The impossibility of quantum computing

Oscar Gras Garzón
Independent researcher

February 9, 2023

Abstract

This article analyzes the feasibility of implementing the mathematical model used in quantum computing systems. The article questions whether certain mathematical properties of the qubit can be physically implemented, highlighting that quantum theory may have been built by misinterpreting experimental evidence.

At the end of the article, it is justified mathematically that a feasible quantum-computing mathematical model is equivalent to a classical-computing mathematical model without states, so it can be concluded that quantum supremacy is unattainable.

Keywords

Quantum computing, quantum supremacy, computational complexity theory.

1 Introduction

Scientists have defined an alternative computing system to classical computing by making use of their quantum theory. The mathematical model on which quantum computing is based is believed to be possible because it takes advantage of the phenomena described by this theory.

Mathematicians have compared the ability to solve mathematical problems of the two models; that is, they have compared the mathematical model of classical computing with the mathematical model of quantum computing. To compare both models, they use a mathematical discipline called computational complexity theory, which studies how the number of operations performed increases by an algorithm as the data required to solve the problem increases. For example, adding a thousand numbers has lower computational complexity than sorting them because more operations are required to sort them. Computational complexity depends on the algorithm used to solve the problem and the algorithms, in turn, depend on the computational model. Thus, there may be a com-

putational model in which ordering a thousand numbers requires the same number of operations as those required to add them in the classical model.

Algorithms have been proposed to solve problems with the quantum computational model whose number of operations necessary to find the solution is much lower than those necessary with an algorithm that solves the same problem with the classical computational model. This suggests that there are problems that are not feasible to solve with the classical computing model, because they require too many operations, but are feasible to solve them with the quantum computing model. Because of this discovery, it is said that the organization that achieves quantum computing will achieve quantum supremacy.

However, it is not possible to implement the mathematical model of quantum computing with any physical system, so quantum supremacy is a chimera. Scientists believe in its feasibility because they have taken several erroneous assumptions from quantum theory. After a brief description of the mathematical model of quantum computation, I will describe these assumptions. Once described, I will modify the model described to avoid them, and I will show that the modified model is computationally equivalent to the classical computational model.

2 Quantum computing's mathematical model

The classical computing model has the bit as an elementary part, while the quantum computing model has the qubit. The bit can take only two values, 0 and 1, while the qubit can take infinite values. However, the reading of a qubit is a random phenomenon between two possible values, 0 and 1, where the probability of obtaining either of the two values depends on the value that the qubit has; moreover, after the reading, the value of the qubit is overwritten with the value obtained from the reading, losing the value it had before it. The two possible values of qubit reading are called primary values.

The possible qubit values are two-dimensional unit vectors whose components can take values from the complex space. In this article, the components of the unit vector will be restricted to values in real space. Since this model is more restricted, the justification for the impossibility of an implementation of the quantum mathematical model will apply to it as well, and it will be obvious to the reader how it applies to it.

Moreover, a description of the function that gives the probability distribution of the primary values according to the value of the qubit is not needed in this paper, since we only need to know two facts about it:

1. Each possible value of the qubit determines the probability distribution between the two primary values of the random phenomena.
2. Any probability distribution between the two primary values is reached with at least one two-dimensional vector value of the qubit with real-space components.

Although the value of the qubit is erased when it is read, it is possible to write in a qubit a value that depends on another qubit without erasing the qubit on which it depends. If we perform consecutive writes to the first qubit whose results depend on the second qubit, we will be able to determine the value stored in the second qubit with the desired precision. This is because the first qubit may have one primary value or another depending on whether any condition needed in the second qubit, to restrict the domain of possible values, is met or not.

The recent description of the definition of the qubit is sufficient to highlight the erroneous assumptions of the physical phenomena with which scientists hope to implement the promising quantum computing mathematical model. Briefly, the erroneous assumptions have to do with the random nature of the phenomenon and with the infinite number of values that the qubit can have.

3 Erroneous assumptions of physical reality

Any random phenomenon, by definition, has the following restrictions on its determination:

1. It is impossible to know the probability distribution of random phenomena.

   Let us imagine that a random event can result in only one of two possible values, for example, on or off; we will say that there is equiprobability between the two values if, in an infinite number of times of the repeating event, we have the same number of results of one value as of the other. However, since it is not possible to repeat the event an infinite number of times, we cannot perform the necessary procedure, according to the definition, to be certain that the event is equiprobable. Neither we can, according to the definition of a random phenomenon, know the probability distribution of these phenomena, with a finite subset of their outcomes, since that set of outcomes does not determine the rest of the outcomes; that is, even if we have a million outcomes of the phenomenon with the same value and none with the other, we cannot establish the frequency of those values in the rest of the outcomes of the random phenomenon. Admitting that one streak determines the subsequent ones implies admitting that the phenomenon is not really random, but pseudo-random.

   It is difficult for us to accept that a previous streak does not determine other subsequent streaks because our intuitive processes have been developed to find the determining rules followed by nature's interactions. If we try to give an answer to a problem about a random phenomenon, letting ourselves be guided by intuition instead of reasoning, the answer will likely be incorrect, as happens to us with the Monty Hall paradox.

2. It is impossible to be certain that a phenomenon is genuinely random rather than pseudo-random.

   We can demonstrate the existence of details in our reality, but not their non-existence, since the absence of observations of these details does not mean that they do not exist. Therefore, we cannot be sure that all interactions of natural phenomena follow rules that determine them, and we also cannot be sure that a phenomenon does not follow determining rules that we do not yet know. Free will is, by definition, a random phenomenon because the decisions made by the subject are determined by his will and can be made independently of the surrounding environment.

   If an event is not random and has been assumed to be random, its use in the implementation of computer systems can have dangerous implications for the security of the systems. If someone were to find partial rules that determine the outcome, they could find ways to take advantage of the error that everyone makes in assuming that the event is random. Proof of the existence of this possibility are the experiences we have in classical computing with erroneous assumptions of randomness. A multitude of security vulnerabilities in computer systems have been revealed as a result of these erroneous assumptions. The following case is a good example of this error:

   Intel suffered this embarrassment when researchers found that its processors were not secure. Processors have an internal memory, called a cache, which they have much faster access than the access they have to the computer's RAM. The cache, thanks to algorithms, stores copies of the most frequently accessed information in RAM memory; in this way, the most frequently used information is retrieved more quickly than it would be if the cache did not exist. By assuming users don't know what information has been accessed previously, processor designers considered the memory read response time to be random. However, researchers found that, by measuring memory response times, they could tell whether the access had been to the cache or not. With this information, they could propose reads to a memory address that partially depended on the value stored at another address, and, depending on how fast they got the response, the stored value was partially revealed. This forced Intel to redesign its new processors and forced some of Intel's customers, who didn't like to be at risk of being attacked by using this vulnerability, to throw away their machines.

   A rule that is only true in random phenomena and that we assume when we suppose that the phenomenon is random is that the concatenation of two phenomena is a random phenomenon, even if we can determine one of them.

3. It is impossible to modify the probability distribution of a random phenomenon.

   Precisely, to be able to modify the probabilities of the results of a phenomenon, we need to interact with it. If we can determine the results of this interaction,

it is because we know a rule that determines these results. As the probability distribution of a random phenomenon cannot be known, it is even less possible to modify its probability distribution because a random phenomenon cannot be affected by its environment. To postulate that there are rules that serve to modify the probability distribution of a random phenomenon makes no sense because there is no intermediate point between random and determined phenomenon; either the phenomenon is deterministic or it is not; a factor that partially determines the non-determinism of a phenomenon sounds contradictory.

We have many millions of pseudo-random phenomena so, if it turned out that the value read from the qubit was not random, all the work that has been done to develop quantum computation would have been useless; unless the motivations for the development quantum computing systems were not in the existence of random phenomena.

On the other hand, if the mathematical model of quantum computing enables us to compute far superior to the present one, we should try to implement it with pseudo-random systems. After all, if such a mathematical model were only possible with genuinely random systems, it would mean that there is a mathematical procedure to distinguish between genuinely random and pseudo-random procedures. Believing in the existence of a mathematical procedure that can only be performed with genuinely random phenomena implies the belief that there are characteristics of reality that can be determined without being observed by using mathematics. To implement the mathematical model of quantum computation there are infinite pseudo-random systems that we can use as a substitute for qubits, so we do not have to wait to achieve quantum computation with quantum phenomena.

Having described the erroneous assumptions about the random nature of quantum physics, I will now describe those that have to do with its capacity to store information.

1. The incommensurability of the qubit.

   The qubit capability to store any value of an infinite number of them is its greatest advantage over the bit. In fact, we would need an infinite number of bits to store the stored value in the qubit. Therefore, the information that a qubit can store is unmanageable for a binary system; we could digitize all the books and images in the world; concatenate all the digitization files to form a single string of zeros and ones; transform that very long string of zeros and ones into a gigantic integer; and then store it in a single qubit. Once stored, we could retrieve the stored information, using an auxiliary qubit, through repeating writes operations, conditioned by this gigantic integer, resulting in1,if the gigantic integer meets a condition, or 0, if it does not. As the auxiliary qubit can be read, each new write will bring us closer to the value to be retrieved, since the new conditions can be chosen according to that read.

If the reader begins to think that the capability of the qubit sounds fanciful, it is precisely because our intuition finds it implausible, anything comparable in our experience cannot be found. If the reader needs some more help, imagine that you want to store in a single qubit the boolean representation of an irrational number, which is an infinite string of boolean digits; you would be storing in a single qubit the information of something that is completely impossible to obtain because it takes infinite time; how could we write in the qubit something that is impossible to obtain?

2. The impossibility of obtaining exactly what is desired.

   We have arrived at the absurdity of the incommensurability of the qubit because we have assumed that we can write in the qubit any desired value exactly. If this were really the case, we would be facing a milestone in technology, there isn't any precedent of such capability in any other technology; for example, we can imagine a perfect circle, but no one can draw it. To this milestone's promise in quantum technology, we must add that the chosen value is used to establish the probability distribution of a random phenomenon; so, it is not only assumed that we can modify it with perfect precision, but that we will achieve this modification on a non-deterministic phenomenon.

   Once it is accepted that we cannot write with perfect precision the desired value in a qubit, we need to consider that the value written could be any one unknown inside a finite interval. If we want a coincidence between what we write and what we later recover, we must divide the range of values that a qubit can store into a finite number of non overlapping intervals; each of them maps to one and only one value to avoid ambiguity. Since the number of intervals is finite, the values that can be stored in the qubit will be any of a finite number of possible values.

   Physically, qubits store unitary two-dimensional vectors, so we each vector in the set of possible values represent a value of the finite domain set of the operands in the algorithm. Even with the vector's components in the complex space, the number of possible vectors that can be stored in the qubit is finite.

4 Non-existence of quantum supremacy technology

With a commensurable qubit, we can conclude that computation, using this restricted quantum model, is computationally equivalent to classical computation. I will demonstrate this claim in this section.

Having the set of possible values stored in a qubit, we can define a set of boolean digit strings, each one with the same number of digits, that meets the following condition: the number of strings of the defined set equals the number of possible values stored in a qubit. With this defined set, we can define a bijective function between the two sets, where each element in one set will have its element in the other set assigned to it and

vice versa. This bijection allows us to represent any value of the qubit in a binary system with a finite number of bits. In this binary system, the number of bits needed for each quantum-system's qubit is the logarithm in base two of the number of elements in the set of possible values of the qubit rounded to the closet greater integer.

When the quantum computing system performs an elementary operation, both the arguments and the results of the operation must be stored in qubits. Since the system has finite number of qubits; the number of elements of the set of all possible arguments' values is finite, as well as the number of elements of the set of all possible results' values. Furthermore, to represent an elementary operation, a surjective function can be drawn between the two sets, the arguments' values set and the results' values set; since a useful computation meets that results must be determined by the operation's arguments, unless a random number is needed. This surjective function is transferable to the classical computation model, since there is a bijective function to maps quantum values to classical values. Classical computing can implement any surjective function, and quantum random values can be substituted by a result from a classical algorithm of psedorandom numbers.

Algorithms are successions or concatenations of elementary operations, and elementary operations are surjections between the set of possible values of the arguments and the set of possible values of the results. If the elementary operations of quantum computation are transferable to classical computation, the algorithms will also be transferable, concluding that both models are computationally equivalent. Since classical and quantum computing are equivalent, quantum supremacy is a chimera.

5 Conclusion

The above demonstration was made without using any fact of physical phenomenons, the reasoning questions the certainty of the assumptions made in the mathematical model and the feasibility of a technology that meets those assumptions. Thus, quantum supremacy will not be achieved even by discovering new phenomena in which the technology is based to implement the model.

The reasons that have led us to make these erroneous assumptions are outside the scope of this short article. Briefly, the current scientific method is wrong and needs to be replaced by a new one that I am describing in a new book I am writing. Many current theories will not meet this method's requisites. My motivation to write this article is to reveal the wrongness of the current scientific method.

I understand the necessity of the scientific community to ignore the facts stated in this article due to these facts drive them to doubt the current knowledge they have. An appendix attached to this paper discusses the current scientific method.

Appendix: Fundaments of the current scientific method

In the current scientific method, there are two types of reasoning:

- Deduction.
- Inference.

The deduction is a type of reasoning that parts from a general statement and concludes on a specific one. This type of reasoning can be made using logic and if the starting statement is true, then we can be sure that the specific statement is also true. Deduction always needs a statement to start, which is named premise.

Inference is a type of reasoning that goes in the reverse way, parts from a specific statement and concludes on a general one. This type of reasoning cannot be made using logic and even if the starting statement is true, the conclusion could be false because multiple general statements can be the result of this type of reasoning.

It is effortless to find an example of two general statements that conclude, using logic, in the same specific statement. For example, the following two general statements: the set of all even numbers greater than zero, and the set of all prime numbers, can be used two prove through logic that 2 is the first element of the set when the elements are ordered from least to greatest.

We name a hypothesis to a conclusion of an inference reasoning because there isn't a unique inference reasoning that can be made from a specific statement. Hypotheses are needed because general statements are impossible to check with observations or experiments. If a general statement is a rule, each observation or experiment can only check for a specific set of conditions of that rule, to check another set of conditions we require another observation or experiment. As one rule may have an infinite number of sets of conditions, an infinite number of observations or experiments are needed to check it.

If two scientists propose two different hypotheses, we can try to find two specific different statements that meet the following:

- Each of the two follows from only one of the two hypotheses, and both statements follows from a different hypothesis.
- Both statements cannot be true at the same time.
- Each one can be verified with one observation or one experiment.

If each statement has been deduced with a different hypothesis, the one that is false will serve to demonstrate the falsity of its hypothesis.

There are currently theories that include statements that are not observable or able to be checked by experiments. These theories are the ones where scientific objectivity is questionable, since these aspects of the theory are not testable. The hypotheses of these

theories are proposed based on the principle of parsimony, which means that the simplest explanation is chosen based on the observed evidence.

The use of the principle of parsimony expands the area of knowledge treatable by science. Immanuel Kant knew how to separate human knowledge into two categories: the observable and the non-observable. The first category would correspond to scientific knowledge properly meant, and the second category for transcendental knowledge properly meant, that is, the existence of God and the ultimate purpose of our existence. By accepting the principle of parsimony, the categorical separation disappears, and science begins to discuss issues in which our certainty is drastically reduced.

Schrödinger's equation was inferred from the spectroscopy lines observed in different atoms. Its interpretation was difficult to accept even for Erwin Schrödinger, who is also the author of a thought experiment known as Schrödinger's cat. His intention with his experiment's proposition is to reflect an absurd conclusion that follows from accepting his equation's interpretation. Despite the absurd conclusion, today the scientific community believes in facts from the inferred reasoning that justify Schrödinger's equation, even though these facts are not observable.

The mathematical properties of the qubit are deduced from Schrödinger's equation and its interpretation, that is, the randomness phenomena's determination and the superposition's states of the qubit are predicted with the interpretation of Schrödinger's equation.

Quantum computing is an attempt to get a technical application of the interpretation of Schrödinger's equation. As is shown in the article, the uncertainty of the facts in a hypothesis will keep on its applications, unless the facts are observable.