Quantum error correction for various forms of noise

J. Gea-Banacloche and James P. Clemens

Department of Physics, University of Arkansas, Fayetteville, US;

ABSTRACT

Quantum error correction will be an indispensable ingredient of large-scale quantum computations. Conventional quantum error correction codes (QECC) have been devised with an independent-error model in mind, but one may expect that the noise affecting a system of qubits will, in general, exhibit nonzero correlations in time, or space, or both. This talk will present a brief introduction to the principles of quantum error correction, followed by a discussion of the performance of conventional QECCs in the presence of correlated noise.

Keywords: Quantum error correction, correlated noise, quantum computation

1. INTRODUCTION

1.1. Quantum error correcting codes

The possibility to do error correction in a quantum computer, first pointed out by Shor[1] and Steane,[2] was the crucial theoretical development that made it possible, for the first time, to envision large-scale quantum computations, extending beyond the natural decoherence times of the computer's quantum bits (or "qubits"). It was not immediately obvious that quantum error correction would be possible at all. Unlike in classical computers, where the possible states of a physical bit form a (small) discrete set, the states of a qubit span a continuously infinite range. Worse, direct observation of the state of a qubit, or set of qubits, at any time, in order to diagnose and correct any errors that might have occurred, would immediately collapse all coherent superpositions, and in effect terminate the quantum computation.

Nonetheless, an extremely ingenious and elegant formalism for quantum error correction was developed in short order by the pioneering authors and a handful of others, and today the principles are clearly understood, and have even been demonstrated experimentally in a limited way. Several good reviews[3,4] of the subject exist; here we shall present only enough of the background to make this presentation as self-contained as possible.

The first important realization was that the most general kind of noise affecting a single qubit could be viewed as a superposition of just a few basic errors, represented by the three Pauli matrices σ_x, σ_y and σ_z. In the "computational basis" of the two states $|0\rangle, |1\rangle\}$, these matrices have the form

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

Since these three matrices, together with the identity, form a basis of the space of all 2×2 matrices, it follows that any linear operator acting on the qubit could be resolved into a superposition of them. A special kind of indirect measurement (the second crucial ingredient) would then project the system into one particular error space, where the appropriate error would be diagnosed so that the error-free state could be restored.

When acting on a single qubit, whose most general state is of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2}$$

the operator σ_x ("bit flip") produces $\alpha|1\rangle + \beta|0\rangle$, whereas the operator σ_z ("phase flip") produces $\alpha|0\rangle - \beta|1\rangle$, and σ_y yields the equivalent of a joint bit and phase flip. Clearly, all these operations cannot in general be distinguished perfectly from just looking at the one affected qubit, since, in general, the resulting states are not orthogonal, and it is well known that only orthogonal quantum states can be distinguished unambiguously.

E-mail addresses: jgeabana@uark.edu; jpcleme@uark.edu

Fluctuations and Noise in Photonics and Quantum Optics II, edited by Peter Heszler, Derek Abbott, Julio R. Gea-Banacloche, Philip R. Hemmer, Proceedings of SPIE Vol. 5468 (SPIE, Bellingham, WA, 2004) 0277-786X/04/$15 · doi: 10.1117/12.547112

However, one may use redundancy here in much the same way as with a classical error correcting code: by using a certain number of physical qubits (say, N_c) to encode a single logical qubit, one may be able to determine which error occurred by looking at the whole set.

The minimum number of auxiliary qubits required can be determined as follows. Suppose that we use a particular state of N_c qubits as the "logical 0," $|0\rangle_L$, and an orthogonal state as the "logical 1," $|1\rangle_L$. Together they span a two-dimensional subspace; the most general one-logical-qubit state is now $|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$. To make sure that any single one-qubit error can be diagnosed and corrected, we want to arrange things so that every one of the $3N_c$ error operators σ_{ix}, σ_{iy}, σ_{iz} (with $1 \leq i \leq N_c$) sends the state $|\psi\rangle$ into a different orthogonal two-dimensional subspace (the orthogonality is necessary, as pointed out above, to make sure that all possible errors can be distinguished; the size of each subspace must be two to ensure that the information contained in an arbitrary superposition such as $|\psi\rangle$ can be fully recovered). Including the original subspace of $|\psi\rangle$, this means we need at least a $6N_c + 2$-dimensional Hilbert space. Since the Hilbert space of N_c qubits has dimension 2^{N_c}, we require

$$2^{N_c} \geq 6N_c + 2 \tag{3}$$

It is easy to see that the first number N_c that satisfies this equation—with the equal sign, in fact—is $N_c = 5$, so this is the minimum number of physical qubits needed to encode a logical qubit in such a way that any single-qubit error can be corrected. Of course, this reasoning does not prove that the necessary error-correcting code can, in fact, be constructed, but this was done explicitly by Laflamme, Miquel, Paz and Zurek,[?] and independently Bennett, DiVincenzo, Smolin and Wooters,[6] in 1996. This so-called five-qubit code has a number of interesting properties, but it might not be the easiest to work with in an actual quantum computer, since applying logical operations to the five-qubit blocks is somewhat awkward. Much more popular (if less efficient) is a 7-qubit code introduced also in 1996 by Steane,[2] whose 128-dimensional space is large enough to allow for the correction of all 21 single-qubit errors given by σ_{ix}, σ_{iy}, σ_{iz}, as well as all the 42 two-qubit errors of the form $\sigma_{ix}\sigma_{jz}$, with $i \neq j$. (The latter result is pretty much a "freebie," and not likely to prove terribly important in practice.)

If one does not want to correct the most general type of error possible, one may work with smaller codes. This may be appropriate when one knows that the environment is most likely to introduce only one particular kind of noise—for example, bit flips, or phase flips only. To correct only errors caused by the operators σ_{ix}, say, one would need $2^{N_c} > 2N_c + 2$, and the smallest N_c that satisfies this inequality, again optimally, is $N_c = 3$.

We can exhibit this 3-qubit code (which will be used in much of what follows) explicitly here. Its logical 0 and 1 states are formed by the simple repetition of physical 0's and 1's:

$$\begin{aligned} |0\rangle_L &= |000\rangle \\ |1\rangle_L &= |111\rangle \\ |\psi\rangle &= \alpha|000\rangle + \beta|111\rangle \end{aligned} \tag{4}$$

To read out the "error syndrome" caused by the action of any σ_{ix}, $1 \leq i \leq 3$, on $|\psi\rangle$, one can perform a number of operations directly on the three qubits, or introduce *ancillary qubits*, which is by far the preferred method, as it entails the smallest risk of contaminating the data, if the error decoding operations are themselves subject to errors.

A "fault-tolerant" readout scheme using three ancillary qubits, labeled a, b and c, would proceed as follows. First, prepare the ancillas in a superposition state of the two "codewords" $|0\rangle_L$ and $|1\rangle_L$: $|\Phi\rangle_{abc} = \frac{1}{\sqrt{2}}(|110\rangle_{abc} + |001\rangle_{abc})$. Then apply a "transverse CNOT" operation from the data qubits $1, 2, 3$ onto the ancilla qubits a, b, c (which really means three simple CNOT operations, one with qubit 1 as the control and qubit a as the target, another one with qubit 2 as the control and qubit b as the target, and another one with qubit 3 as the control and qubit c as the target). It is easy to see that, if the initial state is $|\psi\rangle \otimes |\Phi\rangle_{abc}$ (for arbitrary $|\psi\rangle$), it is left unchanged by such an operation. More importantly, however, if the initial state is $(\sigma_{ix}|\psi\rangle) \otimes |\Phi\rangle_{abc}$, the result of the transverse CNOT is

$$(\sigma_{ix}|\psi\rangle) \otimes |\Phi\rangle_{abc} \to (\sigma_{ix}|\psi\rangle) \otimes (\sigma_{ix}|\Phi\rangle_{abc})\,. \tag{5}$$

What is most interesting about this result is that the ancilla qubits and data qubits are still disentangled, so the state of the former can be read without disturbing the latter, and the action of the error operator that affected the data has been imprinted on the ancillae, so it can be easily determined, and corrective action taken. This basic idea will work with any code that has the property that the logical 1 state is the "complementary" (i.e., has all its bits flipped) of the logical zero.

If more than one qubit is affected, this simple code will not work, as can be easily seen. Suppose that bits 1 and 2 are flipped. The state of the ancilla qubits will become $\sigma_{1x}\sigma_{2x}|\Phi\rangle_{abc} = \frac{1}{\sqrt{2}}(|110\rangle_{abc} + |001\rangle_{abc})$. But this is the same as $\sigma_{3x}|\Phi\rangle_{abc}$, so when it is read out, the error affecting the data qubits will be misdiagnosed, and the wrong corrective action will be taken: in this case, the operator σ_{3x} will be applied to the data block. As a result, the original error plus the botched error "correction" results in an overall flip of the logical qubit, $|0\rangle_L \to |1\rangle_L, |1\rangle_L \to |0\rangle_L$.

Since, by using three physical qubits instead of one, we increase the chances of multiple errors, it is legitimate to ask whether this encoding can really do any good. If the errors affect the qubits independently, and with small probability p, the probability for a single qubit to experience a flip is p, whereas the probability for the whole block to be flipped is $\sim 3p^2$ (since the probability of two qubits experiencing an accidental flip is given by the product of the two probabilities, $p \cdot p = p^2$, for independent events, and there are 3 ways to choose a pair of qubits out of three). Thus, this simple error-correcting code will reduce the overall failure probability of a logical qubit provided that

$$3p^2 < p \tag{6}$$

or $p < 1/3$. Note that this simple estimate does not include the probability that the error-correcting operations may themselves introduce errors. When this is taken into consideration, a more stringent condition will be derived, but in any case the code may be expected to help provided that p is small enough.

1.2. Dealing with multiple-qubit errors

Although the simple codes introduced above will, in general, reduce the overall failure probability of a data block provided p is small enough, they will still fail, as we have seen, if more than one qubit in the same block fails. There are a number of strategies to deal with multiple-qubit errors, which we shall briefly review here.

In the first place, one can develop codes that can, by themselves, correct multiple errors. For bit flips, a natural choice are repetition codes, generalizing the encoding of (4) in an obvious way. Thus, by encoding the logical zero in $2n+1$ physical qubits as $|0\rangle_L = |00\ldots0\rangle_{12\ldots n}$, and the logical 1 as $|1\rangle_L = |11\ldots1\rangle_{12\ldots n}$, we can diagnose any errors that affect n or fewer qubits, just by observing the state of the $2n+1$ ancilla qubits after a transverse CNOT operation and taking a simple "majority vote." This is a rather efficient encoding; the probability of $n+1$ errors occurring in a block of $2n+1$ qubits will go as

$$P(n+1) \sim \binom{2n+1}{n+1} p^{n+1} = \frac{(2n+1)!}{n!(n+1)!} p^{n+1} \simeq 2p\sqrt{n}\,(4p)^n \tag{7}$$

where the last result makes use of Stirling's formula for large n. This result suggests that the failure probability of the encoded qubit can be made arbitrarily small, simply by increasing n, provided that $p < 1/4$ to begin with.

There are also codes that can correct arbitrary (i.e., not just bit flips, but also phase flips) errors on multiple qubits. A popular such code, introduced by Steane,[7] is the [[23, 1, 7]] Golay code, where we have used a notation such that the first number in the double square brackets is the number of physical qubits used in the encoding (what we called N_c above), the second number is the number of logical qubits encoded in this way, and the third one is the so-called "distance" of the code, where a code of distance d can correct errors affecting as many as $(d-1)/2$ qubits simultaneously. Thus, the Golay code encodes one logical qubit in 23 physical qubits and can correct errors affecting as many as 2 (of the 23) qubits in the data block. The number of physical qubits required may seem enormous when compared to the simple repetition code discussed above, that could correct as many as two bit flips in a block of 5 qubits, but this is the price one has to pay for wanting to correct the action of σ_z (and σ_y) operators, in addition to just σ_x. (Note that, since bit flips are the only errors of relevance to classical computation, the repetition codes could be used whenever a quantum computer is run in "classical mode," if ever the need for such a thing arises.[8])

Finally, a conceptually very simple (although, in general, even more inefficient) way to design codes that can correct multiple errors is to *concatenate* a one-error correcting code. To illustrate this approach with the simple 3-qubit repetition code, for instance, suppose that one makes the zeros and ones in equation (4) not states of individual physical qubits, but 3-qubit encoded "logical" zeros and ones themselves. That is, we would be looking at encoding one logical qubit into a block of nine qubits divided into subblocks of 3:

$$\begin{aligned} |0\rangle_L &= |000\rangle|000\rangle|000\rangle \\ |1\rangle_L &= |111\rangle|111\rangle|111\rangle \end{aligned} \tag{8}$$

Now we would proceed with error correction by, first, looking at the smaller subblocks and dealig with errors there, and then coming back up one level and looking at the subblocks as logical qubits themselves. If two qubits fail inside one subblock, the low-level error correction will, as dicussed in the previous subsection, misdiagnose the problem and return a totally flipped subblock; but when this is looked at next to the other two subblocks one will see (in the ancilla qubits) something like

$$\frac{1}{\sqrt{2}}(|111\rangle|000\rangle|000\rangle + |000\rangle|111\rangle|111\rangle) \tag{9}$$

and will know right away that the first subblock needs to be flipped back to its correct state.

The procedure above will work, provided no more than one subblock fails. That is to say, the first uncorrectable error event would involve two two-qubit errors in two different subblocks. For independent errors such an event would happen with probability $27p^4$, since four qubits need to fail; there are three ways to choose the two subblocks; and there are three ways to choose the qubits that fail inside each subblock. For this to be smaller than the single 3-qubit block failure probability, $3p^2$ (see Eq. (6)), we require

$$27p^4 < 3p^2 \tag{10}$$

which leads to the same condition, $p < 1/3$, as before. Provided this condition holds, concatenation will succesfully reduce the encoded-qubit failure probability.

The beauty of concatenation is that it is immediately obvious how to generalize the idea to an arbitrary degree, to provide protection against as many simultaneous errors as one might deem necessary. By using m layers of encoding, the number of physical qubits needed grows exponentially, as N_c^m, but the overall failure probability decreases in a *superexponential* way, as p^{2^m}. The result is that, provided p is below a certain *threshold value* p_{th} (which will depend on the code adopted, and on assumptions about the noise that may be introduced by the error-recovery operations themselves), successive concatenation can quickly make the overall failure probability of an encoded qubit arbitrarily small.

1.3. Motivation for this study: correlated errors

Finally, we are in a position to motivate the present study. All of the probability estimates in the previous subsections have assumed errors that happened randomly and independently on different qubits; however, in "real life," one can expect error sources (such as, for instance, environmental noise) to be correlated both in space and in time. This will make it more likely, for instance, for a qubit to fail, if the qubit next to it fails.

The question we have wished to address is how these correlations affect the performance of conventional quantum error-correcting codes, both in simple and concatenated form. Our most recent results will be presented at the talk; the following sections summarize the results submitted for publication at the time of this writing.[9]

2. CORRELATED ERRORS AND REPETITION CODES

To begin with, we assume a situation in which the main environmental noise source is expected to introduce bit-flips only, and rely on repetition codes for protection. We assume that the "noise" is described by a Hamiltonian of the form

$$H_{noise} = \sum B_i \sigma_{ix} \tag{11}$$

where the B_i are random classical fields (it could be, for instance, an environmental magnetic field, evaluated at the different positions, $\mathbf{r}_i$, of the qubits). We make the simplest assumption, that the noise obeys Gaussian statistics, so that all the higher order moments are determined by the lowest-order correlation function, which we take to be

$$\langle B_i B_j \rangle = B_0^2 e^{-|\mathbf{r}_i - \mathbf{r}_j|/l_c} \tag{12}$$

where B_0 is a constant that characterizes the noise strength and l_c is its correlation length.

When subject to the Hamiltonian (11), the probability for a single qubit to flip in a short time t is given by

$$p = \left(\frac{B_0 t}{\hbar}\right)^2 \tag{13}$$

On the other hand, for a block of three qubits, encoded as in Eq. (4), we find a failure probability

$$\begin{aligned} p_3 &= \gamma \left(\frac{t}{\hbar}\right)^4 \left(\langle B_1^2 B_2^2\rangle + \langle B_2^2 B_3^2\rangle + \langle B_1^2 B_3^2\rangle\right) \\ &= \gamma p^2 \left(3 + 2e^{-2|\mathbf{r}_1 - \mathbf{r}_2|/l_c} + 2e^{-2|\mathbf{r}_2 - \mathbf{r}_3|/l_c} + 2e^{-2|\mathbf{r}_1 - \mathbf{r}_3|/l_c}\right) \end{aligned} \tag{14}$$

where γ is a state-dependent constant ($\gamma = 1-(\alpha^*\beta+\alpha\beta^*)^2$, in the notation of Eq. (4)). In Eq. (14), use has been made of the assumption of Gaussian statistics and the first-order correlation funtion (12). If we take the "worst-case scenario" value of 1 for γ, and assume the qubits are evenly spaced along a line with a nearest-neighbor distance d, this expression reduces to

$$p_3 = p^2(3 + 4e^{-2d/l_c} + 2e^{-4d/l_c}) \tag{15}$$

to be compared to the result $p_3 = 3p^2$ of the independent error model. Thus, correlations may increase the encoded-qubit failure rate by as much as a factor of 3 (in the limit, $d \ll l_c$, of perfectly correlated noise).

It is natural to ask then what happens for larger repetition codes, such as those considered in section 2.2. If $N_c = 2n + 1$ qubits are used to encode a single qubit, up to n bit-flip errors can be corrected, and one expects the failure probability to scale as p^{n+1} (cf. Eq. (7)). More generaly, let

$$p_{2n+1} = p\,(p f_n(x))^n \tag{16}$$

where $x = e^{-2d/l_c}$ and f_n is some kind of function that takes care of the correlations between qubits, as well as the combinatorics of the error locations. From Eq. (14) we see that $f_1(x) = 3 + 4x + 2x^2$; by Eq. (7), for the independent error model, we expect $f_n(0) \to 1/4$ as $n \to \infty$. In general, for any given value of n and x, we see that $p_{2n+1} < p$ only if $p < 1/f_n(x)$, that is, only if this inequality is satisfied will it make sense to encode in $2n+1$ qubits, for that particular value of x. Otherwise put, the curve $p = 1/f_n(x)$ defines the region (below it) in the p, x plane where a $2n+1$-qubit repetition code is useful. Figure 1 shows these curves $1/f_n$ for $n = 1, 2$ and 3 (blocks of 3, 5, or 7 qubits, respectively). The corresponding functions are $f_2(x) = (10 + 24x + 42x^2 + 44x^3 + 30x^4)^{1/2}$ and $f_3(x) = (35 + 140x + 320x^2 + 536x^3 + 780x^4 + 844x^5 + 700x^6 + 160x^7 + 100x^8 + 40x^9 + 20x^{10})^{1/3}$

Clearly, the larger x, and the larger n, the more stringent the constraints on p become. The limit as $n \to \infty$ can be regarded as a sort of threshold: only if p lies below that curve is it possible to make the failure probability arbitrarily small by going to larger and larger values of n. We have not been able to obtain an exact result for this limit curve, but from numerical analysis with n as large as 8 we have extrapolated the gray thick line shown in Fig. 1.

Note that two things can be said with certainty about this threshold curve. First, by Eq. (7), it must approach 0.25 at $x = 0$. Second, at the opposite limit of perfectly correlated noise ($x \to 1$), it must be zero, since, in that case, if any one qubit flips all of them flip, and the code is useless for any p, no matter how small. In between, our numerical calculations indicate that p_{th} is as low as 0.06 when $d = l_c/5$ (qubits spaced by 1/5 of the coherence length; $x \simeq 0.67$), which is a reduction of about 1/4 over the uncorrelated, $x = 0$ case.

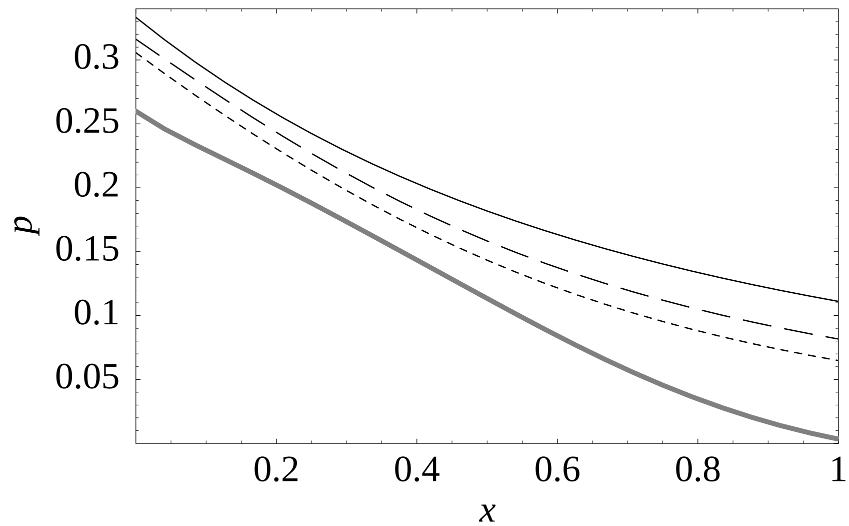

Figure 1. Curves $p = 1/f_n(x)$ for repetition codes of $2n+1$ qubits with $n = 1$ (solid), $n = 2$ (dashed) and $n = 3$ (dotted). Here $x = e^{-2d/l_c}$ is a measure of the strength of the noise correlations over a characteristic interqubit distance. The solid line is an asymptotic extrapolation for $n \to \infty$ based on results (not shown) for $n \geq 5$.

3. CORRELATED ERRORS AND CONCATENATED CODES

We have carried out a similar exploration to the one in the previous Section for more complex codes and error models. In particular, both for Steane's 7-qubit code and for the Golay code, we have considered a noise Hamiltonian

$$H_{noise} = g\hbar \sum \left(E_i e^{i\phi_i} \sigma_{i+} + E_i e^{-i\phi_i} \sigma_{i-} \right) \tag{17}$$

where $\sigma_{i\pm} = \sigma_x \pm i\sigma_y$. This Hamiltonian can cause both bit flips and phase flips, if the phases ϕ_i are nontrivial. We again assume Gaussian statistics for the complex fields $\mathcal{E}_i = E_i e^{i\phi_i}$. That is to say, we assume that any correlation function in which the number of $\mathcal{E}$'s does not match the number of $\mathcal{E}^*$ vanishes, and the first nonvanishing correlation function is given by

$$\langle \mathcal{E}_i^* \mathcal{E}_j \rangle = E_0^2 e^{-|\mathbf{r}_i - \mathbf{r}_j|/l_c} \tag{18}$$

For the 7-qubit code we find that the failure probability $p^{(1)}(x)$ (where the superscript (1) refers to only one level of encoding, in anticipation of the results for concatenated codes to follow) is approximately given by

$$p^{(1)} = p^2(21 + 12x + 10x^2 + 8x^3 + 6x^4 + 4x^5 + 2x^6) \tag{19}$$

in terms of the same variable $x = e^{-2d/l_c}$ as before, and also for qubits evenly spaced along a line. For $x = 1$, this expression gives $p^{(1)} = 63p^2$, which is 3 times the failure probability for uncorrelated errors (coincidentally, this is the same enhancement factor as for the 3-qubit repetition code considered in the previous Section).

For the Golay code the corresponding expression is much longer and will not be given here; it should be noted, however, that in that case the enhancement factor is also much larger: $p^{(1)}(1) = 105p^{(1)}(0)$. This might be expected simply from the much larger size of the code (23 physical qubits), which yields many opportunities for uncorrectable errors (errors affecting 3 qubits or more, whose probability is substantially enhanced by correlated noise). Nonetheless, observe that for the Golay code the failure probability goes as p^3 (where p is the single-qubit failure probability) rather than p^2, so to offset an enhancement factor of 105 one could think of reducing p by a factor $105^{1/3} = 4.7$. Whether this is a difficult goal to achieve in practice would depend, of course, on the physical implementation.

We have also calculated the effect of correlations on the performance of concatenated codes, although here an exact calculation is very difficult and we have had to resort to some approximations. Specifically, we have

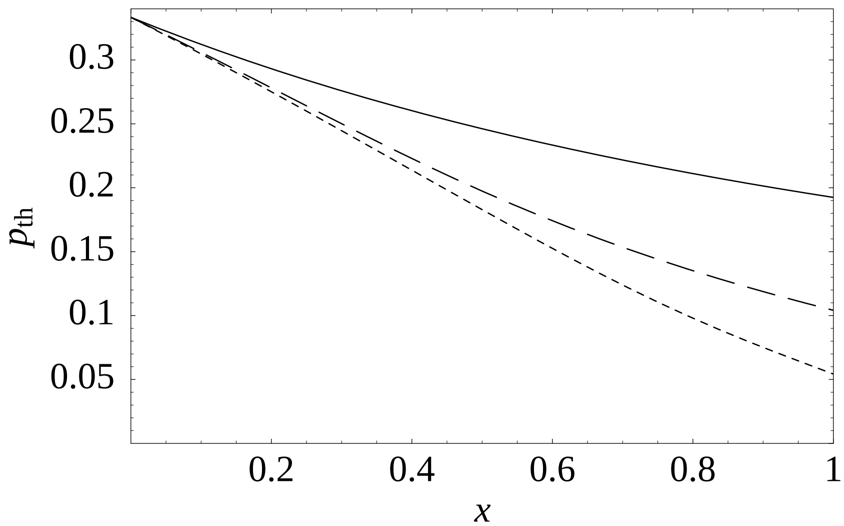

Figure 2. Estimates of the threshold single-qubit failure probability for infinitely-concatenated 3-qubit code. Each successive estimate is obtained assuming that the correlations factorize into blocks of 3^j qubits. Solid curve: $j = 1$. Dashed curve: $j = 2$. Dotted curve: $j = 3$.

calculated the threshold by assuming that the correlations factorize into blocks of N_c^j qubits, with $j = 1, 2, \ldots$ yielding successively better approximations (note that taking $j = 1$ is exact for a single code; $j = 2$ is exact for a code concatenated once, i.e., two levels deep, and so on).

Results for the concatenated three-qubit code (with the noise operator (11), rather than (17)) are shown in Fig. 2, for $j = 1$, 2 and 3. Note that this figure is not directly comparable to Fig. 1 (which shows another approach to correcting multiple bit-flip errors); the curves in Fig. 2 are successive approximations to the threshold probability p_{th} below which concatenation to an *infinite* depth is feasible, but they do not necessarily represent directly the value of p below which concatenation to any particular (finite) depth is advantageous.

Analogous results for the 7-qubit code (with the noise Hamiltonian (17)) for $j = 1$ and 2 are shown in Fig. 3. The same figure also shows the lowest-order estimate of p_{th} for the Golay code (obtained for $j = 1$, which corresponds to neglecting correlations between blocks of 23 qubits.)

4. CONCATENATION WITH A DECOHERENCE-FREE SUBSPACE

One way to deal with correlated errors is to encode quantum information in decoherence-free subspaces (or, more generally, subsystems). These are similar to quantum error-correcting codes (they can, in fact, be regarded as special cases of QECCs), but they are especially designed to exploit any symmetry properties that the noise operators might have (such as, for instance, translational invariance, which would make the noise affect all the qubits in an area in the same way simultaneously). See Ref. 10 for a recent, very comprehensive review of the field.

An example of a DFS that protects a logical qubit against simultaneous flipping of two bits is the encoding

$$\begin{aligned} |0\rangle_L &= \frac{1}{2}(|0\rangle + |1\rangle)(|1\rangle - |0\rangle) \\ |1\rangle_L &= \frac{1}{2}(|0\rangle - |1\rangle)(|1\rangle + |0\rangle) \end{aligned} \tag{20}$$

A simultaneous bit flip of the two qubits simply changes the overall sign of both state vectors, which clearly has no physical consequences. Such encoding would be ideal to work with perfectly correlated noise of the form (11); that is to say, in the limit that the interqubit distance d is much less than the coherence length of the noise, l_c.

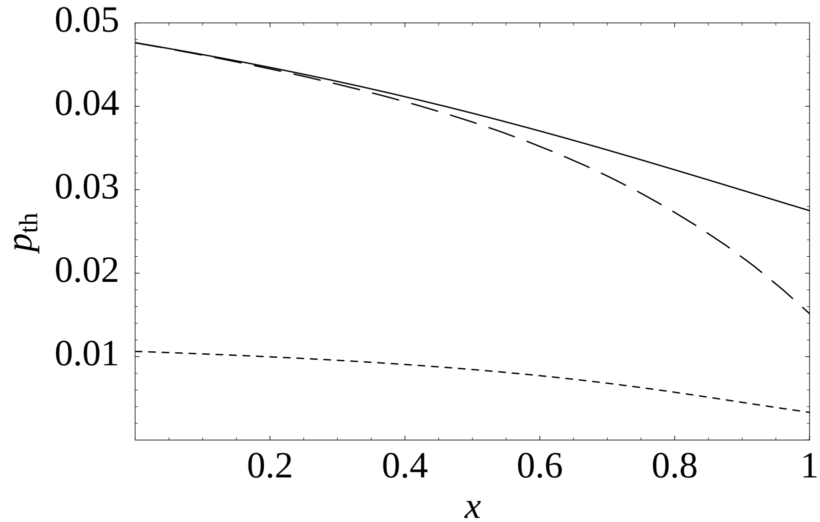

Figure 3. Estimates of the threshold single-qubit failure probability for infinitely-concatenated codes with $N_c = 7$ and $N_c = 23$. Each successive estimate is obtained assuming that the correlations factorize into blocks of N_c^j qubits. Solid curve: 7-qubit code, $j = 1$. Dashed curve: 7-qubit code, $j = 2$. Dotted curve: 23-qubit code, $j = 1$

On the other hand, for a finite l_c, one can think of concatenating the DFS (20) with an appropriate quantum error-correcting code; the DFS would provide protection against noise with large l_c, and the QECC protection against noise with small l_c. For the specific case of (20), notice that if only *one* of the qubit flips, then only one of the basis vectors changes sign; that is to say, a single-physical-qubit, unmatched, bit flip, with the encoding (20), is equivalent to a phase flip of the encoded logical qubit. Protection against partially correlated noise will then be provided by concatenating (20) with a code designed to correct phase flips, which can be obtained easily from (4) by a change of basis. The overall encoding requires six physical qubits and looks like this:

$$\begin{aligned} |0\rangle_{LL} &= \frac{1}{2^{3/2}}\left(|0\rangle_L + |1\rangle_L\right)\left(|0\rangle_L + |1\rangle_L\right)\left(|0\rangle_L + |1\rangle_L\right) \\ |1\rangle_{LL} &= \frac{1}{2^{3/2}}\left(|0\rangle_L - |1\rangle_L\right)\left(|0\rangle_L - |1\rangle_L\right)\left(|0\rangle_L - |1\rangle_L\right) \end{aligned} \tag{21}$$

In terms of the six fields now acting on the qubits, the short-time failure probability now becomes

$$p_{DFS} = \left(\frac{t}{\hbar}\right)^4 \left(\left\langle (B_1 - B_2)^2 (B_3 - B_4)^2 \right\rangle + \left\langle (B_3 - B_4)^2 (B_5 - B_6)^2 \right\rangle + \left\langle (B_1 - B_2)^2 (B_5 - B_6)^2 \right\rangle\right) \tag{22}$$

assuming that the DFS pairs are $(1,2)$,$(3,4)$, $(5,6)$. When this expression is evaluated, one finds again an error probability of the form $p^2 f(x)$, with $x = e^{-2d/l_c}$ as before. The function $f(x)$ is plotted as a dashed line in Figure 4; the solid line shows the function $f_1(x)$ discussed in Section 2 for the simple 3-qubit QECC. The graph shows that for $x > 0.2$ it is advantageous to concatenate the QECC with a DFS, although for smaller x the DFS actually increases the failure probability.

5. CONCLUSIONS

One may conclude from all of the above that, all things considered, conventional QECCs would perform remarkably well even in the presence of correlated noise. For what one might expect to be typical conditions, the performance is impaired by numerical factors which seem to be always smaller than one whole order of magnitude, whether one looks at the increase in failure probability for a fixed concatenation depth or at the decrease in the threshold for successful concatenation. In addition, concatenation with DFSs provides a viable

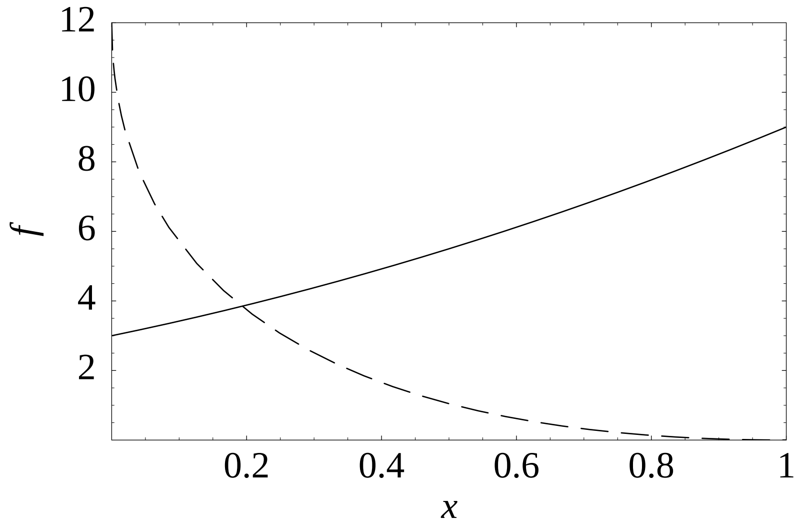

Figure 4. The factor multiplying p^2 in the expression for the failure probability of a logical qubit encoded in a 3-qubit QECC (solid line) and in a 2-qubit DFS concatenated with a 3-qubit QECC (dashed line) as a function of the noise correlation parameter x.

alternative to handle noise with very large correlation lengths, although at the expense of an increase (again, by a factor ~ 4) of the error rate for uncorrelated noise.

Overall, then, our conclusions are not pessimistic, although they should warn against excessive optimism regarding the estimates of the threshold for fault-tolerant quantum computation. These estimates are typically derived assuming an independent (or quasi-independent) error model; our results suggest that, in the presence of correlated noise, one might want to divide those estimates by at least a factor of 2, to be on the safe side. We should point out that recent estimates[11] of the minumum energy necessary for quantum logical operations can be cast into a form that shows an extreme sensitivity to the actual value of the threshold, and hence even a relatively small numerical factor may have important consequences.

Finally, all of these calculations assume perfect error diagnosis and correction, and completely ignore the effects of imperfect gates and ancilla noise. Work to incorporate these effects into more realistic estimates is currently in progress.

ACKNOWLEDGMENTS

This work has been supported by the Army Research Office.

REFERENCES

1. P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, **52**, pp. R2493–R2496, 1995.
2. A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.* **77**, pp. 793–796, 1996.
3. J. Preskill, "Reliable quantum computers," *Proc. R. Soc. London A*, **454** pp. 385–410, 1998.
4. M. A. Nielsen and I. .L. Chuang, *Quantum Computation and Quantum Information*, Chapter 10, Cambridge University Press, Cambridge, 2000.
5. R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek, "Perfect quantum error correction code," *Phys. Rev. Lett.*, **77**, pp. 198–201, 1996.
6. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, **54**, pp. 3824–3851, 1996.

7. A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, **54**, pp. 4741–4751, 1996.
8. J. Gea-Banacloche and L. B. Kish, "Comparison of energy requirements for classical and quantum information processing," *Fluctuations and Noise Letters*, **3**, C3–C7, 2003
9. J. P. Clemens, S. Siddiqui, and J. Gea-Banacloche, "Quantum error correction against correlated noise," submitted to *Phys. Rev. A*, 2004.
10. D. A. Lidar and K. B. Whaley, "Decoherence-Free Subspaces and Subsystems," in *Irreversible Quantum Dynamics*, F. Benatti and R. Floreanini (Eds.), pp. 83-120 (Springer Lecture Notes in Physics vol. 622, Berlin, 2003); also as quant-ph/0301032.
11. J. Gea-Banacloche, "Minimum energy requirements for quantum computation," *Phys. Rev. Lett.* **89**, 217901-1–217901-4, 2002.