Quantum Computing, Here We Come!

Vladik Kreinovich

Department of Computer Science
University of Texas at El Paso
El Paso, TX 79968, USA
vladik@utep.edu
http://www.cs.utep.edu/vladik

1. Faster, Faster, Faster: Why?

- Computers are getting faster.
- On the cheapest laptop, we can now solve problem that decades ago, required a supercomputer.
- For customers, this means faster downloads, more detailed video games.
- But seriously, why do we need faster computers?

2. Why Faster

- Why do we need faster computers?
- Because for many practical problems, the current speed is not enough.
- For example, we can usually predict tomorrow's weather reasonably well.
- The corresponding computations may take hours on a high performance computer.
- However, the results are still available way before tomorrow.
- In principle, similar algorithms can also predict where a tornado will go in the next 10 minutes.
- However, in this case, we cannot wait hours.

3. Blame It on Einstein's Special Relativity

- In the past, computer speed doubled every 1-2 years: Moore's law.
- But now, this speeding-up slowed down.
- Why?
- One of the main reasons is special relativity.
- According to special relativity, all velocities are bounded by the speed of light.
- Light travels very fast, at 300,000 km/sec.
- This means that to go through a laptop of usual size 30 cm, a signal needs at least 10^{-9} seconds.
- This may sound fast, but modern computers have several GHz speed.
- This means that several operations can be performed while we reach a computer cell.

4. Honey, I Shrunk the Computer

- So, the only way to make computers faster is to make them smaller in size.
- This means decreasing the size of each memory and processing cell.
- Here comes a problem.
- Already now, on fastest computers, a cell consists of several dozen molecules.
- When we shrink it even further, it will consist of a few molecules.
- As a result, we will have to take into account quantum physics – physics of micro-objects like molecules.

5. Why Is Micro-World Different?

- But why is micro-world different?
- We can simply say that this is what physics experiments show.
- But in reality, there is a good reason for this difference.
- How do we describe the state of a macro-object – e.g., of a car?
- We can describe its location, its velocity, how much gas is left, etc.
- In principle, all these values can be measured very accurately.
- A police officer shoots a beam of photons to the car, and she gets the car's speed.

6. Why Is Micro-World Different (cont-d)

- We can (and do) shoot a laster beam to the Moon.
- It bounces back and we can find the exact distance to the Moon.
- In both cases, the beam is much much smaller than the object; thus, the beam does not affect the object.
- The car does not change its direction just because its speed is measured (unless a driver breaks :-)
- The Moon does not change its trajectory because we shot a laser beam at it.
- Thus, at any given moment of time, we can get an exact description of the state.
- Thus, we can accurately predict future behavior.
- For example, we can predict Lunar eclipses centuries ahead.

7. Micro-World Is Different

- It is different for micro-objects.
- To find a location of an electron, we can also shoot a photon at it.
- But now the photon is about the same size as the electron.
- As a result, each measurement drastically changes the state of the object.
- Once we measured the location, the velocity changes, and vice versa.
- As a result, we cannot determine the exact state – and thus, cannot make exact predictions.
- At best, we can predict the probability of different future states.

8. At First Glance, This Is Bad for Computing

- Computers are very precise machines.
- Humans make mistakes, computers usually don't.
- A computer can perform billions of operations – and still get a correct result.
- If we repeat the computations twice, we get the exact same result.
- But this assumes that everything works deterministically.

9. Bad for Computing?

- If we decrease the size of computer cells to a few molecules, we need to account for quantum effects.
- This means that the outcome becomes probabilistic.
- We run the same program twice, and get two different results – a disaster.
- A disaster?

10. Making Lemonade Out of Lemons

- For a long time, quantum effects on computing were viewed as distracting noise.
- Indeed, if we run the existing algorithms on a quantum-size computer, the results will drown in noise.
- What can we do?
- The previous phrase has a hint: *existing* algorithms.
- It turns out that we can modify algorithms so that:
  - not only we are affected by noise,
  - we can even further speed up computations!

11. Fast Search

- In action movies, an enemy is often hiding in one of the main rooms, we do not know in which one.
- If there are n rooms, then the only way to find the bad guy is to look into all the rooms until we find him.
- In the worst case, we need to look into all the rooms – if we do not search all the rooms, we may miss him.
- Similarly:
  - if we have an unsorted database with n records,
  - in the worst case, we need to look at all n records.
- In quantum computing, Grover's algorithm can find an element in $\sqrt{n}$ steps.
- How faster is it?

12. Fast Search (cont-d)

- If a database has a million records, we need 1,000 steps instead of 1,000,000: 1,000 times faster.
- How can we achieve such a drastic speed-up?
- As we mentioned, in quantum physics, states are blurred.
- So, instead of sending a signal to a single cell, we send a blurred signal, that can reach several cells at a time.
- Interestingly, the corresponding mathematics is about complex numbers, i.e., numbers $a+b\cdot\mathrm{i}$, where $\mathrm{i}=\sqrt{-1}$.
- A general state of a quantum bit is not 0 or 1, but $c_0\cdot|0\rangle+c_1\cdot|1\rangle$ for complex c_i for which $|c_0|^2+|c_1|^2=1$.

13. End of Privacy, End of Secrecy?

- An even more spectacular speed up is Shor's algorithm for factoring integers.
- A natural question is: who cares (other than elementary school teachers)?
- Well, it is more serious that it sounds.
- Factoring a reasonably small number is easy: you give a kid $n = 35$, the kid will factor it into $5 \cdot 7$.
- Worst comes to worst, this can be done by trying all prime numbers p smaller than n.
- (Actually, it is enough to check all $p \leq \sqrt{n}$).
- But this does not work for 200-digit numbers.
- For such numbers, trying all $p \leq \sqrt{n}$ would require trying 10^{100} numbers.

14. End of Privacy (cont-d)

- Trying 10^{100} numbers will take longer than the lifetime of the Universe.
- People tried, but so far, there is no efficient algorithm for factoring large numbers.
- The difficulty of factoring large integers is the main idea behind modern encryptions like RSA algorithm.
- This algorithm is what is used when we buy stuff on the web.
- Amazon.com finds two large prime numbers c_1 and c_2, keeps them secret and publicly releases their product c.
- Then http changes to https (s for secure).
- Then, credit card numbers and other information are encrypted by using the public code c.
- To decrypt, we need to know the secret value c_1.

15. End of Privacy (cont-d)

- So far, it works – no classical algorithm can decode without knowing c_1.
- No classical algorithm – because Shor's quantum algorithm does exactly this.
- This is one of the main reasons why governments invest millions in quantum computing.
- Once we have a quantum computer, we will be able to read all the messages that people ever sent.
- We will all know who nought what, who sent a love letter to whom, what CIA did, etc.
- This will be a true end of privacy and secrecy.
- So be careful what you send – sooner or later it will all be decoded.

16. We Will Beat RSA Encryption, But We Will Gain Unbeatable (?) Quantum Encryption

- If all known encryption schemes will be most, does it mean that in the future, there will no privacy?
- Not necessarily.
- Computer scientists came up with a new idea, of *quantum encryption*.
- Its main idea is the same as the main idea behind quantum physics.
- In traditional communication, we exchange bits.
- These bits may be encrypted, but they can be read.
- They can be read legally, from the server.
- They can be read illegally, if someone taps to a cable through which the signals travel.

17. Towards Quantum Encryption

- It is not possible to know if someone listens to your bits or not.
- Just like it is not possible to check if someone is secretly listening to your phone conversations.
- In quantum physics, the situation is different.
- Listening and recording is, in some sense, the same as measuring.
- And we already know that in the quantum world, measuring changes the state.

18. Towards Quantum Encryption (cont-d)

- In the quantum world, measuring changes the state.
- So, if we use quantum-size particle as signals, any attempts to read the message will change the message.
- So, if we periodically exchange test messages, we will immediately see if someone is listening.
- Namely, if someone is listening, the pre-arranged test message will be corrupted.
- In this sense, quantum encryption is unbeatable.

19. Quantum Encryption Is Here Already

- Since RSA will eventually be broken, governments already use quantum encryption for important messages.
- Historically the first was the quantum link between the Pentagon and the White House.
- So, unless the participants in these dialogues describe them in their best-selling memoirs, we will never know.
- (Actually, even if they publish their memoirs, we will never know which of them is telling the truth.)
- Now China has similar links.
- They even a quantum link to a communication satellite.

20. Back to the Future

- So, once quantum computers are invented, what will the future look like?
- First, there will be a turmoil: secrets revealed, crimes uncovered, lies exposed.
- After that, not much different from computing now.
- Computers will be much faster:
  - first, they will be smaller and thus faster,
  - second, they will be using faster (quantum) algorithms.
- Computer security will be even stricter.

21. Consequence for Us: Not So Bad

- Yes in computing business will have to re-train to program quantum computers.
- But don't we have to re-train ourselves all the time anyway?
- Many things required re-training:
  - programming across the web,
  - programming in the cloud,
  - parallel computing.
- Good news is that we will (hopefully) be able to predict where a tornado will do.

22. Beyond Quantum Computing

- But there may be new problems for which even faster computers will be needed.
- And future computer scientists will think of new even faster devices.
- There are already many such ideas – all rather radical.
- For example, we can make the Solar system travel with velocity close to speed of light.
- Then, according to special relativity, time for us will slow down.
- For example, one year on an outside planet will feel like one hour for us.
- We can then leave a computer on one of the slower-moving planets.

23. Beyond Quantum Computing (cont-d)

- One year of actual computing – and we will get the result in an hour.
- Another possibility is to move close to a big black hole.
- According to general relativity, this will also slow us down (remember *Interstellar*).
- So, one year of computing outside will feel for us like one hour.
- And if a time machine is invented, then we do not care how long computations take.
- We can let a computer run for millions of years – and then use a time machine to bring the result to now.
- This way, we will get the computation results right away (or even before we formulate the problem).

24. Maybe the Future Is Closer than It Appears

- And maybe it is not just a distant future.
- Maybe somebody right now – even someone in this room – is already working on a new idea?
- Or maybe this talk will inspire them to work on it?
- Let us all work together to make the future of computing as spectacular as it can be.