Why Majority Rule Does Not Work in Quantum Computing: A Pedagogical Explanation

Oscar Galindo[1], Olga Kosheleva[2], and Vladik Kreinovich[1]
[1]Department of Computer Science
[2]Department of Teacher Education
University of Texas at El Paso
500 W. University
El Paso, TX 79968, USA
ogilndomo@miners.utep.edu, olgak@utep.edu, vladik@utep.edu

Abstract

To increase the reliability of computations result, a natural idea is to use duplication: we let several computers independently perform the same computations, and then, if their results differ, we select the majority's result. Reliability is an important issue for quantum computing as well, since in quantum physics, all the processes are probabilistic, so there is always a probability that the result will be wrong. It thus seems natural to use the same majority rule for quantum computing as well. However, it is known that for general quantum computing, this scheme does not work. In this paper, we provide a simplified explanation of this impossibility.

1 Need for Increasing Reliability of Quantum Computing Results

Quantum computing: a brief introduction. In spite of the tremendous computational speed of modern computers, for many important practical problems, it is still not possible to solve them in reasonable time. For example, in principle, we can use computer simulations to find which biochemical compound can block a virus, but even on the existing high-performance computers, this would take thousands of years.

It is therefore desirable to design faster computers. One of the main obstacles to this design is the speed of light: according to relativity theory, no physical process can be faster than a speed of light, and on a usual 30-cm-size laptop, light takes 1 nanosecond to go from one side to another – the time during which even the cheapest laptop can perform four operations. Thus, the only way to speed up computations is to further shrink computers – and therefore, to shrink their elements.

Already an element of the computer consists of a few hundred or thousand molecules, so if we shrink it even more, we will get to the level of individual molecules, the level at which we need to take into account quantum physics – the physics of the micro-world.

Computations on this level are known as *quantum computing.*

Quantum computing: challenges and successes. One of the main features of quantum physics is that:

- in contrast to Newtonian mechanics, where we can, e.g., predict the motions of celestial bodies hundreds of years ahead,
- in quantum physics, only probabilistic predictions are possible.

This is a major challenge for quantum computing; see, e.g., [1, 3].

In spite of this challenge, several algorithms were invented that produce the results with probability close to 1 – and even produce them much faster than all known non-quantum algorithms; see, e.g., [2]. For example:

- Grover's quantum algorithm can find an element in an unsorted n-element array in time proportional to $\sqrt{n}$, while
- the fastest possible non-quantum algorithm needs to look, in the worst case, at all n elements, and thus, requires n computational steps.

An even more impressive speed-up occurs with Shor's algorithm for factoring large numbers:

- this algorithm requires time bounded by a polynomial of the number's length, while
- all known non-quantum algorithms requires exponential time.

This is very important since most existing computer security techniques are based on the difficulty of factoring large numbers.

Still, reliability is a problem for quantum computing. In the ideal case, when all quantum operations are performed exactly, we get correct results with probability practically indistinguishable from 1. In reality, however, operations can only be implemented with some accuracy, as a result of which the probability of an incorrect answer becomes non-negligible.

How can we increase the reliability of quantum computations?

2 Majority Rule – A Usual Way to Increase Reliability of Non-Quantum Computations

Duplication: a natural idea. If there is a probability that a pen will not work when needed, a natural idea is to carry two pens. If there is a probability that a computer on board of a spacecraft will malfunction, a natural idea is to have two computers. If there is a probability that a hardware problem will cause data to be lost, a natural idea is to have a backup – or, better yet, two (or more) backups, to make the probability of losing the data truly negligible.

Similarly, for usual (non-quantum) algorithms, a natural way to increase their reliability is to have several computers performing the same computations. Then, if the results are different, we select the result of the majority – this way, we increase the probability of having a correct result.

Indeed, suppose, e.g., that we use three computers independently working in parallel, and for each of then, the probability of malfunctioning is some small (but not negligible) value p. Then, since the computers are independent, the probability that all three of them malfunction is equal to p^3, and for each two of them, the probability that these two malfunction and the remaining one perform correctly is equal to $p^2 \cdot (1-p)$. There are three possible pairs, so the overall probability that this majority scheme will produce a wrong result is equal to $3p^2 \cdot (1-p) + p^3$, which for small p is much much smaller than the probability p that a single computer will malfunction.

In principle, we can use the same idea for quantum computing. Nothing prevents us from having three independent quantum computers working in parallel: this will similarly decrease the probability of malfunctioning and thus, increase the reliability of the corresponding computations.

But what if the desired computation result is quantum? The majority rule works when the desired result is non-quantum, as in the above-mentioned quantum algorithms. Sometimes, however, the desired result is itself quantum – e.g., in quantum cryptography algorithms; see, e.g., [2]. Will a similar idea work?

What we do in this paper. It is known that for computations with purely quantum results, the majority rule does not work. The usual arguments why it does not work refer to rather complex results.

In this paper, we provide a simple pedagogical explanation for this fact – OK, as simple as it is possible when we talk about quantum computing.

Comment. To provide our explanation, we need to remind the readers the main specifics of quantum physics and quantum computing.

3 Specifics of Quantum Physics and Quantum Computing: A Brief Reminder

Quantum states. One of the specifics of quantum physics is that, in addition to non-quantum states $s_1, \ldots, s_n$, we can also have *superpositions* of these states, i.e., states of the type $a_1 \cdot s_1 + \ldots + a_n \cdot s_n$, where a_i are complex numbers for which $|a_1|^2 + \ldots + |a_n|^2 = 1$; see, e.g., [1, 3].

If some physical quantity has value v_i on each state s_i, then, if we measure this quantity in the superposition state, we get each value v_i with probability $|a_i|^2$. These probabilities have to add to 1 – which explains the above constraint on possible values of a_i.

In particular, for a 1-bit system, in addition to the usual states 0 and 1 – which in quantum physics are usually denoted by $|0\rangle$ and $|1\rangle$ – we can also have superpositions $a_0|0\rangle + a_1|1\rangle$, with $|a_0|^2 + |a_1|^2 = 1$.

Similarly, for 2-bit systems, which in non-quantum case can be in four possible states: 00, 01, 10, and 11 – in the quantum case, we can have general superpositions

$$a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle,$$

where

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1.$$

Transitions between quantum states. One of the specifics of quantum physics is that all the transitions preserve superpositions: if the original state s has the form $a_1 \cdot s_1 + \ldots + a_n \cdot s_n$, and then each s_i is transformed into some state s'_i, then the state s gets transformed into a similar superposition $a_1 \cdot s'_1 + \ldots + a_n \cdot s'_n$.

In other words, transformations are *linear* in terms of the coefficients a_i.

States of several independent particles. Linearity applies also to describing the joint state of several independent particles.

For example, for two 1-bit systems, if the first system is in the state $|0\rangle$ and the second in the state $|0\rangle$, then the 2-bit system is in the state $|00\rangle$.

Similarly, if the first system is in the state $|1\rangle$ and the second system is in the state $|0\rangle$, then the 2-bit system is in the state $|10\rangle$.

Thus, if the first system is in the superposition state $a_0|0\rangle + a_1|1\rangle$ and the second is in the state $|0\rangle$, then the joint state of these two 1-bit systems is the corresponding superposition of the states $|00\rangle$ and $|10\rangle$, i.e., the state

$$a_0|00\rangle + a_1|10\rangle.$$

Similarly, if the first system is in the state $a_0|0\rangle + a_1|1\rangle$ and the second system is in the state $|1\rangle$, then the joint state of these two 1-bit system is the corresponding superposition of the states $|01\rangle$ and $|11\rangle$, i.e., the state

$$a_0|01\rangle + a_1|11\rangle.$$

What if the second system is also in the superposition state $b_0|0\rangle + b_1|1\rangle$? The resulting joint state is the similar superposition of the $a_0|00\rangle + a_1|10\rangle$ and $a_0|01\rangle + a_1|11\rangle$, i.e., the state

$$b_0 \cdot (a_0|00\rangle + a_1|10\rangle) + b_1 \cdot (a_0|01\rangle + a_1|11\rangle).$$

If we open parentheses, we get the state

$$(a_0 \cdot b_0)|00\rangle + (a_0 \cdot b_1)|01\rangle + (a_1 \cdot b_0)|10\rangle + (a_1 \cdot b_1)|11\rangle.$$

This state is called the *tensor product* of the original states $a_0|0\rangle + a_1|1\rangle$ and $b_0|0\rangle + b_1|1\rangle$; it is usually denoted by

$$(a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle).$$

What we will do. Let us use these specifics to explain why the majority rule cannot work for quantum computing when the result of the computation is a general quantum state – i.e., a general superposition.

4 Why the Majority Rule Does Not Work: Our Explanation

What would a majority rule mean. Suppose that we have three different systems in states s_1, s_2, and s_3. Based on these three states, we want to come up with the state in which, if two of three original states coincide, the resulting state of the first system will be equal to this coinciding state.

Examples. If we consider three 1-bit systems, then, e.g., the original joint state $|001\rangle$ should convert into a state $|0\ldots\rangle$ in which the first 1-bit system is in the 0 state. Similarly:

- the original states $|000\rangle$, $|010\rangle$, and $|100\rangle$ should convert into states of the type $|0\ldots\rangle$, and
- the original states $|111\rangle$, $|011\rangle$, $|101\rangle$, and $|110\rangle$ should convert into states of the type $|1\ldots\rangle$.

Similarly, if the first two systems are originally both in the same state

$$c|0\rangle + c|1\rangle,$$

where $c \stackrel{\text{def}}{=} \dfrac{1}{\sqrt{2}}$, and the third system is originally in the state $|1\rangle$, then the resulting state of the first system should be $c|0\rangle + c|1\rangle$.

In this case, if we measure the resulting state of the first system, we will get both 0 and 1 with the same probability $|c|^2 = \dfrac{1}{2}$.

Let us show why all this is impossible. In the last example, the joint state of the three systems is equal to

$$(c|0\rangle + c|1\rangle) \otimes (c|0\rangle + c|1\rangle) \otimes |1\rangle =$$

$$\frac{1}{2}|001\rangle + \frac{1}{2}|011\rangle + \frac{1}{2}|101\rangle + \frac{1}{2}|111\rangle.$$

We know that the state $|001\rangle$ gets converted into a state $|0\ldots\rangle$, and each of the states $|011\rangle$, $|101\rangle$, and $|111\rangle$ gets converted into a state of the type $|1\ldots\rangle$.

Thus, due to linearity, the original state gets transformed into a new state

$$\frac{1}{2}|0\ldots\rangle + \frac{1}{2}|1\ldots\rangle + \frac{1}{2}|1\ldots\rangle + \frac{1}{2}|1\ldots\rangle.$$

So, in the resulting state, the probability that after measuring the first bit, we get 0 is equal to

$$\left|\frac{1}{2}\right|^2 = \frac{1}{4},$$

but, as we have mentioned earlier, the majority rule requires that this probability be equal to $\frac{1}{2}$.

Thus, the majority rule cannot be implemented for quantum states.

Discussion. We showed that we cannot have majority rule for *all* possible quantum states, but maybe we can have it for *some* quantum states? A simple modification of the above argument shows that it is not possible.

Indeed, suppose that the majority rule is possible for some quantum state $a_0|0\rangle + a_1|1\rangle$, where $a_0 \neq 0$, $a_1 \neq 0$, and $|a_0|^2 + |a_1|^2 = 1$. Then, if two systems are in this state and the third 1-bit system is in the state $|1\rangle$, the majority rule would mean that in the resulting state, the first system will be in the same state $a_0|0\rangle + a_1|1\rangle$. Thus, the probability that measurement will find the first system in the state 0 is equal to $|a_0|^2$.

On the other hand, here, the original joint state of the three systems has the form

$$(a_0|0\rangle + a_1|1\rangle) \otimes (a_0|0\rangle + a_1|1\rangle) \otimes |1\rangle =$$

$$a_0^2|001\rangle + (a_0 \cdot a_1)|011\rangle + (a_0 \cdot a_1)|101\rangle + a_1^2|111\rangle.$$

Thus, this state gets transformed into

$$a_0^2|0\ldots\rangle + (a_0 \cdot a_1)|1\ldots\rangle + (a_0 \cdot a_1)|1\ldots\rangle + a_1^2|1\ldots\rangle.$$

For this state, the probability that the measurement will find the first system in the state 0 is equal to $\left|a_0^2\right|^2 = |a_0|^4$.

The only case when these two values coincide, i.e., when $|a_0|^2 = |a_0|^4$, is when $|a_0|^2 = 0$ or $|a_0|^2 = 1$.

- In the first case, we have $a_0 = 0$ but we assumed that $a_0 \neq 0$.
- In the second case, due to the general constraint $|a_0|^2 + |a_1|^2 = 1$, we have $|a_1|^2 = 1 - |a_0|^2 = 0$, hence $a_1 = 0$, but we assumed that $a_1 \neq 0$.

So, the majority rule is not possible for *any* properly quantum state – i.e., for any quantum state which is different from the original non-quantum states 0 and 1.

Acknowledgments

This work was supported in part by the US National Science Foundation grants 1623190 (A Model of Change for Preparing a New Generation for Professional Practice in Computer Science) and HRD-1242122 (Cyber-ShARE Center of Excellence).

References

[1] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics*, Addison Wesley, Boston, Massachusetts, 2005.

[2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, U.K., 2000.

[3] K. S. Thorne and R. D. Blandford, *Modern Classical Physics: Optics, Fluids, Plasmas, Elasticity, Relativity, and Statistical Physics*, Princeton University Press, Princeton, New Jersey, 2017.