Detrimental Decoherence

Gil Kalai*
Hebrew University of Jerusalem and Yale University

November 23, 2007

Abstract

We propose and discuss two conjectures on the nature of information leaks (decoherence) for quantum computers. These conjectures, if (or when) they hold, are damaging for quantum error-correction as required by fault-tolerant quantum computation.

The first conjecture asserts that information leaks for a pair of substantially entangled qubits are themselves substantially positively correlated.

The second conjecture asserts that in a noisy quantum computer with highly entangled qubits there will be a strong effect of error synchronization.

We present a more general conjecture for arbitrary noisy quantum systems: prescribing (or describing) noisy quantum systems at a state ρ is subject to error E which "tends to commute" with every unitary operator that stabilizes ρ.

*Research supported in part by an NSF grant, an ISF grant, and a BSF grant. This paper is a draft of a revised version of the more formal part of [26]. I am grateful to Dorit Aharonov, Michael Ben-Or, Greg Kuperberg, and Robert Raussendorf 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 has generated a large body of research, in theoretical and experimental physics, computer science, and mathematics. 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 Landauer [4, 5], Unruh [6], and others) concerned the matter of noise:

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

The foundations of noisy quantum computational complexity were laid by Bernstein and Vazirani in [7]. A major step in showing that noise can be handled was the discovery by Shor [8] and Steane [9] of quantum error-correcting codes. The hypothesis of fault-tolerant quantum computation (FTQC) was supported in the mid-90s by the "threshold theorem" [10, 11, 12, 13], 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 [14, 15].

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., [16, 17, 18, 19]. Concerns about noise models with statistical dependence are mentioned in several places, e.g., [21, 22]. Specific models of noise that may be problematic for quantum error-correction are studied in [23]. 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 [24].

The purpose of this paper is to present two conjectures concerning decoherence for quantum computers which, if (or when) true, are damaging for quantum error-correction and fault-tolerance. We will now state these conjectures informally.

The first conjecture concerns entangled pairs of qubits.

[A] A noisy quantum computer is subject to error with the property that information leaks for two substantially correlated qubits have a substantial positive correlation.

We emphasize that Conjecture [A] (and Conjecture [D] below) refer to part of the overall error affecting a noisy quantum computer (or a noisy quantum system), which we call *detrimental*. Other forms of errors and, in particular, errors consistent with current noise models may also be present. (We conjecture that the effects of detrimental errors described by Conjectures [B] and [C] cannot be remedied by additional errors of a different nature.)

Error-synchronization refers to a situation where, while the error rate is small, there is a substantial probability for errors affecting a large fraction of qubits.

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

We will refer informally to a pure state of a quantum computer that up to a small error is induced by its "marginal distribution" on small sets of

qubits as "approximately local." We pose a related conjecture to the two conjectures above regarding the effect of detrimental decoherence:

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

Section 2 gives more background on noise and fault-tolerance. The main Section 3 is devoted to mathematical formulations of the above conjectures. In the Appendix, stronger versions of Conjecture [A] are formulated and some connections with Conjectures [B] and [C] are indicated. Section 4 discusses extensions of these conjectures to a more general framework. We first consider more general quantum systems and pose and discuss the following extension:

[D] A description (or prescription) of a noisy quantum system at a state ρ is subject to error described by a quantum operation E that tends to commute with every unitary operator that stabilizes ρ.

(Here, "tends to commute" reflects a small bias towards commutativity that will be described formally in Section 4.) We also briefly discuss classical noise. Section 5 discusses examples that may give the conjectured behavior and actual models of noise that may demonstrate them. Section 6 discusses related aspects of computational complexity and Section 7 concludes.

2 Quantum computers, noise and fault tolerance

The state of a digital computer having n bits is a string of length n of zeros and ones. As a first step towards quantum computers we can consider (abstractly) stochastic versions of digital computers where the state is 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 elements of a basis in U_q.) We can think of 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.

Moving from a qubit q to the probability distribution on '0' and '1' that it represents is called a "measurement" and it can be considered as an additional 1-qubit gate. We will assume that measurements of qubits that amount to a sampling of 0-1 strings according to the distribution these qubits represent is the final step of the computation.

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 "storage errors" or as "qubit errors." In addition, the gates that carry the computation itself are imperfect. We can suppose that every such gate involves a small number of qubits and that the gate's imperfection can take an arbitrary form, so that the errors (referred to as "gate errors") created on the few qubits involved in a gate can be statistically dependent. (Of course, qubit errors and gate errors propagate along the computation.)

The basic picture we 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 that are essentially noiseless.

Our conjectures apply to the same model of quantum computers but they require a more general notion of errors. They require that the storage errors will not be statistically independent (in fact, they should be instead very dependent) or that the gate errors will not be restricted to the qubits involved in the gates and will be of sufficiently general form. (Note that the errors may also reflect the translation from the ideal notion of quantum computers to a physical realization.)

3 A mathematical formulation

In this section we give a mathematical formulations for Conjectures [A], [B], and [C]. Our setting is as follows. We have a quantum computer running on n qubits. The ideal (or "intended") state of the computer is pure. We want to propose a picture for noisy quantum computation based on this model.

The errors 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. We will not give a specific model of detrimental error but rather describe some of its expected properties.

3.1 Two qubits

We first describe a measure of information leak. For a state ρ of the computer and a set A of qubits let $\rho|_A$ be the induced state on A.

Consider a quantum operation E. Note that when the state τ of the quantum computer is a tensor product pure state then for every set A of

qubits, $S(\tau|_A) = 0$. Here, $S(*)$ is the (von Neumann) entropy function; see, e.g., [3], Ch. 11. The information leak of the noise operator E from the set of qubits A, w.r.t. τ, can be measured by the entropy $S((E(\tau)|_A)$. For a tensor product state τ and a qubit a define $L_E(a;\tau) = S(E(\tau)|_a))$; more generally, for a set A of qubits define

$$L_E(A;\tau) = S(E(\tau)|_A)).$$

We will now state mathematically a version of Conjecture [A]. Our setting is as follows. Let ρ be the "intended" ("ideal") pure state of the computer and consider two qubits a and b. We use as the (rather standard) measure of entanglement between qubits at pure states

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

As a measure of correlation of information leaks we use

$$EL_E(a, b; \tau) = L_E(a;\tau) + L_E(b;\tau) - L_E(\{a, b\};\tau).$$

Conjecture [A] can be formulated as follows:

For every tensor product state τ,

$$EL_E(a, b; \tau) \geq K(L_E(a;\tau), L_E(b;\tau)) \cdot ENT(\rho; a, b), \tag{1}$$

where $K(x, y)/\min(x, y)^2 >> 0$ when x and y are positive and small. ($K(x, y) = 0$, when $\min(x, y) = 0$ so that relation (1) tells us nothing about noiseless entangled qubits.)

In the Appendix we will describe and motivate several stronger forms of Conjecture [A], and point out alternative mathematical formulations.

A simple extention that we would like to mention at this point is to pairs of qudits rather than pairs of qubits. The term qudit is used to denote a unit of quantum information in a d-level quantum system. Relation (1) extends to qudits without any change. This applies, in particular, to two disjoint sets of qubits in a quantum computer.

Remark: Consider two qudits a and b, with d and d' possible levels respectively. The ideal pure state of this pair of qudits is represented by a d by d' matrix. Our conjecture (roughly) asserts that when the state is not represented by (or close to) a rank one matrix then neither is the error. (Or at least part of the error.) We expect that in wider contexts it is not reasonable to expect noisy data described by general matrices to be well approximated up to a rank-one error matrix.

3.2 Error synchronization

A simple way to describe error-synchronization is in terms of the expansion of the quantum operation E in terms of multi-Pauli operators. A quantum operation E can be expressed as a linear combination

$$E = \sum v^I P^I,$$

where I is a multi-index $i_1, i_2, \ldots, i_n$, where $i_k \in \{0, 1, 2, 3\}$ for every k, P^I is the quantum operation that corresponds to the tensor product of Pauli operators described by the multi-index I on the individual qubits, and v^I are vectors. We can describe the error distribution of E by

$$f(t) =: \sum \{\|v^I\|_2^2 : |I| = t\},$$

and regard $\int f(t)t$ as the error rate.

Suppose that the error rate is a. All noise models studied in the original papers of the "threshold theorem," as well as some extensions that allow time- and space- dependencies (e.g., [24]), have the property that $f(t)$ decays exponentially (with n) for $t = (a + \epsilon)n$, where a is the error rate and $\epsilon > 0$ is any fixed real number.

In contrast, we say that E leads to *error-synchronization* if $f(\geq t)$ is substantial for some $t >> a$. We say that E leads to a *strong* error-synchronization if $f(\geq t)$ is substantial for $t = 1/2 - \delta$ where $\delta = o(1)$ as n

tends to infinity, and to *very strong* error-synchronization if $f(\geq t)$ is substantial for $t = 3/4 - \delta$ where $\delta = o(1)$ as n tends to infinity. A random unitary operator on the qubits of the computer with or without additional qubits representing the environment admits a very strong error-synchronization.

3.3 Censorship

Here is a suggestion for an entropy-based mathematical formulation for Conjecture [C]. We remind the reader that in this section we always assume that the "ideal" state of the quantum computer (before the noise is applied) is a pure state. Some adjustments to our conjectures will be required when the ideal state itself is a mixed state.

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

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

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.

Next, define

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

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

Conjecture **[C]**: 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,

$$\widetilde{ENT}(\rho) \leq P(n). \tag{2}$$

4 Extensions

4.1 General quantum systems

The purpose of Section 3 was to describe formally the conjectures on decoherence of quantum computers based on the basic model for such a computer. In the context of general quantum systems these conjectures are thus somewhat arbitrary. (In particular, we always talk about Hilbert spaces of dimensions 2^m.) The main idea behind the conjectures is that the error-independence assumption (for different qubits) amounts to an extremely strong dependence of the errors on the tensor product structure of the Hilbert space describing the state of the computer. It can be useful to suggest and examine formulations of our conjectures which do not depend on the tensor product structure of the Hilbert space in question.

We want to consider quantum physical systems described by a complex Hilbert space V. Our conjectures suggest that if E represents the error for state ρ and E' represents the error for state $U(\rho)$, for a unitary operator U on V, then E' will be "close" to $U^{-1}EU$. In particular, this implies that if $U(\rho) = \rho$ then E' is "close" to $U^{-1}EU$; hence UE is "close" to EU. In other words, E and U "tend" to commute if $U(\rho) = \rho$.

Here is a first attempt at a formal conjecture. We will restrict our attention to the case where the error is described by a quantum operation E which is a convex combination of unitary operators.

[D] There is an $\alpha > 0$ such that a prescription (or description) of a noisy quantum system at a state ρ is subject to error E with the property that for every unitary operator U such that $U(\rho) = \rho$

$$\|EU - UE\|_2 \quad \leq (1 - \alpha)\sqrt{2}. \tag{3}$$

Here we do not insist that the prescribed (or described) state be pure.

Remark: Greg Kuperberg pointed out that at a thermodynamics equilibrium a certain limiting error E will actually commute with every U that stabilizes ρ. One possible way to regard Conjecture [D] is as a statement referring to non-equilibrium thermodynamics.[1]

4.2 Classical noise

Conjectures [A] and [B] were motivated and originally formulated in [26] also for "natural" noisy classical correlated systems. For example, the analog of [A] asserts that in a noisy system the errors for two highly correlated elements tend to be substantially correlated. Because of the heuristic (or subjective) nature of the notion of noise in classical systems (and of the notion of probability itself), such a formulation, while of interest, leads to several difficulties.

Understanding noise and the study of de-noising methods span wide areas. (For example, in machine learning we can see the example where text and speech represent respectively the intended (ideal) and noisy signals.) Certain statistical methods of de-noising are based on assumptions that run contrary to [A]. However, our conjectures are in agreement with insights asserting that such statistical de-noising methods will leave a substantial amount of noise uncorrected. Moreover, "natural" examples of noisy highly correlated classical systems exhibit a moderate degree of dependence and appear to be in agreement with Conjecture [C].

[1] In this context, the works (and even the small controversy) on quantum analogs of "Onsager's regression theorem" come to mind.

5 Examples and models

5.1 Unprotected quantum circuits

A basic remaining challenge is to present concrete models of noise that support our conjectures.

We first point out that error-synchronization is a familiar phenomenon for error propagation of *unprotected* quantum programs (or circuits). Take the standard model of independent errors and suppose that the error rate is so small that it accumulates at the end of the computation to a small constant-rate error. It is instructive to see in this context that error-synchronization (and also [A] and [C]) are often created. (This goes back to Unruh [6].) Understanding the nature of errors described by ordinary models of noise applied to unprotected programs is of further interest. We should offer a precise definition of "unprotected programs." A random circuit leading to a given state ρ or a random perturbation of a specific circuit leading to ρ may serve this purpose. In such a model the errors for a certain state ρ of the computer do depend systematically on the state itself, and understanding this further may be of interest.

Remark: For noise propagation for unprotected programs the error rate is also related to the intended state. In this paper we assume that the error rate (in each computer cycle) is small and fixed. Trying to understand systematic relations between the error rate itself and the intended state ρ may be of interest. A natural informal conjecture would be

[E] In any noisy quantum computer the more entangled the intended state is, the higher the (detrimental) error rate.

Conjecture [E] is close to the negation of the FTQC hypothesis and as such it cannot be very useful. If FTQC fails then propagation of errors will make the error rate dependent on the amount of computation leading to ρ. A useful form of [E] should relate directly (not through computational notions)

the error rate to an entanglement measure and perhaps be formulated for general quantum systems. One possibility for such a connection is that when the evolution of a quantum system is prescribed, the rate of detrimental errors depends on the overall space of unitary operators which describe the incremental changes along the evolution.[2] [3]

5.2 Models

As much as error propagation for unprotected programs may supply useful insights it is not directly relevant to our conjectures. We emphasize that a model for decoherence that supports conjectures [A] and [B] (and [E]) should already exhibit [A] and [B] (and [E]) for the "new errors" — either storage errors or gate errors[4] or both — and thus be quite different from current models and current perceptions regarding noise. Models that satisfy our conjectures may be based on the storage-errors (in a single computer cycle) being represented by a rather primitive (but quick) stochastic quantum program (or circuit).

Remarks: 1) Such noise models can be regarded as a further step in the direction considered recently by Aharonov, Kitaev, and Preskill [24] (and a few earlier works). In these works, interactions between nearby qubits that

[2] In some models of decoherence (such as those related to "Lindblad dynamics"), when the decoherence is described as the effect of several non-commuting noise operations, the rate of decoherence is related to "uncertainty measures" for the quantum nature of these noise operators. Thus properties of decoherence in the spirit of our conjectures may reflect on the rate of decoherence.

[3] The rate of detrimental decoherence may reflect the process leading to the current state and also the ability of the device to carry the prescribed evolution ahead. For example, the rate of detrimental decoherence for faraway entangled photons may well be zero. But any intervention to bring them back together in order to carry additional joint operations is expected to introduce strong correlation between their errors.

[4] As mentioned we should allow gate errors to "apply" also to qubits not involved in the gate. Allowing this may reflect several concerns expressed in the literature regarding the qubit/gate model such as the issue of "slow" gates [27].

lead to statistical dependence between the noise acting on them is considered and it is shown that the threshold theorem prevails if the independence assumption still applies to faraway qubits. Interactions between nearby qubits expressed by a quick quantum circuit may lead to errors that are not covered by the assumptions of [24].

2) Klesse and Frank [28] described a physical system in which qubits (spins) are coupled to a bath of massless bosons and thet reached (after certain simplifications) a noise model with error-synchronization.

3) The earlier models suggested by Alicki, Horodecki, Horodecki, and Horodecki [23] appear to be relevant to our conjectures.

4) Let me also mention the relevance of *cluster states* defined by Briegel and Raussendorf (see, [29]). The description of cluster states involves an array of qubits located on the vertices of a rectangular lattice in the plane (or in space). Cluster states are "generated" by local entanglement between pairs of nearby qubits on the lattice grid. They can be regarded as the quantum analogs of the Ising and Potts classical models.

Controlled creation and manipulation of cluster states can be important for building quantum computers. On the other hand, cluster states and the local processes leading to them can possibly serve as a basis for concrete models of detrimental decoherence.

6 Computation complexity

Scott Aaronson's interesting "Sure/Shor challenge" [30] ask for restrictions on feasible (physical) states for quantum computers which do not allow for polynomial time factoring of integers and at the same time do not violate what can already be demonstrated empirically. This looks like a difficult challenge. In a similar spirit, while it looks intuitively correct that our conjectures are damaging for quantum computation, proving it, and especially proving a reduction all the way to the classical model of computation, is not

going to be easy.

A realistic task would be to show that our conjectures exclude fault tolerance based on linear quantum error-correction, e.g., deriving relations (1) and (2) (or even (3)) for any form of "protected qubits" obtained by linear quantum error-correction.[5]

A more ambitious goal than excluding quantum linear error-correction would be finding a reduction of noisy quantum computation (with detrimental errors) to the computational power of log-depth quantum circuits. (This will still fall short of Aaronson's challenge in view of a result by Cleve and Watrous [31].) Such reductions are known under the standard assumptions on noise, for reversible quantum computation [15], and when the error rate is above 45% [20].

When we insist on small error rate it may well be the case that log-depth polynomial size quantum circuits represent the true complexity power of quantum computers with detrimental errors. Consider a log-depth circuit, and suppose that the storage (and gate) errors demonstrate perfect error-synchronization. If we run the computation a polynomial number of times, with high probability there will be no errors in one of the runs. If we replace a given log-depth circuit by a larger one capable of correcting local errors we may reach polynomial size (or quasi-polynomial size) circuits that are immune to low-rate errors of the kind considered in this paper.

[5]Following is a simple argument proposed by Kuperberg why even the simplest form of conjecture [A] would not allow quantum computation. "If quantum computing is possible, then a quantum computer could have prepared a state S and then communicated it to the system that has the noise operation E. If it is true quantum computing, then S can be secret from E, for reasons similar to those that make quantum key distribution possible. In this case E can act on S but it cannot otherwise depend on it." The difficulty with this argument (as with a similar argument in Section 8.1) is that moving from a logical protected state S to a physical realization of S on a different device requires some computation and fault tolerance and thus relies on assumptions regarding errors which we cannot assume. Still Kuperberg's proposed reduction can be useful.

7 Conclusion

If (or when) true, our conjectures on the nature of information leaks (decoherence) for quantum computers are damaging to the possibility of storing and manipulating highly entangled quantum qubits. The conjectures do not contravene quantum mechanics and, to the best of my knowledge, established physics phenomena. Nor do our conjectures contravene with the feasibility of classical forms of error-correction and fault-tolerant computation.

Testing these conjectures empirically may be possible for quantum computers with a relatively small number of qubits. The conjectures can also be refuted by constructions of highly stable qubits based on strong entanglement, such as stable non-Abelian anyons [17, 32, 33].

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, *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] R. Landauer, Is quantum mechanics useful? *Philos. Trans. Roy. Soc. London Ser. A* 353 (1995), 367–376.

[5] R. Landauer, The physical nature of information, *Phys. Lett. A* 217 (1996), 188–193.

[6] W. G. Unruh, Maintaining coherence in quantum computers, *Phys. Rev. A* 51 (1995), 992–997.

[7] E. Bernstein and U. Vazirani, Quantum complexity theory, *Siam J. Comp.* 26 (1997), 1411-1473. (Earlier version, *STOC*, 1993.)

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

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

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

[11] 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.

[12] 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.

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

[14] 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.

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

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

[17] 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), pp. 267–272, Amer. Math. Soc., Providence, RI, 2002.

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

[19] A. Razborov, An upper bound on the threshold quantum decoherence rate, quant-ph/0310136.

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

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

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

[23] 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.

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

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

[26] G. Kalai, How quantum computers can fail, quant-ph/0607021.

[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] R. Klesse and S. Frank, Quantum error correction in spatially correlated quantum noise, *Phys. Rev. Lett.* 95 (2005), 230503.

[29] R. Raussendorf, D.E. Browne, and H.J. Briegel, Measurement-based quantum computation with cluster states, *Phys. Rev. A* 68 (2003), 022312.

[30] S. Aaronson, Multilinear formulas and skepticism of quantum computing, *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, 118–127, ACM, New York, 2004., quant-ph/0311039.

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

[32] 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.

[33] G. Moore and N. Read, Nonabelions in the fractional quantum hall effect, *Nuclear Physics B* 360 (1991), 362-393.

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

8 Appendix: Conjecture [A] - stronger forms

Given a quantum operation E our measure

$$L(A) = L_E(A; \tau)$$

for the information leaks for a set A of qubits depended on a pure tensor product state τ. The two-qubits basic property of detrimental decoherence was made for every τ separately. For the stronger conjectures below we will continue to make the statements in terms of an auxiliary tensor product state τ. We will write $L(A) = L_E(A; \tau)$ and similarly delete E and τ from other definitions based on $L(A)$.

An alternative approach is as follows: Let ψ be the state of the computer's qubits and the environment that is represented by a set N of qubits. Let U be a unitary operator of the computer and environment qubits representing the noise. A standard measure of the information that the environment has on the qubits in A is

$$L'(A) = S(U(\psi)|_A) + S(U(\psi)|_N) - S(U(\psi)|_{A \cup N}).$$

For our purposes we take $\psi = \psi_0(A) \otimes \psi_1(N)$ where $\psi_1(N)$ is any pure state on the environement and $\psi_0(A)$ is the mixed state of maximum entropy on A. I would expect that $L'(A)$ can replace $L(A)$ for the formulation of Conjecture [A] and the stronger conjectures below.

8.1 Two qubits: A stronger version

We proceed to describe and motivate a stronger form of Conjecture [A] and an extension to more than two qubits.

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 that can be called "emergent entanglement," which we are now going to define. This measure, denoted by $EE(\rho; a, b)$, captures (roughly) the expected amount of entanglement among the two qubits when we measure some other qubits, "look at the outcome," and condition on all possible outcomes for the measurement. It appears to be related to Briegel and Raussendorf's notion of "persistent entanglement" [34].

For every representation ω of $\rho|_{\{a,b\}}$ as a mixture (convex combination) of joint states

$$\rho|_{\{a,b\}} = \sum_{i=1}^{t} p_k \rho_k,$$

let

$$ENT_\omega(\rho; a, b) = \sum p_k ENT(\rho_k; a, b).$$

Define

$$EE(\rho; a, b) = \max ENT_\omega(\rho; a, b),$$

where the maximum is taken over all representations ω. (We can assume that ω is a mixture of pure joint states.)

A strong form of relation (1) is

$$EL(a, b) \geq K(L(a), L(b)) \cdot EE(\rho; a, b), \tag{4}$$

where, as before, $K(x, y)/\min(x, y)^2 >> 0$ when x and y are positive and small.

The motivation for this strong version of Conjecture [A] 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 Conjecture [A] does not directly apply. Consider an error-correcting code and let s be the minimal number of qubits whose state "determines" that of the others, so

that once they are measured and their values 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 remaining qubits.

Now, if we assume Conjecture [A] and 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 Conjecture [A] should apply to pairs of qubits in a quantum computer running FTQC even though pairs of qubits are independent.

(Of course, this argument does not prove that for noisy quantum computers relation (5) follows from relation (1) since it relies on an assumption regarding the errors that we do not make. See also Section 6.)

8.2 More qubits

Here is a suggestion for an extension of the above conjecture from pairs of qubits to larger sets of qubits. This suggestion goes beyond Conjectures [A] and [B] and is related to a strong error-synchronization.

For a set $A = \{a_1, a_2, \ldots, a_m\}$ of m qubits recall that

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

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

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

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

Using these definitions we will extend our conjectures, given by relations (1) and (4), from pairs of qubits to larger sets of qubits. Let ρ be an ideal

state of the computer and let A be a set of m qubits. Extending (1) we conjecture that

$$EL(A) \geq K_m ENT(\rho|_A). \tag{5}$$

Here, $K_m = K_m(\{L(a) : a \in A\})$ is substantially larger than $\min\{L(a))) : a \in A\}^2$ and it vanishes when all the individual information leaks vanish.

Here again we further conjecture that for every representation ω of the state $\rho|_A$ as a convex combination $\rho|_A = \sum p_k \rho_k$ of pure joint states,

$$EL(A) \geq K_m \sum p_k ENT(\rho_k; A). \tag{6}$$

Remark: 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.

We will mention now some mathematical challenges. It will be interesting to prove relation (2) based on relation (5), and to formulate and prove weak and strong forms of error-synchronization based, respectively, on relations (1) and (5). A further goal would be to derive, based on the assumptions on noise for the physical qubits (relations (5) and (6)), the same relations as well as relation (2), for "protected" qubits, namely logical qubits represented by quantum error-correction. It will also be of interest to find the right general formulation of "tend to commute" as in relation (3) and to relate it to the specific conjectures for quantum computers.

The additional conjectures of this section are meant to draw the following picture: we have an ideal notion of a quantum computer that 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 that 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.