Quantum Computers – How Can They Fail?

Gil Kalai*
Hebrew University of Jerusalem and Yale University

May 9, 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.

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 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

*Research supported in part by an NSF grant, by an ISF Bikura grant, and by a BSF grant. The presentation here is an informal short description of some ideas evolved from [21], and it follows my comments in the discussion at Bacon's "Quantum Pontiff" http://dabacon.org/pontiff/?p=1203.

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], 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 for FTQC. Several other crucial requirements for fault-tolerance were also described in [9, 10].

The study of quantum error correction and its limitations, as well as of various approaches to fault-tolerance quantum computation, is extensive and beautiful; see, for example, [11, 12, 13, 14]. Concerns about noise models with statistical dependence are mentioned (inter alia) in [15, 16]. Specific models of noise that may be problematic for quantum error-correction are studied in [17]. 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 [18, 19, 20].

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 "qubits errors". In addition, the gates which carry the computation itself are not perfect. We can suppose that every such gate involves two qubits and that the gate's imperfection (or the "noise on the gate") 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.

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 constant 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 puropses, 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. The noise or errors will also be represented by a probability distribution on such strings.

When we consider a system with many correlated bits (or entangled qubits), an error in one bit will also affect the other bits. On an intuitive level this looks like an obstacle to error correction but, as is, it is not. Errors affecting a substantial but small fraction of — even highly correlated – bits 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 (bits/qubits) 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 themselves substantially statistically dependent are themseves 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] 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.

1. **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. (The proof of the threshold theorem implies that this property of having almost independent errors, will be satisfied by *most* pairs of qubits when the overall number of qubits is large.) This "purification" nature of fault tolerance for quantum computation is arguably an element we do not find in fault tolerance for deterministic computation. (Recall that fault tolerance does not improve the "quality" of individual qubits, and fault-tolerant computation allows computation in noisy computers where at any point the state of an individual qubit can only be estimated up to a substantial small error.)

2. **Real-life examples: The weather and the stock market.** We can discuss Postulate [P1] for cases of (classical) stochastic systems with highly correlated noise. 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.

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?

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. Can we expect that the difference $\mathcal{D}-\mathcal{D}'$ will be almost statistically independent for the different locations?

3. **Going beyond pairs.** Pairwise (almost) independence for qubits errors appears necessary for fault-tolerant quantum computation (and thus is the first thing to question). However, note that for the conclusion of the threshold theorem, the assumption of pairwise (almost) independence for qubits errors is not sufficient. Independence (or at least almost independence) for errors on larger sets of bits/qubits is also crucial.

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.

Postulate [P2] of error synchronization follows from a strong form of [P1]. If it is the case that the correlation of the noise "hitting" a pair of highly correlated elements is substantial and *positive*, then this would imply a strong effect of error synchronization.

For the case, described in the introduction, where the errors are represented by a distribution $\mathcal{D}$ on strings of bits, error synchronization refers to a situation where, although the expected number of errors is small, there is a substantial probability that the number of errors is a large fraction of all bits. (An even stronger form of error synchronization is considered in [21], and there, a more 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). Having such devices where the qubits themselves are sufficiently stable is well down the road, but still expected long before the superior complexity power of quantum computers kicks in. (I suspect that [P2] will be easier to test experimentally than [P1].)

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, the theory of evolution, the evolution of scientific thought, and so on.[2] We can examine the possibility of error synchronization for the examples we 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 related also 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 the quantum computation itself.

[2] This idea is conveyed in the Hebrew proverb "troubles come in clusters", and the English one "it never rains it pours."

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.) However, there is no quantum error-correction code for such noise (and most likely also no error correction that allows correlated classical information to prevail).

This means that deterministic noiseless bits can prevail even for some forms of highly correlated errors. (Our postulates do not imply 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 certain classical forms of storing information and computation.)

The method of "clown 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 stochastic noisy correlated data.

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 [21].

[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 increase the effect of error synchronization which in turn will push the system towards locality.

4 Discussion

Our conjectures on the nature of noise (more precisely, the nature of feasible approximations) 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 correlations between the qubits, or simply just by the ability of the device to achieve strong forms of correlation.

How it comes about

The most basic challenge is to present concrete models of noise that support Postulates [P1] and [P2]. (Of course, there is a big difference between showing that the type of behavior we are looking for is possible and showing that it is unavoidable.) One possibility is to consider for this purpose "generic" (both in terms of dependence among the elements and dependence in time) locally-defined noise models. (See also [21].)

One way to view the noise is as represented by a rather primitive 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 a device that allows the high amount of correlation required for quantum computation is vulnerable to highly correlated noise, no matter what the state of the computer is. (In this case $\mathcal{N}$ can represent a certain form of "random" quantum program.)

It can also be instructive to check [P1] and [P2] for the case of a very small amount of independent errors for the initial state of your classical or quantum computer program $\mathcal{P}$, which accumulates to constant-rate error over a large number (say, a polynomial number in the number of bits/qubits) of computer steps. It is interesting to observe that indeed in many examples of this kind we witness strong forms of error synchronization. (Of course, fault tolerance easily deals with such a noise for the original program $\mathcal{P}$. But if our computer actually runs along $\mathcal{P}$ some weak perturbations of $\mathcal{P}$ that are not directly targeted by the error correction, then this may be damaging.)

The models suggested by Alicki, Horodecki, Horodecki, and Horodecki [17] appear to be relevant. Also relevant is Alicki's idea [22] (see also [23]) 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., [24, 25, 26, 27, 28]) as well as in the emergence of patterns in stochastic (correlated) systems.

Linearity

Do our postulates violate 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 noisy highly correlated systems — or, in other words, to the nature of feasible approximations for highly correlated physical 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.

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 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 a "genuine" stochastic behavior of a physical device.[3] 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.[4]

However, note that like in the case of faraway qubits, the noisy distribuion $\mathcal{D}+\mathcal{E}$, 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.

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

[3] Compare the interesting debate between Goldreich and Aaronson [29], whether nature can "really" manipulate exponentially long vectors.

[4] The distinction between the two basic interpretations of probability as 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 [30]. Opinions vary from those who see no distinction at all between these concepts to those who regard human uncertainty as the only genuine interpretation.

is an interesting question in computational complexity [21].) Let me mention that the problem of describing complexity classes of quantum computers subject to various models of noise was proposed by Peter Shor [31] in the 90s, but apparently was not picked up. Compare also Aaronson [32]. In particular, going below the computation power of logarithmic depth polynomial-size quantum circuits appears to be difficult (and to require more than just [P1] and [P2]), yet such circuits combined with classical computers are strong enough to allow a polynomial-time algorithm for factoring. (This follows from a recent result of Cleve and Watrous [33].)

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 looks like a remote possibility.

Conclusion

My belief is that the interesting question of the physically realistic complexity class (put forward mainly by Deutsch) and, in particular, the feasibility of computationally superior quantum computers, will have a convincing solution, and that, no matter what this solution will be, 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?" is an important part of the quantum information and quantum computers endeavor, as is 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.

[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. 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.

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

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

[12] 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.

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

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

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

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

[17] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, Dynamical description of quantum computing: Generic nonlocality of quantum noise, 2001, quant-ph/0105115.

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

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

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

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

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

[23] R. Alicki, D.A. Lidar, and P. Zanardi, Are the assumptions of fault-tolerant quantum error correction internally consistent? 2005, quant-ph/0506201.

[24] 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.

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

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

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

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

[29] 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.

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

[31] P. Shor, personal communication.

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

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