On the (im)possibility of quantum computing

G. S. Paraoanu*
Low Temperature Laboratory, Helsinki University of Technology, P.O. Box 5100, FIN-02015 TKK, Finland

We are witnesses nowadays in physics to an intense effort to built a quantum computer. In this essay, I point out that the failure of this enterprize could be in fact more intellectually exciting than its success. I conjecture that, despite the fact that we do not know any law of nature that would prevent us from building such a machine, it might not be possible, after all, to scale up the few qubits that have been realized so far. If this turns out to be the case, the consequences could be truly amazing: it would mean that quantum mechanics is indeed an incomplete description of reality, as Einstein thought, and it would also imply that certain types of computation - and the knowledge derived from it - are fundamentally inaccessible.

I. ENTHUSIASM

Quantum computing is a young discipline at the interface between computer science and quantum physics. It rests on the discovery that certain computational tasks such as number factorization, period finding, and database search could be sped up if these problems were to be encoded in states of objects and in operations that - unlike the classical Turing machine - would behave quantum-mechanically. These objects (called qubits), would acquire properties such as superposition and entanglement by sequences of externally-controlled manipulations that result in unitary transformations (quantum gates) between sets of qubits. The effect of measurement on the qubits is described by the standard von Neumann projection postulate [1].

It is somewhat counterintuitive that a more efficient processing of information can be obtained by using quantum mechanics. Shouldn't exactly the opposite be the case - since objects in quantum mechanics do not in general have well-defined properties, any information associated with such properties should be diffuse and, due to the randomness of the measurement process, unreliable to recover? After all, isn't it the case that the Heisenberg uncertainty relation sets a fundamental limit to our knowledge of physical variables? The clever trick of quantum computing is to bypass all these objections by avoiding to encode the classical bit of information directly into a corresponding observable. Typically, the data of the problem are embedded in the initial conditions of the system, which are amenable to a fully classical description. Then, the system evolves quantum-mechanically under the application of a sequence of quantum gates, and the final state is measured. The result, which encodes the solution to the problem, is as such cast irreversibly - *alea jacta est!* - into the classical world. In other words, to perform a computation there does not have to be a one-to-one correspondence between the bit and the "it" at every step of the program: all that matters is how the "output" results correlate with the "input" [2]. As it turns out, quantum mechanics offers a way to produce stronger correlations between the input and output - stronger than correlations achievable by the correspondence mentioned above. This is a profound consequence of the fact that there cannot be any local realistic variables "hidden" behind the quantum formalism. It has been known, since the groundbreaking work of Bell, that one cannot produce a theory with such variables which would reproduce the predictions of quantum theory. The correlations between experimentally measured results (as predicted by quantum physics) are stronger than any theory of hidden variables satisfying conditions such as locality and realism [3] - which would be the right type of "it" to use for embedding the "bit" in a one-to-one correspondence. This is why, when counting resources such as the number of operations needed to solve a problem, a quantum computer could be more efficient than a classical one.

II. REALITY CHECK

Quantum computers do not exist yet. The experimental effort in this direction is already more than 10 years old. Progress has been made for sure. Many physical systems have been proposed as candidates for the magic qubit: trapped ions, photons, superconducting circuits, atomic nuclei in certain materials *etc.*. Most important quantum algorithms have been demonstrated for a few-qubit systems (less then 10). This looks like solid progress, and one might wonder what exactly stops physicists from declaring the problem solved, passing on the task of adding more qubits to engineers, and then move on to other issues. The reason is that scaling up from a few-qubit demo processor to a machine that would really be able to compete in solving certain problems more efficiently does not amount to just a simple redesign of a chip. What exactly is the difficulty? It depends on the type of quantum processor. For example, with photonic quantum processors the main issue is the smallness of photon-photon interaction: interaction is responsible for entanglement, which is needed in quantum computers, so to get more photons entangled (or higher probability of entangled pairs) one needs to ramp up the power of the

*Electronic address: paraoanu@cc.hut.fi

lasers - a strategy which obviously runs fast into technical problems. In the NMR version, the signal falls off exponentially with the number of qubits. In ion traps, various sources of decoherence and instabilities are the main constraining factor. In superconducting qubits, decoherence coming from the electromagnetic degrees of freedom and impurities in the junctions are known obstacles to scalability. When we add the detectors into the picture, a new set of restrictions can be listed: detectors are not perfect either, and their efficiency add up their own set of limits. Baring the issue of decoherence - an interesting phenomenon to study in the context of quantum computing - for most theorists working in the field of quantum computing many of these look rather like unfortunate technological limitations of the present times. It is hoped that they can be surpassed, for example, through advances in material science - availability of technologies that would produce defect-free insulating barriers for Josephson junctions, and more efficient detectors - or by employing new design ideas (segmented ion traps, better microwave-engineered superconducting circuits). As for decoherence, if it will not be significantly enough alleviated by the constant progress in microfabrication, materials, and design, then new ideas such as the use of decoherence-free subspaces or topological quantum computing could be put to good use. In many cases in science, constant progress in a predictable direction do happen. It is what Thomas Kuhn called "normal science", as opposed to revolutionary periods during which changes of paradigm occur. There are cases in which tedious, sustained work towards a goal reaches the desired destination, sometimes even against the ironic musing of the outsiders. Some examples are Edison's electric light bulk, Wrights' airplane, and probably many others.

III. DOUBTS

But it is not always obvious that something that looks perfectly plausible and in tune with the present science cannot be done in principle: history is also full of cases in which common sense and accepted knowledge is defied by unexpected findings. Most scientists at the end of the XIX'th century would have considered the limitless division of objects into smaller parts possible, just limited by inadequate technology. Boltzmann, ill and depressed by the lack of adherence to his atomistic theory, committed suicide in 1906 (decisive experimental evidence for the existence of atoms would come only 3 years later, in 1909, from Rutherfords' lab). And Hilbert's program of axiomatization of mathematics must have looked challenging but feasible to Russell and Whitehead but then Gödel's incompleteness theorem came along.

There are no convincing arguments that building a quantum computer is impossible. So far, the only disproof of quantum computing comes from the griding of the teeth of hundreds of graduate students and postdocs who are trying to make it work in practice [4]. For, as it is often said, quantum computing is a theorist's dream and an experimentalist's nightmare. However, a bit of contemplation on the nature of many-body quantum physics shows that nothing comes with a warranty when we talk about complex quantum systems such as those required for a quantum computer [5]. A first observation is that the Hilbert space is extremely large. This "extremely large" is an understatement. For a system of only 1000 qubits (something which would constitute a minimal requirement for a decent start-up quantum processor) the Hilbert space has $2^{1000} = 10^{301}$ dimensions. This number is so large that any human effort to intuitively grasp it is hopeless. Then how do we get around this problem in condensed-matter physics? - after all here the number of quantum entities, such as electrons in a metal, is even larger, of the order of 10^{23}. The answer is that in this case we are using certain symmetries of the Hamiltonian resulting from the regularities in the crystalline structure of the solid. For example, when calculating energy bands in a semiconductor, the electrons are assumed to move in a periodic potential due to atoms being placed in a regular lattice. The Hamiltonians involved in quantum computing are not of this type: they are, in fact, time-dependent Hamiltonians acting for a finite amount of time on certain pairs of qubits. The resulting states are highly entangled states with a very different structure from the ground and excited states that appear naturally in various condensed-matter systems. As the complexity of these states increases, the time needed to prepare and to characterize them increases as well. For example, to do quantum tomography on an ion-trap system of 8 qubits it took more than half a milion measurements over a time of 10 hours [6] (and analyzing this data is yet another big hurdle [7]). Not only that it is not practical, but it is blatantly impossible to do the same for a number of qubits only one order of magnitude larger. Now, enter any lab specialized in quantum computing: the "quantum processor" itself can be a device no bigger than a few milimiters - but take a deep breath and look around you. You see piles of generators, amplifiers, digitizers, lasers and lenses, complicated vacuum and cryogenic devices. The more qubits, the more such stuff. Accounting for the classical resources needed to run a quantum computer is not straightforward [8], and it requires a serious dose of optimism to imagine all this hardware multiplied by orders of magnitude and compressed in a laptop. Needless to say, the reason that we got so far with miniaturization for classical computers is that such formidable overhead to support and pamper matter and field at the level of single quanta is not needed: classical computers process information by using incoherent, large electrical currents and potentials consisting of many electrons, which are stable and relatively easy to obtain.

This struggle to increase the number of qubits resembles the uphill battle to factorize numbers - consider for example the latest record in factorization on classical computers, that of a 200 -digit number in 2005 [9]: a 80-CPU cluster was used and the calculation took 3 months.

It is tempting to speculate that, in both cases, the source of the difficulty comes from the fact that the amount of (classical) information potentially encoded in both a highly entangled state and a large semiprime number is immense.

IV. A LIMITING PRINCIPLE

Have we actually seen this situation before in science? In fact, yes. There is *a priori* no reason to suspect that it would not be possible to cool an object to lower and lower temperatures. If you suddenly forget all that you know about thermodynamics, you might however be still surprised by the fact that there are plenty of examples of phenomena that naturally produce heat to hundreds and thousands of degree Celsius but not so many that result in below-zero Celsius temperatures. Cold is difficult to create. In the biological world, animals have developed sophisticated machineries of producing heat at the cellular level, but the trick used to cool off is very rudimentary: sweating. Another hint comes from the instruments we use to measure temperature: it is difficult to imagine a simple thermometer that would work at very low temperatures, as most fluids would freeze. Of course, we know that indeed these are not just accidents and there is a fundamental limit, zero Kelvin, which is unattainable [10]. The purpose of this paper is to conjecture that the same will be the case with quantum computing. We will reach a universal, fundamental limit of quantum complexity. Truly desirable forms of quantum computing might be possible only asymptotically - requiring either so extensive resources that relativistic effects become important or, oppositely, having to be confined in a so small space that virtual excitations start to play a role. The Hilbert space indicates indeed what is possible according to the knowledge we gathered from a number of particular cases: but we have no warranty that all these vast arrays of possibilities are physical. It is wishful thinking to believe that there is no limiting principle at work here.

Note that this historical argument cannot be made for example for the speed of light, and the reason is that for most part our technology is limited to much lower speeds. However, in the case of quantum complexity, everything seems to point to the fact that this limit is close to our present-day technological capabilities. I imagine this limiting principle in analogy with the second law of thermodynamics, which prevents us from building 100% efficient heat engines - full conversion of heat into mechanical work is forbidden. And forget about 99.9% efficiency: most machines don't go anywhere nearby (a car for example has about 25% heat-to-work efficiency). A similar principle could hold for information processing: to outperform a classical computer, we might need to be either close or trespass a critical informational barrier. Indeed, remember that what quantum algorithms seem to offer is a more efficient way of processing correlations between logical entities without the need to represent them onto (separate) physical entities. This means that, while running a quantum algorithm, the amount of spurious classical information generated (say due to the recording of intermediate results) is much smaller than for a classical computer performing the same task. Ideally, it should be zero, meaning that the states in a quantum processor do not decay, get entangled with the states of other nearby devices (*e.g.* those used for measurement, trapping, and so on), or do anything that would broadcast information to the rest of the Universe [2]. This extraneous classical information could play the role of the heat which must be dissipated in order to extract work from a heat reservoir.

Two scenarios

What could happen as we approach this limit? Imagine that we struggle to build a quantum computer for twenty years or so more and fail [11], in the sense that it would become clear that progress is harder and harder as the number of qubits and quantum gates increases. In other words, it is very possible that instead of some geometric progression, as in Moore's famous prediction for semiconductor-based computing technology, we will not even have a linear increase but instead a logarithmic curve of the number of qubits as a function of time. There are two ways in which this can happen.

The first scenario can be described in the following way: the experimentalists are confident that they fully understand all the sources of relaxation, dephasing, instabilities, material defects, *etc.* in their single-qubit and few-qubit systems. With the parameters extracted from such preparatory experiments, there are clear theoretical predictions about what to expect when the number of qubits is doubled, tripled, and so on. Yet all attempts to assemble a processor with a larger number of qubits and to run a quantum algorithm fail. In this case we would clearly have discovered an experimental situation which quantum mechanics fails to describe. Einstein would be revenged. Needless to say, the implications would be revolutionary: it would mean that there is fresh, experimentally-accessible physics beyond quantum mechanics to explore out there, and I cannot think of a single physicist who wouldn't want to unveil the mysteries of the new science.

This could be a discovery with extraordinary implications, for there would then be a way to extract ourselves from the epistemological conundrums dug by physicists and philosophers with every "interpretation" of quantum physics. The idea that there could be some unexplored physics beyond quantum mechanics is one that has excited theorists for a long time: but the direction they indicated to search for it (*e.g.* the Planck scale) has been quite remote from the possibilities of what can be achieved in the lab. But what is the likelihood that quantum mechanics would break at so much lower energy scales - isn't it the case, after all, that quantum mechanics has been thoroughly tested and that it works even for relatively large objects, as confirmed by quan-

tum superpositions in SQUIDs and interfering macromolecules? Such spectacular experiments have indeed been done: but large is not necessarily complex. In fact, for all these experiments one can identify a collective observable (magnetic flux for SQUIDs and center-of-mass trajectory for molecule interference) - which behaves indeed quantum-mechanically. In the end, the types of meso- or macroscopic states for which quantum mechanical behavior has been proved so far have been rather limited. The same goes for statistical properties: while it is often claimed that the Pauli exclusion principle has been tested with a precision of the order of 10^{-26} [13], it should be remembered that such tests have been performed on very specific states. It would be preposterous to try to guess how the new physics would look like: it all depends on what the experiments will reveal. One possibility could be that the problem of quantum-to-classical transition will be clarified. For example we could find a process of spontaneous collapse of these complex many-body wavefunctions onto classical states. Penrose and Diósi [14] have theorized that a process of spontaneous collapse of the wavefunction could exist because of the gravitational self-energy of the object - in other words, the mere property of carrying mass (above a certain critical value) would for example suppress superpositions of the object in spatially distinct states. We suggest that, instead, the wavefunction could collapse above a critical level of complexity. Metaphorically speaking, this level of complexity is a direct reflection of the amount of information the state is carrying, which in turn is directly related to a preparation procedure. This preparation procedure is expressed in classical terms: it is a list of operations we perform in the lab in order to get the state. In this sense, we have no guarantee that Nature has provided us with a physical support that would allow us to distinguish between any two possible lists of such operations, especially when considering how vast is the number of combinations. Entire classes of states could become coalescent and it might be possible that certain states can never be prepared.

A second scenario is that in which, by diligently applying quantum mechanics as we know it, we find out that the states required for quantum computing are indeed extremely unstable under external perturbations, and having these effects under control is not possible with the present techniques; or that, as a direct consequence of quantum mechanics, the inclusion of spurious higher-order effects such as co-tunneling, two-photon processes, *etc.* is in blatant contradiction with the intensities required to produce entanglement at a reasonably high rate and would shave off any advantage of quantum computing. And we are able to show that such considerations can be applied to all the proposed quantum-computing schemes. This would leave us stuck in the epistemological crevasse in which Bohr dragged us already some 80 years ago: there is no way to surpass quantum physics, which not only represents the new physics of quanta but also is a new way - and the only scientifically valid way - of doing science: that is, by declaring meaningless any reference to the reality of properties residing as such in objects, and tying all the statements one is allowed to make about a physical system to a highly qualified specification of the measurement context. This scenario would probably be very disappointing for most practitioners of the field: but physicists are good at dealing with frustration, and most likely the optimists and the very smart will continue to improve the designs, to come up with new error correction ideas and fault-tolerant computing schemes, and to try out other systems as qubits.

On the other hand, even if we will not discover the limits of quantum mechanics, there could still be good physics ahead. Let us assume that it turns out that, due to say decoherence, the states that we want to produce in a quantum computer would inevitably collapse to something else. Examples for such behavior exist: for example, a GHZ state of say N particles (which is a type of highly entangled state) collapses to a trivial state (the ground state of N-1 particles) under loss (or ground-state projection) of a single particle. However, a W-state of N particles collapses to a W-state with N-1 particles under the same type of process. Another interesting case is that of two-mode Fock states (fragmented states) which become phase-coherent only after detecting a few particles. In analogy to what we find when going toward zero Kelvin, new phase transitions and symmetry breaking states could emerge. There might be other nice surprises ahead: for example, to discover that while in principle we should be able to calculate the state onto which the quantum processor gets projected, in practice we find out that this state is very sensitive to the parameters used to describe the decohering effects. This would be similar to chaotic behavior, and it could result in the system switching between complex many-body metastable states - a kind of quantum weather. Also, it is possible that the system would start to self-assemble into states that could, in principle, support some type of functionality or behave in completely unexpected way. This is, what happens, after all, in biology, which is a good illustration of the idea that absence of large-scale regularity could lead to very interesting outcomes (us for example).

If the second scenario were to happen, while we failed indeed to produce something potentially useful for the society, it also means that we have put our finger on something deep which requires explanation. For why would Nature oppose so fiercely to us factorizing numbers? It is fair to assume in this context that Der Alte does not have much interest into hacking our bank accounts or finding out the latest long-range missile strategic game of the military. Then, what is it in the structure of the world that would prevent us from doing calculations such as fast-searching? Does it necessarily have to be like that? Could it be that our mere existence is incompatible with the possibility of performing certain mathematical tasks in this Universe (is the anthropic principle ruling out quantum computing)? Number theory is one of the most difficult branches of mathematics, yet a result

such as Fermat's last theorem does not require more than elementary-school mathematics to formulate. We do not know the answer to simple questions such as what is the distribution of primes amongst the integers - Riemann's hypothesis has not yet been proven. For an outsider, it might look like number theory should be the primary mathematical tool for a physicist: after all, numbers is what we get from experiments. But concepts such as prime numbers, which form the backbone of number theory, have little relevance for a physicist: the numbers that come out of a physics experiment are a string of rational numbers, and mathematically-relevant questions such as countability or the density of rational numbers into the set of reals are either irrelevant or completely buried under instrumentational errors. Physics is about describing the continuous dynamics of point objects and fields in space in space and time, and therefore calculus, differential geometry, group theory, and linear algebra should offer the natural tools for the physicist. But surprising connections between number theory and physics have been discovered [15]. Something tells us that we are just scratching the top of the iceberg here, and the reason for saying so is that these connections seem to occur precisely in topics such as renormalizable field theories, low-dimensional field theories, *etc.*, where (despite the success in comparison with experiments), we have the least intellectual confidence that the concepts we are using are the optimal one. Indeed, summing over Feynman diagrams would probably look to a physics student of the future as conceptually awkward and cumbersome as it looks to us combining motions on epicycles to get the trajectories of the planets in the solar system.

V. FINAL WORDS

It is indeed astonishing how little we understand about deceptively simple concepts such as numbers: we do not know where the building blocks of arithmetics - the primes - come from. Instead, we know that arithmetic cannot be completely and consistently axiomatized and we know that it has deep connections with most of the other branches of mathematics and, inevitably, with physics. We also seem to have uncovered some ways in which quantum mechanics - arguably the most intellectually devastating theory ever produced by humankind - is connected to one of the most elementary mathematical concept we can imagine: that of a number. Counting is surely the first mathematical trick we learn as children, and it would be indeed amazing to discover how much of the construction of the Universe relies on this skill. Maybe, after all [16], in the beginning was the number.

Acknowledgements: The author wishes to acknowledge stimulating discussions with scientists at IQOQI Vienna, during a visit there. This does not imply that they either endorse or they bear any responsibility for the (probably controversial) views presented here.

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

[2] A. M. Steane, Studies in History and Philosophy of Modern Physics **34B**, p. 469 (2003).

[3] A. Peres, Quantum theory: Concepts and Methods, Kluwer Academic Publishers, Dordrecht Netherlands, 1995. p. 373

[4] The author of this essay has heard rumors that a few well-known scientists have expressed doubts that quantum computing can be ever realized. However, he is not aware of any proof or decisive argument in this direction published in the mainstream physics journals.

[5] I am using the word "complexity" in a very general sense, just as the opposite of "accesible/simple to characterize/calculate/produce" - its meaning covers for example high-complexity classes of problems (in the computational sense) and also highly entangled many-particle states.

[6] H. Häffner *et. al.*, Nature **438**, 643 (2005).

[7] One can say that quantum tomography aims at extracting and mapping in a classical format all the information contained in a quantum states, while quantum computing attempts to extract only some information, namely the solution to the problem. In this sense, quantum computing fares better. However, what is worrying is that a quantum computer does have to go through states which require a large amount of classical resources to characterize.

[8] S. Wallentowitz, I.A. Walmsley, and J. H. Eberly, "How big is a quantum computer?", arXiv:quant-ph/0009069.

[9] Eric W. Weisstein, RSA-200 Factored Math-World Headline News, May 10, 2005 (http://mathworld.wolfram.com/news/2005-05-10/rsa-200/).

[10] The record for the lowest temperature ever produced belongs to the laboratory where the author of this essay works: 100 pK. At MIT, temperatures of the order of 500 pK have been obtained in a different system (a Bose-Einstein condensate.)

[11] I take as a gentlemen's agreement that the readers of this essay will be so kind as to not distribute it to any funding agency.

[12] A. J. Leggett, J. Phys. Condens. Matter **14**, R415 (2002).

[13] E. Ramberg and G. A. Snow, Phys. Lett. **B238**, 438 (1990).

[14] L. Diósi, Phys. Lett. A **120**, 377 (1987); R. Penrose, Gen. Relativ. Gravit. **28**, 581 (1996).

[15] For a collection of such results, see *e.g.* http://www.secamlocal.ex.ac.uk/people/staff /mr-watkin/zeta/physics.htm

[16] "In the beginning was the Word, and the Word was with God, and the Word was God", John 1:1.