When Noise Accumulates

Gil Kalai *

Abstract

We propose a model for noisy quantum evolutions where the noise is forced to accumulate, and consider related noise models, called "detrimental noise," that will cause quantum error correction and fault-tolerant quantum computation to fail. We start with properties of detrimental noise for two qubits and proceed to a discussion of highly entangled states, the rate of noise, and general noisy quantum systems.

1 Introduction

Quantum computers were offered by Feynman and others and formally described by Deutsch [12]. The idea was that since computations in quantum physics require an exponential number of steps on digital computers, computers based on quantum physics may outperform classical computers. A spectacular support for this idea came with Shor's theorem [27] that asserts that factoring is in BQP (the complexity class described by quantum computers).

The feasibility of computationally superior quantum computers is one of the most fascinating and clear-cut scientific problems of our time. The main concern regarding quantum-computer feasibility is that quantum systems are inherently noisy. (This concern was put forward in the mid-90s by Landauer [21, 22], Unruh [30], and others.)

The theory of quantum error correction and fault-tolerant quantum computation (FTQC) and, in particular, the *threshold theorem* [3, 18, 19], which asserts that under certain conditions FTQC is possible, provides strong support for the possibility of building quantum computers.

However, as far as we know, quantum error correction and quantum fault tolerance (and the highly entangled quantum states that enable them) are not experienced in natural quantum processes. It is therefore not clear if computationally superior quantum computation is necessary to describe natural quantum processes.

We will try to address two closely related questions. The first is, what are the properties of quantum processes that do not exhibit quantum fault tolerance and how to formally model such processes. The second is, what kind of noise models cause quantum error correction and FTQC to fail.

A main point we would like to make is that it is possible that there is a systematic relation between the noise and the intended state of a quantum computer. Such a systematic relation does not violate linearity of quantum mechanics, and it is expected to occur in processes that do not exhibit fault tolerance.

Let me give an example: suppose that we want to simulate on a noisy quantum computer a certain bosonic state. The standard view of noisy quantum computers asserts that this can be done up to some error that is described by the computational basis. In contrast, the type of noise we expect amounts to having a mixed state between the intended bosonic state and other bosonic states (that represent the noise).

The first obvious obstacle for fault tolerance, supported by the threshold theorem, is that fault tolerance fails "above the threshold," namely, when the noise rate is high. There are several papers ([3, 26, 9, 17]) that show that a high error rate is an obstacle for fault-tolerant quantum computation (and also for fault-tolerant classical computation). Another simple suggestion (see, e.g., [25],) that we will study here is that highly correlated noise may cause quantum error cor-

*kalai@math.huji.ac.il, The Hebrew University of Jerusalem and Yale University. Work supported by a NSF grant and by a BSF grant.

rection and fault tolerance to fail.

The paper relies on a more detailed discussion paper [13], see also [15, 14, 16]. We will now describe the structure of the paper. Section 2 describes the basic framework for noisy quantum computers and the threshold theorem.

While a major property of FTQC is that it allows suppression of noise propagation, in Section 3 we propose a mathematical model that aims to describe quantum evolutions with unsuppressed noise propagation. The model is a variation of the standard model with a certain additional "smoothing" in time. A formal definition of detrimental noise based on this model is given.

In Section 4 we discuss highly correlated noise, the notion of noise synchronization, and the rate of highly correlated noise. We draw a line between the types of correlations to which the threshold theorem applies and those to which it does not apply.

In Section 5, we propose two conjectures about detrimental noise: the first is in terms of two-qubit behavior, and the second is in terms of many highly entangled qubits states. The two-qubit conjecture asserts informally that information leaks for two entangled qubits are necessarily positively correlated. The second conjecture asserts that the noise for a highly entangled state manifests strong error synchronization.

In Section 6 we describe how our picture of decoherence differs from the standard one for general quantum systems. In Section 7 we discuss linearity, causality, and the rate of detrimental noise. In Section 8 we discuss some computational complexity aspects, and in Section 9 we briefly discuss physical aspects.

2 Quantum computers, noise, fault tolerance, and the threshold theorem

2.1 Quantum computers and noisy quantum computers

We assume the standard model of quantum computer based on qubits and gates with pure-state evolution. The state of a quantum computer with n qubits is a unit vector in a complex Hilbert space $\mathcal{H}$: the 2^n-dimensional tensor product of 2-dimensional complex vector spaces for the individual qubits. 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 the (2^k-dimensional) tensor product of the spaces that correspond to these k qubits. At every "cycle time" a large number of gates acting on disjoint sets of qubits operate. We will assume that measurement of qubits that amount to a sampling of 0-1 strings according to the distribution that these qubits represent is the final step of the computation.

The basic locality conditions for noisy quantum computers asserts that the way in which the state of the computer changes between computer steps is approximately statistically independent for different qubits. We will refer to such changes as "storage errors" or "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, and hence the errors (referred to as "gate errors") created on the few qubits involved in a gate can be statistically dependent. We will denote as "fresh errors" the storage errors and gate errors in one computer cycle. Of course, qubit errors and gate errors propagate along the computation. The "overall error" describing the gap between the intended state of the computer and its noisy state takes into account also the cumulated effect of errors from earlier computer cycles.

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.

In this paper we will consider the same model of quantum computers with more general notions of errors. We will study more general models for the fresh errors. (We will not distinguish between the different components of fresh errors, gate errors and storage errors.) Our models require that the storage errors not be statistically independent (on the contrary, they should be very dependent) or that the gate errors not be restricted to the qubits involved in the gates and be of sufficiently general form.

There are several other models of quantum computers that are equivalent in terms of their computa-

tional power to the one described here. This equivalence does not extend automatically to noisy versions and exploring fault tolerance in noisy versions of these models is an important challenge in FTQC.

2.2 The threshold theorem

We will not specify the noise at each computer cycle but rather consider a large set, referred to as the *noise envelope*, of quantum operations the noise can be selected from.

Let $\mathcal{D}$ be the following envelope of noise operations for the fresh errors: the envelope for storage errors $\mathcal{D}_s$ will consist of quantum operations that have a tensor product structure over the individual qubits. The envelope for gate errors $\mathcal{D}_g$ will consist of quantum operations that have a tensor product structure over all the gates involved in a single computer cycle (more precisely, over the Hilbert spaces representing the qubits in the gates). For a specific gate the noise can be an arbitrary quantum operation on the space representing the qubits involved in the gate. (The threshold theorem concerns a specific universal set of gates $\mathcal{G}$ that is different in different versions of the theorem.)

Theorem 2.1 (Threshold theorem)**.** *[3, 18, 19] Consider quantum circuits with a universal set of gates $\mathcal{G}$. A noisy quantum circuit with a set of gates $\mathcal{G}$ and noise envelopes $\mathcal{D}_s$ and $\mathcal{D}_g$ is capable of effectively simulating an arbitrary noiseless quantum circuit, provided that the error rate for every computer cycle is below a certain threshold $\eta > 0$.*

The value of the threshold in original proofs of the threshold theorem was around $\eta = 10^{-6}$ and it has since been improved by at least one order of magnitude. Recently, Knill [20] used error-detection codes rather than error-correction codes and massive post-selection for raising the value of η (based on numerical simulations) to 3%. (It also leads to substantially higher provable bounds [7].)

The threshold theorem relies on another important assumption. It is allowed to add new qubits, "cold ancillas" that are initialized to an error-free state $|0\rangle$. Roughly speaking, they are needed to "cool" the system. We will continue to make this assumption for our adversarial noise models throughout the paper.

3 Modeling quantum systems with unsuppressed noise propagation

A main property of FTQC is that it enables us to suppress noise propagation: the effect of the noise at a certain computer cycle diminishes almost completely already after a constant number of computer cycles. In this section we would like to formally model quantum systems for which noise propagation is not suppressed.

A way to force unsuppressed noise propagation into the model is as follows. Start with an ideal quantum evolution $\rho_t : 0 \leq t \leq 1$ and suppose that $U_{s,t}$ denotes the unitary operator describing the transformation from time s to time t, ($s < t$). Next consider a noisy version where E_t is a noise operation describing the infinitesimal noise at time t.

We will now describe a certain "smoothing" in time of the noise. Let K be a positive continuous function on [-1,1]. (We can assume that K is supported in a neighborhood of 0.) We write $\bar{K}(t) = \int_{t-1}^{t} K(s)ds$. Replace the noise E_t at time t by

$$E'_t = \tag{1}$$

$$(1/\bar{K}(t)) \cdot \int_0^1 K(t-s)U_{s,t}E_sU_{s,t}^{-1}ds.$$

> **Main Conjecture:** (i) Relation (1) properly models natural noisy quantum systems,
>
> (ii) It will not allow quantum fault tolerance.[1]

For the rest of the paper we will restrict somewhat the class of noise operators and we will suppose that E_t and hence E'_t are described by POVM-measurements (see [24], Chapter 2).

> **Definition:** *Detrimental noise* refers to noise (described by a POVM-measurement) that can be described by equation (1).

What could be a motivation for our main conjecture? We will mention four reasons:

[1] For the second part of the conjecture we take noiseless classical computation for granted and continue to assume unlimited supply of "cold ancillas." We get both these assumptions for free from our conjecture on the rate of noise in Section 7.3.

1) Regardless of the feasibility of quantum computers, unsuppressed noise propagation appears to be the rule for open quantum systems in nature. The reason is that we do not witness in nature quantum error correction needed to suppress noise propagation or other mechanisms for this purpose. Relation (1) should allow modeling information leaks for quantum systems in nature.

2) We expect that properties of unsuppressed noise propagation can have various other physical causes.

3) If FTQC is not possible by whatever fundamental principle, the conclusion is that noise propagation cannot be suppressed. If unsuppressed noise propagation is a consequence of any hypothetical fundamental principle that would cause FTQC to fail, we may as well consider unsuppressed noise propagation to be such a fundamental principle.

4) We expect that the main conjecture will have interesting mathematical consequences leading to a coherent picture.

We can replace relation (1) by a discrete-time description. When we consider a quantum computer that runs T computer cycles, we start with standard storage noise E_t for the t-step. Then we consider instead the noise operator

$$E'_t = 1/(\sum_{s=1}^{T} K((t-s)/T))\cdot \sum_{s=1}^{T} K((t-s)/T)U_{s,t}E_tU_{s,t}^{-1}, \quad (2)$$

where again $U_{s,t}$ is the intended unitary operation between step s and step t.

Remarks: 1. Relation (1) is offered as a mathematical device to describe the situation where noise propagation is not suppressed. Relation (1) can represent various scenarios. It may apply to noisy quantum circuits with standard noise above the threshold. It can apply simply to standard noisy quantum circuits that do not contain error-correction ingredients.

Relation (1) resembles somewhat the suggestion that in the qubits/gates model, the gates are "slow" (not instantaneous) and the noise occurs continuously as gates are being applied. This notion appears in skeptical works regarding quantum computers ([6]), and is also taken into account in various threshold theorems [4]. (Our description, interpreted this way, amounts to "very slow gates," where the action of a gate spans a constant fraction of the entire evolution. Even for such a harsh assumption, the possibility of FTQC can be quite delicate.)

2. In relation (1), it is not enough to assume that K is supported in an interval $[0, t]$ for some positive real t. Greg Kuperberg pointed out that in this case FTQC is possible!

4 Correlated noise and noise synchronization

4.1 Describing error synchronization via Pauli expansion

The concern regarding highly correlated noise has been raised in several papers, yet there have been only a few systematic attempts to study what kind of correlated errors will cause the threshold theorem to fail.[2]

Error synchronization refers to a situation where, while the expected number of qubit errors is small, there is a substantial probability of errors affecting a large fraction of qubits.

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

$$E = \sum v^w P_w, \quad (3)$$

where w is a word of length n $(i_1, i_2, \ldots, i_n)$, and $i_k \in \{I, X, Y, Z\}$ for every k, v^w is a vector, and P^w is the quantum operation that corresponds to the tensor product of Pauli operators whose action on the individual qubits is described by the multi-index w.

The amount of error on the kth qubit is described by $\sum\{\|v^w\|_2^2 : i_k \neq I\}$. For a multi-index w define $|w| := |\{k : i_k \neq I\}|$. Let

$$f(s) := \sum\{\|v^w\|_2^2 : |w| = s\}.$$

We regard $\sum_{s=1}^{n} f(s)s$ as the *expected number of qubit errors*.

[2] Of course, everyone has always known that the threshold theorem will fail for some noise models; e.g., it's hard to protect your quantum computer (or digital computer for that matter) from a meteor strike. But such models were considered as uninteresting and unrealistic.

Define the *rich error syndrome* to be the probability distribution described by assigning to the word w the value $\|v^w\|$ (normalized). We will define the *coarse error syndrome* as the binary word of length n obtained from w by replacing I with '0' and the other letters by '1'. Given a noise operation E, the distribution $\mathcal{E}$ of the rich error syndrome is an important feature of the noise. Given E we will denote by $\mathcal{D}$ the probability distribution of coarse error syndrome. $f(s)$ is simply the probability of a word drawn according $\mathcal{D}$ having s '1's.

Suppose that the expected number of qubit errors is αn where n is the number of qubits.

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., [29, 7, 4]), have the property that $f(s)$ decays exponentially (with n) for $s = (\alpha + \epsilon)n$, where $\epsilon > 0$ is any fixed real number. (This is particularly simple when we consider storage error, which is statistically independent over different qubits.)

In contrast, we say that E leads to *error synchronization* if $f(\geq s)$ is substantial for some $s \gg \alpha n$. We say that E leads to a *very strong* error synchronization if $f(\geq s)$ is substantial for $s = 3/4 - \delta$ where $\delta = o(1)$ as n tends to infinity. By "substantial" we mean larger than some absolute constant times α/s, or, in other words, the multi-Pauli terms for $|I| \geq s$ contributes a constant fraction of the expected number of qubit errors.

Remark: Error syndromes obtained by measuring the noise in terms of the tensor product of Pauli operators is an important ingredient of several fault-tolerant schemes. Note that our definition of the rich error syndrome (unlike error-syndromes used in quantum error correction) is based on the quantum operation E representing the noise. (Since quantum states can have non-trivial Pauli stabilizers the rich error syndrome is not defined uniquely just in terms of the intended and noisy states.)

4.2 Generic noise

Proposition 4.1. *Conditioning on the expected number αn of qubit errors, a random unitary operator acting on all the qubits of the computer yields a very strong error synchronization.*

The proposition extends to the case where we allow additional qubits representing the environment.

The proof of Proposition 4.1 is based on a standard "concentration of measure" argument (see, e.g., [23]). (We will give only a rough sketch.) When we consider a typical expression of the form $\sum a_w P_w$ where $\sum a_w^2 = 1$ and $\sum\{a_w^2|w|\} = an$, it will have a large support on $a_{\mathbf{0}}$ and the other coefficients will be supported on a_w where w itself is typical; i.e., I (the error syndrome) behaves like a random string of length n with entries I,X,Y,Z. Hence $|w|$ is around $(3/4)n$.

How relevant is Proposition 4.1? It is well known that random unitary operations on the entire 2^n-dimensional vector space describing the state of the computer are not "realistic" (in other words, not "physical" or not "local"). The best formal explanation why random unitary operators are "not physical" is actually computational and relies on the following well-known

Proposition 4.2. *For large n, it is impossible to express or even to approximate a random unitary operator using a polynomial-size quantum circuit with gates of bounded fan-in (namely, gates that operate on a bounded number of qubits).*

An interesting problem (posed in [16]) is to what extent we can describe the basic statistical properties of a random unitary operation U, conditioned on the value of $a(U)$, as the outcome of simple polynomial-size quantum circuits.

4.3 The boundary of the threshold theorem

Recent works [29, 7, 4] show that the threshold theorem prevails if we allow certain space- and time-dependencies for the noise operations. We would now like to draw a distinction between noise models that support the threshold theorem and noise models that do not.

For a quantum operation E describing the noise for a quantum computer with n qubits we denote by $\alpha(E)$ the expected number of qubit errors in terms of the multi-Pauli expansion as described above.

Proposition 4.3. *For the known noise models that allow FTQC via the threshold theorem:*

1) The fresh noise E expanded in terms of multi-Pauli operations decays exponentially above $\alpha(E)$.

2) The overall (cumulated) noise E' expanded in terms of multi-Pauli operations decays exponentially above $\alpha(E')$.

There is an even simpler property of fresh and cumulated noise for noise models for which the threshold theorem holds.

Proposition 4.4. *For the known noise models that allow FTQC via the threshold theorem:*

3) The fresh noise (at every computer cycle) for almost every pair of qubits in the computer is almost statistically independent for the two qubits in the pair.

4) The overall noise for almost every pair of qubits in the computer is almost statistically independent for the two qubits in the pair.

Here when we talk about "almost every pair" we refer to $(1 - o(1))\binom{n}{2}$ of the pairs when n is large.

The (rich) error syndrome will provide a simple way to express correlation between the noise acting on two qubits. For two qubits i and j, denote by $cor_{ij}(E)$ the correlation between the events that the qubit i is faulty and the event that the qubit j is faulty. In other words, $cor_{ij}(E)$ is the correlation between the events that w_i is not I, and w_j is not I when w is a word drawn according to the distribution of error syndromes described by E. Proposition 4.4 implies, in particular, that for models allowing the threshold theorem, $cor_{ij}(E)$ and $cor_{ij}(E')$ are close to 0 for most pairs i, j of qubits. We will further discuss two-qubit behavior in Section 5.

Note that properties 1 and 3 refer to the noise model, which is one of the assumptions for the threshold theorem, while properties 2 and 4 are consequences of the threshold theorem and, in particular, of suppressing error propagation. For the very basic noise models where the storage errors are statistically independent property 3 follows from the fact that the number of pairs of interacting qubits at each computer cycle is at most linear in n. Property 3 continues to hold for models that allow decay of correlations between qubit errors that depend on the (geometric) distance between them. Property 1 is a simple consequence of the independence (or locality) assumptions on the noise for noise models that allow the threshold theorem.

4.4 The rate of highly correlated noise

Recall that the trace distance $D(\sigma, \rho)$ between two density matrices ρ and σ is equal to the maximum difference in the results of measuring ρ and σ in the same basis. $D(\sigma, \rho) = 1/2\|\sigma - \rho\|_{tr}$. When the error is represented by a quantum operation E the rate of error for an individual qubit is the maximum over all possible states ρ of the qubit of the trace distance between ρ and $E(\rho)$.

Highly correlated errors are damaging for quantum error correction, but a potentially even more damaging property we face for highly correlated noise is that the notion of "rate of noise for individual qubits" becomes sharply different from the rate of noise as measured by trace distance for the entire Hilbert space describing the state of the computer.

Consider two extreme scenarios. In the first scenario, for a time interval of length t there is a depolarizing storage noise that hits every qubit with probability pt. In the second scenario the noise is highly correlated: all qubits are hit with probability pt and with probability $(1 - pt)$ nothing happens. In terms of the expected number of qubit errors both these noises represent the same rate. The probability of every qubit being corrupted at a time interval of length t is pt. However, in terms of trace distance (and here we must assume that t is very small), the rate of the correlated noise is n^{-1} times that of the uncorrelated noise. What should be the correct assumption for the rate of noise when we move away from the statistical independence assumption? If noise propagation is the "role model" then measuring the noise in terms of trace distance for the entire Hilbert space appears to be correct.

5 Detrimental noise from two qubits to many

5.1 Two conjectures

In this subsection we present qualitative statements of two conjectures concerning decoherence for quantum computers which, if (or when) true, are damaging to quantum error correction and fault tolerance.

The first conjecture concerns entangled pairs of qubits.

Conjecture A: A noisy quantum computer

is subject to error with the property that information leaks for two substantially entangled qubits have a substantial positive correlation.

We emphasize that Conjecture A refers to part of the overall error affecting a noisy quantum computer. Other forms of errors and, in particular, errors consistent with current noise models may also be present.

Recall that error synchronization refers to a situation where, although the error rate is small, there is nevertheless a substantial probability that errors will affect a large fraction of qubits.

Conjecture B: In any noisy quantum computer in a highly entangled state there will be a strong effect of error synchronization.

We should informally explain already at this point why these conjectures, if true, are damaging. We start with Conjecture B. The states of quantum computers that apply error-correcting codes needed for FTQC are highly entangled (by any formal definition of "high entanglement"). Conjecture B will imply that at every computer cycle there will be a small but substantial probability that the number of faulty qubits will be much larger than the threshold.[3] This is in contrast to standard assumptions that the probability of the number of faulty qubits being much larger than the threshold decreases exponentially with the number of qubits. Having a small but substantial probability of a large number of qubits being faulty is enough to cause the quantum error-correction codes to fail.

Why is conjecture A damaging? Here the situation is trickier since without some additional assumptions conjecture A is not relevant to the highly entangles states used for FTQC. For such states, pairs of qubits are not entangled.

Let us make the additional assumption that individual qubits can be measured without inducing errors on other qubits. This is a standard assumption regarding noisy quantum computers.[4] When we start from highly entangled states needed for FTQC and measure (and look at the results for) all but two qubits, we will reach pairs of qubits (whose intended state is pure) with almost statistically independent noise, in contrast to Conjecture A. Under this assumption it is also possible to deduce Conjecture B from Conjecture A.

5.2 Mathematical formulation of Conjecture A

In this subsection we will describe a mathematical formulation of Conjecture A.

The first step in this formal definition is to restrict our attention to noise described by POVM-measurements. This is a large class of quantum operations describing information leaks from the quantum computer to the environment.

Our setting is as follows. Let ρ be the intended ("ideal") state of the computer and consider two qubits a and b. Consider a POVM-measurement E representing the noise. We describe correlation between the qubit errors via the expansion in tensor products of Pauli operators, or, in other words, via the error syndrome.

Associated to E (see Section 4.1) is a distribution $\mathcal{E}(E)$ of error syndromes, i.e., words of length n in the alphabet $\{I, X, Y, Z\}$. A coarser distribution $\mathcal{D}(E)$ of binary strings of length n is obtained by replacing the letter I with '0' and all other letters by '1'.

As a measure of correlation $cor_{i,j}(E)$ between information leaks for the ith and jth qubit we will simply take the correlation between the events $x_i = 1$ and $x_j = 1$ according to $\mathcal{D}(E)$.

We also define $r_i(E)$ as the probability that $x_i = 1$ according to the distribution $\mathcal{D}$.

We now discuss how to measure entanglement. Suppose that ρ is the intended state of the computer. For a set Z of qubits and a state ρ we denote by $\rho|_Z$ the density matrix obtained after tracing out the qubits not in Z. If Z contains only the ith qubit, we write ρ_i instead of $\rho|_Z$.

As a measure of entanglement we simply take the trace distance between the state induced on the two qubits and a separable state. Formally, let $SEP(i, j)$ denote the set of mixed separable states on $Z = \{i\} \cup \{j\}$, namely, states that are mixtures of tensor product pure states $\tau = \tau_i \otimes \tau_j$. Define $Ent(\rho : i, j) =$

[3] Here we continue to assume that the probability of a qubit being faulty is small for every computer cycle.

[4] It should be emphasized that the assumption that we can *always* measure a qubit without inducing errors on others, goes contrary to the picture of noisy quantum computers we try to draw. We use it to examine stronger forms of the notion of entanglement that are relevant.

$max\{\|\rho_{i,j} - \psi\| : \psi \in SEP(i,j)\}$.

Here is the statement of Conjecture A for two qubits:

Conjecture A: (mathematical formulation)

For every two qubits

$$cor_{i,j}(E) \geq \tag{4}$$

$$\geq K(r_i(E), r_j(E)) \cdot Ent(\rho : i, j).$$

Here, $K(x,y)$ is a function of x and y so that $K(x,y)/\min(x,y)^2 \gg 1$ when x and y are positive and small. (Note that Conjecture A) does not claim anything when the two qubits are noiseless.) If $r_i(E) = r_j(E) = \alpha$ for a small real number α, then the conjecture asserts that $cor_{i,j}(E) \gg \alpha^2$, and, as we will see later, this is what is needed to derive error synchronization.

Remark: We mainly use Conjecture A for the case where the two qubits are in joint pure state. In this case we can simply take the entropy of one of the qubits as the measure of entanglement.

5.3 Emergent entanglement and Conjecture B

We now describe Conjecture B formally and propose a strong form of Conjecture A for two qubits based on a notion of "emergent entanglement."

Definition: The *emergent entanglement* of two qubits is the maximum over all *separable* measurements of the remaining qubits of the expected amount of entanglement between the two qubits when we look at the outcome of the measurements.

Define a *highly entangled state* as a state where the expected emergent entanglement among pairs of qubits is large. This is the case for states used in quantum error correction. A strong form of Conjecture A is obtained if we take emergent entanglement as the measure of entanglement.

Theorem 5.1. *For noisy quantum computers Conjecture A implies conjecture B in the following two cases:*

(1) When we add the assumptions that qubits can be measured without introducing noise on other qubits.

(2) When we formulate Conjecture A for "emergent entanglement".

The proof is based on applying Proposition 5.1 below to the coarse error-syndrome.

Proposition 5.1. *Let $\eta < 1/20$ and $s > 4\eta$. Suppose that $\mathcal{D}$ is a distribution of 0-1 strings of length n such that $p_i(\mathcal{D}) \geq \eta$ and $cor_{ij}(\mathcal{D}) \geq s$. Then*

$$\mathbf{Prob}(\sum_{i=1}^{n} x_i > sn/2) > s\eta/4. \tag{5}$$

The proof of this proposition is described in [14].

5.4 Mathematical challenges and censorship

The main mathematical challenge is to show that Conjectures A and B are satisfied when we force unsuppressed noise propagation.

> **Main mathematical conjecture:** The assertion of Conjectures A and B are satisfied for noisy quantum computers where the noise is described by equation (1).

It will be interesting to check whether the assertion of Conjectures A and B holds for noisy adiabatic computers [11].

Several extensions of Conjecture A to pairs of qudits (rather than qubits), and to a larger number of qubits are proposed in [15, 14, 13]. Several alternative approaches for how to define "highly entangled states" for Conjecture B are also considered.

We can expect that detrimental noise will lead to "very highly entangled states" being completely infeasible for noisy quantum computers. Limitations on feasible states of a quantum computer are referred to as "censorship." Computational complexity poses severe restrictions on the feasible states of (noiseless) quantum computers. For example, as we already mentioned, a state that is approximately the outcome of a random unitary operator on the entire 2^n-dimensional Hilbert space is computationally out of reach when the number of qubits is large. We expect that detrimental noise will lead to further (statistical) restrictions on feasible states for noisy quantum computers and it will be interesting to study what can be the nature of such statistical censorship.[5] Some proposals in this direction are suggested in [13].

[5] One interesting potential aspect of statistical censorship (following suggestions by Ronnie Kosloff) is that there are mixed

6 Detrimental noise for general quantum systems

Consider the very simple example of a quantum computer where, when the quantum memory is in a state ρ and $\rho = U\rho_0$, the noise E will be UE_0U^{-1}. Here, ρ_0 is the initial state of the computer and U is the unitary intended evolution leading to ρ. When we try to describe the relation between the state of the computer and the noise, this example describes, for every state ρ, an envelope of noise $D_\rho = \{UE_0U^{-1} : U\rho_0 = \rho\}$. This is a huge class of quantum operations most of which are irrelevant (being computationally infeasible.) An important property of this noise is:

$$\mathcal{D}_{U\rho} = U\mathcal{D}_\rho U^{-1}. \quad (6)$$

Relation (6) amounts to saying that there is a component of quantum noise that is invariant under unitary operations and thus does not depend on the device that carries these operations. Note that relation (6) applies to the envelope of noise operations as a set (and not to individual quantum operations in the noise envelope).

As before, we restrict our attention to noise described by POVM-measurements. We can now ask: what are the laws of decoherence for general noisy quantum systems that follow the properties of (unsuppressed) noise propagation?

As with the case of standard models of noise, we would like to describe an envelope of noise, i.e., a large set of quantum operations, so that when we model noisy quantum operations or more general processes the incremental (or infinitesimal) noise should be taken from this envelope. Conjectures A and B propose some systematic connection between the noise and the state. However, in these conjectures both the assumption in terms of entanglement and the conclusion in terms of correlation rely on the tensor product structure of $\mathcal{H}$.

Here is a proposal on how to formalize this connection for general systems:

> **Definition:** A D-noise of a quantum system at a state ρ is a quantum operation E that commutes with some non-identity unitary quantum operation that stabilizes ρ.

states that cannot be "cooled." Such a property is not expected for computationally based censorship.

This definition describes a (huge) class $\mathcal{D}_\rho$ of quantum operations that respect the relation $\mathcal{D}_{U\rho} = U\mathcal{D}_\rho U^{-1}$.

> **Conjecture D:**
>
> D-noise cannot be avoided in a noisy quantum process described by relation (1).

On its own our suggested definition of D-noise is extremely inclusive, and so is any (nonempty) envelope of noise operations that satisfies relation (6). For example, a D-noise on a state of the form $\rho \otimes \rho$ can be standard even if ρ is highly entangled. However, there are two additional conditions we have to keep in mind:

1. The hypothesis that the overall noise contains a large D-component applies to every subsystem of our original system. (An appropriate "hereditary" version of Conjecture D may suffice to imply Conjectures A and B for noisy quantum computers. This has yet to be explored.)

2. The operation describing the noise should be "local"; namely, it should be computationally feasible in terms of local operations describing the system.

Remark: There are three related contexts for which the discussion of decoherence for quantum systems applies. The first and the closest to the discussion regarding quantum computers is when we regard the gap between an intended controlled evolution and the process actually carried out. A second context is the study of information leaks from the system to its environment. Finally, a third context is the study of errors in any *description* of the evolution of a noisy quantum system.

7 Linearity, causality, and rate

7.1 Linearity

Our conjectures for noisy quantum computers and for noisy quantum systems amount to a nonlinear relation between the noise envelope and the state of the computer. Such nonlinear relations do not violate linearity of quantum mechanics. For example, if we consider the noise in our main relation (1) as a function of

the entire evolution, then it is completely linear. Nonlinearity is caused by ignoring the entire evolution and considering the relation between the noise and the state for all possible evolutions leading to this state.

7.2 Causality

Consider an intended pure-state evolution ρ_t, $0 \leq t \leq 1$ of a quantum computer, and a noisy realization σ_t, $0 \leq t \leq 1$. Assuming that σ_t is close[6] to ρ_t for the *entire* time interval may create a systematic relation of the infinitesimal noise at an intermediate time t on the *entire* intended evolution ρ_t.[7]

It is a *consequence* of FTQC that the dependence of the errors on past evolution and on future intended evolution becomes negligible.

7.3 The rate of noise for noisy quantum evolutions

We can exhibit extremely stable entangled quantum states, and yet we believe that quantum systems are inherently noisy. We can also have isolated qubits that do not interact at all that are subject to uncorrelated noise, and yet we propose in this paper that for the appropriate model of noisy quantum computers the noise should be highly correlated. The noise (its rate and its form) depends on the fact that we need to manipulate the qubits, but what is the formal description of such a dependence?

When we model the fresh (or infinitesimal) noise for the evolution of a noisy quantum computer or even a general noisy system, what should be a lower bound on the rate of noise? This is an interesting issue even when it comes to a single noisy qubit.

Recall that the usual assumption regarding the rate of noise is that for every qubit the probability of it being faulty is a small constant for every computer cycle. We propose the following refinement of this assumption.

> **Conjecture E:** A noisy quantum computer is subject to (detrimental) noise with the following property: the rate of noise at time t (in terms of trace distance) is bounded from below by a measure of noncommutativity between the operators describing the evolution prior to time t and those describing it after time t.

The lower bound according to Conjecture E for the rate of noise when the process starts or ends is zero. The rate of noise can also vanish for classical systems where all the operations commute. (Conjecture E also gives cold ancillas qubits for free.) Conjecture E can be regarded as a proposed refinement on the assumptions regarding the rate of noise even for a single qubit.

8 Computational complexity

The problem of describing complexity classes of quantum computers subject to various models of noise was proposed by Peter Shor in the nineties. (Although we naturally expect computational power between BQP and BPP it is possible, in principle, that certain noise models will allow efficient algorithms even for problems not in BQP.) Scott Aaronson [1] asked for the computational complexity consequences of various hypothetical restrictions on feasible (physical) states for quantum computers. In particular, he posed the interesting "Sure/Shor challenge": to describe such restrictions that do not allow for polynomial-time factoring of integers and at the same time do not violate what can already be demonstrated empirically.

The threshold theorem and some of its recent versions give a fairly good description of the board models of noise that allow universal quantum computing when the noise rate is sufficiently small. There are several results ([5, 26, 17]) showing that for the standard noise models when the computation is reversible or when the noise rate is high, the computational power reduces to BPP (for some results) or BPP^{BQNC} (the power of classical computers together with log-depth quantum circuits).

How bad can the effect of correlated errors be? I tend to think that for an arbitrary form of noise, if the expected number of qubit errors in a computer cycle is sufficiently small then problems in BPP^{BQNC} and, in particular, polynomial-time factoring can prevail.[8]

[6] In some sense, e.g., in terms of the expected number of qubit errors.

[7] This is easier to understand if the success of σ_t in approximating ρ_t is achieved via post-selection.

[8] Cleve and Watrous [10] gave a polynomial algorithm for factoring that requires, beyond classical computation, only log-depth

A rough argument in this direction would go as follows. First replace a given log-depth circuit by a larger one capable of correcting standard errors; then run the computation a polynomial or quasi-polynomial (depending on the precise overhead in the fault-tolerant circuit) number of times to account for highly synchronized errors.

On the other hand, it may be possible (but not easy) to prove that highly correlated errors of the kind under consideration do not allow fault tolerance based on quantum error correction, and perhaps also that they suffice to reduce the computational power to BPP^{BQNC}.

The most interesting direction, in my opinion, would be to show that with the full power of detrimental errors, e.g., as defined in equation (1), including the conjectured effect on the expected number of qubit errors in one computer cycle (Sections 4.4,7.3), the computational power of noisy quantum computers reduces to BPP.

9 Physics

A criticism expressed by several readers of an early version of this paper is that no attempt is made to motivate the conjectures from a physical point of view and that the suggestions seem "unphysical." What can justify the assumption that a given error lasts for a constant fraction of the entire length of the process? If a noisy quantum computer at a highly entangled state has correlated noise between faraway qubits as we suggest, wouldn't it allow signaling faster than the speed of light?

It is important and may be fruitful, in our opinion, to examine various models of noise while putting the physics aside. Nevertheless, we will briefly discuss some physical aspects.

Let us go back to the example of simulating bosonic states with a noisy quantum computer. When errors accumulate I expect that a large (even dominant) part of the noise will not consist of local noise based on the computational bases but rather it will be a mix of the intended bosonic state with other unintended bosonic states.

We do not yet have quantum computers that simulate bosonic states but we do have several natural and experimental processes that come close to this description, like phonons, which can be regarded as a bosonic state (on a macroscopic scale) "simulated" on microscopic "qudits". (There are several other examples as well.) These examples can serve as a good place to examine noise.

Another place to examine some suggestions of this paper is current implementations of ion-trap computers. In these implementations we need to move qubits together in order to gate them, and this suggests that, in each computer cycle, errors will be correlated for *all* pairs of qubits. At present, the rate of noise is still the major concern of experimentalists, but it is not clear how a large pairwise correlation between all pairs of qubits can be avoided in current architecture. Specific alternative suggestions (based on teleportation) of performing gates for ion-trap computers without moving the qubits may not solve this problem since we cannot assume for these suggested implementations that measuring qubits will not induce noise on other qubits.

If our suggested properties of noise for some (hypothetical) quantum computer architecture at some quantum state ρ allow instantaneous signaling, then the proposed conclusion is that this quantum computer architecture simply does not accommodate the quantum state ρ.

Finally, another comment was that FTQC via topological quantum computing does not rely on the threshold theorem and Conjectures A and B are not relevant for this model. However, the underlying mathematics behind the threshold theorem and behind FTQC via topological quantum computers is quite similar. The extreme stability to noise expected for non-Abelian anyons (and Abelian anyons) relies on similar assumptions to those enabling quantum error correction. When we create Abelian anyons in the laboratory, or try to create non-Abelian anyons, there is no reason to believe that the process for creating them will involve suppression of propagated noise and therefore, just as when we simulate fermions or bosons, we expect a mixture of the intended state with other states of the same type. When noise accumulates there is no reason to expect the strong stability of certain anyons that is predicted by current models.

quantum computation.

References

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

[2] 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.

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

[4] D. Aharonov, A. Kitaev, and J. Preskill, Fault-tolerant quantum computation with long-range correlated noise, *Phys. Rev. Lett.* 96 (2006), 050504, quant-ph/0510231.

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

[6] 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.

[7] P. Aliferis, D. Gottesman, and J. Preskill, Quantum accuracy threshold for concatenated distance-3 codes, *Quant. Inf. Comput.* 6 (2006), 97–165, quant-ph/0504218.

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

[9] H. Buhrman, R. Cleve, N. Linden, M. Laurent, A. Schrijver, and F. Unger, New limits on fault-tolerant quantum computation, *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2006, pp. 411–419, quant-ph/0604141.

[10] R. Cleve and J. Watrous, Fast parallel circuits for the quantum Fourier transform, *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, 2000, pp. 526–536, quant-ph/0006004.

[11] A. M. Childs, E. Farhi, and J. Preskill, Robustness of adiabatic quantum computation, *Phys. Rev A* 65 (2002), 012322, quant-ph/0108048.

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

[13] G. Kalai, Quantum computers: noise propagation and adversarial noise models, 2009, arXiv:0904.3265.

[14] G. Kalai, Detrimental decoherence, 2008, quant-ph/08062443.

[15] G. Kalai, How quantum computers can fail, 2006, quant-ph/0607021.

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

[17] J. Kempe, O. Regev, F. Unger, and R. de Wolf, Upper bounds on the noise threshold for fault-tolerant quantum computing, quant-ph 0802.1462.

[18] 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.

[19] 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.

[20] E. Knill, Quantum computing with very noisy devices, *Nature* 434 (2005), 39-44, quant-ph/0410199.

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

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

[23] M. Ledoux, *The Concentration of Measure Phenomenon*, American Mathematical Society, Providence, RI, 2001.

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

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

[26] A. Razborov, An upper bound on the threshold quantum decoherence rate, *Quantum Information and Computation* 4 (2004), 222-228, quant-ph/0310136.

[27] 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.)

[28] P. Shor, Fault-tolerant quantum computation, *Annual Symposium on Foundations of Computer Science*, 1996.

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

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