Upper Bounds on the Noise Threshold for Fault-tolerant Quantum Computing

Julia Kempe* Oded Regev† Falk Unger‡ Ronald de Wolf§

April 17, 2008

Abstract

We prove new upper bounds on the tolerable level of noise in a quantum circuit. We consider circuits consisting of unitary k-qubit gates each of whose input wires is subject to depolarizing noise of strength p, as well as arbitrary one-qubit gates that are essentially noise-free. We assume that the output of the circuit is the result of measuring some designated qubit in the final state. Our main result is that for $p > 1 - \Theta(1/\sqrt{k})$, the output of any such circuit of large enough depth is essentially independent of its input, thereby making the circuit useless. For the important special case of $k = 2$, our bound is $p > 35.7\%$. Moreover, if the only allowed gate on more than one qubit is the two-qubit CNOT gate, then our bound becomes 29.3%. These bounds on p are notably better than previous bounds, yet are incomparable because of the somewhat different circuit model that we are using. Our main technique is the use of a Pauli basis decomposition, which we believe should lead to further progress in deriving such bounds.

1 Introduction

The field of quantum computing faces two main tasks: to build a large-scale quantum computer, and to figure out what it can do once it exists. In general the first task is best left to (experimental) physicists and engineers, but there is one crucial aspect where theorists play an important role, and that is in analyzing the level of noise that a quantum computer can tolerate before breaking down.

The physical systems in which qubits may be implemented are typically tiny and fragile (electrons, photons and the like). This raises the following paradox: On the one hand we want to isolate these systems from their environment as much as possible, in order to avoid the noise caused by unwanted interaction with the environment—so-called "decoherence". But on the other hand we

[*] School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel. Supported by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848, by an Alon Fellowship of the Israeli Higher Council of Academic Research and by an Individual Research Grant of the Israeli Science Foundation.

[†] School of Computer Science, Tel-Aviv University, Tel-Aviv 69978, Israel. Supported by the Binational Science Foundation, by the Israel Science Foundation, and by the European Commission under the Integrated Project QAP funded by the IST directorate as Contract Number 015848.

[‡] Partially supported by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

[§] Partially supported by a Veni grant from the Netherlands Organization for Scientific Research (NWO), and by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

need to manipulate these qubits very precisely in order to carry out computational operations. A certain level of noise and errors from the environment is therefore unavoidable in any implementation, and in order to be able to compute one would have to use techniques of error correction and fault tolerance.

Unfortunately, the techniques that are used in classical error correction and fault tolerance do not work directly in the quantum case. Moreover, extending these techniques to the quantum world seems at first sight to be nearly impossible due to the continuum of possible quantum states and error patterns. Indeed, when the first important quantum algorithms were discovered [6, 27, 26, 13], many dismissed the whole model of quantum computing as a pipe dream, because it was expected that decoherence would quickly destroy the necessary quantum properties of superposition and entanglement.

It thus came as a great surprise when, in the mid-1990s, *quantum error correcting codes* were developed by Shor and Steane [24, 25, 28], and these ideas later led to the development of schemes for *fault-tolerant quantum computing* [18, 15, 1, 14, 12]. Such schemes take any quantum algorithm designed for an ideal noiseless quantum computer, and turn it into an implementation that is robust against noise, as long as the amount of noise is below a certain threshold, known as the *fault-tolerance threshold*. The overhead introduced by the fault-tolerant schemes is typically quite modest (a polylogarithmic factor in the total running time of the algorithm).

The existence of fault-tolerant schemes turns the problem of building a quantum computer into a hard but possible-in-principle engineering problem: if we just manage to store our qubits and operate upon them with a level of noise below the fault-tolerance threshold, then we can perform arbitrarily long quantum computations. The actual *value* of the fault-tolerance threshold is far from determined, but will have a crucial influence on the future of the area—the more noise a quantum computer can tolerate in theory, the more likely it is to be realized in practice.[1]

The first fault-tolerant schemes were only able to tolerate noise on the order of 10^{-6}, which is way below the level of accuracy that experimentalists can hope to achieve in the foreseeable future. These initial schemes have been substantially improved in the past decade. In particular, Knill has recently developed various schemes which, according to numerical calculations, seem to be able to tolerate more than 1% noise [17, 16]. If we insist on provable constructions, the best known threshold is on the order of 0.1% [4, 3, 2, 21].

Constructions of fault-tolerant schemes provide a *lower bound* on the fault-tolerance threshold. A very interesting question, which is the topic of the current paper, is whether one can prove *upper bounds* on the fault-tolerance threshold. Such bounds give an indication on how far away we are from finding optimal fault-tolerant schemes. They can also give hints as to how one should go about constructing improved fault-tolerant schemes. Such upper bounds are statements of the form "any quantum computation performed with noise level higher than p is essentially useless", where "essentially useless" is usually some strong indication that interesting quantum computations are impossible in such a model. For instance, Buhrman et al. [9] quantify this by giving a classical simulation of such noisy quantum computation, and Razborov [19] shows that if the computation is too long, the output of the circuit is essentially independent of its input.

The best known upper bounds on the threshold are 50% by Razborov [19] and 45.3% by Buhrman et al. [9]. (These bounds are incomparable because they work in different models; see the end of this section for more accurate statements.) As one can see, there are still about two

[1] The "fault-tolerance threshold" is actually not a universal constant, but rather depends on the details of the circuit model (allowed set of gates, type of noise, etc.). A more precise discussion will be given later.

orders of magnitude between our best upper and lower bounds on the fault-tolerance threshold. This leaves experimentalists in the dark as to the level of accuracy they should try to achieve in their experiments. In this paper, we somewhat reduce this gap. So far, much more work has been spent on lower bounds than on upper bounds. Our approach will be the less-trodden road from above, hoping to bring new techniques to bear on this problem.

Our model. In order to state our results, we need to describe our circuit model. We consider parallel circuits, composed of n *wires* and T *levels* of gates (see Figure 1). We sometimes use the term *time* to refer to one of the $T+1$ "vertical cuts" between the levels. For convenience, we assume that the number of qubits n does not change during the computation. Each level is described by a partition of the qubits, as well as a gate assigned to each set in the partition. Notice that at each level, all qubits must go through some gate (possibly the identity). Notice also that for each gate the number of input qubits is the same as the number of output qubits.

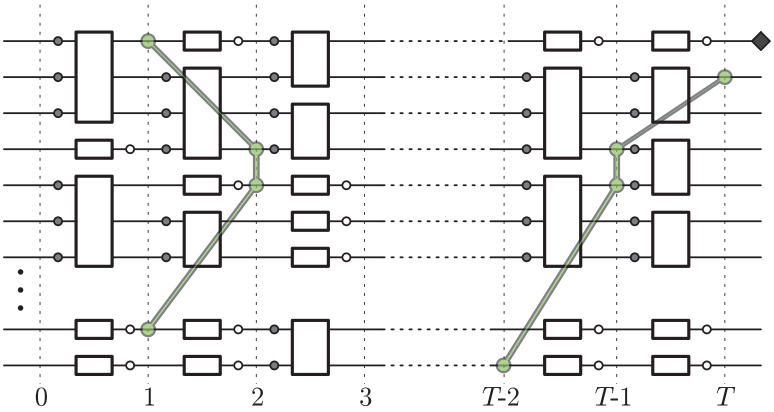

Figure 1: Parallel circuit with $k = 3$ and T levels. Dark circles denote ε_k-depolarizing noise, and light circles denote ε_1-depolarizing noise. Also marked are two consistent sets (defined in Section 3), each containing four qubits. The first has distance 1, the second has distance $T-2$. The output qubit is in the upper right corner.

We assume the circuit is composed of k-qubit gates that are probabilistic mixtures of unitary operations, as well as arbitrary (i.e., all completely-positive trace-preserving) one-qubit gates. In particular, it is possible to do intermediate one-qubit measurements. We assume the output of the circuit is the outcome of a measurement of a designated output qubit in the computational basis. Finally, we assume that the circuit is subject to noise as follows. Recall that p-depolarizing noise on a certain qubit replaces that qubit by the completely mixed state with probability p, and does not alter the qubit otherwise. Formally, this is described by the superoperator $\mathcal{E}$ acting on a qubit ρ as $\mathcal{E}(\rho) = (1-p)\rho + pI/2$. We assume that each one-qubit gate is followed by at least ε_1-depolarizing noise on its output qubit, where $\varepsilon_1 > 0$ is an arbitrarily small constant. Thus one-qubit gates can be essentially noise-free. We also assume that each k-qubit gate is preceded by at least ε_k-depolarizing noise on each of its input qubits, where $\varepsilon_k > 1 - \sqrt{2^{1/k} - 1} = 1 - \Theta(1/\sqrt{k})$.

Our results. In Section 3 we prove our main result:

Theorem 1. *Fix any T-level quantum circuit as above. Then for any two states ρ and τ, the probabilities of obtaining measurement outcome 1 at the output qubit starting from ρ and starting from τ, respectively, differ by at most $2^{-\Omega(T)}$.*

In other words, for any $\eta > 0$, the probability of measuring 1 at the output qubit of a circuit running for $T = O(\log(1/\eta))$ levels is independent of the input (up to $\pm\eta$). This makes the output essentially independent of the starting state, and renders long computations "essentially useless".

Of special interest from an experimental point of view is the case $k = 2$, for which our bound becomes about 35.7%. Furthermore, for the case in which the only allowed two-qubit gate is the controlled-NOT (CNOT) gate, we can improve our bound further to about 29.3%, as we show in Section 4. This case is interesting both theoretically and experimentally. Note also that the CNOT gate together with all one-qubit gates forms a universal set [5]. The same noise-bound applies if we also allow controlled-Y and controlled-Z gates.

Significance of results. Here we comment on the significance of our results and of our model.

First, it is known that fault-tolerant quantum computation is impossible (for any positive noise level) without a source of fresh qubits. Our model takes care of this by allowing arbitrary one-qubit gates—in particular, this includes gates that take any input, and output a fixed one-qubit state, for instance $|0\rangle$. This justifies our assumption that the number of qubits in the circuit remains the same throughout the computation: all qubits can be present from the start, since we can reset them to whatever we want whenever needed.

Second, our assumption that all k-qubit gates are mixtures of unitaries does slightly restrict generality. Not every completely-positive trace-preserving map can be written as a mixture of unitaries.[2] However, we believe that it is still a reasonable assumption. For instance, to the best of our knowledge, all known fault-tolerant constructions can be implemented using such gates (in addition to arbitrary one-qubit gates). Moreover, all known quantum algorithms obtain their speed-up over classical algorithms by using only unitary gates.

Third, we only analyze depolarizing noise acting independently on each qubit. Depolarizing noise is the "most symmetric" type of one-qubit noise and therefore a natural choice for our analysis. Also, it is a relatively weak type of noise: it is not adversarial and does not have correlations between the errors occurring on different qubits. However, since we are proving an *upper bound* on the fault-tolerance threshold, this weakness is actually a good thing, making our result stronger. In principle one can extend our results to various other one-qubit noise models, using an analysis similar to the one developed in Lemma 8. However, not all noise models can actually yield a result like ours. For instance, if we have Toffoli gates with only phaseflip errors, then we can do perfect classical computation. Statements like Theorem 1 are just false in that case.

A slightly more severe restriction is the assumption that the output consists of just one qubit. However, we believe that in many instances this is still a reasonable assumption. For instance, this is the case whenever the circuit is required to solve a decision problem. Moreover, our results can easily be extended to the case where the output is obtained by a measurement on a small number of qubits, instead of only one.

By allowing essentially noise-free one-qubit gates, our model addresses the fact that gates on more than one qubit are generally much harder to implement than one-qubit gates. It should also

[2] One can implement an arbitrary gate by a unitary gate acting on the original qubits and additional ancilla qubits in a fixed pure state, but notice that this increases the arity of the gate and moreover the ancilla qubits will be affected by the noise operators that precede the unitary.

be noted that the exact value of the constant ε_1 is inessential and can be chosen arbitrarily small, as this just affects the constant in the $\Omega(\cdot)$ of Theorem 1. In fact, $\varepsilon_1 > 0$ is only necessary because otherwise it would be possible to let $\rho := |0\rangle\langle 0| \otimes \rho'$ and $\tau := |1\rangle\langle 1| \otimes \tau'$, do nothing for T levels (i.e., apply noise-free one-qubit identity gates on all wires) and then measure the first qubit. The resulting difference between output probabilities is then 1. Instead of assuming an $\varepsilon_1 > 0$ amount of noise, we could alternatively deal with this issue by requiring that every path from the input to the output qubit goes through enough k-qubit gates. Our proof can easily be adapted to this case.

Note that since our theorem applies to arbitrary starting states, it in particular applies to the case that the initial state is encoded in some good quantum error-correcting code, or that it is some sort of "magic state" [7, 20]. In all these cases, our theorem shows that the computation becomes essentially independent of the input after sufficiently many levels.

Finally, it is interesting to note that our bound on the threshold behaves like $1-\Theta(1/\sqrt{k})$. This matches what is known for classical circuits [10, 11], and therefore probably represents the correct asymptotic behavior. Previous bounds only achieved an asymptotic behavior of $1 - \Theta(1/k)$ [19].

Techniques. We believe that a main part of our contribution is introducing a new technique for obtaining upper bounds on the fault-tolerance threshold. Namely, we use a Pauli basis decomposition in order to track the state of the computation. We believe this framework will be useful also for further analysis of quantum fault-tolerance. A finer analysis of the Pauli coefficients might improve the bounds we achieve here, and possibly obtain bounds that are tailored to other computational models.

Related work. The work most closely related to ours is that of Razborov [19]. There, he proves an upper bound of $\varepsilon_k = 1-1/k$ on the fault-tolerance threshold. On one hand, his result is stronger than ours as it allows arbitrary k-qubit gates and not just mixtures of unitaries. Razborov also has a second result, namely the trace distance between the two states obtained by applying the circuit to starting states ρ and τ, respectively, is upper bounded by $n2^{-\Omega(T)}$. Hence even the results of arbitrary n-qubit measurement on the full final state become essentially independent of the initial state after $T = O(\log n)$ levels. On the other hand, the value of our bound is better for all values of k, and we also allow essentially noise-free one-qubit gates. Hence the two results are incomparable. Razborov's proof is based on tracking how the trace distance evolves during the computation. Our proof is similar in flavor, but instead of working with the trace distance, we work with the Frobenius distance (since it can easily be expressed in terms of the Pauli decomposition).

Buhrman et al. [9] show that classical circuits can efficiently simulate any quantum circuit that consists of perfect, noise-free *stabilizer operations* (meaning Clifford gates (Hadamard, phase gate, CNOT), preparations of states in the computational basis, and measurements in the computational basis) and arbitrary one-qubit unitary gates that are followed by 45.3% depolarizing noise. Hence such circuits are not significantly more powerful than classical circuits.[3] This result is incomparable to ours: the noise models and the set of allowed gates are different (and we feel ours is more realistic). In particular, in our case noise hits the qubits going into the k-qubit gates but barely affects the one-qubit gates, while in their case the noise only hits the non-Clifford one-qubit unitaries.

[3] The 45.3%-bound of [9] is in fact *tight* if one additionally allows perfect classical control (i.e., the ability to condition future gates on the earlier classical measurement outcomes): circuits with perfect stabilizer operations and arbitrary one-qubits gates suffering from less than 45.3% noise, can simulate perfect quantum circuits. See [22] and [9, Section 5]. These assumptions are not very realistic, however. In particular the assumption that one can implement perfect, noise-free CNOTs is a far cry from experimental practice.

Another related result is by Virmani et al. [29]. Instead of depolarizing noise, they consider "dephasing noise". This models phase-errors: rather than replacing a qubit by the completely mixed state with some probability p, dephasing noise applies the Z-gate to a qubit with probability $p/2$. Virmani et al. [29] show, among other results, that we can efficiently classically simulate any quantum circuit consisting of perfect stabilizer operations, and one-qubit unitary gates that are diagonal in the computational basis and are followed by more than 29.3% dephasing noise. Their result is incomparable to ours for essentially the same reasons as why the Buhrman et al. result is incomparable: a different noise model and a different statement about the resulting power of their noisy quantum circuits.

Finally, it is known that it is impossible to transmit quantum information through a p-depolarizing channel for $p > 1/3$ [8]. As Razborov [19] noticed, this seems to suggest that quantum computation is impossible with depolarizing noise of strength greater than 1/3, but there is no proof that this is indeed the case.

2 Preliminaries

Let $\mathcal{P} = \{I, X, Y, Z\}$ be the set of one-qubit Pauli matrices,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

and let $\mathcal{P}_* = \{X, Y, Z\}$. We use $\mathcal{P}^n$ to denote the set of all tensor products of n one-qubit Pauli matrices. For a Pauli matrix $S \in \mathcal{P}^n$ we define its *support*, denoted $\mathrm{supp}(S)$, to be the qubits on which S is not identity. We sometimes use superscripts to indicate the qubits on which certain operators act. Thus $I^{\mathcal{A}}$ denotes the identity operator applied to the qubits in set $\mathcal{A}$.

The set of all $2^n \times 2^n$ Hermitian matrices forms a 4^n-dimensional real vector space. On this space we consider the Hilbert-Schmidt inner product, given by $\langle A, B\rangle := \mathrm{Tr}(A^\dagger B) = \mathrm{Tr}(AB)$. Note that for any $S, S' \in \mathcal{P}^n$, $\mathrm{Tr}(SS') = 2^n$ if $S = S'$ and 0 otherwise, and hence $\mathcal{P}^n$ is an orthogonal basis of this space. It follows that we can uniquely express any Hermitian matrix δ in this basis as

$$\delta = \frac{1}{2^n} \sum_{S \in \mathcal{P}^n} \widehat{\delta}(S) S$$

where $\widehat{\delta}(S) := \mathrm{Tr}(\delta S)$ are the (real) coefficients.

We now state some easy observations which will be used in the proof of our main result. First, by the orthogonality of $\mathcal{P}^n$, it follows that for any δ,

$$\mathrm{Tr}(\delta^2) = \frac{1}{2^n} \sum_{S \in \mathcal{P}^n} \widehat{\delta}(S)^2.$$

This easily leads to the following observation.

Observation 2 (Unitary preserves sum of squares)**.** *For any unitary matrix U and any Hermitian matrix δ, if we denote $\delta' = U\delta U^\dagger$, then*

$$\sum_{S \in \mathcal{P}^n} \widehat{\delta'}(S)^2 = 2^n \mathrm{Tr}(\delta'^2) = 2^n \mathrm{Tr}(U\delta U^\dagger U \delta U^\dagger) = 2^n \mathrm{Tr}(\delta^2) = \sum_{S \in \mathcal{P}^n} \widehat{\delta}(S)^2.$$

This also shows that the operation of conjugating by a unitary matrix, when viewed as a linear operation on the vector of Pauli coefficients, is an orthogonal transformation.

Observation 3 (Tracing out qubits)**.** *Let δ be some Hermitian matrix on a set of qubits W. For $V \subseteq W$, let $\delta_V = \mathrm{Tr}_{W \setminus V}(\delta)$. Then,*

$$\widehat{\delta}(SI^{W\setminus V}) = \mathrm{Tr}(\delta \cdot SI^{W\setminus V}) = \mathrm{Tr}(\delta_V \cdot S) = \widehat{\delta_V}(S).$$

Observation 4 (Noise in the Pauli basis)**.** *Applying a p-depolarizing noise $\mathcal{E}$ to the j-th qubit of Hermitian matrix δ changes the coefficients as follows:*

$$\widehat{\mathcal{E}(\delta)}(S) = \left\{ \begin{array}{rl} \widehat{\delta}(S) & \text{if } S_j = I \\ (1-p)\widehat{\delta}(S) & \text{if } S_j \neq I \end{array} \right.$$

In other words, $\mathcal{E}$ "shrinks" by a factor $1-p$ all coefficients that have support on the j-th coordinate.

Observation 5. *Let ρ and τ be two one-qubit states and let $\delta = \rho - \tau$. Consider the two probability distributions obtained by performing a measurement in the computational basis on ρ and τ, respectively. Then the variation distance between these two distributions is $\frac{1}{2}|\widehat{\delta}(Z)|$.*

Proof: Since there are only two possible outcomes for the measurements, the variation distance between the two distributions is exactly the difference in the probabilities of obtaining the outcome 0, which is given by

$$|\mathrm{Tr}((\rho - \tau) \cdot |0\rangle\langle 0|)| = \left| \mathrm{Tr}\left(\delta \cdot \frac{I+Z}{2}\right)\right| = \frac{1}{2}|\mathrm{Tr}(\delta \cdot Z)| = \frac{1}{2}|\widehat{\delta}(Z)|,$$

where we have used $\mathrm{Tr}(\delta) = 0$. ■

Our final observation follows immediately from the convexity of the function x^2.

Observation 6 (Convexity)**.** *Let p_i be any probability distribution, and δ_i a set of Hermitian matrices. Let $\delta = \sum_i p_i \delta_i$. Then*

$$\sum_{S \in \mathcal{P}^n} \widehat{\delta}(S)^2 \leq \sum_i p_i \sum_{S \in \mathcal{P}^n} \widehat{\delta}_i(S)^2.$$

3 Proof of Theorem 1

In this section we prove Theorem 1. The rough idea is the following. Fix two arbitrary initial states ρ and τ. Our goal is to show that after applying the noisy circuit, the state of the output qubit is nearly the same with both starting states. Equivalently, we can define $\delta = \rho - \tau$ and show that after applying the noisy circuit to δ, the "state" of the output qubit is essentially 0 (the noisy circuit is a linear operation, and hence there is no problem in applying it to δ, which is the difference of two density matrices). In order to show this, we will examine how the coefficients of δ in the Pauli basis develop through the circuit. Initially we might have many large coefficients. Our goal is to show that the coefficients of the output qubit are essentially 0. This is established by analyzing the balance between two opposing forces: noise, which shrinks coefficients by a constant factor (as in Observation 4), and gates, which can increase coefficients. As we saw in Observation 2, unitary gates preserve the sum of squares of coefficients. They can, however, "concentrate" several small coefficients into one large coefficient. One-qubit operations need not preserve the sum of squares (a good example is the gate that resets a qubit to the $|0\rangle$ state), but we can still deal with them by using a known characterization of one-qubit gates. This characterization allows us to bound the amount by which one-qubit gates can increase the Pauli coefficients, and very roughly speaking shows that the gate that resets a qubit to $|0\rangle$ is "as bad as it gets".

Before continuing with the proof, we introduce some terminology. From now on we use the term *qubit* to mean a wire at a specific time, so there are $(T+1)n$ qubits (although during the proof we will also consider qubits that are located between a gate and its associated noise). We say that a set of qubits V is *consistent* if we can meaningfully talk about a "state of the qubits of V" (see Figure 1). More formally, we define a consistent set as follows. The set of all qubits at time 0 and all its subsets are consistent. If V is some consistent set of qubits, which contains all input qubits IN of some gate (possibly a one-qubit identity gate), then also $(V \setminus IN) \cup OUT$ and all its subsets are consistent, where OUT denotes the gate's output qubits. Note that here we think of the noise as being part of the gate. For a consistent set V and a state (or more generally, a Hermitian matrix) ρ, we denote the state of V when the circuit is applied with the initial state ρ, by ρ_V. In other words, ρ_V is the state one obtains by applying some initial part of the circuit to ρ, and then tracing out from the resulting state all qubits that are not in V.

If v is a qubit, we use $\mathrm{dist}(v)$ to denote its distance from the input, i.e., the level of the gate just preceding it. The qubits of the starting state have $\mathrm{dist}(v) = 0$. For a nonempty set V of qubits we define $\mathrm{dist}(V) = \min\{\mathrm{dist}(v) \mid v \in V\}$, and extend it to the empty set by $\mathrm{dist}(\emptyset) = \infty$. Note that $\mathrm{dist}(V)$ does not increase if we add qubits to V.

In the rest of this section we prove the following lemma, showing that a certain invariant holds for all consistent sets V.

Lemma 7. *For all $\varepsilon_1 > 0$ and $\varepsilon_k > 1 - \sqrt{2^{1/k} - 1}$ there exists a $\theta < 1$ such that the following holds. Fix any T-level circuit in our model, let ρ and τ be some arbitrary initial states, and let $\delta = \rho - \tau$. Then for every consistent V,*

$$\sum_{S \in \mathcal{P}^V} \widehat{\delta_V}(S)^2 \leq 2 \cdot 2^{|V|} \cdot \theta^{\mathrm{dist}(V)}, \tag{1}$$

or equivalently,

$$\mathrm{Tr}(\delta_V^2) \leq 2 \cdot \theta^{\mathrm{dist}(V)}.$$

In particular, if we consider the consistent set V containing the designated output qubit at time T, then we get that $\widehat{\delta_V}(Z)^2 \leq 4\theta^T$. By Observation 5, this implies Theorem 1.

3.1 Proof of Lemma 7

The proof of the invariant is by induction on the sets V. At the base of the induction are all sets V contained entirely within time 0. All other sets are handled in the induction step. In order to justify the inductive proof, we need to provide an ordering on the consistent sets V such that for each V, the proof for V uses the inductive hypothesis only on sets V' that appear before V in the ordering. As will become apparent from the proof, if we denote by $\mathrm{latest}(V)$ the maximum time at which V contains a qubit, then each V' for which we use the induction hypothesis has strictly less qubits than V at time latest(V). Therefore, we can order the sets V first in increasing order of latest(V) and then in increasing order of the number of qubits at time latest(V).

3.1.1 Base case

Here we consider the case that V is fully contained within time 0. If $V = \emptyset$ then both sides of the invariant are zero, so from now on assume V is nonempty. In this case dist$(V) = 0$. The matrix δ_V is the difference of two density matrices, say $\delta_V = \rho_V - \tau_V$, and hence $\mathrm{Tr}(\delta_V^2) = \mathrm{Tr}(\rho_V^2) + \mathrm{Tr}(\tau_V^2) - 2\mathrm{Tr}(\rho_V \tau_V) \leq 2$, and the invariant is satisfied.

3.1.2 Induction step

Let V'' be any consistent set containing at least one qubit at time greater than zero. Our goal in this section is to prove the invariant for V''. Consider any of the qubits of V'' located at time latest(V'') and let G be the gate that has this qubit as one of its output qubits. We now consider two cases, depending on whether G is a k-qubit gate or a one-qubit gate.

Case 1: ***G* is a *k*-qubit gate.** Here we consider the case that G is a probabilistic mixture of k-qubit unitaries. First note that by Observation 6 it suffices to prove the invariant for k-qubit unitaries. So assume G is a k-qubit unitary acting on the qubits $\mathcal{A} = \{A_1, \ldots, A_k\}$. Let $\mathcal{A}' = \{A'_1, \ldots, A'_k\}$ be the qubits after the ε_k-noise but before the gate G and $\mathcal{A}'' = \{A''_1, \ldots, A''_k\}$ the qubits after G (see Figure 2). By our choice of G, $\mathcal{A}'' \cap V'' \neq \emptyset$. Define $V' = (V'' \setminus \mathcal{A}'') \cup \mathcal{A}'$ and $V = (V'' \setminus \mathcal{A}'') \cup \mathcal{A}$. Note that V and its subsets are consistent sets with strictly fewer qubits than V'' at time latest(V''), and hence we can apply the induction hypothesis to them.

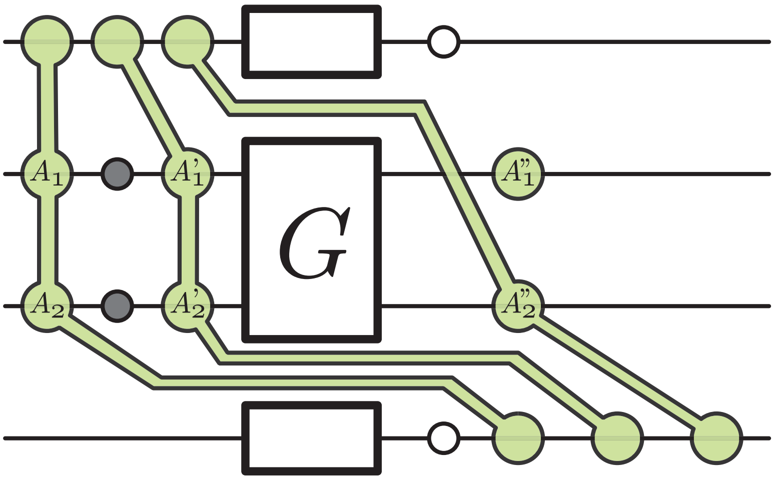

Figure 2: An example showing the sets V, V', and V'' for a two-qubit gate G.

Recall that our goal is to prove the invariant Eq. (1) for V''. To begin, using Observation 3,

$$\sum_{S \in \mathcal{P}^{V''}} \widehat{\delta_{V''}}(S)^2 \leq \sum_{S \in \mathcal{P}^{V'' \cup \mathcal{A}''}} \widehat{\delta_{V'' \cup \mathcal{A}''}}(S)^2. \tag{2}$$

Because G (which maps $\delta_{V'}$ to $\delta_{V''\cup\mathcal{A}''}$) is unitary, it preserves the sum of squares of $\widehat{\delta}$-coefficients (see Observation 2), so the right hand side of (2) is equal to

$$\sum_{S\in\mathcal{P}^{V'}} \widehat{\delta_{V'}}(S)^2 = \sum_{S\in\mathcal{P}^{V'\setminus\mathcal{A}'}} \sum_{R\in\mathcal{P}^{\mathcal{A}'}} \widehat{\delta_{V'}}(RS)^2.$$

Since the only difference between δ_V and $\delta_{V'}$ is noise on the qubits $A_1,\dots,A_k$, using Observation 4 and denoting $\mu = 1-\varepsilon_k$, we get that the above is at most

$$\begin{aligned} &\sum_{S\in\mathcal{P}^{V\setminus\mathcal{A}}} \sum_{R\in\mathcal{P}^{\mathcal{A}}} \mu^{2|\mathrm{supp}(R)|}\widehat{\delta_V}(RS)^2 \\ &= \sum_{S\in\mathcal{P}^{V\setminus\mathcal{A}}} \sum_{a\subseteq\mathcal{A}} \mu^{2|a|}(1-\mu^2)^{k-|a|} \sum_{R\in\mathcal{P}^a\otimes I^{\mathcal{A}\setminus a}} \widehat{\delta_V}(RS)^2, \end{aligned}$$

where the equality follows by noting that for any fixed S and any $R\in\mathcal{P}^{\mathcal{A}}$, the term $\widehat{\delta_V}(RS)^2$, which appears with coefficient $\mu^{2|\mathrm{supp}(R)|}$ on the left hand side, appears with the same coefficient $\sum_{a\supseteq\mathrm{supp}(R)} \mu^{2|a|}(1-\mu^2)^{k-|a|} = \mu^{2|\mathrm{supp}(R)|}$ on the right hand side. By rearranging and using Observation 3 we get that the above is equal to

$$\begin{aligned} &\sum_{a\subseteq\mathcal{A}} \mu^{2|a|}(1-\mu^2)^{k-|a|} \sum_{S\in\mathcal{P}^{(V\setminus\mathcal{A})\cup a}} \widehat{\delta_{(V\setminus\mathcal{A})\cup a}}(S)^2 \\ &\le \sum_{a\subseteq\mathcal{A}} \mu^{2|a|}(1-\mu^2)^{k-|a|} 2\cdot 2^{|(V\setminus\mathcal{A})\cup a|}\cdot\theta^{\mathrm{dist}((V\setminus\mathcal{A})\cup a)} \end{aligned}$$

where we used the inductive hypothesis. Note that $\mathrm{dist}((V\setminus\mathcal{A})\cup a) \ge \mathrm{dist}(V)$, so the above is

$$\begin{aligned} &\le 2\cdot 2^{|V\setminus\mathcal{A}|}\cdot\theta^{\mathrm{dist}(V)} \sum_{a\subseteq\mathcal{A}} 2^{|a|}\mu^{2|a|}(1-\mu^2)^{k-|a|} \\ &= 2\cdot 2^{|V\setminus\mathcal{A}|}\cdot\theta^{\mathrm{dist}(V)}((1-\mu^2)+2\mu^2)^k \\ &= 2\cdot 2^{|V\setminus\mathcal{A}|}\cdot\theta^{\mathrm{dist}(V)}(1+\mu^2)^k. \end{aligned} \tag{3}$$

Note that $|V\setminus\mathcal{A}| \le |V''|-1$ and $\mathrm{dist}(V'')-1 \le \mathrm{dist}(V)$, so the right hand side is bounded by

$$\le 2\cdot 2^{|V''|-1}\cdot\theta^{\mathrm{dist}(V'')-1}(1+\mu^2)^k.$$

Since $\varepsilon_k > 1-\sqrt{2^{1/k}-1}$, we have that $(1+\mu^2)^k \le 2\theta$ if θ is close enough to 1, so we can finally bound the last expression by

$$\le 2\cdot 2^{|V''|}\cdot\theta^{\mathrm{dist}(V'')}$$

which proves the invariant for V''.

Case 2: G is a one-qubit gate. Before proving the invariant, we need to prove the following property of completely-positive trace-preserving (CPTP) maps on one qubit.

Lemma 8. *For any CPTP map G on one qubit there exists a $\beta\in[0,1]$ such that the following holds. For any Hermitian matrix δ, if we let δ' denote the result of applying G to δ, then we have*

$$\widehat{\delta'}(X)^2 + \widehat{\delta'}(Y)^2 + \widehat{\delta'}(Z)^2 \le (1-\beta)\cdot\widehat{\delta}(I)^2 + \beta\cdot(\widehat{\delta}(X)^2 + \widehat{\delta}(Y)^2 + \widehat{\delta}(Z)^2).$$

Proof: The proof is based on the characterization of trace-preserving completely-positive maps on one qubit due to Ruskai, Szarek, and Werner [23, Sections 1.2 and 1.3]. This characterization implies that any one-qubit gate G can be written as a convex combination of gates of the form $U_1 \circ J \circ U_2$. Here U_1 and U_2 are one-qubit unitaries (acting on the density matrix by conjugation), and J is a one-qubit map that in the Pauli basis has the form

$$J = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & 0 \\ t & 0 & 0 & \lambda_1\lambda_2 \end{pmatrix}$$

for some $\lambda_1, \lambda_2 \in [-1, 1]$ and $t = \pm\sqrt{(1-\lambda_1^2)(1-\lambda_2^2)}$.

First observe that by the convexity of the square function, it suffices to prove the lemma for G of the form $U_1 \circ J \circ U_2$ (with the resulting β being the appropriate average of the individual β's). Next note that since U_1 and U_2 are unitary, they act on the vector of coefficients $(\widehat{\delta}(X), \widehat{\delta}(Y), \widehat{\delta}(Z))$ as an orthogonal transformation, and hence leave the sum of squares invariant. This shows that it suffices to prove the lemma for a map J as above. For this map,

$$\widehat{\delta'}(X)^2 + \widehat{\delta'}(Y)^2 + \widehat{\delta'}(Z)^2 = \lambda_1^2\widehat{\delta}(X)^2 + \lambda_2^2\widehat{\delta}(Y)^2 + (t\widehat{\delta}(I) + \lambda_1\lambda_2\widehat{\delta}(Z))^2.$$

Assume without loss of generality that $\lambda_1^2 \geq \lambda_2^2$. Applying Cauchy-Schwarz to the two 2-dimensional vectors $(\pm\sqrt{1-\lambda_1^2}a, \lambda_1 b)$ and $(\sqrt{1-\lambda_2^2}, \lambda_2)$, we get that for any $a, b \in \mathbb{R}$, $(ta + \lambda_1\lambda_2 b)^2 \leq (1-\lambda_1^2)a^2 + \lambda_1^2 b^2$. Hence the above expression is upper bounded by

$$\lambda_1^2\widehat{\delta}(X)^2 + \lambda_1^2\widehat{\delta}(Y)^2 + (1-\lambda_1^2)\widehat{\delta}(I)^2 + \lambda_1^2\widehat{\delta}(Z)^2$$

and we complete the proof by choosing $\beta = \lambda_1^2$. ■

Let A be the qubit G is acting on, and recall that our goal is to prove the invariant for the set V''. Denote by A' the qubit of G after the gate but before the ε_1 noise, and by A'' the qubit after the noise. As before, by our choice of G, we have $A'' \in V''$. Let $\mathcal{A} = \{A\}$, $\mathcal{A}' = \{A'\}$, $\mathcal{A}'' = \{A''\}$. Define $V' = (V'' \setminus \mathcal{A}'') \cup \mathcal{A}'$ and $V = (V'' \setminus \mathcal{A}'') \cup \mathcal{A}$ and notice that $|V| = |V'| = |V''|$. By using Lemma 8, we obtain a $\beta \in [0, 1]$ such that

$$\begin{aligned} \sum_{S \in \mathcal{P}^{V''}} \widehat{\delta_{V''}}(S)^2 &\leq \sum_{S \in \mathcal{P}^{V' \setminus \mathcal{A}'}} \left(\widehat{\delta_{V'}}(IS)^2 + (1-\varepsilon_1)^2 \sum_{R \in \mathcal{P}_*^{\mathcal{A}'}} \widehat{\delta_{V'}}(RS)^2 \right) \\ &\leq \sum_{S \in \mathcal{P}^{V \setminus \mathcal{A}}} \left((1 + (1-\varepsilon_1)^2(1-2\beta))\widehat{\delta_V}(IS)^2 + (1-\varepsilon_1)^2\beta \sum_{R \in \mathcal{P}^{\mathcal{A}}} \widehat{\delta_V}(RS)^2 \right). \end{aligned}$$

By applying the induction hypothesis to both $V \setminus \mathcal{A}$ and V, we can upper bound the above by

$$\begin{aligned} &(1 + (1-\varepsilon_1)^2(1-2\beta)) \cdot 2 \cdot 2^{|V|-1} \cdot \theta^{\mathrm{dist}(V \setminus \mathcal{A})} + (1-\varepsilon_1)^2\beta \cdot 2 \cdot 2^{|V|} \cdot \theta^{\mathrm{dist}(V)} \\ &\leq \frac{1 + (1-\varepsilon_1)^2}{2\theta} \cdot 2 \cdot 2^{|V''|} \cdot \theta^{\mathrm{dist}(V'')} \end{aligned}$$

where we used that $|V| = |V''|$, and $\mathrm{dist}(V'') - 1 \leq \mathrm{dist}(V) \leq \mathrm{dist}(V \setminus \mathcal{A})$. Hence the invariant remains valid if we choose $\theta < 1$ such that $1 + (1-\varepsilon_1)^2 \leq 2\theta$.

4 Arbitrary one-qubit gates and CNOT gates

In this section we consider the case where CNOT is the only allowed gate acting on more than one qubit. We still allow arbitrary one-qubit gates. The proof follows along the lines of that of Theorem 1 with one small modification. As before, we will prove that for all $\varepsilon_1 > 0$ and $\varepsilon_2 > 1 - 1/\sqrt{2} \approx 0.293$ the invariant, Eq. (1), holds. The proof for the case that G is a one-qubit gate holds without change. We will give the modified proof for the case that G is a CNOT gate. The idea for the improved bound is to make use of the fact that the CNOT gate merely permutes the 16 elements of $\mathcal{P} \otimes \mathcal{P}$, and does not map elements from $I \otimes \mathcal{P}_*$ to $\mathcal{P}_* \otimes I$ or vice versa (as illustrated in Figure 3). As a result we need to apply the induction hypothesis on one less term, which in turn improves the bound.

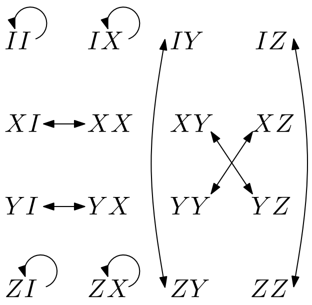

Figure 3: The action of CNOT on $\mathcal{P} \otimes \mathcal{P}$ under conjugation with the control wire corresponding to the first qubit.

Assume the CNOT acts on qubits $\mathcal{A} = \{A, B\}$, with $\mathcal{A}' = \{A', B'\}$ and $\mathcal{A}'' = \{A'', B''\}$ as before, where again $\mathcal{A}'' \cap V'' \neq \emptyset$. If both A'' and B'' are contained in V'' then the proof of the general case (cf. Eq. (3)) already gives a bound of

$$2 \cdot 2^{|V \setminus \mathcal{A}|} \cdot \theta^{\mathrm{dist}(V)} (1+\mu^2)^2 \leq 2 \cdot 2^{|V''|-2} \cdot \theta^{\mathrm{dist}(V'')-1} (1+\mu^2)^2 \leq 2 \cdot 2^{|V''|} \cdot \theta^{\mathrm{dist}(V'')}$$

where the last inequality holds for all $\mu < 1$. Hence it suffices to consider the case that exactly one of A'' and B'' is in V''. Assume without loss of generality that $A'' \in V''$ and $B'' \notin V''$. As before, our goal is to upper bound

$$\sum_{S \in \mathcal{P}^{V''}} \widehat{\delta_{V''}}(S)^2 = \sum_{S \in \mathcal{P}^{V''}} \widehat{\delta_{V'' \cup B''}}(S I^{B''})^2,$$

where the equality follows from Observation (3). Because of the property of CNOT mentioned above, we can now upper bound this by

$$\sum_{S \in \mathcal{P}^{V' \setminus \mathcal{A}'}} \Big(\widehat{\delta_{V'}}(I^{A'} I^{B'} S)^2 + \sum_{R \in \mathcal{P}_*^{A'}} \widehat{\delta_{V'}}(R I^{B'} S)^2 + \sum_{R \in \mathcal{P}_*^{A'} \otimes \mathcal{P}_*^{B'}} \widehat{\delta_{V'}}(RS)^2 \Big).$$

This is the crucial change compared to the case of general two-qubit gates (the latter case also includes a term of the form $\sum_{R \in \mathcal{P}_*^{B'}} \widehat{\delta_{V'}}(I^{A'} R S)^2$). The rest of the proof is similar to the earlier proof. Using the induction hypothesis we can upper bound the above by

$$\begin{aligned}
&\sum_{S\in\mathcal{P}^{V\setminus\mathcal{A}}} \Big(\widehat{\delta_V}(I^AI^BS)^2 + \mu^2 \sum_{R\in\mathcal{P}_*^A} \widehat{\delta_V}(RI^BS)^2 + \mu^4 \sum_{R\in\mathcal{P}_*^A\otimes\mathcal{P}_*^B} \widehat{\delta_V}(RS)^2\Big) \\
\le\ & (1-\mu^2) \sum_{S\in\mathcal{P}^{V\setminus\mathcal{A}}} \widehat{\delta_{V\setminus\mathcal{A}}}(S)^2 + (\mu^2-\mu^4) \sum_{S\in\mathcal{P}^{V\setminus\{B\}}} \widehat{\delta_{V\setminus\{B\}}}(S)^2 + \mu^4 \sum_{S\in\mathcal{P}^V} \widehat{\delta_V}(S)^2) \\
\le\ & (1-\mu^2)2\cdot 2^{|V\setminus\mathcal{A}|}\cdot\theta^{\mathrm{dist}(V\setminus\mathcal{A})} + (\mu^2-\mu^4)2\cdot 2^{|V\setminus\{B\}|}\cdot\theta^{\mathrm{dist}(V\setminus\{B\})} + \mu^4\ 2\cdot 2^{|V|}\cdot\theta^{\mathrm{dist}(V)} \\
\le\ & 2\cdot 2^{|V''|}\cdot\theta^{\mathrm{dist}(V)}\Big(\frac{1+\mu^2}{2}+\mu^4\Big) \\
\le\ & 2\cdot 2^{|V''|}\cdot\theta^{\mathrm{dist}(V'')}\Big(\frac{1+\mu^2}{2}+\mu^4\Big)\frac{1}{\theta}.
\end{aligned}$$

Hence the invariant remains valid as long as $\frac{1+\mu^2}{2}+\mu^4 \le \theta < 1$. This can be satisfied as long as $\mu < 1/\sqrt{2}$, equivalently $\varepsilon_2 > 1-1/\sqrt{2} \approx 0.293$.

5 Future work

As we already pointed out in the "Significance of results" part of the introduction, our models of noise and computation are not yet fully satisfactory. We feel our results can and should be strengthened in a number of directions:

- We should make it work for all possible k-qubit gates (CPTP maps), rather than just mixtures of unitaries.
- We should allow some classical side-processing, where classical outcomes of intermediate measurements can be stored noise-free for a while, and later fed back into the circuit. Allowing such "classical control" requires a type of theorem different from the one we have now: if initial states ρ and τ were bits 0 and 1, respectively, we could just measure this right at the start, store the bit noise-free, and feed it back into the circuit only at the last step, yielding distinguishable final states.
- We should relax the assumption that the final output is determined by a measurement on one or a few qubits of the final state. Often in fault-tolerant schemes one encodes each "logical qubit" in a large block of physical qubits, and needs to measure all qubits in that block to obtain the final outcome of the computation.
- Last but not least, our upper bounds on the fault-tolerance threshold are still much higher than one would expect, and we would like to decrease them much further.

Acknowledgment

We thank Mary Beth Ruskai for a pointer to [23] and for sharing her insights on the characterization of one-qubit operations; Peter Shor for a discussion on entanglement breaking channels which is related to the discussion of [8] at the end of Section 1; and an anonymous ICALP referee for helpful comments.

References

[1] D. Aharonov and M. Ben-Or. Fault tolerant quantum computation with constant error. In *Proceedings of 29th ACM STOC*, pages 176–188, 1997.

[2] P. Aliferis. *Level Reduction and the Quantum Threshold Theorem.* PhD thesis, Caltech, 2007. quant-ph/0703264.

[3] P. Aliferis. Threshold lower bounds for Knill's Fibonacci scheme. quant-ph/0709.3603, 22 Sep 2007.

[4] P. Aliferis, D. Gottesman, and J. Preskill. Accuracy threshold for postselected quantum computation. *Quantum Information and Computation*, 8(3):181–244, 2008.

[5] A. Barenco, C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 52:3457–3467, 1995.

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997. Earlier version in STOC'93.

[7] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Physical Review A*, 71(022316), 2005.

[8] D. Bruss, D. DiVincenzo, A. Ekert, C. Fuchs, C. Macchiavello, and J. Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 43:2368–2378, 1998.

[9] H. Buhrman, R. Cleve, M. Laurent, N. Linden, A. Schrijver, and F. Unger. New limits on fault-tolerant quantum computation. In *Proc. 47th IEEE FOCS*, pages 411–419, 2006.

[10] W. S. Evans and L. J. Schulman. Signal propagation and noisy circuits. *IEEE Trans. Inform. Theory*, 45(7):2367–2373, 1999.

[11] W. S. Evans and L. J. Schulman. On the maximum tolerable noise of k-input gates for reliable computation by formulas. *IEEE Trans. Inform. Theory*, 49(11):3094–3098, 2003.

[12] D. Gottesman. *Stabilizer Codes and Quantum Error Correction.* PhD thesis, Caltech, 1997. quant-ph/9702052.

[13] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of 28th ACM STOC*, pages 212–219, 1996.

[14] A. Yu. Kitaev. Quantum computations: Algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[15] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349):342–345, 1998.

[16] M. Knill. Fault-tolerant postselected quantum computation: Threshold analysis. quant-ph/0404104, 19 Apr 2004.

[17] M. Knill. Quantum computing with realistically noisy devices. *Nature*, 434:39–44, 2005.

[18] M. Knill, R. Laflamme, and W. Zurek. Accuracy threshold for quantum computation. quant-ph/9610011, 15 Oct 1996.

[19] A. Razborov. An upper bound on the threshold quantum decoherence rate. *Quantum Information and Computation*, 4(3):222–228, 2004.

[20] B. Reichardt. Quantum universality from Magic States Distillation applied to CSS codes. *Quantum Information Processing*, 4:251–264, 2005.

[21] B. Reichardt. *Error-Detection-Based Quantum Fault Tolerance Against Discrete Pauli Noise.* PhD thesis, UC Berkeley, 2006. quant-ph/0612004.

[22] B. Reichardt. Quantum universality by distilling certain one- and two-qubit states with stabilizer operations. quant-ph/0608085, 2006.

[23] M. B. Ruskai, S. Szarek, and E. Werner. An analysis of completely-positive trace-preserving maps on $\mathcal{M}_2$. *Linear Algebra and its Applications*, 347:159–187, 2002.

[24] P. W. Shor. Scheme for reducing decoherence in quantum memory. *Physical Review A*, 52:2493, 1995.

[25] P. W. Shor. Fault-tolerant quantum computation. In *Proc. 37th IEEE FOCS*, pages 56–65, 1996.

[26] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. Earlier version in FOCS'94.

[27] D. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. Earlier version in FOCS'94.

[28] A. Steane. Multiple particle interference and quantum error correction. In *Proceedings of the Royal Society of London*, volume A452, pages 2551–2577, 1996.

[29] S. Virmani, S. Huelga, and M. Plenio. Classical simulability, entanglement breaking, and quantum computation thresholds. *Physical Review A*, 71(042328), 2005.