When shall we have a quantum computer?

M.I. Dyakonov

Laboratoire Charles Coulomb, Université Montpellier, France

- Quantum versus classical computer
- Quantum computer is an analog machine
- ARDA roadmap for quantum computing (2002)
- Current state of the art

  Experimental

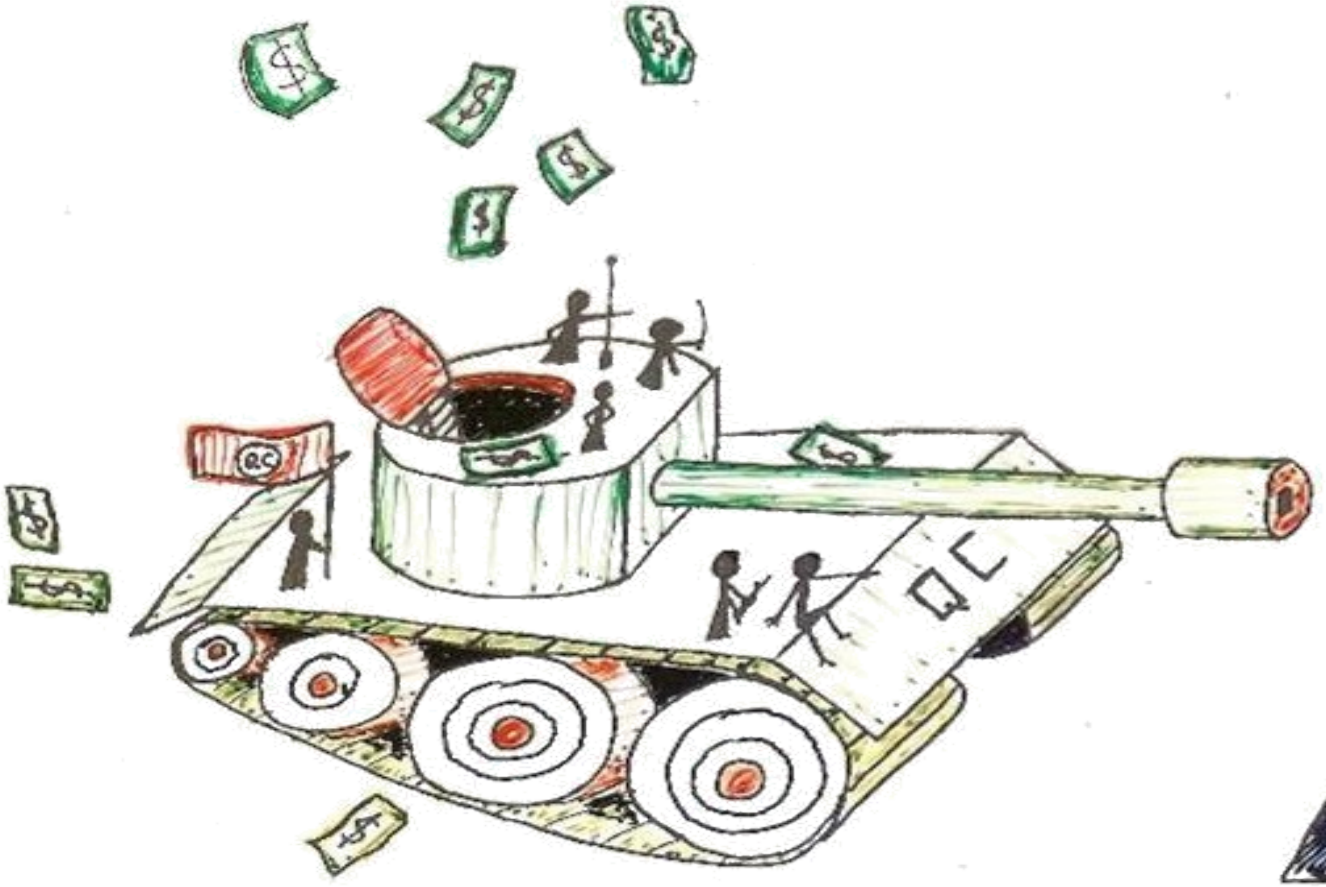
  Theoretical

- Conclusion: **Take-away message**

Reminiscence

Quantum computing: a view from the enemy camp

M.I. Dyakonov, Future Trends in Microelectronics (2001)



The enemy camp is here

.

Some numbers illustrating the scale of craziness

(modern quest for the Holy Grail)

Google search gives

Quantum computing:	6,450,000 results
Quantum computer:	1,460,000 results
Quantum computation:	815,000 results
Qubits :	1,420,000 results
Quantum error correction:	135,000 results
Quantum technology:	351,000 results
Quantum gates:	134,000 results
Quantum computing with:	133, 000 results (!)

And still no quantum computer in sight!

Classical computer

At a given moment, the state of the classical computer is described by a sequence (↑↓↑↑↓↑↓↓…), where ↑ and ↓ represent **bits** of information – physically realized as the *on* and *off* states of individual transistors.

With N transistors, there are $\mathbf{2}^{N}$ different possible states of the computer.

The computation process consists in a sequence of switching some transistors between their ↑ and ↓ states according to a prescribed program.

Hypothetical quantum computer

In *quantum* computing one replaces the classical two-state element by a quantum element with two *basic states*, the *qubit.*

The simplest object of this kind is the electron internal angular momentum, *spin*, with the peculiar quantum property of having only *two* possible projections on ***any*** **axis**: +1/2 or -1/2 (in units of Planck constant).

For some chosen axis, we again denote the two ***basic*** quantum states of the spin as ↑ and ↓.

Hypothetical quantum computer
(continued)

However, the *arbitrary* spin state is described by the *wave function:*

$$\psi = a\uparrow + b\downarrow,$$

where a and b are complex numbers, satisfying the normalization condition:

$$|a|^2 + |b|^2 = 1$$

In contrast to the **classical bit,** that can be only in ***one*** of the two states, ↑ or ↓, the **qubit** can be in a ***continuum*** of states defined by the complex quantum amplitudes a and b,

(exactly as for a classical object, like a compass needle)

This is basic quantum mechanics!

This is also the origin of the supposed power of the quantum computer

However this is also the source of its enormous fragility and vulnerability!

With 2 qubits, there are $2^2 = 4$ basic states: (↑↑), (↑↓), (↓↑), and (↓↓).

Accordingly, the system is described by the wave function:

$\psi = a(\uparrow\uparrow) + b(\uparrow\downarrow) + c(\downarrow\uparrow) + d(\downarrow\downarrow)$ **with 4 complex amplitudes** a, b, c, and d.

In the general case of *N* qubits, the state of the system is described by 2^N complex amplitudes restricted by the normalization condition only

(a corresponding classical system would be described by 2*N* parameters)

While the state of the classical computer with N bits at any given moment coincides with *one* of its 2^N possible *discreet states*, the state of a *quantum* computer with N qubits is described by the values of 2^N *continuous parameters* (quantum amplitudes)

The information processing is supposed to be done by applying unitary transformations (quantum gates), that change these amplitudes (which are *continuous variables!!!*) in a precise and controlled manner.

How many qubits do we need?

The number of qubits **needed to beat your laptop** in factoring large numbers is estimated as $N \sim 1000$ (without error correction)

An arbitrary state of such a quantum computer is characterized by $2^{1000} \sim 10^{300}$ complex amplitudes

That's quite a lot, compared to the number of particles in the whole Universe, which is only $\sim 10^{80}$ …

NB. *With* error correction (which is indispensible), the number of qubits must increase from $N=10^3$ to $N = 10^5$, or more …. **What about 2^N ?**

When shall we have a useful quantum computer?

Optimistic experts say: in 10 years

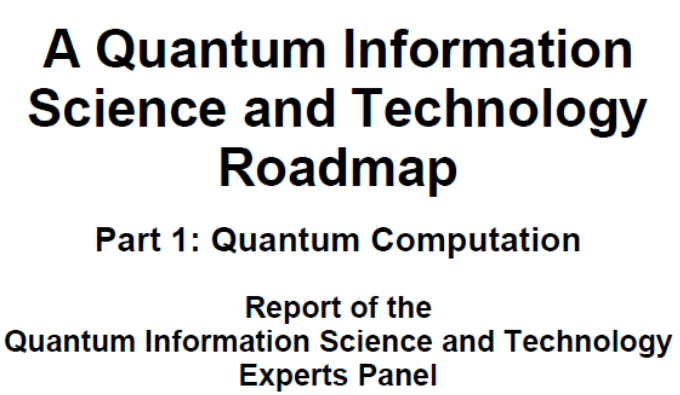
Other experts anticipate 20 to 30 years

(Note that those estimates have not changed during the last 20 years!)

The most cautious ones say: Not in my lifetime

My answer: ***when physicists and engineers will learn to keep under control 10^{300} continuous parameters (quantum amplitudes) defining the state of the whole machine.***

Which means: *NEVER* …



ARDA Roadmap (2002)

(The 5- and 10-year goals and reality)

The 2007 goal requires "something on the order of 10 physical qubits and multiple logic operations between them", while the 2012 goal "requires on the order of 50 physical qubits, exercises multiple logical qubits through the full range of operations required for fault-tolerant QC in order to perform a simple instance of a relevant quantum algorithm".

While a benevolent jury could consider the first two of the 2007 goals to be *partly* achieved by now, the expectations for the third 2007 goal, and especially for the 2012 goal, are **wildly off the mark**.

EXPERIMENTAL
(respect and admiration)

Experimental studies related to the idea of quantum computing make only a small part of the huge QC literature. They represent the *nec plus ultra* of the modern experimental technique and are extremely difficult.

The goal of such experiments is to demonstrate some elements of quantum algorithms. **In particular, factoring 15 and 21 by Shor's algorithm was achieved!**

The number of qubits used is below 10, usually from 3 to 5

Apparently, going from 5 qubits to 50 **(**the goal set by the ARDA Experts Panel roadmap **for the year 2012!)** presents hardly surmountable experimental difficulties and **the reasons for this should be understood.**

Most probably, they are related to the simple fact that

$2^5 = 32$, while $2^{50} = 1125899906842624$

Concerning experimental factoring of 15 and 21 by Shor

In these experiments the ***compiled*** version of the Shor's algorithm was used.

The full algorithm can factor a k-bit number using $72k^3$ elementary quantum gates;

factoring 15 requires 4608 gates operating on 21 qubits [Beckman et al (1996)]

This **enourmously surpasses** the today's (and tomorrow's) experimental possibilities. Beckman et al introduced a ***compiling technique*** which **exploits properties of the number to be factored**, allowing exploration of Shor's algorithm with a vastly reduced number of resources.

One might say that this is a sort of (innocent) cheating:

knowing in advance that $15=3\times5$, we can take some shortcuts, which would not be possible if the result were not known beforehand.

All the existing experimental testing of Shor's algorithm use this approach!

Quantum versus classical precision

Consider a **classical** system of 1000 compass needles

By a) applying external fields to individual needles and
b) introducing controlled interactions betweens pairs,
we wish to impose a prescribed evolution of the whole system

- Uncontrolled rotations due to noise
- Manipulations are not exact
- Undesired interactions between our needles

Some trivial remarks:

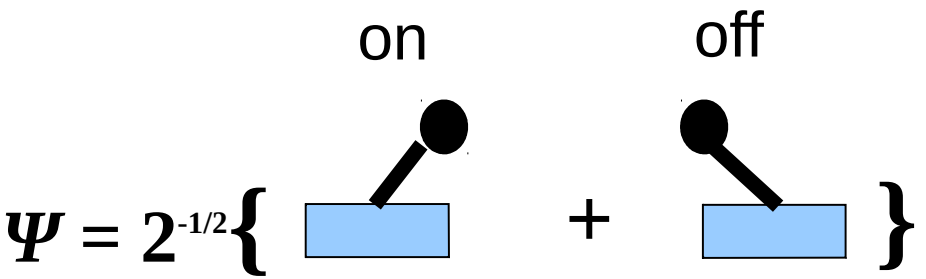
We fix a coordinate system *xyz* related to some physical objects, with the *z* axis pointing towards the Polar Star

* This direction, as well as the angles between our axes cannot be defined exactly
* The orientation of the needle with respect to our axes cannot be defined exactly
* Two needles NEVER point in *exactly* the same direction
* etc, etc

Quantum versus classical precision

Apparently, things are not so obvious in the magic world of quantum mechanics!

There is a **widespread belief** that the $|1\rangle$ and $|0\rangle$ states "in the computational basis" are something absolute, akin to the on/off states of a classical switch, but with the advantage that one can have quantum superpositions of these states



The theorists' view of a qubit

In reality, pure $|1\rangle$ and $|0\rangle$ states can never exist!

Similarly, a classical vector can never point *exactly* in the ***z*** direction.
(We simply never know exactly *what* is the *z* direction)

Instead of pure $|1\rangle$, we ***always*** have $|1\rangle + c\,|0\rangle$ with some unknown c
(where $|c|$ is hopefully small).

Quantum versus classical precision

The classical statement:

the orientation of any vector is known only within a certain precision

is translated into quantum language as:

there is always an admixture of unwanted states to any desirable state

reflecting our inability to exactly define the “computational basis”

and has nothing to do with quantum mechanics, or “errors per qubit per gate”

Thus the $(|1\rangle + |0\rangle)/2^{1/2}$ state, and especially the “cat” state

$$|\text{cat}\rangle = (|1111111\rangle + |0000000\rangle)/2^{1/2},$$

as well as $\sqrt{2}$, are **abstractions**, that can **never exist in reality!**

There will always be an admixture of ALL other 126 states,

albeit with small amplitudes !

What is an “error”?

Many QC theorists believe that errors in a desired quantum state consist in the fact that one or more qubits instead of being in the ↑ state are in the ↓ state, or vice versa (in full analogy with a classical digital computer)

This certainly would be a **strong** error. However, more common (and more dangerous) are **weak** errors, consisting in rotations of qubits by a **small** angle, when, instead of ↑, one obtains $(\uparrow + \varepsilon\downarrow)$, where $|\varepsilon| << 1$

(a small admixture of the ↓ state)

My own Axiom

(concerning the physical, not the mathematical, world)

Axiom 1: **No continuous variable can have an exact value**

Corollary: **No continuous variable can be exactly equal to zero**

(contrary to the situation with discrete quantities)

Example: Any action on the wave function of 1000 qubits with 10^{300} amplitudes is described by a matrix $10^{300} \times 10^{300}$.

You ***think***, that you can apply a matrix, corresponding to a two-qubit gate.

That is, you want to act somehow on 2 qubits, and do ***nothing*** to the other 998

However, according to Axiom 1 this is impossible. You can never *completely* isolate all the other qubits from the action of your applied fields!

In addition, your action on the chosen 2 qubits will not be exact either

The fundamental trouble with the error-correction scheme

consists in not respecting Axiom 1:

i.e. assuming that ***all*** the numerous assumptions are fulfilled ***exactly,***

and this is at the ***heart of the theory*** of error correcton

A responsible theorist should provide estimates on:

- How small should be the undesired influence of gates on other qubits
- How small should be the undesired interaction between qubits
- How small should be errors of gates and measurements
- How small should be undesired admixture of the other 126 states

to the *cat state:* $|\text{cat}\rangle = 1/\sqrt{2}\ (|1111111\rangle + |0000000\rangle)$

- With what precision the irrational number $\sqrt{2}$ should be experimentally realized?

Should it be 1.41, or 1.41421356237 ?

No answers ...

Not only are there no answers to those obvious questions, but they have neve been even discussed!

If this problem were realized, the theshold theorem would not be formulated in terms of **“**error per qubit per gate**”** only,

but also by indicating the required ***precision*** with which various assumptions and operations should be fulfilled

One should not tell the engineer:

“Make this angle 45° and then my proposed vehicle will run as predicted, provided the road is flat**”**

Tell him instead:

“Make this angle 45°± 0.001° and then my proposed vehicle will run as predicted, provided the roughness of the road does not exceed 3 micrometers**”**

Only then he will be in a position to understand whether it is possible or not

Evolution of the *QC* state due to low-amplitude noise

Initial state of *N* qubits: $\psi(0) = |\uparrow\uparrow\uparrow\uparrow\ldots\uparrow\uparrow\rangle$

It can be shown that in the simplest case of uncorrelated noise acting on individual qubits **this state will deteriorate** during a time τ */N,* where τ is the spin relaxation time (or decoherence time of a single qubit).

This means that the overlap of the actual state of an *N*-qubit QC with the desired state will decay in time as exp(- *Nt*/τ), i.e. ***N* times faster that the relaxation time of an individual qubit.**

Thus the time we have to perform the entire quantum computation cannot exceed 1/*N*-th of the spin relaxation time!

Conclusions

- It is **absolutely incredible**, that one can continuously protect the grand wavefunction from the random drift of its 10^{300} amplitudes and make these amplitudes change in a precise and regular manner needed for large-scale quantum computations

- The (theoretical) success of error-correcting schemes is based on the introduction of *ideal elements* and assumptions that are supposed to be satisfied *exactly*. The consequences of unavoidable small deviations from the ideal situation were *never analysed*

- Such an analysis is likely to show that one needs a precision which is exponential in the size of computation. **"It is exponentially difficult** to build a large (useful) QC**"** – MD (2001)

- **Summary**: **No quantum computer in any foreseeable future**

Take-away message

The hypothetical quantum computer is an *analog machine* with

a super- astronomical number of *degrees of freedom*:

the values of 2^N quantum amplitudes (where $N \sim 1000$),

which are *continuous parameters*

This is just basic text-book Quantum Mechanics…

Let's hope that this obvious fact and its consequences

will be understood during the next 20 years…