# A Diophantine equation as a condition of equiprobability

Andrea Prunotto
Haslacherstraße 119, 79115 Freiburg im Breisgau, Germany
andrea.prunotto@gmail.com

February 5, 2018

**Abstract**

The condition of equiprobability among two events involving independent extractions of elements from a finite set is shown to be related to the solutions of a Diophantine equation.

## 1 Definitions of the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$

A set $C$ contains $c$ elements of three different kinds: there are $\alpha > 0$ elements of kind $A$, $\beta > 0$ elements of kind $B$ and $\gamma \geq 0$ elements of kind $G$, and $|C| = c = \alpha + \beta + \gamma$.

We perform $n > 0$ independent extractions (i.e. with replacement) of one element at a time from the set $C$ and we define the event $\mathscr{E}_n^G$ as "to get, in $n$ independent trials, exactly $n$ times one element of kind $G$", so that $P(\mathscr{E}_n^G) = \left(\frac{\gamma}{c}\right)^n$ (the order of the trials matters).

We define also the event $\mathscr{L}_n^{AB}$ as "to get, in $n$ independent trials, at least one element of kind $A$ and at least one element of kind $B$", so that $P(\mathscr{L}_n^{AB}) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n$.

## 2 Distributions of successes for $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$

Given the $n$ trials $k \in \{1, 2 \dots n\}$, we can define the $n$ events $\mathscr{E}_{n,k}^G$ as "to verify the event $\mathscr{E}_n^G$ in correpondence of the trial $k$" and the $n$ events $\mathscr{L}_{n,k}^{AB}$ as "to verify the event $\mathscr{L}_n^{AB}$ in correpondence of the trial $k$", so that $P(\mathscr{E}_{n,k}^G) = \left(\frac{\gamma}{c}\right)^n \delta_{n,k}$ (the event $\mathscr{E}_n^G$ can occur only in correspondence of the last trial) and $P(\mathscr{L}_{n,k}^{AB}) = 1 - \left(\frac{\alpha+\gamma}{c}\right)^k - \left(\frac{\beta+\gamma}{c}\right)^k + \left(\frac{\gamma}{c}\right)^k$. Clearly, $P(\mathscr{E}_{n,n}^G) = P(\mathscr{E}_n^G)$ and $P(\mathscr{L}_{n,n}^{AB}) = P(\mathscr{L}_n^{AB})$.

Given $\alpha, \beta, \gamma$, we will refer to the discrete functions of $k$ $P(\mathscr{E}_{n,k}^G)$ and $P(\mathscr{L}_{n,k}^{AB})$ as to the "distributions of successes" for the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$, respectively.

### 2.1 Distributions of successes as sets of $n$ targets

In order to facilitate the comparison between the two distributions of successes as a function of $k \in \{1, 2 \dots n\}$ (given the same $\alpha, \beta, \gamma$), each value of $P(\mathscr{E}^G_{n,k})$ and of $P(\mathscr{L}^{AB}_{n,k})$ can be represented by the area of a target, and each trial $k$ can be interpreted as a single, random shot aiming the corresponding target.

The configuration of the sets of $n$ targets related to the two distributions are different (see Fig. 1), in particular because $P(\mathscr{L}^{AB}_{n,k'}|\mathscr{L}^{AB}_{n,k}) = 1$ for each $k' > k$: If the target related to $P(\mathscr{L}^{AB}_{n,k})$ is hit, all the targets related to $P(\mathscr{L}^{AB}_{n,k'})$, with $k' > k$, will result hit as well (in fact, if we get at least one element of kind $A$ and at least one element of kind $B$ in correspondence of the $k$-th trial, then we would have already obtained them at least once in all the next trials, verifying $\mathscr{L}^{AB}_n$, no matter the kinds of element extracted after the $k$-th trial).

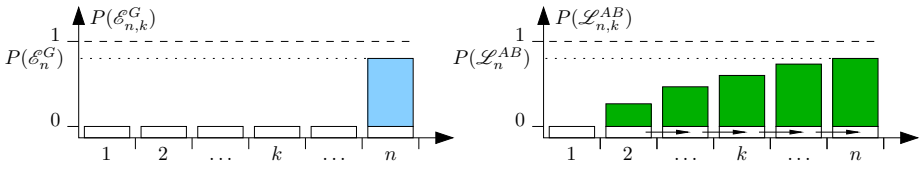


**Figure 1:** Distributions of successes for the events $\mathscr{E}^G_n$ (right) and $\mathscr{L}^{AB}_n$ (left), related to the same $\alpha, \beta, \gamma$, as a function of the (ordered) number of trial $k$. The target areas associated to $P(\mathscr{E}^G_{n,k})$ are colored in blue, whereas the ones associated to $P(\mathscr{L}^{AB}_{n,k})$ are colored in green. In each trial ($x$-axis), one single shot aims the related target. Each target has the same width, therefore the probabilities to hit the targets are fully described by the targets heights ($y$-axis). The left graph shows that the event $\mathscr{E}^G_n$ can occur only in correspondence of the last trial, with probability $P(\mathscr{E}^G_n) = P(\mathscr{E}^G_{n,n})$. The arrows at the bottom of the green targets (right graph) represent a device implementing the property $P(\mathscr{L}^{AB}_{n,k'}|\mathscr{L}^{AB}_{n,k}) = 1$: If a green target $k$ is hit, all the green targets $k' > k$ are hit (but not viceversa), with a domino-effect. In this example we assumed $P(\mathscr{E}^G_n) = P(\mathscr{L}^{AB}_n)$.

## 3 Equiprobability between $\mathscr{E}^G_n$ and $\mathscr{L}^{AB}_n$

Given the same $\alpha, \beta, \gamma$, we study for which $n$ it applies $P(\mathscr{E}^G_n) = P(\mathscr{L}^{AB}_n)$.

### 3.1 Observation 1

If $P(\mathscr{E}^G_n) = P(\mathscr{L}^{AB}_n)$ and $n > 2$, the probability to hit targets related to the event $\mathscr{E}^G_n$ (i.e. the first one, *or* the second one, *or* the third one, etc., given the available $n$ shots, one for each target) is less than the probability to hit targets related to the event $\mathscr{L}^{AB}_n$, because the last target has the same height in both cases, i.e. $P(\mathscr{E}^G_{n,n}) = P(\mathscr{L}^{AB}_{n,n})$, but there are $n-2$ more targets (with non-zero height) related to $\mathscr{L}^{AB}_n$, but not to $\mathscr{E}^G_n$.

This observation is represented in Fig. 1, in which $P(\mathscr{E}^G_n) = P(\mathscr{L}^{AB}_n)$.

### 3.2 Observation 2

We notice that $P(\mathscr{E}_n^G) = P(\mathscr{E}_{n,1}^G \cup \mathscr{E}_{n,2}^G \ldots \cup \mathscr{E}_{n,n}^G)$, since the only $\mathscr{E}_{n,k}^G \neq \emptyset$ is $\mathscr{E}_{n,n}^G = \mathscr{E}_n^G$, and that $P(\mathscr{L}_n^{AB}) = P(\mathscr{L}_{n,1}^{AB} \cup \mathscr{L}_{n,2}^{AB} \ldots \cup \mathscr{L}_{n,n}^{AB})$, since $\mathscr{L}_{n,k}^{AB} \subset \mathscr{L}_{n,k'}^{AB}$ for each $1 \leq k < k' \leq n$. Therefore, the request $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$ implies also $P(\mathscr{E}_{n,1}^G \cup \mathscr{E}_{n,2}^G \ldots \cup \mathscr{E}_{n,n}^G) = P(\mathscr{L}_{n,1}^{AB} \cup \mathscr{L}_{n,2}^{AB} \ldots \cup \mathscr{L}_{n,n}^{AB})$.

### 3.3 Contradiction between the two observations

In the final equation of the Observation 2, the symbol $\cup$ can be substituted with the word *or*. Therefore, this observation excludes any difference between the probability to hit targets related to the event $\mathscr{E}_n^G$ (i.e. the first one, *or* the second one, *or* the third one, etc.) and the probability to hit targets related to the event $\mathscr{L}_n^{AB}$, in contradiction with the Observation 1.

### 3.4 Avoiding the contradiction

Since the structure of $\mathscr{E}_n^G$ prevents to add any target (in particular, any target with non-zero height) to the single one associated to its distribution of successes, there are only two possibilities to keep the equiprobability (and the same values of $\alpha, \beta, \gamma$), avoiding the above contradiction: Either to reduce the number of targets related to the distribution of successes of $\mathscr{L}_n^{AB}$ to a single one as well – which, thus, must be of height $P(\mathscr{E}_n^G)$ – or to remove all the targets. In detail,

- If $\alpha, \beta, \gamma > 0$, the distribution $P(\mathscr{L}_{n,k}^{AB})$ is a strictly monotonically increasing function of $k$. Therefore, $\mathscr{L}_n^{AB}$ is associated to a unique target if and only if $n = 2$.
- Alternatively, we can remove all the targets, which means to impose $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB}) = 0$ (i.e. $\gamma = 0$, i.e no elements of kind $G$) and to perform $n = 1$ trials ($\mathscr{L}_n^{AB}$ cannot occur at the first trial).

In conclusion, the equiprobability between the events $\mathscr{E}_n^G$ and $\mathscr{L}_n^{AB}$, related to the same set $C$ (i.e. to the same values of $\alpha, \beta, \gamma$), can be achieved only if $n \leq 2$.

## 4 Equiprobability as a Diophantine equation

An appropriate choice of $\alpha, \beta > 0$ and $\gamma \geq 0$ allows the naturals $a \equiv \alpha + \gamma$ and $b \equiv \beta + \gamma$ to assume any value greater than 1. Similarly, given $c = \alpha + \beta + \gamma \geq 2$, we can build any $a, b$ such that $a, b < c$ and $a + b \geq c$ (e.g. by means of the sides of a triangle whose hypotenuse is of lenght $c$).

We notice that these two conditions are implicit in the Diophantine equation $a^n + b^n = c^n$. In fact, if either $a \geq c$ or $b \geq c$, the equation cannot be verified. Moreover, by means of the triangular inequality, we have $(a+b)^n \geq a^n + b^n = c^n$, which implies $a + b \geq c$.

Eventually, we observe that the request of equiprobability $P(\mathscr{E}_n^G) = P(\mathscr{L}_n^{AB})$, given the same $\alpha, \beta, \gamma$, can be written as $\left(\frac{\gamma}{c}\right)^n = 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n$, and also $0 = 1 - \left(\frac{a}{c}\right)^n - \left(\frac{b}{c}\right)^n$, which coincides with the the mentioned Diophantine equation. Therefore, since we have already shown that the equiprobability can be achieved only in case of $n = 1$ or $n = 2$, this result must apply also to the solutions of the Diophantine equation of the type $a^n + b^n = c^n$.

The cases $\alpha = 0$, $\beta = 0$ and $\alpha = \beta = 0$ are excluded because they imply the degenerate case of $C = \emptyset$.

# 5 Appendix

## 5.1 Expression of $P(\mathscr{L}_n^{AB})$

We define the event $\mathscr{L}_n^A$ as "to get, in $n$ independent trials, at least one element of kind $A$", and the event $\mathscr{L}_n^B$ as "to get, in $n$ independent trials, at least one element of kind $B$", so that $P(\mathscr{L}_n^A) = 1 - \left(\frac{c-\alpha}{c}\right)^n$ and $P(\mathscr{L}_n^B) = 1 - \left(\frac{c-\beta}{c}\right)^n$.

Eventually, we define the event $\mathscr{L}_n^{AB} \equiv \mathscr{L}_n^A \cap \mathscr{L}_n^B$ as "to get, in $n$ independent trials, at least one element of kind $A$ and at least one element of kind $B$". By means of Bayes' theorem and the concept of opposite event, we find

$$P(\mathscr{L}_n^{AB}) = P(\mathscr{L}_n^A \cap \mathscr{L}_n^B) = P(\mathscr{L}_n^A|\mathscr{L}_n^B)P(\mathscr{L}_n^B) = [1 - P(\overline{\mathscr{L}_n^A}|\mathscr{L}_n^B)]P(\mathscr{L}_n^B) =$$

$$= P(\mathscr{L}_n^B) - P(\mathscr{L}_n^B|\overline{\mathscr{L}_n^A})P(\overline{\mathscr{L}_n^A}) = 1 - \left(\frac{c-\beta}{c}\right)^n - \left[1 - \left(\frac{\gamma}{\beta+\gamma}\right)^n\right]\left(\frac{\beta+\gamma}{c}\right)^n =$$

$$= 1 - \left(\frac{\alpha+\gamma}{c}\right)^n - \left(\frac{\beta+\gamma}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n = 1 - \left(\frac{a}{c}\right)^n - \left(\frac{b}{c}\right)^n + \left(\frac{\gamma}{c}\right)^n,$$

where $a \equiv \alpha + \gamma = c - \beta$ and $b \equiv \beta + \gamma$.

## 5.2 Expressions of $P(\mathscr{E}_{n,k}^G)$ and $P(\mathscr{L}_{n,k}^{AB})$

Analyzing the tree diagram in Fig. 2 (related to $n = 3$ trials), we find that the probability to get a success for the event $\mathscr{E}_3^G$ is zero at any trial, except the last one, therefore $P(\mathscr{E}_{3,k}^G) = P(\mathscr{E}_3^G)\delta_{3,k} = \left(\frac{\gamma}{c}\right)^3 \delta_{3,k}$. The term $P(\mathscr{E}_{3,3}^G)$ corresponds to the height of the unique blue target represented in Fig. 1 (left graph). This result can be easily generalized to $P(\mathscr{E}_{n,k}^G) = P(\mathscr{E}_n^G)\delta_{n,k} = \left(\frac{\gamma}{c}\right)^n \delta_{n,k}$.

Similarly, by means of the tree diagram, we can compute the probabilities to verify the event $\mathscr{L}_3^{AB}$ in correspondence of $k \in \{1, 2, 3\}$:

$$P(\mathscr{L}_{3,1}^{AB}) = 0 = 1 - \left(\frac{\alpha+\gamma}{c}\right) - \left(\frac{\beta+\gamma}{c}\right) + \left(\frac{\gamma}{c}\right),$$

$$P(\mathscr{L}_{3,2}^{AB}) = 2\frac{\alpha\beta}{c^2} = 1 - \left(\frac{\alpha+\gamma}{c}\right)^2 - \left(\frac{\beta+\gamma}{c}\right)^2 + \left(\frac{\gamma}{c}\right)^2,$$

$$P(\mathscr{L}_{3,3}^{AB}) = 3\frac{\alpha^2\beta}{c^3} + 6\frac{\alpha\beta\gamma}{c^3} + 3\frac{\alpha\beta^2}{c^3} = 1 - \left(\frac{\alpha+\gamma}{c}\right)^3 - \left(\frac{\beta+\gamma}{c}\right)^3 + \left(\frac{\gamma}{c}\right)^3.$$

These values are obtained summing all the probabilities to select an ordered sequence of $k$ trials (highlighted with a green node on the $k$-th magenta circle

in Fig. 2) in which the event $\mathscr{L}_n^{AB}$ occurs. The sum is justified by the fact that these possible sequences are all mutually exclusive. The three terms correspond to the heights of the first three green targets illustrated in Fig. 1 (right graph). We can easily generalize this result to $P(\mathscr{L}_{n,k}^{AB}) = 1 - \left(\frac{a}{c}\right)^k - \left(\frac{b}{c}\right)^k + \left(\frac{\gamma}{c}\right)^k$.

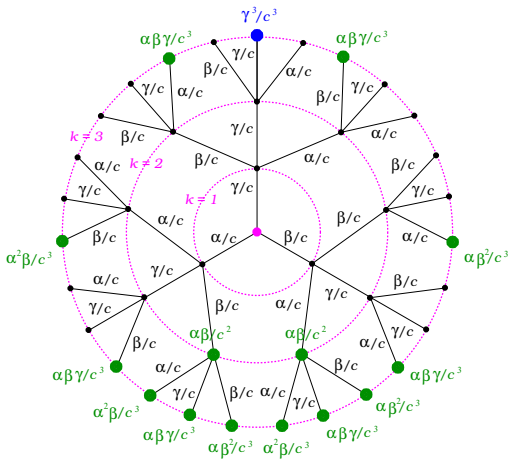


**Figure 2:** Tree diagram illustrating the distributions $P(\mathscr{E}_{3,k}^G)$ and $P(\mathscr{L}_{3,k}^{AB})$, with $k \in \{1, 2, 3\}$. The root-node (in magenta) is located at the center of the picture, and each trial is indicated with a dashed circle (in magenta). The probability to get a success for the event $\mathscr{E}_3^G$ is zero at any trial, except the third one (where the unique blue node is located). The sum of the probabilities in each green node related to each trial, gives the terms $P(\mathscr{L}_{3,1}^{AB}) = 0$ (no green nodes related to $k = 1$), $P(\mathscr{L}_{3,2}^{AB}) = 2\frac{\alpha\beta}{c^2}$ (2 green nodes related to $k = 2$), and $P(\mathscr{L}_{3,3}^{AB}) = 3\frac{\alpha^2\beta}{c^3} + 6\frac{\alpha\beta\gamma}{c^3} + 3\frac{\alpha\beta^2}{c^3}$ (12 green nodes related to $k = 3$).

## 5.3 Illustration of $P(\mathscr{L}_{n,k'}^{AB}|\mathscr{L}_{n,k}^{AB}) = 1$ for each $k' > k$

In the tree diagram of Fig. 2 we can also pinpoint the property $P(\mathscr{L}_{n,k'}^{AB}|\mathscr{L}_{n,k}^{AB}) = 1$ for each $k' > k$. Let focus on one of the two green nodes in correpondence of $k = 2$. These nodes represent the two different ways of extracting two elements (one at a time, with replacement) from the set $C$ yielding to a success for the event $\mathscr{L}_n^{AB}$ in correspondence of the second trial $k = 2$.

In the trials following one of these branches of the tree, the event $\mathscr{L}_n^{AB}$ has already been verified (no matter which kind of element would be extracted). Therefore, all the possible ways to extract elements from $C$ descending from these two branches will represent however a success for the event $\mathscr{L}_n^{AB}$ in the next trials, contributing to the probability $\mathscr{L}_{n,k'}^{AB}$ to get a success for the event $\mathscr{L}_n^{AB}$ in correspondence of the trial $k' > k$ (as illustrated by means of the six green nodes at the bottom of Fig. 2, in correspondence of $k = 3$).

This property is used to define the distribution $P(\mathscr{L}_{n,k}^{AB})$ as a strictly monotonically increasing function of $k$ (since $\alpha + \gamma < c$, $\beta + \gamma < c$ and $\alpha + \gamma > \gamma$, $\beta + \gamma > \gamma$) and to prove that $P(\mathscr{L}_{n,1}^{AB} \cup \mathscr{L}_{n,2}^{AB} \ldots \cup \mathscr{L}_{n,n}^{AB}) = P(\mathscr{L}_n^{AB})$.