Is Fault-Tolerant Quantum Computation Really Possible?

M. I. Dyakonov
Laboratoire de Physique Théorique et Astroparticules
Université Montpellier II, France

1. Introduction

The answer that the quantum computing community currently gives to this question is a cheerful "yes". The so-called "threshold" theorem says that, once the error rate per qubit per gate is below a certain value, estimated as $10^{-4}$, indefinitely long quantum computation becomes feasible, even if all of the $10^2-10^5$ qubits involved are subject to relaxation processes, and all the manipulations with qubits are not exact. By active intervention, errors caused by decoherence can be detected and corrected during the computation. Though today we may be several orders of magnitude above the required threshold, quantum engineers may achieve it tomorrow (or in a thousand years). Anyway large-scale quantum computation is possible in principle, and we should work hard to achieve this goal.

The enormous literature devoted to this subject (Google gives 29,300 hits for "fault-tolerant quantum computation") is purely mathematical. It is mostly produced by computer scientists with a limited understanding of physics and a somewhat restricted perception of quantum mechanics as nothing more than unitary transformations in the Hilbert space plus "entanglement". On the other hand, the heavy machinery of the theoretical quantum computation with its specific terminology, lemmas, etc., is not readily accessible to most physicists (including myself). The vast majority of researchers, who start their articles with the standard mantra that the topic is pertinent to quantum computation, do not really understand, nor care, what stands behind the threshold theorem and how quantum error correction is supposed to work. They simply accept these things as a proven justification of their activity.

Meanwhile, even the most ardent proponents of quantum computing recognize today that it is impossible to build a useful machine without implementing efficient error correction. Thus the question in the title is equivalent to asking whether quantum computing is possible altogether.

In a previous publication, I too accepted the threshold theorem but argued that the required enormous precision will not be achieved in any foreseeable future. The purpose of this article, intended for physicists, is to outline the ideas of quantum error correction and take a look at the technical instructions for fault-tolerant quantum computation, first put forward by Shor and elaborated by other mathematicians. It seems that the mathematics behind the threshold theorem is
somewhat detached from the physical reality, and that some flawless elements are inevitably present in the construction. This raises serious doubts about the possibility of large-scale quantum computation, even as a matter of principle.

2. Brief outline of ideas

The idea of quantum computing is to store information in the values of \(2^N\) amplitudes describing the wavefunction of \(N\) two-level systems, called qubits, and to process this information by applying unitary transformations (quantum gates), that change these amplitudes in a very precise and controlled manner, see the clear and interesting review by Steane. The value of \(N\) needed to have a useful machine is estimated as \(10^8 - 10^9\). Even for \(N = 1000\), the number of continuous variables (the complex amplitudes of this grand wavefunction) that we are supposed to control, is \(2^{3000} \approx 10^{100}\). For comparison, the total number of protons in the Universe is only about \(10^{80}\) (give or take a couple of orders of magnitude).

The interest in quantum computing surged after Shor\(^5\) invented his famous algorithm for factoring very large numbers and showed that an ideal quantum computer can solve this problem much faster than a classical computer that would require exponentially time and resources.

Generally, there are many interesting and useful things one could accomplish with ideal machinery, not necessarily quantum. For example, one could become younger by exactly reversing all the velocities of atoms in one's body (and in the immediate vicinity), or write down the full text of all the books in the world in the exact position of a single particle, or store information in the \(10^{30}\) vibrational amplitudes of a cubic centimeter of a solid. Unfortunately, unwanted noise, fluctuations, and inaccuracies of our manipulations impose severe limits to such ambitions. Thus, while the ideas of quantum computing are fascinating and stimulating, the possibility of actually building a quantum computer, even in some distant future, was met from the start with a healthy scepticism.

Unlike the digital computer employing basically the on/off switch, which is stable against small-amplitude noise, the quantum computer is an analog machine where small errors in the values of the continuous amplitudes are bound to accumulate exponentially. So, it seems that a quantum computer of a complexity sufficient to be of any practical interest will never work.

In response to this challenge, Shor\(^7\) and Steane\(^8\) proposed the idea of quantum error correction – an ingenious method designed primarily to overcome the so-called "no cloning" theorem: an unknown quantum state cannot be copied. At first glance, this theorem prevents us from checking for errors in the quantum amplitudes, so that one can correct them. The idea of quantum error correction is to spread the information contained in a logical qubit among several physical qubits and to apply a special operator, which detects errors in physical qubits (the error syndrome) and writes down the result by changing the state of some auxiliary (ancilla) qubits. By measuring the ancilla qubits only, we can see the error in the original quantum state and then correct it (see Section 6).
However, this method assumed that the ancilla qubits, the measurements, and the unitary transformations to be applied, remain ideal. It is said that this type of error correction is not fault-tolerant, whatever this may mean. (If the ancilla qubits are flawless, why not use them in the first place?) The ultimate solution, the fault-tolerant quantum computation, was advanced by Shor\textsuperscript{12} and further developed by other mathematicians, see Refs. 10-14 and references therein. Now, nothing is ideal: all the qubits are subject to noise, measurements may contain errors, and our quantum gates are not perfect. Nevertheless, the threshold theorem says that arbitrarily long quantum computations are possible, so long as the errors are not correlated in space and time and the noise level remains below a certain threshold. In particular, with error correction a single qubit may be stored in memory, i.e. it can be maintained arbitrarily close to its initial state for an indefinitely long time.

This striking statement implies among other things that, once the spin resonance is narrow enough, it can be made arbitrarily narrow by active intervention with imperfect instruments. This contradicts all of our experience in physics. Imagine a pointer that can rotate in a plane around a fixed axis. Fluctuating external fields cause random rotations of the pointer, so that after a certain relaxation time the initial position gets completely forgotten. How can the use of other identical pointers (also subject to random rotations) and some external fields (that cannot be controlled perfectly) make it possible to maintain indefinitely a given pointer close to its initial position!? The answer we get from experts in the field, is that it may work because of quantum mechanics: "We fight entanglement with entanglement"\textsuperscript{15} or, in the words of the Quantum Error Correction Somat by Gottesman:\textsuperscript{11}

\begin{quote}
With group and eigenstate, we've learned to fix
Your quantum errors with our quantum tricks.
\end{quote}

This does look suspicious, because in the physics that we know, quantum-mechanical effects are more susceptible to noise than classical ones. Before going into the details of the proposed fault-tolerant computation, the following section will present a slight divagation relevant to our subject.

3. Capturing a lion in the desert

The scientific folklore knows an anecdote about specialists in various fields proposing their respective methods of capturing a lion in a desert. (For example, the Philosopher says that a captured lion should be defined as one who is separated from us by steel bars. So, let us go into the cage and the lion will be captured). Here, we are concerned with the Mathematician's method:\textsuperscript{15}

The desert $D$ being a separable topological space, it contains a countable subset $S$ that is everywhere dense therein. (For example, the set of points with rational coordinates is eligible as $S$) Therefore, letting $x \in D$ be the point at which the lion is located, we can find a sequence $\{x_n\} \subset S$ with
\[ \lim_{n \to \infty} x_n = x. \] This done, we approach the point \( x \) along the sequence \( \{x_n\} \) and capture the lion.

This method, illustrated in Fig. 1, assumes that the only relevant property of the lion is to be located at a given point in 2D space. Note also that neither time nor what can happen to the lion and the hunter during the process is a point of concern. And finally, it is not specified how the sequence \( \{x_n\} \) should be chosen, nor what the limit as \( n \to \infty \) could mean in practice. These points are left to be elaborated by the practical workers in the field.

Certainly, mathematics is a wonderful thing, both in itself, and as a powerful tool in science and engineering. However, we must be very careful and reluctant in accepting theorems, and especially technical instructions, provided by mathematicians in domains outside pure mathematics. Whenever there is a complicated issue, whether in many-particle physics, climatology, or economics, one can be almost certain that no theorem will be applicable or relevant, because the explicit or implicit underlying assumptions will never hold in reality. The Hunter must first explain to the Mathematician, what a lion looks like.

\[ \forall x \in D, \exists \{x_n\}_{n=1}^{\infty} \subset S \mid \lim_{n \to \infty} x_n = x \]

**Figure 1.** The Mathematician’s method of capturing the lion in the desert.
4. Spin relaxation or decoherence

While the relaxation of two-level systems was thoroughly studied during a large part of the 20th century, and is quite well understood, in the quantum computing literature there is a strong tendency to mystify the relaxation process and make it look as an obscure quantum phenomenon. "The qubit (spin) gets entangled with the environment ..." or "The environment is constantly trying to look at the state of a qubit: a process called decoherence", etc.

In a way, this sophisticated description may be true, however it is not normally quite sufficient to understand spin relaxation as a result of the action of a time-dependent Hamiltonian $H(t) = A(t)\sigma$, where $A(t)$ is a random vector function, and $\sigma$ are Pauli matrices. In simple words, the spin continuously performs precession around magnetic fields that fluctuate in time. In most cases these magnetic fields are not real, but rather effectively induced by some interactions. A randomly fluctuating field is characterized by its correlation time $t_c$ and by the average angle of spin precession $\alpha$ during the time $t_c$. For the most frequent case when $\alpha \ll 1$, the spin vector experiences a slow angular diffusion. The RMS angle after a time $\tau \gg t_c$ is $\alpha = \alpha(\sqrt{t_c}\tau)^{1/2}$. Hence the relaxation time $\tau$ is given by $\tau \sim t_c/\alpha^2$. If one chooses a time step $t_0$, such that $t_c \ll t_0 \ll \tau/\alpha^2$, it can be safely assumed that $\tau \ll 1$, and that rotations during successive time steps are not correlated.

These random rotations persist continuously for all the qubits inside the quantum computer. It is important to understand that the wavefunction describing an arbitrary state of $N$ qubits will deteriorate much faster than any individual qubit. The reason is that this wavefunction

$$\Psi = A_0|000..00\rangle + A_1|000..01\rangle + A_2|000..10\rangle + ... + A_{2^n-1}|111...11\rangle$$

describes complicated correlations between the $N$ qubits, and correlations always decay more rapidly. For simplicity, suppose that all qubits are subject to random and uncorrelated rotations around the $z$ axis only. Then during one step the state of the $j$th qubit will change accordingly to the rule: $|0_j\rangle + |1_j\rangle \rightarrow \exp(i\theta_j)|1\rangle$, where $\theta_j$ is the random rotation angle for this qubit. Then the amplitudes $A$ will acquire phases $\exp(\theta_j)$, where the sum goes over all qubits that are in the state $1_j$ in a given term of $\Psi$. The typical RMS value of this phase is $\sim eN^{1/2}$. Thus the time it takes for unwanted phase differences between the amplitudes $A$ to become large is $\sim N$ times shorter than the relaxation time for an individual qubit.

For this reason, it seems that if we choose the time step so that $\tau^2 = 10^6$ (the most cautious of existing estimates for the noise threshold), but the quantum state contains $10^9$ qubits, then the computer is likely to crash during a single time step. I am unaware of anybody discussing this problem.

5. Quantum computation with decoherence-free subspaces

This is a flourishing and respectable branch of quantum computing mathematics (Google gives 24800 hits for "decoherence-free subspaces"). The idea is that there
may exist some special symmetry of the relaxation processes, due to which certain many-qubit states do not relax at all. (The simplest model is to consider a relaxation process, in which all the qubits are rotated collectively.) It is then discussed how information can be hidden in this decoherence-free subspace, and what would be the best way to proceed with quantum computation. The conditions for the existence of such subspaces are given\textsuperscript{17} by the following:

\textbf{Theorem 4.} If no special assumptions are made on the coefficient matrix \(a_{ef}\) [Eq. (8)] and on the initial conditions \(p_0\) [Eq. (13)] then a necessary and sufficient condition for a subspace \(\mathcal{H} = \text{Span}\{\{k\} : k = -\alpha \cdot k\}\) to be decoherence-free is that all the basis states \(\{k\}\) are degenerate eigenstates of all Lindblad operators \(\{F_{ij}\}\).

\[ F_{ij} \{k\} = c_{ij} \{k\} + \sigma_{ij} \{k\}. \]

This gives the reader an idea of what the quantum computing literature looks like.

Although it is not difficult to construct artificial models with special symmetries, my guess is that in any real situation the Lindblad operators do not have common eigenstates at all. Obviously, the simplest way to fight noise is to suppose that at least \textit{something is ideal} (noiseless). Unfortunately, this is not what happens in the real world.

6. Quantum error correction by encoding

Below is a simplified example\textsuperscript{12,18} of quantum error correction using \textit{encoding}. The simplification results from the assumption that the only errors allowed are rotations around the \(y\) axis, described by the matrix \(E = \cos(\theta/2)I + i\sin(\theta/2)\sigma_y\), where \(I\) is the unit matrix and \(\sigma_y\) is the Pauli matrix. For small rotation angles \(\theta = 2\pi \ll 1\), this gives \(E = I - i\sigma_y\). In the case when these are the only possible errors for individual qubits, it is sufficient to encode the logical \(|0\rangle\) and \(|1\rangle\) by three physical qubits: \(|0\rangle \rightarrow |000\rangle, \quad |1\rangle \rightarrow |111\rangle\). The encoding procedure requires the following steps:

1) The general state of a qubit, \(a|0\rangle + b|1\rangle\), is encoded as \(\psi = a|000\rangle + b|111\rangle\). Suppose that the three physical qubits experience small and uncorrelated rotations \(F_1, F_2,\) and \(F_3\). Let us see how the initial state can be recovered. For example, suppose there is an error in the second qubit only. The wavefunction becomes:

\[ F_{2e} = [a|000\rangle + b|111\rangle] \quad i\sigma_y[a|010\rangle + b|101\rangle]. \]

2) We now mechanically add 3 auxiliary ancilla qubits, obtaining the state:

\[ E_{3e} = [a|000\rangle + b|111\rangle] \quad |000\rangle \quad i\sigma_y[a|010\rangle + b|101\rangle] |000\rangle. \]

3) Next we introduce the syndrome extraction operator \(S\), defined as follows:

\[ S(000) |000\rangle = |000\rangle |000\rangle, \quad S(111) |000\rangle = |111\rangle |000\rangle, \]

\[ S(000) |000\rangle = |000\rangle |000\rangle, \quad S(111) |000\rangle = |111\rangle |000\rangle, \]

\[ S(000) |000\rangle = |000\rangle |000\rangle, \quad S(111) |000\rangle = |111\rangle |000\rangle, \]
The first 3 qubits, containing the data, are left intact. If one of them is flipped, then the ancilla bits are changed accordingly. The operator \( S \) writes down the error into the ancilla, allowing us to identify the error location. Now:

\[
SE_{2} = [a|000\rangle + b|111\rangle]|000\rangle - i\varepsilon [a|010\rangle + b|011\rangle]|111\rangle.
\]

4) Finally, we measure the three ancilla qubits. If we get \( |000\rangle \), then we do nothing, since this result shows that the state automatically has been reduced to the initial state \( \psi = a|000\rangle + b|111\rangle \). If (with a small probability equal to \( \varepsilon^2 \)) we obtain the result \( |101\rangle \), then we know that there is an error in the second qubit, and that the state of the remaining (data) qubits is \( a|010\rangle + b|101\rangle \). This error is easily corrected by applying the operator \( \sigma_x \) to the second qubit. Thus, in both cases we recover the original state \( \psi = a|000\rangle + b|111\rangle \), a 0; \( |b| \rangle \)!

The method works equally well if all three data qubits have errors, provided that the second-order terms proportional to \( \sigma_x \sigma_x \sigma_x \) and \( \sigma_x \sigma_z \) in the \( E_{12} E_{23} \) wavefunction can be neglected. This is justified by the small probability for the admixture of the corresponding states, proportional to \( \varepsilon^2 \) (compared to the \( \varepsilon^2 \) probability of one-qubit errors). However, this method does work if errors in different qubits are correlated, i.e., if there is an admixture of states with two errors with an amplitude \( \varepsilon \) rather than \( \varepsilon^2 \). This is why the requirement that errors are uncorrelated is crucial.

There is, indeed, a remarkable "quantum trick": here, the measurement of the ancilla qubits automatically reduces the wavefunction representing a large superposition of states to only one of its terms! Because of this, knowing how to correct a bit-flip \((|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle)\), referred to as "first error", we can also correct "slow errors", \( E - I - i\varepsilon \sigma_x \), for arbitrary (but small) values of \( \varepsilon \). This property is called "digitization of noise".

To correct general one-qubit errors a more sophisticated encoding \(^7\) \(^6\) by a greater numbers of qubits is needed. For example, the logical \( |0\rangle \) might be encoded as: \( |0\rangle \rightarrow (1/\sqrt{8}) [000|000\rangle + 000|111\rangle + 011|001\rangle + 011|100\rangle + 010|011\rangle + 010|100\rangle + 111|001\rangle - 111|100\rangle] \). However, the principle of error correction is the same. It is believed that it may be advantageous to use concatenated encoding, in which each encoding qubit should be further encoded in the same manner, and so on... It is supposed that the future quantum engineer\(^9\) might wish to encode the logical \( |0\rangle \) and \( |1\rangle \) by complicated superpositions of the states of \( 7^4 = 343 \) physical qubits!

What if we apply the same method of error correction not just to one qubit, but to some \( N \)-qubit state? Making exactly the same assumptions, we encode each of the \( N \) logical qubits by three physical ones, add an appropriate number of ancilla qubits, and proceed in the same way as above. Then, in accordance with the
remark at the end of Section 4, the condition for the method to work will be $Ne^2 << 1$, not simply $e^2 << 1$. Indeed, after applying the syndrome extraction operator, the number of one-qubit error terms with probabilities $e^2$ is $N$, while the number of two-qubit error terms with probabilities $e^2$ is $N(N-1)/2$. In order for the method to work, the total probability of obtaining any two-error state during measurements should be small, which is true when $Ne^2 << 1$.

7. The imperfect two-qubit gate

For quantum computation one needs to apply one-qubit gates, but also two-qubit and three-qubit gates. Application of two-qubit gates is necessary from the outset to perform the first step, encoding. The problem is not only that individual qubits are subject to relaxation, as described in Section 4, but also that the quantum gates are also not perfect, because neither the Hamiltonian that should be switched on at the desired moment, nor the duration of its action can be controlled exactly. While an error in a one-qubit gate can be simply added to the random rotations that exist anyway, errors in two-qubit gates requires more care.

We should first decide what an imperfect two-qubit gate is. It seems that the generally accepted model is the following: "For the error model in our quantum gates, we assume that with some probability $p$, the gate produces unreliable output, and with probability $1-p$, the gate works perfectly."

A more detailed description also specifies the exact meaning of an unreliable output: "The failure of a two-qubit gate is modeled as a process where, with probability $1-\gamma_2$, no change takes place before the gate, and with equal probabilities $\gamma_2/2$ one of the $15$ possible single- or two-qubit failures take place."

In other words, the faulty gate is supposed to act as an ideal one (with high probability) or to act as an ideal one preceded by uncorrelated errors in the two qubits involved (with low probability). In reality, there will always be some more or less narrow probability distribution around their desired values of the $16$ real parameters defining the unitary transformation. Never, under any circumstances, will an ideal gate exist. The crucial difference is that any real gate will introduce correlated errors of the two qubits. Such correlated errors are not correctable within the error-correcting scheme described in Section 6.

Here is a more sophisticated model: "The noise model we will consider can be formulated in terms of a time-dependent Hamiltonian $H$ that governs the joint evolution of the system and the bath. We may express $H$ as $H = H_s + H_b + H_{sb}$, where $H_s$ is the time-dependent Hamiltonian of the system that realizes the ideal quantum circuit, $H_b$ is the arbitrary Hamiltonian of the bath, and $H_{sb}$ couples the system to the bath."

This is a quite general approach, especially if the arbitrary (7) Hamiltonian of the "bath" also describes the electronic equipment and the quantum engineer himself. However, in reality there is no such thing as a "time-dependent Hamiltonian of the system that realizes the ideal quantum circuit", just as there is no such thing as square root of 2 with all the infinite number of its digits. True,
such abstractions are routinely used in mathematics and theoretical physics. However the whole issue at hand is to understand whether the noisy nature of the real Hamiltonian does, or does not, make it possible to realize anything sufficiently close to the "ideal quantum circuit". Thus, it could well happen that the supposed success of fault-tolerant quantum computation schemes is entirely due to the uncontrolled use of innocent-looking abstractions and models (see Section 3). A very careful analysis is needed to understand the true consequences of any simplifications of this kind.

Another implicit assumption, which may be not quite innocent, is that the gates are infinitely fast. In fact, new errors may appear during error correction.21

8. The prescription for fault-tolerant quantum computation

The error correction scheme, briefly described in Section 6, assumes that encoding, syndrome extraction, and recovery are all ideal operations, that ancilla qubits are error-free, and that measurements are exact. Fault-tolerant methods are based on the same idea, but are supposed to work even if all these unrealistic assumptions (making, in fact, error correction unnecessary) are lifted. The full instructions9,13 are extraordinarily complicated, details that may be important are often omitted, and the statements are not always quite clear. The basic ideas are as follows.

1) There exists a universal set of three gates, sufficient for quantum computation. "The proof of this involves showing that these gates can be combined to produce a set of gates dense in the set of 3-qubit gates" (see Section 3). In other words, any gate can be approximated to any desired accuracy by application of a large enough number of the three special gates belonging to the universal set.

2) These three gates can be used in a fault-tolerant manner, which means in such a way that only uncorrelated, and thus correctable, errors are produced. Fault-tolerance is achieved by encoding the logical qubits, using specially prepared states of ancilla qubits, and some rules designed to avoid error propagation. Thus application of a single 3-qubit gate fault-tolerantly amounts to a mini-quantum computation with thousands of elementary operations.

3) The encoding itself cannot be done fault-tolerantly.10 "Therefore, we should carry out a measurement that checks that the encoding has been done correctly. Of course, the verification itself may be erroneous, so we must repeat the verification a few times before we have sufficient confidence that the encoding was correct." A similar prescription concerns ancilla states:11 "However, the process of creating the ancilla blocks may introduce correlated errors, and if those errors enter the data, it will be a serious problem. Therefore, we must also verify the ancilla blocks to eliminate such correlated errors. Precisely how we do this is not important for the discussion below, but it will certainly involve a
It is recommended that one construct auxiliary "cat states": $(1/\sqrt{2})(|00\ldots00\rangle + |11\ldots11\rangle)$, where the size of the cat depends on the number of qubits used for encoding. Again, since there may be (one might better say: there always will be) errors in the cat state, it must be verified before being used.

4) Some operations should be repeated. If we mistakenly accept the measured syndrome and act accordingly, we will cause further damage instead of correcting the error. Therefore, it is important to be highly confident that the syndrome measurement is correct before we perform the recovery. To achieve sufficient confidence, we must repeat the syndrome measurement several times.

5) All these precautions still do not guarantee that the computer will not crash. However, what matters is the probability of crash. Once this probability is small enough, which is supposed to happen at a low enough noise rate, we can repeat the whole quantum calculation many times to get reliable results. By estimating the crash probability, one obtains an estimate for the threshold noise level.

A detailed description of the fault-tolerant computation rules can be found in Ref. 10. I do not find this description clear and/or convincing enough. Taking into account the continuous nature of random qubit rotation and gate inaccuracies, even with all the verifications and repetitions, there seems no way to avoid small admixtures of unwanted states.

In fact, the pure spin-up state can never exist in reality (one reason is that we never know the exact direction of the z axis). Similarly, in the classical world, one can never have a pointer pointing exactly in the z direction. Generally, no desired state can ever be achieved exactly. Rather, whatever we do, we will always have an admixture of unwanted states, more or less rich. One can never have an exact $|0\rangle + |1\rangle/\sqrt{2}$ state, let alone more complicated "cat" states like $(|000000\rangle + |111111\rangle)/\sqrt{2}$. Such abstractions must be used with extreme caution when discussing the role of errors and inaccuracies.

When the small undetected and unknown admixture of unwanted states together with the "useful" state is fed into the subsequent stages of the quantum network, it is most likely that the error will grow exponentially in time. Accordingly, the crash time will depend only logarithmically on the initial error value. This is what happens when one tries to reverse the evolution of a gas of hard balls. At a given moment one reverses the direction of all the velocities, but years later the gas will never return to its initial state (even in computer simulation, let alone reality). The reason is that however small the initial (and subsequent) computer errors are, they will increase exponentially (the Lyapunov exponent). It is a great illusion to think that things are different in quantum mechanics.

Related to this, there is another persistent misunderstanding of quantum mechanics that plagues the quantum error correction literature. Using the classical language, it is said that the qubit "decoheres" with probability $p = \sin^2\theta$, instead of saying that the qubit is in the state $\psi = \cos\theta|0\rangle + \sin\theta|1\rangle$. This makes only a
semantic difference if we are going to immediately measure the qubit, since the probability of finding it in a state $|1\rangle$ is indeed $p$. However, this language becomes completely wrong if we consider some further evolution of our qubit described by some unitary matrix $R$. The common thinking (applied, for example, to estimating the noise threshold) is that we will have the state $R|0\rangle$ with probability $1-p$, and the state $R|1\rangle$ with probability $p$. In reality, we will have the state $R\psi$, which is not the same thing. The former line of reasoning gives the probability of measuring $0$ in the final state as $(1-p)|\langle 0|R|\psi\rangle|^2 - p|\langle 1|R|\psi\rangle|^2$, while the latter (and correct) one will give $|\langle 0|R|\psi\rangle|^2$, and these results are very different. As an exercise, the reader can take for $R$ a rotation of our qubit around the $x$ axis by some angle and compare the results. A quantum-mechanical surprise lies in store. In quantum mechanics, one cannot calculate probabilities by considering what happens to ideal states. Instead, one must look at the evolution of real states, which always differ from ideal ones by some admixture of unwanted states.

Another important point is that the finite time required to do anything at all is usually not taken into account (see Section 3). According to the procedure described in Section 6, measuring the syndrome and obtaining $(000)$ indicates the correct state that requires no further action. In fact, while we were making our measurements, the data qubits have experienced their random rotations. And this will happen no matter how many times we repeat the syndrome measurement. So why bother with error correction?

Alicki has made a mathematical analysis of the consequences of finite gate duration. I am not in a position to check his math, but I like his result: the fidelity exponentially decreases in time. He writes: "... unfortunately, the success of existing error correction procedures is due to the discrete in time modeling of quantum evolution. In physical terms, discrete models correspond to unphysical infinitely fast gates."

9. Designing perpetual motion machines of the second kind

This is certainly not equivalent to achieving fault-tolerant quantum computation, during which we will put some energy into the system by applying external fields and performing measurements.

However there is a certain similarity between the two problems in the sense that what we are trying to do is to maintain a reversible evolution of a large system with many degrees of freedom in the presence of noise and using noisy devices. People who have had the opportunity of examining proposals for perpetual motion machines, know their basic principle: insert at least one ideal (i.e. not sensitive to thermal fluctuations) element somewhere deep within a complicated construction. Finding and identifying such an ideal element may be a daunting task.

Naively, one starts by proposing a valve that preferentially lets through only fast molecules. Next, one understands that the valve itself is "noisy," so that it will not work as expected. However, if one adopts a noise model in which the valve is faulty with a probability $p$ but works perfectly with a probability $(1-p)$, or makes a
sophisticated construction involving many valves connected by wheels and springs, and if just one of these elements is considered as ideal (or even working perfectly with some probability), one can immediately arrive at the conclusion that a perpetual motion machine feeding on thermal energy is possible.

This lesson should make us extremely vigilant to the explicit or implicit presence of ideal elements within the theoretical error-correcting schemes.

10. Challenge

After ten years of doing mathematics devoted to fault-tolerant quantum computation, maybe the time is ripe for a simple numerical test. Let us focus on the simplest, almost "trivial" task of storing just one qubit and let us verify the statement that its initial state can be maintained indefinitely in the presence of low-amplitude noise. Take, for example, an initial state \((0 + \ii) \sqrt{2} - \text{a spin pointing in the x direction.}\)

Assume that all qubits experience continuous random uncorrelated rotations, the RMS rotation angle being small during a single time step. As a further simplification, one could restrict the random rotations to the \(xy\) plane only. The two- and three-qubit gates have a narrow probability distribution for all of the parameters, defining the corresponding unitary transformation around their desired values. Errors in successive gates are not correlated. We have a refrigerator containing an unlimited number of ancilla qubits in the pure state \(|0\). Once the ancillas are out of the refrigerator, they become subject to the same random rotations. Measurements involve errors: when the state \(\psi \equiv (0 + \ii) \sqrt{2}\) is measured with the result \(0\), the quantum state is not reduced to exactly \((0\), but rather to \((0 \pm \epsilon) \sqrt{2}\) with some unknown, but hopefully small \(\epsilon\). Allocate a certain time for measurements and duration of gates and take into account that all qubits continue to be rotated randomly during this time. This simple model cannot be relaxed further without entering an imaginary world where something is ideal.

Presumably, to maintain our single qubit close to its initial state, a certain sequence of operations (with possible branching depending on the result of intermediate measurements) should be applied periodically. *Provide a complete list of these elementary operations*, so that anybody can use a PC to check whether qubit storage really works. The future quantum engineer will certainly need such a list! If it works, this demonstration would be a convincing, though partial, proof that the idea of fault-tolerant quantum computation is sound.

Steane\(^12\) undertook a thorough numerical simulation of error propagation in a quantum computer with results confirming the threshold theorem. Since an exact simulation of quantum computing on a classical computer is impossible, he used a partly phenomenological model, based on the (questionable) assumption that "it is sufficient to keep track of the propagation of errors, rather than the evolution of the complete computer state". Since the real errors always consist in admixtures of unwanted states, considering the quantum evolution of the complete computer state seems to be the only way to respect quantum mechanics (see Section 8).
The task of maintaining a single qubit in memory is much simpler and, once the list of required operations is provided, it hopefully can be simulated in a straightforward manner. I predict that the result will be negative.

11. Conclusions

It is premature to accept the threshold theorem as a proven result. The state of a quantum computer is described by the monstrous wavefunction with its $10^{\varphi^N}$ complex amplitudes, all of which are continuously changing variables. If left alone, this wavefunction will completely deteriorate during $1/N$ of the relaxation time of an individual qubit, where $N \approx 10^2 - 10^6$ is the number of qubits within the computer. It is absolutely incredible, that by applying external fields, which cannot be calibrated perfectly, doing imperfect measurements, and using converging sequences of "fault-tolerant", but imperfect, gates from the universal set, one can continuously repair this wavefunction, protecting it from the random drift of its $10^{\varphi^N}$ amplitudes, and moreover make these amplitudes change in a precise and regular manner needed for quantum computations. And all of this on a time scale greatly exceeding the typical relaxation time of a single qubit.

The existing prescriptions for fault-tolerant computation are rather vague, and the exact underlying assumptions are not always clear. There are several subtle issues, some of which are discussed in this chapter, that should be examined more closely. It seems likely that the (theoretical) success of fault-tolerant computation is due not so much to "quantum tricks", but rather to the backdoor introduction of ideal (flawless) elements in an extremely complicated construction. Previously, this view was expressed by Kak.24

It would be useful to check whether the fault-tolerant methods really work by numerically simulating quantum evolution during the proposed recovery procedures for a single qubit using a realistic noise model that does not contain any ideal elements.

References


15. I thank K. M. Dyakonov for providing the following text and E. M. Diakonova for drawing Figure 1.
16. Somebody has proved a theorem concerning the existence of bound states for the one-dimensional Schrödinger equation. The surprise comes for repulsive potentials $U(x) = -Ax^2$: it is proved that for $n = 4, 6, \ldots$ bound states always exist. The reader might be interested to find out (a) why this theorem is true; (b) what is its physical meaning; and (c) why it is irrelevant to the real world.
19. The future quantum engineer is a mythical personage, who will not only develop and implement the hardware for the future quantum computer, but also design the sequence of the necessary operations based on the ideas presented in Refs. 9, 14 (see Ref. 1 for the job description).


23. Because of this similarity, it is quite probable that the design and the theory of such machines will become the next hot topic, especially if a good name (beginning with the magic word "quantum") for this activity can be invented.