12-1-2022

Will Nanotechnology Bring in the Judgement Day?

Olga Kosheleva
The University of Texas at El Paso, olgak@utep.edu

Vladik Kreinovich
The University of Texas at El Paso, vladik@utep.edu

Comments:
Technical Report: UTEP-CS-22-128

Will Nanotechnology Bring in the Judgement Day?

Olga Kosheleva[0000-0003-2587-4209] and Vladik Kreinovich[0000-0002-1244-1650]

University of Texas at El Paso, El Paso TX 79968, USA
olgak@utep.edu, vladik@utep.edu

Abstract. There are many current and prospective positive aspects of nanotechnology. However, while we look forward to its future successes, we need to keep our eyes open and be prepared for what will really be a future shock: that quantum computing – an inevitable part of nanotechnology – will enable the future folks to read all our encrypted messages and thus, learn everything that we wanted to keep secret. This will be really the Judgement Day, when all our sins will be open to everyone. How we will react to it? Will this destroy our civilization? Let us hope that the civilization will survive – as it survived many calamities so far. But to survive, we need to be prepared, we need to know what lies ahead. The earlier we will start seriously thinking about this future shock, the better prepared we will be.

Keywords: Quantum Computing, RSA Algorithm, Quantum Cryptography, Social Consequences.

1 Need for Nanotechnology

While modern computers are fast, there are still many practical problems that require faster computers.

1.1 Tornado Prediction: An Example of a Need for Faster Computers

One of the problems in which faster computations are needed is the problem of tornado predictions. Tornados cause great damage, they cause human injuries and deaths. Most places in tornado-prone areas have tornado shelters where people can be safe when the tornado hits. The problem is that tornados move fast and move in directions which are difficult to predict. As a result, during the tornado season, tornado warnings are sent practically every day, and these warning are sent to the whole area. For each warning, most of the towns are unaffected. So, after a while, people start ignoring these warnings, since you cannot spend your whole life in shelters – and then the next tornado hits, and people die. Millions of people live in tornado-prone areas, you cannot evacuate them all. What is needed is a way to predict where the tornado will turn.

This way, we will be able to send selected warnings, only to those areas where the tornado will most probably be heading.

There is no fundamental reason why we cannot make such more accurate predictions. Tornado is an atmospheric phenomenon which is similar to other atmospheric phenomena like storms and hurricanes. We have learned to reasonable accurately predict the directions in which the storms and hurricanes move – this is an important part of weather prediction. An hour-long run of weather prediction program on a high performance computer can predict tomorrow's weather – including the directions in which storms and hurricanes will move – with reasonably high accuracy.

A similar program can also predict in which direction a tornado will move. The problem is that tornados are much smaller in size and, because of that, their dynamics changes much faster. For a perturbation to change the direction of a storm, this perturbation – that spreads with the speed of sound, of about 340 meters per second – needs to reach all the storm areas, and this takes at least a day – usually more. In contrast, a tornado is relative small in size, so in 15 minutes it can completely change its direction. Because of this difference in time scale, it takes the same amount of time to predict the tornado motion in the next 15 minutes as it takes to predict tomorrow's weather – which is about an hour on a high performance computer. And here lies the big difference:

- It makes perfect sense to spend an hour if our objective is to predict tomorrow's weather.
- However, spending an hour to predict in what direction the tornado will move in the next 15 minutes makes no sense: we will get this "prediction" 45 minutes after the tornado has already moved.

To become useful, predictions must be made in 5 minutes or so – to give people time to reach the shelters. In other words, we need to speed up computations by an order of magnitude.

1.2 How Can We Make Computers Faster?

There are many other practical problems in which a similar (or even larger) speedup is needed. How can we make computers that much faster?

Engineers are actively working on making computers faster, but what most people do not realize is that there are fundamental obstacles preventing us from making computers much faster. One of the main obstacles to computer speed increase is, somewhat surprisingly, Einstein's special relativity theory: namely, the fact that, according to this theory, the speed of all communications is limited by the speed of light; see, e.g., (Feynman at al. 2005), (Thorne and Blandford 2021).

At first glance, this may sounds strange: the speed of light is about 300 000 kilometers per second, several orders of magnitude faster than the fastest missiles. But it *is* an obstacle. For example, a usual laptop – like the one in which we are typing this text – is of 30 cm size. So, even if communications where as fast as the speed of light, it would still take 30 cm / 300 000 km = 1 nanosecond for a signal to go from one side of the computer to another. During this time, even the cheapest 4 GHz laptop already performs 4 arithmetic operations.

1.3 We Need Nanotechnology

Thus, to make computers much faster, we need to make computers much smaller. This means that we need to make their components much smaller -- this is why computer engineers are always trying to decrease the size of computer components. In other words, we need *nanotechnology*.

2 Nanotechnology Leads to Quantum Computing

Already computer components are comparable in size to molecules -- there is only a few orders of magnitude difference. To get an order of magnitude speedup, we need to decrease the size of a computer – and thus, the size of a typical component – also by the order of magnitude. Very soon, we will get to the sizes comparable with the sizes of individual molecules.

Once we start operating on this size level, we will need to take into account that the laws governing such small objects are different from the usual laws of Newtonian physics – they follow the laws of quantum physics; see, e.g., (Feynman et al. 2005), (Thorne and Blandford 2021). To be more precise, all the objects in the world follow the laws of quantum physics, but:

- for macro-bodies, the difference between the quantum predictions and Newton's laws is practically undetectable, while
- for micro-bodies, this difference is drastic.

So, when we will drastically decrease the size of computer elements, we will have to take laws of quantum physics into account. Computing under laws of quantum physics is known as *quantum computing*; see, e.g., (Nielsen and Chuang 2011). So, nanotechnology will eventually lead us to quantum computing.

3 Quantum Computing Can Break All the Encryptions

At first glance it may sound as if all we need to speed up computations is to make computer components much smaller. Unfortunately, the situation is more complicated.

3.1 Probabilistic Character of Quantum Physics

Yes, if we make the component smaller, it indeed opens the opportunity to perform computations much faster. But, as have mentioned, making computer components smaller means that now we have to take effects of quantum physics into account. And one of the main features of quantum physics is that, in contrast to Newton's mechanics, we cannot exactly predict the results of future observations, we can only predict the *probability* of different future observation results; see, e.g., (Feynman et al. 2005), (Thorne and Blandford 2021).

A typical example is radioactivity:

- there is no way to predict whether a given atom will experience radioactive decay during the given time interval,
- we can only predict that it will decay with a certain probability.

3.2 The Probabilistic Character of Quantum Physics Is a Challenge for Quantum Computing

This probabilistic character of quantum systems makes interesting physics, but it contradicts the main idea of computations – that we should get the exact same desired result every time we run the computer.

If we simply replace each computer component with a much smaller one, we will not get the desired result. Indeed, for this to happen, this would mean that all millions and billions of operations were performed correctly. And even if the probability p of each operation to be performed correctly is close to 1, the probability that N operations will be performed correctly is p^N – which for large N is close to 0.

So to reliably perform computations on such nano-size components, we need to drastically change the algorithms – so that the results will be deterministic in spite of the probabilistic character of all the components.

3.3 How We Can Overcome This Challenge

For many computations, researchers found a way to design such new algorithms; see, e.g., (Nielsen and Chuang 2011). Interestingly, there is an additional factor – other than the size-related computation speed – that makes quantum computing potentially effective; namely:

- In a usual computer, all the information is stored and processed in terms of bits; an elementary unit – the bit – can be in two states: 0 and 1.
- In quantum physics, a bit, like every system, in addition to its usual states – that are denoted $|0\rangle$ and $|1\rangle$ -- can also be in a so-called *superposition* state $a|0\rangle + b|1\rangle$, where a and b are complex numbers for which $|a|^2 + |b|^2 = 1$.

Thus, each *qu*antum analogue of a *bit* – qubit, for short – can be in infinitely many different states and thus, can carry more information that a classical bit.

As a result, many quantum algorithms are even faster than they should be if we only take into account the decrease in size. There are two main examples of such algorithms.

3.4 Grover's Algorithm

The first example is Grover's quantum algorithm that searches for an element in an unsorted array.

In classical physics, all we can do at each computational step is to check whether one element of the array is the one we are looking for. So, if we have an array consisting of n elements, we need, in some cases, to look over all n elements – if we skip even one element, this may be exactly the desired element and we will miss it. Thus, the worst-case search time is proportional to the size n of the array.

It turns out that in the quantum case, we can find the desired element much faster: in time proportional to the square root of n. This may sound impossible at first glance, but the trick is that instead of simply asking a query j that checks whether the j-th element is the desired one, in the quantum case, we can submit a query which is a superposition of several such indices. In effect, this is like searching in several locations at the same time – and this drastically decreases the computation time. For example, for an array of 1 million records, the quantum algorithm would find the desired element in 1000 computational steps – thousand times faster than the non-quantum one.

3.5 Shor's Algorithm

Another example is Shor's quantum algorithm for factoring integers.

In the non-quantum case, the way to find divisors of a given number is, in effect, to try all possible prime numbers smaller than the square root of the given number. So, if we take a huge number, with 200 decimal digits, this would take 10^{100} computational steps – which even on the fastest computers will take much longer than the lifetime of the Universe.

Interestingly, a quantum algorithm can do it in feasible time – for a number with d decimal digits, the time is bounded by a small power of d.

3.6 Why This Is Important

This may sound, at first glance, as a purely mathematical problem of no specific practical use. But in reality, this result is extremely important.

This importance is related to the fact that most current encryption systems are secure exactly because it is not possible to factor large integers. In the most widely used RSA encryption (see, e.g., (Cormen et al. 2022) – named after the first letters of the names of its authors – the computer that wants to receive an encoded message select two large prime numbers p and q and computes their product n = pq. This product is then openly broadcast, and anyone can use this number to encode their message. To decide the encoded message, however, it is necessary to know p and q. So:

- the person who distributed this code can decode all these messages, since he/she knows both p and q, but
- no one else can read these encoded messages.

But if we have a quantum computer, we can factor n, find p and q and read all the encrypted messages!

3.7 Quantum Computing Will Enables Us to Break All the Codes

There are other encoding algorithms which are somewhat more complex than RSA. However, for all these algorithms, researchers have designed modifications of Shor's quantum algorithm, modifications that crack all these encodings.

So, once sufficiently powerful quantum computers become available, these computers will enable us to read *all* messages:

- between people,
- between and within companies,
- between and within governments, etc.

This perspective is one of the main reasons why governments all over the world invest heavily in quantum computers: they want to be the first to learn their adversaries' secrets.

4 This Does Not Necessarily Mean End of Privacy

The fact that quantum computers can crack all algorithmic encoding invented so far does not mean that with quantum computers, we will have no privacy anymore. Actually, by using quantum effects, we can also come up with a cryptographic scheme (known as *quantum cryptography*) that cannot be so easily broken; see, e.g., (Nielsen and Chuang 2011).

It should be mentioned that, in contrast to quantum computing -- which is mostly about the future -- quantum cryptography is already used for several decades -- in the US and in other countries -- for secure communications.

5 But Will This Bring the Judgment Day?

5.1 Let Us Summarize What We Learned

Natural progress in nanotechnology will lead to quantum computing. In turn, quantum computing will enable to read all the secrets – at least all the secrets generated before quantum cryptography became available.

5.2 What Will Be the Social Consequences?

What will be the social consequences of the code-breaking aspects of quantum computing? Remember, *all* communications will be open and read.

5.3 What Will Happen on a Personal Level?

On the personal level, the vast majority of extramarital affairs will be disclosed – since they usually involve at least some – supposedly secure – communications: emails, phone calls, text messages, communications via social networks. All this is now protected by RSA or by similar schemes. Thus, with the advent of quantum computers, all this will be disclosed.

Will marriages survive such a disclosure?

5.3 What Will Happen to Crimes?

Most crimes will be revealed – since crimes usually involve some communications, and these communications will be disclosed.

5.4 What Will Happen to Companies? To Politics? To Religion?

Many damaging -- and even criminal -- internal communications within companies will be there in the open.

Clergy will not be immune to these disclosure, it will be much worse that all previous scandals -- since now *all* will be revealed.

All embarrassing -- and sometimes criminal -- messages between politicians will become known. Some people may naively hope that politicians from their country or, more precisely, from their political party will turn out to be innocent -- but the experience of many leaks show that no one is without sin.

5.5 What Will People Do?

What will people do? There is no way millions of guilty people will go to jail -- especially since many judges will turn out to be guilty too.

So maybe we will all forgive each other and promise to sin no more (and then continue to do the same thing but now using only quantum encryption)?

5.6 We Hope That This Will Be a Shock but Not a Catastrophe (and This Hope Is Justified)

Yes, it is theoretically possible that these disclosures will bring our civilization to an end. But we are optimistic.

What makes us optimistic is that – on a smaller scale -- such situations already happened. Let us give two examples from Russian history, one involving Russia only and one involving other countries as well. Both examples date back to 1917, the year when the Czar was overthrown in February and then the Communists came to power in October.

The first example is that in February 1917, when the revolutionaries overthrew the Russian Czar, they decide to burn down the archives of the Secret Police. These archives contained dossiers on many Russian citizens -- including the revolutionaries themselves. And it turned out that no one was without sin: many were collaborating with the regime, many were guilty of other sins. Different revolutionary factions hated each other, fought with each other – but when they burned down the archives, they acted in good solidarity. Did they stop sinning? No way. Of course, many of them started sinning again :-)

Another example is that in October 1917, when the Communists took over, they published all secret treaties and secret communications between the governments of different countries. It turned out that in many cases, countries claiming freedom and liberty as their motivations were actually interested more in oppression and economic advantages. The Communists' motivation for publishing these treaties was that people

would be shocked and overthrow their governments. Did it happen? No. There was not even a hint of a scandal: no opposition leader wanted to inflame this, since they were all guilty. Most people studying history are not even aware of this episode – we know it only because we studied Russian history when living in Russia.

5.7 But We Need to Be Ready

So we hope that this coming Judgment Day shock will not be a catastrophe. And to decrease the potential harm, we all need to be prepared, we all need to know that this shock will come – and this is one of the reasons why we are writing this paper.

Let us be prepared!

Acknowledgments

This work was supported in part by the National Science Foundation grants 1623190 (A Model of Change for Preparing a New Generation for Professional Practice in Computer Science), and HRD-1834620 and HRD-2034030 (CAHSI Includes), and by the AT\&T Fellowship in Information Technology.

It was also supported by the program of the development of the Scientific-Educational Mathematical Center of Volga Federal District No. 075-02-2020-1478, and by a grant from the Hungarian National Research, Development and Innovation Office (NRDI).

The author are greatly thankful to Raffaele Pisano for his encouragement and help.

References

Cormen ThH, Leiserson CE, Rivest RL, Stein C (2022) Introduction to Algorithms, MIT Press, Cambridge, Massachusetts.

Feynman R, Leighton R, Sands M (2005) The Feynman Lectures on Physics. Addison Wesley, Boston, Massachusetts.

Nielsen MA, Chuang IL (2011) Quantum Computation and Quantum Information. 10th edn. Cambridge University Press, Cambridge, UK

Thorne KS, Blanford RD (2021) Modern Classical Physics: Optics, Fluids, Plasmas, Elasticity, Relativity, and Statistical Physics. Princeton University Press, Princeton, New Jersey.