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

1. Quantum Computing: A Brief Introduction

- Modern computers are very fast.
- However, for many important practical problems, it is still not possible to solve them in reasonable time.
- E.g., in principle, we can use computer simulations to find which biochemical compound can block a virus.
- However, 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.
- On a usual 30-cm-size laptop, light takes 1 nanosecond to go from one side to another.

2. Quantum Computing (cont-d)

- During this time even the cheapest laptop can perform four operations.
- Thus, the only way to speed up computations is to further shrink computers.
- Thus, 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.
- At this level, we need to take into account quantum physics – the physics of the micro-world.
- Computations on this level are known as *quantum computing*.

3. Quantum Computing: Challenges and Successes

- In Newton's mechanics, we can, e.g., predict the motions of celestial bodies hundreds of years ahead.
- In contrast, in quantum physics, only probabilistic predictions are possible.
- This is a major challenge for quantum computing.
- However, several algorithms were invented that produce the results with probability close to 1.
- Some even produce them much faster than all known non-quantum algorithms
- Grover's quantum algorithm can find an element in an unsorted n-element array in time proportional to $\sqrt{n}$.
- The fastest possible non-quantum algorithm needs to look, in the worst case, at all n elements.

4. Quantum Computing: Successes (cont-d)

- Thus, it requires, in the worst case, 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.
- However, 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.

5. Still, Reliability Is a Problem for Quantum Computing

- In the ideal case, all quantum operations are performed exactly.
- Then, we get correct results with probability practically indistinguishable from 1.
- In reality, however, operations can only be implemented with some accuracy.
- As a result, the probability of an incorrect answer becomes non-negligible.
- How can we increase the reliability of quantum computations?

6. Duplication: A Natural Idea

- There is a probability that a pen will not work when needed, so a natural idea is to carry two pens.
- There is a probability that a computer on board of a spacecraft will malfunction.
- So, 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.
- Better yet, have 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.

7. Duplication (cont-d)

- 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.
- For each of then, the probability of malfunctioning is some small (but not negligible) value p.
- Since the computers are independent, the probability that all three of them malfunction is equal to p^3.
- For each pair, the probability that these two malfunction and the remaining one perform correctly is:

$$p^2 \cdot (1 - p).$$

8. Duplication (cont-d)

- There are three possible pairs.
- So the overall probability that this majority scheme will produce a wrong result is equal to $3p^2 \cdot (1-p) + p^3$.
- For small p, this is much much smaller than the probability p that a single computer will malfunction.

9. What About Quantum Computing?

- Nothing prevents us from having three independent quantum computers working in parallel.
- This will similarly decrease the probability of malfunctioning.
- Sometimes, however, the desired result is itself quantum – e.g., in quantum cryptography algorithms.
- 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, only as simple as it is possible when we talk about quantum computing.

10. Quantum States

- Let us recall the main specifics of quantum physics and quantum computing.
- 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 $a_1 \cdot s_1 + \ldots + a_n \cdot s_n$.
- Here, a_i are complex numbers s.t. $|a_1|^2 + \ldots + |a_n|^2 = 1$.
- If some physical quantity has value v_i on each state s_i:
  - then, when 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; this explains the constraint on a_i.

11. Quantum States (cont-d)

- 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 $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$;
  - here, $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.

12. 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.

13. 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 $|10\rangle$.

14. Independent Particles (cont-d)

- 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 similar superposition of $|00\rangle$ and $|10\rangle$:

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

- 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 superposition $|01\rangle$ and $|11\rangle$:

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

15. Independent Particles (cont-d)

- 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 states $a_0|0\rangle + a_1|1\rangle$ and $b_0|0\rangle + b_1|1\rangle$; it is denoted by:

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

- Let us use these specifics to explain why the majority rule cannot work for quantum computing.

16. 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.
- Let us consider three 1-bit systems.
- Then, the original joint state $|001\rangle$ should convert into a state $|0\ldots\rangle$: the first 1-bit system is in the 0 state.
- The original states $|000\rangle$, $|010\rangle$, and $|100\rangle$ should convert into states of the type $|0\ldots\rangle$.
- The original states $|111\rangle$, $|011\rangle$, $|101\rangle$, and $|110\rangle$ should convert into states of the type $|1\ldots\rangle$.

17. Majority Rule (cont-d)

- 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

$$|c|^2 = \frac{1}{2}.$$

18. Let Us Show Why All This Is Impossible

- In the last example, the joint state of 3 systems is:

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

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

- 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

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

19. Majority Rule Is Impossible (cont-d)

- We get the state

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

- In this state, the probability that after measuring the first bit, we get 0 is $\left|\frac{1}{2}\right|^2 = \frac{1}{4}$.
- However, 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.

20. Discussion

- We showed that we cannot have majority rule for *all* possible quantum states.
- 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:

$$a_0 \neq 0, \quad a_1 \neq 0, \text{ and } |a_0|^2 + |a_1|^2 = 1.$$

- If two systems are in this state and the third is in the state $|1\rangle$, the majority rule means that:
  - in the resulting state,
  - the first system will be in the same state

$$a_0|0\rangle + a_1|1\rangle.$$

21. Discussion (cont-d)

- 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 $|a_0|^2 = 1$.

22. Discussion (cont-d)

- We have either $|a_0|^2 = 0$ or $|a_0|^2 = 1$.
- In the 1st case, we have $a_0 = 0$ but we assumed $a_0 \neq 0$.
- In the second case, due to $|a_0|^2 + |a_1|^2 = 1$, we have $|a_1|^2 = 1 - |a_0|^2 = 0$, hence $a_1 = 0$.
- However, 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.

23. Acknowledgments

This work was supported in part by the following US National Science Foundation grants:

- 1623190 (A Model of Change for Preparing a New Generation for Professional Practice in Computer Science);
- HRD-1242122 (Cyber-ShARE Center of Excellence).