^\infty = B_t$$

Let us develop now some more theory for these Bessel laws. According to our various results above, the Bessel laws appear in practice as follows:

THEOREM 10.24. *The Bessel laws are given by the formula*

$$b_t^s = \text{law}\left(\sum_{k=1}^{s} w^k a_k\right)$$

with $a_1, \ldots, a_s$ being Poisson (t/s) and independent, and $w = e^{2\pi i/s}$.

PROOF. This comes indeed from our general formula from Theorem 10.10. □

We will need in our computations the level s exponential function, given by:

$$\exp_s z = \sum_{k=0}^{\infty} \frac{z^{sk}}{(sk)!}$$

We have the following formula, in terms of root of unity $w = e^{2\pi i/s}$:

$$\exp_s z = \frac{1}{s} \sum_{k=1}^{s} \exp(w^k z)$$

Observe also that at $s = 1, 2$ we have the following formulae:

$$\exp_1 = \exp \quad , \quad \exp_2 = \cosh$$

We have the following result, regarding the Fourier transform of the Bessel laws:

THEOREM 10.25. *The Fourier transform of b_t^s is given by*

$$\log F_t^s(z) = t\left(\exp_s z - 1\right)$$

so in particular the measures b_t^s are additive with respect to t.

PROOF. Consider, as in Theorem 10.24, the following variable:

$$a = \sum_{k=1}^{s} w^k a_k$$

We have the following computation, for the corresponding Fourier transform:

$$\begin{aligned}\log F_a(z) &= \sum_{k=1}^{s} \log F_{a_k}(w^k z)\\ &= \sum_{k=1}^{s} \frac{t}{s}\left(\exp(w^k z) - 1\right)\end{aligned}$$

But this gives the following formula, in terms of the above function $\exp_s$:

$$\begin{aligned}\log F_a(z) &= t\left(\left(\frac{1}{s}\sum_{k=1}^{s}\exp(w^k z)\right) - 1\right)\\ &= t\left(\exp_s z - 1\right)\end{aligned}$$

Now since b_t^s is the law of a, this gives the formula in the statement. □

We can go back now to the reflection groups, and we have the following result:

THEOREM 10.26. *For the complex reflection group*

$$H_N^s = \mathbb{Z}_s \wr S_N$$

we have, with $N \to \infty$, the main character law estimate

$$\chi_t \sim b_t^s$$

where $b_t^s = p_{t\varepsilon_s}$, with ε_s being the uniform measure on the s-th roots of unity.

PROOF. The best is to proceed in two steps, as follows:

(1) Let us first work out the case $t = 1$. Since the limit probability for a random permutation to have exactly k fixed points is $e^{-1}/k!$, we get:

$$\lim_{N\to\infty} law(\chi_1) = e^{-1}\sum_{k=0}^{\infty}\frac{1}{k!}\,\varepsilon_s^{*k}$$

On the other hand, we get from the definition of the Bessel law b_1^s:

$$\begin{aligned} b_1^s &= \lim_{N\to\infty}\left(\left(1-\frac{1}{N}\right)\delta_0+\frac{1}{N}\,\varepsilon_s\right)^{*N}\\ &= \lim_{N\to\infty}\sum_{k=0}^{N}\binom{N}{k}\left(1-\frac{1}{N}\right)^{N-k}\frac{1}{N^k}\,\varepsilon_s^{*k}\\ &= e^{-1}\sum_{k=0}^{\infty}\frac{1}{k!}\,\varepsilon_s^{*k} \end{aligned}$$

But this gives the assertion for $t=1$, as desired.

(2) Now in the case where $t>0$ is arbitrary, we can use the same method, by performing the following modifications to the above computation:

$$\begin{aligned} \lim_{N\to\infty} law(\chi_t) &= e^{-t}\sum_{k=0}^{\infty}\frac{t^k}{k!}\,\varepsilon_s^{*k}\\ &= \lim_{N\to\infty}\left(\left(1-\frac{1}{N}\right)\delta_0+\frac{1}{N}\,\varepsilon_s\right)^{*[tN]}\\ &= b_t^s \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Summarizing, we have unified and generalized our previous results for S_N, H_N, with Theorem 10.26, regarding the complex reflection groups $H_N^s\subset U_N$, being our new main result. We should mention that for the subgroups $H_N^{sd}\subset H_N^s$ from Theorem 10.20 the asymptotic laws of characters do not depend on d, so no need for more, and Theorem 10.26 is therefore something final. Which is quite remarkable, and good to know.

10d. Density, moments

We would like to develop now some more theory for the Bessel laws b_t^s that we found above. In what regards the density of b_t^s, we have here the following result:

THEOREM 10.27. *We have the formula*

$$b_t^s=e^{-t}\sum_{p_1=0}^{\infty}\cdots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\delta\left(\sum_{k=1}^{s}w^kp_k\right)$$

where $w=e^{2\pi i/s}$, and the δ symbol is a Dirac mass.

PROOF. In order to prove the result, we compute the Fourier transform of the measure on the right. This is given by the following formula:

$$\begin{aligned}
F(z) &= e^{-t}\sum_{p_1=0}^{\infty}\ldots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}F\delta\left(\sum_{k=1}^{s}w^kp_k\right)(z)\\
&= e^{-t}\sum_{p_1=0}^{\infty}\ldots\sum_{p_s=0}^{\infty}\frac{1}{p_1!\ldots p_s!}\left(\frac{t}{s}\right)^{p_1+\ldots+p_s}\exp\left(\sum_{k=1}^{s}w^kp_kz\right)\\
&= e^{-t}\sum_{r=0}^{\infty}\left(\frac{t}{s}\right)^r\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^{s}w^kp_kz\right)}{p_1!\ldots p_s!}
\end{aligned}$$

We multiply by e^t, and we compute the derivative with respect to t:

$$\begin{aligned}
(e^tF(z))' &= \sum_{r=1}^{\infty}\frac{r}{s}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\frac{\exp\left(\sum_{k=1}^{s}w^kp_kz\right)}{p_1!\ldots p_s!}\\
&= \frac{1}{s}\sum_{r=1}^{\infty}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\left(\sum_{l=1}^{s}p_l\right)\frac{\exp\left(\sum_{k=1}^{s}w^kp_kz\right)}{p_1!\ldots p_s!}\\
&= \frac{1}{s}\sum_{r=1}^{\infty}\left(\frac{t}{s}\right)^{r-1}\sum_{\Sigma p_i=r}\sum_{l=1}^{s}\frac{\exp\left(\sum_{k=1}^{s}w^kp_kz\right)}{p_1!\ldots p_{l-1}!(p_l-1)!p_{l+1}!\ldots p_s!}
\end{aligned}$$

By using the variable $u=r-1$, we get:

$$\begin{aligned}
(e^tF(z))' &= \frac{1}{s}\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^u\sum_{\Sigma q_i=u}\sum_{l=1}^{s}\frac{\exp\left(w^lz+\sum_{k=1}^{s}w^kq_kz\right)}{q_1!\ldots q_s!}\\
&= \left(\frac{1}{s}\sum_{l=1}^{s}\exp(w^lz)\right)\left(\sum_{u=0}^{\infty}\left(\frac{t}{s}\right)^u\sum_{\Sigma q_i=u}\frac{\exp\left(\sum_{k=1}^{s}w^kq_kz\right)}{q_1!\ldots q_s!}\right)\\
&= (\exp_s z)(e^tF(z))
\end{aligned}$$

On the other hand, consider the following function:

$$\Phi(t)=\exp(t\exp_s z)$$

This function satisfies as well the equation found above, namely:

$$\Phi'(t)=(\exp_s z)\Phi(t)$$

We conclude from this that we have the following equality of functions:

$$e^tF(z)=\Phi(t)$$

But this gives the following formula, for the logarithm of the Fourier transform:

$$\begin{aligned}\log F &= \log(e^{-t}\exp(t\exp_s z))\\ &= \log(\exp(t(\exp_s z-1)))\\ &= t(\exp_s z-1)\end{aligned}$$

Thus, we are led to the formulae in the statement. □

In order to discuss now the moments of the Bessel laws, things here are quite tricky, and it is convenient to do this via representation theory, by using the general results from chapter 9. Let us start with the following notion, in the general group theory context:

DEFINITION 10.28. *Given a compact group G, and two of its representations,*

$$u:G\to U_N\quad,\quad v:G\to U_M$$

we define the linear space of intertwiners between these representations as being

$$Hom(u,v)=\left\{T\in M_{M\times N}(\mathbb{C})\Big|Tu_g=v_gT,\forall g\in G\right\}$$

and we use the following conventions:

(1) *We use the notations $Fix(u)=Hom(1,u)$, and $End(u)=Hom(u,u)$.*
(2) *We write $u\sim v$ when $Hom(u,v)$ contains an invertible element.*
(3) *We say that u is irreducible, and write $u\in Irr(G)$, when $End(u)=\mathbb{C}1$.*

The terminology here is very standard, with Hom and End standing for "homomorphisms" and "endomorphisms", and with Fix standing for "fixed points".

In practice, it is useful to think of the representations of G as being the objects of some kind of abstract combinatorial structure associated to G, and of the intertwiners between these representations as being the "arrows" between these objects. We have in fact the following result, making the link with this viewpoint, called categorical:

THEOREM 10.29. *Given a compact group G, the following happen:*

(1) *The intertwiners are stable under composition:*

$$T\in Hom(u,v)\ ,\ S\in Hom(v,w)\implies ST\in Hom(u,w)$$

(2) *The intertwiners are stable under taking tensor products:*

$$S\in Hom(u,v)\ ,\ T\in Hom(w,t)\implies S\otimes T\in Hom(u\otimes w,v\otimes t)$$

(3) *The intertwiners are stable under taking adjoints:*

$$T\in Hom(u,v)\implies T^*\in Hom(v,u)$$

(4) *Thus, the Hom spaces form a tensor $*$-category.*

PROOF. All this is clear from definitions, the verifications being as follows:

(1) This follows indeed from the following computation, valid for any $g \in G$:

$$STu_g = Sv_gT = w_gST$$

(2) Again, this is clear, because we have the following computation:

$$\begin{aligned}(S \otimes T)(u_g \otimes w_g) &= Su_g \otimes Tw_g\\ &= v_gS \otimes t_gT\\ &= (v_g \otimes t_g)(S \otimes T)\end{aligned}$$

(3) This follows from the following computation, valid for any $g \in G$:

$$\begin{aligned}Tu_g = v_gT &\implies u_g^*T^* = T^*v_g^*\\ &\implies T^*v_g = u_gT^*\end{aligned}$$

(4) This is just an abstract conclusion of what we have in (1,2,3), with a tensor $*$-category being by definition an abstract beast satisfying these conditions (1,2,3). □

The above result is quite interesting, because it shows that the combinatorics of G is described by a certain collection of linear spaces, which can be investigated by using tools from linear algebra. Thus, what we have here is a useful "linearization" idea.

But all this might be a bit too abstract. Getting now to the case of the reflection groups, we first have the following result, concerning the symmetric group S_N itself:

THEOREM 10.30. *For the symmetric group $S_N \subset_u O_N$ we have the formula*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in P(k,l)\right)$$

with $P(k,l)$ being the set of partitions of k upper points, and l lower points, and where

$$T_\pi(e_{i_1} \otimes \ldots \otimes e_{i_k}) = \sum_{j_1 \ldots j_l} \delta_\pi \begin{pmatrix} i_1 & \ldots & i_k\\ j_1 & \ldots & j_l\end{pmatrix} e_{j_1} \otimes \ldots \otimes e_{j_l}$$

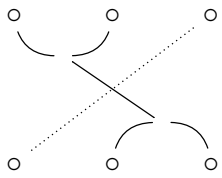
where $\delta_\pi \in \{0,1\}$ is 1 when the indices fit, and is 0 otherwise.

PROOF. This is something nice and elementary, the idea being as follows:

(1) First, at the level of notations, we denote as mentioned by $P(k,l)$ the set of partitions of k upper points, and l lower points, and with these partitions being represented as pictures, with the blocks being represented by strings. As an example, here is a partition

in $P(3,3)$, with two blocks, represented by strings, in the obvious way:

η =



(2) Now given $\pi \in P(k,l)$ and multi-indices $i = (i_1, \ldots, i_k)$ and $j = (j_1, \ldots, j_l)$, we can put i, j on the legs of π, in the obvious way. Then, if the "indices fit", meaning that all the strings of π join equal indices of i, j, we set $\delta_\pi \binom{i}{j} = 1$. Otherwise, we set $\delta_\pi \binom{i}{j} = 0$. As an example, for the above partition $\eta \in P(3,3)$, we have the following formula:

$$\delta_\eta \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = \delta_{abef}\delta_{cd}$$

(3) In order to prove now the result, let us first work out the case $k = 0$, that we will regularly need in what follows. It is traditional here, and convenient, to change a bit notations. So, let us associate to any $\pi \in P(k)$ a vector, as follows:

$$\xi_\pi = \sum_{i_1 \ldots i_k} \delta_\pi(i_1 \ldots i_k) e_{i_1} \otimes \ldots \otimes e_{i_k}$$

With this notation, we must prove that we have the following equality:

$$C_{0k} = span\left(\xi_\pi \middle| \pi \in P(k)\right)$$

(4) Let us first prove that we have $\supset$. Given $\sigma \in S_N$, we have indeed:

$$\begin{aligned}
\sigma^{\otimes k}\xi_\pi &= \sum_{i_1 \ldots i_k} \delta_\pi(i_1 \ldots i_k)\sigma(e_{i_1}) \otimes \ldots \otimes \sigma(e_{i_k}) \\
&= \sum_{i_1 \ldots i_k} \delta_\pi(i_1 \ldots i_k) e_{\sigma(i_1)} \otimes \ldots \otimes e_{\sigma(i_k)} \\
&= \sum_{i_1 \ldots i_k} \delta_\pi(\sigma^{-1}(j_1) \ldots \sigma^{-1}(j_k)) e_{j_1} \otimes \ldots \otimes e_{j_k} \\
&= \sum_{i_1 \ldots i_k} \delta_\pi(j_1 \ldots j_k) e_{j_1} \otimes \ldots \otimes e_{j_k} \\
&= \xi_\pi
\end{aligned}$$

(5) In order to prove now $\subset$, consider an arbitrary vector of $\mathbb{C}^N$, as follows:

$$\xi = \sum_{i_1 \ldots i_k} \lambda_{i_1 \ldots i_k} e_{i_1} \otimes \ldots \otimes e_{i_k}$$

Given $\sigma \in S_N$, by reasoning as before, we have the following formula:

$$\sigma^{\otimes k}\xi = \sum_{i_1 \ldots i_k} \lambda_{\sigma^{-1}(i_1)\ldots\sigma^{-1}(i_k)} e_{i_1} \otimes \ldots \otimes e_{i_k}$$

Thus the condition $\sigma^{\otimes k}\xi = \xi$ for any $\sigma \in S_N$ is equivalent to:

$$\lambda_{i_1\ldots i_k} = \lambda_{\sigma(i_1)\ldots\sigma(i_k)} \quad , \quad \forall i, \sigma$$

But this latter condition is equivalent to the following condition:

$$\ker i = \ker j \implies \lambda_i = \lambda_j$$

Thus, we are led to the conclusion that $\lambda : \{1, \ldots, N\}^k \to \mathbb{C}$ must come from a function $\varphi : P(k) \to \mathbb{C}$, via a formula of type $\lambda_i = \varphi(\ker i)$, and it follows that the inclusion $\supset$ that we established in (4) is indeed an equality, as desired.

(6) Summarizing, and getting back now to our theorem as stated, we have proved the formula of C_{kl} there, in the case $k = 0$. In order to pass now to the general case, two methods are available. We can either fine-tune the above computation, and we will leave this as an instructive exercise, or we can argue that the result at $k = 0$ gives the result in general, via Frobenius duality, and we will leave this as an instructive exercise too. □

The above result is quite encouraging, and suggests looking into other reflection groups. For the hyperoctahedral group H_N, the result is quite similar, as follows:

THEOREM 10.31. *For the hyperoctadedral group $H_N = \mathbb{Z}_2 \wr S_N \subset_u O_N$ we have*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in P_{even}(k, l)\right)$$

where P_{even} means partitions all whose blocks have even size.

PROOF. This follows a bit as for S_N. Consider indeed a vector of $\mathbb{C}^N$, as follows:

$$\xi = \sum_{i_1 \ldots i_k} \lambda_{i_1\ldots i_k} e_{i_1} \otimes \ldots \otimes e_{i_k}$$

Then the condition $g^{\otimes k}\xi = \xi$ for any $g = \sigma^w \in H_N$ is equivalent to:

$$\lambda_{i_1\ldots i_k} = w_{i_1} \ldots w_{i_k} \lambda_{\sigma(i_1)\ldots\sigma(i_k)} \quad , \quad \forall i, \sigma$$

But this latter condition is equivalent to the following condition, along with the fact that we must have $w_{i_1} \ldots w_{i_k} = 1$, which amounts in saying that $\ker i \in P_{even}$:

$$\ker i = \ker j \implies \lambda_i = \lambda_j$$

Thus, we are led to the conclusion in the statement. □

Quite remarkably, the results for S_N, H_N can be generalized as follows:

THEOREM 10.32. *For the complex reflection group $H_N^s = \mathbb{Z}_s \wr S_N \subset_u U_N$ we have*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in P^s(k,l)\right)$$

for any two colored integers k, l, with the tensor powers being as usual given by

$$u^{\otimes\circ} = u \quad , \quad u^{\otimes\bullet} = \bar{u} \quad , \quad u^{\otimes kl} = u^{\otimes k} \otimes u^{\otimes l}$$

where $P^s(k,l)$ is the set of partitions of k upper points and l lower points, satisfying

$$\#\circ = \#\bullet \ (s)$$

as a weighted equality, in each block.

PROOF. This follows a bit as for S_N, H_N. Consider indeed a vector, as follows:

$$\xi = \sum_{i_1 \ldots i_k} \lambda_{i_1 \ldots i_k} e_{i_1} \otimes \ldots \otimes e_{i_k}$$

Then the condition $g^{\otimes k}\xi = \xi$ for any $g = \sigma^w \in H_N^s$ is equivalent to:

$$\lambda_{i_1 \ldots i_k} = w_{i_1} \ldots w_{i_k} \lambda_{\sigma(i_1) \ldots \sigma(i_k)} \quad , \quad \forall i, \sigma$$

But this latter condition is equivalent to the following condition, along with the fact that we must have $w_{i_1} \ldots w_{i_k} = 1$, which amounts in saying that $\ker i \in P^s(k)$:

$$\ker i = \ker j \implies \lambda_i = \lambda_j$$

Thus, we are led to the conclusion in the statement. □

Good news, with the above understood, we can go back now to our moment problem, for the Bessel laws b_t^s. We first have the following result, dealing with the case $t = 1$:

THEOREM 10.33. *The moments of the Bessel law b_1^s are the numbers*

$$M_k = |P^s(k)|$$

where $P^s(k)$ is the set of partitions of $\{1, \ldots, k\}$ satisfying

$$\#\circ = \#\bullet \ (s)$$

as a weighted equality, in each block.

PROOF. This follows indeed from Theorem 10.32, via the standard fact, that we know well from chapter 9, that the integrals of characters count the fixed points. And with the comment that the linear maps T_π in Theorem 10.32 are indeed linearly independent, as needed, and we will leave some study or learning here as an instructive exercise. □

In the general parametric case the result is similar, as follows:

THEOREM 10.34. *The moments of the Bessel law b_t^s are the numbers*

$$M_k = \sum_{\pi\in P^s(k)} t^{|\pi|}$$

where $P^s(k)$ is the set of partitions of $\{1,\ldots,k\}$ satisfying

$$\#\circ = \#\bullet\,(s)$$

as a weighted sum, in each block.

PROOF. This is something more technical, the idea being that a suitable extension of our integration results from chapter 9, involving truncated characters, leads via Theorem 10.32 to the result. As before, we will leave some learning here as an exercise. □

And with this, end of our learning, in this chapter. Finally, let me mention that I personally got into this some time ago, in the context of some research work with Bichon and Collins, then Belinschi and Capitaine, and then Curran, Skalski, Speicher and Vergnioux too, on the free analogues of the measures b_t^s, called free Bessel laws. For more on the story here, and technical details, you have my free probability book [12].

10e. Exercises

This was a quite technical and exciting chapter, and as exercises, we have:

EXERCISE 10.35. *Learn more about finite groups, in general.*

EXERCISE 10.36. *In particular, learn about the finite abelian groups.*

EXERCISE 10.37. *Try enumerating the elements of H_3, with bare hands.*

EXERCISE 10.38. *Learn more about the Bessel functions, and their properties.*

EXERCISE 10.39. *Learn more about the CPLT, notably regarding the convergence.*

EXERCISE 10.40. *Learn more about the reflection groups H_N^{sd}, generalizing H_N^s.*

EXERCISE 10.41. *Learn about the classification of the complex reflection groups.*

EXERCISE 10.42. *Do the probabilistic computations for the groups H_N^{sd}.*

As bonus exercise, and no surprise here, read more group theory, in general.

CHAPTER 11

Hypergeometric laws

11a. Hypergeometric laws

We learned many interesting things in the previous two chapters, but time now to get to a more normal pace, and develop some more traditional probability theory, as a direct continuation of what we did in Part II. This being said, don't celebrate yet, because usually in mathematics the price to pay for doing less abstractions is that of doing more computations. So, in short, hope you are ready for some tough combinatorics.

Let us go back to the various types of binomial laws studied in chapters 6-7. As a variation of that constructions, we can talk about hypergeometric laws, as follows:

THEOREM 11.1. *Given a population of size $N \in \mathbb{N}$, with $m \in \{0, \ldots, N\}$ of these objects having a certain feature, the probability of having s successes, when performing $p \in \{0, \ldots, N\}$ draws without replacement, and looking for that feature, is*

$$P(s) = \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}}$$

with this being called hypergeometric law of parameters (N, m, p). When doing the same thing, but with replacement, we obtain a binomial law of parameter m/N.

PROOF. Many things can be said here, the idea being as follows:

(1) To start with, the main assertion is clear, because we have a total of $\binom{N}{p}$ possibilities for our p draws without replacement, and among these draws, those amounting to s successes come by multiplying $\binom{m}{s}$, standing for the s successes, and $\binom{N-m}{p-s}$, standing for the $p-s$ fails. Thus, we are led to the formula of $P(s)$ in the statement.

(2) Next, observe that the number of successes $s \in \mathbb{N}$ cannot be anything, because it must be subject to the condition that all binomial coefficients appearing in the formula of $P(s)$ must be well-defined, as usual binomial coefficients. Thus, we must have:

$$0 \leq s \leq m \quad , \quad 0 \leq p - s \leq N - m$$

In other words, the number of successes $s \in \mathbb{N}$, where $P(s) > 0$, is subject to:

$$s \in \{\max(0, p + m - N), \ldots, \min(m, p)\}$$

(3) Regarding now the fact that we have indeed a probability measure, this is something which is plainly clear, because when performing our p draws, something must happen, I mean we have a well-defined number of successes $s \in \mathbb{N}$, and $\sum_s P(s) = 1$.

(4) However, let us comment more on this. The formula $\sum_s P(s) = 1$ looks in practice as follows, with the bounds for the summing parameter s being those found in (2):

$$\sum_s \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} = 1$$

Equivalently, $\sum_s P(s) = 1$ tells us in practice that the following must happen:

$$\sum_s \binom{m}{s}\binom{N-m}{p-s} = \binom{N}{p}$$

But this is something which is clear indeed, because when drawing p objects out of N objects, with m of the objects having a certain feature, we have $\binom{N}{p}$ choices on one hand, and $\sum_s \binom{m}{s}\binom{N-m}{p-s}$ choices on the other hand, by looking at this feature.

(5) As a further comment on this, $\sum_s P(s) = 1$, this is related as well to the Vandermonde formula, which is as follows, coming itself from $(1+x)^m(1+x)^n = (1+x)^{m+n}$, by looking at the coefficient of x^p, on the left and on the right:

$$\sum_{s=0}^{p} \binom{m}{s}\binom{n}{p-s} = \binom{m+n}{p}$$

To be more precise, the formula from (4) is of this type, obtained by looking at the coefficient of x^p inside $(1+x)^m(1+x)^{N-m} = (1+x)^N$, which gives:

$$\sum_s \binom{m}{s}\binom{N-m}{p-s} = \binom{N}{p}$$

(6) Finally, in what regards the second assertion of the theorem, assume that we are doing our p draws, but this time with replacement. In this case, for having s successes, we have $\binom{p}{s}$ choices for the occurences of these successes, and then $(m/N)^s$ probability for the successes, and $(1-m/N)^{n-s}$ probability for the fails, so we obtain:

$$P(s) = \binom{p}{s}\left(\frac{m}{N}\right)^s\left(1-\frac{m}{N}\right)^{n-s}$$

But this is a binomial law of parameter m/N, as stated. □

Still at the theoretical level, as an interesting observation about our hypergeometric laws, which is not exactly obvious when looking at their definition, we have:

THEOREM 11.2. *The hypergeometric law of parameters (N, m, p) is given by*

$$P(s) = \frac{m!p!(N-m)!(N-p)!}{s!(m-s)!(p-s)!N!(N-m-p+s)!}$$

symmetric in m, p, and so equal to the hypergeometric law of parameters (N, p, m).

PROOF. As said above, the symmetry property in the statement is not obvious from the definition of the hypergeometric laws, involving the Bernoulli trials from Theorem 11.1. However, the math is there, as shown by the following computation:

$$\begin{aligned} P(s) &= \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} \\ &= \frac{m!}{s!(m-s)!} \cdot \frac{(N-m)!}{(p-s)!(N-m-p+s)!} \cdot \frac{p!(N-p)!}{N!} \\ &= \frac{m!p!(N-m)!(N-p)!}{s!(m-s)!(p-s)!N!(N-m-p+s)!} \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Many other theoretical things can be said about the hypergeometric laws, notably with an interesting relation with the permutation groups, and with a construction of negative hypergeometric laws as well. We will be back to this, later in this chapter.

Getting now to our usual business, computation of moments of low order, regarding the mean and variance of the hypergeometric laws, these are as follows:

THEOREM 11.3. *The mean and variance of the hypergeometric laws are*

$$E = \frac{mp}{N} \quad , \quad V = \frac{mp(N-m)(N-p)}{N^2(N-1)}$$

with (N, m, p) standing as usual for the parameters.

PROOF. The computations are similar to those for the binomial laws, as follows:

(1) Regarding the mean, we can compute it is as follows, by making use of the Vandermonde formula discussed above, that is, by making use of $\sum_s P(s) = 1$, for a certain

related hypergeometric law, with slightly different parameters:

$$\begin{aligned}
E &= \sum_s s\,\frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} \\
&= \frac{1}{\binom{N}{p}}\sum_s s\binom{m}{s}\binom{N-m}{p-s} \\
&= \frac{1}{\binom{N}{p}}\sum_s m\binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m}{\binom{N}{p}}\sum_s \binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m}{\binom{N}{p}}\binom{N-1}{p-1} \\
&= m\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-1)!}{(p-1)!(N-p)!} \\
&= \frac{mp}{N}
\end{aligned}$$

(2) Next, with the same trick we can compute $M_2 - M_1$, as follows:

$$\begin{aligned}
M_2 - M_1 &= \sum_s (s^2 - s)\,\frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} \\
&= \frac{1}{\binom{N}{p}}\sum_s s(s-1)\binom{m}{s}\binom{N-m}{p-s} \\
&= \frac{1}{\binom{N}{p}}\sum_s m(m-1)\binom{m-2}{s-2}\binom{N-m}{p-s} \\
&= \frac{m(m-1)}{\binom{N}{p}}\sum_s \binom{m-2}{s-2}\binom{N-m}{p-s} \\
&= \frac{m(m-1)}{\binom{N}{p}}\binom{N-2}{p-2} \\
&= m(m-1)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-2)!}{(p-2)!(N-p)!} \\
&= \frac{mp(m-1)(p-1)}{N(N-1)}
\end{aligned}$$

(3) Thus, the second moment is given by the following formula:

$$\begin{aligned} M_2 &= \frac{mp(m-1)(p-1)}{N(N-1)} + \frac{mp}{N} \\ &= \frac{mp}{N}\left(\frac{(m-1)(p-1)}{N-1} + 1\right) \\ &= \frac{mp(mp-m-p+N)}{N(N-1)} \end{aligned}$$

(4) We conclude that the variance is given by the following formula:

$$\begin{aligned} V &= M_2 - M_1^2 \\ &= \frac{mp(mp-m-p+N)}{N(N-1)} - \frac{m^2p^2}{N^2} \\ &= \frac{mp}{N}\left(\frac{mp-m-p+N}{N-1} - \frac{mp}{N}\right) \\ &= \frac{mp}{N} \cdot \frac{mp - m(m+p-N)}{N(N-1)} \\ &= \frac{mp(N-m)(N-p)}{N^2(N-1)} \end{aligned}$$

Thus, we are led to the conclusions in the statement. □

11b. Higher moments

Let us discuss now the computation of the higher moments of the hypergeometric laws. We will be mostly interested in the computation of M_3, M_4, allowing the computation of the skewness and kurtosis, and the study here, which is quite similar to the study that we did in chapter 6 for the usual binomial laws, leads to the following result:

THEOREM 11.4. *For the hypergeometric law of parameters (N, m, p) we have*

$$M_1 = \frac{mp}{N}$$

$$M_2 = \frac{mp(mp-m-p+N)}{N(N-1)}$$

$$M_3 = \frac{mp[(m-1)(p-1)(m-2)(p-2) + 3(m-1)(p-1)(N-2) + (N-1)(N-2)]}{N(N-1)(N-2)}$$

$$\vdots$$

and the higher moments can be computed as well, by recurrence.

PROOF. We already know the first two formulae from Theorem 11.3 and its proof, and the continuation is by using the same trick, as follows:

(1) Regarding the third moment, we can use here the following formula:

$$s^3 = s(s-1)(s-2) + 3s(s-1) + s$$

Indeed, this gives the following formula for the third moment:

$$\begin{aligned}
M_3 &= \sum_s s^3 \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} \\
&= \frac{1}{\binom{N}{p}} \sum_s s(s-1)(s-2)\binom{m}{s}\binom{N-m}{p-s} \\
&\quad + \frac{3}{\binom{N}{p}} \sum_s s(s-1)\binom{m}{s}\binom{N-m}{p-s} \\
&\quad + \frac{1}{\binom{N}{p}} \sum_s s\binom{m}{s}\binom{N-m}{p-s} \\
&= \frac{1}{\binom{N}{p}} \sum_s m(m-1)(m-2)\binom{m-3}{s-3}\binom{N-m}{p-s} \\
&\quad + \frac{3}{\binom{N}{p}} \sum_s m(m-1)\binom{m-2}{s-2}\binom{N-m}{p-s} \\
&\quad + \frac{1}{\binom{N}{p}} \sum_s m\binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m(m-1)(m-2)}{\binom{N}{p}} \sum_s \binom{m-3}{s-3}\binom{N-m}{p-s} \\
&\quad + \frac{3m(m-1)}{\binom{N}{p}} \sum_s \binom{m-2}{s-2}\binom{N-m}{p-s} \\
&\quad + \frac{m}{\binom{N}{p}} \sum_s \binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m(m-1)(m-2)}{\binom{N}{p}} \binom{N-3}{p-3} \\
&\quad + \frac{3m(m-1)}{\binom{N}{p}} \binom{N-2}{p-2} \\
&\quad + \frac{m}{\binom{N}{p}} \binom{N-1}{p-1}
\end{aligned}$$

Now by computing this quantity, we are led to the formula in the statement:

$$\begin{aligned}
M_3 &= \frac{m(m-1)(m-2)}{\binom{N}{p}}\binom{N-3}{p-3}\\
&\quad+\frac{3m(m-1)}{\binom{N}{p}}\binom{N-2}{p-2}\\
&\quad+\frac{m}{\binom{N}{p}}\binom{N-1}{p-1}\\
&= m(m-1)(m-2)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-3)!}{(p-3)!(N-p)!}\\
&\quad+3m(m-1)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-2)!}{(p-2)!(N-p)!}\\
&\quad+m\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-1)!}{(p-1)!(N-p)!}\\
&= m(m-1)(m-2)\cdot\frac{p(p-1)(p-2)}{N(N-1)(N-2)}\\
&\quad+3m(m-1)\cdot\frac{p(p-1)}{N(N-1)}\\
&\quad+m\cdot\frac{p}{N}\\
&= \frac{mp}{N(N-1)(N-2)}[(m-1)(p-1)(m-2)(p-2)\\
&\quad+3(m-1)(p-1)(N-2)+(N-1)(N-2)]
\end{aligned}$$

(2) Regarding the fourth moment, we can use here the following formula:

$$s^4=s(s-1)(s-2)(s-3)+6s(s-1)(s-2)+7s(s-1)+s$$

Indeed, this gives the following formula for the fourth moment:

$$\begin{aligned}
M_4 &= \sum_s s^4 \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}} \\
&= \frac{1}{\binom{N}{p}} \sum_s s(s-1)(s-2)(s-3)\binom{m}{s}\binom{N-m}{p-s} \\
&\quad + \frac{6}{\binom{N}{p}} \sum_s s(s-1)(s-2)\binom{m}{s}\binom{N-m}{p-s} \\
&\quad + \frac{7}{\binom{N}{p}} \sum_s s(s-1)\binom{m}{s}\binom{N-m}{p-s} \\
&\quad + \frac{1}{\binom{N}{p}} \sum_s s\binom{m}{s}\binom{N-m}{p-s} \\
&= \frac{1}{\binom{N}{p}} \sum_s m(m-1)(m-2)(m-3)\binom{m-4}{s-4}\binom{N-m}{p-s} \\
&\quad + \frac{6}{\binom{N}{p}} \sum_s m(m-1)(m-2)\binom{m-3}{s-3}\binom{N-m}{p-s} \\
&\quad + \frac{7}{\binom{N}{p}} \sum_s m(m-1)\binom{m-2}{s-2}\binom{N-m}{p-s} \\
&\quad + \frac{1}{\binom{N}{p}} \sum_s m\binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m(m-1)(m-2)(m-3)}{\binom{N}{p}} \sum_s \binom{m-4}{s-4}\binom{N-m}{p-s} \\
&\quad + \frac{6m(m-1)(m-2)}{\binom{N}{p}} \sum_s \binom{m-3}{s-3}\binom{N-m}{p-s} \\
&\quad + \frac{7m(m-1)}{\binom{N}{p}} \sum_s \binom{m-2}{s-2}\binom{N-m}{p-s} \\
&\quad + \frac{m}{\binom{N}{p}} \sum_s \binom{m-1}{s-1}\binom{N-m}{p-s} \\
&= \frac{m(m-1)(m-2)(m-3)}{\binom{N}{p}} \binom{N-4}{p-4} + \frac{6m(m-1)(m-2)}{\binom{N}{p}} \binom{N-3}{p-3} \\
&\quad + \frac{7m(m-1)}{\binom{N}{p}} \binom{N-2}{p-2} + \frac{m}{\binom{N}{p}} \binom{N-1}{p-1}
\end{aligned}$$

Now by computing this quantity, we are led to the following formula:

$$\begin{aligned}
M_4 &= \frac{m(m-1)(m-2)(m-3)}{\binom{N}{p}}\binom{N-4}{p-4}\\
&\quad+\frac{6m(m-1)(m-2)}{\binom{N}{p}}\binom{N-3}{p-3}\\
&\quad+\frac{7m(m-1)}{\binom{N}{p}}\binom{N-2}{p-2}\\
&\quad+\frac{m}{\binom{N}{p}}\binom{N-1}{p-1}\\
&= m(m-1)(m-2)(m-3)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-4)!}{(p-4)!(N-p)!}\\
&\quad+6m(m-1)(m-2)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-3)!}{(p-3)!(N-p)!}\\
&\quad+7m(m-1)\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-2)!}{(p-2)!(N-p)!}\\
&\quad+m\cdot\frac{p!(N-p)!}{N!}\cdot\frac{(N-1)!}{(p-1)!(N-p)!}\\
&= m(m-1)(m-2)(m-3)\cdot\frac{p(p-1)(p-2)(p-3)}{N(N-1)(N-2)(N-3)}\\
&\quad+6m(m-1)(m-2)\cdot\frac{p(p-1)(p-2)}{N(N-1)(N-2)}\\
&\quad+7m(m-1)\cdot\frac{p(p-1)}{N(N-1)}
\end{aligned}$$

Thus, we are led to the following formula, for the fourth moment:

$$\begin{aligned}
M_4 &= \frac{mp}{N(N-1)(N-2)(N-3)}\times\\
&\quad[(m-1)(p-1)(m-2)(p-2)(m-3)(p-3)\\
&\quad+6(m-1)(p-1)(m-2)(p-2)(N-2)\\
&\quad+7(m-1)(p-1)(N-2)(N-3)\\
&\quad+(N-1)(N-2)(N-3)]
\end{aligned}$$

(3) As a continuation of this, it is quite clear that we can compute M_k by recurrence. We will be back to this later in this chapter, with some precise results. □

Let us record as well a result about the corresponding central moments:

THEOREM 11.5. *The central moments of the hypergeometric law are*

$$M_1' = 0$$

$$M_2' = \frac{mp(N-m)(N-p)}{N^2(N-1)}$$

$$M_3' = \frac{mp(N-m)(N-p)(N-2m)(N-2p)}{N^3(N-1)(N-2)}$$

$$\vdots$$

with the computation in general being possible by recurrence.

PROOF. The first central moments are $M_1' = 0$, and then $M_2' = V$, whose formula we know from Theorem 11.3. Regarding the higher central moments, we recall from chapter 6 that these appear from the usual moments via the following formula:

$$\begin{aligned} M_k' &= E\left(\sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r f^{k-r}\right) \\ &= \sum_{r=0}^{k}(-1)^r\binom{k}{r}E^r M_{k-r} \\ &= \sum_{r=0}^{k-2}(-1)^r\binom{k}{r}E^r M_{k-r} + (-1)^{k-1}(k-1)E^k \end{aligned}$$

Now with $k = 3$, by using the formulae from Theorem 11.4, we obtain, after some computations, that I will leave to you as an exercise:

$$\begin{aligned} & M_3' \\ = \; & M_3 - 3EM_2 + 2E^3 \\ = \; & \frac{mp[(m-1)(p-1)(m-2)(p-2) + 3(m-1)(p-1)(N-2) + (N-1)(N-2)]}{N(N-1)(N-2)} \\ & -3\frac{mp}{N}\cdot\frac{mp(mp-m-p+N)}{N(N-1)} + 2\frac{m^3p^3}{N^3} \\ = \; & \frac{mp(N-m)(N-p)(N-2m)(N-2p)}{N^3(N-1)(N-2)} \end{aligned}$$

At $k=4$ now, again by using the formulae from Theorem 11.4 and its proof, we have the following formula, for the normalized fourth moment:

$$\begin{aligned}
M_4' &= M_4-4EM_3+6E^2M_2-3E^4\\
&= \frac{mp}{N(N-1)(N-2)(N-3)}\times\\
&\quad [(m-1)(p-1)(m-2)(p-2)(m-3)(p-3)\\
&\quad +6(m-1)(p-1)(m-2)(p-2)(N-2)\\
&\quad +7(m-1)(p-1)(N-2)(N-3)\\
&\quad +(N-1)(N-2)(N-3)]\\
&\quad -4\,\frac{mp}{N}\cdot\frac{mp}{N(N-1)(N-2)}\times\\
&\quad [(m-1)(p-1)(m-2)(p-2)+3(m-1)(p-1)(N-2)+(N-1)(N-2)]\\
&\quad +6\,\frac{m^2p^2}{N^2}\cdot\frac{mp(mp-m-p+N)}{N(N-1)}-3\frac{m^4p^4}{N^4}
\end{aligned}$$

Of course, this expression still needs to be simplified, and have fun with this. As for the last assertion, regarding higher moments, we will be back to it later, with details. □

Let us end this discussion with the following result, capturing the essentials:

THEOREM 11.6. *For the hypergeometric law of parameters (N,m,p),*

$$E=\frac{mp}{N}$$

$$V=\frac{mp(N-m)(N-p)}{N^2(N-1)}$$

$$\gamma=\frac{(N-2m)(N-2p)\sqrt{N-1}}{(N-2)\sqrt{mp(N-m)(N-p)}}$$

$$\kappa=3+\frac{\begin{pmatrix}N^2(N-1)[N(N+1)-6m(N-m)-6p(N-p)]\\ +6mp(N-m)(N-p)(5N-6)\end{pmatrix}}{mp(N-m)(N-p)(N-2)(N-3)}$$

are the mean, variance, skewness and kurtosis.

PROOF. Regarding the formulae of E, V, we know these from Theorem 11.3. Next, by using the formula of M_3' from Theorem 11.5, the skewness is given by:

$$\begin{aligned}\gamma &= M_3'/V\sqrt{V}\\ &= \frac{mp(N-m)(N-p)(N-2m)(N-2p)}{N^3(N-1)(N-2)}\times\\ &\quad\frac{N^2(N-1)}{mp(N-m)(N-p)}\sqrt{\frac{N^2(N-1)}{mp(N-m)(N-p)}}\\ &= \frac{(N-2m)(N-2p)\sqrt{N-1}}{(N-2)\sqrt{mp(N-m)(N-p)}}\end{aligned}$$

Finally, I will leave to you the computation of the kurtosis, based on what we have in Theorem 11.5 and its proof, and enjoy this computation. Needless to say, the higher normalized central moments can be computed too, by recurrence. □

11c. Permutations, again

In relation now with algebra, consider the standard coordinates over the symmetric group S_N, regarded as usual as group of orthogonal matrices, $S_N \subset O_N$:

$$u = \begin{pmatrix} u_{11} & \ldots & u_{1N}\\ \vdots & & \vdots\\ u_{N1} & \ldots & u_{NN}\end{pmatrix}$$

Now given two integers $m, p \leq N$, let us write this matrix as follows:

$$u = \begin{pmatrix} u_{11} & \ldots & u_{1p} & \ldots & \ldots & u_{1N}\\ \vdots & \star & \vdots & & & \vdots\\ u_{m1} & \ldots & u_{mp} & \ldots & \ldots & u_{mN}\\ \vdots & & \vdots & & & \vdots\\ \vdots & & \vdots & & & \vdots\\ u_{N1} & \ldots & u_{Np} & \ldots & \ldots & u_{NN}\end{pmatrix}$$

Consider now the rectangular matrix appearing in the upper left corner, marked with a $\star$ symbol, and let us make the sum of the entries of this matrix:

$$S_{mp} = \sum_{i=1}^{m}\sum_{j=1}^{p} u_{ij}$$

The point is then that this variable is hypergeometric:

THEOREM 11.7. *The following variable over the symmetric group $S_N \subset O_N$,*

$$S_{mp} = \sum_{i=1}^{m} \sum_{j=1}^{p} u_{ij}$$

is hypergeometric, having parameters (N, m, p).

PROOF. We know that the coordinates of the symmetric group, viewed as group of permutation matrices, $S_N \subset O_N$ are given by the following formula:

$$u_{ij} = \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

Thus, the variable in the statement is given by the following formula:

$$S_{mp} = \sum_{i=1}^{m} \sum_{j=1}^{p} \chi\left(\sigma \in S_N \middle| \sigma(j) = i\right)$$

Let us compute now the law of this variable. We have the following formula:

$$\begin{aligned} P(S_{mp} = s) &= \frac{1}{N!} \#\left(\sigma \in S_N \middle| S_{mp}(\sigma) = s\right) \\ &= \frac{1}{N!} \#\left(\sigma \in S_N \middle| \#\left\{i \leq m, j \leq p \middle| \sigma(j) = i\right\} = s\right) \\ &= \frac{1}{N!} \#\left(\sigma \in S_N \middle| \#\left\{j \leq p \middle| \sigma(j) \leq m\right\} = s\right) \end{aligned}$$

Now let us try to count the permutations on the right. Such a permutation $\sigma \in S_N$ comes from 5 operations involved, as follows:

(1) We first have to pick a subset $X \subset \{1, \ldots, p\}$, with $|X| = s$.

(2) We also have to pick a subset $Y \subset \{1, \ldots, m\}$, with $|Y| = s$.

(3) Then, we have to bijectively map $X \to Y$.

(4) Next, we have to map injectively $\{1, \ldots, p\} - X \to \{m+1, \ldots, N\}$.

(5) And finally, we have to bijectively map $\{p+1, \ldots, N\}$ to what is left.

Regarding now the precise numbers of choices for these 5 operations involved, these are easy to compute, as follows:

(1) Here we have $\binom{p}{s}$ choices.

(2) Here we have $\binom{m}{s}$ choices.

(3) Here we have $s!$ choices.

(4) Here we have $\frac{(N-m)!}{(N-m-p+s)!}$ choices.

(5) Here we have $(N-p)!$ choices.

We can now finish our probability computation started above, as follows:

$$\begin{aligned}
P(S_{mp}=s) &= \frac{1}{N!}\binom{p}{s}\binom{m}{s}s!\,\frac{(N-m)!}{(N-m-p+s)!}(N-p)! \\
&= \frac{1}{N!}\cdot\frac{p!}{s!(p-s)!}\cdot\frac{m!}{s!(m-s)!}\cdot s!\cdot\frac{(N-m)!}{(N-m-p+s)!}(N-p)! \\
&= \frac{p!m!(N-m)!(N-p)!}{N!s!(p-s)!(m-s)!(N-m-p+s)!} \\
&= \frac{m!}{s!(m-s)!}\cdot\frac{(N-m)!}{(p-s)!(N-m-p+s)!}\cdot\frac{p!(N-p)!}{N!} \\
&= \frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}}
\end{aligned}$$

We are therefore led to the conclusion in the statement. □

All this is quite interesting. As a first consequence, we have:

PROPOSITION 11.8. *The hypergeometric law of parameters (N,m,p), namely*

$$P(s)=\frac{\binom{m}{s}\binom{N-m}{p-s}}{\binom{N}{p}}$$

is symmetric in m,p, and with this being obvious via the permutation approach.

PROOF. The symmetry assertion is something that we already know, from Theorem 11.3, but as explained there, this is something quite tricky, basically coming from:

$$P(s)=\frac{p!m!(N-m)!(N-p)!}{N!s!(p-s)!(m-s)!(N-m-p+s)!}$$

However, and here comes the point, while this computation remains something quite opaque, our result is clear by using the interpretation from Theorem 11.7. □

In order to discuss now the moment problematics, using our group theory approach coming from Theorem 11.7, we will need the following standard fact:

PROPOSITION 11.9. *The integrals over the symmetric group S_N are given by*

$$\int_{S_N}u_{i_1j_1}\ldots u_{i_kj_k}=\begin{cases}\frac{(N-|\ker i|)!}{N!} & \text{if } \ker i=\ker j\\ 0 & \text{otherwise}\end{cases}$$

where $\ker i$ denotes as usual the partition of $\{1,\ldots,k\}$ whose blocks collect the equal indices of i, and where $|.|$ denotes the number of blocks.

PROOF. This is indeed something that we know well, from chapter 9, and we refer to the material there for the details, and for illustrations for this formula. □

Getting back now to the hypergeometric variables, we have:

THEOREM 11.10. *For the hypergeometric law of parameters (N, m, p) we have*

$$M_k = \sum_{\pi \in P(k)} \frac{m!}{(m - |\pi|)!} \cdot \frac{p!}{(p - |\pi|)!} \cdot \frac{(N - |\pi|)!}{N!}$$

where $|.|$ denotes as usual the number of blocks.

PROOF. This is something very standard, the idea being as follows:

(1) Some numerics first. At $k = 1$ we only have one partition, namely $|$, and the formula in the statement holds indeed, as shown by the following computation:

$$\begin{aligned} \sum_{\pi \in P(1)} \frac{m!}{(m - |\pi|)!} \cdot \frac{p!}{(p - |\pi|)!} \cdot \frac{(N - |\pi|)!}{N!} &= \frac{m!}{(m-1)!} \cdot \frac{p!}{(p-1)!} \cdot \frac{(N-1)!}{N!} \\ &= \frac{mp}{N} \end{aligned}$$

(2) At $k = 2$ now, we have two partitions, namely $||$ and $\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned} & \sum_{\pi \in P(2)} \frac{m!}{(m - |\pi|)!} \cdot \frac{p!}{(p - |\pi|)!} \cdot \frac{(N - |\pi|)!}{N!} \\ = \ & \frac{m!}{(m-2)!} \cdot \frac{p!}{(p-2)!} \cdot \frac{(N-2)!}{N!} + \frac{m!}{(m-1)!} \cdot \frac{p!}{(p-1)!} \cdot \frac{(N-1)!}{N!} \\ = \ & \frac{m(m-1)p(p-1)}{N(N-1)} + \frac{mp}{N} \\ = \ & \frac{mp}{N}[(m-1)(p-1) + N - 1] \\ = \ & \frac{mp(mp - m - p + N)}{N(N-1)} \end{aligned}$$

(3) At $k=3$ we have 5 partitions, namely $|\,|\,|$, $\sqcap\,|$, $\sqcap\!\!\sqcap$, $|\,\sqcap$, $\sqcap\!\!\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}
&\sum_{\pi\in P(3)}\frac{m!}{(m-|\pi|)!}\cdot\frac{p!}{(p-|\pi|)!}\cdot\frac{(N-|\pi|)!}{N!}\\
=\;&\frac{m!}{(m-3)!}\cdot\frac{p!}{(p-3)!}\cdot\frac{(N-3)!}{N!}\\
&+3\,\frac{m!}{(m-2)!}\cdot\frac{p!}{(p-2)!}\cdot\frac{(N-2)!}{N!}+\frac{m!}{(m-1)!}\cdot\frac{p!}{(p-1)!}\cdot\frac{(N-1)!}{N!}\\
=\;&\frac{m(m-1)(m-2)p(p-1)(p-2)}{N(N-1)(N-2)}+\frac{3m(m-1)p(p-1)}{N(N-1)}+\frac{mp}{N}\\
=\;&\frac{mp[(m-1)(p-1)(m-2)(p-2)+3(m-1)(p-1)(N-2)+(N-1)(N-2)]}{N(N-1)(N-2)}
\end{aligned}$$

(4) At $k=4$ now, we have 15 partitions, with the list of relevant partitions, and their multiplicities up to permutations, which is self-explanatory, being as follows:

$$|\,|\,|\,|\times 1\quad,\quad\sqcap\,|\,|\times 6\quad,\quad\sqcap\,\sqcap\times 3\quad,\quad\sqcap\!\!\sqcap\,|\times 4\quad,\quad\sqcap\!\!\sqcap\!\!\sqcap\times 1$$

Now by doing the computation, as before, we obtain the following formula:

$$\begin{aligned}
&\sum_{\pi\in P(4)}\frac{m!}{(m-|\pi|)!}\cdot\frac{p!}{(p-|\pi|)!}\cdot\frac{(N-|\pi|)!}{N!}\\
=\;&\frac{m!}{(m-4)!}\cdot\frac{p!}{(p-4)!}\cdot\frac{(N-4)!}{N!}+6\,\frac{m!}{(m-3)!}\cdot\frac{p!}{(p-3)!}\cdot\frac{(N-3)!}{N!}\\
&+(3+4)\,\frac{m!}{(m-2)!}\cdot\frac{p!}{(p-2)!}\cdot\frac{(N-2)!}{N!}+\frac{m!}{(m-1)!}\cdot\frac{p!}{(p-1)!}\cdot\frac{(N-1)!}{N!}\\
=\;&\frac{m(m-1)(m-2)(m-3)p(p-1)(p-2)(p-3)}{N(N-1)(N-2)(N-3)}\\
&+\frac{6m(m-1)(m-2)p(p-1)(p-2)}{N(N-1)(N-2)}+\frac{7m(m-1)p(p-1)}{N(N-1)}+\frac{mp}{N}
\end{aligned}$$

And this agrees with the moment formula from the proof of Theorem 11.4, namely:

$$\begin{aligned}
M_4\;=\;&\frac{mp}{N(N-1)(N-2)(N-3)}\times\\
&[(m-1)(p-1)(m-2)(p-2)(m-3)(p-3)\\
&+6(m-1)(p-1)(m-2)(p-2)(N-2)\\
&+7(m-1)(p-1)(N-2)(N-3)\\
&+(N-1)(N-2)(N-3)]
\end{aligned}$$

(5) In general now, by some magic, we have the following computation, using the interpretation from Theorem 11.7, and the integration formula in Proposition 11.9:

$$\begin{aligned}
M_k &= \int_{S_N} S_{mp}^k \\
&= \int_{S_N} \left(\sum_{i=1}^{m} \sum_{j=1}^{p} u_{ij} \right)^k \\
&= \int_{S_N} \sum_{i_1=1}^{m} \cdots \sum_{i_k=1}^{m} \sum_{j_1=1}^{p} \cdots \sum_{j_k=1}^{p} u_{i_1 j_1} \ldots u_{i_k j_k} \\
&= \sum_{i_1=1}^{m} \cdots \sum_{i_k=1}^{m} \sum_{j_1=1}^{p} \cdots \sum_{j_k=1}^{p} \int_{S_N} u_{i_1 j_1} \ldots u_{i_k j_k} \\
&= \sum_{i_1=1}^{m} \cdots \sum_{i_k=1}^{m} \sum_{j_1=1}^{p} \cdots \sum_{j_k=1}^{p} \delta_{\ker i, \ker j} \frac{(N - |\ker i|)!}{N!} \\
&= \sum_{\pi \in P(k)} \sum_{i_1=1}^{m} \cdots \sum_{i_k=1}^{m} \sum_{j_1=1}^{p} \cdots \sum_{j_k=1}^{p} \delta_{\ker i, \ker j, \pi} \frac{(N - |\pi|)!}{N!} \\
&= \sum_{\pi \in P(k)} \left(\sum_{i_1=1}^{m} \cdots \sum_{i_k=1}^{m} \delta_{\ker i, \pi} \right) \left(\sum_{j_1=1}^{p} \cdots \sum_{j_k=1}^{p} \delta_{\ker j, \pi} \right) \frac{(N - |\pi|)!}{N!} \\
&= \sum_{\pi \in P(k)} \frac{m!}{(m - |\pi|)!} \cdot \frac{p!}{(p - |\pi|)!} \cdot \frac{(N - |\pi|)!}{N!}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

11d. Negative versions

As a variation of what we did so far in this chapter, regarding the hypergeometric laws, we can talk as well about negative hypergeometric laws, as follows:

THEOREM 11.11. *Given a population of size $N \in \mathbb{N}$, with $m \in \{0, \ldots, N\}$ of these objects having a certain feature, the probability of having s successes, when performing draws without replacement, and stopping after $r \in \{0, \ldots, N - m\}$ failures, is*

$$P(s) = \frac{\binom{s+r-1}{s} \binom{N-r-s}{m-s}}{\binom{N}{m}}$$

with this being called negative hypergeometric law of parameters (N, m, r). When doing this with replacement, we obtain a negative binomial law of parameter m/N.

PROOF. Many things can be said here, the idea being as follows:

(1) Observe first the similarity with the definition of the usual hypergeometric laws, from Theorem 11.1. To be more precise, the common part is that, in both these cases, we have a population of size $N \in \mathbb{N}$, with $m \in \{0, \ldots, N\}$ of these objects having a certain feature, and we are looking for the probability of having s successes, when performing draws with replacement. The difference comes from the stopping convention, for the hypergeometric laws this being after $p \in \{0, \ldots, N\}$ draws, and for the negative hypergeometric laws this being after $r \in \{0, \ldots, N-m\}$ failures.

(2) In practice, based on this observation, we can develop the theory of negative hypergeometric laws by using the previously developed theory of the usual hypergeometric laws. Indeed, to start with, the probability $P(s)$ that we are interested in comes by multiplying a probability coming from a usual hypergeometric law, corresponding to the m succeses in the first $m+r-1$ draws, and a basic fraction, corresponding to the failure required at the $(m+r)$-th draw. In practice, this gives the following formula:

$$\begin{aligned}
P(s) &= \frac{\binom{m}{s}\binom{N-m}{s+r-1-s}}{\binom{N}{s+r-1}} \cdot \frac{N-m-(r-1)}{N-(s+r-1)} \\
&= \frac{\binom{m}{s}\binom{N-m}{r-1}}{\binom{N}{s+r-1}} \cdot \frac{N-m-r+1}{N-s-r+1} \\
&= \frac{m!(N-m)!(s+r-1)!(N-s-r+1)!(N-m-r+1)}{s!(m-s)!(r-1)!N!(N-m-r+1)!(N-s-r+1)} \\
&= \frac{m!(N-m)!(s+r-1)!(N-s-r)!}{s!(m-s)!(r-1)!N!(N-m-r)!} \\
&= \frac{(s+r-1)!(N-r-s)!(N-m)!m!}{s!(r-1)!(m-s)!(N-r-m)!N!} \\
&= \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}}
\end{aligned}$$

Thus, we have indeed the formula of $P(s)$ in the statement.

(3) Regarding now the fact that we have indeed a probability measure, this is something which is plainly clear, because when performing our draws, something must happen, I mean we have a well-defined number of successes $s \in \mathbb{N}$, and $\sum_s P(s) = 1$.

(4) However, let us comment more on this. The formula $\sum_s P(s) = 1$ looks in practice as follows, with the bounds for the summing parameter s being the obvious ones:

$$\sum_s \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}} = 1$$

Equivalently, $\sum_s P(s) = 1$ tells us in practice that the following must happen:

$$\sum_s \binom{s+r-1}{s}\binom{N-r-s}{m-s} = \binom{N}{m}$$

But this is something which is clear indeed, combinatorially speaking.

(5) As a further comment on this, $\sum_s P(s) = 1$, this can be deduced as well from the Vandermonde formula, which is as follows, coming from $(1+x)^m(1+x)^n = (1+x)^{m+n}$, by looking at the coefficient of x^p, on the left and on the right:

$$\sum_s \binom{m}{s}\binom{n}{p-s} = \binom{m+n}{p}$$

Indeed, by using this formula, along with the identity $\binom{n}{k} = (-1)^k\binom{k-n-1}{k}$ for the generalized binomial coefficients, which is something trivial, we have:

$$\begin{aligned}
\sum_s \binom{s+r-1}{s}\binom{N-r-s}{m-s} &= \sum_s (-1)^s\binom{-r}{s}(-1)^{m-s}\binom{m+r-N-1}{m-s}\\
&= (-1)^m\sum_s \binom{-r}{s}\binom{m+r-N-1}{m-s}\\
&= (-1)^m\binom{m-N-1}{m}\\
&= \binom{N}{m}
\end{aligned}$$

(6) Finally, in what regards the second assertion of the theorem, assume that we are doing our draws, but this time with replacement. In this case, for having s successes, we have $\binom{s+r-1}{s}$ choices for the occurences of these successes, and then $(m/N)^s$ probability for the successes, and $(1-m/N)^r$ probability for the fails, so we obtain:

$$P(s) = \binom{s+r-1}{s}\left(\frac{m}{N}\right)^s\left(1-\frac{m}{N}\right)^r$$

But this is a negative binomial law of parameter m/N, as stated. □

Regarding the mean and variance of the negative hypergeometric laws, these can be computed a bit as for the usual hypergeometric laws, the result being as follows:

THEOREM 11.12. *The mean and variance of the negative hypergeometric laws are*

$$E = \frac{mr}{N-m+1} \quad , \quad V = \frac{mr(N+1)(N-m-r+1)}{(N-m+1)^2(N-m+2)}$$

with (N, m, r) standing as usual for the parameters.

PROOF. The computations are quite similar to those from before, as follows:

(1) Regarding the mean, we can compute it with a trick, namely:

$$s = (s + r) - r$$

Indeed, by using this trick, and the summation formula based on Vandermonde discussed in (5) in the proof of Theorem 11.11, we obtain the following formula:

$$\begin{aligned}
E &= \sum_s s \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}} \\
&= \sum_s [(s + r) - r] \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}} \\
&= \left[\sum_s (s + r) \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}}\right] - r \\
&= \frac{r}{\binom{N}{m}} \left[\sum_s \frac{s+r}{r}\binom{s+r-1}{s}\binom{N-r-s}{m-s}\right] - r \\
&= \frac{r}{\binom{N}{m}} \left[\sum_s \binom{s+r}{s}\binom{N-r-s}{m-s}\right] - r \\
&= \frac{r}{\binom{N}{m}} \binom{N+1}{m} - r \\
&= r \cdot \frac{m!(N-m)!}{N!} \cdot \frac{(N+1)!}{m!(N-m+1)!} - r \\
&= \frac{(N+1)r}{N-m+1} - r \\
&= \frac{mr}{N-m+1}
\end{aligned}$$

(2) In order to compute now $M_2 - M_1$, we can use a similar trick, as follows:

$$s^2 - s = (s + r)(s + r + 1) - 2(r + 1)(s + r) + r(r + 1)$$

Indeed, by summing as in (1), using Vandermonde, we get the following formula:

$$\begin{aligned}
& M_2 - M_1 \\
= \ & \sum_s (s^2 - s) \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}} \\
= \ & \sum_s [(s+r)(s+r+1) - 2(r+1)(s+r) + r(r+1)] \frac{\binom{s+r-1}{s}\binom{N-r-s}{m-s}}{\binom{N}{m}} \\
= \ & \frac{1}{\binom{N}{m}} \sum_s (s+r)(s+r+1)\binom{s+r-1}{s}\binom{N-r-s}{m-s} \\
& -\frac{2(r+1)}{\binom{N}{m}} \sum_s (s+r)\binom{s+r-1}{s}\binom{N-r-s}{m-s} + r(r+1) \\
= \ & \frac{r(r+1)}{\binom{N}{m}} \sum_s \binom{s+r+1}{s}\binom{N-r-s}{m-s} \\
& -\frac{2r(r+1)}{\binom{N}{m}} \sum_s \binom{s+r}{s}\binom{N-r-s}{m-s} + r(r+1) \\
= \ & \frac{r(r+1)}{\binom{N}{m}} \binom{N+2}{m} - \frac{2r(r+1)}{\binom{N}{m}} \binom{N+1}{m} + r(r+1) \\
= \ & r(r+1)\left[\frac{m!(N-m)!(N+2)!}{N!m!(N-m+2)!} - 2 \cdot \frac{m!(N-m)!(N+1)!}{N!m!(N-m+1)!} + 1\right] \\
= \ & r(r+1)\left[\frac{(N+1)(N+2)}{(N-m+1)(N-m+2)} - 2 \cdot \frac{N+1}{N-m+1} + 1\right] \\
= \ & r(r+1)\left[\frac{(N+1)(N+2)}{(N-m+1)(N-m+2)} - \frac{N+m+1}{N-m+1}\right] \\
= \ & \frac{r(r+1)}{(N-m+1)(N-m+2)}[(N+1)(N+2) - (N+m+1)(N-m+2)] \\
= \ & \frac{r(r+1)}{(N-m+1)(N-m+2)}(m^2 - m) \\
= \ & \frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)}
\end{aligned}$$

(3) We conclude that the second moment is given by the following formula:

$$M_2 = \frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)} + \frac{mr}{N-m+1}$$

(4) Getting now to the variance, this is given by the following formula:

$$\begin{aligned}
V &= M_2 - M_1^2\\
&= \frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)} + \frac{mr}{N-m+1} - \frac{m^2r^2}{(N-m+1)^2}\\
&= \frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)} + \frac{mr}{N-m+1}\left(1 - \frac{mr}{N-m+1}\right)\\
&= \frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)} + \frac{mr(N-m+1-mr)}{(N-m+1)^2}\\
&= \frac{mr}{(N-m+1)^2(N-m+2)} \times\\
&\quad [(m-1)(r+1)(N-m+1) + (N-m+1-mr)(N-m+2)]\\
&= \frac{mr}{(N-m+1)^2(N-m+2)} \times\\
&\quad [(N+1)((m-1)(r+1) + N - m + 2) - m(r+1)(m-1+N-m+2)]\\
&= \frac{mr}{(N-m+1)^2(N-m+2)} \times\\
&\quad [(N+1)(mr - r + N + 1) - (mr+m)(N+1)]\\
&= \frac{mr(N+1)(N-m-r+1)}{(N-m+1)^2(N-m+2)}
\end{aligned}$$

Thus, we are led to the conclusions in the statement. □

As a main result now regarding the negative hypergeometric laws, we have:

THEOREM 11.13. *For the negative hypergeometric law of parameters (N, m, r),*

$$M_k = \sum_{\pi \in P(k)} \frac{m!}{(m-|\pi|)!} \cdot \frac{(r+|\pi|-1)!}{(r-1)!} \cdot \frac{(N-m)!}{(N-m+|\pi|)!}$$

where $|.|$ denotes as usual the number of blocks.

PROOF. This is something quite standard, the idea being as follows:

(1) Some numerics first. At $k = 1$ we only have one partition, namely $|$, and the formula in the statement holds indeed, as shown by the following computation:

$$\begin{aligned}
&\sum_{\pi \in P(1)} \frac{m!}{(m-|\pi|)!} \cdot \frac{(r+|\pi|-1)!}{(r-1)!} \cdot \frac{(N-m)!}{(N-m+|\pi|)!}\\
&= \frac{m!}{(m-1)!} \cdot \frac{r!}{(r-1)!} \cdot \frac{(N-m)!}{(N-m+1)!}\\
&= \frac{mr}{N-m+1}
\end{aligned}$$

(2) At $k = 2$ now, we have two partitions, namely $||$ and $\sqcap$, and the formula in the statement holds again, as shown by the following computation:

$$\begin{aligned}
&\sum_{\pi\in P(2)} \frac{m!}{(m-|\pi|)!}\cdot\frac{(r+|\pi|-1)!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+|\pi|)!}\\
=\ &\frac{m!}{(m-2)!}\cdot\frac{r!}{(r-2)!}\cdot\frac{(N-m)!}{(N-m+2)!}+\frac{m!}{(m-1)!}\cdot\frac{r!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+1)!}\\
=\ &\frac{m(m-1)r(r+1)}{(N-m+1)(N-m+2)}+\frac{mr}{N-m+1}
\end{aligned}$$

(3) At $k = 3$ we have 5 partitions, namely $|||$, $\sqcap|$, $\sqcap\!\!|$, $|\sqcap$, $\sqcap\!\sqcap$, and the quantity in the statement is given by the following formula:

$$\begin{aligned}
&\sum_{\pi\in P(3)} \frac{m!}{(m-|\pi|)!}\cdot\frac{(r+|\pi|-1)!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+|\pi|)!}\\
=\ &\frac{m!}{(m-3)!}\cdot\frac{r!}{(r-3)!}\cdot\frac{(N-m)!}{(N-m+3)!}+3\,\frac{m!}{(m-2)!}\cdot\frac{r!}{(r-2)!}\cdot\frac{(N-m)!}{(N-m+2)!}\\
&+\frac{m!}{(m-1)!}\cdot\frac{r!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+1)!}\\
=\ &\frac{m(m-1)(m-2)r(r+1)(r+2)}{(N-m+1)(N-m+2)(N-m+3)}+\frac{3m(m-1)r(r+1)}{(N-m+1)(N-m+2)}+\frac{mr}{N-m+1}
\end{aligned}$$

But this is the same as M_3, computed as in the proof of Theorem 11.12.

(4) At $k = 4$ now, we have 15 partitions, with the list of relevant partitions, and their multiplicities up to permutations, which is self-explanatory, being as follows:

$$|||| \times 1 \quad , \quad \sqcap|| \times 6 \quad , \quad \sqcap\sqcap \times 3 \quad , \quad \sqcap\!\sqcap| \times 4 \quad , \quad \sqcap\!\sqcap\!\sqcap \times 1$$

Now by doing the computation, as before, we obtain the following formula:

$$\begin{aligned}
&\sum_{\pi\in P(4)}\frac{m!}{(m-|\pi|)!}\cdot\frac{(r+|\pi|-1)!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+|\pi|)!}\\
=\ &\frac{m!}{(m-4)!}\cdot\frac{r!}{(r-4)!}\cdot\frac{(N-m)!}{(N-m+4)!}+6\,\frac{m!}{(m-3)!}\cdot\frac{r!}{(r-3)!}\cdot\frac{(N-m)!}{(N-m+3)!}\\
&+(3+4)\,\frac{m!}{(m-2)!}\cdot\frac{r!}{(r-2)!}\cdot\frac{(N-m)!}{(N-m+2)!}+\frac{m!}{(m-1)!}\cdot\frac{r!}{(r-1)!}\cdot\frac{(N-m)!}{(N-m+1)!}\\
=\ &\frac{m(m-1)(m-2)(m-3)r(r+1)(r+2)(r+3)}{(N-m+1)(N-m+2)(N-m+3)(N-m+4)}\\
&+\frac{6m(m-1)(m-2)r(r+1)(r+2)}{(N-m+1)(N-m+2)(N-m+3)}\\
&+\frac{7m(m-1)r(r+1)}{(N-m+1)(N-m+2)}+\frac{mr}{N-m+1}
\end{aligned}$$

But this is the same as M_4, computed as in the proof of Theorem 11.12.

(5) In general now, the formula in the statement follows by recurrence, by using the tricks from the proof of Theorem 11.12. We will leave this as an exercise, and come back to this in the next chapter, directly in a more general setting. □

11e. Exercises

This was a quite technical chapter, as we like them, and as exercises, we have:

Exercise 11.14. *Meditate on the symmetry of the hypergeometric law in m, p.*

Exercise 11.15. *Do the missing hypergeometric law computations, at $k = 3$.*

Exercise 11.16. *Do the missing hypergeometric law computations, at $k = 4$.*

Exercise 11.17. *Compute the higher moments by a direct recurrence.*

Exercise 11.18. *Work out the asymptotics of the hypergeometric laws.*

Exercise 11.19. *Learn more about the negative hypergeometric laws.*

Exercise 11.20. *Try finding a group-theoretical model for these latter laws.*

Exercise 11.21. *Do the missing moment computations, for these latter laws.*

As bonus exercise, work hard on week-ends, and with the money, buy a computer.

CHAPTER 12

Beta distributions

12a. Gamma function

As a continuation of what we learned in the previous chapter, we would like to discuss now some more specialized distributions, called beta binomial distributions.

However, introducing these distributions requires a substantial number of preliminaries. Let us start with the following basic fact, which is something elementary:

THEOREM 12.1. *The following integral converges for any real number $s > 0$,*

$$\Gamma(s) = \int_0^\infty x^{s-1} e^{-x}\, dx$$

satisfies $\Gamma(s+1) = s\Gamma(s)$, and extends the usual factorial, $\Gamma(n) = (n-1)!$ for $n \in \mathbb{N}$.

PROOF. There are several assertions here, the idea being as follows:

(1) Regarding the convergence claim, the integral converges at ∞, due to the presence of the exponential, and converges at 0 too, because x^{s-1} with $s > 0$ is integrable at 0.

(2) Next, by partial integration we have the following formula, as claimed:

$$\begin{aligned}
\Gamma(s+1) &= \int_0^\infty x^s e^{-x}\, dx \\
&= \int_0^\infty s x^{s-1} e^{-x}\, dx \\
&= s\Gamma(s)
\end{aligned}$$

(3) Regarding now the case $n \in \mathbb{N}$, for the initial value $n = 1$ we have:

$$\Gamma(1) = \int_0^\infty e^{-x} dx = 1$$

Thus, by recurrence we obtain $\Gamma(n) = (n-1)!$ for any $n \in \mathbb{N}$, as claimed. □

The above result is something quite magic, because it allows to talk about the factorial of any real number $n > 0$, according to the following formula:

$$n! = \Gamma(n+1)$$

Many interesting things can be said about the gamma function, notably with an explicit computation at the half-integers, which leads to the following result:

THEOREM 12.2. *The gamma function is given at half-integers by*

$$\Gamma(n) = (n-1)! \quad , \quad \Gamma\left(n+\frac{1}{2}\right) = \frac{(2n)!!}{2^n}\sqrt{\pi}$$

and we have the following almost uniform formula for it, valid for any $N \in \mathbb{N}$,

$$\Gamma\left(\frac{N}{2}\right) = \frac{(N-1)!!}{2^{(N-1)/2}}\, c$$

with $M!! = (M-1)(M-3)\ldots$ as usual, and $c = \sqrt{2}, \sqrt{\pi}$ for N even, odd.

PROOF. There are several things going on here, the idea being as follows:

(1) Regarding the first formula, values of the gamma function at the positive integers, we know indeed, from Theorem 12.1, that for $n \in \mathbb{N}$ we have:

$$\Gamma(n) = (n-1)!$$

(2) Regarding now the half-integers, we first have the following computation:

$$\begin{aligned}
\Gamma\left(\frac{1}{2}\right) &= \int_0^\infty x^{-1/2} e^{-x}\, dx \\
&= \int_0^\infty y^{-1} e^{-y^2} 2y\, dy \\
&= 2\int_0^\infty e^{-y^2}\, dy \\
&= 2 \times \frac{\sqrt{\pi}}{2} \\
&= \sqrt{\pi}
\end{aligned}$$

Next, by using the formula $\Gamma(s+1) = s\Gamma(s)$, we have the following computations:

$$\Gamma\left(\frac{3}{2}\right) = \frac{1}{2}\,\Gamma\left(\frac{1}{2}\right) = \frac{1}{2}\sqrt{\pi}$$

$$\Gamma\left(\frac{5}{2}\right) = \frac{3}{2}\,\Gamma\left(\frac{3}{2}\right) = \frac{3}{4}\sqrt{\pi}$$

$$\Gamma\left(\frac{7}{2}\right) = \frac{5}{2}\,\Gamma\left(\frac{5}{2}\right) = \frac{15}{8}\sqrt{\pi}$$

$$\vdots$$

Thus, we can solve the problem by recurrence, and we obtain in this way, with our usual convention $N!! = (N-1)(N-3)(N-5)\ldots$ for the double factorials:

$$\begin{aligned}\Gamma\left(n+\frac{1}{2}\right) &= \frac{2n-1}{2}\cdot\frac{2n-3}{2}\cdots\frac{5}{2}\cdot\frac{3}{2}\cdot\frac{1}{2}\,\Gamma\left(\frac{1}{2}\right)\\ &= \frac{1.3.5\ldots(2n-1)}{2^n}\sqrt{\pi}\\ &= \frac{(2n)!!}{2^n}\sqrt{\pi}\end{aligned}$$

(3) Regarding now the unification of the formulae that we have in (1) and (2), let us first rewrite the formula that we just found in (2), in the following way:

$$\Gamma\left(\frac{2n+1}{2}\right)=\frac{(2n)!!}{2^n}\sqrt{\pi}$$

Which looks good and in final form, no questions about this, so for a unification we are left with refurbishing the nice formula found in (1), in the following way:

$$\begin{aligned}\Gamma\left(\frac{2n}{2}\right) &= \Gamma(n)\\ &= (n-1)!\\ &= \frac{2.4.6\ldots(2n-2)}{2^{n-1}}\\ &= \frac{(2n-1)!!}{2^{n-1}}\\ &= \frac{(2n-1)!!}{2^{n-1/2}}\sqrt{2}\end{aligned}$$

And with this, job done, we are led to the uniform formula in the statement. □

As an interesting comment now, the above formulae are related to the well-known formulae for the volumes of spheres. In order to discuss this, let us start with:

PROPOSITION 12.3. *We have the following formulae,*

$$\int_0^{\pi/2}\cos^p t\,dt=\int_0^{\pi/2}\sin^p t\,dt=\left(\frac{\pi}{2}\right)^{\varepsilon(p)}\frac{p!!}{(p+1)!!}$$

where $\varepsilon(p)=1$ if p is even, and $\varepsilon(p)=0$ if p is odd, and where

$$m!!=(m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 if m is odd, and ending at 1 if m is even.

PROOF. Let us first compute the integral on the left I_p. We have:

$$\begin{aligned}(\cos^p t\sin t)' &= p\cos^{p-1}t(-\sin t)\sin t+\cos^p t\cos t\\ &= p\cos^{p+1}t-p\cos^{p-1}t+\cos^{p+1}t\\ &= (p+1)\cos^{p+1}t-p\cos^{p-1}t\end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain the following formula:

$$(p+1)I_{p+1}=pI_{p-1}$$

Thus we can compute I_p by recurrence, and we obtain:

$$\begin{aligned}I_p &= \frac{p-1}{p}\,I_{p-2}\\ &= \frac{p-1}{p}\cdot\frac{p-3}{p-2}\,I_{p-4}\\ &= \frac{p-1}{p}\cdot\frac{p-3}{p-2}\cdot\frac{p-5}{p-4}\,I_{p-6}\\ &\vdots\\ &= \frac{p!!}{(p+1)!!}\,I_{1-\varepsilon(p)}\end{aligned}$$

Thus, we obtain the result, by recurrence. As for the second formula, regarding $\sin t$, this follows from the first formula, with the change of variables $t=\frac{\pi}{2}-s$. □

More generally now, we have the following result:

THEOREM 12.4. *We have the following formula,*

$$\int_0^{\pi/2}\cos^p t\sin^q t\,dt=\left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)}\frac{p!!q!!}{(p+q+1)!!}$$

where $\varepsilon(p)=1$ if p is even, and $\varepsilon(p)=0$ if p is odd, and where

$$m!!=(m-1)(m-3)(m-5)\ldots$$

with the product ending at 2 if m is odd, and ending at 1 if m is even.

PROOF. Let I_{pq} be the integral in the statement. In order to do the partial integration, a bit as we previously did at $p=0$ or $q=0$, observe that we have:

$$\begin{aligned}(\cos^p t\sin^q t)' &= p\cos^{p-1}t(-\sin t)\sin^q t\\ &+ \cos^p t\cdot q\sin^{q-1}t\cos t\\ &= -p\cos^{p-1}t\sin^{q+1}t+q\cos^{p+1}t\sin^{q-1}t\end{aligned}$$

By integrating between 0 and $\pi/2$, we obtain, for $p,q>0$:

$$pI_{p-1,q+1}=qI_{p+1,q-1}$$

Thus, we can compute I_{pq} by recurrence. When q is even we have:

$$\begin{aligned} I_{pq} &= \frac{q-1}{p+1} I_{p+2,q-2} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} I_{p+4,q-4} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} \cdot \frac{q-5}{p+5} I_{p+6,q-6} \\ &= \vdots \\ &= \frac{p!!q!!}{(p+q)!!} I_{p+q} \end{aligned}$$

But the last term comes from Proposition 12.3, and we obtain the result:

$$\begin{aligned} I_{pq} &= \frac{p!!q!!}{(p+q)!!} I_{p+q} \\ &= \frac{p!!q!!}{(p+q)!!} \left(\frac{\pi}{2}\right)^{\varepsilon(p+q)} \frac{(p+q)!!}{(p+q+1)!!} \\ &= \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)} \frac{p!!q!!}{(p+q+1)!!} \end{aligned}$$

Observe that this gives the result for p even as well, by symmetry. Indeed, we have $I_{pq} = I_{qp}$, by using the following change of variables:

$$t = \frac{\pi}{2} - s$$

In the remaining case now, where both p, q are odd, we can use once again the formula $pI_{p-1,q+1} = qI_{p+1,q-1}$ established above, and the recurrence goes as follows:

$$\begin{aligned} I_{pq} &= \frac{q-1}{p+1} I_{p+2,q-2} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} I_{p+4,q-4} \\ &= \frac{q-1}{p+1} \cdot \frac{q-3}{p+3} \cdot \frac{q-5}{p+5} I_{p+6,q-6} \\ &= \vdots \\ &= \frac{p!!q!!}{(p+q-1)!!} I_{p+q-1,1} \end{aligned}$$

In order to compute the last term, observe that we have:

$$\begin{aligned} I_{p1} &= \int_0^{\pi/2} \cos^p t \sin t \, dt \\ &= -\frac{1}{p+1} \int_0^{\pi/2} (\cos^{p+1} t)' \, dt \\ &= \frac{1}{p+1} \end{aligned}$$

Thus, we can finish our computation in the case p, q odd, as follows:

$$\begin{aligned} I_{pq} &= \frac{p!!q!!}{(p+q-1)!!} I_{p+q-1,1} \\ &= \frac{p!!q!!}{(p+q-1)!!} \cdot \frac{1}{p+q} \\ &= \frac{p!!q!!}{(p+q+1)!!} \end{aligned}$$

Thus, we obtain the formula in the statement, the exponent of $\pi/2$ appearing there being $\varepsilon(p)\varepsilon(q) = 0 \cdot 0 = 0$ in the present case, and this finishes the proof. □

Getting now to the volumes of the spheres, we have the following result:

THEOREM 12.5. *The volume of the unit sphere in $\mathbb{R}^N$ is given by*

$$V = \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^N}{(N+1)!!}$$

with the convention

$$N!! = (N-1)(N-3)(N-5)\ldots$$

with the product ending at 2 if N is odd, and ending at 1 if N is even.

PROOF. Let us denote by B^+ the positive part of the unit sphere, or rather unit ball B, obtained by cutting this unit ball in 2^N parts. At the level of volumes, we have:

$$V = 2^N V^+$$

We have the following computation, using spherical coordinates:

$$\begin{aligned}
V^+ &= \int_{B^+} 1 \\
&= \int_0^1 \int_0^{\pi/2} \ldots \int_0^{\pi/2} r^{N-1} \sin^{N-2} t_1 \ldots \sin t_{N-2}\, dr dt_1 \ldots dt_{N-1} \\
&= \int_0^1 r^{N-1}\, dr \int_0^{\pi/2} \sin^{N-2} t_1\, dt_1 \ldots \int_0^{\pi/2} \sin t_{N-2} dt_{N-2} \int_0^{\pi/2} 1 dt_{N-1} \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{(N-2)!!}{(N-1)!!} \cdot \frac{(N-3)!!}{(N-2)!!} \ldots \frac{2!!}{3!!} \cdot \frac{1!!}{2!!} \cdot 1 \\
&= \frac{1}{N} \times \left(\frac{\pi}{2}\right)^{[N/2]} \times \frac{1}{(N-1)!!} \\
&= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{1}{(N+1)!!}
\end{aligned}$$

Here we have used the following formula for computing the exponent of $\pi/2$, where $\varepsilon(r) = 1$ if r is even and $\varepsilon(r) = 0$ if r is odd, as in Theorem 12.4:

$$\begin{aligned}
\varepsilon(0) + \varepsilon(1) + \varepsilon(2) + \ldots + \varepsilon(N-2) &= 1 + 0 + 1 + 0 + \ldots + \varepsilon(N-2) \\
&= \left[\frac{N-2}{2}\right] + 1 \\
&= \left[\frac{N}{2}\right]
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

As main particular cases of the above formula, we have:

PROPOSITION 12.6. *The volumes of the low-dimensional spheres are as follows:*

(1) *At $N = 1$, the length of the unit interval is $V = 2$.*
(2) *At $N = 2$, the area of the unit disk is $V = \pi$.*
(3) *At $N = 3$, the volume of the unit sphere is $V = \frac{4\pi}{3}$*
(4) *At $N = 4$, the volume of the corresponding unit sphere is $V = \frac{\pi^2}{2}$.*

PROOF. These formulae, which are all well-known, are all particular cases of the formula in Theorem 12.5, with the computations being as follows:

(1) At $N = 1$ we obtain $V = (\pi/2)^0 \cdot 2/1 = 2$.

(2) At $N = 2$ we obtain $V = (\pi/2)^1 \cdot 4/2 = \pi$.

(3) At $N = 3$ we obtain $V = (\pi/2)^1 \cdot 8/3 = 4\pi/3$.

(4) At $N = 4$ we obtain $V = (\pi/2)^2 \cdot 16/8 = \pi^2/2$. □

We can compute in the same way the area of the sphere, as follows:

THEOREM 12.7. *The area of the unit sphere in $\mathbb{R}^N$ is given by*

$$A=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^N}{(N-1)!!}$$

with the our usual convention for double factorials, namely:

$$N!!=(N-1)(N-3)(N-5)\ldots$$

In particular, at $N=2,3,4$ we obtain respectively $A=2\pi,4\pi,2\pi^2$.

PROOF. Regarding the first assertion, there is no need to compute again, because the formula in the statement can be deduced from Theorem 12.5, as follows:

(1) We can either use a standard "pizza" argument, as in 2D, which shows that the area and volume of the sphere in $\mathbb{R}^N$ are related by the following formula:

$$A=N\cdot V$$

(2) Or, we can start the computation in the same way as we started the proof of Theorem 12.5, the beginning of this computation being as follows:

$$vol(S^+)=\int_0^{\pi/2}\ldots\int_0^{\pi/2}\sin^{N-2}t_1\ldots\sin t_{N-2}\,dt_1\ldots dt_{N-1}$$

Now by comparing with the beginning of the proof of Theorem 12.5, the only thing that changes is the following quantity, which now dissapears:

$$\int_0^1 r^{N-1}\,dr=\frac{1}{N}$$

Thus, we have $vol(S^+)=N\cdot vol(B^+)$, and so we obtain the following formula:

$$vol(S)=N\cdot vol(B)$$

But this means $A=N\cdot V$, and together with the formula in Theorem 12.5 for V, this gives the result. As for the last assertion, this can be either worked out directly, or deduced from the results for volumes that we have so far, by multiplying by N. □

Getting back now to the gamma function, we have the following result:

THEOREM 12.8. *The volume and area of the unit sphere in $\mathbb{R}^N$, given by*

$$V=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^N}{(N+1)!!}\quad,\quad A=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^N}{(N-1)!!}$$

can be expressed in terms of the gamma function, the formulae being

$$V=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^{(N-1)/2}c}{\Gamma(N/2+1)}\quad,\quad A=\left(\frac{\pi}{2}\right)^{[N/2]}\frac{2^{(N+1)/2}c}{\Gamma(N/2)}$$

with $c=\sqrt{2},\sqrt{\pi}$ for N even, odd, as before.

PROOF. There are several things going on here, the idea being as follows:

(1) The first formulae of V, A are something that we know, from Theorems 12.5 and 12.7. Getting now to the second series of formulae, involving gamma, recall from Theorem 12.2 that we have the following formula, with $c = \sqrt{2}, \sqrt{\pi}$ for N even, odd:

$$\Gamma\left(\frac{N}{2}\right) = \frac{(N-1)!!}{2^{(N-1)/2}}\, c$$

Thus, the double factorials can be expresed as follows, in terms of gamma:

$$(N-1)!! = \frac{2^{(N-1)/2}}{c}\, \Gamma\left(\frac{N}{2}\right)$$

(2) But with this in hand, the previous volume formula for the sphere becomes:

$$\begin{aligned} V &= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^N}{(N+1)!!} \\ &= \left(\frac{\pi}{2}\right)^{[N/2]} 2^N \cdot \frac{c}{2^{(N+1)/2}} \cdot \frac{1}{\Gamma(N/2+1)} \\ &= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^{(N-1)/2} c}{\Gamma(N/2+1)} \end{aligned}$$

As for the formula for the area of the sphere, this becomes, again as claimed:

$$\begin{aligned} A &= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^N}{(N-1)!!} \\ &= \left(\frac{\pi}{2}\right)^{[N/2]} 2^N \cdot \frac{c}{2^{(N-1)/2}} \cdot \frac{1}{\Gamma(N/2)} \\ &= \left(\frac{\pi}{2}\right)^{[N/2]} \frac{2^{(N+1)/2} c}{\Gamma(N/2)} \end{aligned}$$

(3) Time perhaps for some numerics? At $N = 2$ we have $c = \sqrt{2}$, and we get:

$$V = \frac{\pi}{2} \cdot \frac{\sqrt{2} \cdot \sqrt{2}}{\Gamma(2)} = \pi \quad , \quad A = \frac{\pi}{2} \cdot \frac{2\sqrt{2} \cdot \sqrt{2}}{\Gamma(1)} = 2\pi$$

Also, at $N = 3$ we have $c = \sqrt{\pi}$, and we obtain, again as we should:

$$V = \frac{\pi}{2} \cdot \frac{2 \cdot \sqrt{\pi}}{3\sqrt{\pi}/4} = \frac{4\pi}{3} \quad , \quad A = \frac{\pi}{2} \cdot \frac{4 \cdot \sqrt{\pi}}{\sqrt{\pi}/2} = 4\pi$$

(4) Thus, formulae proved and doublechecked. And with the remark, however, that the original formulae, in terms of double factorials, are quite often better in practice. □

As a last piece of mathematics regarding the gamma function, we have:

THEOREM 12.9. *The gamma function is given at half-integers by*

$$\Gamma(n) \simeq \left(\frac{n}{e}\right)^n \sqrt{\frac{2\pi}{n}} \quad , \quad \Gamma\left(n+\frac{1}{2}\right) \simeq \left(\frac{n}{e}\right)^n \sqrt{2\pi}$$

and we have the following uniform approximation formula for it,

$$\Gamma\left(\frac{N}{2}\right) \simeq \left(\frac{N}{2e}\right)^{N/2} \sqrt{\frac{4\pi}{N}}$$

valid for $N \in \mathbb{N}$, in the $N \to \infty$ limit.

PROOF. This is very standard, based on the formulae in Theorem 12.2:

(1) At the usual integers $n \in \mathbb{N}$ we have the following Stirling estimate:

$$\begin{aligned}
\Gamma(n) &= (n-1)! \\
&\simeq \left(\frac{n-1}{e}\right)^{n-1} \sqrt{2\pi(n-1)} \\
&= \left(\frac{n}{e}\right)^{n-1} \left(\frac{n-1}{n}\right)^{n-1} \sqrt{2\pi(n-1)} \\
&\simeq \left(\frac{n}{e}\right)^{n-1} \frac{\sqrt{2\pi n}}{e} \\
&= \left(\frac{n}{e}\right)^n \sqrt{\frac{2\pi}{n}}
\end{aligned}$$

(2) At the half-integers, $n+1/2$ with $n \in \mathbb{N}$, we have the following estimate:

$$\begin{aligned}
\Gamma\left(n+\frac{1}{2}\right) &= \frac{(2n)!!}{2^n}\sqrt{\pi} \\
&= \frac{(2n)!}{4^n n!}\sqrt{\pi} \\
&\simeq \left(\frac{2n}{e}\right)^{2n} \sqrt{4\pi n}\left(\frac{e}{n}\right)^n \frac{1}{\sqrt{2\pi n}} \cdot \sqrt{\pi} \\
&= \left(\frac{n}{e}\right)^n \sqrt{2\pi}
\end{aligned}$$

(3) Regarding the uniform formula, with $N = 2n$ the estimate in (1) reads:

$$\Gamma\left(\frac{N}{2}\right) \simeq \left(\frac{N}{2e}\right)^{N/2} \sqrt{\frac{4\pi}{N}}$$

(4) Also, with $N=2n+1$, the estimate that we found in (2) reads:

$$\begin{aligned}\Gamma\left(\frac{N}{2}\right) &\simeq \left(\frac{N-1}{2e}\right)^{(N-1)/2}\sqrt{2\pi}\\ &= \left(\frac{N}{2e}\right)^{(N-1)/2}\left(\frac{N-1}{N}\right)^{(N-1)/2}\sqrt{2\pi}\\ &\simeq \left(\frac{N}{2e}\right)^{(N-1)/2}\sqrt{\frac{2\pi}{e}}\\ &\simeq \left(\frac{N}{2e}\right)^{N/2}\sqrt{\frac{4\pi}{N}}\end{aligned}$$

We are therefore led to the uniform formula in the statement.

(5) Finally, let us mention that the uniform approximation formula that we found works in fact in general, with the formula being as follows, for $s>>0$:

$$\Gamma(s)\simeq\left(\frac{s}{e}\right)^s\sqrt{\frac{2\pi}{s}}$$

And we will leave some further learning here as an exercise. □

Many other things can be said about the gamma function, some in relation with the usual factorial of the integers, and some other being analysis specific. We will be back to this, in what follows. For the moment, what we have in the above will do.

12b. Beta distributions

Good news, we can talk now about the beta binomial distributions, that we wanted to talk about, in this chapter. These distributions are defined as follows:

DEFINITION 12.10. *The beta binomial distributions are given by*

$$P(s)=\binom{n}{s}\frac{B(s+a,n-s+b)}{B(a,b)}$$

with B being the beta function, defined as follows,

$$B(a,b)=\frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

with Γ being the gamma function.

As a first comment, such things obviously look like something quite specialized, that will probably take us some time to digest. So, let us get now into this, understanding what Definition 12.10 exactly says, and no hurry with anything, of course.

We first have the following fact, which is the key to understanding all this:

PROPOSITION 12.11. *At integer values of the parameters, $a, b \in \mathbb{N}$, we have*

$$P(s) = \frac{\binom{s+a-1}{s}\binom{n-s+b-1}{n-s}}{\binom{n+a+b-1}{n}}$$

and our beta binomial distribution is a negative hypergeometric law.

PROOF. We recall from Theorem 12.1 that for the integers $n \in \mathbb{N}$, we have:

$$\Gamma(n) = (n-1)!$$

Thus, at integer values of the parameters a, b, the beta function is given by:

$$B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} = \frac{(a-1)!(b-1)!}{(a+b-1)!}$$

By using this, the formula of the beta binomial distribution is as follows:

$$\begin{aligned} P(s) &= \binom{n}{s}\frac{B(s+a,n-s+b)}{B(a,b)} \\ &= \frac{n!}{s!(n-s)!}\cdot\frac{(s+a-1)!(n-s+b-1)!}{(n+a+b-1)!}\cdot\frac{(a+b-1)!}{(a-1)!(b-1)!} \\ &= \frac{n!(a+b-1)!}{(n+a+b-1)!}\cdot\frac{(s+a-1)!}{s!(a-1)!}\cdot\frac{(n-s+b-1)!}{(n-s)!(b-1)!} \\ &= \frac{\binom{s+a-1}{s}\binom{n-s+b-1}{n-s}}{\binom{n+a+b-1}{n}} \end{aligned}$$

But this is a negative hypergeometric law, of parameters as follows:

$$(N,m,r) = (n+a+b-1,n,a)$$

Thus, we are led to the conclusion in the statement. □

We can see now the interest in Definition 12.10, the point being that, in certain situations where the negative hypergeometric laws do not produce accurate results, we can use the beta binomial distributions, instead. It is possible to be a bit more precise here, the idea being that the uniform sampling used in chapter 11 in order to define the negative hypergeometric laws can be replaced with a sampling based on a continuous beta distribution, and this is what produces the beta binomial laws from Definition 12.10.

However, all this remains something quite complicated, going beyond the purposes of the present book. So, let us summarize this discussion as follows, and for more regarding the phenomenology of the beta binomial laws, recommend a solid statistics book:

FACT 12.12. *The beta binomial distributions are useful in advanced statistics, as a handy technical version of the negative hypergeometric laws.*

In what follows we will be mostly interested in the abstract mathematics of the beta binomial laws, which is something quite interesting. So, as a continuation of Proposition 12.11, let us see what happens when the parameters a, b are half-integers. We have:

THEOREM 12.13. *At half-integer parameters, $a, b \in \mathbb{N}/2$, we still have the formula*

$$P(s) = \frac{\binom{s+a-1}{s}\binom{n-s+b-1}{n-s}}{\binom{n+a+b-1}{n}}$$

with the following convention for the quantities in brackets,

$$\binom{n}{k} = \frac{(2n+1)!!}{(2k+1)!!(2n-2k+1)!!}$$

where $M!! = (M-1)(M-3)\ldots$ for any integer $M \in \mathbb{N}$, as usual.

PROOF. This is something standard, based on Theorem 12.2, as follows:

(1) To start with, we have the following formula, valid for any $n \in \mathbb{N}$:

$$n! = \frac{(2n+1)!!}{2^n}$$

Thus, at $n, k \in \mathbb{N}$, the quantities in brackets in the statement are indeed binomials:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{(2n+1)!!}{(2k+1)!!(2n-2k+1)!!}$$

(2) Next, we recall from Theorem 12.2 that we have the following formula for the gamma function at the half-integers, with $c = \sqrt{2}, \sqrt{\pi}$ for N even, odd:

$$\Gamma\left(\frac{N}{2}\right) = \frac{(N-1)!!}{2^{(N-1)/2}}\, c$$

Thus, at half-integer values of the parameters, $a, b \in \mathbb{N}/2$, say $a = A/2$ and $b = B/2$ with $A, B \in \mathbb{N}$, the beta function is given by the following formula:

$$\begin{aligned}
B(a,b) &= \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)} \\
&= \frac{\Gamma(A/2)\Gamma(B/2)}{\Gamma((A+B)/2)} \\
&= \frac{(A-1)!!}{2^{(A-1)/2}}\, c_A \cdot \frac{(B-1)!!}{2^{(B-1)/2}}\, c_B \cdot \frac{2^{(A+B-1)/2}}{(A+B-1)!!} \cdot \frac{1}{c_{A+B}} \\
&= \frac{(A-1)!!(B-1)!!}{(A+B-1)!!} \cdot \frac{\sqrt{2}c_A c_B}{c_{A+B}}
\end{aligned}$$

(3) By using now (1) and (2), the formula of the beta binomial distribution is:

$$\begin{aligned}
P(s) &= \binom{n}{s}\frac{B(s+a,n-s+b)}{B(a,b)}\\
&= \frac{(2n+1)!!}{(2s+1)!!(2n-2s+1)!!}\cdot\frac{(2s+A-1)!!(2n-2s+B-1)!!}{(2n+A+B-1)!!}\cdot\frac{\sqrt{2}c_Ac_B}{c_{A+B}}\\
&\quad\cdot\frac{(A+B-1)!!}{(A-1)!!(B-1)!!}\cdot\frac{c_{A+B}}{\sqrt{2}c_Ac_B}\\
&= \frac{(2n+1)!!(2s+A-1)!!(2n-2s+B-1)!!(A+B-1)!!}{(2s+1)!!(2n-2s+1)!!(2n+A+B-1)!!(A-1)!!(B-1)!!}\\
&= \frac{(2n+1)!!(A+B-1)!!}{(2n+A+B-1)!!}\cdot\frac{(2s+A-1)!!}{(2s+1)!!(A-1)!!}\cdot\frac{(2n-2s+B-1)!!}{(2n-2s+1)!!(B-1)!!}\\
&= \frac{\binom{s+a-1}{s}\binom{n-s+b-1}{n-s}}{\binom{n+a+b-1}{n}}
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Getting now the study of the beta binomial distributions in general, as introduced in Definition 12.10, as a first job for us, let us verify that we have indeed are probability measures, of mass 1. For this purpose, we will need the following standard fact:

PROPOSITION 12.14. *We have the following formula,*

$$\sum_{s=0}^{n}\binom{n}{s}B(s+a,n-s+b)=B(a,b)$$

generalizing the usual Vandermonde formula for binomials.

PROOF. This is very standard, as for the usual Vandermonde formula, as follows:

(1) At $n=0$ the formula to be proved is $B(a,b)=B(a,b)$, true.

(2) At $n=1$ now, the formula to be proved is as follows, called Pascal formula:

$$B(a,b+1)+B(a+1,b)=B(a,b)$$

But this can be proved by using the identity $\Gamma(s+1)=s\Gamma(s)$, as follows:

$$\begin{aligned}
B(a,b+1)+B(a+1,b) &= \frac{\Gamma(a)\Gamma(b+1)}{\Gamma(a+b+1)}+\frac{\Gamma(a+1)\Gamma(b)}{\Gamma(a+b+1)}\\
&= \frac{b\Gamma(a)\Gamma(b)}{(a+b)\Gamma(a+b)}+\frac{a\Gamma(a)\Gamma(b)}{(a+b)\Gamma(a+b)}\\
&= \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}\\
&= B(a,b)
\end{aligned}$$

(3) At $n = 2$ now, the formula to be proved is as follows:

$$B(a, b + 2) + 2B(a + 1, b + 1) + B(a + 2, b) = B(a, b)$$

But this can be proved by using the above Pascal formula three times, as follows:

$$\begin{aligned} & B(a, b + 2) + 2B(a + 1, b + 1) + B(a + 2, b) \\ = \ & [B(a, b + 2) + B(a + 1, b + 1)] + [B(a + 1, b + 1) + B(a + 2, b)] \\ = \ & B(a, b + 1) + B(a + 1, b) \\ = \ & B(a, b) \end{aligned}$$

(4) And so on, with the general case following by iterating Pascal, as above. □

Good news, we can now complement Definition 12.10 with:

PROPOSITION 12.15. *The beta binomial distributions, given by*

$$P(s) = \binom{n}{s} \frac{B(s + a, n - s + b)}{B(a, b)} \quad , \quad B(a, b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a + b)}$$

are indeed probability distributions, of mass 1*, as they should.*

PROOF. We have indeed the following computation, using Proposition 12.14:

$$\begin{aligned} \sum_{s=0}^{n} P(s) &= \sum_{s=0}^{n} \binom{n}{s} \frac{B(s + a, n - s + b)}{B(a, b)} \\ &= \frac{1}{B(a, b)} \sum_{s=0}^{n} \binom{n}{s} B(s + a, n - s + b) \\ &= \frac{B(a, b)}{B(a, b)} \\ &= 1 \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Regarding now the mean and variance of the beta binomial laws, we have:

THEOREM 12.16. *The mean and variance of the beta binomial laws are*

$$E = \frac{na}{a + b} \quad , \quad V = \frac{nab(n + a + b)}{(a + b)^2(a + b + 1)}$$

in terms of the parameters (n, a, b)*.*

PROOF. This is something quite straightforward, the idea being as follows:

(1) We recall from chapter 11 that the computation of the mean for the negative hypergeometric laws was based on the following trick, and the Vandermonde formula:

$$s = (s + r) - r$$

To be more precise, in terms of our new parameters (n, a, b) here, which are given by $(N, m, r) = (n + a + b - 1, n, a)$ the computation from chapter 11 was as follows:

$$\begin{aligned}
E &= \sum_s s \frac{\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}}{\binom{n+a+b-1}{n}} \\
&= \sum_s [(s+a)-a] \frac{\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}}{\binom{n+a+b-1}{n}} \\
&= \left[\sum_s (s+a) \frac{\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}}{\binom{n+a+b-1}{n}}\right] - a \\
&= \frac{a}{\binom{n+a+b-1}{n}} \left[\sum_s \frac{s+a}{a}\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}\right] - a \\
&= \frac{a}{\binom{n+a+b-1}{n}} \left[\sum_s \binom{s+a}{s}\binom{n+b-s-1}{n-s}\right] - a \\
&= \frac{a}{\binom{n+a+b-1}{n}} \binom{n+a+b}{n} - a \\
&= a \cdot \frac{n!(a+b-1)!}{(n+a+b-1)!} \cdot \frac{(n+a+b)!}{n!(a+b)!} - a \\
&= \frac{(n+a+b)a}{a+b} - a \\
&= \frac{na}{a+b}
\end{aligned}$$

But the same trick works in general, at any $a, b > 0$, by using the generalized Vandermonde formula from Proposition 12.14 for the summation, as desired.

(2) Next, again by following the material in chapter 11, corresponding to the case $a, b \in \mathbb{N}$, in order to compute $M_2 - M_1$, we can use a similar trick, as follows:

$$s^2 - s = (s+r)(s+r+1) - 2(r+1)(s+r) + r(r+1)$$

To be more precise, in terms of our new parameters (n, a, b) here, which are given by $(N, m, r) = (n + a + b - 1, n, a)$ the computation from chapter 11 was as follows:

$$\begin{aligned}
& M_2 - M_1 \\
= \; & \sum_s (s^2 - s) \frac{\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}}{\binom{n+a+b-1}{n}} \\
= \; & \sum_s [(s+a)(s+a+1) - 2(a+1)(s+a) + a(a+1)] \frac{\binom{s+a-1}{s}\binom{n+b-s-1}{n-s}}{\binom{n+a+b-1}{n}} \\
= \; & \frac{1}{\binom{n+a+b-1}{n}} \sum_s (s+a)(s+a+1) \binom{s+a-1}{s}\binom{n+b-s-1}{n-s} \\
& - \frac{2(a+1)}{\binom{n+a+b-1}{n}} \sum_s (s+a) \binom{s+a-1}{s}\binom{n+b-s-1}{n-s} + a(a+1) \\
= \; & \frac{a(a+1)}{\binom{n+a+b-1}{n}} \sum_s \binom{s+a+1}{s}\binom{n+b-s-1}{n-s} \\
& - \frac{2a(a+1)}{\binom{n+a+b-1}{n}} \sum_s \binom{s+a}{s}\binom{n+b-s-1}{n-s} + a(a+1) \\
= \; & \frac{a(a+1)}{\binom{n+a+b-1}{n}} \binom{n+a+b+1}{n} - \frac{2a(a+1)}{\binom{n+a+b-1}{n}} \binom{n+a+b}{n} + a(a+1) \\
= \; & a(a+1) \left[\frac{n!(a+b-1)!(n+a+b+1)!}{(n+a+b-1)!n!(a+b+1)!} - 2 \cdot \frac{n!(a+b-1)!(n+a+b)!}{(n+a+b-1)!n!(a+b)!} + 1 \right] \\
= \; & a(a+1) \left[\frac{(n+a+b)(n+a+b+1)}{(a+b)(a+b+1)} - 2 \cdot \frac{n+a+b}{a+b} + 1 \right] \\
= \; & a(a+1) \left[\frac{(n+a+b)(n+a+b+1)}{(a+b)(a+b+1)} - \frac{2n+a+b}{a+b} \right] \\
= \; & \frac{a(a+1)}{(a+b)(a+b+1)} [(n+a+b)(n+a+b+1) - (2n+a+b)(a+b+1)] \\
= \; & \frac{a(a+1)}{(a+b)(a+b+1)} (n^2 - n) \\
= \; & \frac{n(n-1)a(a+1)}{(a+b)(a+b+1)}
\end{aligned}$$

But the same trick works in general, at any $a, b > 0$, by using the generalized Vandermonde formula from Proposition 12.14 for the summation. Thus, we have $M_2 - M_1$.

(3) We conclude that the second moment is given by the following formula:

$$\begin{aligned} M_2 &= (M_2 - M_1) + M_1 \\ &= \frac{n(n-1)a(a+1)}{(a+b)(a+b+1)} + \frac{na}{a+b} \\ &= \frac{na(na+n+b)}{(a+b)(a+b+1)} \end{aligned}$$

(4) Getting now to the variance, this is given by the following formula:

$$\begin{aligned} V &= M_2 - M_1^2 \\ &= \frac{na(na+n+b)}{(a+b)(a+b+1)} - \frac{n^2a^2}{(a+b)^2} \\ &= \frac{nab(n+a+b)}{(a+b)^2(a+b+1)} \end{aligned}$$

Thus, we are led to the formulae in the statement. □

Summarizing, we have so far a beginning of understanding of the beta binomial distributions, as introduced in Definition 12.10. More to come, in what follows.

12c. Factorial moments

Regarding the higher moments, again in view of what we found in chapter 11 for the negative hypergeometric laws, things are more complicated. In order to deal with this question, let us introduce the following notion, which is something quite subtle:

DEFINITION 12.17. *The factorial moments of $f : X \to \mathbb{R}$ are the numbers*

$$\widetilde{M}_k = E[f(f-1)\ldots(f-k+1)]$$

with the convention $\widetilde{M}_0 = 1$.

As a first comment here, you would probably say, we already have moments M_k, central moments M'_k, and normalized central moments M''_k, so why complicating things with one more definition. In answer, there is some magic in Definition 12.17, the idea being that the normalization there "kills the underlying partitions".

As an illustration for this principle, for the Poisson law p_t, which is the central object in discrete probability theory, we have the following remarkable result:

THEOREM 12.18. *The factorial moments of the Poisson law p_t are*

$$\widetilde{M}_k = t^k$$

and with this being something infinitely simpler than the formula of M_k.

PROOF. This is something quite fundamental, which can be viewed in several ways, which are all worth learning, the idea with all this being as follows:

(1) A first approach is via limits of binomial laws. Indeed, for the binomial law b_{np} of parameters $n \in \mathbb{N}$ and $p \in [0,1]$, we have the following formula:

$$\begin{aligned}
\widetilde{M}_k(b_{np}) &= \sum_{s=k}^{n} s(s-1)\ldots(s-k+1)\binom{n}{s}p^s(1-p)^{n-s} \\
&= \sum_{s=k}^{n} \frac{s!}{(s-k)!}\cdot\frac{n!}{s!(n-s)!}\,p^s(1-p)^{n-s} \\
&= \sum_{s=k}^{n} \frac{n!}{(s-k)!(n-s)!}\,p^s(1-p)^{n-s} \\
&= \sum_{r=0}^{n-k} \frac{n!}{r!(n-k-r)!}\,p^{k+r}(1-p)^{n-k-r} \\
&= \frac{n!p^k}{(n-k)!}\sum_{r=0}^{n-k}\frac{(n-k)!}{r!(n-k-r)!}\,p^r(1-p)^{n-k-r} \\
&= \frac{n!p^k}{(n-k)!}\sum_{r=0}^{n-k}\binom{n-k}{r}p^r(1-p)^{n-k-r} \\
&= \frac{n!p^k}{(n-k)!}[p+(1-p)]^{k-r} \\
&= \frac{n!p^k}{(n-k)!}
\end{aligned}$$

Now recall from the Poisson Limit Theorem from chapter 8 that we have $b_{np} \to p_t$, when $p = t/n$ with $t > 0$ fixed. Thus, by doing a Poisson limit we obtain, as claimed:

$$\begin{aligned}
\widetilde{M}_k(p_t) &= \widetilde{M}_k\left(\lim_{n\to\infty} b_{n,t/n}\right) \\
&= \lim_{n\to\infty}\widetilde{M}_k(b_{n,t/n}) \\
&= \lim_{n\to\infty}\frac{n!(t/n)^k}{(n-k)!} \\
&= t^k\lim_{n\to\infty}\frac{n(n-1)\ldots(n-k+1)}{n^k} \\
&= t^k
\end{aligned}$$

(2) A second approach is via the moment formula for Poisson laws that we established in chapter 8, which was as follows, with $|.|$ being as usual the number of blocks:

$$M_k(p_t) = \sum_{\pi\in P(k)} t^{|\pi|}$$

Now in order to convert this into a formula regarding the factorial moments, we need a general conversion formula, connecting the usual and the factorial moments. So, recall from chapter 6 the following magic formula, valid for any number $s \in \mathbb{N}$:

$$\begin{aligned} s^k &= \sum_{i_1=1}^{s} \ldots \sum_{i_k=1}^{s} 1 \\ &= \sum_{\pi\in P(k)} \#\left\{(i_1,\ldots,i_k) \in \{1,\ldots,s\}^k \,\middle|\, \ker i = \pi\right\} \\ &= \sum_{\pi\in P(k)} \frac{s!}{(s-|\pi|)!} \end{aligned}$$

Now since this is an equality of polynomials in s, we can replace our $s \in \mathbb{N}$ by anything, and in particular, by an arbitrary random variable $f : X \to \mathbb{R}$. We obtain:

$$f^k = \sum_{\pi\in P(k)} f(f-1)\ldots(f-|\pi|+1)$$

By taking now the expectation, on both sides, we obtain the following conversion formula, connecting the usual and the factorial moments of a variable $f : X \to \mathbb{R}$:

$$M_k = \sum_{\pi\in P(k)} \widetilde{M}_{|\pi|}$$

But with this formula in hand, back to the Poisson law, we can convert our formula above for the moments of p_t into a formula for the factorial moments, and we obtain:

$$\widetilde{M}_k(p_t) = t^k$$

(3) Thus, one way or another, we are led to the formula in the statement. We will be back to such things later in this book, when discussing partitions and cumulants. □

Getting now to the negative hypergeometric laws, the result for them is:

THEOREM 12.19. *The factorial moments of the negative hypergeometric laws are*

$$\widetilde{M}_k = \frac{m!}{(m-k)!} \cdot \frac{r!}{(r-k)!} \cdot \frac{(N-k)!}{N!}$$

with (N, m, r) being as usual the parameters.

PROOF. We recall from chapter 11 that the moments of the negative hypergeometric law of parameters (N, m, r) are given by the following formula:

$$M_k = \sum_{\pi \in P(k)} \frac{m!}{(m - |\pi|)!} \cdot \frac{(r + |\pi| - 1)!}{(r - 1)!} \cdot \frac{(N - m)!}{(N - m + |\pi|)!}$$

Now recall from the proof of Theorem 12.18 that we have the following formula:

$$M_k = \sum_{\pi \in P(k)} \widetilde{M}_{|\pi|}$$

Thus, we are led via some combinatorics to the formula in the statement, namely:

$$\widetilde{M}_k = \frac{m!}{(m - k)!} \cdot \frac{r!}{(r - k)!} \cdot \frac{(N - k)!}{N!}$$

We will leave the details here as an exercise, and we will be back to such things later in this book, when discussing partitions and cumulants. □

Getting now to what we wanted to do, for the beta binomial distribution, we have:

THEOREM 12.20. *The factorial moments of the beta binomial distribution are*

$$\widetilde{M}_k = \frac{n!}{(n - k)!} \cdot \frac{B(a + k, b)}{B(a, b)}$$

with B being as usual the beta function.

PROOF. Many things can be said here, the idea being as follows:

(1) To start with, let us record the following more digest formulation of the moment formula in the statement, in terms of the gamma function only:

$$\begin{aligned} \widetilde{M}_k &= \frac{n!}{(n - k)!} \cdot \frac{B(a + k, b)}{B(a, b)} \\ &= \frac{n!}{(n - k)!} \cdot \frac{\Gamma(a + k)\Gamma(b)}{\Gamma(a + b + k)} \cdot \frac{\Gamma(a + b)}{\Gamma(a)\Gamma(b)} \\ &= \frac{n!}{(n - k)!} \cdot \frac{\Gamma(a + k)}{\Gamma(a)} \cdot \frac{\Gamma(a + b)}{\Gamma(a + b + k)} \end{aligned}$$

(2) Equivalently, by using the formula $\Gamma(s + 1) = s\Gamma(s)$ from Theorem 12.1, we have the following formula, directly in terms of the parameters $a, b > 0$:

$$\widetilde{M}_k = \frac{n(n - 1) \ldots (n - k + 1)a(a + 1) \ldots (a + k - 1)}{(a + b)(a + b + 1) \ldots (a + b + k - 1)}$$

(3) But with this we can see, as a first observation, that our formula fits with the moment formulae at $k = 1, 2$ from Theorem 12.16 and its proof, which were as follows:

$$\widetilde{M}_1 = \frac{na}{a+b} \quad , \quad \widetilde{M}_2 = \frac{n(n-1)a(a+1)}{(a+b)(a+b+1)}$$

(4) Next, in the case of integer parameters, what we have fits with the formula in Theorem 12.19, for the negative hypergeometric laws. Indeed, let us set:

$$(N, m, r) = (n + a + b - 1, n, a)$$

But with this, we obtain indeed the formulae from Theorem 12.19.

(5) In general now, this is indeed something quite standard, by using the various tricks from the proof of Theorem 12.16, exactly as for the negative hypergeometric laws. □

As a main application, we can now compute the skewness and kurtosis:

THEOREM 12.21. *For the beta binomial distribution we have*

$$\widetilde{M}_1 = \frac{na}{a+b}$$

$$\widetilde{M}_2 = \frac{n(n-1)a(a+1)}{(a+b)(a+b+1)}$$

$$\widetilde{M}_3 = \frac{n(n-1)(n-2)a(a+1)(a+2)}{(a+b)(a+b+1)(a+b+2)}$$

$$\widetilde{M}_4 = \frac{n(n-1)(n-2)(n-3)a(a+1)(a+2)(a+3)}{(a+b)(a+b+1)(a+b+2)(a+b+3)}$$

and this allows the computation of the corresponding skewness and kurtosis.

PROOF. This is indeed something self-explanatory, based on the general moment formula from Theorem 12.20, and I would leave the details to you, as an exercise. □

12d. Negative beta

As a last topic for this chapter, yes I know that it's late, but we still have a couple of things to do, we can talk as well about negative beta binomial laws, as follows:

DEFINITION 12.22. *The negative beta binomial distributions are given by*

$$P(s) = \frac{\Gamma(s+b)}{s!\Gamma(b)} \cdot \frac{B(s+r, a+b)}{B(r, a)}$$

with B being the beta function, defined as follows,

$$B(a, b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

with Γ being the gamma function.

Many things can be here, and as before for the usual beta binomial distributions, for more on the phenomenology of these laws, we refer to a solid statistics book.

In what follows we will just record a few useful formulae regarding these laws, by leaving the proofs as exercises. To start with, we have the following result:

PROPOSITION 12.23. *The negative beta binomial distribution, given by*

$$P(s) = \frac{\Gamma(s+b)}{s!\Gamma(b)} \cdot \frac{B(s+r, a+b)}{B(r,a)} \quad , \quad B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

is indeed a probability distribution, of mass 1*, as it should.*

PROOF. As mentioned above, this would be a good exercise for you. □

Regarding the mean of the negative beta binomial distributions, we have:

THEOREM 12.24. *The mean of the negative beta binomial law is given by*

$$E = \frac{rb}{a-1}$$

if $a > 1$*, and is* $E = \infty$ *otherwise.*

PROOF. Again, this would be a good exercise for you. □

Regarding the variance of the negative beta binomial distributions, we have:

THEOREM 12.25. *The variance of the negative beta binomial law is given by*

$$V = \frac{rb(r+a-1)(a+b-1)}{(a-1)^2(a-2)}$$

if $a > 2$*, and is* $E = \infty$ *otherwise.*

PROOF. This would be again a good exercise for you. □

Regarding the skewness of the negative beta binomial distributions, we have:

THEOREM 12.26. *The skewness of the negative beta binomial law is given by*

$$\gamma = \frac{(2r+a-1)(2b+a-1)}{(a-3)\sqrt{\frac{rb(r+a-1)(a+b-1)}{a-2}}}$$

if $a > 3$*, and is* $E = \infty$ *otherwise.*

PROOF. Again, this would be a good exercise for you. □

Finally, regarding the moments of negative beta binomial distributions, we have:

THEOREM 12.27. *The factorial moments of the negative beta binomial law are*

$$\widetilde{M}_k = \frac{\Gamma(r+k)\Gamma(a-k)\Gamma(b+k)}{\Gamma(r)\Gamma(a)\Gamma(b)}$$

with (r, a, b) *being as usual the parameters.*

PROOF. This would be again a good exercise for you, and with the remark of course that it would be smart to start with this, because you would get afterwards Proposition 12.23, Theorem 12.24, Theorem 12.25 and Theorem 12.26, coming for free. □

And with this, end of our discussion regarding the beta binomial laws, positive and negative. As already mentioned on several occasions, this was just a modest introduction to the subject, and for more on all this, we recommend a solid statistics book.

12e. Exercises

This was a quite technical chapter, and as exercises, all technical, we have:

EXERCISE 12.28. *Learn about the gamma function at* $z \in \mathbb{C}$*, with* $Re(z) > 0$ *or not.*

EXERCISE 12.29. *Learn the proof of the generalized Stirling formula, for gamma.*

EXERCISE 12.30. *Learn more about the phenomenology of the beta binomial laws.*

EXERCISE 12.31. *Learn more about the factorial moments, and their properties.*

EXERCISE 12.32. *Compute the skewness and kurtosis of the beta binomial laws.*

EXERCISE 12.33. *Learn about the phenomenology of negative beta binomial laws.*

EXERCISE 12.34. *Do the moment computations for the negative beta binomial laws.*

EXERCISE 12.35. *Compute the kurtosis of the negative beta binomial laws.*

As bonus exercise, quite frightening, read about hypergeometric functions.

Part IV

Advanced aspects

Viaje de Barein hasta Beirut
Fui desde el norte hasta el Polo Sur
Y no encontre ojos asi
Como los que tienes tu

CHAPTER 13

Random walks

13a. Random walks

We have learned so far the basics of probability theory, and time now to see if this knowledge can be of help, in relation with more advanced questions. Quite often this will lead us into continuous phenomena and probability, and our plan will be as follows:

(1) We will first investigate a very basic question, related to percolation and many more, namely random walks on graphs. And, we will discover that the case of the infinite graphs, leading to some interesting continuous laws, is in fact the simplest.

(2) Then we will investigate, as a continuation of our previous limiting results from Part II, the central limits, and the resulting bell-shaped curves. This will be a key study, bringing us into the fundamentals of continuous probability theory.

(3) With this done, we will systematically discuss then the moment combinatorics of the various laws that we have accumulated, namely the advanced discrete laws from Part III, and the continuous laws appearing from random walks, and central limits.

(4) Our study will suggest that, besides the usual dichotomies real/complex and discrete/continuous, there is a third dichotomy in probability, namely classical/free. And we will end with an introduction to this, freeness, explained via random matrices.

So, this will be the plan for the 4 chapters of the present Part IV, and as before with other such things, it is probably better for me to ask for some advice first. I am particularly worried about the order of (1) and (2), honestly, which comes first?

Going as usual for the rat, that we last met at the beginning of Part III, and who's done since then with quantum mechanics, now chewing through my thermodynamics and statistical mechanics books, what a disaster for my wallet, here is what he says:

RAT 13.1. *Classical mathematics is more complicated than free mathematics, appearing from it via some tricky thermodynamic limits.*

Okay, thanks rat, and not that I understand a single word from what you say, you are obviously far more advanced now, than both me and cats, who are rather into mild quantum, but I will take this as an encouragement, (1) most likely comes before (2).

Getting to work now, random walks on the menu, for this present chapter. The question that we would like to discuss, which is something very basic, is as follows:

QUESTION 13.2. *Given a graph X, with a distinguished vertex $*$:*

(1) *What is the number L_k of length k loops on X, based at $*$?*
(2) *Equivalently, what is the measure μ having L_k as moments?*

To be more precise, we are mainly interested in the first question, counting loops on graphs, with this being notoriously related to many applied mathematics questions, of discrete type. As for the second question, this is a technical, useful probabilistic reformulation of the first question, that we will usually prefer, in what follows.

In order to discuss this, let us start with some graph theory basics. We first have:

PROPOSITION 13.3. *A graph X, with vertices labeled $1, \ldots, N$, is uniquely determined by its adjacency matrix, which is the matrix $d \in M_N(0,1)$ given by:*

$$d_{ij} = \begin{cases} 1 & \text{if } i - j \\ 0 & \text{if } i \neq j \end{cases}$$

Moreover, the matrices $d \in M_N(0,1)$ which can appear in this way, from graphs, are precisely those which are symmetric, and have 0 on the diagonal.

PROOF. We have two things to be proved, the idea being as follows:

(1) Given a graph X, we can construct a matrix $d \in M_N(0,1)$ as in the statement, and this matrix is obviously symmetric, and has 0 on the diagonal.

(2) Conversely, given a matrix $d \in M_N(0,1)$ which is symmetric, and has 0 on the diagonal, we can associate to it the graph X having as vertices the numbers $1, \ldots, N$, and with the edges between these vertices being defined as follows:

$$i - j \iff d_{ij} = 1$$

It is then clear that the adjacency matrix of this graph X is the matrix d itself. Thus, we have established a correspondence $X \leftrightarrow d$, as in the statement. □

Getting now to the walks on graphs, this brings us into the mathematics of the corresponding adjacency matrix d, thanks to the following key observation:

PROPOSITION 13.4. *For a graph X, with adjacency matrix $d \in M_N(0,1)$, we have:*

$$(d^k)_{ij} = \#\Big\{i = i_0 - i_1 - \ldots - i_{k-1} - i_k = j\Big\}$$

That is, the k-th power of d describes the length k paths on X.

PROOF. According to the usual rule of matrix multiplication, the formula for the powers of the adjacency matrix $d \in M_N(0,1)$ is as follows:

$$\begin{aligned}(d^k)_{i_0 i_k} &= \sum_{i_1,\ldots,i_{k-1}} d_{i_0 i_1} d_{i_1 i_2} \ldots d_{i_{k-1} i_k} \\ &= \sum_{i_1,\ldots,i_{k-1}} \delta_{i_0 - i_1} \delta_{i_1 - i_2} \ldots \delta_{i_{k-1} - i_k} \\ &= \sum_{i_1,\ldots,i_{k-1}} \delta_{i_0 - i_1 - \ldots - i_{k-1} - i_k} \\ &= \#\Big\{i_0 - i_1 - \ldots - i_{k-1} - i_k\Big\}\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

Of particular interest are the paths which begin and end at the same point. These are called loops, and in the case of loops, Proposition 13.4 particularizes as follows:

PROPOSITION 13.5. *For a graph X, with adjacency matrix $d \in M_N(0,1)$, we have:*

$$(d^k)_{ii} = \#\Big\{k - \text{loops based at } i \in I\Big\}$$

Also, the total number of k-loops on X, at various vertices, is the number

$$Tr(d^k) = \sum_i (d^k)_{ii}$$

which can be computed by diagonalizing d.

PROOF. There are several things going on here, the idea being as follows:

(1) The first assertion follows from Proposition 13.4, which at $i = j$ gives the following formula, which translates into the first formula in the statement:

$$(d^k)_{ii} = \#\Big\{i = i_0 - i_1 - \ldots - i_{k-1} - i_k = i\Big\}$$

(2) Regarding now the second assertion, this follows from the first one, simply by summing over all the vertices $i \in X$, which gives, as desired:

$$Tr(d^k) = \sum_i \#\Big\{k - \text{loops based at } i \in I\Big\}$$

(3) Finally, the third assertion is something well-known from linear algebra, the idea being that once we diagonalize a matrix, $A = PDP^{-1}$, we have:

$$\begin{aligned}A = PDP^{-1} &\implies A^k = PD^kP^{-1} \\ &\implies Tr(A^k) = Tr(D^k)\end{aligned}$$

Thus, back now to our graph case, if we denote by $\lambda_1, \ldots, \lambda_N \in \mathbb{R}$ the eigenvalues of d, then the formula of the trace of d^k, that we are interested in, is as follows:

$$Tr(d^k) = \lambda_1^k + \ldots + \lambda_N^k$$

Here we have used the fact that d, which is a real symmetric matrix, is indeed diagonalizable, and with real eigenvalues, that you know from basic linear algebra. □

Getting now to Question 13.2 as stated, we still have to talk about the associated probability measure μ. So, here is the result that we will need, in what follows:

THEOREM 13.6. *Given a graph X, with adjacency matrix $d \in M_N(0,1)$, and with a distinguished vertex $*$, the number L_k of loops of length k based at $*$ is given by:*

$$L_k = (d^k)_{**}$$

When writing $d = UDU^t$ with $U \in O_N$ and $D = diag(\lambda_1, \ldots, \lambda_N)$ with $\lambda_i \in \mathbb{R}$, we have

$$L_k = \sum_i U_{*i}^2 \lambda_i^k$$

and the real probability measure μ having these numbers as moments is given by

$$\mu = \sum_i U_{*i}^2 \delta_{\lambda_i}$$

with the delta symbols standing as usual for Dirac masses.

PROOF. There are several things going on here, the idea being as follows:

(1) According to Proposition 13.5, we have the first formula in the statement:

$$(d^k)_{**} = \#\Big\{ * - i_1 - \ldots - i_{k-1} - * \Big\} = L_k$$

(2) Now since $d \in M_N(0,1)$ is symmetric, this matrix is diagonalizable, with the diagonalization being as follows, with $U \in O_N$, and $D = diag(\lambda_1, \ldots, \lambda_N)$ with $\lambda_i \in \mathbb{R}$:

$$d = UDU^t$$

By using this formula, we obtain the second formula in the statement:

$$\begin{aligned} L_k &= (d^k)_{**} \\ &= (UD^kU^t)_{**} \\ &= \sum_i U_{*i} \lambda_i^k (U^t)_{i*} \\ &= \sum_i U_{*i}^2 \lambda_i^k \end{aligned}$$

(3) Finally, the last assertion is clear from this, because the moments of the measure in the statement, $\mu = \sum_i U_{*i}^2 \delta_{\lambda_i}$, are the following numbers:

$$M_k = \int_{\mathbb{R}} x^k d\mu(x) = \sum_i U_{*i}^2 \lambda_i^k = L_k$$

Observe also that μ is indeed of mass 1, because all rows of $U \in O_N$ must be of norm 1, and so $\sum_i U_{*i}^2 = 1$. Thus, we are led to the conclusions in the statement. □

So long for the general theory of random walks on graphs. Getting now to the examples, as a first philosophical question, what are the simplest non-trivial graphs X, that we can try to do some computations for? And here, we have 3 possible answers:

FACT 13.7. *The following are graphs X, with a distinguished vertex $* \in X$:*

(1) *The circle graph, having N vertices, with $*$ being one of the vertices.*
(2) *The segment graph, having N vertices, with $*$ being the vertex at left.*
(3) *The segment graph, having $2N + 1$ vertices, with $*$ being in the middle.*

So, let us start with these. For the circle, the computations are quite non-trivial, and you can try doing some, in order to understand what I am talking about. The problem comes from the fact that loops of length $k = 0, 2, 4, 6, \ldots$ are quite easy to count, but then, once we pass $k = N$, the loops can turn around the circle or not, and they can even turn several times, and so on, and all this makes the count too complicated. In addition, again due to loop turning, when N is odd, we have as well loops of odd length.

As for the two segment graphs, here the computations look again complicated, and even more complicated than for the circle, because, again, once we pass $k = N$ many things can happen, and this makes the count too complicated. And here, again you can try doing some computations, in order to understand what I am talking about.

So, what to do? In the lack of a bright idea, let us pull an analysis trick, and formulate the following asymptotic result, which is of course something quite modest:

PROPOSITION 13.8. *For the circle graph, having N vertices, the number of length k loops based at one of the vertices is approximately*

$$L_k \simeq \frac{2^k}{N}$$

in the $k \to \infty$ limit, when N is odd, and is approximately

$$L_k \simeq \begin{cases} \frac{2^{k+1}}{N} & (k \text{ even}) \\ 0 & (k \text{ odd}) \end{cases}$$

also with $k \to \infty$, when N is even.

PROOF. This is something quite standard, the idea being as follows:

(1) Consider the circle graph X, with vertices denoted $0, 1, \ldots, N-1$. Since each vertex has valence 2, any length k path based at 0 will consist of a binary choice at the beginning, then another binary choice afterwards, and so on up to a k-th binary choice at the end. Thus, there is a total of 2^k such paths, based at 0, and having length k.

(2) But now, based on the obvious "uniformity" of the circle, we can argue that, in the $k \to \infty$ limit, the endpoint of such a path will become random among the vertices $0, 1, \ldots, N-1$. Thus, if we want this endpoint to be 0, as to have a loop, we have $1/N$ chances for this to happen, so the total number of loops is $L_k \simeq 2^k/N$, as stated.

(3) With the remark, however, that the above argument works fine only when N is odd. Indeed, when N is even, the endpoint of a length k path will be random among $0, 2, \ldots, 2N-2$ when k is even, and random among $1, 3, \ldots, 2N-1$ when k is odd. Thus for getting a loop we must assume that k is even, and in this case the number of such loops is the total number of length k paths, namely 2^k, approximately divided by $N/2$, the number of points in $\{0, 2, \ldots, 2N-2\}$, which gives $L_k = 2^k/(N/2)$, as stated.

(4) All this was of course a bit borderline, I know, with respect to what rigorous mathematics is supposed to be, but honestly, I think that the argument is there, and good, in short I trust this proof. More about this later, with better tools. □

In terms of probability measures, the above result translates as follows:

THEOREM 13.9. *For the circle graph, having N vertices, the probability measure μ having the numbers of loops L_k as moments is approximately*

$$\mu \simeq \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\,\delta_2$$

when N is odd, and is approximately

$$\mu \simeq \frac{1}{N}\,\delta_{-2} + \left(1 - \frac{2}{N}\right)\delta_0 + \frac{1}{N}\,\delta_2$$

when N is even, with these approximations being in the $N \to \infty$ limit.

PROOF. We have to construct the asymptotic measure μ out of the moment formulae from Proposition 13.8. When N is odd the answer is obvious, coming from:

$$\mu = \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\,\delta_2 \quad \implies \quad M_k = \frac{2^k}{N}$$

As for the case where N is even, here a bit of thinking leads to:

$$\mu = \frac{1}{N}\,\delta_{-2} + \left(1 - \frac{2}{N}\right)\delta_0 + \frac{1}{N}\,\delta_2 \quad \implies \quad M_k = \begin{cases} \frac{2^{k+1}}{N} & (k \text{ even}) \\ 0 & (k \text{ odd}) \end{cases}$$

Thus, we are led to the conclusions in the statement. □

Getting now to the segment graphs from Fact 13.7, in the context of the proof of Proposition 13.8, it is pretty much clear that for both, we lack the "uniformity" needed in (2) there, and this due to the 2 endpoints of the segment. In fact, thinking well, these graphs are no longer 2-valent, again due to the 2 endpoints, each having valence 1, and so even (1) there must be fixed. And so, we will normally have to stop here.

This being said, as a matter of not leaving this subject empty-handed, let us record the following result, which is something more advanced, based on diagonalization:

THEOREM 13.10. *For the segment graphs having N vertices, the characteristic polynomials P_N of the adjacency matrices are subject to the following recurrence,*

$$P_0 = 1 \quad , \quad P_1 = x \quad , \quad P_{N+1} = xP_N - P_{N-1}$$

and are the well-known Chebycheff polynomials, enjoying many interesting properties. The corresponding numbers of loops and measures can be deduced from this.

PROOF. Obviously, many things going on here, the idea being as follows:

(1) To start with, by computing determinants, we are led to the recurrence formula in the statement. Here is the proof at $N = 4$, the general case being similar:

$$\begin{aligned}
P_5 &= \begin{vmatrix} x & -1 & 0 & 0 & 0 \\ -1 & x & -1 & 0 & 0 \\ 0 & -1 & x & -1 & 0 \\ 0 & 0 & -1 & x & -1 \\ 0 & 0 & 0 & -1 & x \end{vmatrix} \\
&= x \begin{vmatrix} x & -1 & 0 & 0 \\ -1 & x & -1 & 0 \\ 0 & -1 & x & -1 \\ 0 & 0 & -1 & x \end{vmatrix} + \begin{vmatrix} -1 & -1 & 0 & 0 \\ 0 & x & -1 & 0 \\ 0 & -1 & x & -1 \\ 0 & 0 & -1 & x \end{vmatrix} \\
&= x \begin{vmatrix} x & -1 & 0 & 0 \\ -1 & x & -1 & 0 \\ 0 & -1 & x & -1 \\ 0 & 0 & -1 & x \end{vmatrix} - \begin{vmatrix} x & -1 & 0 \\ -1 & x & -1 \\ 0 & -1 & x \end{vmatrix} \\
&= xP_4 - P_3
\end{aligned}$$

(2) Regarding the intial values, these are normally $P_2 = x^2 - 1$ and $P_3 = x^3 - 2x$, but we can formally add the values $P_0 = 1$ and $P_1 = x$, with this being justified by:

$$\begin{aligned}
&P_0 = 1 \\
&P_1 = x \\
\implies &P_2 = xP_1 - P_0 = x^2 - 1 \\
\implies &P_3 = xP_2 - P_1 = x^3 - 2x
\end{aligned}$$

(3) Thus, we have the recurrence formula in the statement, and with the initial values there, and an internet search, or some advanced calculus know-how, tells us that these are the well-known Chebycheff polynomials, enjoying lots of interesting properties.

(4) Finally, in what regards the numbers of loops L_k, and the corresponding measures μ, these can be in principle computed by using Theorem 13.6. However, the computations are quite tough here, and we will not choose this path. More on all this, later. □

13b. Infinite graphs

Time perhaps for a conclusion? The loop counting business on graphs looks like a nice activity, but in practice, when trying this for the simplest possible graphs, we got into quite complicated mathematics. So, if there is a conclusion to this, we're in trouble.

Well, instead of giving up, let us look face-to-face at the difficulties that we met. We are led this way, after analyzing the situation, to the following thought:

THOUGHT 13.11. *The difficulties that we met, with the circle and the two segments, come from the fact that our loops are not "free to move",*

(1) *for the circle, because these can circle around the circle,*

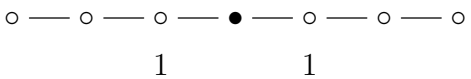
(2) *for the segments, obviously because of the endpoints,*

and so our difficulties will dissapear, and we will be able to do our exact loop count, once we find a graph X where the loops are truly "free to move".

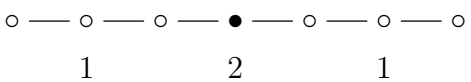
Thinking some more, all this definitely buries the first interval graph, where the vertex 0 is one of the endpoints. However, we can still try to recycle the circle, by unwrapping it, or extend our second interval graph up to ∞. But in both cases what we get is the graph $\mathbb{Z}$ formed by the integers. So, let us formulate the following definition:

DEFINITION 13.12. *An infinite graph is the same thing as a finite graph, but now with an infinity of vertices, $|X| = \infty$. As a basic example, we have $\mathbb{Z}$. We also have $\mathbb{N}$.*

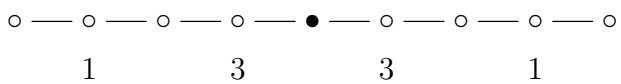
Leaving aside now $\mathbb{N}$, which looks more complicated, let us try to count the length k paths on $\mathbb{Z}$, based at 0. At $k = 1$ we have 2 such paths, ending at -1 and 1, and the count results can be pictured as follows, with everything being self-explanatory:



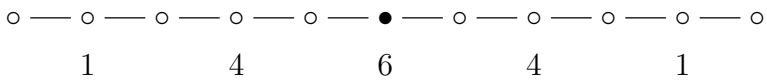
At $k = 2$ now, we have 4 paths, one of which ends at -2, two of which end at 0, and one of which ends at 2. The results can be pictured as follows:



At $k = 3$ now, we have 8 paths, the distribution of the endpoints being as follows:



As for $k = 4$, here we have 16 paths, the distribution of the endpoints being as follows:



And good news, we can see in the above the Pascal triangle. Thus, getting back now to Question 13.2, we can answer it for the graph $\mathbb{Z}$, the result being as follows:

THEOREM 13.13. *The paths on $\mathbb{Z}$ are counted by the binomial coefficients. In particular, the $2k$-paths based at 0 are counted by the central binomial coefficients,*

$$L_{2k} = \binom{2k}{k}$$

and μ is the centered measure having these numbers as even moments.

PROOF. This basically follows from the above discussion, as follows:

(1) In what regards the count, we certainly have the Pascal triangle, as discovered above, and the rest is just a matter of finishing. There are many possible ways here, a straightforward one being that of arguing that the number C_k^l of length k loops $0 \to l$ is subject, due to the binary choice at the end, to the following recurrence relation:

$$C_k^l = C_{k-1}^{l-1} + C_{k-1}^{l+1}$$

But this is exactly the recurrence for the Pascal triangle, so done with the count.

(2) As for the second assertion, the first part, regarding L_{2k}, is clear from this, and the second part is more of an empty statement, with μ still remaining to be computed. □

As a second illustration, let us try to count the loops of $\mathbb{N}$, based at 0. This is something less obvious, and at the experimental level, the result is as follows:

PROPOSITION 13.14. *The numbers C_k counting the loops on $\mathbb{N}$ based at 0,*

$$C_k = \#\Big\{0 - i_1 - \ldots - i_{2k-1} - 0\Big\}$$

are numerically $1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, \ldots$

PROOF. To start with, we have indeed $C_1 = 1$, the only loop here being $0 - 1 - 0$. Then we have $C_2 = 2$, due to two possible loops, namely:

$$0 - 1 - 0 - 1 - 0$$

$$0 - 1 - 2 - 1 - 0$$

Then we have $C_3 = 5$, the possible loops here being as follows:

$$0-1-0-1-0-1-0$$
$$0-1-0-1-2-1-0$$
$$0-1-2-1-0-1-0$$
$$0-1-2-1-2-1-0$$
$$0-1-2-3-2-1-0$$

And so on, and I will leave some more computations to you, as an exercise. □

In practice now, and coming as good news, all this makes the link with some things that we know well, from chapter 1, and notably with the following result, from there:

THEOREM 13.15. *The following objects are counted by the same numbers C_k, called Catalan numbers, given by $C_0 = C_1 = 1$ and $C_{k+1} = \sum_{a+b=k} C_a C_b$:*

(1) *The length $2k$ loops on $\mathbb{N}$, based at 0.*
(2) *The noncrossing pairings of $1, \ldots, 2k$.*
(3) *The noncrossing partitions of $1, \ldots, k$.*
(4) *The length $2k$ Dyck paths in the plane.*

PROOF. As explained in chapter 1, this is indeed standard combinatorics, with the recurrence formula in the statement $C_{k+1} = \sum_{a+b=k} C_a C_b$ being clear in all cases, and with bijective proofs for the equivalence of the counts in (1,2,3,4) being possible as well. □

Still following chapter 1, as a continuation of Theorem 13.15, we have:

THEOREM 13.16. *The Catalan numbers are given by the formula*

$$C_k = \frac{1}{k+1}\binom{2k}{k}$$

with this being best seen by counting the length $2k$ Dyck paths in the plane.

PROOF. This is indeed something very standard, obtained by using a reflection trick for the Dyck paths, and for details here, we refer to the material in chapter 1. □

Finally, still talking Catalan numbers, let us recall as well from chapter 8 that we have the following result, providing a purely analytic approach to them:

THEOREM 13.17. *The Catalan numbers have the following properties:*

(1) *They satisfy $C_{k+1} = \sum_{a+b=k} C_a C_b$.*
(2) *The series $f(z) = \sum_{k \geq 0} C_k z^k$ satisfies $zf^2 - f + 1 = 0$.*
(3) *This series is given by $f(z) = \frac{1-\sqrt{1-4z}}{2z}$.*
(4) *We have the formula $C_k = \frac{1}{k+1}\binom{2k}{k}$.*

PROOF. This is indeed something that we know from chapter 8, the key ingredient being the generalized binomial formula, which allows extracting the square root. □

Getting back now to graphs, we can complement Theorem 13.13 with:

THEOREM 13.18. *The loops on $\mathbb{N}$ are counted by the Catalan numbers,*

$$L_{2k} = \frac{1}{k+1}\binom{2k}{k}$$

and μ is the centered measure having these numbers as even moments.

PROOF. This follows indeed from what we have, namely Theorem 13.15 for the recurrence, and then Theorem 13.16 or Theorem 13.17 for the solution of the recurrence. □

Summarizing, loop count question solved for both the graphs $\mathbb{Z}$ and $\mathbb{N}$. Which is very nice, and in what follows we will keep working on these two graphs, $\mathbb{Z}$ and $\mathbb{N}$.

13c. Stieltjes inversion

According to what we have in Theorems 13.13 and 13.18, the problem is now, how to recover a probability measure out of its moments. And things here are quite subtle, because, unlike in the discrete case, where a bit of thinking using Dirac masses will do, as we did in the proof of Theorem 13.9, in the continuous case, which is most likely the one that we are interested in, the graphs $\mathbb{Z}$, $\mathbb{N}$ being infinite, we have so far no tools.

Fortunately, there is an answer to this question, recovering a continuous measure out of its moments. The result here, which is something quite technical, is as follows:

THEOREM 13.19. *The density of a continuous probability measure μ can be recaptured from the sequence of moments $\{M_k\}_{k\geq 0}$ via the Stieltjes inversion formula*

$$d\mu(x) = \lim_{t\searrow 0} -\frac{1}{\pi}\, Im\left(G(x+it)\right)\cdot dx$$

where the function on the right, given in terms of moments by

$$G(\xi) = \xi^{-1} + M_1\xi^{-2} + M_2\xi^{-3} + \ldots$$

is the Cauchy transform of the measure μ.

PROOF. The Cauchy transform of our measure μ is given by:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^{\infty} M_k\xi^{-k} \\ &= \int_{\mathbb{R}} \frac{\xi^{-1}}{1-\xi^{-1}y}\, d\mu(y) \\ &= \int_{\mathbb{R}} \frac{1}{\xi - y}\, d\mu(y) \end{aligned}$$

Now with $\xi = x + it$, we obtain the following formula:

$$\begin{aligned} Im(G(x+it)) &= \int_{\mathbb{R}} Im\left(\frac{1}{x-y+it}\right) d\mu(y) \\ &= \int_{\mathbb{R}} \frac{1}{2i}\left(\frac{1}{x-y+it} - \frac{1}{x-y-it}\right) d\mu(y) \\ &= -\int_{\mathbb{R}} \frac{t}{(x-y)^2+t^2}\, d\mu(y) \end{aligned}$$

By integrating over $[a, b]$ we obtain, with the change of variables $x = y + tz$:

$$\begin{aligned} \int_a^b Im(G(x+it))dx &= -\int_{\mathbb{R}} \int_a^b \frac{t}{(x-y)^2+t^2}\, dx\, d\mu(y) \\ &= -\int_{\mathbb{R}} \int_{(a-y)/t}^{(b-y)/t} \frac{t}{(tz)^2+t^2}\, t\, dz\, d\mu(y) \\ &= -\int_{\mathbb{R}} \int_{(a-y)/t}^{(b-y)/t} \frac{1}{1+z^2}\, dz\, d\mu(y) \\ &= -\int_{\mathbb{R}} \left(\arctan\frac{b-y}{t} - \arctan\frac{a-y}{t}\right) d\mu(y) \end{aligned}$$

Now observe that with $t \searrow 0$ we have:

$$\lim_{t\searrow 0}\left(\arctan\frac{b-y}{t} - \arctan\frac{a-y}{t}\right) = \begin{cases} \frac{\pi}{2} - \frac{\pi}{2} = 0 & (y < a) \\ \frac{\pi}{2} - 0 = \frac{\pi}{2} & (y = a) \\ \frac{\pi}{2} - (-\frac{\pi}{2}) = \pi & (a < y < b) \\ 0 - (-\frac{\pi}{2}) = \frac{\pi}{2} & (y = b) \\ -\frac{\pi}{2} - (-\frac{\pi}{2}) = 0 & (y > b) \end{cases}$$

We therefore obtain the following formula:

$$\lim_{t\searrow 0} \int_a^b Im(G(x+it))dx = -\pi\left(\mu(a,b) + \frac{\mu(a)+\mu(b)}{2}\right)$$

Thus, we are led to the conclusion in the statement. □

Before getting further, let us mention that the above result does not fully solve the moment problem, because we still have the question of understanding when a sequence of numbers $M_1, M_2, M_3, \ldots$ can be the moments of a measure μ. We have here:

THEOREM 13.20. *A sequence of numbers $M_0, M_1, M_2, M_3, \ldots \in \mathbb{R}$, with $M_0 = 1$, is the series of moments of a real probability measure μ precisely when:*

$$\left|M_0\right| \geq 0 \quad , \quad \begin{vmatrix} M_0 & M_1 \\ M_1 & M_2 \end{vmatrix} \geq 0 \quad , \quad \begin{vmatrix} M_0 & M_1 & M_2 \\ M_1 & M_2 & M_3 \\ M_2 & M_3 & M_4 \end{vmatrix} \geq 0 \quad , \quad \ldots$$

That is, the associated Hankel determinants must be all positive.

PROOF. This is something a bit more advanced, the idea being as follows:

(1) As a first observation, the positivity conditions in the statement tell us that the following associated linear forms must be positive:

$$\sum_{i,j=1}^{n} c_i \bar{c}_j M_{i+j} \geq 0$$

(2) But this is something very classical, in one sense the result being elementary, coming from the following computation, which shows that we have positivity indeed:

$$\begin{aligned} \int_{\mathbb{R}} \left| \sum_{i=1}^{n} c_i x^i \right|^2 d\mu(x) &= \int_{\mathbb{R}} \sum_{i,j=1}^{n} c_i \bar{c}_j x^{i+j} d\mu(x) \\ &= \sum_{i,j=1}^{n} c_i \bar{c}_j M_{i+j} \end{aligned}$$

(3) As for the other sense, here the result comes once again from the above formula, this time via some standard functional analysis. So, this is the situation, welcome to the moment problem, and of course exercise for you, to learn a bit more about all this. □

Getting back now to the Stieltjes formula from Theorem 13.19, let us try to solve the moment problem for the Catalan numbers C_k, and for the central binomial coefficients D_k. We first have the following result, coming as a complement to Theorem 13.18:

THEOREM 13.21. *The real measure having as even moments the Catalan numbers, $C_k = \frac{1}{k+1}\binom{2k}{k}$, and having all odd moments 0 is the measure*

$$\gamma_1 = \frac{1}{2\pi}\sqrt{4 - x^2}dx$$

called Wigner semicircle law on $[-2, 2]$.

PROOF. In order to apply the inversion formula, our starting point will be the formula from Theorem 13.17 for the generating series of the Catalan numbers, namely:

$$\sum_{k=0}^{\infty} C_k z^k = \frac{1 - \sqrt{1 - 4z}}{2z}$$

By using this formula with $z = \xi^{-2}$, we obtain the following formula:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^{\infty} C_k \xi^{-2k} \\ &= \xi^{-1} \cdot \frac{1-\sqrt{1-4\xi^{-2}}}{2\xi^{-2}} \\ &= \frac{\xi}{2}\left(1-\sqrt{1-4\xi^{-2}}\right) \\ &= \frac{\xi}{2} - \frac{1}{2}\sqrt{\xi^2-4} \end{aligned}$$

Now let us apply Theorem 13.19. The study here goes as follows:

(1) According to the general philosophy of the Stieltjes formula, the first term, namely $\xi/2$, which is "trivial", will not contribute to the density.

(2) As for the second term, which is something non-trivial, this will contribute to the density, the rule here being that the square root $\sqrt{\xi^2-4}$ will be replaced by the "dual" square root $\sqrt{4-x^2}\,dx$, and that we have to multiply everything by $-1/\pi$.

(3) As a conclusion, by Stieltjes inversion we obtain the following density:

$$d\mu(x) = -\frac{1}{\pi} \cdot -\frac{1}{2}\sqrt{4-x^2}\,dx = \frac{1}{2\pi}\sqrt{4-x^2}dx$$

Thus, we have obtained the mesure in the statement, and we are done. □

Next, we have the following interesting version of the above result, whose precise interest will become clear later in this chapter, and in chapters 15-16 as well:

THEOREM 13.22. *The real measure having as sequence of moments the Catalan numbers, $C_k = \frac{1}{k+1}\binom{2k}{k}$, is the measure*

$$\pi_1 = \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

called Marchenko-Pastur law on $[0,4]$.

PROOF. As before, we use the standard formula for the generating series of the Catalan numbers. With $z = \xi^{-1}$ in that formula, we obtain the following formula:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^{\infty} C_k\xi^{-k} \\ &= \xi^{-1}\cdot\frac{1-\sqrt{1-4\xi^{-1}}}{2\xi^{-1}} \\ &= \frac{1}{2}\left(1-\sqrt{1-4\xi^{-1}}\right) \\ &= \frac{1}{2}-\frac{1}{2}\sqrt{1-4\xi^{-1}} \end{aligned}$$

With this in hand, let us apply now the Stieltjes inversion formula, from Theorem 13.19. We obtain, a bit as before in Theorem 13.21, the following density:

$$d\mu(x) = -\frac{1}{\pi}\cdot-\frac{1}{2}\sqrt{4x^{-1}-1}\,dx = \frac{1}{2\pi}\sqrt{4x^{-1}-1}\,dx$$

Thus, we are led to the conclusion in the statement. □

Getting now to the central binomial coefficients, we normally have two computations to do for them, in the spirit of those done in Theorems 13.21 and 13.22, for the Catalan numbers. And here, going for the analogue of Theorem 13.22, trust me, we have:

THEOREM 13.23. *The real probability measure having as moments the central binomial coefficients, $D_k = \binom{2k}{k}$, is the measure*

$$\alpha_1 = \frac{1}{\pi\sqrt{x(4-x)}}\,dx$$

called arcsine law on $[0,4]$.

PROOF. We have the following computation, using some standard formulae:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^{\infty} D_k\xi^{-k} \\ &= \frac{1}{\xi}\sum_{k=0}^{\infty} D_k\left(-\frac{t}{4}\right)^k \\ &= \frac{1}{\xi}\cdot\frac{1}{\sqrt{1-4/\xi}} \\ &= \frac{1}{\sqrt{\xi(\xi-4)}} \end{aligned}$$

But this gives the density in the statement, via Theorem 13.19. □

Finally, we have the following useful technical version of the above result:

THEOREM 13.24. *The real probability measure having as moments the middle binomial coefficients, $E_k = \binom{k}{[k/2]}$, is the following law on $[-2,2]$,*

$$\sigma_1 = \frac{1}{2\pi}\sqrt{\frac{2+x}{2-x}}\,dx$$

called modified arcsine law on $[-2,2]$.

PROOF. In terms of the central binomial coefficients D_k, we have:

$$E_{2k} = \binom{2k}{k} = \frac{(2k)!}{k!k!} = D_k$$

$$E_{2k-1} = \binom{2k-1}{k} = \frac{(2k-1)!}{k!(k-1)!} = \frac{D_k}{2}$$

Standard calculus based on the Taylor formula for $(1+t)^{-1/2}$ gives:

$$\frac{1}{2x}\left(\sqrt{\frac{1+2x}{1-2x}} - 1\right) = \sum_{k=0}^{\infty} E_k x^k$$

With $x = \xi^{-1}$ we obtain the following formula for the Cauchy transform:

$$\begin{aligned} G(\xi) &= \xi^{-1}\sum_{k=0}^{\infty} E_k \xi^{-k} \\ &= \frac{1}{\xi}\left(\sqrt{\frac{1+2/\xi}{1-2/\xi}} - 1\right) \\ &= \frac{1}{\xi}\left(\sqrt{\frac{\xi+2}{\xi-2}} - 1\right) \end{aligned}$$

By Stieltjes inversion we obtain the density in the statement. □

And with this, end of our discussion regarding random walks on basic infinite graphs, and related topics. Good learning this was, and more on such things, later.

13d. ADE graphs

With the above understood, let us get back now to the finite graphs. We have been stuck with them previously, but in view of our latest results regarding the infinite graphs, which are very nice, let us declare ourselves strong and optimistic, and forgetting any kind of modesty, let us formulate a quite ambitious question, as follows:

QUESTION 13.25. *What are the most important finite graphs, that we should do our computations for?*

Which is actually not an easy question, and with me writing this book, and basically doing quantum physics, as daytime job, I will choose the ADE graphs, based on:

FACT 13.26. *The ADE graphs classify the following:*

(1) *Basic Lie groups and algebras.*
(2) *Subgroups of SU_2 and of SO_3.*
(3) *Singularities of algebraic manifolds.*
(4) *Basic invariants of knots and links.*
(5) *Subfactors and planar algebras of small index.*
(6) *Subgroups of the quantum permutation group S_4^+.*
(7) *Basic quantum field theories, and other physics beasts.*

Which sounds exciting, doesn't it. So, if interested in astrology and related topics, such as the origin, functioning and future of the universe, have a look at this, modern mathematics and physics united, with a nice introduction here being Jones [58].

Getting to work now, we first need to know what the ADE graphs are. The A graphs, which are the simplest, are as follows, with the distinguished vertex being denoted $\bullet$, and with A_n having $n \geq 2$ vertices, and $\tilde{A}_{2n}$ having $2n \geq 2$ vertices:

$$A_n = \bullet - \circ - \circ \cdots \circ - \circ - \circ \qquad A_\infty = \bullet - \circ - \circ - \circ \cdots$$

$$\tilde{A}_{2n} = \begin{array}{ccccccccccc} & \circ & - & \circ & - & \circ & \cdots & \circ & - & \circ & - & \circ \\ & | & & & & & & & & & | & \\ \bullet & - & \circ & - & \circ & - & \cdots & - & \circ & - & \circ & \end{array} \qquad \tilde{A}_\infty = \begin{array}{ccccccc} & \circ & - & \circ & - & \circ & \cdots \\ & | & & & & & \\ \bullet & - & \circ & - & \circ & - & \circ \cdots \end{array}$$

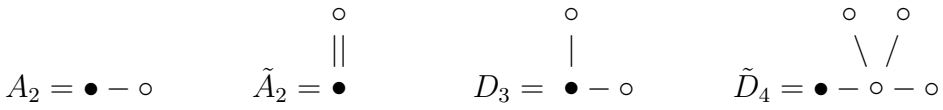
You might probably say, why not stopping here, and doing our unfinished business for the segment and the circle, with whatever new ideas that we might have. Good point, but in answer, these ideas will apply as well, with minimal changes, to the D graphs, which are as follows, with D_n having $n \geq 3$ vertices, and $\tilde{D}_n$ having $n + 1 \geq 5$ vertices:

$$D_n = \begin{array}{ccccccccc} & & & & & & \circ & & \\ & & & & & & | & & \\ \bullet & - & \circ & - & \circ & \cdots & \circ & - & \circ \end{array}$$

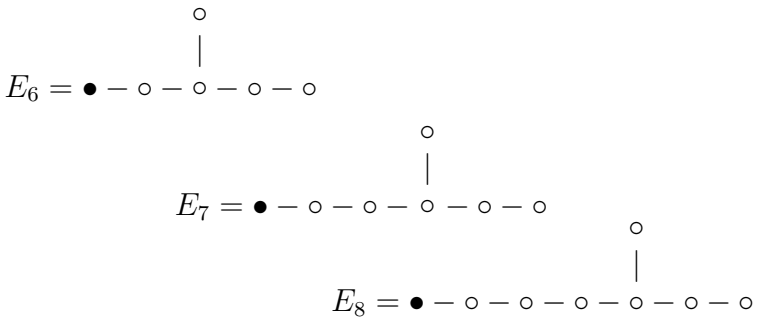
$$\tilde{D}_n = \begin{array}{ccccccccccc} & & & & & & \circ & & \circ & & \\ & & & & & & | & & | & & \\ \bullet & - & \circ & - & \circ & \cdots & \circ & - & \circ & - & \circ \end{array}$$

$$D_\infty = \begin{array}{ccccccc} & & & & & & \circ \\ & & & & & & | \\ \bullet & - & \circ & - & \circ & - & \circ \cdots \end{array}$$

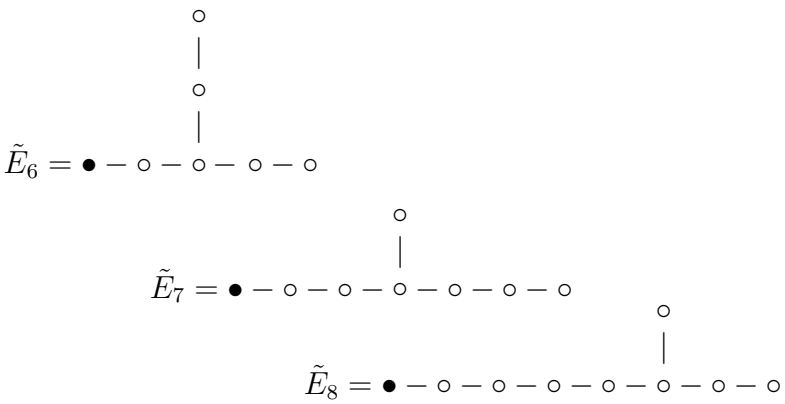
As a comment here, the labeling conventions for the AD graphs, while very standard, can be a bit confusing. The first graph in each series is by definition as follows:



Finally, there are also a number of exceptional ADE graphs. First we have:



Then, we have extended versions of the above exceptional graphs, as follows:



And good news, according to the general theory, that is all. Getting now to work, we have plenty of graphs here, and the problem that we would like to solve is:

PROBLEM 13.27. *How to count loops on the ADE graphs?*

In answer now, as a first observation, we know that A_∞ and $\tilde{A}_\infty$ are respectively the graphs that we previously called $\mathbb{N}$ and $\mathbb{Z}$, and studied in great detail.

So, based on our previous work for these graphs, where the combinatorics naturally led us into generating series, let us formulate the following definition:

DEFINITION 13.28. *The Poincaré series of a rooted bipartite graph X is*

$$f(z)=\sum_{k=0}^{\infty}L_{2k}z^k$$

where L_{2k} is the number of $2k$-loops based at the root.

To be more precise, observe that all the above ADE graphs are indeed bipartite. Now the point is that, for a bipartite graph, the loops based at any point must have even length. Thus, in order to study the loops on the ADE graphs, we are led to $f(z)$.

Before getting into computations, let us introduce as well:

DEFINITION 13.29. *The positive spectral measure ν of a rooted bipartite graph X is the real probability measure having the numbers L_{2k} as moments:*

$$\int_{\mathbb{R}}x^k d\nu(x)=L_{2k}$$

Equivalently, we must have the Stieltjes transform formula

$$f(z)=\int_{\mathbb{R}}\frac{1}{1-xz}\,d\nu(x)$$

where f is the Poincaré series of X.

Here the existence of ν, and the fact that this is indeed a positive measure, meaning a measure supported on $[0,\infty)$, comes from the following simple fact:

THEOREM 13.30. *The positive spectral measure of a rooted bipartite graph X is given by the following formula, with d being the adjacency matrix of the graph,*

$$\nu=law(d^2)$$

and with the probabilistic computation being with respect to the expectation

$$A\to<A>$$

with $<A>$ being the $(*,*)$-entry of a matrix A, where $*$ is the root.

PROOF. With the above conventions, we have the following computation:

$$\begin{aligned}f(z)&=\sum_{k=0}^{\infty}L_{2k}z^k\\&=\sum_{k=0}^{\infty}\left\langle d^{2k}\right\rangle z^k\\&=\left\langle\frac{1}{1-d^2z}\right\rangle\end{aligned}$$

But this shows that we have $\nu=law(d^2)$, as desired. □

The above result shows that computing ν might be actually a simpler problem than computing f, and in practice, this is indeed the case. So, in what follows we will rather forget about loops and Definition 13.28, and use Definition 13.29 instead, with our computations to follow being based on the concrete interpretation from Theorem 13.30.

However, even with this probabilistic trick in our bag, things are not exactly trivial. Let us introduce as well the following notion, which is something more subtle, coming from the work of Jones on subfactor theory, and related topics [58]:

DEFINITION 13.31. *The circular measure ε of a rooted bipartite graph X is given by*

$$d\varepsilon(q) = d\nu((q + q^{-1})^2)$$

where ν is the associated positive spectral measure.

To be more precise, we know from Theorem 13.30 that the positive measure ν is the spectral measure of a certain positive matrix, $d^2 \geq 0$, and it follows from this, and from basic spectral theory, that this measure is supported by the positive reals:

$$supp(\nu) \subset \mathbb{R}_+$$

But then, with this observation in hand, we can define indeed the circular measure ε as above, as being the pullback of ν via the following map:

$$\mathbb{R} \cup \mathbb{T} \to \mathbb{R}_+ \quad , \quad q \to (q + q^{-1})^2$$

As a basic example for this, to start with, assume that ν is a discrete measure, supported by n positive numbers $x_1 < \ldots < x_n$, with corresponding densities $p_1, \ldots, p_n$:

$$\nu = \sum_{i=1}^{n} p_i \delta_{x_i}$$

For each $i \in \{1, \ldots, n\}$ the equation $(q + q^{-1})^2 = x_i$ has then four solutions, that we can denote $q_i, q_i^{-1}, -q_i, -q_i^{-1}$. And with this notation, we have:

$$\varepsilon = \frac{1}{4} \sum_{i=1}^{n} p_i \left(\delta_{q_i} + \delta_{q_i^{-1}} + \delta_{-q_i} + \delta_{-q_i^{-1}} \right)$$

In general, the basic properties of ε can be summarized as follows:

THEOREM 13.32. *The circular measure has the following properties:*

(1) *ε has equal density at $q, q^{-1}, -q, -q^{-1}$.*
(2) *The odd moments of ε are 0.*
(3) *The even moments of ε are half-integers.*
(4) *When X has norm ≤ 2, ε is supported by the unit circle.*
(5) *When X is finite, ε is discrete.*
(6) *If K is a solution of $d = K + K^{-1}$, then $\varepsilon = law(K)$.*

PROOF. These results can be deduced from definitions, the idea being that (1-5) are trivial, and that (6) follows from the formula of ν from Theorem 13.30. □

Getting now to computations, we first have the following result:

THEOREM 13.33. *The circular measure of the basic index* 4 *graph, namely*

$$\tilde{A}_{2n} = \begin{array}{c} \circ - \circ - \circ \cdots \circ - \circ - \circ \\ | \qquad\qquad\qquad\qquad | \\ \bullet - \circ - \circ - \circ - \circ - \circ \end{array}$$

is the uniform measure on the $2n$*-roots of unity.*

PROOF. Let us identify the vertices of $X = \tilde{A}_{2n}$ with the group $\{w^k\}$ formed by the $2n$-th roots of unity in the complex plane, where $w = e^{\pi i/n}$. The adjacency matrix of X acts then on the functions $f \in C(X)$ in the following way:

$$df(w^s) = f(w^{s-1}) + f(w^{s+1})$$

But this shows that we have $d = K + K^{-1}$, where K is given by:

$$Kf(w^s) = f(w^{s+1})$$

Thus we can use Theorem 13.30 and Theorem 13.32 (6), and we get:

$$\varepsilon = law(K)$$

But this is the uniform measure on the $2n$-roots of unity, as claimed. □

Observe that Theorem 13.33 nukes our previous work on the circle graph. In order to deal now with the other ADE graphs, let us introduce the following densities:

$$\alpha = Re(1 - q^2)$$

$$\beta = Re(1 - q^4)$$

$$\gamma = Re(1 - q^6)$$

We have then the following result, d_n being the uniform measure on the $2n$-th roots of unity, and $d'_n = 2d_{2n} - d_n$ being the uniform measure on the odd $4n$-roots of unity:

THEOREM 13.34. *The circular measures of ADE graphs are given by:*

(1) $A_{n-1} \to \alpha_n$.
(2) $\tilde{A}_{2n} \to d_n$.
(3) $D_{n+1} \to \alpha'_n$.
(4) $\tilde{D}_{n+2} \to (d_n + d'_1)/2$.
(5) $E_6 \to \alpha_{12} + (d_{12} - d_6 - d_4 + d_3)/2$.
(6) $E_7 \to \beta'_9 + (d'_1 - d'_3)/2$.
(7) $E_8 \to \alpha'_{15} + \gamma'_{15} - (d'_5 + d'_3)/2$.
(8) $\tilde{E}_{n+3} \to (d_n + d_3 + d_2 - d_1)/2$.

PROOF. This is something which can be proved in three steps, as follows:

(1) For the simplest graph, namely the circle $\tilde{A}_{2n}$, we already have the result, from Theorem 13.33, with the proof there being something elementary.

(2) For the other non-exceptional graphs, that is, of type A and D, the same method works, namely direct loop counting, with some matrix tricks.

(3) As for the exceptional graphs, of type E, basically the same method works, but the computations are more complicated, using some root of unity know-how. □

And with this, end of our discussion on random walks. I should mention that I personally got into such things, random walks on ADE graphs, some time ago, in the context of some joint research work with my colleague Dietmar Bisch from Nashville, Tennessee, on the algebraic aspects of Jones' subfactor theory. So, as a final advice here, learn mathematics and physics from Jones [58], listen to Johnny Cash, and for more on the above, details and whole story, you can have a look at my book [12].

13e. Exercises

This was a quite tricky chapter, and as exercises on this, we have:

EXERCISE 13.35. *Work out loop count results for various products of graphs.*

EXERCISE 13.36. *Learn more about Catalan numbers, the more, the better.*

EXERCISE 13.37. *Clarify what happens to the atoms, in the Stieltjes formula.*

EXERCISE 13.38. *Learn more about Hankel determinants, and the moment problem.*

EXERCISE 13.39. *Learn about the Wigner law, and its various remarkable properties.*

EXERCISE 13.40. *Learn about the Marchenko-Pastur law, and its various properties.*

EXERCISE 13.41. *Learn as well about the arcsine law, and its various properties.*

EXERCISE 13.42. *Learn about various ADE classifications, in math and physics.*

As bonus exercise, reiterated, learn about subfactors, from Jones [58].

CHAPTER 14

Central limits

14a. Central limits

Time and again I said in this book, on various occasions, a bit as I do when teaching classes at my university, that what we just did previously was not acceptable, far too complicated all that stuff, and that starting from today we should go back to a more normal pace, and learn fundamental things only, and done in great detail.

Well, time for me I guess to keep my word, at least this time, because the material scheduled for this chapter is something truly fundamental, which needs to be properly understood. So let's hope that we will learn here interesting things, all done well.

Getting started now, it is actually technically convenient to forget everything that we just learned in chapter 13, and in fact forget about what we did in chapters 9-12 too, nice but a bit too specialized, all that material. So, here we are at the end of chapter 8, with the aim of further building on one of our main results there, namely:

THEOREM 14.1 (Law of large numbers). *Given i.i.d. variables $f_1, f_2, f_3, \ldots$, with common mean $E(f_i) = E$, we have the convergence*

$$\frac{f_1 + \ldots + f_n}{n} \to E$$

happening almost surely.

PROOF. This is something that we know from chapter 8, the idea being as follows:

(1) The convergence in law is clear, because the Fourier transform of the average on the left converges to e^{iEt}, which is the Fourier transform of the constant variable E.

(2) The convergence in probability, which is something stronger, called weak law of large numbers, is elementary too, using the Chebycheff inequality from chapter 5.

(3) As for the convergence almost surely, called strong law of large numbers, this is something more technical, using Borel-Cantelli and a higher Chebycheff inequality. □

With this discussed, what is next? A finer study I guess, normally leading to bell-shaped curves, that you have certainly heard about, and perhaps even observed in physics or chemistry class, because any routine measurement leads to such curves.

Mathematically, here is the question that we would like to solve:

QUESTION 14.2. *Given random variables $f_1, f_2, f_3, \ldots$, say taken discrete, which are i.i.d., centered, and with common variance $t > 0$, do we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim g_t$$

in the $n \to \infty$ limit, for some bell-shaped density g_t? And, what is the formula of g_t?

Observe that this question perfectly makes sense, with the probability theory that we know, by assuming that our random variables $f_1, f_2, f_3, \ldots$ are discrete, as said above. As for the $1/\sqrt{n}$ factor, there is certainly need for a normalization factor there, as for things to have a chance to converge, and the good factor is $1/\sqrt{n}$, as shown by:

PROPOSITION 14.3. *In order for a sum of the following type to have a chance to converge, with $f_1, f_2, f_3, \ldots$ being i.i.d., centered, and with common variance $t > 0$,*

$$S = \sum_{i=1}^{n} f_i$$

we must normalize this sum by a $1/\sqrt{n}$ factor, as in Question 14.2.

PROOF. The idea here is to look at the moments of S. Since all variables f_i are centered, $E(f_i) = 0$, so is their sum, $E(S) = 0$, and no contradiction here. However, when looking at the variance of S, which equals the second moment, due to $E(S) = 0$, things become interesting, due to the following computation:

$$\begin{aligned} V(S) &= E(S^2) \\ &= E\left(\sum_{ij} f_i f_j\right) \\ &= \sum_{ij} E(f_i f_j) \\ &= \sum_{i} E(f_i^2) + \sum_{i \neq j} E(f_i) E(f_j) \\ &= \sum_{i} E(f_i^2) \\ &= nt \end{aligned}$$

Thus, we are in need a normalization factor α, in order for our sum to have a chance to converge. But, repeating the computation with S replaced by αS gives:

$$V(\alpha S) = \alpha^2 nt$$

Thus, the good normalization factor is $\alpha = 1/\sqrt{n}$, as claimed. □

So far, so good, we have a nice problem above, and time now to make a plan, in order to solve it. With the tools that we have, from this book so far, here is such a plan:

PLAN 14.4. *In order to solve our central limiting question, we have to:*

(1) *Apply Fourier and let $n \to \infty$, as to compute the Fourier transform of g_t.*
(2) *Do some combinatorics and calculus, as to compute the moments of g_t.*
(3) *Recover g_t out of its moments, again via combinatorics and calculus.*

Getting to work now, let us start with (1). Things are quickly done here, by using the standard linearization results for convolution, which lead to:

THEOREM 14.5. *Given discrete variables $f_1, f_2, f_3, \ldots$, which are i.i.d., centered, and with common variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim g_t$$

with $n \to \infty$, with g_t being the law having $F(x) = e^{-tx^2/2}$ as Fourier transform.

PROOF. There are several things going on here, the idea being as follows:

(1) Observe first that in terms of moments, the Fourier transform of an arbitrary random variable $f : X \to \mathbb{R}$ is given by the following formula:

$$\begin{aligned} F_f(x) &= E(e^{ixf}) \\ &= E\left(\sum_{k=0}^{\infty} \frac{(ixf)^k}{k!}\right) \\ &= \sum_{k=0}^{\infty} \frac{(ix)^k E(f^k)}{k!} \\ &= \sum_{k=0}^{\infty} \frac{i^k M_k(f)}{k!}\, x^k \end{aligned}$$

(2) In particular, in the case of a centered variable, $E(f) = 0$, as those that we are interested in, the Fourier transform formula that we get is as follows:

$$F_f(x) = 1 - \frac{M_2(f)}{2} \cdot x^2 - i\,\frac{M_3(f)}{6} \cdot x^3 + \ldots$$

Moreover, by further assuming that the Fourier variable is small, $x \simeq 0$, the Fourier transform formula that we get, that we will use in what follows, becomes:

$$F_f(x) = 1 - \frac{M_2(f)}{2} \cdot x^2 + O(x^2)$$

(3) In addition to this, we will also need to know what happens to the Fourier transform when rescaling. But the formula here is very easy to find, as follows:

$$\begin{aligned} F_{\alpha f}(x) &= E(e^{ix\alpha f}) \\ &= E(e^{i\alpha xf}) \\ &= F_f(\alpha x) \end{aligned}$$

(4) Good news, we can now do our computation. By using the above formulae in (2) and (3), the Fourier transform of the variable in the statement is given by:

$$\begin{aligned} F(x) &= \left[F_f\left(\frac{x}{\sqrt{n}}\right)\right]^n \\ &= \left[1-\frac{M_2(f)}{2}\cdot\frac{x^2}{n}+O(n^{-2})\right]^n \\ &= \left[1-\frac{tx^2}{2n}+O(n^{-2})\right]^n \\ &\simeq \left[1-\frac{tx^2}{2n}\right]^n \\ &\simeq e^{-tx^2/2} \end{aligned}$$

(3) We are therefore led to the conclusion in the statement, modulo the fact that we do not know yet that a density g_t having as Fourier transform $F(x)=e^{-tx^2/2}$ really exists, plus perhaps some other abstract issues, related to the continuous measures, to be discussed too. But too late to go back, with our theory on the way, we will go ahead. So, theorem proved, modulo finding that law g_t, which still remains to be done. □

Getting now to step (2) of our Plan 14.4, that is easy to work out too, via some elementary one-variable calculus, with the result here being as follows:

THEOREM 14.6. *The "normal" law g_t, having as Fourier transform*

$$F(x)=e^{-tx^2/2}$$

must have all odd moments zero, and its even moments must be the numbers

$$M_k(g_t)=t^{k/2}\times k!!$$

where $k!!=(k-1)(k-3)(k-5)\ldots$, for $k\in 2\mathbb{N}$.

PROOF. Again, several things going on here, the idea being as follows:

(1) To start with, at the level of formalism and notations, in view of Question 14.2 and of Theorem 14.5, we have adopted the term "normal" for the mysterious law g_t that we are looking for, the one having $F(x)=e^{-tx^2/2}$ as Fourier transform.

(2) Getting towards the computation of the moments, as a first useful observation, according to Theorem 14.5 this normal law g_t must be centered, as shown by:

$$\begin{aligned} f_i = \text{centered} &\implies \sum_{i=1}^{n} f_i = \text{centered} \\ &\implies \frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i = \text{centered} \\ &\implies g_t = \text{centered} \end{aligned}$$

Moreover, the same argument works by replacing "centered" with "having an even function as density", and this shows, via some standard calculus, that we will leave here as an exercise, that the odd moments of our normal law must vanish:

$$M_{2l+1}(g_t) = 0$$

Thus, first assertion proved, and we only have to care about the even moments.

(3) As a comment here, as we will see in a moment, our study below of the moments computes in fact the odd moments too, as being all equal to 0, this time without making reference to Theorem 14.5. Thus, definitely no worries with the odd moments.

(4) Getting to work now, we must reformulate the equation $F(x) = e^{-tx^2/2}$, in terms of moments. We know from the proof of Theorem 14.5 that we have:

$$F(x) = \sum_{k=0}^{\infty} \frac{i^k M_k(g_t)}{k!} x^k$$

On the other hand, we have the following formula, for the exponential:

$$e^{-tx^2/2} = \sum_{r=0}^{\infty} (-1)^r \frac{t^r x^{2r}}{2^r r!}$$

Thus, our equation $F(x) = e^{-tx^2/2}$ takes the following form:

$$\sum_{k=0}^{\infty} \frac{i^k M_k(g_t)}{k!} x^k = \sum_{r=0}^{\infty} (-1)^r \frac{t^r x^{2r}}{2^r r!}$$

(5) As a first observation, the odd moments must vanish, as said in (2) above. As for the even moments, these can be computed as follows:

$$\begin{aligned}
M_k(g_t) &= k! \times \frac{t^{k/2}}{2^{k/2}(k/2)!}\\
&= t^{k/2} \times \frac{k!}{2^{k/2}(k/2)!}\\
&= t^{k/2} \times \frac{2\cdot 3\cdot 4\ldots(k-1)\cdot k}{2\cdot 4\cdot 6\ldots(k-2)\cdot k}\\
&= t^{k/2} \times 3\cdot 5\ldots(k-3)(k-1)\\
&= t^{k/2} \times k!!
\end{aligned}$$

Thus, we are led to the formula in the statement. □

The moment formula that we found is quite interesting, and before going ahead with step (3) of our Plan 14.4, let us look a bit at this, and see what we can further say.

To be more precise, in analogy with what we know about the Poisson laws, and about the Bessel laws too, making reference to interesting combinatorics and partitions, when it comes to moments, we have the following result, regarding the normal laws:

THEOREM 14.7. *The moments of the normal law g_t are given by*

$$M_k(g_t) = t^{k/2}|P_2(k)|$$

for any $k \in \mathbb{N}$, with $P_2(k)$ standing for the pairings of $\{1,\ldots,k\}$.

PROOF. This is a reformulation of Theorem 14.6, the idea being as follows:

(1) We know from Theorem 14.6 that the moments of the normal law $M_k = M_k(g_t)$ that we are interested in are given by the following formula, with the convention $k!! = 0$ for k odd, and $k!! = (k-1)(k-3)(k-5)\ldots$ for k even, for the double factorials:

$$M_k(g_t) = t^{k/2} \times k!!$$

Now observe that, according to our above convention for the double factorials, these are subject to the following recurrence relation, with initial data $1!! = 0, 2!! = 1$:

$$k!! = (k-1)(k-2)!!$$

We conclude that the moments of the normal law $M_k = M_k(g_t)$ are subject to the following recurrence relation, with initial data $M_1 = 0, M_2 = t$:

$$M_k = t(k-1)M_{k-2}$$

(2) On the other hand, let us first count the pairings of the set $\{1,\ldots,k\}$. In order to have such a pairing, we must pair 1 with one of the numbers $2,\ldots,k$, and then use a

pairing of the remaining $k-2$ numbers. Thus, we have the following recurrence formula for the number P_k of such pairings, with the initial data $P_1 = 0, P_2 = 1$:

$$P_k = (k-1)P_{k-2}$$

Now by multiplying by $t^{k/2}$, the resulting numbers $N_k = t^{k/2}P_k$ will be subject to the following recurrence relation, with initial data $N_1 = 0, N_2 = t$:

$$N_k = t(k-1)N_{k-2}$$

(3) Thus, the moments $M_k = M_k(g_t)$ and the numbers $N_k = t^{k/2}P_k$ are subject to the same recurrence relation, with the same initial data, so they are equal, as claimed. □

Still in analogy with what we know about the Poisson laws, and about the Bessel laws too, we can further process what we found in Theorem 14.7, and we are led to:

THEOREM 14.8. *The moments of the normal law g_t are given by*

$$M_k(g_t) = \sum_{\pi \in P_2(k)} t^{|\pi|}$$

where $P_2(k)$ is the set of pairings of $\{1, \ldots, k\}$, and $|.|$ is the number of blocks.

PROOF. This is a quick reformulation of Theorem 14.7, with the number of blocks of a pairing of $\{1, \ldots, k\}$ being trivially $k/2$, independently of the pairing. □

It is possible to do some more study here, again in relation with what we know about the Poisson laws, and the Bessel laws too, and we have for instance:

THEOREM 14.9. *The normal laws satisfy the formula*

$$g_s * g_t = g_{s+t}$$

for any $s, t > 0$. Thus, they form a convolution semigroup.

PROOF. This is standard from what we have, the idea being as follows:

(1) To start with, the semigroup property of the normal laws follows indeed from Theorem 14.5, the log of the Fourier transform being linear in t.

(2) However, as a technical remark, the linearization result for the convolution that we used was formally established before only for the discrete measures. So, instead of further thinking at this, let us pull out a new, elementary proof for $g_s * g_t = g_{s+t}$.

(3) In order to do this, consider, as in Theorem 14.5, on one hand i.i.d. centered variables $f_1, f_2, f_3, \ldots$ having variance $s > 0$, and on the other hand i.i.d. centered variables $h_1, h_2, h_3, \ldots$ having variance $t > 0$. According to Theorem 14.5, we have:

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim g_s \quad , \quad \frac{1}{\sqrt{n}} \sum_{i=1}^{n} h_i \sim g_t$$

Now let us sum these formulae. Assuming that the variables $f_1, f_2, f_3, \ldots$ that we used were independent from the variables $h_1, h_2, h_3, \ldots$, we obtain in this way:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(f_i+h_i)\sim g_s*g_t$$

(4) On the other hand, yet another application of Theorem 14.5, with the remark that by independence, the variance of f_i+h_i is indeed $s+t$, gives the following formula:

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}(f_i+h_i)\sim g_{s+t}$$

Thus, we are led to the semigroup formula $g_s*g_t=g_{s+t}$, as desired. □

As a philosophical conclusion now to all this, let us formulate:

CONCLUSION 14.10. *The normal laws g_t have properties which are quite similar to those of the Poisson laws p_t, and combinatorially, the passage*

$$p_t\to g_t$$

appears by replacing the partitions with the pairings.

Which sounds quite conceptual, and promising, hope you agree with me. In the meantime, however, we still need to know what the density of g_t is.

14b. Gauss, normality

So, let us get now to step (3) of our Plan 14.4. This does not look obvious at all, but some partial integration know-how leads us to the following statement:

THEOREM 14.11. *The normal laws are given by*

$$g_t=\frac{1}{\sqrt{2t}\cdot I}\,e^{-x^2/2t}dx$$

with the constant on the bottom being $I=\int_{\mathbb{R}}e^{-x^2}dx$.

PROOF. This comes from partial integration, as follows:

(1) Let us first do a naive computation. Consider the following quantities:

$$M_k=\int_{\mathbb{R}}x^ke^{-x^2}dx$$

It is quite obvious that by partial integration we will get a recurrence formula for these numbers, similar to the one that we have for the moments of the normal laws. So, let us

do this. By partial integration we obtain the following formula, for any $k \in \mathbb{N}$:

$$\begin{aligned} M_k &= -\frac{1}{2}\int_{\mathbb{R}} x^{k-1}\left(e^{-x^2}\right)' dx \\ &= \frac{1}{2}\int_{\mathbb{R}} (k-1)x^{k-2}e^{-x^2}dx \\ &= \frac{k-1}{2}\cdot M_{k-2} \end{aligned}$$

(2) Thus, we are on the good way, with the recurrence formula that we got being the same as that for the moments of $g_{1/2}$. Now let us fine-tune this, as to reach to the same recurrence as for the moments of g_t. Consider the following quantities:

$$N_k = \int_{\mathbb{R}} x^k e^{-x^2/2t}dx$$

By partial integration as before, we obtain the following formula:

$$\begin{aligned} N_k &= \int_{\mathbb{R}} (tx^{k-1})\left(-e^{-x^2/2t}\right)' dx \\ &= \int_{\mathbb{R}} t(k-1)x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)\int_{\mathbb{R}} x^{k-2}e^{-x^2/2t}dx \\ &= t(k-1)N_{k-2} \end{aligned}$$

(3) Thus, almost done, and it remains to discuss normalization. We know from the above that we must have a formula as follows, with I_t being a certain constant:

$$g_t = \frac{1}{I_t}\cdot e^{-x^2/2t}\,dx$$

But the constant I_t must be the one making g_t of mass 1, and so:

$$\begin{aligned} I_t &= \int_{\mathbb{R}} e^{-x^2/2t}\,dx \\ &= \int_{\mathbb{R}} e^{-2ty^2/2t}\sqrt{2t}dy \\ &= \sqrt{2t}\int_{\mathbb{R}} e^{-y^2}dy \end{aligned}$$

Thus, we are led to the formula in the statement. □

What we did in the above is good work, and it remains to compute the constant I appearing in Theorem 14.11, given by the following formula, and called Gauss integral:

$$I=\int_{\mathbb{R}}e^{-x^2}dx$$

With some advanced integration know-how, this can be done, as follows:

THEOREM 14.12. *We have the following formula,*

$$\int_{\mathbb{R}}e^{-x^2}dx=\sqrt{\pi}$$

called Gauss integral formula.

PROOF. This is something truly magic, the idea being as follows:

(1) To start with, we can certainly integrate e^{-x^2} by using the formula of the exponential series, and the primitive which is worth 0 at $x=0$ is given by:

$$\int e^{-x^2}=\sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{(2k+1)k!}$$

However, this series is not computable, in terms of the known, familiar series.

(2) Thus, no primitive, but we can still ask for the computation of $\int_{\mathbb{R}}e^{-x^2}dx$, who knows. And here, another surprise awaits us, this is simply undoable, with bare hands, I mean all the formulae and tricks that we learned so far fail, for this integral.

(3) Which seems to send our problem to the trash can. However, and here comes the magic, the Gauss integral can be computed by using two dimensions, as follows:

$$\begin{aligned}\int_{\mathbb{R}}\int_{\mathbb{R}}e^{-x^2-y^2}dxdy&=4\int_0^{\infty}\int_0^{\infty}e^{-x^2-y^2}dxdy\\&=4\int_0^{\infty}\int_0^{\infty}e^{-t^2y^2-y^2}ydtdy\\&=4\int_0^{\infty}\int_0^{\infty}ye^{-y^2(1+t^2)}dydt\\&=2\int_0^{\infty}\int_0^{\infty}\left(-\frac{e^{-y^2(1+t^2)}}{1+t^2}\right)'dydt\\&=2\int_0^{\infty}\frac{dt}{1+t^2}\\&=2\int_0^{\infty}(\arctan t)'dt\\&=\pi\end{aligned}$$

(4) Amazing all this, isn't it. Let us mention too that there are some other known proof of the Gauss formula, but all using two dimensions. Among these, we have for instance the following quick computation, assuming some polar coordinate know-how:

$$\begin{aligned}\int_{\mathbb{R}}\int_{\mathbb{R}}e^{-x^2-y^2}dxdy &= \int_0^{2\pi}\int_0^{\infty}e^{-r^2\cos^2t-r^2\sin^2t}rdrdt\\ &= \int_0^{2\pi}\int_0^{\infty}e^{-r^2}rdrdt\\ &= 2\pi\int_0^{\infty}\left(-\frac{e^{-r^2}}{2}\right)'dr\\ &= \pi\end{aligned}$$

And for more on this, and more specifically on the formula $dxdy=rdrdt$ that we used, you can check any reasonably advanced calculus book, such as mine [11]. □

Very nice, so as a final conclusion to our study, started long ago, in the beginning of this chapter, we can now formulate the Central Limit Theorem (CLT), as follows:

THEOREM 14.13 (CLT). *Given discrete random variables $f_1,f_2,f_3,\ldots$, which are i.i.d., centered, and with common variance $t>0$, we have*

$$\frac{1}{\sqrt{n}}\sum_{i=1}^{n}f_i\sim g_t$$

in the $n\to\infty$ limit, in moments, with the limiting mesure being

$$g_t=\frac{1}{\sqrt{2\pi t}}e^{-x^2/2t}dx$$

called normal, or Gaussian law of parameter $t>0$.

PROOF. This follows indeed from our various results above, and more specifically from Theorem 14.5 and Theorem 14.6 for the general discussion and terminology, and from Theorem 14.11 and Theorem 14.12 for the computations which are needed. □

Quite nice all this, we just built here good foundations for advanced probability, and mathematics in general. However, thinking a bit retrospectively, frankly, who could have guessed that such a fundamental topic as central limits would lead us into the complicated mathematics of the Gauss integral, involving that 2 dimensions instead of 1.

Mystery, I don't have an answer to this, and nor do you, I guess. This being said, wait, I can hear some noise coming from the living room, where rat studies:

RAT 14.14. *I told you mate, classical mathematics and Gauss' $\frac{1}{\sqrt{2\pi}}e^{-x^2/2}$ are more complicated than free mathematics and Wigner's $\frac{1}{2\pi}\sqrt{4-x^2}$.*

Humm, quite interesting all this, closing I guess a centuries-old debate, about why the proof of the Gauss formula is something so complicated. So, with the hope that us humans will someday reach to the level of understanding of cats and rats, on how this world was made by its creator, from bare freeness, via suitable thermodynamic limits.

Getting back now to our regular business, probability theory developed without much philosophy, let us study more in detail the laws that we found. Normally we already have everything that is needed, but it is instructive at this point to do some computations, based on the explicit formula of g_t found above, and on Theorem 14.12.

With this idea in mind, that of rewriting everything that we knew, prior to our work in this section on the Gauss formula, we first have the following result:

PROPOSITION 14.15. *We have the variance formula*

$$V(g_t) = t$$

valid for any $t > 0$.

PROOF. We already know this, but we can establish this as well directly, starting from our formula of g_t from Theorem 14.13. Indeed, the first moment is 0, because our normal law g_t is centered. As for the second moment, this can be computed as follows:

$$\begin{aligned} M_2 &= \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} x^2 e^{-x^2/2t} dx \\ &= \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} (tx) \left(-e^{-x^2/2t} \right)' dx \\ &= \frac{1}{\sqrt{2\pi t}} \int_{\mathbb{R}} t e^{-x^2/2t} dx \\ &= t \end{aligned}$$

We conclude from this that the variance is $V = M_2 = t$, as claimed. □

More generally, we can recover in this way the computation of all moments:

THEOREM 14.16. *The even moments of the normal law are the numbers*

$$M_k(g_t) = t^{k/2} \times k!!$$

where $k!! = (k-1)(k-3)(k-5)\ldots$, *and the odd moments vanish.*

PROOF. Again, we already know this, but we can establish this as well directly, starting from our formula above of g_t. Indeed, we have the following computation:

$$\begin{aligned}
M_k &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} y^k e^{-y^2/2t}dy\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} (ty^{k-1})\left(-e^{-y^2/2t}\right)' dy\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} t(k-1)y^{k-2}e^{-y^2/2t}dy\\
&= t(k-1)\times\frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} y^{k-2}e^{-y^2/2t}dy\\
&= t(k-1)M_{k-2}
\end{aligned}$$

Thus by recurrence, we are led to the formula in the statement. □

Let us end this discussion with the following result, that we already knew as well:

THEOREM 14.17. *We have the following formula, valid for any $t > 0$:*

$$F_{g_t}(x) = e^{-tx^2/2}$$

In particular, the normal laws satisfy $g_s * g_t = g_{s+t}$, for any $s, t > 0$.

PROOF. As before, we already know this, but we can establish now the Fourier transform formula as well directly, by using the explicit formula of g_t, as follows:

$$\begin{aligned}
F_{g_t}(x) &= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-y^2/2t+ixy}dy\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-(y/\sqrt{2t}-\sqrt{t/2}ix)^2-tx^2/2}dy\\
&= \frac{1}{\sqrt{2\pi t}}\int_{\mathbb{R}} e^{-z^2-tx^2/2}\sqrt{2t}dz\\
&= \frac{1}{\sqrt{\pi}}e^{-tx^2/2}\int_{\mathbb{R}} e^{-z^2}dz\\
&= e^{-tx^2/2}
\end{aligned}$$

As for the last assertion, this follows from the fact that $\log F_{g_t}$ is linear in t. □

14c. Complex variables

Let us discuss now the complex analogues of all the above, with a notion of complex normal, or Gaussian law. To start with, we have the following definition:

DEFINITION 14.18. *A complex random variable is a variable $f : X \to \mathbb{C}$. In the discrete case, the law of such a variable is the complex probability measure*

$$\mu = \sum_i \alpha_i \delta_{z_i} \quad , \quad \alpha_i \geq 0 \quad , \quad \sum_i \alpha_i = 1 \quad , \quad z_i \in \mathbb{C}$$

given by the following formula, with P being the probability over X,

$$\mu = \sum_{z \in \mathbb{C}} P(f = z) \delta_z$$

with the sum being finite or countable, as per our discretness assumption.

In order to understand the precise relation with the real theory, that we know well, we can decompose any complex variable $f : X \to \mathbb{C}$ as a sum, as follows:

$$f = g + ih \quad , \quad g = Re(f),\ h = Im(f)$$

With this done, we have the following computation, for the corresponding law:

$$\begin{aligned}
\mu &= \sum_{z \in \mathbb{C}} P(f = z) \delta_z \\
&= \sum_{x,y \in \mathbb{R}} P(f = x + iy) \delta_{x+iy} \\
&= \sum_{x,y \in \mathbb{R}} P(g + ih = x + iy) \delta_{x+iy} \\
&= \sum_{x,y \in \mathbb{R}} P(g = x, h = y) \delta_{x+iy}
\end{aligned}$$

In the case where the real and imaginary parts $g, h : X \to \mathbb{R}$ are independent, we can say more about this, with the above computation having the following continuation:

$$\begin{aligned}
\mu &= \sum_{x,y \in \mathbb{R}} P(g = x, h = y) \delta_{x+iy} \\
&= \sum_{x,y \in \mathbb{R}} P(g = x) P(h = y) \delta_{x+iy} \\
&= \sum_{x,y \in \mathbb{R}} P(g = x) P(h = y) \delta_x * \delta_{iy} \\
&= \left(\sum_{x \in \mathbb{R}} P(g = x) \delta_x \right) * \left(\sum_{y \in \mathbb{R}} P(h = y) \delta_{iy} \right) \\
&= \mu_g * i\mu_h
\end{aligned}$$

To be more precise, we have used here in the beginning the independence of the variables $h, g : X \to \mathbb{R}$, and at the end we have denoted the measure on the right, which is obtained from μ_h by putting this measure on the imaginary axis, by $i\mu_h$.

All this is quite interesting, going beyond what we know so far about basic probability, in the real case, so let us record this finding, along with a bit more, as follows:

THEOREM 14.19. *For a discrete variable $f : X \to \mathbb{C}$, decomposed into real and imaginary parts as $f = g + ih$, and with g, h assumed independent, we have*

$$\mu_f = \mu_g * i\mu_h$$

with $*$ being the usual convolution operation, $\delta_z * \delta_t = \delta_{z+t}$, and with $\mu \to i\mu$ denoting the rotated version, $\mathbb{R} \to i\mathbb{R}$. If g, h are not independent, this formula does not hold.

PROOF. We already know that the first assertion holds, as explained in the above. As for the second assertion, this follows by carefully examining the above computation. Indeed, we have used only at one point the independence of g, h, so for the formula $\mu_f = \mu_g * i\mu_h$ to hold, the equality used at that point, which is as follows, must hold:

$$\sum_{x,y\in\mathbb{R}} P(g = x, h = y)\delta_{x+iy} = \sum_{x,y\in\mathbb{R}} P(g = x)P(h = y)\delta_{x+iy}$$

But this is the same as saying that the following must hold, for any x, y:

$$P(g = x, h = y) = P(g = x)P(h = y)$$

We conclude that, in order for the decomposition formula $\mu_f = \mu_g * i\mu_h$ to hold, the real and imaginary parts $g, h : X \to \mathbb{R}$ must be independent, as stated. □

Going now to the point, probabilistic limiting theorems, let us discuss the complex analogue of the CLT. We have the following statement, to start with:

THEOREM 14.20. *Given discrete complex variables $f_1, f_2, f_3, \ldots$ whose real and imaginary parts are i.i.d., centered, and with common variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim C_t$$

with $n \to \infty$, in moments, where C_t is the law of a complex variable whose real and imaginary parts are independent, and each following the law g_t.

PROOF. This follows indeed from the real CLT, established in Theorem 14.13, simply by taking the real and imaginary parts of all the variables involved. □

It is tempting at this point to call Theorem 14.20 the complex CLT, or CCLT, but before doing that, let us study a bit more all this. We would like to have a better

understanding of the limiting law C_t at the end, and for this purpose, let us look at a sum as follows, with a, b being real independent variables, both following the normal law g_t:

$$c = a + ib$$

To start with, this variable is centered, in a complex sense, because we have:

$$\begin{aligned} E(c) &= E(a + ib) \\ &= E(a) + iE(b) \\ &= 0 + i \cdot 0 \\ &= 0 \end{aligned}$$

Regarding now the variance, things are more complicated, because the usual variance formula from the real case, which is $V(c) = E(c^2)$ in the centered case, will not provide us with a positive number, in the case where our variable is not real. So, in order to have a variance which is real, and positive too, we must rather use a formula of type $V(c) = E(|c|^2)$, in the centered case. And, with this convention for the variance, we have then the following computation, for the variance of the above variable c:

$$\begin{aligned} V(c) &= E(|c|^2) \\ &= E(a^2 + b^2) \\ &= E(a^2) + E(b^2) \\ &= V(a^2) + V(b^2) \\ &= t + t \\ &= 2t \end{aligned}$$

But this suggests to divide everything by $\sqrt{2}$, as to have in the end a variable having complex variance t, in our sense, and we are led in this way into:

DEFINITION 14.21. *The complex normal, or Gaussian law of parameter $t > 0$ is*

$$G_t = law\left(\frac{1}{\sqrt{2}}(a + ib)\right)$$

where a, b are real and independent, each following the law g_t.

In short, the complex normal laws appear as natural complexifications of the real normal laws. As in the real case, these measures form convolution semigroups:

PROPOSITION 14.22. *The complex Gaussian laws have the property*

$$G_s * G_t = G_{s+t}$$

for any $s, t > 0$, and so they form a convolution semigroup.

PROOF. This follows indeed from the real result, namely $g_s * g_t = g_{s+t}$, established in Theorem 14.9, simply by taking real and imaginary parts. □

We have as well the following complex analogue of the CLT:

THEOREM 14.23 (CCLT). *Given discrete complex variables $f_1, f_2, f_3, \ldots$ whose real and imaginary parts are i.i.d. and centered, and having variance $t > 0$, we have*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} f_i \sim G_t$$

with $n \to \infty$, in moments.

PROOF. This follows indeed from our previous CCLT result, from Theorem 14.20, by dividing everything by $\sqrt{2}$, as explained in the above. □

Regarding now the moments, the situation here is more complicated than in the real case, because in order to have good results, we have to deal with both the complex variables, and their conjugates. Let us formulate the following definition:

DEFINITION 14.24. *The moments a complex variable $f \in L^\infty(X)$ are the numbers*

$$M_k = E(f^k)$$

depending on colored integers $k = \circ \bullet \bullet \circ \ldots$, with the conventions

$$f^\emptyset = 1 \quad , \quad f^\circ = f \quad , \quad f^\bullet = \bar{f}$$

and multiplicativity, in order to define the colored powers f^k.

As an illustration for this notion, which is something very intuitive, here are the formulae of the four possible order 2 moments of a complex variable f:

$$M_{\circ\circ} = E(f^2) \quad , \quad M_{\circ\bullet} = E(f\bar{f})$$

$$M_{\bullet\circ} = E(\bar{f}f) \quad , \quad M_{\bullet\bullet} = E(\bar{f}^2)$$

Observe that, since $f, \bar{f}$ commute, we have the following identity, which shows that there is a bit of redundancy in our above definition, as formulated:

$$M_{\circ\bullet} = M_{\bullet\circ}$$

In fact, again since $f, \bar{f}$ commute, we can permute terms, in the general context of Definition 14.24, and restrict the attention to exponents of the following type:

$$k = \ldots \circ\circ\circ \bullet\bullet\bullet\bullet \ldots$$

However, our results about the complex Gaussian laws, and other complex laws, later on, not to talk about laws of matrices, random matrices and other noncommuting variables, that will appear later too, will look better without doing this. So, we will use Definition 14.24 as stated. Getting to work now, we first have the following result:

THEOREM 14.25. *The moments of the complex normal law are given by*

$$M_k(G_t) = \begin{cases} t^p p! & (k \text{ uniform, of length } 2p) \\ 0 & (k \text{ not uniform}) \end{cases}$$

where $k = \circ\bullet\bullet\circ\ldots$ is called uniform when it contains the same number of $\circ$ and $\bullet$.

PROOF. We must compute the moments, with respect to colored integer exponents $k = \circ\bullet\bullet\circ\ldots$ as above, of the variable from Definition 14.21, namely:

$$f = \frac{1}{\sqrt{2}}(a + ib)$$

We can assume that we are in the case $t = 1$, and the proof here goes as follows:

(1) As a first observation, in the case where our exponent $k = \circ\bullet\bullet\circ\ldots$ is not uniform, a standard rotation argument shows that the corresponding moment of f vanishes. To be more precise, the variable $f' = wf$ is complex Gaussian too, for any complex number $w \in \mathbb{T}$, and from $M_k(f) = M_k(f')$ we obtain $M_k(f) = 0$, in this case.

(2) In the uniform case now, where the exponent $k = \circ\bullet\bullet\circ\ldots$ consists of p copies of $\circ$ and p copies of $\bullet$, the corresponding moment can be computed as follows:

$$\begin{aligned} M_k &= \int (f\bar{f})^p \\ &= \frac{1}{2^p}\int (a^2 + b^2)^p \\ &= \frac{1}{2^p}\sum_r \binom{p}{r}\int a^{2r}\int b^{2p-2r} \\ &= \frac{1}{2^p}\sum_r \binom{p}{r}(2r)!!(2p-2r)!! \\ &= \frac{1}{2^p}\sum_r \frac{p!}{r!(p-r)!}\cdot\frac{(2r)!}{2^r r!}\cdot\frac{(2p-2r)!}{2^{p-r}(p-r)!} \\ &= \frac{p!}{4^p}\sum_r \binom{2r}{r}\binom{2p-2r}{p-r} \end{aligned}$$

(3) In order to finish now the computation, let us recall that we have the following formula, coming from the generalized binomial formula, that we know from chapter 8:

$$\frac{1}{\sqrt{1+t}} = \sum_{q=0}^{\infty}\binom{2q}{q}\left(\frac{-t}{4}\right)^q$$

By taking the square of this series, we obtain the following formula:

$$\frac{1}{1+t}=\sum_p\left(\frac{-t}{4}\right)^p\sum_r\binom{2r}{r}\binom{2p-2r}{p-r}$$

Now by looking at the coefficient of t^p on both sides, we conclude that the sum on the right equals 4^p. Thus, we can finish the moment computation in (2), as follows:

$$M_k=\frac{p!}{4^p}\times 4^p=p!$$

We are therefore led to the conclusion in the statement. □

Before going further, with a finer study of the moments of the complex normal laws, let us record the following interesting consequence, of the above:

THEOREM 14.26. *The moments of the Rayleigh law, given by*

$$R_t=law(|G_t|)$$

are given by the formula $M_k=t^kk!$.

PROOF. This follows indeed from Theorem 14.25, or simply from the computation (2) in the above proof, first at $t=1$, and then by rescaling by $t>0$, in general. □

Many other interesting things can be said about the Rayleigh laws, notably with the following statement, called Rayleigh Central Limiting Theorem:

THEOREM 14.27 (RCLT). *Given discrete complex variables $f_1,f_2,f_3,\ldots$ whose real and imaginary parts are i.i.d. and centered, and having variance $t>0$, we have*

$$\left|\frac{1}{\sqrt{n}}\sum_{i=1}^nf_i\right|\sim R_t$$

with $n\to\infty$, in moments.

PROOF. This follows indeed from our previous Central Limiting result, namely the CCLT from Theorem 14.23, by taking absolute values on both sides. □

And I will leave it to you to learn more about this, Rayleigh laws and related mathematics, notably with the notion of Gaussian vectors, and their lengths.

Getting back now to the complex normal laws, what we have in Theorem 14.25 about them is usually what is needed in practice, when dealing with moments. But, as before with the real Gaussian laws, or even further before with the Poisson and Bessel laws, a better-looking statement regarding the moments is in terms of partitions.

Indeed, given a colored integer $k=\circ\bullet\bullet\circ\ldots$, let us say that $\pi\in P_2(k)$ is matching when it pairs $\circ-\bullet$ symbols. With this convention, we have the following result:

THEOREM 14.28. *The moments of the complex normal law are the numbers*

$$M_k(G_t) = \sum_{\pi\in\mathcal{P}_2(k)} t^{|\pi|}$$

where $\mathcal{P}_2(k)$ are the matching pairings of $\{1,\ldots,k\}$, and $|.|$ is the number of blocks.

PROOF. This is a reformulation of Theorem 14.25. Indeed, we can assume that we are in the case $t = 1$, and here we know from Theorem 14.25 that the moments are:

$$M_k = \begin{cases} (|k|/2)! & (k \text{ uniform}) \\ 0 & (k \text{ not uniform}) \end{cases}$$

On the other hand, the numbers $|\mathcal{P}_2(k)|$ are given by exactly the same formula. Indeed, in order to have a matching pairing of k, our exponent $k = \circ\bullet\bullet\circ\ldots$ must be uniform, consisting of p copies of $\circ$ and p copies of $\bullet$, with $p = |k|/2$. But then the matching pairings of k correspond to the permutations of the $\bullet$ symbols, as to be matched with $\circ$ symbols, and so we have $p!$ such pairings. Thus, we have the same formula as for the moments of f, and we are led to the conclusion in the statement. □

In practice, we also need to know how to compute joint moments. We have here:

THEOREM 14.29 (Wick formula). *Given independent variables f_i, each following the complex normal law G_t, with $t > 0$ being a fixed parameter, we have the formula*

$$E\left(f_{i_1}^{k_1}\ldots f_{i_s}^{k_s}\right) = t^{s/2}\#\left\{\pi\in\mathcal{P}_2(k)\Big|\pi\leq\ker i\right\}$$

where $k = k_1\ldots k_s$ and $i = i_1\ldots i_s$, for the joint moments of these variables, where $\pi\leq\ker i$ means that the indices of i must fit into the blocks of π, in the obvious way.

PROOF. This is something well-known, which can be proved as follows:

(1) Let us first discuss the case where we have a single variable f, which amounts in taking $f_i = f$ for any i in the formula in the statement. What we have to compute here are the moments of f, with respect to colored integer exponents $k = \circ\bullet\bullet\circ\ldots$, and the formula in the statement tells us that these moments must be:

$$E(f^k) = t^{|k|/2}|\mathcal{P}_2(k)|$$

But this is the formula in Theorem 14.28, so we are done with this case.

(2) In general now, when expanding the product $f_{i_1}^{k_1}\ldots f_{i_s}^{k_s}$ and rearranging the terms, we are left with doing a number of computations as in (1), and then making the product of the expectations that we found. But this amounts in counting the partitions in the statement, with the condition $\pi\leq\ker i$ there standing for the fact that we are doing the various type (1) computations independently, and then making the product. □

14d. Hyperspherical laws

Now that we know about the normal laws, their algebra and analysis, what about geometry? In answer, there is something here quite interesting, to be discovered too. Let us start with the following result, making us experts in multivariable calculus:

THEOREM 14.30. *The polynomial integrals over the unit sphere $S_{\mathbb{R}}^{N-1} \subset \mathbb{R}^N$, with respect to the normalized, mass 1 measure, are given by the following formula,*

$$\int_{S_{\mathbb{R}}^{N-1}} x_1^{k_1} \ldots x_N^{k_N}\, dx = \frac{(N-1)!!k_1!! \ldots k_N!!}{(N+\Sigma k_i-1)!!}$$

valid when all exponents k_i are even. If an exponent k_i is odd, the integral vanishes.

PROOF. Assume first that one of the exponents k_i is odd. We can make then the following change of variables, which shows that the integral in the statement vanishes:

$$x_i \to -x_i$$

Assume now that all exponents k_i are even. As a first observation, the result holds indeed at $N = 2$, due to the Wallis formula from chapter 12, which reads:

$$\int_0^{\pi/2} \cos^p t \sin^q t\, dt = \left(\frac{\pi}{2}\right)^{\varepsilon(p)\varepsilon(q)} \frac{p!!q!!}{(p+q+1)!!} = \frac{p!!q!!}{(p+q+1)!!}$$

In the general case now, where the dimension $N \in \mathbb{N}$ is arbitrary, the integral in the statement can be written in spherical coordinates, as follows:

$$I = \frac{2^N}{A} \int_0^{\pi/2} \ldots \int_0^{\pi/2} x_1^{k_1} \ldots x_N^{k_N}\, J\, dt_1 \ldots dt_{N-1}$$

Here A is the area of the sphere, J is the Jacobian, and the 2^N factor comes from the restriction to the $1/2^N$ part of the sphere where all the coordinates are positive. According to the formulae in chapter 12, the normalization constant in front of the integral is:

$$\frac{2^N}{A} = \left(\frac{2}{\pi}\right)^{[N/2]} (N-1)!!$$

As for the unnormalized integral, this is given by:

$$\begin{aligned} I' = \int_0^{\pi/2} \ldots \int_0^{\pi/2} \quad & (\cos t_1)^{k_1} (\sin t_1 \cos t_2)^{k_2} \\ & \vdots \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \cos t_{N-1})^{k_{N-1}} \\ & (\sin t_1 \sin t_2 \ldots \sin t_{N-2} \sin t_{N-1})^{k_N} \\ & \sin^{N-2} t_1 \sin^{N-3} t_2 \ldots \sin^2 t_{N-3} \sin t_{N-2} \\ & dt_1 \ldots dt_{N-1} \end{aligned}$$

By rearranging the terms, we obtain the following formula:

$$\begin{aligned} I' &= \int_0^{\pi/2} \cos^{k_1} t_1 \sin^{k_2+\ldots+k_N+N-2} t_1 \, dt_1 \\ &\quad \int_0^{\pi/2} \cos^{k_2} t_2 \sin^{k_3+\ldots+k_N+N-3} t_2 \, dt_2 \\ &\quad \vdots \\ &\quad \int_0^{\pi/2} \cos^{k_{N-2}} t_{N-2} \sin^{k_{N-1}+k_N+1} t_{N-2} \, dt_{N-2} \\ &\quad \int_0^{\pi/2} \cos^{k_{N-1}} t_{N-1} \sin^{k_N} t_{N-1} \, dt_{N-1} \end{aligned}$$

Now by using the above-mentioned formula at $N = 2$, this gives:

$$\begin{aligned} I' &= \frac{k_1!!(k_2+\ldots+k_N+N-2)!!}{(k_1+\ldots+k_N+N-1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-2)} \\ &\quad \frac{k_2!!(k_3+\ldots+k_N+N-3)!!}{(k_2+\ldots+k_N+N-2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(N-3)} \\ &\quad \vdots \\ &\quad \frac{k_{N-2}!!(k_{N-1}+k_N+1)!!}{(k_{N-2}+k_{N-1}+l_N+2)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(1)} \\ &\quad \frac{k_{N-1}!!k_N!!}{(k_{N-1}+k_N+1)!!}\left(\frac{\pi}{2}\right)^{\varepsilon(0)} \end{aligned}$$

By simplifying and putting everything together, we obtain from this:

$$I = \left(\frac{2}{\pi}\right)^{[N/2]} (N-1)!! \times \frac{k_1!! \ldots k_N!!}{(\Sigma k_i + N - 1)!!}$$

Thus, we are led to the conclusion in the statement. □

Good news, we can now formulate a quite conceptual result, as follows:

THEOREM 14.31. *The moments of the hyperspherical variables are*

$$\int_{S_{\mathbb{R}}^{N-1}} x_i^k dx = \frac{(N-1)!!k!!}{(N+k-1)!!}$$

and the rescaled variables $y_i = \sqrt{N}x_i$ *become normal and independent with* $N \to \infty$.

PROOF. The moment formula in the statement follows from the general formula in Theorem 14.30. As a consequence, with $N \to \infty$ we have the following estimate:

$$\begin{aligned}\int_{S_{\mathbb{R}}^{N-1}} x_i^k dx &\simeq N^{-k/2} \times k!! \\ &= N^{-k/2} M_k(g_1)\end{aligned}$$

Thus, the rescaled variables $\sqrt{N}x_i$ become normal with $N \to \infty$, as claimed. As for the proof of the asymptotic independence, this is standard too, once again by using the formula in Theorem 14.30. Indeed, the joint moments of $x_1, \ldots, x_N$ are given by:

$$\begin{aligned}\int_{S_{\mathbb{R}}^{N-1}} x_1^{k_1} \ldots x_N^{k_N}\, dx &= \frac{(N-1)!!k_1!! \ldots k_N!!}{(N+\Sigma k_i-1)!!} \\ &\simeq N^{-\Sigma k_i} \times k_1!! \ldots k_N!!\end{aligned}$$

By rescaling, the joint moments of the variables $y_i = \sqrt{N}x_i$ are given by:

$$\int_{S_{\mathbb{R}}^{N-1}} y_1^{k_1} \ldots y_N^{k_N}\, dx \simeq k_1!! \ldots k_N!!$$

Thus, we have multiplicativity, and so independence with $N \to \infty$, as claimed. □

In order to discuss now the complex analogue of Theorem 14.31, we will need:

THEOREM 14.32. *We have the following integration formula over the complex sphere $S_{\mathbb{C}}^{N-1} \subset \mathbb{C}^N$, with respect to the normalized uniform measure,*

$$\int_{S_{\mathbb{C}}^{N-1}} |z_1|^{2k_1} \ldots |z_N|^{2k_N}\, dz = \frac{(N-1)!k_1! \ldots k_n!}{(N+\sum k_i-1)!}$$

valid for any exponents $k_i \in \mathbb{N}$. As for the other polynomial integrals in $z_1, \ldots, z_N$ and their conjugates $\bar{z}_1, \ldots, \bar{z}_N$, these all vanish.

PROOF. Consider indeed a polynomial integral over $S_{\mathbb{C}}^{N-1}$, containing the same number of plain and conjugated variables, as to not vanish trivially, written as follows:

$$I = \int_{S_{\mathbb{C}}^{N-1}} z_{i_1} \bar{z}_{i_2} \ldots z_{i_{2k-1}} \bar{z}_{i_{2k}}\, dz$$

By using transformations of type $p \to \lambda p$ with $|\lambda| = 1$, we see that this integral I vanishes, unless each z_a appears as many times as $\bar{z}_a$ does, and this gives the last assertion. So, assume now that we are in the non-vanishing case. Then the k_a copies of z_a and the k_a copies of $\bar{z}_a$ produce by multiplication a factor $|z_a|^{2k_a}$, so we have:

$$I = \int_{S_{\mathbb{C}}^{N-1}} |z_1|^{2k_1} \ldots |z_N|^{2k_N}\, dz$$

Now by using the standard identification $S_{\mathbb{C}}^{N-1} \simeq S_{\mathbb{R}}^{2N-1}$, we obtain:

$$\begin{aligned} I &= \int_{S_{\mathbb{R}}^{2N-1}} (x_1^2 + y_1^2)^{k_1} \ldots (x_N^2 + y_N^2)^{k_N} \, d(x,y) \\ &= \sum_{r_1 \ldots r_N} \binom{k_1}{r_1} \ldots \binom{k_N}{r_N} \int_{S_{\mathbb{R}}^{2N-1}} x_1^{2k_1-2r_1} y_1^{2r_1} \ldots x_N^{2k_N-2r_N} y_N^{2r_N} \, d(x,y) \end{aligned}$$

But with this in hand, we can use Theorem 14.30 for the integration, and after some summation work, good exercise for you, we are led to the formula in the statement. □

We can now complement Theorem 14.31 with a complex analogue of it, as follows:

THEOREM 14.33. *The moments of the complex hyperspherical variables are*

$$\int_{S_{\mathbb{C}}^{N-1}} |z_i|^{2k} \, dz = \frac{(N-1)!k!}{(N+k-1)!}$$

and the variables $y_i = \sqrt{N} x_i$ become complex normal and independent with $N \to \infty$.

PROOF. This is nearly identical to the proof of Theorem 14.31, by using Theorem 14.32 as input. Thus, we are led to the conclusion in the statement. □

14e. Exercises

Good and slow learning this was, but as a drawback, many must-do exercises:

EXERCISE 14.34. *Try computing the Gauss integral, by other means.*

EXERCISE 14.35. *Can Stieltjes inversion help, in relation with our questions?*

EXERCISE 14.36. *What about complex numbers and Rayleigh variables?*

EXERCISE 14.37. *Do not forget as well to learn a bit about the heat kernel.*

EXERCISE 14.38. *Do the computations for the complex spherical integrals.*

EXERCISE 14.39. *Compute the hyperspherical laws at small $N \in \mathbb{N}$. Worth it.*

EXERCISE 14.40. *Compute the continuous limits of the various discrete laws.*

EXERCISE 14.41. *Why was the kurtosis always of the form $\kappa = 3 + \kappa'$?*

As bonus exercise, difficult, further meditate on what rat said, about all this.

CHAPTER 15

Combinatorics

15a. Cumulants

We have seen a lot of interesting combinatorics in the previous chapters, but this is not the end of the story. Following Rota, let us formulate the following definition:

DEFINITION 15.1. *Associated to any real probability measure $\mu = \mu_f$ is the following modification of the logarithm of the Fourier transform $F_\mu(\xi) = E(e^{i\xi f})$,*

$$K_\mu(\xi) = \log E(e^{\xi f})$$

called cumulant-generating function. The Taylor coefficients $k_n(\mu)$ of this series, given by

$$K_\mu(\xi) = \sum_{n=1}^{\infty} k_n(\mu)\,\frac{\xi^n}{n!}$$

are called cumulants of the measure μ. We also use the notations k_f, K_f for these cumulants and their generating series, where f is a variable following the law μ.

In other words, the cumulants are more or less the coefficients of the logarithm of the Fourier transform $\log F_\mu$, up to some normalizations. To be more precise, we have $K_\mu(\xi) = \log F_\mu(-i\xi)$, so the formula relating $\log F_\mu$ to the cumulants $k_n(\mu)$ is:

$$\log F_\mu(-i\xi) = \sum_{n=1}^{\infty} k_n(\mu)\,\frac{\xi^n}{n!}$$

Equivalently, the formula relating $\log F_\mu$ to the cumulants $k_n(\mu)$ is:

$$\log F_\mu(\xi) = \sum_{n=1}^{\infty} k_n(\mu)\,\frac{(i\xi)^n}{n!}$$

We will see in a moment the reasons for the above normalizations, namely change of variables $\xi \to -i\xi$, and Taylor coefficients instead of plain coefficients, the idea being that for simple laws like p_t, g_t, we will obtain in this way very simple quantities. Let us also mention that there is a reason for indexing the cumulants by $n = 1, 2, 3, \ldots$ instead of $n = 0, 1, 2, \ldots$, and more on this later, once we will have some theory and examples.

As a first observation, the sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, the numerics being as follows:

PROPOSITION 15.2. *The sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, and uniquely determines μ. We have*

$$k_1 = M_1$$

$$k_2 = -M_1^2 + M_2$$

$$k_3 = 2M_1^3 - 3M_1M_2 + M_3$$

$$k_4 = -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4$$

$$\vdots$$

in one sense, and in the other sense we have

$$M_1 = k_1$$

$$M_2 = k_1^2 + k_2$$

$$M_3 = k_1^3 + 3k_1k_2 + k_3$$

$$M_4 = k_1^4 + 6k_1^2k_2 + 3k_2^2 + 4k_1k_3 + k_4$$

$$\vdots$$

with in both cases the correspondence being polynomial, with integer coefficients.

PROOF. We know from Definition 15.1 that the cumulants are given by:

$$\log E(e^{\xi f}) = \sum_{s=1}^{\infty} k_s(f)\,\frac{\xi^s}{s!}$$

By exponentiating, we obtain from this the following formula:

$$E(e^{\xi f}) = \exp\left(\sum_{s=1}^{\infty} k_s(f)\,\frac{\xi^s}{s!}\right)$$

Now by looking at the terms of order $1, 2, 3, 4$, this gives the above formulae. □

The interest in the cumulants comes from the fact that $\log F_\mu$, and so the cumulants $k_n(\mu)$ too, linearize the convolution. To be more precise, we have the following result:

THEOREM 15.3. *The cumulants have the following properties:*

(1) $k_n(cf) = c^n k_n(f)$.
(2) $k_1(f + d) = k_1(f) + d$, *and* $k_n(f + d) = k_n(f)$ *for* $n > 1$.
(3) $k_n(f + g) = k_n(f) + k_n(g)$, *if* f, g *are independent.*

PROOF. Here (1) and (2) are both clear from definitions, because we have:

$$\begin{aligned} K_{cf+d}(\xi) &= \log E(e^{\xi(cf+d)}) \\ &= \log[e^{\xi d} \cdot E(e^{\xi cf})] \\ &= \xi d + K_f(c\xi) \end{aligned}$$

As for (3), this follows from the fact that the Fourier transform $F_f(\xi) = E(e^{i\xi f})$ satisfies the following formula, whenever f, g are independent random variables:

$$F_{f+g}(\xi) = F_f(\xi)F_g(\xi)$$

Indeed, by applying the logarithm, we obtain the following formula:

$$\log F_{f+g}(\xi) = \log F_f(\xi) + \log F_g(\xi)$$

With the change of variables $\xi \to -i\xi$, we obtain the following formula:

$$K_{f+g}(\xi) = K_f(\xi) + K_g(\xi)$$

Thus, at the level of coefficients, we obtain $k_n(f+g) = k_n(f) + k_n(g)$, as claimed. □

Summarizing, the cumulants are useful combinatorial tools, related to the moments, which appear to be complementary to the Fourier transform.

At the level of examples now, let us compute the cumulants for a number of basic measures that we know. We first have here the following result:

PROPOSITION 15.4. *The sequence of cumulants $k_1, k_2, k_3, \ldots$ is as follows:*

(1) *For $\mu = \delta_c$ the cumulants are $c, 0, 0, \ldots$*
(2) *For $\mu = g_t$ the cumulants are $0, t, 0, 0, \ldots$*
(3) *For $\mu = p_t$ the cumulants are $t, t, t, \ldots$*
(4) *For $\mu = b_t^2$ the cumulants are $0, t, 0, t, \ldots$*

PROOF. We have 4 computations to be done, the idea being as follows:

(1) For a Dirac mass, $\mu = \delta_c$, we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log E(e^{c\xi}) \\ &= \log(e^{c\xi}) \\ &= c\xi \end{aligned}$$

But the plain coefficients of this series are the numbers $c, 0, 0, \ldots$, and so the Taylor coefficients of this series are these same numbers $c, 0, 0, \ldots$, as claimed.

(2) For a normal law, $\mu = g_t$, we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log F_\mu(-i\xi) \\ &= \log \exp\left[-t(-i\xi)^2/2\right] \\ &= t\xi^2/2 \end{aligned}$$

But the plain coefficients of this series are the numbers $0, t/2, 0, 0, \ldots$, and so the Taylor coefficients of this series are the numbers $0, t, 0, 0, \ldots$, as claimed.

(3) For a Poisson law, $\mu = p_t$, we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log F_\mu(-i\xi) \\ &= \log \exp\left[(e^{i(-i\xi)} - 1)t\right] \\ &= (e^\xi - 1)t \end{aligned}$$

But the plain coefficients of this series are the numbers $t/n!$, and so the Taylor coefficients of this series are the numbers $t, t, t, \ldots$, as claimed.

(4) For a Bessel law, $\mu = b_t^2$, we have the following computation:

$$\begin{aligned} K_\mu(\xi) &= \log F_\mu(-i\xi) \\ &= \log \exp\left[\left(\frac{e^\xi + e^{-\xi}}{2} - 1\right) t\right] \\ &= \left(\frac{e^\xi + e^{-\xi}}{2} - 1\right) t \end{aligned}$$

But the plain coefficients of this series are the numbers $(1 + (-1)^n)t/n!$, so the Taylor coefficients of this series are the numbers $0, t, 0, t, \ldots$, as claimed. □

At a more theoretical level, we have the following result, generalizing (3,4) above, and which is something very useful, when dealing with the compound Poisson laws:

THEOREM 15.5. *For a compound Poisson law p_ν we have*

$$k_n(p_\nu) = M_n(\nu)$$

valid for any integer $n \geq 1$.

PROOF. We can assume, by using a continuity argument, that our measure ν is discrete, as follows, with $t_i > 0$ and $z_i \in \mathbb{R}$, and with the sum being finite:

$$\nu = \sum_i t_i \delta_{z_i}$$

By using now the Fourier transform formula for p_ν, we obtain:

$$\begin{aligned}
K_{p_\nu}(\xi) &= \log F_{p_\nu}(-i\xi)\\
&= \log\exp\left[\sum_i t_i(e^{\xi z_i}-1)\right]\\
&= \sum_i t_i\sum_{n\geq 1}\frac{(\xi z_i)^n}{n!}\\
&= \sum_{n\geq 1}\frac{\xi^n}{n!}\sum_i t_i z_i^n\\
&= \sum_{n\geq 1}\frac{\xi^n}{n!}\,M_n(\nu)
\end{aligned}$$

Thus, we are led to the conclusion in the statement. □

15b. Inversion formula

Getting back to theory now, the sequence of cumulants $k_1, k_2, k_3, \ldots$ appears as a modification of the sequence of moments $M_1, M_2, M_3, \ldots$, and understanding the relation between moments and cumulants will be our next task. We recall from Proposition 15.2 that we have the following formulae, for the cumulants in terms of moments:

$$k_1 = M_1$$

$$k_2 = -M_1^2 + M_2$$

$$k_3 = 2M_1^3 - 3M_1M_2 + M_3$$

$$k_4 = -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4$$

$$\vdots$$

Also, we have the following formulae, for the moments in terms of cumulants:

$$M_1 = k_1$$

$$M_2 = k_1^2 + k_2$$

$$M_3 = k_1^3 + 3k_1k_2 + k_3$$

$$M_4 = k_1^4 + 6k_1^2k_2 + 3k_2^2 + 4k_1k_3 + k_4$$

$$\vdots$$

In order to understand what exactly is going on, with moments and cumulants, which reminds a bit the Möbius inversion formula, we need to do some combinatorics, in relation with the partitions. Let us start with the following key definition:

DEFINITION 15.6. *The Möbius function of any lattice, and so of P, is given by*

$$\mu(\pi,\nu)=\begin{cases}1 & \text{if } \pi=\nu\\ -\sum_{\pi\leq\tau<\nu}\mu(\pi,\tau) & \text{if } \pi<\nu\\ 0 & \text{if } \pi\not\leq\nu\end{cases}$$

with the construction being performed by recurrence.

As an illustration here, for $P(2)=\{||,\sqcap\}$, we have by definition:

$$\mu(||,||)=\mu(\sqcap,\sqcap)=1$$

Also, $||<\sqcap$, with no intermediate partition in between, so we obtain:

$$\mu(||,\sqcap)=-\mu(||,||)=-1$$

Finally, we have $\sqcap\not\leq||$, and so we have as well the following formula:

$$\mu(\sqcap,||)=0$$

Thus, the Möbius matrix $M_{\pi\nu}=\mu(\pi,\nu)$ of the lattice $P(2)=\{||,\sqcap\}$ is as follows:

$$M=\begin{pmatrix}1&-1\\0&1\end{pmatrix}$$

At $k=3$ now, we have the following formula for the Möbius matrix $M_{\pi\nu}=\mu(\pi,\nu)$, once again written with the indices picked increasing in $P(3)=\{|||,\sqcap|,|\sqcap,|\sqcap|,\sqcap\sqcap\}$:

$$M=\begin{pmatrix}1&-1&-1&-1&2\\0&1&0&0&-1\\0&0&1&0&-1\\0&0&0&1&-1\\0&0&0&0&1\end{pmatrix}$$

In general, the Möbius matrix of $P(k)$ looks a bit like the above matrices at $k=2,3$, being upper triangular, with 1 on the diagonal, and so on. We will be back to this.

Back to the general case now, the main interest in the Möbius function comes from the Möbius inversion formula, which can be formulated as follows:

THEOREM 15.7. *We have the following implication,*

$$f(\pi)=\sum_{\nu\leq\pi}g(\nu)\quad\implies\quad g(\pi)=\sum_{\nu\leq\pi}\mu(\nu,\pi)f(\nu)$$

valid for any two functions $f,g:P(n)\to\mathbb{C}$.

PROOF. Consider the adjacency matrix of P, given by the following formula:

$$A_{\pi\nu}=\begin{cases}1 & \text{if } \pi\leq\nu\\ 0 & \text{if } \pi\not\leq\nu\end{cases}$$

Our claim is that the inverse of this matrix is the Möbius matrix of P, given by:

$$M_{\pi\nu}=\mu(\pi,\nu)$$

Indeed, the above matrix A is upper triangular, and when trying to invert it, we are led to the recurrence in Definition 15.6, so to the Möbius matrix M. Thus we have:

$$M=A^{-1}$$

Thus, in practice, we are led to the inversion formula in the statement. □

As a first illustration, for $P(2)$ the formula $M=A^{-1}$ appears as follows:

$$\begin{pmatrix}1&-1\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}^{-1}$$

At $k=3$ now, the formula $M=A^{-1}$ for $P(3)$ takes the following form:

$$\begin{pmatrix}1&-1&-1&-1&2\\0&1&0&0&-1\\0&0&1&0&-1\\0&0&0&1&-1\\0&0&0&0&1\end{pmatrix}=\begin{pmatrix}1&1&1&1&1\\0&1&0&0&1\\0&0&1&0&1\\0&0&0&1&1\\0&0&0&0&1\end{pmatrix}^{-1}$$

In general, the formula $M=A^{-1}$ looks quite similar. We will be back to this.

With these ingredients in hand, let us go back to probability. We first have:

DEFINITION 15.8. *We define quantities $M_\pi(f),k_\pi(f)$, depending on partitions*

$$\pi\in P(k)$$

by starting with $M_n(f),k_n(f)$, and using multiplicativity over the blocks.

To be more precise, the convention here is that for the one-block partition $1_n\in P(n)$, the corresponding moment and cumulant are the usual ones, namely:

$$M_{1_n}(f)=M_n(f)\quad,\quad k_{1_n}(f)=k_n(f)$$

Then, for an arbitrary partition $\pi\in P(k)$, we decompose this partition into blocks, having sizes $b_1,\ldots,b_s$, and we set, by multiplicativity over blocks:

$$M_\pi(f)=M_{b_1}(f)\ldots M_{b_s}(f)\quad,\quad k_\pi(f)=k_{b_1}(f)\ldots k_{b_s}(f)$$

With this convention, following Rota and others, we can now formulate a key result, fully clarifying the relation between moments and cumulants, as follows:

THEOREM 15.9. *We have the moment-cumulant formulae*

$$M_n(f)=\sum_{\nu\in P(n)}k_\nu(f)\quad,\quad k_n(f)=\sum_{\nu\in P(n)}\mu(\nu,1_n)M_\nu(f)$$

or, equivalently, we have the moment-cumulant formulae

$$M_\pi(f)=\sum_{\nu\leq\pi}k_\nu(f)\quad,\quad k_\pi(f)=\sum_{\nu\leq\pi}\mu(\nu,\pi)M_\nu(f)$$

where μ is the Möbius function of $P(n)$.

PROOF. There are several things going on here, the idea being as follows:

(1) According to our conventions above, the first set of formulae is equivalent to the second set of formulae. Also, due to the Möbius inversion formula, in the second set of formulae, the two formulae there are in fact equivalent. Thus, the 4 formulae in the statement are all equivalent. In what follows we will focus on the first 2 formulae.

(2) Let us first work out some examples. At $n=1,2,3$ the moment formula gives the following equalities, which are in tune with the findings from Proposition 15.2:

$$M_1=k_{|}=k_1$$

$$M_2=k_{||}+k_{\sqcap}=k_1^2+k_2$$

$$M_3=k_{|||}+k_{\sqcap|}+k_{\sqcap\!\!\sqcap}+k_{|\sqcap}+k_{\sqcap\sqcap}=k_1^3+3k_1k_2+k_3$$

At $n=4$ now, which is a case which is of particular interest for certain considerations to follow, the computation is as follows, again in tune with Proposition 15.2:

$$\begin{aligned}M_4&=k_{|||}+(\underbrace{k_{\sqcap||}+\ldots}_{6\ terms})+(\underbrace{k_{\sqcap\sqcap}+\ldots}_{3\ terms})+(\underbrace{k_{\sqcap\sqcap|}+\ldots}_{4\ terms})+k_{\sqcap\sqcap\sqcap}\\&=k_1^4+6k_1^2k_2+3k_2^2+4k_1k_3+k_4\end{aligned}$$

As for the cumulant formula, at $n=1,2,3$ this gives the following formulae for the cumulants, again in tune with the findings from Proposition 15.2:

$$k_1=M_{|}=M_1$$

$$k_2=(-1)M_{||}+M_{\sqcap}=-M_1^2+M_2$$

$$k_3=2M_{|||}+(-1)M_{\sqcap|}+(-1)M_{\sqcap\!\!\sqcap}+(-1)M_{|\sqcap}+M_{\sqcap\sqcap}=2M_1^3-3M_1M_2+M_3$$

Finally, at $n=4$, after computing the Möbius function of $P(4)$, we obtain the following formula for the fourth cumulant, again in tune with Proposition 15.2:

$$\begin{aligned}k_4&=(-6)M_{|||}+2(\underbrace{M_{\sqcap||}+\ldots}_{6\ terms})+(-1)(\underbrace{M_{\sqcap\sqcap}+\ldots}_{3\ terms})+(-1)(\underbrace{M_{\sqcap\sqcap|}+\ldots}_{4\ terms})+M_{\sqcap\sqcap\sqcap}\\&=-6M_1^4+12M_1^2M_2-3M_2^2-4M_1M_3+M_4\end{aligned}$$

(3) Time now to get to work, and prove the result. As mentioned above, the formulae in the statement are all equivalent, and it is enough to prove the first one, namely:

$$M_n(f) = \sum_{\nu \in P(n)} k_\nu(f)$$

In order to do this, we use the very definition of the cumulants, namely:

$$\log E(e^{\xi f}) = \sum_{s=1}^{\infty} k_s(f) \frac{\xi^s}{s!}$$

By exponentiating, we obtain from this the following formula:

$$E(e^{\xi f}) = \exp\left(\sum_{s=1}^{\infty} k_s(f) \frac{\xi^s}{s!} \right)$$

(4) Let us first compute the function on the left. This is easily done, as follows:

$$E(e^{\xi f}) = E\left(\sum_{n=0}^{\infty} \frac{(\xi f)^n}{n!} \right) = \sum_{n=0}^{\infty} M_n(f) \frac{\xi^n}{n!}$$

(5) Regarding now the function on the right, this is given by:

$$\begin{aligned} \exp\left(\sum_{s=1}^{\infty} k_s(f) \frac{\xi^s}{s!} \right) &= \sum_{p=0}^{\infty} \frac{\left(\sum_{s=1}^{\infty} k_s(f) \frac{\xi^s}{s!} \right)^p}{p!} \\ &= \sum_{p=0}^{\infty} \frac{1}{p!} \sum_{s_1=1}^{\infty} k_{s_1}(f) \frac{\xi^{s_1}}{s_1!} \ldots\ldots \sum_{s_p=1}^{\infty} k_{s_p}(f) \frac{\xi^{s_p}}{s_p!} \\ &= \sum_{p=0}^{\infty} \frac{1}{p!} \sum_{s_1=1}^{\infty} \ldots \sum_{s_p=1}^{\infty} k_{s_1}(f) \ldots k_{s_p}(f) \frac{\xi^{s_1+\ldots+s_p}}{s_1! \ldots s_p!} \end{aligned}$$

But the point now is that all this leads us into partitions. Indeed, we are summing over indices $s_1, \ldots, s_p \in \mathbb{N}$, which can be thought of as corresponding to a partition of $n = s_1 + \ldots + s_p$. So, let us rewrite our sum, as a sum over partitions. For this purpose, recall that the number of partitions $\nu \in P(n)$ having blocks of sizes $s_1, \ldots, s_p$ is:

$$\binom{n}{s_1, \ldots, s_p} = \frac{n!}{p_1! \ldots p_s!}$$

Also, when resumming over partitions, there will be a $p!$ factor as well, coming from the permutations of $s_1, \ldots, s_p$. Thus, our sum can be rewritten as follows:

$$\begin{aligned}
\exp\left(\sum_{s=1}^{\infty} k_s(f)\,\frac{\xi^s}{s!}\right) &= \sum_{n=0}^{\infty}\sum_{p=0}^{\infty}\frac{1}{p!}\sum_{s_1+\ldots+s_p=n} k_{s_1}(f)\ldots k_{s_p}(f)\,\frac{\xi^n}{s_1!\ldots s_p!}\\
&= \sum_{n=0}^{\infty}\frac{\xi^n}{n!}\sum_{p=0}^{\infty}\frac{1}{p!}\sum_{s_1+\ldots+s_p=n}\binom{n}{s_1,\ldots,s_p}k_{s_1}(f)\ldots k_{s_p}(f)\\
&= \sum_{n=0}^{\infty}\frac{\xi^n}{n!}\sum_{\nu\in P(n)} k_\nu(f)
\end{aligned}$$

(6) We are now in position to conclude. According to (3,4,5), we have:

$$\sum_{n=0}^{\infty} M_n(f)\,\frac{\xi^n}{n!} = \sum_{n=0}^{\infty}\frac{\xi^n}{n!}\sum_{\nu\in P(n)} k_\nu(f)$$

Thus, we have the following formula, valid for any $n \in \mathbb{N}$:

$$M_n(f) = \sum_{\nu\in P(n)} k_\nu(f)$$

We are therefore led to the conclusions in the statement. □

The above cumulant technology is quite powerful, and can be applied as well to more specialized measures that we know, such as the scary ones from chapters 11-12, in order to get more conceptual proofs for the various moments results found there. We will leave this as a long, instructive exercise, for your long Summer nights.

15c. Groups, easiness

As a next job for us, time to connect the above cumulant theory, which is advanced combinatorics, with the group theory from chapter 10, which was advanced combinatorics too. In order to discuss this, let us start with the following definition:

Definition 15.10. *Given a partition $\pi \in P(k,l)$, between an upper row of k points, and a lower row of l points, and an integer $N \in \mathbb{N}$, we define a linear map*

$$T_\pi : (\mathbb{C}^N)^{\otimes k} \to (\mathbb{C}^N)^{\otimes l}$$

by the following formula, with $e_1, \ldots, e_N$ being the standard basis of $\mathbb{C}^N$,

$$T_\pi(e_{i_1}\otimes\ldots\otimes e_{i_k}) = \sum_{j_1\ldots j_l}\delta_\pi\begin{pmatrix} i_1 & \ldots & i_k\\ j_1 & \ldots & j_l\end{pmatrix} e_{j_1}\otimes\ldots\otimes e_{j_l}$$

and with the coefficients on the right being Kronecker type symbols.

To be more precise here, in order to compute $\delta_\pi\binom{i}{j} \in \{0,1\}$, we put the multi-indices $i = (i_1, \ldots, i_k)$ and $j = (j_1, \ldots, j_l)$ on the legs of π, in the obvious way. If all blocks of π contain equal indices of i, j, we set $\delta_\pi\binom{i}{j} = 1$. Otherwise, we set $\delta_\pi\binom{i}{j} = 0$.

With the above notion in hand, we can formulate the following key definition:

DEFINITION 15.11. *A closed subgroup $G \subset U_N$ is called easy when*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any two colored integers k, l, for certain sets of partitions $D(k,l) \subset P(k,l)$.

As a basic example here, according to our results from chapter 10, the symmetric group $S_N \subset O_N$ is easy, coming from the full collection of sets of partitions, namely:

$$P = \bigsqcup_{k,l} P(k,l)$$

Along the same lines, the hyperoctahedral group $H_N \subset O_N$ and the full complex reflection group $K_N \subset U_N$ are easy too, coming respectively from the following collections of sets of partitions, with these being those that we found in chapter 10:

$$P_{even} = \bigsqcup_{k,l} P_{even}(k,l) \quad , \quad \mathcal{P}_{even} = \bigsqcup_{k,l} \mathcal{P}_{even}(k,l)$$

As further basic examples, which are perhaps even more fundamental, thanks to some old results of Brauer, the orthogonal and unitary groups O_N, U_N are known to be easy too, coming respectively from the following collections of sets of pairings:

$$P_2 = \bigsqcup_{k,l} P_2(k,l) \quad , \quad \mathcal{P}_2 = \bigsqcup_{k,l} \mathcal{P}_2(k,l)$$

Summarizing, easiness is something very concrete, and useful. In order to better understand what easiness means, inspired by the above examples, let us formulate:

DEFINITION 15.12. *Let $P(k,l)$ be the set of partitions between an upper colored integer k, and a lower colored integer l. A collection of subsets*

$$D = \bigsqcup_{k,l} D(k,l)$$

with $D(k,l) \subset P(k,l)$ is called a category of partitions when it has the following properties:

(1) *Stability under the horizontal concatenation, $(\pi, \sigma) \to [\pi\sigma]$.*
(2) *Stability under vertical concatenation $(\pi, \sigma) \to \left[\begin{smallmatrix}\sigma\\ \pi\end{smallmatrix}\right]$, with matching middle symbols.*
(3) *Stability under the upside-down turning $*$, with switching of colors, $\circ \leftrightarrow \bullet$.*
(4) *Each set $P(k,k)$ contains the identity partition $||\ldots||$.*
(5) *The sets $P(\emptyset, \circ\bullet)$ and $P(\emptyset, \bullet\circ)$ both contain the semicircle $\cap$.*
(6) *The sets $P(k, \bar{k})$ with $|k| = 2$ contain the crossing partition $\times$.*

As basic examples, we have the various sets of partitions discussed above, which are all categories of partitions, in the above abstract sense. There are many other examples, and more on this later, when discussing classification results, for such beasts.

At the abstract level, the interest in Definition 15.12 comes from the following fact:

PROPOSITION 15.13. *The assignement $\pi \to T_\pi$ is categorical, in the sense that*

$$T_\pi \otimes T_\sigma = T_{[\pi\sigma]} \quad , \quad T_\pi T_\sigma = N^{c(\pi,\sigma)} T_{[\frac{\sigma}{\pi}]} \quad , \quad T_\pi^* = T_{\pi^*}$$

where $c(\pi, \sigma)$ are certain integers, coming from the erased components in the middle.

PROOF. The verification of the first axiom is something elementary, as follows, with $c(\pi, \sigma) \in \mathbb{N}$ counting the middle components, when concatenating:

$$\begin{aligned}
& T_\pi T_\sigma(e_{i_1} \otimes \ldots \otimes e_{i_p}) \\
= \ & \sum_{j_1 \ldots j_q} \delta_\sigma \begin{pmatrix} i_1 & \ldots & i_p \\ j_1 & \ldots & j_q \end{pmatrix} \sum_{k_1 \ldots k_r} \delta_\pi \begin{pmatrix} j_1 & \ldots & j_q \\ k_1 & \ldots & k_r \end{pmatrix} e_{k_1} \otimes \ldots \otimes e_{k_r} \\
= \ & \sum_{k_1 \ldots k_r} N^{c(\pi,\sigma)} \delta_{[\frac{\sigma}{\pi}]} \begin{pmatrix} i_1 & \ldots & i_p \\ k_1 & \ldots & k_r \end{pmatrix} e_{k_1} \otimes \ldots \otimes e_{k_r} \\
= \ & N^{c(\pi,\sigma)} T_{[\frac{\sigma}{\pi}]}(e_{i_1} \otimes \ldots \otimes e_{i_p})
\end{aligned}$$

As for the verification of the two other axioms, this is similar. □

Time now to put everyting together. In relation with the groups, we have:

THEOREM 15.14. *Each category of partitions $D = (D(k, l))$ produces a family of easy groups $G = (G_N)$, one for each $N \in \mathbb{N}$, via the formula*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k, l)\right)$$

and the Tannakian duality correspondence.

PROOF. Given an integer $N \in \mathbb{N}$, consider the correspondence $\pi \to T_\pi$ constructed in Definition 15.10, and then the collection of linear spaces in the statement, namely:

$$C_{kl} = span\left(T_\pi \middle| \pi \in D(k, l)\right)$$

According to the formulae in Proposition 15.13, and to our axioms for the categories of partitions, from Definition 15.12, this collection of spaces $C = (C_{kl})$ satisfies the axioms for the Tannakian categories, from abstract group theory. Thus the Tannakian duality result applies, and provides us with a closed subgroup $G_N \subset U_N$ such that:

$$C_{kl} = Hom(u^{\otimes k}, u^{\otimes l})$$

Thus, we are led to the conclusion in the statement, modulo some learning of Tannakian duality, which is something non-trivial, that we will leave as an exercise. □

In relation with the easiness property, we can now formulate a key result, which can serve as an alternative definition for the easy groups, as follows:

THEOREM 15.15. *A closed subgroup $G \subset U_N$ is easy precisely when*

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

for any colored integers k, l, for a certain category of partitions $D \subset P$.

PROOF. This basically follows from Theorem 15.14, as follows:

(1) In one sense, we know from Theorem 15.14 that any category of partitions $D \subset P$ produces a family of closed groups $G \subset U_N$, one for each $N \in \mathbb{N}$, according to:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in D(k,l)\right)$$

But these groups $G \subset U_N$ are indeed easy, in the sense of Definition 15.11.

(2) In the other sense now, assume that $G \subset U_N$ is easy, in the sense of Definition 15.11, coming via the above Hom space formula, from a collection of sets as follows:

$$D = \bigsqcup_{k,l} D(k,l)$$

Consider now the category of partitions $\widetilde{D} =< D >$ generated by this family. This is by definition the smallest category of partitions containing D, whose existence follows by starting with D, and performing the various categorical operations, namely horizontal and vertical concatenation, and upside-down turning. It follows then, via another application of Tannakian duality, that we have the following formula, for any k, l:

$$Hom(u^{\otimes k}, u^{\otimes l}) = span\left(T_\pi \middle| \pi \in \widetilde{D}(k,l)\right)$$

Thus, our group $G \subset U_N$ can be viewed as well as coming from $\widetilde{D}$, and so appearing as particular case of the construction in Theorem 15.14, and this gives the result. □

Getting now to the examples, in order to cut from complexity, we will need:

PROPOSITION 15.16. *For an easy group $G = (G_N)$, coming from a category of partitions $D \subset P$, the following conditions are equivalent:*

(1) *$G_{N-1} = G_N \cap U_{N-1}$, via the embedding $U_{N-1} \subset U_N$ given by $u \to diag(u, 1)$.*
(2) *$G_{N-1} = G_N \cap U_{N-1}$, via the N possible diagonal embeddings $U_{N-1} \subset U_N$.*
(3) *D is stable under the operation which consists in removing blocks.*

If these conditions are satisfied, we say that $G = (G_N)$ is uniform.

PROOF. We use the general easiness theory explained above, as follows:

(1) $\iff$ (2) This is something standard, coming from the inclusion $S_N \subset G_N$, which makes everything S_N-invariant. The result follows as well from the proof of (1) $\iff$ (3) below, which can be converted into a proof of (2) $\iff$ (3), in the obvious way.

(1) $\iff$ (3) Given a subgroup $K \subset U_{N-1}$, with fundamental representation u, consider the $N \times N$ matrix $v = diag(u, 1)$. Then, for any $\pi \in P(k)$ we have:

$$\xi_\pi \in Fix(v^{\otimes k}) \iff \xi_{\pi'} \in Fix(v^{\otimes k'}),\ \forall \pi' \in P(k'), \pi' \subset \pi$$

But with this observation in hand, the result follows from Tannakian duality. □

We can now formulate a nice classification result, as follows:

THEOREM 15.17. *The uniform orthogonal easy groups $G \subset O_N$, and their associated categories of partitions $D \subset P$, all coming from subsets $L \subset \mathbb{N}$, are as follows,*

$$\begin{array}{ccc} B_N & \longrightarrow & O_N \\ \uparrow & & \uparrow \\ S_N & \longrightarrow & H_N \end{array} \quad : \quad \begin{array}{ccc} P_{12} & \longleftarrow & P_2 \\ \downarrow & & \downarrow \\ P & \longleftarrow & P_{even} \end{array} \quad : \quad \begin{array}{ccc} \{1,2\} & \longleftarrow & \{2\} \\ \downarrow & & \downarrow \\ \mathbb{N} & \longleftarrow & 2\mathbb{N} \end{array}$$

with D consisting of the partitions $\pi \in P$ whose blocks have lengths belonging to $L \subset \mathbb{N}$.

PROOF. The various groups in the statement, with $B_N \subset O_N$ being the bistochastic group, consisting of matrices having sum 1 on each row and column, are indeed easy and uniform, the corresponding categories of partitions being those in the statement, with $P_{12} \subset P$ standing for the category of partitions consisting of singletons and pairings. Regarding now the classification, consider an arbitrary easy group, as follows:

$$S_N \subset G_N \subset O_N$$

This group must then come from a category of partitions, as follows:

$$P_2 \subset D \subset P$$

Now if we assume $G = (G_N)$ to be uniform, as in Proposition 15.16, this category of partitions D is uniquely determined by the subset $L \subset \mathbb{N}$ consisting of the sizes of the blocks of the partitions in D. Our claim is that the admissible sets are as follows:

(1) $L = \{2\}$, producing O_N.

(2) $L = \{1, 2\}$, producing B_N.

(3) $L = \{2, 4, 6, \ldots\}$, producing H_N.

(4) $L = \{1, 2, 3, \ldots\}$, producing S_N.

Indeed, assume that $L \subset \mathbb{N}$ is such that the set P_L consisting of partitions whose sizes of the blocks belong to L is a category of partitions. We know from the axioms of the categories of partitions that the semicircle $\cap$ must be in the category, so we have $2 \in L$. Our claim is that the following conditions must be satisfied as well:

$$k, l \in L,\ k > l \implies k - l \in L$$

$$k \in L,\ k \geq 2 \implies 2k - 2 \in L$$

But these conditions both follow from the axioms of the categories of partitions, and with these two formulae in hand, we can conclude in the following way:

Case 1. Assume $1 \in L$. By using the first formula with $l = 1$ we get:

$$k \in L \implies k - 1 \in L$$

This condition shows that we must have $L = \{1, 2, \ldots, m\}$, for a certain number $m \in \{1, 2, \ldots, \infty\}$. On the other hand, by using the second formula we get:

$$\begin{aligned} m \in L &\implies 2m - 2 \in L \\ &\implies 2m - 2 \leq m \\ &\implies m \in \{1, 2, \infty\} \end{aligned}$$

The case $m = 1$ being excluded by the condition $2 \in L$, we reach to one of the two sets producing the groups S_N, B_N.

Case 2. Assume $1 \notin L$. By using the first formula with $l = 2$ we get:

$$k \in L \implies k - 2 \in L$$

This condition shows that we must have $L = \{2, 4, \ldots, 2p\}$, for a certain number $p \in \{1, 2, \ldots, \infty\}$. On the other hand, by using the second formula we get:

$$\begin{aligned} 2p \in L &\implies 4p - 2 \in L \\ &\implies 4p - 2 \leq 2p \\ &\implies p \in \{1, \infty\} \end{aligned}$$

Thus L must be one of the two sets producing O_N, H_N, and we are done. □

Now back to probability, in relation with cumulants, we have the following result:

THEOREM 15.18. *The cumulants of the asymptotic truncated characters for the uniform orthogonal easy groups $G = (G_N)$ are given by the formula*

$$k_n(\chi_t) = t\delta_{n \in L}$$

with $L \subset \mathbb{N}$ being the associated subset, and at the level of asymptotic moments this gives

$$M_k(\chi_t) = \sum_{\pi \in D(k)} t^{|\pi|}$$

with $D \subset P$ being the associated category of partitions.

PROOF. This comes indeed from what we have in Theorem 15.17, by performing a case-by-case analysis, with the cases $G = O, S, H$ corresponding to the cumulant computations for g_t, p_t, b_t^2 from Proposition 15.4, and with the remaining case, that of the group $G = B$, being similar. We will leave some study and learning here as an exercise. □

As a conclusion to all this, we managed to merge the advanced group combinatorics from chapter 10 with the advanced combinatorics of Rota's cumulants. Nice.

15d. Free cumulants

As an interesting phenomenon, the cumulant technology does not apply well to the measures from chapter 13, namely Wigner, Marchenko-Pastur, arcsine and modified arcsine, and with the reasons for this being something quite subtle, the idea being that these latter measures are "free" in nature, and are therefore in need of "free cumulants".

In order to discuss this, following Voiculescu and Speicher, let us start with:

DEFINITION 15.19. *Let A be a C^*-algebra, coming with a trace $tr : A \to \mathbb{C}$.*

(1) *The elements $a \in A$ are called noncommutative random variables.*
(2) *The moments of such a variable are the numbers $M_k(a) = tr(a^k)$.*
(3) *The law of such a variable is the functional $\mu_a : P \to tr(P(a))$.*

Obviously, this is something a bit advanced, requiring for good understanding some knowledge of functional analysis, and our comments on this are as follows:

(1) In what regards the C^*-algebra A, this must be by definition a complex algebra with unit, coming with an involution $*$ and a norm $||.||$, such that A is complete with respect to the norm, and such that the key identity $||aa^*|| = ||a||^2$ is satisfied.

(2) As basic examples of C^*-algebras, we have the algebras of type $A = C(X)$, with X being a compact space. Such algebras are commutative, $ab = ba$, and a theorem of Gelfand states precisely that any commutative C^*-algebra must be of this form.

(3) However, we have noncommutative examples too, such as the matrix algebra $M_N(\mathbb{C})$, or any of its $*$-subalgebras $A \subset M_N(\mathbb{C})$. More generally, any closed $*$-algebra of operators $A \subset B(H)$ is a C^*-algebra, and in fact, any C^*-algebra appears in this way.

(4) In view of this, we can think of any C^*-algebra as being of the form $A = C(X)$, with X being a "quantum space". But with this in mind, a trace $tr : A \to \mathbb{C}$ corresponds to an expectation, so we start understanding what Definition 15.19 is about.

Generally speaking, the above definition is something quite abstract, but there is no other way of doing things, at least at this level of generality. However, in certain special cases, the formalism simplifies, and we recover more familiar objects, as follows:

PROPOSITION 15.20. *Assuming that $a \in A$ is normal, $aa^* = a^*a$, its law corresponds to a probability measure on its spectrum $\sigma(a) \subset \mathbb{C}$, according to the following formula:*

$$tr(P(a)) = \int_{\sigma(a)} P(x) d\mu(x)$$

When the trace is faithful we have $supp(\mu) = \sigma(a)$. Also, in the particular case where the variable is self-adjoint, $a = a^*$, this law is a real probability measure.

PROOF. Since the C^*-algebra $< a >$ generated by a is commutative, the Gelfand theorem applies to it, and gives an identification of C^*-algebras, as follows:

$$< a >= C(\sigma(a))$$

Now by using the Riesz theorem, the restriction of tr to this algebra must come from a probability measure μ as in the statement, and this gives all the assertions. □

Getting now where we wanted to get, following Voiculescu [89], let us formulate:

DEFINITION 15.21. *Two subalgebras $A, B \subset C$ are called independent when*

$$tr(a) = tr(b) = 0 \implies tr(ab) = 0$$

holds for any $a \in A$ and $b \in B$, and free when

$$tr(a_i) = tr(b_i) = 0 \implies tr(a_1 b_1 a_2 b_2 \ldots) = 0$$

holds for any $a_i \in A$ and $b_i \in B$.

In order to understand now what is going on, let us discuss some basic models for independence and freeness. We first have the following result, which clarifies things:

PROPOSITION 15.22. *Given two algebras (A, tr) and (B, tr), the following hold:*

(1) *A, B are independent inside their tensor product $A \otimes B$.*
(2) *A, B are free inside their free product $A * B$.*

PROOF. Both the assertions are clear from definitions, after some standard discussion regarding the tensor product and free product trace. See Voiculescu [89]. □

In relation with groups and algebra, we have the following result, with the group C^*-algebras involved being some natural completions of the usual group algebras:

PROPOSITION 15.23. *We have the following results, valid for group algebras:*

(1) *$C^*(\Gamma), C^*(\Lambda)$ are independent inside $C^*(\Gamma \times \Lambda)$.*
(2) *$C^*(\Gamma), C^*(\Lambda)$ are free inside $C^*(\Gamma * \Lambda)$.*

PROOF. This follows from the general results in Proposition 15.22, along with the following two isomorphisms, which are both standard:

$$C^*(\Gamma \times \Lambda) = C^*(\Lambda) \otimes C^*(\Gamma) \quad , \quad C^*(\Gamma * \Lambda) = C^*(\Lambda) * C^*(\Gamma)$$

Alternatively, we can prove this directly, by using the fact that each algebra is spanned by the corresponding group elements, and checking the result on group elements. □

In order to study independence and freeness, the main tools are as follows:

THEOREM 15.24. *The convolution is linearized by the log of the Fourier transform,*

$$F_f(x) = E(e^{ixf})$$

and the free convolution is linearized by the Voiculescu R-transform, which is given by

$$G_\mu(\xi) = \int_{\mathbb{R}} \frac{d\mu(t)}{\xi - t} \implies G_\mu\left(R_\mu(\xi) + \frac{1}{\xi}\right) = \xi$$

and so is the inverse of the Cauchy transform, up to a ξ^{-1} factor.

PROOF. The first assertion is something that we know well, since chapter 6. Regarding now the second assertion, we need a good model for free convolution, and the best is to use the semigroup algebra of the free semigroup on two generators:

$$A = C^*(\mathbb{N} * \mathbb{N})$$

Indeed, we have some freeness in the semigroup setting, a bit in the same way as for the group algebras $C^*(\Gamma * \Lambda)$, from Proposition 15.23. In addition to this fact, and to what happens in the group algebra case, the following things happen:

(1) The variables of type $S^* + f(S)$, with $S \in C^*(\mathbb{N})$ being the shift, and with $f \in \mathbb{C}[X]$ being a polynomial, model in moments all the distributions $\mu : \mathbb{C}[X] \to \mathbb{C}$. This is indeed something elementary, which can be checked via a direct algebraic computation.

(2) Given $f, g \in \mathbb{C}[X]$, the variables $S^* + f(S)$ and $T^* + g(T)$, where $S, T \in C^*(\mathbb{N} * \mathbb{N})$ are the shifts corresponding to the generators of $\mathbb{N} * \mathbb{N}$, are free, and their sum has the same law as $S^* + (f + g)(S)$. This follows indeed by using a 45° argument.

(3) But with this in hand, we can see that $\mu \to f$ linearizes the free convolution. We are therefore left with a computation inside $C^*(\mathbb{N})$, whose conclusion is that $R_\mu = f$ can be recaptured from μ via the Cauchy transform G_μ, as stated. See [89]. □

As a main application of the above linearization technology, we have:

THEOREM 15.25 (CLT). *Given self-adjoint random variables $x_1, x_2, x_3, \ldots$ assumed to be i.i.d./f.i.d., centered, with variance $t > 0$, we have, with $n \to \infty$, in moments,*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} x_i \sim g_t/\gamma_t$$

where the limiting laws g_t/γ_t are the following measures,

$$g_t = \frac{1}{\sqrt{2\pi t}} e^{-x^2/2t} dx \quad , \quad \gamma_t = \frac{1}{2\pi t} \sqrt{4t^2 - x^2}\, dx$$

which are the normal, or Gaussian, and Wigner semicircle law of parameter t.

PROOF. This is indeed something routine, by using the linearization properties of the Fourier transform and the R-transform from Theorem 15.24, and for details here, we refer to chapter 14 for the classical result, and to Voiculescu [89] for the free result. □

Next, we have the following complex version of the CLT:

THEOREM 15.26 (CCLT). *Given variables $x_1, x_2, x_3, \ldots$ which are i.i.d./f.i.d., centered, with variance $t > 0$, we have, with $n \to \infty$, in moments,*

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} x_i \sim G_t/\Gamma_t$$

where G_t/Γ_t are the complex normal and Voiculescu circular law of parameter t, given by:

$$G_t = law\left(\frac{1}{\sqrt{2}}(a + ib)\right) \quad , \quad \Gamma_t = law\left(\frac{1}{\sqrt{2}}(\alpha + i\beta)\right)$$

where $a, b/\alpha, \beta$ are independent/free, each following the law g_t/γ_t.

PROOF. This follows indeed from the CLT, by taking real and imaginary parts of all the variables involved, and for details and more here, including the combinatorics of the Voiculescu circular law Γ_t, which is quite subtle, we refer again to [89]. □

We denote by $\boxplus$ the free convolution of real probability measures, given by the fact that $\mu_{a+b} = \mu_a \boxplus \mu_b$, when a, b are free. With this convention, we have the following discrete version of the CLT, called Poisson Limit Theorem (PLT):

THEOREM 15.27 (PLT). *The following Poisson limits converge, for any $t > 0$,*

$$p_t = \lim_{n\to\infty} \left(\left(1 - \frac{t}{n}\right)\delta_0 + \frac{t}{n}\delta_1\right)^{*n} \quad , \quad \pi_t = \lim_{n\to\infty} \left(\left(1 - \frac{t}{n}\right)\delta_0 + \frac{t}{n}\delta_1\right)^{\boxplus n}$$

the limiting measures being the Poisson law p_t, and the Marchenko-Pastur law π_t,

$$p_t = \frac{1}{e^t} \sum_{k=0}^{\infty} \frac{t^k \delta_k}{k!} \quad , \quad \pi_t = \max(1 - t, 0)\delta_0 + \frac{\sqrt{4t - (x - 1 - t)^2}}{2\pi x}\, dx$$

with at $t = 1$, the Marchenko-Pastur law being $\pi_1 = \frac{1}{2\pi}\sqrt{4x^{-1} - 1}\, dx$.

PROOF. This is again routine, by using the Fourier and R-transform, and as before we refer here to any classical probability book, and to [89]. □

Getting now to combinatorial aspects, following Speicher [75], let us formulate:

DEFINITION 15.28. *The free cumulants $\kappa_n(a)$ of a variable $a \in A$ are defined by*

$$R_a(\xi) = \sum_{n=1}^{\infty} \kappa_n(a)\xi^{n-1}$$

with R being as usual the Voiculescu R-transform.

As before with the classical cumulants, we have a number of basic examples and illustrations, and a number of basic general results. Let us start with some numerics:

PROPOSITION 15.29. *The free cumulants $\kappa_1, \kappa_2, \kappa_3, \ldots$ appear as a modification of the moments $M_1, M_2, M_3, \ldots$, and uniquely determine μ. We have*

$$\kappa_1 = M_1$$
$$\kappa_2 = -M_1^2 + M_2$$
$$\kappa_3 = 2M_1^3 - 3M_1M_2 + M_3$$
$$\kappa_4 = -5M_1^4 + 10M_1^2M_2 - 2M_2^2 - 4M_1M_3 + M_4$$
$$\vdots$$

in one sense, and in the other sense we have

$$M_1 = \kappa_1$$
$$M_2 = \kappa_1^2 + \kappa_2$$
$$M_3 = \kappa_1^3 + 3\kappa_1\kappa_2 + \kappa_3$$
$$M_4 = \kappa_1^4 + 6\kappa_1^2\kappa_2 + 2\kappa_2^2 + 4\kappa_1\kappa_3 + \kappa_4$$
$$\vdots$$

with in both cases the correspondence being polynomial, with integer coefficients.

PROOF. All this is very standard, and for details here, you can check [75]. □

Observe the similarity with the formulae for classical cumulants. In fact, we have:

CONCLUSION 15.30. *The first three classical and free cumulants coincide,*

$$k_1 = \kappa_1 \quad , \quad k_2 = \kappa_2 \quad , \quad k_3 = \kappa_3$$

but the formulae for the fourth classical and free cumulants are different,

$$k_4 = -6M_1^4 + 12M_1^2M_2 - 3M_2^2 - 4M_1M_3 + M_4$$
$$\kappa_4 = -5M_1^4 + 10M_1^2M_2 - 2M_2^2 - 4M_1M_3 + M_4$$

and the same happens at higher order as well.

This is something quite interesting, and we will back later with a conceptual explanation for this, via partitions, the idea being that all this comes from:

$$P(n) = NC(n) \iff n \leq 3$$

But more on this later. At the level of basic general results, we first have:

THEOREM 15.31. *The free cumulants have the following properties:*

(1) $\kappa_n(\lambda a) = \lambda^n \kappa_n(a)$.
(2) $\kappa_n(a + b) = \kappa_n(a) + \kappa_n(b)$, *if a, b are free.*

PROOF. This is something very standard, the idea being as follows:

(1) We have the following Cauchy transform computation:

$$\begin{aligned} G_{\lambda a}(\xi) &= \int_{\mathbb{R}} \frac{d\mu_{\lambda a}(t)}{\xi - t} \\ &= \int_{\mathbb{R}} \frac{d\mu_a(s)}{\xi - \lambda s} \\ &= \frac{1}{\lambda} \int_{\mathbb{R}} \frac{d\mu_a(s)}{\xi/\lambda - s} \\ &= \frac{1}{\lambda} G_a\left(\frac{\xi}{\lambda}\right) \end{aligned}$$

But this gives the following formula, by using the definition of the R-transform:

$$\begin{aligned} G_{\lambda a}\left(\lambda R_a(\lambda\xi) + \frac{1}{\xi}\right) &= \frac{1}{\lambda} G_a\left(R_a(\lambda\xi) + \frac{1}{\lambda\xi}\right) \\ &= \frac{1}{\lambda} \cdot \lambda\xi \\ &= \xi \end{aligned}$$

Thus we have the formula $R_{\lambda a}(\xi) = \lambda R_a(\lambda\xi)$, which gives (1).

(2) This follows from the standard fact, that we know well from before, that the R-transform linearizes the free convolution operation. □

Again in analogy with the classical case, at the level of examples, we have:

THEOREM 15.32. *The sequence of free cumulants $\kappa_1, \kappa_2, \kappa_3, \ldots$ is as follows:*

(1) *For $\mu = \delta_c$ the free cumulants are $c, 0, 0, \ldots$*
(2) *For $\mu = \gamma_t$ the free cumulants are $0, t, 0, 0, \ldots$*
(3) *For $\mu = \pi_t$ the free cumulants are $t, t, t, \ldots$*
(4) *For $\mu = \beta_t^2$ the free cumulants are $0, t, 0, t, \ldots$*

Also, for the compound free Poisson laws the free cumulants are $k_n(\pi_\nu) = M_n(\nu)$.

PROOF. The proofs are analogous to those from the classical case, as follows:

(1) For $\mu = \delta_c$ we have $G_\mu(\xi) = 1/(\xi - c)$, and so $R_\mu(\xi) = c$, as desired.

(2) For $\mu = \gamma_t$ we have, as computed before, $R_\mu(\xi) = t\xi$, as desired.

(3) For $\mu = \pi_t$ we have, also from before, $R_\mu(\xi) = t/(1 - \xi)$, as desired.

(4) For $\mu = \beta_t^2$, a free Bessel law, this can be established directly, but the best is to prove directly the last assertion, which generalizes (3,4). With $\nu = \sum_i c_i \delta_{z_i}$ we have:

$$\begin{aligned} R_{\pi_\nu}(\xi) &= \sum_i \frac{c_i z_i}{1 - \xi z_i} \\ &= \sum_{n \geq 1} \xi^{n-1} \sum_i c_i z_i^n \\ &= \sum_{n \geq 1} \xi^{n-1} M_n(\nu) \end{aligned}$$

Thus, we are led to the conclusion in the statement. □

As before in the classical case, we can define now generalized free cumulants, $\kappa_\pi(a)$ with $\pi \in P(k)$, by starting with the numeric free cumulants $\kappa_n(a)$, as follows:

DEFINITION 15.33. *We define free cumulants $\kappa_\pi(a)$, depending on partitions*

$$\pi \in P(k)$$

by starting with $\kappa_n(a)$, and using multiplicativity over the blocks.

To be more precise, the convention here is that for the one-block partition $1_n \in P(n)$, the corresponding free cumulant is the usual one, namely:

$$\kappa_{1_n}(a) = \kappa_n(a)$$

Then, for an arbitrary partition $\pi \in P(k)$, we decompose this partition into blocks, having sizes $b_1, \ldots, b_s$, and we set, by multiplicativity over blocks:

$$\kappa_\pi(a) = \kappa_{b_1}(a) \ldots \kappa_{b_s}(a)$$

With this convention, we have the following result, due to Speicher [75]:

THEOREM 15.34. *We have the moment-cumulant formulae*

$$M_n(a) = \sum_{\nu \in NC(n)} \kappa_\nu(a) \quad , \quad \kappa_n(a) = \sum_{\nu \in NC(n)} \mu(\nu, 1_n) M_\nu(a)$$

or, equivalently, we have the moment-cumulant formulae

$$M_\pi(a) = \sum_{\nu \leq \pi} \kappa_\nu(a) \quad , \quad \kappa_\pi(a) = \sum_{\nu \leq \pi} \mu(\nu, \pi) M_\nu(a)$$

where μ is the Möbius function of $NC(n)$.

PROOF. As before in the classical case, the 4 formulae in the statement are equivalent, via Möbius inversion. Thus, it is enough to prove one of them, and we will prove the first formula, which in practice is the most useful one. Thus, we must prove that:

$$M_n(a) = \sum_{\nu \in NC(n)} \kappa_\nu(a)$$

(1) In order to prove this formula, let us get back to the construction of the free cumulants, from Definition 15.28. The Cauchy transform of a is the following function:

$$G_a(\xi)=\sum_{n=0}^{\infty}\frac{M_n(a)}{\xi^{n+1}}$$

Consider the inverse of this Cauchy transform G_a, with respect to composition:

$$G_a(K_a(\xi))=K_a(G_a(\xi))=\xi$$

According to Definition 15.28, the free cumulants $\kappa_n(a)$ appear then as follows:

$$K_a(\xi)=\frac{1}{\xi}+\sum_{n=1}^{\infty}\kappa_n(a)\xi^{n-1}$$

Thus, we can compute moments in terms of free cumulants by using either of the inversion formulae $G_a(K_a(\xi))=\xi$ and $K_a(G_a(\xi))=\xi$.

(2) In practice, as seen in the proof of Proposition 15.29, the best is to use the second inversion formula, $K_a(G_a(\xi))=\xi$, which after some manipulations reads:

$$\begin{aligned}&\kappa_1z+\kappa_2z^2(1+M_1z+M_2z^2+\ldots)+\kappa_3z^3(1+M_1z+M_2z^2+\ldots)^2+\ldots\\ =\;&(M_1z+M_2z^2+\ldots)-(M_1z+M_2z^2+\ldots)^2+(M_1z+M_2z^2+\ldots)^3-\ldots\end{aligned}$$

But, in case you have fully understood the proof of Proposition 15.29, you know how to exploit this formula at order $n=1,2,3,4$. The same method works in general, and after some computations, this leads to the formula that we want to establish, namely:

$$M_n(a)=\sum_{\nu\in NC(n)}\kappa_\nu(a)$$

(3) We are therefore led to the conclusions in the statement. All this was of course quite brief, and for details here, we refer for instance to Nica-Speicher [75]. □

Observe that the above result leads among others to a more conceptual explanation for Conclusion 15.30, with the equalities and non-equalities there coming from:

$$P(n)=NC(n)\iff n\leq 3$$

As a main application now of the theories of Rota cumulants and Speicher free cumulants, following Bercovici and Pata, we can formulate the following simple and bright definition, making the connection between classical and free:

DEFINITION 15.35. *We say that a convolution semigroup of measures*

$$\{m_t\}_{t>0}\quad:\quad m_s*m_t=m_{s+t}$$

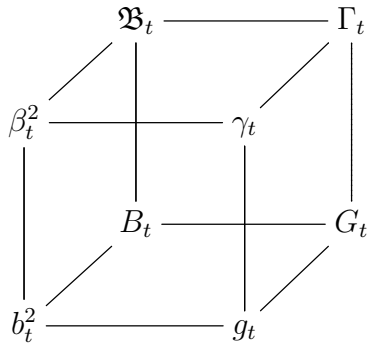
is in Bercovici-Pata bijection with a free convolution semigroup of measures

$$\{\mu_t\}_{t>0}\quad:\quad \mu_s\boxplus\mu_t=\mu_{s+t}$$

when the classical cumulants of m_t coincide with the free cumulants of μ_t.

And, this fits with what we did so far in this book, and notably with the theory of the measures coming from limiting theorems. Indeed, we have the following result:

THEOREM 15.36. *In the standard cube of basic semigroups of measures,*



the upper semigroups are in Bercovici-Pata bijection with the lower semigroups.

PROOF. This is indeed very standard, coming from the classical and free cumulant formulae that we have. For more on this, including group theoretical aspects too, involving some beasts called quantum groups, you can have a look at my book [12]. □

15e. Exercises

This was a quite advanced chapter, yes I know, and as exercises here, we have:

EXERCISE 15.37. *Learn more about partitions, and Möbius inversion.*

EXERCISE 15.38. *Among others, learn as well about the Lindstöm formula.*

EXERCISE 15.39. *Compute the cumulants of the various laws in chapters 11-12.*

EXERCISE 15.40. *Learn more about group easiness, and related topics.*

EXERCISE 15.41. *Learn as well about quantum groups, and quantum easiness.*

EXERCISE 15.42. *Learn, with full details, the Voiculescu theory of the R-transform.*

EXERCISE 15.43. *Learn also, with full details, the Speicher theory of free cumulants.*

EXERCISE 15.44. *Fully learn about the standard cube, and further meditate on it.*

As bonus exercise, and no surprise here, start reading a free probability book.

CHAPTER 16

Random matrices

16a. Operator theory

After the combinatorial horrors from the previous chapter, which are nevertheless something modern, conceptual and powerful, I mean if you plan a research career in mathematics or physics, please be sure that you will have to deal with such things, or worse, on a daily basis, we would like to end this book with something simpler, extremely useful, and refreshing. We will be interested here in the random matrices.

These matrices, which appear in a wide array of interesting questions in mathematics and physics, and even in more fringe contexts, such as economics and finance, but let's not talk about such bad things here, are something very simple, as follows:

DEFINITION 16.1. *A random matrix is a matrix with random variables as entries,*

$$Z \in M_N(L^\infty(X))$$

with X being a probability space.

Regarding the mathematics of such matrices, we will be mainly interested in computing their law. We will see in a moment that such matrices have indeed laws, with a suitable definition for the law, and in view of this, the following question makes sense:

QUESTION 16.2. *What are the laws of the various basic types of random matrices, as for instance those having i.i.d. entries, subject to simple constraints? Also, what happens to these laws in the $N >> 0$ regime, do we have some interesting asymptotics?*

Getting to work now, as a first task, we must talk about the laws of random matrices. Normally these come via the general constructions from chapter 15, but since the material in chapter 15 was missing many details, time now to properly do this.

So, let us start with the basics. As a first remark, since the random matrix algebras $M_N(L^\infty(X))$ from Definition 16.1 are obviously infinite dimensional, the best is to start our study with a discussion of the infinite dimensional algebras.

And here, the basic examples are the operator algebras. So, let us have as starting point the following definition, which is something that you certainly met before:

DEFINITION 16.3. *A Hilbert space is a complex vector space H with a scalar product $< x, y >$, taken linear at left and antilinear at right,*

$$< \lambda x, y >= \lambda < x, y > \quad , \quad < x, \lambda y >= \bar{\lambda} < x, y >$$

which is complete with respect to corresponding norm

$$||x|| = \sqrt{< x, x >}$$

in the sense that any sequence $\{x_n\}$ which is a Cauchy sequence, having the property $||x_n - x_m|| \to 0$ with $n, m \to \infty$, has a limit, $x_n \to x$.

Here the fact that $||x|| = \sqrt{< x, x >}$ is indeed a norm, satisfying $||x+y|| \leq ||x|| + ||y||$, follows from Cauchy-Schwarz, $| < x, y > | \leq ||x|| \cdot ||y||$, which itself follows as in the $H = \mathbb{C}^N$ case, by looking at the discriminant of the following degree 2 polynomial:

$$f(t) = ||wx + ty||^2$$

At the level of examples of Hilbert spaces, generalizing $H = \mathbb{C}^N$, we have:

THEOREM 16.4. *Given an index set I, which can be finite or not, the space of square-summable vectors having indices in I, namely*

$$l^2(I) = \left\{ (x_i)_{i \in I} \Big| \sum_i |x_i|^2 < \infty \right\}$$

is a Hilbert space, with scalar product as follows:

$$< x, y >= \sum_i x_i \bar{y}_i$$

When I is finite, $I = \{1, \ldots, N\}$, we obtain in this way the usual space $H = \mathbb{C}^N$.

PROOF. This is something very standard, the idea being as follows:

(1) We know that $l^2(I) \subset \mathbb{C}^I$ is the space of vectors satisfying $||x|| < \infty$. We want to prove that $l^2(I)$ is a vector space, that $< x, y >$ is a scalar product on it, that $l^2(I)$ is complete with respect to $||.||$, and finally that for $|I| < \infty$ we have $l^2(I) = \mathbb{C}^{|I|}$.

(2) The last assertion, $l^2(I) = \mathbb{C}^{|I|}$ for $|I| < \infty$, is clear, because in this case the sums are finite, so the condition $||x|| < \infty$ is automatic. So, we know at least one thing.

(3) Regarding the rest, we have Cauchy-Schwarz, $| < x, y > | \leq ||x|| \cdot ||y||$, proved as usual, by looking at $f(t) = ||wx+ty||^2$, and we deduce that we have $||x+y|| \leq ||x|| + ||y||$. Thus $l^2(I)$ is indeed a vector space, the other vector space conditions being trivial.

(4) Also, the quantity $< x, y >$ is surely a scalar product on this vector space, because all the conditions for a scalar product are trivially satisfied.

(5) Finally, the fact that our space $l^2(I)$ is indeed complete with respect to its norm $||.||$ follows in the obvious way, the limit of a Cauchy sequence $\{x_n\}$ being the vector $y = (y_i)$ given by $y_i = \lim_{n \to \infty} x_{ni}$, with all the verifications here being trivial. □

Going now a bit more abstract, we have, more generally, the following result:

THEOREM 16.5. *Given an arbitrary space X with a positive measure μ on it, the space of square-summable complex functions on it, namely*

$$L^2(X) = \left\{ f : X \to \mathbb{C} \Big| \int_X |f(x)|^2 \, d\mu(x) < \infty \right\}$$

is a Hilbert space, with scalar product as follows:

$$< f, g >= \int_X f(x)\overline{g(x)} \, d\mu(x)$$

When $X = I$ is discrete, meaning that the measure μ on it is the counting measure, $\mu(\{x\}) = 1$ for any $x \in X$, we obtain in this way the previous spaces $l^2(I)$.

PROOF. This is something routine, remake of Theorem 16.4, as follows:

(1) The proof of the first, and main assertion is something perfectly similar to the proof of Theorem 16.4, by replacing everywhere the sums by integrals.

(2) With the remark that we forgot to say in the statement that the L^2 functions are by definition taken up to equality almost everywhere, $f = g$ when $||f - g|| = 0$.

(3) As for the last assertion, when μ is the counting measure all our integrals here become usual sums, and so we recover in this way Theorem 16.4. □

As a third and last theorem about Hilbert spaces, that we will need, we have:

THEOREM 16.6. *Any Hilbert space H has an orthonormal basis $\{e_i\}_{i \in I}$, which is by definition a set of vectors whose span is dense in H, and which satisfy*

$$< e_i, e_j >= \delta_{ij}$$

with δ being a Kronecker symbol. The cardinality $|I|$ of the index set, which can be finite, countable, or worse, depends only on H, and is called dimension of H. We have

$$H \simeq l^2(I)$$

in the obvious way, mapping $\sum \lambda_i e_i \to (\lambda_i)$. The Hilbert spaces with $\dim H = |I|$ being countable, including $l^2(\mathbb{N})$ and $L^2(\mathbb{R})$, are all isomorphic, and are called separable.

PROOF. We have many assertions here, the idea being as follows:

(1) In finite dimensions an orthonormal basis $\{e_i\}_{i \in I}$ can be constructed by starting with any vector space basis $\{x_i\}_{i \in I}$, and using the well-known Gram-Schmidt procedure. As for the other assertions, these are all clear, from basic linear algebra.

(2) In general, the same method works, namely Gram-Schmidt, with a subtlety coming from the fact that the basis $\{e_i\}_{i \in I}$ will not span in general the whole H, but just a dense subspace of it, as it is in fact obvious by looking at the standard basis of $l^2(\mathbb{N})$.

(3) And there is a second subtlety as well, coming from the fact that the recurrence procedure needed for Gram-Schmidt must be replaced by some sort of "transfinite recurrence", using scary tools from logic, and more specifically the Zorn lemma.

(4) Finally, everything at the end is clear from definitions, except perhaps for the fact that $L^2(\mathbb{R})$ is separable. But here we can argue that, since functions can be approximated by polynomials, we have a countable algebraic basis, namely $\{x^n\}_{n\in\mathbb{N}}$, called the Weierstrass basis, that we can orthogonalize afterwards by using Gram-Schmidt. □

Moving ahead, now that we know what our vector spaces are, we can talk about infinite matrices with respect to them. And the situation here is as follows:

THEOREM 16.7. *Given a Hilbert space H, consider the linear operators $T : H \to H$, and for each such operator define its norm by the following formula:*

$$||T|| = \sup_{||x||=1} ||Tx||$$

The operators which are bounded, $||T|| < \infty$, form then a complex algebra $B(H)$, which is complete with respect to $||.||$. When H comes with a basis $\{e_i\}_{i\in I}$, we have

$$B(H) \subset M_I(\mathbb{C})$$

with the correspondence $T \to M$ coming via the usual linear algebra formulae, namely:

$$T(x) = Mx \quad , \quad M_{ij} = < Te_j, e_i >$$

In infinite dimensions, the inclusion $B(H) \subset M_I(\mathbb{C})$ is not an equality.

PROOF. This is something straightforward, the idea being as follows:

(1) The fact that we have indeed an algebra, satisfying the product condition in the statement, follows from the following estimates, which are all elementary:

$$||S + T|| \leq ||S|| + ||T|| \quad , \quad ||\lambda T|| = |\lambda| \cdot ||T|| \quad , \quad ||ST|| \leq ||S|| \cdot ||T||$$

(2) Regarding now the completness assertion, if $\{T_n\} \subset B(H)$ is Cauchy then $\{T_n x\}$ is Cauchy for any $x \in H$, so we can define the limit $T = \lim_{n\to\infty} T_n$ by setting:

$$Tx = \lim_{n\to\infty} T_n x$$

Let us first check that the application $x \to Tx$ is linear. We have:

$$\begin{aligned} T(x + y) &= \lim_{n\to\infty} T_n(x + y) \\ &= \lim_{n\to\infty} T_n(x) + T_n(y) \\ &= \lim_{n\to\infty} T_n(x) + \lim_{n\to\infty} T_n(y) \\ &= T(x) + T(y) \end{aligned}$$

Similarly, we have $T(\lambda x) = \lambda T(x)$, and we conclude that $x \to Tx$ is linear.

(3) With this done, it remains to prove now that we have $T \in B(H)$, and that $T_n \to T$ in norm. For this purpose, observe that we have:

$$\begin{aligned} ||T_n - T_m|| \leq \varepsilon \ , \ \forall n, m \geq N &\implies ||T_n x - T_m x|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n, m \geq N \\ &\implies ||T_n x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \ , \ \forall n \geq N \\ &\implies ||T_N x - Tx|| \leq \varepsilon \ , \ \forall ||x|| = 1 \\ &\implies ||T_N - T|| \leq \varepsilon \end{aligned}$$

But this gives both $T \in B(H)$, and $T_N \to T$ in norm, and we are done.

(4) Regarding the embedding, the correspondence $T \to M$ in the statement is indeed linear, and its kernel is $\{0\}$, so we have indeed an embedding as follows, as claimed:

$$B(H) \subset M_I(\mathbb{C})$$

In finite dimensions we have an isomorphism, because any matrix $M \in M_N(\mathbb{C})$ determines a linear operator $T : \mathbb{C}^N \to \mathbb{C}^N$, given by the following formula:

$$< Te_j, e_i >= M_{ij}$$

However, in infinite dimensions we have matrices not producing operators, as for instance the all-one matrix, so the embedding $B(H) \subset M_I(\mathbb{C})$ is not an isomorphism. □

Finally, as a second and last basic result regarding the operators, we will need:

THEOREM 16.8. *Each operator $T \in B(H)$ has an adjoint $T^* \in B(H)$, given by:*

$$< Tx, y >=< x, T^* y >$$

The operation $T \to T^*$ is antilinear, antimultiplicative, involutive, and satisfies:

$$||T|| = ||T^*|| \quad , \quad ||TT^*|| = ||T||^2$$

When H comes with a basis $\{e_i\}_{i \in I}$, the operation $T \to T^*$ corresponds to

$$(M^*)_{ij} = \overline{M}_{ji}$$

at the level of the associated matrices $M \in M_I(\mathbb{C})$.

PROOF. This is standard too, and can be proved in 3 steps, as follows:

(1) The existence of the adjoint operator T^*, given by the formula in the statement, comes from the fact that the function $\varphi(x) =< Tx, y >$ being a linear map $H \to \mathbb{C}$, we must have a formula as follows, for a certain vector $T^* y \in H$:

$$\varphi(x) =< x, T^* y >$$

Moreover, since this vector is unique, T^* is unique too, and we have as well:

$$(S + T)^* = S^* + T^* \quad , \quad (\lambda T)^* = \bar{\lambda} T^* \quad , \quad (ST)^* = T^* S^* \quad , \quad (T^*)^* = T$$

Observe also that we have indeed $T^* \in B(H)$, because:

$$\begin{aligned} ||T|| &= \sup_{||x||=1} \sup_{||y||=1} < Tx, y > \\ &= \sup_{||y||=1} \sup_{||x||=1} < x, T^*y > \\ &= ||T^*|| \end{aligned}$$

(2) Regarding now $||TT^*|| = ||T||^2$, which is a key formula, observe that we have:

$$||TT^*|| \leq ||T|| \cdot ||T^*|| = ||T||^2$$

On the other hand, we have as well the following estimate:

$$\begin{aligned} ||T||^2 &= \sup_{||x||=1} | < Tx, Tx > | \\ &= \sup_{||x||=1} | < x, T^*Tx > | \\ &\leq ||T^*T|| \end{aligned}$$

By replacing $T \to T^*$ we obtain from this $||T||^2 \leq ||TT^*||$, as desired.

(3) Finally, when H comes with a basis, the formula $< Tx, y >=< x, T^*y >$ applied with $x = e_i$, $y = e_j$ translates into the formula $(M^*)_{ij} = \overline{M}_{ji}$, as desired. □

16b. Random matrices

Getting now a bit abstract, we need to talk about operator algebras, as to suitably cover the random matrix algebras $M_N(L^\infty(X))$. Which can be something quite tricky, but fortunately, we have the following quick and clever definition, due to Gelfand:

Definition 16.9. *An abstract operator algebra, or C^*-algebra, is a complex algebra A having a norm $||.||$ and an involution $*$, subject to the following conditions:*

(1) *A is closed with respect to the norm.*
(2) *We have $||aa^*|| = ||a||^2$, for any $a \in A$.*

In other words, what we did here is to axiomatize the abstract properties of the operator algebras $A \subset B(H)$, without reference to the ambient Hilbert space H.

As basic examples now, we have the usual matrix algebras $M_N(\mathbb{C})$, with the norm and the involution being the usual matrix norm and involution, given by:

$$||A|| = \sup_{||x||=1} ||Ax|| \quad , \quad (A^*)_{ij} = \overline{A}_{ji}$$

Some other basic examples are the algebras $L^\infty(X)$ of essentially bounded functions $f : X \to \mathbb{C}$ on a measured space X, with the usual norm and involution, namely:

$$||f|| = \sup_{x \in X} |f(x)| \quad , \quad f^*(x) = \overline{f(x)}$$

We can put these two basic classes of examples together, as follows:

PROPOSITION 16.10. *The random matrix algebras $A = M_N(L^\infty(X))$ are C^*-algebras, with their usual norm and involution, given by:*

$$||Z|| = \sup_{x\in X} ||Z_x|| \quad , \quad (Z^*)_{ij} = \overline{Z}_{ij}$$

These algebras generalize both the algebras $M_N(\mathbb{C})$, and the algebras $L^\infty(X)$.

PROOF. The fact that the C^*-algebra axioms are satisfied is clear from definitions. As for the last assertion, this follows by taking $X = \{.\}$ and $N = 1$, respectively. □

We can in fact say more about the above algebras, as follows:

THEOREM 16.11. *Any algebra of type $L^\infty(X)$ is an operator algebra, as follows:*

$$L^\infty(X) \subset B(L^2(X)) \quad , \quad f \to (g \to fg)$$

More generally, any random matrix algebra is an operator algebra, as follows,

$$M_N(L^\infty(X)) \subset B\left(\mathbb{C}^N \otimes L^2(X)\right)$$

with the embedding being the above one, tensored with the identity.

PROOF. We have two assertions to be proved, the idea being as follows:

(1) Given $f \in L^\infty(X)$, consider the following operator, acting on $H = L^2(X)$:

$$T_f(g) = fg$$

Observe that T_f is indeed well-defined, and bounded as well, because:

$$||fg||_2 = \sqrt{\int_X |f(x)|^2|g(x)|^2 d\mu(x)} \leq ||f||_\infty ||g||_2$$

The application $f \to T_f$ being linear, involutive, continuous, and injective as well, we obtain in this way a C^*-algebra embedding $L^\infty(X) \subset B(H)$, as desired.

(2) Regarding the second assertion, this is best viewed in the following way:

$$\begin{aligned} M_N(L^\infty(X)) &= M_N(\mathbb{C}) \otimes L^\infty(X) \\ &\subset M_N(\mathbb{C}) \otimes B(L^2(X)) \\ &= B\left(\mathbb{C}^N \otimes L^2(X)\right) \end{aligned}$$

Here we have used (1), and some standard tensor product identifications. □

Our purpose in what follows is to develop the spectral theory of the C^*-algebras, and in particular that of the random matrix algebras $A = M_N(L^\infty(X))$ that we are interested in, one of our objectives being that of talking about spectral measures, in the normal case, in analogy with what we know about the usual matrices. Let us start with:

THEOREM 16.12. *Given an element $a \in A$ of a C^*-algebra, define its spectrum as:*

$$\sigma(a) = \left\{\lambda \in \mathbb{C}\middle| a - \lambda \notin A^{-1}\right\}$$

The following spectral theory results hold, exactly as in the $A = B(H)$ case:

(1) *We have $\sigma(ab) \cup \{0\} = \sigma(ba) \cup \{0\}$.*
(2) *We have $\sigma(f(a)) = f(\sigma(a))$, for any $f \in \mathbb{C}(X)$ having poles outside $\sigma(a)$.*
(3) *The spectrum $\sigma(a)$ is compact, non-empty, and contained in $D_0(||a||)$.*
(4) *The spectra of unitaries ($u^* = u^{-1}$) and self-adjoints ($a = a^*$) are on $\mathbb{T}, \mathbb{R}$.*
(5) *The spectral radius of normal elements ($aa^* = a^*a$) is given by $\rho(a) = ||a||$.*

In addition, assuming $a \in A \subset B$, the spectra of a with respect to A and to B coincide.

PROOF. Here the assertions (1-5), which are of course formulated a bit informally, are well-known for the full operator algebra $A = B(H)$, and the proof in general is similar:

(1) Assuming that $1 - ab$ is invertible, with inverse c, we have $abc = cab = c - 1$, and it follows that $1 - ba$ is invertible too, with inverse $1 + bca$. Thus $\sigma(ab), \sigma(ba)$ agree on $1 \in \mathbb{C}$, and by linearity, it follows that $\sigma(ab), \sigma(ba)$ agree on any point $\lambda \in \mathbb{C}^*$.

(2) The formula $\sigma(f(a)) = f(\sigma(a))$ is clear for polynomials, $f \in \mathbb{C}[X]$, by factorizing $f - \lambda$, with $\lambda \in \mathbb{C}$. Then, the extension to the rational functions is straightforward, because $P(a)/Q(a) - \lambda$ is invertible precisely when $P(a) - \lambda Q(a)$ is.

(3) By using $1/(1-b) = 1 + b + b^2 + \ldots$ for $||b|| < 1$ we obtain that $a - \lambda$ is invertible for $|\lambda| > ||a||$, and so $\sigma(a) \subset D_0(||a||)$. It is also clear that $\sigma(a)$ is closed, so what we have is a compact set. Finally, assuming $\sigma(a) = \emptyset$ the function $f(\lambda) = \varphi((a - \lambda)^{-1})$ is well-defined, for any $\varphi \in A^*$, and by Liouville we get $f = 0$, contradiction.

(4) Assuming $u^* = u^{-1}$ we have $||u|| = 1$, and so $\sigma(u) \subset D_0(1)$. But with $f(z) = z^{-1}$ we obtain via (2) that we have as well $\sigma(u) \subset f(D_0(1))$, and this gives $\sigma(u) \subset \mathbb{T}$. As for the result regarding the self-adjoints, this can be obtained from the result for the unitaries, by using (2) with functions of type $f(z) = (z + it)/(z - it)$, with $t \in \mathbb{R}$.

(5) It is routine to check, by integrating quantities of type $z^n/(z - a)$ over circles centered at the origin, and estimating, that the spectral radius is given by $\rho(a) = \lim ||a^n||^{1/n}$. But in the self-adjoint case, $a = a^*$, this gives $\rho(a) = ||a||$, by using exponents of type $n = 2^k$, and then the extension to the general normal case is straightforward.

(6) Regarding now the last assertion, the inclusion $\sigma_B(a) \subset \sigma_A(a)$ is clear. For the converse, assume $a - \lambda \in B^{-1}$, and set $b = (a - \lambda)^*(a - \lambda)$. We have then:

$$\sigma_A(b) - \sigma_B(b) = \left\{\mu \in \mathbb{C} - \sigma_B(b)\middle|(b - \mu)^{-1} \in B - A\right\}$$

Thus this difference in an open subset of $\mathbb{C}$. On the other hand b being self-adjoint, its two spectra are both real, and so is their difference. Thus the two spectra of b are equal, and in particular b is invertible in A, and so $a - \lambda \in A^{-1}$, as desired. □

We can now prove a key result about the operator algebras, as follows:

THEOREM 16.13 (Gelfand). *If X is a compact space, the algebra $C(X)$ of continuous functions on it $f : X \to \mathbb{C}$ is a C^*-algebra, with usual norm and involution, namely:*

$$||f|| = \sup_{x\in X} |f(x)| \quad , \quad f^*(x) = \overline{f(x)}$$

Conversely, any commutative C^*-algebra is of this form, $A = C(X)$, with

$$X = \left\{\chi : A \to \mathbb{C} \ , \ \text{normed algebra character}\right\}$$

with topology making continuous the evaluation maps $ev_a : \chi \to \chi(a)$.

PROOF. There are several things going on here, the idea being as follows:

(1) The first assertion is clear from definitions. Observe that we have indeed:

$$||ff^*|| = \sup_{x\in X} |f(x)|^2 = ||f||^2$$

Observe also that the algebra $C(X)$ is commutative, because $fg = gf$.

(2) Conversely, given a commutative C^*-algebra A, let us define X as in the statement. Then X is compact, and $a \to ev_a$ is a morphism of algebras, as follows:

$$ev : A \to C(X)$$

(3) We first prove that ev is involutive. We use the following formula, which is similar to the $z = Re(z) + iIm(z)$ decomposition formula for usual complex numbers:

$$a = \frac{a + a^*}{2} + i \cdot \frac{a - a^*}{2i}$$

Thus it is enough to prove $ev_{a^*} = ev_a^*$ for the self-adjoint elements a. But this is the same as proving that $a = a^*$ implies that ev_a is a real function, which is in turn true, by Theorem 16.12, because $ev_a(\chi) = \chi(a)$ is an element of $\sigma(a)$, contained in $\mathbb{R}$.

(4) Since A is commutative, each element is normal, so ev is isometric:

$$||ev_a|| = \rho(a) = ||a||$$

It remains to prove that ev is surjective. But this follows from the Stone-Weierstrass theorem, because $ev(A)$ is a closed subalgebra of $C(X)$, which separates the points. □

As a main consequence of the Gelfand theorem, we have:

THEOREM 16.14. *For any normal element $a \in A$ we have an identification as follows:*

$$< a >= C(\sigma(a))$$

In addition, given a function $f \in C(\sigma(a))$, we can apply it to a, and we have

$$\sigma(f(a)) = f(\sigma(a))$$

which generalizes the previous rational calculus formula, in the normal case.

PROOF. Since a is normal, the C^*-algebra $< a >$ that is generates is commutative, so if we denote by X the space of the characters $\chi :< a >\to \mathbb{C}$, we have:

$$< a >= C(X)$$

Now since the map $X \to \sigma(a)$ given by evaluation at a is bijective, we obtain:

$$< a >= C(\sigma(a))$$

Thus, we are dealing here with usual functions, and this gives all the assertions. □

In order to get now towards noncommutative probability, we first have to develop the theory of positive elements, and linear forms. First, we have the following result:

PROPOSITION 16.15. *For an element $a \in A$, the following are equivalent:*

(1) *a is positive, in the sense that $\sigma(a) \subset [0, \infty)$.*
(2) *$a = b^2$, for some $b \in A$ satisfying $b = b^*$.*
(3) *$a = cc^*$, for some $c \in A$.*

PROOF. This is something very standard, as follows:

(1) $\implies$ (2) Observe first that $\sigma(a) \subset \mathbb{R}$ implies $a = a^*$. Thus the algebra $< a >$ is commutative, and by using Theorem 16.14, we can set $b = \sqrt{a}$.

(2) $\implies$ (3) This is trivial, because we can simply set $c = b$.

(2) $\implies$ (1) This is clear too, because we have:

$$\sigma(a) = \sigma(b^2) = \sigma(b)^2 \subset \mathbb{R}^2 = [0, \infty)$$

(3) $\implies$ (1) We can proceed here by contradiction. Indeed, by multiplying c by a suitable element of the algebra $< cc^* >$, we are led to the existence of an element $d \neq 0$ satisfying $-dd^* \geq 0$. By writing now $d = x + iy$ with $x = x^*, y = y^*$ we have:

$$dd^* + d^*d = 2(x^2 + y^2) \geq 0$$

Thus $d^*d \geq 0$, which is easily seen to contradict the condition $-dd^* \geq 0$. □

We can talk as well about positive linear forms, as follows:

DEFINITION 16.16. *Consider a linear map $\varphi : A \to \mathbb{C}$.*

(1) *φ is called positive when $a \geq 0 \implies \varphi(a) \geq 0$.*
(2) *φ is called faithful and positive when $a \geq 0, a \neq 0 \implies \varphi(a) > 0$.*

In the commutative case, $A = C(X)$, the positive linear forms appear as follows, with μ being positive, and strictly positive if we want φ to be faithful and positive:

$$\varphi(f) = \int_X f(x)d\mu(x)$$

In general, the positive linear forms can be thought of as being integration functionals with respect to some underlying "positive measures". Based on this, we can formulate:

DEFINITION 16.17. *Let A be a C^*-algebra, given with a positive trace $tr : A \to \mathbb{C}$.*

(1) *The elements $a \in A$ are called random variables.*
(2) *The moments of such a variable are the numbers $M_k(a) = tr(a^k)$.*
(3) *The law of such a variable is the functional $\mu_a : P \to tr(P(a))$.*

To be more precise, here the exponent $k = \circ\bullet\bullet\circ\ldots$ is by definition a colored integer, and the powers a^k are defined by the following formulae, and multiplicativity:

$$a^\emptyset = 1 \quad , \quad a^\circ = a \quad , \quad a^\bullet = a^*$$

As for the polynomial P, this is a noncommuting $*$-polynomial in one variable:

$$P \in \mathbb{C} < X, X^* >$$

Observe that the law is uniquely determined by the moments, because we have:

$$P(X) = \sum_k \lambda_k X^k \implies \mu_a(P) = \sum_k \lambda_k M_k(a)$$

At the level of the general theory, we have the following key result, extending the various results from linear algebra, regarding the self-adjoint and normal matrices:

THEOREM 16.18. *Let A be a C^*-algebra, with a trace tr, and consider an element $a \in A$ which is normal, in the sense that $aa^* = a^*a$.*

(1) *μ_a is a complex probability measure, satisfying $supp(\mu_a) \subset \sigma(a)$.*
(2) *In the self-adjoint case, $a = a^*$, this measure μ_a is real.*
(3) *Assuming that tr is faithful, we have $supp(\mu_a) = \sigma(a)$.*

PROOF. In the normal case, $aa^* = a^*a$, the Gelfand theorem, or rather the subsequent continuous functional calculus theorem, tells us that we have:

$$< a >= C(\sigma(a))$$

Thus the functional $f(a) \to tr(f(a))$ can be regarded as an integration functional on the algebra $C(\sigma(a))$, and by the Riesz theorem, this latter functional must come from a probability measure μ on the spectrum $\sigma(a)$, in the sense that we must have:

$$tr(f(a)) = \int_{\sigma(a)} f(z) d\mu(z)$$

We are therefore led to the conclusions in the statement, with the uniqueness assertion coming from the fact that the elements a^k, taken as usual with respect to colored integer exponents, $k = \circ\bullet\bullet\circ\ldots$, generate the whole C^*-algebra $C(\sigma(a))$. □

As a first concrete application now, by getting back to the random matrices, and to the various questions raised in the beginning of this chapter, we have:

THEOREM 16.19. *Given a random matrix $Z \in M_N(L^\infty(X))$ which is normal,*

$$ZZ^* = Z^*Z$$

its law, which is by definition the following abstract functional,

$$\mu : \mathbb{C} < X, X^* > \to \mathbb{C} \quad , \quad P \to \frac{1}{N} \int_X tr(P(Z))$$

when restricted to the usual polynomials in two variables,

$$\mu : \mathbb{C}[X, X^*] \to \mathbb{C} \quad , \quad P \to \frac{1}{N} \int_X tr(P(Z))$$

must come from a probability measure on the spectrum $\sigma(Z) \subset \mathbb{C}$, as follows:

$$\mu(P) = \int_{\sigma(T)} P(x) d\mu(x)$$

We agree to use the symbol μ for all these notions.

PROOF. This follows indeed from what we know from Theorem 16.18, applied to the normal element $a = Z$, belonging to the C^*-algebra $A = M_N(L^\infty(X))$. □

At the level of the basic examples, the situation is as follows:

THEOREM 16.20. *The basic random matrices $Z \in M_N(L^\infty(X))$ are as follows:*

(1) *In the case $N = 1$ the random matrix is a usual random variable, $f \in L^\infty(X)$, automatically normal, and its law as defined above is the usual law.*
(2) *In the case $X = \{.\}$ the random matrix is a usual scalar matrix, $A \in M_N(\mathbb{C})$, and in the diagonalizable case, the law is $\mu = \frac{1}{N}(\delta_{\lambda_1} + \ldots + \delta_{\lambda_N})$.*

PROOF. This is clear indeed, with the first assertion coming from definitions, and the second assertion coming by diagonalizing the matrix, in the obvious way. □

At a more advanced level now, the main problem regarding the random matrices is that of computing the law of various classes of such matrices, coming in series:

QUESTION 16.21. *What is the law of random matrices coming in series*

$$Z_N \in M_N(L^\infty(X))$$

in the $N >> 0$ regime?

The general strategy here, coming from physicists, is that of computing first the asymptotic law μ^0, in the $N \to \infty$ limit, and then looking for the higher order terms as well, as to finally reach to a series in N^{-1} giving the law of Z_N, as follows:

$$\mu_N = \mu^0 + N^{-1}\mu^1 + N^{-2}\mu^2 + \ldots$$

As a basic example here, of particular interest are the matrices having i.i.d. complex normal entries, under the constraint $Z = Z^*$. Here the asymptotic law μ^0 is the Wigner semicircle law on $[-2, 2]$. We will discuss this in a moment, after some preliminaries.

16c. Gaussian matrices

We recall that a random matrix algebra is an algebra of type $A = M_N(L^\infty(X))$, and that we are interested in the computation of the laws of the operators $Z \in A$, called random matrices. Regarding the precise classes of random matrices that we are interested in, first we have the complex Gaussian matrices, which are constructed as follows:

DEFINITION 16.22. *A complex Gaussian matrix is a random matrix of type*

$$Z \in M_N(L^\infty(X))$$

which has i.i.d. complex normal entries.

We will see that the above matrices have an interesting, and "central" combinatorics, among all kinds of random matrices, with the study of the other random matrices being usually obtained as a modification of the study of the Gaussian matrices.

As a somewhat surprising remark, using real normal variables in Definition 16.22, instead of the complex ones appearing there, leads nowhere. The correct real versions of the Gaussian matrices are the Wigner random matrices, constructed as follows:

DEFINITION 16.23. *A Wigner matrix is a random matrix of type*

$$Z \in M_N(L^\infty(X))$$

which has i.i.d. complex normal entries, up to the constraint $Z = Z^*$.

In other words, a Wigner matrix must be as follows, with the diagonal entries being real normal variables, $a_i \sim g_t$, for some $t > 0$, the upper diagonal entries being complex normal variables, $b_{ij} \sim G_t$, the lower diagonal entries being the conjugates of the upper diagonal entries, as indicated, and with all the variables a_i, b_{ij} being independent:

$$Z = \begin{pmatrix} a_1 & b_{12} & \ldots & \ldots & b_{1N} \\ \bar{b}_{12} & a_2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{N-1} & b_{N-1,N} \\ \bar{b}_{1N} & \ldots & \ldots & \bar{b}_{N-1,N} & a_N \end{pmatrix}$$

As a comment here, for many concrete applications the Wigner matrices are in fact the central objects in random matrix theory, and in particular, they are often more important than the Gaussian matrices. In fact, these are the random matrices which were first considered and investigated, a long time ago, by Wigner himself.

Finally, we will be interested as well in the complex Wishart matrices, which are the positive versions of the above random matrices, constructed as follows:

DEFINITION 16.24. *A complex Wishart matrix is a random matrix of type*

$$Z = YY^* \in M_N(L^\infty(X))$$

with Y being a complex Gaussian matrix.

As before with the Gaussian and Wigner matrices, there are many possible comments that can be made here, of technical or historical nature. First, using in the above real Gaussian variables instead of complex ones leads to a less interesting combinatorics. Also, these matrices were introduced and studied by Marchenko-Pastur not long after Wigner, and so historically came second. Finally, in what regards their combinatorics and applications, these matrices quite often come first, before both the Gaussian and the Wigner ones, with all this being of course a matter of knowledge and taste.

Summarizing, we have three main types of random matrices, which can be somehow designated as "complex", "real" and "positive", and that we will study in what follows. Let us also mention that there are many other interesting classes of random matrices, usually appearing as modifications of the above. More on these later.

Getting to work now, we first have the following result:

THEOREM 16.25. *Given a sequence of Gaussian random matrices*

$$Z_N \in M_N(L^\infty(X))$$

having independent G_t variables as entries, for some fixed $t > 0$, we have

$$M_k\left(\frac{Z_N}{\sqrt{N}}\right) \simeq t^{|k|/2}|\mathcal{NC}_2(k)|$$

for any colored integer $k = \circ\bullet\bullet\circ\ldots$, in the $N \to \infty$ limit.

PROOF. This is something standard, which can be done as follows:

(1) We fix $N \in \mathbb{N}$, and we let $Z = Z_N$. Let us first compute the trace of Z^k. With $k = k_1 \ldots k_s$, and with the convention $(ij)^\circ = ij, (ij)^\bullet = ji$, we have:

$$\begin{aligned} Tr(Z^k) &= Tr(Z^{k_1} \ldots Z^{k_s}) \\ &= \sum_{i_1=1}^{N} \ldots \sum_{i_s=1}^{N} (Z^{k_1})_{i_1 i_2} (Z^{k_2})_{i_2 i_3} \ldots (Z^{k_s})_{i_s i_1} \\ &= \sum_{i_1=1}^{N} \ldots \sum_{i_s=1}^{N} (Z_{(i_1 i_2)^{k_1}})^{k_1} (Z_{(i_2 i_3)^{k_2}})^{k_2} \ldots (Z_{(i_s i_1)^{k_s}})^{k_s} \end{aligned}$$

(2) Next, we rescale our variable Z by a $\sqrt{N}$ factor, as in the statement, and we also replace the usual trace by its normalized version, $tr = Tr/N$. Our formula becomes:

$$tr\left(\left(\frac{Z}{\sqrt{N}}\right)^k\right) = \frac{1}{N^{s/2+1}}\sum_{i_1=1}^{N}\cdots\sum_{i_s=1}^{N}(Z_{(i_1i_2)^{k_1}})^{k_1}(Z_{(i_2i_3)^{k_2}})^{k_2}\ldots(Z_{(i_si_1)^{k_s}})^{k_s}$$

Thus, the moment that we are interested in is given by:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) = \frac{1}{N^{s/2+1}}\sum_{i_1=1}^{N}\cdots\sum_{i_s=1}^{N}\int_X(Z_{(i_1i_2)^{k_1}})^{k_1}(Z_{(i_2i_3)^{k_2}})^{k_2}\ldots(Z_{(i_si_1)^{k_s}})^{k_s}$$

(3) Let us apply now the Wick formula, from chapter 14. We conclude that the moment that we are interested in is given by the following formula:

$$\begin{aligned}
&M_k\left(\frac{Z}{\sqrt{N}}\right)\\
=\ &\frac{t^{s/2}}{N^{s/2+1}}\sum_{i_1=1}^{N}\cdots\sum_{i_s=1}^{N}\#\left\{\pi\in\mathcal{P}_2(k)\Big|\pi\leq\ker\left((i_1i_2)^{k_1},(i_2i_3)^{k_2},\ldots,(i_si_1)^{k_s}\right)\right\}\\
=\ &t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\frac{1}{N^{s/2+1}}\#\left\{i\in\{1,\ldots,N\}^s\Big|\pi\leq\ker\left((i_1i_2)^{k_1},(i_2i_3)^{k_2},\ldots,(i_si_1)^{k_s}\right)\right\}
\end{aligned}$$

(4) Our claim now is that in the $N\to\infty$ limit the combinatorics of the above sum simplifies, with only the noncrossing partitions contributing to the sum, and with each of them contributing precisely with a 1 factor, so that we will have, as desired:

$$\begin{aligned}
M_k\left(\frac{Z}{\sqrt{N}}\right) &= t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\left(\delta_{\pi\in NC_2(k)}+O(N^{-1})\right)\\
&\simeq t^{s/2}\sum_{\pi\in\mathcal{P}_2(k)}\delta_{\pi\in NC_2(k)}\\
&= t^{s/2}|\mathcal{NC}_2(k)|
\end{aligned}$$

(5) In order to prove this, the first observation is that when k is not uniform, in the sense that it contains a different number of $\circ$, $\bullet$ symbols, we have $\mathcal{P}_2(k)=\emptyset$, and so:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) = t^{s/2}|\mathcal{NC}_2(k)| = 0$$

(6) Thus, we are left with the case where k is uniform. Let us examine first the case where k consists of an alternating sequence of $\circ$ and $\bullet$ symbols, as follows:

$$k = \underbrace{\circ\bullet\circ\bullet\ldots\ldots\circ\bullet}_{2p}$$

In this case it is convenient to relabel our multi-index $i = (i_1, \ldots, i_s)$, with $s = 2p$, in the form $(j_1, l_1, j_2, l_2, \ldots, j_p, l_p)$. With this done, our moment formula becomes:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) = t^p \sum_{\pi\in\mathcal{P}_2(k)} \frac{1}{N^{p+1}} \#\left\{j, l \in \{1, \ldots, N\}^p \Big| \pi \leq \ker\left(j_1 l_1, j_2 l_1, j_2 l_2, \ldots, j_1 l_p\right)\right\}$$

Now observe that, with k being as above, we have an identification $\mathcal{P}_2(k) \simeq S_p$, obtained in the obvious way. With this done too, our moment formula becomes:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) = t^p \sum_{\pi\in S_p} \frac{1}{N^{p+1}} \#\left\{j, l \in \{1, \ldots, N\}^p \Big| j_r = j_{\pi(r)+1}, l_r = l_{\pi(r)}, \forall r\right\}$$

(7) We are now ready to do our asymptotic study, and prove the claim in (4). Let indeed $\gamma \in S_p$ be the full cycle, which is by definition the following permutation:

$$\gamma = (1\, 2\, \ldots\, p)$$

In terms of γ, the conditions $j_r = j_{\pi(r)+1}$ and $l_r = l_{\pi(r)}$ found above read:

$$\gamma\pi \leq \ker j \quad , \quad \pi \leq \ker l$$

Counting the number of free parameters in our moment formula, we obtain:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) = \frac{t^p}{N^{p+1}} \sum_{\pi\in S_p} N^{|\pi|+|\gamma\pi|} = t^p \sum_{\pi\in S_p} N^{|\pi|+|\gamma\pi|-p-1}$$

(8) The point now is that the last exponent is well-known to be ≤ 0, with equality precisely when the permutation $\pi \in S_p$ is geodesic, which in practice means that π must come from a noncrossing partition. Thus we obtain, in the $N \to \infty$ limit, as desired:

$$M_k\left(\frac{Z}{\sqrt{N}}\right) \simeq t^p |\mathcal{NC}_2(k)|$$

This finishes the proof in the case of the exponents k which are alternating, and the case where k is an arbitrary uniform exponent is similar, by permuting everything. □

We can further improve Theorem 16.25 by using free probability, as follows:

THEOREM 16.26. *Given a sequence of complex Gaussian matrices*

$$Z_N \in M_N(L^\infty(X))$$

having independent G_t variables as entries, with $t > 0$, we have

$$\frac{Z_N}{\sqrt{N}} \sim \Gamma_t$$

in the $N \to \infty$ limit, with the limiting measure being Voiculescu's circular law.

PROOF. According to Theorem 16.25 that we just proved, the asymptotic moments of the complex Gaussian matrices are given by the following formula:

$$M_k\left(\frac{Z_N}{\sqrt{N}}\right)\simeq t^{|k|/2}|\mathcal{NC}_2(k)|$$

On the other hand, it follows from the free probability theory developed in chapter 15 that an abstract noncommutative variable $a\in A$ is circular, following the Voiculescu circular law Γ_t, precisely when its moments are given by the following formula:

$$M_k(a)=t^{|k|/2}|\mathcal{NC}_2(k)|$$

Thus, we are led to the conclusion in the statement. □

The above result is of course something quite theoretical, and having it formulated as such is certainly something nice. However, and here comes our point, it is actually possible to use free probability theory in order to go well beyond this, with this time some truly new results on the random matrices. More on this, later in this chapter.

16d. Wigner and Wishart

Regarding now the Wigner matrices, which are something more understandable, because they are self-adjoint, we first have the following result, about them:

THEOREM 16.27. *Given a sequence of Wigner random matrices*

$$Z_N\in M_N(L^\infty(X))$$

having independent G_t variables as entries, with $t>0$, up to $Z_N=Z_N^*$, we have

$$M_k\left(\frac{Z_N}{\sqrt{N}}\right)\simeq t^{k/2}|NC_2(k)|$$

for any integer $k\in\mathbb{N}$, in the $N\to\infty$ limit.

PROOF. We have two possible proofs here, as follows:

(1) The formula in the statement can be certainly established via a direct computation based on the Wick formula, similar to that from the proof of Theorem 16.25.

(2) However, the best is to deduce this result from Theorem 16.25 itself. Indeed, we know from there that for Gaussian matrices $Y_N\in M_N(L^\infty(X))$ we have the following formula, valid for any colored integer $K=\circ\bullet\bullet\circ\ldots$, in the $N\to\infty$ limit:

$$M_K\left(\frac{Y_N}{\sqrt{N}}\right)\simeq t^{|K|/2}|\mathcal{NC}_2(K)|$$

By doing now some combinatorics, we deduce that we have the following formula for the moments of the matrices $Re(Y_N)$, with respect to usual exponents, $k \in \mathbb{N}$:

$$\begin{aligned} M_k\left(\frac{Re(Y_N)}{\sqrt{N}}\right) &= 2^{-k}\cdot M_k\left(\frac{Y_N}{\sqrt{N}}+\frac{Y_N^*}{\sqrt{N}}\right)\\ &= 2^{-k}\sum_{|K|=k} M_K\left(\frac{Y_N}{\sqrt{N}}\right)\\ &\simeq 2^{-k}\sum_{|K|=k} t^{k/2}|\mathcal{NC}_2(K)|\\ &= 2^{-k}\cdot t^{k/2}\cdot 2^{k/2}|\mathcal{NC}_2(k)|\\ &= 2^{-k/2}\cdot t^{k/2}|NC_2(k)| \end{aligned}$$

Now since the matrices $Z_N=\sqrt{2}Re(Y_N)$ are of Wigner type, this gives the result. □

In order to recapture now the Wigner measure from its moments, we can use:

PROPOSITION 16.28. *Given $t>0$, the real measure having as even moments the numbers $M_{2k}=t^kC_k$ and having all odd moments 0 is the measure*

$$\gamma_t=\frac{1}{2\pi t}\sqrt{4t-x^2}dx$$

called Wigner semicircle law on $[-2\sqrt{t},2\sqrt{t}]$.

PROOF. This follows indeed from the $t=1$ case, that we know well since chapter 13, when first discussing the Wigner law, via a change of variables. □

Now by putting everything together, we obtain the Wigner theorem, as follows:

THEOREM 16.29. *Given a sequence of Wigner random matrices*

$$Z_N\in M_N(L^\infty(X))$$

which by definition have i.i.d. complex normal entries, up to $Z_N=Z_N^*$, we have

$$Z_N\sim\gamma_t$$

in the $N\to\infty$ limit, where $\gamma_t=\frac{1}{2\pi t}\sqrt{4t-x^2}dx$ is the Wigner semicircle law.

PROOF. This follows indeed from all the above, and more specifically, by combining the moment formula from Theorem 16.27 with Proposition 16.28. □

Let us discuss now the Wishart matrices, which are the positive analogues of the Wigner matrices. Quite surprisingly, the computation here leads to the Catalan numbers, but not in the same way as for the Wigner matrices, the result being as follows:

THEOREM 16.30. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N \times N$ complex Gaussian of parameter $t > 0$, we have

$$M_k\left(\frac{W_N}{N}\right) \simeq t^k C_k$$

for any exponent $k \in \mathbb{N}$, in the $N \to \infty$ limit.

PROOF. There are several possible proofs for this result, as follows:

(1) A first method is by using the formula that we have in Theorem 16.25, for the Gaussian matrices Y_N. Indeed, we know from there that we have the following formula, valid for any colored integer $K = \circ\bullet\bullet\circ\ldots$, in the $N \to \infty$ limit:

$$M_K\left(\frac{Y_N}{\sqrt{N}}\right) \simeq t^{|K|/2}|\mathcal{NC}_2(K)|$$

With $K = \circ\bullet\circ\bullet\ldots$, alternating word of length $2k$, with $k \in \mathbb{N}$, this gives:

$$M_k\left(\frac{Y_N Y_N^*}{N}\right) \simeq t^k|\mathcal{NC}_2(K)|$$

Thus, in terms of the Wishart matrix $W_N = Y_N Y_N^*$ we have, for any $k \in \mathbb{N}$:

$$M_k\left(\frac{W_N}{N}\right) \simeq t^k|\mathcal{NC}_2(K)|$$

The point now is that, by doing some combinatorics, we have:

$$|\mathcal{NC}_2(K)| = |NC_2(2k)| = C_k$$

Thus, we are led to the formula in the statement.

(2) A second method, that we will explain now as well, is by proving the result directly, starting from definitions. The matrix entries of our matrix $W = W_N$ are given by:

$$W_{ij} = \sum_{r=1}^{N} Y_{ir}\bar{Y}_{jr}$$

Thus, the normalized traces of powers of W are given by the following formula:

$$\begin{aligned} tr(W^k) &= \frac{1}{N}\sum_{i_1=1}^{N}\ldots\sum_{i_k=1}^{N} W_{i_1i_2}W_{i_2i_3}\ldots W_{i_ki_1} \\ &= \frac{1}{N}\sum_{i_1=1}^{N}\ldots\sum_{i_k=1}^{N}\sum_{r_1=1}^{N}\ldots\sum_{r_k=1}^{N} Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k} \end{aligned}$$

By rescaling now W by a $1/N$ factor, as in the statement, we obtain:

$$tr\left(\left(\frac{W}{N}\right)^k\right)=\frac{1}{N^{k+1}}\sum_{i_1=1}^{N}\ldots\sum_{i_k=1}^{N}\sum_{r_1=1}^{N}\ldots\sum_{r_k=1}^{N}Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k}$$

By using now the Wick rule, we obtain the following formula for the moments, with $K=\circ\bullet\circ\bullet\ldots$, alternating word of lenght $2k$, and with $I=(i_1r_1,i_2r_1,\ldots,i_kr_k,i_1r_k)$:

$$\begin{aligned}M_k\left(\frac{W}{N}\right)&=\frac{t^k}{N^{k+1}}\sum_{i_1=1}^{N}\ldots\sum_{i_k=1}^{N}\sum_{r_1=1}^{N}\ldots\sum_{r_k=1}^{N}\#\left\{\pi\in\mathcal{P}_2(K)\Big|\pi\leq\ker(I)\right\}\\&=\frac{t^k}{N^{k+1}}\sum_{\pi\in\mathcal{P}_2(K)}\#\left\{i,r\in\{1,\ldots,N\}^k\Big|\pi\leq\ker(I)\right\}\end{aligned}$$

In order to compute this quantity, we use the standard bijection $\mathcal{P}_2(K)\simeq S_k$. By identifying the pairings $\pi\in\mathcal{P}_2(K)$ with their counterparts $\pi\in S_k$, we obtain:

$$M_k\left(\frac{W}{N}\right)=\frac{t^k}{N^{k+1}}\sum_{\pi\in S_k}\#\left\{i,r\in\{1,\ldots,N\}^k\Big|i_s=i_{\pi(s)+1},r_s=r_{\pi(s)},\forall s\right\}$$

Now let $\gamma\in S_k$ be the full cycle, which is by definition the following permutation:

$$\gamma=(1\,2\,\ldots\,k)$$

The general factor in the product computed above is then 1 precisely when following two conditions are simultaneously satisfied:

$$\gamma\pi\leq\ker i\quad,\quad\pi\leq\ker r$$

Counting the number of free parameters in our moment formula, we obtain:

$$M_k\left(\frac{W}{N}\right)=t^k\sum_{\pi\in S_k}N^{|\pi|+|\gamma\pi|-k-1}$$

The point now is that the last exponent is well-known to be ≤ 0, with equality precisely when the permutation $\pi\in S_k$ is geodesic, which in practice means that π must come from a noncrossing partition. Thus we obtain, in the $N\to\infty$ limit:

$$M_k\left(\frac{W}{N}\right)\simeq t^kC_k$$

Thus, we are led to the conclusion in the statement. □

In order to recapture now the corresponding measure, we can use our knowledge of the Marchenko-Pastur law π_1, from chapter 13, and we obtain in this way:

THEOREM 16.31. *Given a sequence of complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N \times N$ complex Gaussian of parameter $t > 0$, we have

$$\frac{W_N}{tN} \sim \frac{1}{2\pi}\sqrt{4x^{-1} - 1}\, dx$$

with $N \to \infty$, with the limiting measure being the Marchenko-Pastur law π_1.

PROOF. This follows indeed from Theorem 16.30, via our knowledge of π_1. □

As a comment now, while the above result is definitely something interesting at $t = 1$, at general $t > 0$ this looks more like a "fake" generalization of the $t = 1$ result, because the law π_1 stays the same, modulo a trivial rescaling. The reasons behind this phenomenon are quite subtle, and skipping some discussion, the point is that Theorem 16.31 is indeed something "fake" at general $t > 0$, and the correct generalization of the $t = 1$ computation, involving more general classes of complex Wishart matrices, is as follows:

THEOREM 16.32. *Given a sequence of general complex Wishart matrices*

$$W_N = Y_N Y_N^* \in M_N(L^\infty(X))$$

with Y_N being $N \times M$ complex Gaussian of parameter 1, we have

$$\frac{W_N}{N} \sim \max(1 - t, 0)\delta_0 + \frac{\sqrt{4t - (x - 1 - t)^2}}{2\pi x}\, dx$$

with $M = tN \to \infty$, with the limiting measure being the Marchenko-Pastur law π_t.

PROOF. This is again something which is very standard, as follows:

(1) In order to prove the formula in the statement, we can proceed as usual, by using the Wick formula. The matrix entries of our Wishart matrix $W = W_N$ are given by:

$$W_{ij} = \sum_{r=1}^{M} Y_{ir}\bar{Y}_{jr}$$

Thus, the normalized traces of powers of W are given by the following formula:

$$\begin{aligned} tr(W^k) &= \frac{1}{N}\sum_{i_1=1}^{N}\cdots\sum_{i_k=1}^{N} W_{i_1i_2}W_{i_2i_3}\ldots W_{i_ki_1} \\ &= \frac{1}{N}\sum_{i_1=1}^{N}\cdots\sum_{i_k=1}^{N}\sum_{r_1=1}^{M}\cdots\sum_{r_k=1}^{M} Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k} \end{aligned}$$

By rescaling now W by a $1/N$ factor, as in the statement, we obtain:

$$tr\left(\left(\frac{W}{N}\right)^k\right) = \frac{1}{N^{k+1}}\sum_{i_1=1}^{N}\cdots\sum_{i_k=1}^{N}\sum_{r_1=1}^{M}\cdots\sum_{r_k=1}^{M} Y_{i_1r_1}\bar{Y}_{i_2r_1}Y_{i_2r_2}\bar{Y}_{i_3r_2}\ldots Y_{i_kr_k}\bar{Y}_{i_1r_k}$$

(2) By using now the Wick rule, we obtain the following formula for the moments, with $K = \circ\bullet\circ\bullet\ldots$, alternating word of lenght $2k$, and $I = (i_1r_1, i_2r_1, \ldots, i_kr_k, i_1r_k)$:

$$\begin{aligned} M_k\left(\frac{W}{N}\right) &= \frac{1}{N^{k+1}}\sum_{i_1=1}^{N}\ldots\sum_{i_k=1}^{N}\sum_{r_1=1}^{M}\ldots\sum_{r_k=1}^{M}\#\left\{\pi\in\mathcal{P}_2(K)\Big|\pi\leq\ker I\right\} \\ &= \frac{1}{N^{k+1}}\sum_{\pi\in\mathcal{P}_2(K)}\#\left\{i\in\{1,\ldots,N\}^k, r\in\{1,\ldots,M\}^k\Big|\pi\leq\ker I\right\} \end{aligned}$$

(3) In order to compute this quantity, we use the standard bijection $\mathcal{P}_2(K)\simeq S_k$. By identifying the pairings $\pi\in\mathcal{P}_2(K)$ with their counterparts $\pi\in S_k$, we obtain:

$$M_k\left(\frac{W}{N}\right) = \frac{1}{N^{k+1}}\sum_{\pi\in S_k}\#\left\{i\in\{1,\ldots,N\}^k, r\in\{1,\ldots,M\}^k\Big|i_s=i_{\pi(s)+1}, r_s=r_{\pi(s)}\right\}$$

Now let $\gamma\in S_k$ be the full cycle, which is by definition the following permutation:

$$\gamma = (1\,2\,\ldots\,k)$$

The general factor in the product computed above is then 1 precisely when following two conditions are simultaneously satisfied:

$$\gamma\pi\leq\ker i\quad,\quad\pi\leq\ker r$$

Counting the number of free parameters in our expectation formula, we obtain:

$$M_k\left(\frac{W}{N}\right)=\frac{1}{N^{k+1}}\sum_{\pi\in S_k}N^{|\gamma\pi|}M^{|\pi|}=\sum_{\pi\in S_k}N^{|\gamma\pi|-k-1}M^{|\pi|}$$

(4) Now by using the same arguments as in the case $M=N$, from the proof of Theorem 16.30, we conclude that in the $M=tN\to\infty$ limit the permutations $\pi\in S_k$ which matter are those coming from noncrossing partitions, and so that we have:

$$M_k\left(\frac{W}{N}\right)\simeq\sum_{\pi\in NC(k)}N^{-|\pi|}M^{|\pi|}=\sum_{\pi\in NC(k)}t^{|\pi|}$$

(5) But these numbers are the moments of the Marchenko-Pastur law π_t, which in addition has the density given by the formula in the statement, as desired. □

And with this, end of our basic learning regarding the random matrices, the conclusion being that the asymptotic laws of these matrices are the main laws in free probability.

We would like to end the present chapter, and book, with some key asymptotic freeness results of Voiculescu [89]. Let us begin with the Wigner matrices. We have here:

THEOREM 16.33. *Given a family of sequences of Wigner matrices,*

$$Z_N^i \in M_N(L^\infty(X)) \quad , \quad i \in I$$

with pairwise independent entries, each following the complex normal law G_t, with $t > 0$, up to the constraint $Z_N^i = (Z_N^i)^*$, the rescaled sequences of matrices

$$\frac{Z_N^i}{\sqrt{N}} \in M_N(L^\infty(X)) \quad , \quad i \in I$$

become with $N \to \infty$ semicircular, each following the Wigner law γ_t, and free.

PROOF. This is something quite subtle, the idea being as follows:

(1) First of all, we know from Theorem 16.29 that for any $i \in I$ the corresponding sequence of rescaled Wigner matrices becomes semicircular in the $N \to \infty$ limit:

$$\frac{Z_N^i}{\sqrt{N}} \simeq \gamma_t$$

(2) Thus, what is new here, and that we have to prove, is the asymptotic freeness assertion. For this purpose we can assume that we are dealing with the case of 2 sequences of matrices, $|I| = 2$. So, assume that we have Wigner matrices as follows:

$$Z_N, Z_N' \in M_N(L^\infty(X))$$

We have to prove that these matrices become asymptotically free, with $N \to \infty$.

(3) But this something that can be proved directly, via various routine computations with partitions, which simplify as usual in the $N \to \infty$ limit, and bring freeness.

(4) However, we can prove this as well by using a trick, based on the result in Theorem 16.26. Consider indeed the following random matrix:

$$Y_N = \frac{1}{\sqrt{2}}(Z_N + iZ_N')$$

This is then a complex Gaussian matrix, and so by using Theorem 16.26, we obtain that in the limit $N \to \infty$, we have:

$$\frac{Y_N}{\sqrt{N}} \simeq \Gamma_t$$

Now recall that the circular law Γ_t was by definition the law of the following variable, with a, b being semicircular, each following the law γ_t, and free:

$$c = \frac{1}{\sqrt{2}}(a + ib)$$

We are therefore in the situation where the variable $(Z_N + iZ_N')/\sqrt{N}$, which has asymptotically semicircular real and imaginary parts, converges to the distribution of

$a + ib$, equally having semicircular real and imaginary parts, but with these real and imaginary parts being free. Thus Z_N, Z'_N become asymptotically free, as desired. □

Getting now to the complex case, we have a similar result here, as follows:

THEOREM 16.34. *Given a family of sequences of complex Gaussian matrices,*

$$Z_N^i \in M_N(L^\infty(X)) \quad , \quad i \in I$$

with pairwise independent entries, each following the complex normal law G_t, with $t > 0$, the rescaled sequences of matrices

$$\frac{Z_N^i}{\sqrt{N}} \in M_N(L^\infty(X)) \quad , \quad i \in I$$

become with $N \to \infty$ circular, each following the Voiculescu law Γ_t, and free.

PROOF. This follows from Theorem 16.33, which applies to the real and imaginary parts of our complex Gaussian matrices, and gives the result. □

We have as well a result for the Wishart matrices, as follows:

THEOREM 16.35. *Given a family of sequences of complex Wishart matrices,*

$$Z_N^i = Y_N^i (Y_N^i)^* \in M_N(L^\infty(X)) \quad , \quad i \in I$$

with each Y_N^i being a $N \times M$ matrix, with entries following the normal law G_1, and with all these entries being pairwise independent, the rescaled sequences of matrices

$$\frac{Z_N^i}{N} \in M_N(L^\infty(X)) \quad , \quad i \in I$$

become with $M = tN \to \infty$ Marchenko-Pastur, each following the law π_t, and free.

PROOF. Here the first assertion is the Marchenko-Pastur theorem, and the second assertion follows from the freeness result for the Gaussian matrices. □

16e. Exercises

Congratulations for having read this book, and no exercises for this final chapter. Instead, you can have a look at the various books referenced below.

Bibliography

[1] A.A. Abrikosov, Fundamentals of the theory of metals, Dover (1988).

[2] G.W. Anderson, A. Guionnet and O. Zeitouni, An introduction to random matrices, Cambridge Univ. Press (2010).

[3] T.M. Apostol, Introduction to analytic number theory, Springer (1976).

[4] V.I. Arnold, Mathematical methods of classical mechanics, Springer (1974).

[5] V.I. Arnold, Catastrophe theory, Springer (1974).

[6] V.I. Arnold, Lectures on partial differential equations, Springer (1997).

[7] N.W. Ashcroft and N.D. Mermin, Solid state physics, Saunders College Publ. (1976).

[8] M.F. Atiyah, The geometry and physics of knots, Cambridge Univ. Press (1990).

[9] J. Baik, P. Deift and T. Suidan, Combinatorics and random matrix theory, AMS (2016).

[10] T. Banica, Principles of mathematics (2026).

[11] T. Banica, Calculus and applications (2026).

[12] T. Banica, Methods of free probability (2024).

[13] R.J. Baxter, Exactly solved models in statistical mechanics, Academic Press (1982).

[14] I. Bengtsson and K. Życzkowski, Geometry of quantum states, Cambridge Univ. Press (2006).

[15] N. Berline, E. Getzler and M. Vergne, Heat kernels and Dirac operators, Springer (2004).

[16] G. Blower, Random matrices: high dimensional phenomena, Cambridge Univ. Press (2009).

[17] S.J. Blundell and K.M. Blundell, Concepts in thermal physics, Oxford Univ. Press (2006).

[18] B. Bollobás, Random graphs, Cambridge Univ. Press (1985).

[19] A. Borodin, I. Corwin and A. Guionnet, eds., Random matrices, AMS (2019).

[20] A. Bose, Random matrices and non-commutative probability, CRC Press (2021).

[21] A. Bose and M. Bhattacharjee, Large covariance and autocovariance matrices, CRC Press (2018).

[22] P.M. Chaikin and T.C. Lubensky, Principles of condensed matter physics, Cambridge Univ. Press (1995).

[23] A. Connes, Noncommutative geometry, Academic Press (1994).

[24] P. Deift, Orthogonal polynomials and random matrices: a Riemann-Hilbert approach, AMS (1999).

[25] P. Di Francesco, P. Mathieu and D. Sénéchal, Conformal field theory, Springer (1996).

[26] P.A.M. Dirac, Principles of quantum mechanics, Oxford Univ. Press (1930).

[27] M.P. do Carmo, Differential geometry of curves and surfaces, Dover (1976).

[28] M. Dresher, The mathematics of games of strategy, Dover (1981).

[29] R. Durrett, Probability: theory and examples, Cambridge Univ. Press (1990).

[30] R. Durrett, Random graph dynamics, Cambridge Univ. Press (2010).

[31] A. Einstein, Relativity: the special and the general theory, Dover (1916).

[32] L.C. Evans, Partial differential equations, AMS (1998).

[33] B. Eynard, Counting surfaces, Birkhäuser (2016).

[34] W. Feller, An introduction to probability theory and its applications, Wiley (1950).

[35] E. Fermi, Thermodynamics, Dover (1937).

[36] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics I: mainly mechanics, radiation and heat, Caltech (1963).

[37] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics II: mainly electromagnetism and matter, Caltech (1964).

[38] R.P. Feynman, R.B. Leighton and M. Sands, The Feynman lectures on physics III: quantum mechanics, Caltech (1966).

[39] R.P. Feynman and A.R. Hibbs, Quantum mechanics and path integrals, Dover (1965).

[40] P. Flajolet and R. Sedgewick, Analytic combinatorics, Cambridge Univ. Press (2009).

[41] A.P. French, Special relativity, Taylor and Francis (1968).

[42] C. Godsil and G. Royle, Algebraic graph theory, Springer (2001).

[43] H. Goldstein, C. Safko and J. Poole, Classical mechanics, Addison-Wesley (1980).

[44] D.L. Goodstein, States of matter, Dover (1975).

[45] M.B. Green, J.H. Schwarz and E. Witten, Superstring theory, Cambridge Univ. Press (2012).

[46] D.J. Griffiths, Introduction to electrodynamics, Cambridge Univ. Press (2017).

[47] D.J. Griffiths and D.F. Schroeter, Introduction to quantum mechanics, Cambridge Univ. Press (2018).

[48] D.J. Griffiths, Introduction to elementary particles, Wiley (2020).

[49] R. Gurau, Random tensors, Oxford Univ. Press (2016).

[50] W.A. Harrison, Solid state theory, Dover (1970).

[51] W.A. Harrison, Electronic structure and the properties of solids, Dover (1980).

[52] F. Hiai and D. Petz, The semicircle law, free random variables and entropy, AMS (2000).

[53] L. Hörmander, The analysis of linear partial differential operators, Springer (1983).

[54] R.A. Horn and C.R. Johnson, Matrix analysis, Cambridge Univ. Press (1985).

[55] K. Huang, Introduction to statistical physics, CRC Press (2001).

[56] K. Huang, Quantum field theory, Wiley (1998).

[57] K. Huang, Quarks, leptons and gauge fields, World Scientific (1982).

[58] V.F.R. Jones, Subfactors and knots, AMS (1991).

[59] L.P. Kadanoff, Statistical physics: statics, dynamics and renormalization, World Scientific (2000).

[60] T. Kibble and F.H. Berkshire, Classical mechanics, Imperial College Press (1966).

[61] M. Kumar, Quantum: Einstein, Bohr, and the great debate about the nature of reality, Norton (2009).

[62] T. Lancaster and K.M. Blundell, Quantum field theory for the gifted amateur, Oxford Univ. Press (2014).

[63] L.D. Landau and E.M. Lifshitz, Mechanics, Pergamon Press (1960).

[64] L.D. Landau and E.M. Lifshitz, The classical theory of fields, Addison-Wesley (1951).

[65] L.D. Landau and E.M. Lifshitz, Quantum mechanics: non-relativistic theory, Pergamon Press (1959).

[66] S. Lang, Algebra, Addison-Wesley (1993).

[67] P. Lax, Linear algebra and its applications, Wiley (2007).

[68] P. Lax, Functional analysis, Wiley (2002).

[69] P. Lax and M.S. Terrell, Calculus with applications, Springer (2013).

[70] P. Lax and M.S. Terrell, Multivariable calculus with applications, Springer (2018).

[71] T.M. Liggett, Interacting particle systems, Springer (1985).

[72] G. Livan, M. Novaes and P. Vivo, Introduction to random matrices: theory and practice, Springer (2018).

[73] M.L. Mehta, Random matrices, Elsevier (2004).

[74] J.A. Mingo and R. Speicher, Free probability and random matrices, Springer (2017).

[75] A. Nica and R. Speicher, Lectures on the combinatorics of free probability, Cambridge Univ. Press (2006).

[76] M.A. Nielsen and I.L. Chuang, Quantum computation and quantum information, Cambridge Univ. Press (2000).

[77] R.K. Pathria and and P.D. Beale, Statistical mechanics, Elsevier (1972).

[78] M. Potters and J.P. Bouchaud, A first course in random matrix theory, Cambridge Univ. Press (2020).

[79] W. Rudin, Principles of mathematical analysis, McGraw-Hill (1964).

[80] W. Rudin, Real and complex analysis, McGraw-Hill (1966).

[81] W. Rudin, Functional analysis, McGraw-Hill (1973).

[82] K. Schmüdgen, The moment problem, Springer (2017).

[83] D.V. Schroeder, An introduction to thermal physics, Oxford Univ. Press (1999).

[84] J. Schwinger and B.H. Englert, Quantum mechanics: symbolism of atomic measurements, Springer (2001).

[85] R. Shankar, Fundamentals of physics, Yale Univ. Press (2014).

[86] A.M. Steane, Thermodynamics, Oxford Univ. Press (2016).

[87] S. Sternberg, Dynamical systems, Dover (2010).

[88] J.R. Taylor, Classical mechanics, Univ. Science Books (2003).

[89] D.V. Voiculescu, K.J. Dykema and A. Nica, Free random variables, AMS (1992).

[90] J. von Neumann, Mathematical foundations of quantum mechanics, Princeton Univ. Press (1955).

[91] J. von Neumann and O. Morgenstern, Theory of games and economic behavior, Princeton Univ. Press (1944).

[92] J. Watrous, The theory of quantum information, Cambridge Univ. Press (2018).

[93] S. Weinberg, Foundations of modern physics, Cambridge Univ. Press (2011).

[94] S. Weinberg, Lectures on quantum mechanics, Cambridge Univ. Press (2012).

[95] S. Weinberg, Lectures on astrophysics, Cambridge Univ. Press (2019).

[96] S. Weinberg, Cosmology, Oxford Univ. Press (2008).

[97] H. Weyl, The theory of groups and quantum mechanics, Princeton Univ. Press (1931).

[98] H. Weyl, The classical groups: their invariants and representations, Princeton Univ. Press (1939).

[99] H. Weyl, Space, time, matter, Princeton Univ. Press (1918).

[100] B. Zwiebach, A first course in string theory, Cambridge Univ. Press (2004).

Index