How Quantum Computers Can Fail

Gil Kalai[*]

Hebrew University of Jerusalem and Yale University

September 4, 2006

Abstract

We propose and discuss two postulates on the nature of errors in highly correlated noisy physical stochastic systems. The first postulate asserts that errors for a pair of substantially correlated elements are themselves substantially correlated. The second postulate asserts that in a noisy system with many highly correlated elements there will be a strong effect of error synchronization. These postulates appear to be damaging for quantum computers.

[*] Research supported in part by an NSF grant, by an ISF Bikura grant, and by a BSF grant. I am grateful to Dorit Aharonov, Michael Ben-Or, Greg Kuperberg and John Preskill for fruitful discussions and to many colleagues for helpful comments.

1 Quantum computers and the threshold theorem

Quantum computers are hypothetical devices based on quantum physics. A formal definition of quantum computers was pioneered by Deutsch [1], who also realized that they can outperform classical computation. The idea of a quantum computer can be traced back to works by Feynman, Manin, and others, and this development is also related to reversible computation and connections between computation and physics that were studied by Bennett in the 1970s. Perhaps the most important result in this field and certainly a major turning point was Shor's discovery [2] of a polynomial quantum algorithm for factorization. The notion of a quantum computer along with the associated complexity class BQP is an exciting gift from physics to mathematics and theoretical computer science, and has generated a large body of research. Quantum computation is also a source of new, deep, and unifying questions in various areas of experimental and theoretical physics. For background on quantum computing, see Nielsen and Chuang's book [3].

Of course, a major question is whether quantum computers are feasible. An early critique of quantum computation (put forward in the mid-90s by Unruh, Landauer, and others) concerned the matter of noise:

[P0] The postulate of noise: Quantum systems are noisy.

A major step in showing that noise can be handled was the discovery by Shor [4] and Steane [5] of quantum error-correcting codes. The hypothesis of fault-tolerant quantum computation (FTQC) was supported in the mid-90s by the "threshold theorem" [6, 7, 8, 9], which asserts that under certain natural assumptions of statistical independence on the noise, if the rate of noise (the amount of noise per step of the computer) is not too large, then

FTQC is possible. It was also proved that high-rate noise is an obstruction to FTQC. Several other crucial requirements for fault tolerance were also described in [11, 12].

The study of quantum error-correction and its limitations, as well as of various approaches to fault-tolerant quantum computation, is extensive and beautiful; see, e.g., [13, 14, 15, 16, 10]. Concerns about noise models with statistical dependence are mentioned in several places, e.g., [17, 18]. Specific models of noise that may be problematic for quantum error-correction are studied in [19]. Current FTQC methods apply even to more general models of noise than those first considered, which allow various forms of time- and space-statistical dependence; see [20, 21, 22].

The basic conjecture of this paper is that noisy highly correlated data cannot be stored or manipulated. This applies to both the quantum and classical cases — but note that in the classical case correlations do not increase the computational power. When we run a randomized computer program, the random bits can be sampled once they are created, and it gives no computational advantage in the classical case to physically maintain highly correlated data.

2 Noise and fault tolerance

The postulate of noise is essentially a hypothesis about approximations. The state of a quantum computer can be prescribed only up to a certain error. For FTQC there is an important additional assumption on the noise, namely on the nature of this approximation. The assumption is that the noise is "local." This condition asserts that the way in which the state of the computer changes between computer steps is statistically independent, for different qubits. We will refer to such changes as "qubit errors." In addition, the gates which carry the computation itself are not perfect. We can suppose that every such gate involves at most two qubits and that the gate's imperfection can have an arbitrary form, so the errors (referred to as “gate errors”) created on the two qubits involved in a gate can be statistically dependent. (Of course, qubit errors and gate errors propagate along the computation and handling this is a main difficulty in fault tolerance.)

The basic picture we can have of a noisy computer is that at any time during the computation we can approximate the state of each qubit only up to some small error term ϵ. Nevertheless, under the assumptions concerning the errors mentioned above, computation is possible. The noisy physical qubits allow the introduction of logical “protected” qubits which are essentially noiseless.

The close analogy between the classical and the quantum cases for error correction and fault tolerance is very useful. For our purposes, a good way to understand the notions of quantum error-correction and fault tolerance is to draw the line not between classical and quantum information but between deterministic information (or even stochastic information where the elements are statistically independent) and stochastic highly correlated information (both classic and quantum). Thus, while the state of a digital computer having n bits is a string of length n of zeros and ones, in the (classical) stochastic version, the state is going to be a (classical) probability distribution on all such strings.

Quantum computers are similar to these (hypothetical) stochastic classical computers and they work on qubits (say n of them). The state of a single qubit q is described by a unit vector $u = a|0> + b|1>$ in a two-dimensional complex space U_q. (The symbols $|0>$ and $|1>$ can be thought of as representing two basis elements in U_q.) We can think about the qubit q as representing $'0'$ with probability $|a|^2$ and $'1'$ with probability $|b|^2$. The state of the entire computer is a unit vector in the 2^n-dimensional tensor product of these vector spaces U_q's for the individual qubits. The state of the computer thus represents a probability distribution on the 2^n strings of length n of zeros and ones. The evolution of the quantum computer is via "gates". Each gate g operates on k qubits, and we can assume $k \leq 2$. Every such gate represents a unitary operator on U_g, the (2^k-dimensional) tensor product of the spaces that correspond to these k qubits.

A simple (rather special) example of noise to keep in mind is that all qubit errors are independent random unitary operators for the individual qubits, and all gate errors are random unitary operators on the spaces U_g. If these errors are small (namely, if all these operators are sufficiently close to the identity), the threshold theorem will apply.

A main insight of quantum error-correction is that errors affecting a substantial but small fraction of — even highly correlated – bits/qubits can be handled. (For this, basic linearity properties of probability theory as well as of quantum physics are crucial.) Errors that exceed, with substantial probabilities, the capacity of the error-corrector are problematic. Under the independence assumptions of the threshold theorems, if the rate of errors is small the probability for exceeding the capacity of the error-corrector is extremely small. The crux of the matter is whether independent (or almost independent) errors on highly correlated elements is a possible or even a physically meaningful notion.

3 Noisy stochastic correlated physical systems

3.1 The postulate of noisy correlated pairs

The purpose of this section is to propose and discuss the following postulate:

[P1] In any noisy physical system, the errors for a pair of elements that are substantially statistically dependent are themselves substantially statistically dependent.

In particular, for quantum computers[1] this postulate reads:

[P1] In a quantum computer, the errors for a pair of substantially correlated qubits are substantially correlated.

Another way to put Postulate [P1] is: noisy correlated elements cannot be approximated up to almost independent error terms: if we cannot have an approximation better than a certain error rate for each of two correlated elements, then an uncorrelated or almost uncorrelated approximation is likewise impossible.

Remarks:

1. **Real-life examples: The weather and the stock market.** We can discuss Postulate [P1] for cases of (classical) stochastic systems with highly correlated elements. I am not aware of a case of a natural system with stochastic highly correlated elements that admits an approximation up to an "almost independent" error term. This is the kind of approximation required for fault-tolerant quantum computation.

[1] Our conjectures themselves come in (highly correlated) pairs. Each conjecture is formulated first for general noisy physical systems and then specified to quantum computers that are physical devices able to maintain and manipulate highly entangled qubits.

Can we expect to estimate the distribution of prices of two very correlated stocks in the stock market up to an error distribution that is almost independent?

Or take, for example, the weather. Suppose you wish to forecast the probabilities for rain in twenty nearby locations. We suppose these probabilities will be strongly dependent. Can we expect to have a forecast that is off by a substantial error that is almost statistically independent for the different locations?

To make this question a little more formal, consider not how accurately a weather forecast predicts the weather, but rather how it predicts (or differs from) a later weather forecast. Let $\mathcal{D}$ be the distribution that represents the best forecast we can give for the rain probabilities at time T from the data we have at time $T-1$. Let $\mathcal{D}'$ be the best forecast from data we have at time $T-1-t$. Suppose that $\mathcal{D}$ is highly correlated. Postulate [P1] asserts that we cannot expect that the difference $\mathcal{D}-\mathcal{D}'$ will be almost statistically independent for two locations where $\mathcal{D}$ itself is substantially correlated.

2. **The threshold theorem and pair purification.** The threshold theorem which allows FTQC has various remarkable applications, but our postulate can be regarded as challenging its simplest non-trivial consequence. The assumptions of the threshold theorem allow the errors on a pair of qubits involved in a gate to be statistically dependent. In other words, the outcome of a gate acting on a pair of qubits prescribes the position of the two qubits only up to an error that is allowed to exhibit an arbitrary form of correlation. The process of fault tolerance allows us to reach pairs of entangled qubits that, while still being noisy, have errors that are almost independent. This "purifying" nature of fault tolerance for quantum computation is arguably an element we do not find in fault tolerance for deterministic computation.

3. **Positive correlations for errors.** Consider a noisy classical computer on n bits and suppose that the overall error is given by taking the XOR of the n bits in the computer with a randomly chosen string e of n bits according to a probability distribution $\mathcal{E}$. Suppose that for every bit, the error probability is 1/1000. If the errors are independent then the probability that e will have $n/500$, say, error is very tiny as n grows. Positive correlations between the errors for every (or most) pairs of bits will change this picture. For example, if for every two bits the probability that for e both these bits are 1 is around 1/50,000 (rather than 10^{-6}), then there will be a substantial probability that more than $n/100$ bits will be "hit" by the error. (The same conclusion will apply if for every triple of bits the probability that they will all be hit is, say, 10^{-7} rather than 10^{-9}.) This effect of positive correlation for errors is the basis for Postulate [P2] below.

4. **Leaks of information.** Rather than talking about errors and noise we can talk about information "leaked" from our physical systems to the outside world. For quantum computers leaking of information automatically amounts to noise and thus a strong form of Postulate [P1] for quantum computers is:

[P1'] For a noisy quantum computer, information leaks for two substantially correlated qubits have a substantial positive correlation.

For general stochastic systems [P1'] reads:

[P1'] In any noisy physical system, the information leaks concerning the states of two elements that are substantially statistically dependent, have a substantial positive correlation.

Postulate [P1'] seems natural for systems where correlations are gradually created and information is gradually leaked. The central question is whether such an effect can be diminished via error correction.

3.2 The postulate of error synchronization

Suppose we have an error rate of ϵ. The assumptions of the various threshold theorems (and other proposed methods for quantum fault-tolerance) imply that the probability of a proportion of δ qubits being "hit" is exponentially small (in the number of bits/qubits) when δ exceeds ϵ. Error synchronization refers to an opposite scenario: there will be a substantial probability of a large fraction of qubits being hit.

[P2] In any noisy physical system with many substantially correlated elements there will be a strong effect of spontaneous error-synchronization.

[P2] In any quantum computer at a highly entangled state there will be a strong effect of spontaneous error-synchronization.

As remarked above, error synchronization is expected for a large system when the errors (or information leaks) are positively correlated. An even stronger form of error synchronization is considered in [23], where formal definitions for the quantum case can be found.

Remarks:

1. **Empiric.** Postulates [P1] and [P2] can be tested, in principle, for quantum computers with a small number of qubits (10-20). If such devices where the qubits themselves are sufficiently stable are still well down the road, they are still expected long before the superior complexity power of quantum computers kicks in.

A rigorous form of [P1] can be suggested as a benchmark for quantum-computer engineers: To construct pairs of noisy entangled qubits with almost independent error-terms.

2. **Spontaneous synchronization for highly correlated systems.** The idea that for the evolution of highly correlated systems changes tend

to be synchronized, so that we may witness rapid changes affecting large portions of the system (between long periods of relative calm), is appealing and may be related to other matters like sharp threshold phenomena and phase transition, the theory of evolution, the evolution of scientific thought, and so on.[2] We can examine the possibility of error synchronization for the examples considered above. Can we expect synchronized errors for weather forecasts? Can we expect stock prices, even in short time scales, to exhibit substantial probabilities for changes affecting a large proportion of stocks? This matter is also related to the issue of pattern formation for correlated systems.

3. **Error synchronization and the concentration of measure phenomenon.** A mathematical reason to find spontaneous synchronization of errors an appealing possibility is that this is what a "random" random noise looks like. Talking about a random form of noise is easier in the quantum context. If you prescribe the noise rate and consider the noise as a random (say unitary) operator (conditioning on the given noise rate), you will see a perfect form of synchronization for the errors, and this property will be violated with extremely low probability.

Random unitary operators with a given noise rate are *not* a realistic form of noise. The qubits in a quantum computer are expected to be quite isolated, so that the errors are described by a "locally defined" process (namely, a process (stochastically) generated by operations on a small number of qubits at a time) — similar to the (noiseless) evolution described by quantum computation itself.

[2] This idea is conveyed in the Hebrew proverb "When troubles come they come together," the English "It never rains but it pours," and the Russian : "When trouble comes, open the door!"

While random unitary operators with prescribed error rate appear to be unapproachable by any process of a "local" nature, their statistical properties may well hold for such stochastic processes describing the errors. The fact that perfect error-synchronization is the "generic" form of noise suggests that stochastic processes describing the noise will approach this "generic" behavior unless they have good reason not to. (One obstruction to error synchronization, pointed out by Greg Kuperberg, is time independence.)

4. **Correcting highly synchronized errors.** An observation that complements the discussion so far is that synchronized errors that are unbiased can be corrected to produce noiseless deterministic bits. Suppose we have a situation in which an error hits every bit with probability $(1 - \epsilon)$ and when a bit is hit it becomes a random unbiased bit. (That is, a bit is flipped with probability $(1 - \epsilon)/2$.) This type of noise can be corrected by representing a 0 bit by a long string of 0's and a 1 bit by a long string of 1's. (If the noise hits a smaller fraction of bits, the condition of it being unbiased can be compromised.) If we start with qubits and again replace each qubit with a random qubit with probability $(1 - \epsilon)$ we can still extract noiseless *bits*. However, there is no quantum error-correction code for such noise.

This means that deterministic noiseless bits can prevail (for classical and quantum systems) even for some forms of highly correlated errors. (Our postulates do not imply a high correlation for the errors when the elements of the system are statistically independent, but mechanisms leading to our conjectural effects may still be relevant for the nature of noise for classical forms of storing information and computation.)

The method of "clone and sample" appears to be essentially the only error-correction method we find in nature. This method allows us to introduce gates where errors on the involved bits will be almost independent to start with, and thus will reduce "noise on gates" to "noise on bits." But this method is not available for quantum information of a general type.

5. **The censorship conjecture**. Notions of "highly correlated" or "highly entangled" systems are not easy to define. We will refer informally to systems that up to a small error are induced by their marginal distributions on small sets of elements as "approximately local." For a suggested definition of "approximately local" (just for the quantum case), and a precise formulation of the conjecture below, see [23].[3]

[C] Censorship conjecture: Noisy stochastic physical systems are approximately local.

[C] The states of quantum computers are approximately local.

The rationale for this conjecture is that high forms of entanglement will necessarily come together with strong effect of error synchronization which in turn will push the system towards approximate locality.

4 A mathematical formulation

4.1 Measuring information leaks

In this section we attempt to give a mathematical formulation for Postulate [P1']. Our setting is as follows. We have a quantum computer running on n qubits. The noise can be described by a unitary operator on the computer qubits and the neighborhood qubits or as a quantum operation E on the space of density matrices for these n qubits.

[3] There are many measures for the "amount of entanglement" (and correlation) that can be used. It is also not clear if we should measure the entanglement of a single state or use a measure that depends on the variety of feasible states for a system. Leggett's paper [24] and his "disconnectivity measure" (D-measure) seem especially relevant.

It is better to think about the conjectures in this section as follows: A noisy quantum computer is subject to noise described by a quantum operation E, such that the error rates for individual qubits are small but substantial and E satisfies the (stronger and stronger) requirements described in this section. The operation E may not be the overall noise that describes the gap between the ideal state and the noisy state of the computer, but we assume that any damaging properties of E will not be remedied by additional noise of a different nature.

We denote by $L(a)$ the "amount of information the neighborhood has on the qubit a." More generally, for a set A of qubits we denote by $L(A)$ the "amount of information the neighborhood has on A." Next we propose mathematical definitions for these notions.

Let ρ be a state of the computer. For a set A of qubits let $\rho|_A$ be the induced state on A. When the state ρ is a tensor product pure state then for every set A of qubits, $S(\rho|_A) = 0$ and the information leak of the noise operator E from the set of qubits A can be measured by the entropy $S((E \circ \rho)|_A)$. (We deam this entropy-based notion appropriate for our purposes although the entropy does not capture every form of "information leak" attributable to a noise operator.)

I am not aware of a canonical way to make the "information leak" a measure of the noise operation E that does not depend on a specific choice for this tensor product state. In what follows we let $\rho_0 = (+)^{\otimes n} = (1/\sqrt{2}((|0> +|1>))^{\otimes n}$ and define $L(A) = L_E(A) = S(E(\rho_0|_A))$.

Remark: Let $\hat{\rho}$ be the state of the computer's qubit and the environment that is represented by a set N of qubits. A standard measure on the information that the environment has on the qubits in A is $L'(A) = S(\hat{\rho}|_A) + S(\hat{\rho}|_N) - S(\hat{\rho}|_{\{A \cup N\}})$. I would expect that $L'(A)$ can replace $L(A)$ for the formulation of the conjectures in this section.

4.2 Two qubits

We will state mathematically a version of Postulate [P1']. Our setting is as follows: Let ρ be the "ideal" state of the computer and consider two qubits a and b. We use as the (rather standard) measure of entanglement

$$ENT(\rho; a, b) = S(\rho|_a) + S(\rho|_b) - S(\rho|_{\{a,b\}}).$$

As a measure of correlation of information leaks we use

$$EL(a, b) = L(a) + L(b) - L(\{a, b\}).$$

Postulate [P1'] can be formulated as follows:

$$EL(a, b) \geq K(L(a), L(b)) \cdot ENT(\rho; a, b), \tag{1}$$

where K is a function of $L(a)$ and $L(b)$, which is substantially larger than their average $(L(a) + L(b))/2$. ($K(0, 0) = 0$, so that relation (1) tells us nothing about noiseless entangled systems.)

Remark: We are mainly interested in the case that the noise rate is fixed, but the dependence of $K(L(a), L(b))$ on the noise rates is also of interest.

4.3 Two qubits: A stronger version

We go on to describe and motivate an even stronger form of [P1'] and an extension to more than two qubits. These extensions go beyond Postulates [P1] and [P2] as discussed so far.

The expression $S(\rho|_a) + S(\rho|_b) - S(\rho|_{\{a,b\}})$ was used as a measure of entanglement between two qubits. We would like to replace it by a measure of what can be called "emergent entanglement," defined as follows. Let $\mathcal{M}_A$ be the class of completely positive separable maps on density matrices, which acts as the identity on a set A of qubits.

$$EE(\rho; a, b) = \max\{(S(Z \circ \rho|_a) + S(Z \circ \rho|_b) - S(Z \circ \rho|_{\{a,b\}}) : Z \in \mathcal{M}_{\{a,b\}}\}.$$

A strong form of relation (1) is

$$EL(a, b) \geq K(L(a), L(b)) \cdot EE(\rho; a, b), \tag{2}$$

where, as before, K is a function of $L(a)$ and $L(b)$ which is substantially larger than their average $(L(a) + L(b))/2$.

Of course, letting Z be the identity we see that $EE(\rho; a, b) \geq ENT(\rho; a, b)$. The measure of "emergent entanglement" may be related to Briegel and Raussendorf's notion of "persistent entanglement" [25] and it also looks like a variant of "distilled entanglement."

The motivation for this strong version of Postulate [P1'] comes from considering the state of a quantum computer that applies a fault-tolerant computation. The state of the computer is t-wise independent for a large value of t; hence every two qubits are statistically independent and Postulate [P1'] does not directly apply. Consider an error-correcting code and let s be the minimal number of qubits whose state "determines" those of the others, so once they are measured and their value are "looked at" the state of the other qubits is determined. When we measure and look at the values of $s - 1$ qubits, we see a very strong dependence between every pair of the remaining qubits. Now, if we assume Postulate [P1'] and (just tentatively) also assume that "measuring and looking at" the contents of some qubits does not induce errors on other qubits (this is a standard assumption in current noise models), we see that the conclusion of Postulate [P1'] should apply for pairs of qubits in a quantum computer running FTQC even though pairs of qubits are independent.

4.4 More qubits

Here is a tentative suggestion for an extension of the above conjecture from pairs of qubits to larger sets of qubits. This suggestion goes beyond Postulates [P1] and [P2] proposed in this paper and is related to a strong form of error synchronization conjectured in [23].

For a set $A = \{a_1, a_2, \dots, a_m\}$ of m qubits let

$$ENT(\rho; A) = -S(\rho) + \max S(\rho^*),$$

where ρ^* is a mixed state with the same marginals on proper sets of qubits as ρ, i.e. $\rho^*|_B = \rho|_B$ for every proper subset B of A.

Define in a similar way

$$EL(A) = -L_E(A) + L_{E^*}(A),$$

where E^* is a quantum operation which satisfies $E^*|_B = E|_B$ for every proper set B of A.

Let ρ be an ideal state of the computer and let A be a set of m qubits.

$$EL(A) \geq K_m ENT(\rho|_A) \tag{3}$$

Here, $K_m = K_m(\{L(a) : a \in A\})$ is substantially larger than $\min\{L(N(a))) : a \in A\}$ and it vanishes when all the individual information leaks vanish.

Also here we can further conjecture that for every completely positive map $Z \in \mathcal{M}_A$

$$EL(A) \geq K_m ENT((Z \circ \rho); A) \tag{4}$$

Remarks: 1. We expect that a quantum error-correcting code that corrects t-errors and has a fixed error rate will have a strong form of error-synchronization as t tends to infinity. Namely, the noise operation will have a similar effect to that of the following operation: with probability ϵ a $(1-o(1)$-fraction of qubits are being measured. (This is referred to as "devastating" noise in [23].) This is also expected when implementing a Fourier transform, which is an important subroutine in quantum computer programs, e.g., if the state of the computer is described by the Hadamard matrix.

I expect (but proving it remains to be done) that Postulate [P1'] as expressed by relation (2) will imply the weaker form of error-synchronization discussed in Section 3.2, while an extension for larger sets of qubits given by (4) will imply the stronger form.

2. The value of $ENT(\rho;A)$ is intended to serve as a measure of the additional information when we pass from "marginal distributions" on proper subsets of qubits to the entire distribution on all qubits. Another measure which express this idea less accurately but may be easier to handle is defined as follows:

$$ENT'(\rho;A) = \sum S(\rho|_{A\backslash\{a_i\}}) - (m-1)S(\rho|_A),$$

The nonnegativity of $ENT'(\rho;A)$ was proved in [12] and it extends a well-known inequality of Shearer for classical entropy. Similarly we can define

$$EL'(A) = \sum L(A\backslash\{a_i\}) - (m-1)L(A).$$

It may be useful to state the conjectures given by relations (3) and (4) while replacing the quantities ENT and EL by ENT' and EL', respectively.

4.5 Censorship

Here is a tentative suggestion for an entropy-based mathematical formulation for Conjecture [C].

Let ρ be a pure state on a set $A = \{a_1, a_2, \ldots, a_n\}$ of n qubits define

$$\widetilde{ENT}(\rho; A) = \sum\{ENT(\rho; B) : B \subset A\}.$$

In this language a way to formulate the censorship conjecture is:

There is a polynomial P (perhaps even a quadratic polynomial) such that: For any quantum computer on n qubits, which describes a pure state ρ, and for every integer k,

$$\widetilde{ENT}(\rho; A) \leq P(n). \tag{5}$$

Remarks: 1. It is interesting to study how the quantities $ENT(A; \rho)$, and $ENT'(A, \rho)$ evolve in time for dynamical systems describing (quantum and classical) physical processes.

2. The additional conjectures of this section are meant to draw the following picture: we have an ideal notion of a quantum computer which has extraordinary physical and computational properties. Next come noisy quantum computers with an ideal notion of noise. If the noise rate is small then FTQC is possible. Next come noisy quantum computers which satisfy relation (1). For those, fault tolerance will require controlling the error rate as well as K_2, which we expect to be much harder. This model is also an idealization as long as $K_3 = 0$ and so on. For such highly entangled states as those required in quantum algorithms, K_i will be more and more damaging for larger values of i.

We expect that for realistic noisy quantum computers statistical dependencies beyond those induced by small sets of elements (perhaps even beyond pairs) will diminish.

5 Discussion

Our conjectures on the nature of noise for correlated systems appear to be damaging to the possibility of storing and manipulating correlated quantum or classical data. It will thus be damaging for quantum computation but not for classical computation (even randomized), because there, for the computation itself, no correlation is needed. Moreover, classical noiseless bits can prevail also in certain cases of highly correlated errors.

Causality

We do not propose that the entanglement of the pair of noisy qubits *causes* the dependence between their errors. The correlation between errors can be caused by the process leading to the correlation between the qubits, or simply just by the ability of the device to achieve strong forms of correlation.

How it comes about

A basic challenge is to present concrete models of noise that support Postulates [P1] and [P2]. (Of course, there is a difference between showing that the type of behavior we are looking for is possible and showing that it is unavoidable.) A model for the noise that supports our postulates should already exhibit [P1] and [P2] for the "new errors" — either qubit-errors or gate-errors (or both) — and would thus be quite different from current models.

It is worth noting that error synchronization is a very familiar phenomenon for error propagation of (unprotected) quantum programs. It is instructive to see in this context how error synchronization is often created when we start with small independent errors and let them propagate along the steps of a computer program.

One way to view the noise is as represented by a rather primitive (but quick) stochastic program (or circuit) "running" along the actual program. We run the program $\mathcal{P}$ and we actually get $\mathcal{P}+\mathcal{N}$. The simplest explanation for why errors of correlated qubits are themselves correlated is that the noise $\mathcal{N}$ depends on $\mathcal{P}$, or can be described as a weak perturbation of the original program itself. But this is not the only possibility. It may be the case that $\mathcal{N}$ does not depend on $\mathcal{P}$ but rather represents a certain form of "generic" quantum program. In both these cases we think of $\mathcal{N}$ as a quantum program with many steps for each computer cycle. This hypothetical "noise program" partially achieves one familiar "computational task" for a distributed system — synchronization.

The models suggested by Alicki, Horodecki, Horodecki, and Horodecki [19] appear to be relevant. Also relevant is Alicki's idea [26] (see also [27]) that "slow gates" (combined with the free evolution of the system) will be an obstacle to error correction.

But perhaps the easiest way to find relevant models of noise is to look for them in the literature. There is a substantial interest in local stochastic behavior leading to spontaneous (collective) synchronization (e.g., [28, 29, 30, 31, 32]). The Glauber dynamics (a very simple locally defined "program") for the Potts model (e.g., [33]) can also be regarded in this way. There is also a substantial amount of work on emergence of patterns in stochastic (correlated) locally described systems.

Linearity

Do our postulates violate the linearity of quantum physics? The plain simple answer is no. Again the analogy with classical stochastic processes is telling. The conjecture that in noisy systems like the weather substantially correlated events are subject to substantially correlated noise (or, in other words, can only be approximated up to error terms that are also substantially correlated) is perhaps bold and may well be false, but it is not remotely bold enough to violate the laws of probability theory. This is also so in the quantum case.

It is indeed correct that these conjectures amount to systematic non-linear inequalities for the noise (or, for feasible approximations,) for noisy highly correlated systems. Such non-linear inequalities, if they exist, may be of independent interest.

Faraway qubits

Suppose we have two qubits that are far away from each other at a given entangled state at time T. Consider their state at time $T+t$. Is there any reason to believe that the changes will not be independent? And if t is small compared to the distance between the qubits isn't it the case that to implement a noise that is not independent we will need to violate the speed of light? And finally isn't this observation a counterexample to Postulate [P1]?

The answer to the final question is negative. There is no difficulty in conceding that changes over time in the states of two faraway entangled qubits will be independent. The problem with this critique is the initial assumption: we are *given* two qubits at time T at a given state. Starting with noiseless correlated elements, we may well reach correlated elements that can be described up to substantial but independent error terms. But for fault tolerance we may not assume noiseless pairs of entangled qubits to start with.[4]

Probability, secrets, and computing

We will now describe a potential difficulty to our conjectures at least in the classical case. Consider a situation where Alice wants to describe to Bob a complicated correlated distribution $\mathcal{D}$ on n bits that can be described by a polynomial-size randomized circuit. Having a noiseless (classical) computation with perfect independent coins, Alice can create a situation where for

[4] Sometimes, we consider a quantum computer that is only partially noisy (e.g., [10]). In such a case we should formulate Postulates [P1], [P2] relative to the noiseless part.

Bob the distribution of the n bits is described precisely by $\mathcal{D}$. In this case the values of the n bits will be deterministic and $\mathcal{D}$ reflects Bob's uncertainty. Alice can also make sure that for Bob the distribution of the n bits will be $\mathcal{D} + \mathcal{E}$, where $\mathcal{E}$ describes independent errors of prescribed rate.

Is this a counterexample to our Postulates [P1] and [P2]? One can argue that the actual state of the n bits is deterministic and the distribution represents Bob's uncertainty rather than "genuine" stochastic behavior of a physical device.[5] But the meaning of "genuine stochastic behavior of a physical device" is vague and perhaps ill-posed. Indeed, what is the difference between Alice's secrets and nature's secrets? In any case, the difficulty described in this paragraph cannot be easily dismissed.[6]

However, note that as in the case of faraway qubits, the noisy distribution $\mathcal{D} + \mathcal{E}$ was based on the ability to achieve the noiseless distribution $\mathcal{D}$. Achieving the distribution $\mathcal{D}$ was based on noiseless classical computation to start with. For the case of quantum computers, we can still defend our Postulates [P1] and [P2] against this argument as follows. Even if nature can simulate Alice, and Bob's "mental" uncertainty can be replaced by a "real" physical situation where a highly correlated distribution is prescribed up to an independent error term, this approximation was achieved via a noiseless computation to start with. Therefore, such an approximation cannot serve, in the quantum case, as a basis for fault tolerance. [7]

[5] Compare the interesting debate between Goldreich and Aaronson [34], whether nature can "really" manipulate exponentially long vectors.

[6] The distinction between the two basic interpretations of probability as either expressing human uncertainty or as expressing some genuine physical phenomenon is an important issue in the foundation of (classical) probability. See, e.g., Anscombe and Aumman [35]. Opinions vary from not seeing any distinction at all between these concepts to regarding human uncertainty as the only genuine interpretation.

[7] The difficulties considered here can perhaps be confronted by considering "information leaks" (Section 3.1, remark 4) rather than "errors." A related idea is to regard a stricter

Running a quantum algorithm with a "random" state at all times

A critique of the possibility of any systematic damaging relation between the state of the quantum computer and the noise was suggested by Ben-Or (see [23]) and is related to some works of Preskill and Shor. (A related concern was pointed out by Preskill. A detailed proof of such a result along with an interesting interpretation was recently offered by Aharonov [36].) Having a classical computer control a quantum computer makes it possible to run a variant of any quantum computer program where at the initial state we apply random Pauli operators on every qubit and modify the action of the gates accordingly. This interesting critique does not apply to the mathematical formulation given in Section 4 for Postulate [P1'], since the measures of entanglement we use are invariant under such an operation.

Computation complexity

While it looks intuitively correct that our postulates are damaging for quantum computation, proving it, and especially proving a reduction all the way to the classic model of computation, is not going to be an easy task. (This is an interesting question in computational complexity [23].) Let me mention that the problem of describing complexity classes of quantum computers subject to various models of noise was proposed by Peter Shor [37] in the 90s, but apparently was not picked up. Compare also Aaronson [38]. In particular, going below the computation power of logarithmic depth polynomial-size quantum circuits appears to be difficult, yet such circuits combined with classical computers are strong enough to allow a polynomial-time algorithm for

definition of a noisy quantum computer as such that at *any time* along the computation for every qubit, and *for every observer*, (who extracts information from the computer) the noise rate for every qubit (namely the difference between its ideal state and its actual state) is at least ϵ.

factoring. (This follows from a recent result of Cleve and Watrous [39].)

Is it possible that our assumptions on noise (and, in particular, the possibility of a dependence of the noise $\mathcal{N}$ on the program $\mathcal{P}$), rather than being harmful, will allow an even stronger computation power than BQP? Well, optimism is always a good human trait, and yes, this is a possibility. But it appears to be a remote possibility.

Topological quantum computers and anyons [8]

There is a beautiful and powerful "dictionary" between certain forms of combinatorial methods for fault tolerance and remarkable objects from physics for "topological quantum computers" [14, 40, 41]. In this case it is suggested that fault tolerance can be realized by "non-Abelian anyons," which can be thought of as analogous to the physical realization of logical bits in a digital computer that are very robust to noise. The two "languages" of this dictionary are a combinatorial description of a quantum error-correction with n qubits, and a physical realization as certain quasi-particles called "anyons". Only a small number of types of non-Abelian anyons are required to realize the full power of quantum computers.

Analyzing the stability of non-Abelian (and Abelian) anyons based on the assumption that the noise is "local" (statistically independent, as discussed above) reveals a remarkable phenomenon referred to as "mass gap." Below a certain temperature the anyon is going to be extremely stable. (Low temperature translates to low error rate.) The mathematical model predicts that as n grows the region of stability (in terms of the temperature) will not become smaller and the "gap" will be maintained. Moreover, in this stable area the robustness to noise will be exponential in n and thus, on the physics

[8] The next three items which discuss connections with physics are necessarily based on incomplete and second-hand knowledge.

side, we will obtain very robust qubits.[9]

The existence of very robust ("protected") qubits based on quantum error-correction via a highly entangled state, whether implemented by "software," say with ion traps, or by "hardware" like anyons, runs counter to our conjectures. We can expect that when we study the effect of noise for the combinatorial model of anyons with highly entangled state, using a perturbation method that reflects Postulates [P1] and [P2], the exponential robustness with n, or even the "mass gap" will disappear.

Other possible counter examples from physics

Several people have suggested that our postulates (and especially Conjecture [C]) are already in conflict with phenomena from physics, like superconductivity and Einstein—Bose condensation. This appears to depend on precise interpretation of these phenomena in our context and also on the rigorous formal description of our conjectures themselves. Superconductivity and related phenomena are indeed physical systems with strong forms of (pairwise) entanglement which appear to be related to what is required for quantum fault-tolerance.

I tend to think that the form of entanglement for superconnectivity is not sufficient to refute Conjecture [C] since the entanglement in this case is "generated" (to a large extent) by dependencies of pairs of elements. Translating and testing Postulate [P1'] for the setting of superconductivity would be of interest.

[9] In the translation between a discrete combinatorial model with n qubits (or n elements) and a concrete physical object, it is not clear what is the interpretation on the physics side for the value of n, and the relevance of the behavior as n tends to infinity should not be taken for granted. Inner dependencies of the physical object appear to be relevant to the best value of n for the combinatorial model describing it.

Noisy quantum computers that respect our postulates are not capable of simulating hypothetical objects like non-Abelian anyons. But are they capable of simulating familiar, much simpler, objects from physics? Perhaps the simplest potential counterexample (not to [P1'] but possibly to its stronger version, relation (2)) is a state X of $2n$ bosons (n large) each having a ground state $|0>$ and an excited state $|1>$, so that $|0>$ has occupation number (precisely) n and $|1>$ has occupation number n. A similar state Y where the occupational number has a binomial distribution can be simulated by a tensor product state. So the question is whether X is physically realistic, or perhaps any realization of X amounts in reality to something like Y. A somewhat similar question (regarding a cat-like state and directly related to the possibility of "superconducting qubits") is raised by Leggett [24] (p.90, (3.8), (3.9)).

Other possible relations to physics

An obvious connection to physics is that a failure of computationally superior quantum computing would suggest that computations of quantum physics that are relevant to physical reality can efficiently be simulated on classical computers, and thus would question the relevance to reality of computations from quantum physics that appear to be computationally hard. We mention two other potential connections.

Perturbation methods. Another connection to physics may come from the perturbation methods used to analyze non-Abelian anyons. These methods are related to standard perturbative methods used in various other areas of physics and mainly in quantum field theory. Statistical independence appears to be a major hidden assumption behind these methods. Modifications of the perturbation method itself, which may amount to amending unjustified hidden probability independence assumptions, and may lead to a drastically different behavior for the extreme situation of (hypothetical) highly entangled systems like quantum error-correcting code and quantum computers, may be of interest also in more mundane situations from physics, where these perturbation methods are (rather successfully) used.

Thermodynamics Connections between fault tolerance and thermodynamics were considered, e.g., in [27, 42], and were intensely debated. (The results and methods of [12] also have a clear thermodynamic flavor.)

For example, in a very recent paper, Alicki and Horodecki [42] propose the following line of thought: 1. Thermodynamics is relevant because very robust storage of quantum inormation requires large systems. 2. Meta-stable states for finite systems are necessarily manifested by equilibrium states of infinite systems. 3. Equilibrium states of infinite systems must have the form: "probability measures over a set of states" and, in particular, cannot support even a single qubit. Of the above points, perhaps the second is the most controversial, and in view of some potential counterexamples may be related to noise models/perturbative methods that are different from the standard ones.

The information-theoretic form of the mathematical formulation of our postulates (which, to a large extent, were required in order to respond to various points discussed in this section) suggests possible connections with thermodynamics. Of particular interest are connections with entropy-type measures of "high order" statistical dependence.

Conclusion

My belief is that the interesting question of the physically realistic "Church-Turing thesis" (put forward mainly by Deutsch) and, in particular, the feasibility of computationally superior quantum computers will have a convincing solution, and that, whatever this solution is, the asymptotic approach —

namely, the relevance of the asymptotic behavior of complexity to real-life computation — which lies behind this question, will prevail.

The question “How can (computationally superior) quantum computers fail?”[10] is as important a part of the quantum information and quantum computers endeavor, as the question “How can (computationally superior) quantum computers succeed?” As a matter of fact, these two questions are the same.

References

[1] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. Roy. Soc. Lond.* A 400 (1985), 96–117.

[2] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Rev.* 41 (1999), 303-332. (Earlier version appeared in: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.)

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[4] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* 52 (1995), 2493–2496.

[5] A. M. Steane, Error-correcting codes in quantum theory, *Phys. Rev. Lett.* 77 (1996), 793–797.

[6] D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error, STOC ’97, ACM, New York, 1999, pp. 176–188.

[10] While the possibility of computationally superior quantum computers certainly captures the imagination, it is worth noting that implementing even simple computations on quantum systems can be important for applications, such as enhancing the performance of medical NMR [43, 44].

[7] A. Y. Kitaev, Quantum error correction with imperfect gates, in *Quantum Communication, Computing, and Measurement* (Proc. 3rd Int. Conf. of Quantum Communication and Measurement) Plenum Press, New York, 1997, pp. 181–188.

[8] E. Knill, R. Laflamme, and W. H. Zurek, Resilient quantum computation: error models and thresholds, *Proc. Royal Soc. London A* 454 (1998), 365–384, quant-ph/9702058.

[9] D. Gottesman, Stamilizer codes and quantum error-correction, Ph. D. Thesis, Caltech, 1997.

[10] H. Buhrman, R. Cleve, N. Linden, M. Lautent, A. Schrijver, and F. Unger, New limits on fault-tolerant quantum computation, *FOCS 2006*, to appear.

[11] D. Aharonov and M. Ben-Or, Polynomial simulations of decohered quantum computers, 37th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press, Los Alamitos, CA, 1996, pp. 46–55.

[12] D. Aharonov, M. Ben-Or, R. Impagliazo, and N. Nisan, Limitations of noisy reversible computation, 1996, quant-ph/9611028.

[13] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* 54 (1996), 1098–1105.

[14] A. Kitaev, Topological quantum codes and anyons, in *Quantum Computation: A Grand Mathematical Challenge for the Twenty-First Century and the Millennium* (Washington, DC, 2000), 267–272, Amer. Math. Soc., Providence, RI, 2002.

[15] A. Kitaev, Fault-tolerant quantum computation by anyons, *Ann. Physics* 303 (2003), 2–30.

[16] E. Knill, Quantum computing with very noisy devices, 2004, quant-ph/0410199.

[17] J. Preskill, Quantum computing: pro and con, *Proc. Roy. Soc. Lond. A* 454 (1998), 469-486, quant-ph/9705032.

[18] L. Levin, The tale of one-way functions, *Problems of Information Transmission (= Problemy Peredachi Informatsii)*, 39 (2003), 92–103, cs.CR/0012023

[19] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, Dynamical description of quantum computing: generic nonlocality of quantum noise, *Phys. Rev. A* 65 (2002), 062101, quant-ph/0105115.

[20] B. B. Terhal and G. Burkard, Fault-tolerant quantum computation for local non-Markovian noise, *Phys. Rev. A* 71 (2005), 012336.

[21] P. Aliferis, D. Gottesman, and J. Preskill, Quantum accuracy threshold for concatenated distance-3 codes, 2005, quant-ph/0504218.

[22] D. Aharonov, A. Kitaev, and J. Preskill, Fault-tolerant quantum computation with long-range correlated noise, 2005, quant-ph/0510231.

[23] G. Kalai, Thoughts on noise and quantum computing, 2005, quant-ph/0508095.

[24] A. J. Leggett, Macroscopic quantum systems and the quantum theory of measurement, *Suppl. of the Prog. of Theor. Physics* 69 (1980), 80–100.

[25] H. J. Briegel and R. Raussendorf, Persistent entanglement in arrays of interacting particles, it Phys. Rev. Lett. 86 (2001) 910–913, quant-ph/0004051.

[26] R. Alicki, Quantum error correction fails for Hamiltonian models, 2004, quant-ph/0411008.

[27] R. Alicki, D.A. Lidar, and P. Zanardi, Are the assumptions of fault-tolerant quantum error correction internally consistent?, *Phys. Rev. A* 73 (2006) 052311, quant-ph/0506201.

[28] L. N. Kanal and A. R. K. Sastry, Models for channels with memory and their applicaions to error control, *Proc. of the IEEE* 66 (1978), 724–744.

[29] S. H. Strogatz and I. Stewart, Coupled oscillators and biological synchronization, *Sci. Am.* 269 (1993), 102–109.

[30] R. Das, J. Crutchfield, M. Mitchell, and J. Hanson, Evolving globally synchronized cellular automata, *Proc. of the Sixth Conf. on Genetic Algorithms*, 336-343, San Francisco, 1995.

[31] Z. Néda, E. Ravasz, T. Vicsek, Y. Brechet, and A.L. Barabási, Physics of the rhythmic applause, *Phys. Rev. E* 61(2000), 6987-6992.

[32] Y. Kuramoto, Collective synchronization of pulse-coupled oscillators and excitable units, *Physica D* 50 (1991), 15–30.

[33] F. Martinelli, Lectures on Glauber dynamics for discrete spin models, (Saint-Flour, 1997) *Lecture Notes in Mathematics* 1717, Springer, Berlin, 1988, pp. 93–191.

[34] O. Goldreich, On quantum computers, 2004, http : //www.wisdom.weizmann.ac.il/˜oded/on − qc.html, and S. Aaronson, Are quantum states exponentially long vectors?, 2005, quant-ph/0507242.

[35] F. J. Anscombe and R. J. Aumann, A definition of subjective probability, *Ann. Math. Statist.* 34 (1963), 199–205.

[36] D. Aharonov, work in progress.

[37] P. Shor, personal communication.

[38] S. Aaronson, Ten Challenges for Quantum Computing Theory (2005), http://www.scottaaronson.com/writings/qchallenge.html.

[39] R. Cleve and J. Watrous, Fast parallel circuits for the quantum Fourier transform, 2004, quant-ph/0006004.

[40] M. Freedman, A. Kitaev, M. Larsen, and Z. Wang, Topological quantum computation, Mathematical Challenges of the 21st Century (Los Angeles, CA, 2000). *Bull. Amer. Math. Soc.* 40 (2003), 31–38.

[41] G. P. Collins, Computing with quantum knots, Scientific Amer. 63 (2006), 56–63.

[42] R. Alicki and M. Horodecki, A no-go theorem for storing quantum information in equilibrium systems. preprint.

[43] J. Baugh, O. Moussa, C. A. Ryan, A. Nayak, and R. Laflamme, Experimental implementation of heat-bath algorithmic cooling using solid-state nuclear magnetic resonance, *Nature* 438 (2005), 470–473.

[44] L. J. Schulman, A bit chilly, *Nature* 438 (2005), 431–432.