Key ideas in quantum error correction

BY ROBERT RAUSSENDORF*

Department of Physics and Astronomy, University of British Columbia, Vancouver, Canada

In this introductory article on the subject of quantum error correction and fault-tolerant quantum computation, we review three important ingredients that enter known constructions for fault-tolerant quantum computation, namely quantum codes, error discretization and transversal quantum gates. Taken together, they provide a ground on which the theory of quantum error correction can be developed and fault-tolerant quantum information protocols can be built.

Keywords: quantum computation; quantum error correction; fault tolerance; quantum codes

1. Introduction

The discovery of an efficient quantum algorithm [1] to break the widespread Rivest–Shamir–Adleman cryptosystem showed that quantum computing has enormous potential for solving hard computational problems. Assuming, of course, that a quantum computer could actually be built. But does not the extra power harnessed in quantum mechanical ways of information processing rely on the assumption that quantum operations could be performed with perfect accuracy? Would not the slightest amount of decoherence ruin any quantum computation if it only takes long enough? ‘No’ says the theory of quantum fault tolerance [2–4]. All that is needed for quantum computation are gate operations of a sufficiently high but fixed quality. If the effect of decoherence per operation is below a certain limit—the error threshold—then arbitrarily long and accurate quantum computation is possible. This is the content of the threshold theorem of fault-tolerant quantum computation [5–7], which is the capstone of the theory of quantum error correction. Put simply, a gate error below the threshold is effectively as good as no error at all.

The purpose of this article was to explain three key ideas upon which the theory of fault-tolerant quantum computation is built. These are quantum codes, error discretization and transversal encoded gates. Woven together, and supplemented by further techniques, they provide the ground on which the celebrated threshold theorem can then be established.

It shall be pointed out from the beginning that the decoherence models discussed in this study are phenomenological and thus overly simplistic. While

*raussen@phas.ubc.ca

One contribution of 11 to a Theme Issue ‘Decoherence’.
they capture essential features of noise in a quantum-mechanical setting, the assumptions that go into them—such as locality and stochastic independence of error events—are not obeyed exactly in any physical system of interest. We hope that this degree of simplification is suited for the purpose of this study, which is to illustrate main ideas and concepts of quantum error correction without too much technicality. In the years since a threshold theorem was first proved, its assumptions have been considerably relaxed. For example, it has been shown that long-range-correlated noise in space or time is not necessarily an obstacle to fault tolerance [8–10].

This study is organized as follows. In §2, we briefly review the circuit model of quantum computation and simple error channels. In §3, a class of quantum codes, the stabilizer codes [4], are developed from classical codes. The phenomenon of error discretization is discussed. Section 4 moves from quantum error correction to fault-tolerant quantum computation. We make some suggestions for further reading in §5 and conclude in §6.

2. Background

(a) The circuit model of quantum computation

The circuit model is not the only, but the ‘standard’ model of quantum computation [11]. Therein, the quantum bit—or qubit for short—is the elementary unit of quantum information. The qubit is a two-level quantum mechanical system, whose general state with respect to a fixed basis $\mathcal{B} = \{ |0\rangle, |1\rangle \}$ is

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (2.1)$$

The qubit exemplifies the unification of information theory with quantum mechanics; namely, it inherits the two distinct basis states $|0\rangle, |1\rangle$ from the classical bit and the superposition principle from quantum mechanics.

A number $n$ of qubits stacked together form a quantum register, the logical structure on which quantum operations are performed in a quantum circuit. The state $|\Psi\rangle$ of the quantum register lives in a tensor product Hilbert space, constructed from the Hilbert spaces of the individual qubits, $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ ($n$ factors). The dimension of this Hilbert space is rapidly growing with the number $n$ of qubits, $\dim(\mathcal{H}) = 2^n$. As a simple counting argument shows, most of the states $|\Psi\rangle \in \mathcal{H}$ are not of product form $|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. Such generic states are called ‘entangled’. Entanglement is a prominent feature that sets apart quantum from classical systems, and is intimately related to the quantum speedup. Specifically, for quantum circuits on pure states, substantial amounts of entanglement must necessarily be present in a quantum computation at some point in the evolution; for otherwise, the quantum computation cannot yield a significant speedup over classical computation [12].

Now, a quantum circuit proceeds in three stages. First, the quantum register is initialized in a fiducial state, e.g. $|\Psi(t=0)\rangle = \bigotimes_{i=1}^{n} |0\rangle_i$. Second, a sequence of unitary operations chosen from a fixed set, the so-called quantum gates, are applied to the quantum register. Third, the qubits of the quantum register are individually measured, wlog in the computational basis $\mathcal{B}_i = \{ |0\rangle_i, |1\rangle_i \}$. To discuss quantum error correction, we need a minor extension of the preceding
description of a quantum circuit. Namely, in the middle part, we do not only allow for unitary gates, but in addition, projective measurements and unitary gates conditioned on the outcomes of those measurements.

For any given physical realization of a quantum computer, the implementation of a single quantum gate is a difficult control problem. With a fixed number of knobs to turn in each physical setup, only a certain family of gates can be realized. It thus makes sense to limit the set of quantum gates that a quantum computer is required to perform. Then, which quantum gates must a quantum computer be able to execute in order to unleash the full power of quantum computation? This question leads to the notion of a universal set of gates. A gate set $G$ is universal, if any unitary evolution on $\mathcal{H}$ can be arbitrarily closely approximated by sequences of gates in $G$. Various universal gate sets have been described in the literature. One such set is

$$G_1 = \{\text{CNOT}_{a,b}, U_i \in SU(2), \text{ for } 1 \leq a \neq b, \ i \leq n\}. \ (2.2)$$

Therein, the controlled NOT (CNOT) gate is a two-qubit gate. It can be defined by its action on a set of basis states,

$$\text{CNOT}_{c,t}|i\rangle_c \otimes |j\rangle_t = |i\rangle_c \otimes |i + j \mod 2\rangle_t. \ (2.3)$$

The action on all states then follows by the linearity of quantum mechanics. In equation (2.3), the qubit $c$ is called the ‘control’ and qubit $i$ the ‘target’. Those names are inherited from the analogous classical XOR gate, where they are justified by the fact the state of the control qubit does not change upon the action by the gate, whereas the state of the target qubit does. Note, however, that for the quantum-mechanical CNOT gate, this is a basis-dependent statement. In the basis $\{|\pm\rangle_c \otimes |\pm\rangle_t\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, the control and target qubits are interchanged.

Furthermore, in equation (2.2), $U_i$ is a one-qubit gate on qubit $i$, namely, a general one-qubit rotation. The strongest and most widespread interactions between physical particles are two body. From the perspective of physics, it thus makes sense to build universal sets out of one-qubit gates (interaction of a qubit with an external control field) and two-qubit gates (qubit–qubit interaction). No set of one-qubit gates can be universal, and the above set $G_1$ thus has minimal requirements for its physical implementation.

It turns out that the above universal set $G_1$ can be shrunk to a smaller one with only a finite number of gates, without losing the property of universality,

$$G_2 = \{\text{CNOT}_{a,b}, H_i, e^{i(\pi/8)Z_i}, \text{ for } 1 \leq a \neq b, \ i \leq n\}. \ (2.4)$$

Therein and in the remainder of this study, we use the shorthand $X_i \equiv \sigma_x^{(i)}$, $Y_i \equiv \sigma_y^{(i)}$ and $Z_i \equiv \sigma_z^{(i)}$. In equation (2.4), $H$ is the so-called Hadamard gate,

$$H = |+\rangle \langle 0| + |-\rangle \langle 1|, \text{ with } |\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \ (2.5)$$

The transition from the universal gate set $G_1$ in equation (2.2) to the finite universal gate set $G_2$ in equation (2.4) is, as we shall see later, an important step for fault-tolerant quantum computation.
Mixed states and error channels

It is convenient for the discussion of decoherence and quantum error correction to represent the state of the quantum register by a density operator \( \rho \) rather than by a state vector \( |\Psi\rangle \). Spurious interactions inevitably entangle the quantum register with the degrees of freedom in the environment that we can neither measure nor control. For the description of the quantum register’s state, it is therefore adequate to trace over the environment. The resulting state of the quantum register is given in terms of a density operator and is generally mixed.

Any evolution of a density operator allowed in quantum mechanics must be linear and preserve Hermiticity, positivity and the trace of all density operators. The corresponding linear (super) operator \( T \) can be cast into the so-called Kraus normal form

\[
T : \rho \rightarrow \sum_{i=1}^{K} A_i \rho A_i^\dagger, \quad \text{with} \quad \sum_{i=1}^{K} A_i^\dagger A_i = I. \quad (2.6)
\]

The above equation contains unitary evolution as a special case. Further examples include the spin-flip channel \( \mathcal{E}_B \), and the partially depolarizing channel \( \mathcal{E}_D \) that we introduce here for later reference. The bit-flip channel

\[
\mathcal{E}_B : \rho \rightarrow (1 - p_B) \rho + p_B X \rho X^\dagger \quad (2.7)
\]

is an essentially classical (bit flip with probability \( p_B \)) channel disguised as a quantum operation. The partially depolarizing channel

\[
\mathcal{E}_D : \rho \rightarrow (1 - p_D) \rho + \frac{p_D}{3} (X \rho X^\dagger + Y \rho Y^\dagger + Z \rho Z^\dagger) \quad (2.8)
\]

better captures what can happen to quantum systems in contact with an environment because it includes both spin-flip errors \( X \) and phase-flip errors \( Z \), as well as their combination \( Y \). The earlier-mentioned two error channels are called ‘probabilistic’ because they describe an environment that roles dice and then conditionally applies Pauli spin and phase to the quantum register.

A limitation of describing individual decoherence processes—one for every time step between two successive error corrections, or one for every gate—by super-operators of form equation (2.6) is that memory effects are excluded from the beginning. Although a more detailed analysis taking memory effects into account \[9,10\] is warranted, we observe that error correction disentangles the quantum computer from its environment, and thereby reduces memory effects over long time scales. We return to this point at the end of §3d.

3. Quantum error correction

(a) A puzzle

To awaken your appetite, let us begin with a puzzle. In this section, we argue that quantum error correction cannot work, based on arguments presented by Landauer \[13\] and Unruh \[14\].

Both theory and daily experience with fax machines, etc., tell us that classical error correction does work. Let us pinpoint the essential assumptions that go into
a classical error-correction procedure, and then check whether a similar procedure can be applied to protect quantum bits.

For concreteness, consider an individual classical bit, stored in the charge state of a capacitor and causing a voltage between the plates. The bit values (0 or 1) correspond to voltage levels of 0 V and 5 V, say. Circuitry connected to the capacitor monitors the voltage level, and, if a deviation from 0 V or 5 V is measured, charges or discharges the capacitor. For example, if the voltage level is found to be 4.7 V, then, with overwhelming likelihood, this represents the encoded state 1, and the capacitor has to be charged until the voltage level is back at 5 V (see figure 1).

Classical error correction, as illustrated in the earlier-mentioned example, proceeds in two steps, namely (i) measurement of the system’s state and (ii) applying a correction operation depending on the measurement outcome. Two conditions must be met for this error correction to be successful, namely, (i) the measurement of the memory device must not destroy the stored information and (ii) the measurement must yield sufficient information for the conditional correction operation to be restored to the correct logical state with high probability.

(i) Argument: why quantum error correction cannot work

Unlike in the classical case, in a quantum mechanical setting, the earlier-mentioned two conditions cannot be met. First, quantum mechanical measurement, in general, changes the measured state. State superpositions are being destroyed and quantum information is thereby lost.

Second, even if a measurement of some kind, e.g. a weak measurement, was tolerable, the amount of information learned would be finite. However, because the valid one-qubit states form a continuous manifold, there are infinitely many possible correction operations. It is impossible to select the correct one based on a finite amount of information. Convinced?

(b) From classical to quantum codes

We will re-examine the earlier-mentioned argument in §3c. Meanwhile, we argue the opposite position, namely, that quantum error correction does work.
The general strategy for protecting quantum information is the same as in the classical case, namely, by introducing redundancy. This leads us to the first of the three ideas discussed in this study: quantum codes.

In order to explain quantum codes, we begin with their classical counterparts. Let us consider a specific example, the classical repetition code with three bits encoding one. The encoded logical states are

$$\bar{0} = 000 \quad \text{and} \quad \bar{1} = 111. \quad (3.1)$$

Errors in such a code can be corrected by majority voting. For example, if an erroneous codeword 010 is found, this either means that bit number 2 was flipped and the encoded state was 000, or that bit numbers 1 and 3 were flipped, and the encoded state was 111. Assuming a local error model with sufficiently low error probability, the occurrence of a single error is way more likely than that of a double error. Therefore, in the present case, the success probability of error correction is maximized if the encoded bit is corrected to 000. This is exactly what majority voting does.

But majority voting is not suitable for generalization to the quantum case because in the process, the encoded state is learned. As noted earlier, in the quantum case, learning the state generally changes it. Quantum information could thereby be lost.

Fortunately, for the repetition code, there is an alternative error-correction procedure, which is exactly as effective as majority voting. Namely, consider an affected codeword \( \tilde{c} = c \oplus e \), where \( c \) is the (unaffected) codeword, \( e \) is the error and \( \oplus \) denotes addition mod 2. Then, there is a parity-check matrix \( P \) and a syndrome vector \( s \) such that

$$s = P\tilde{c}, \quad (3.2)$$

where the parity-check matrix in the present case takes the form \( P = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \), and obeys the condition

$$Pc = 0, \quad \forall \text{ codewords} \ c. \quad (3.3)$$

The parity check yields two bits of syndrome. The correspondence between the four possible syndrome states and eight possible errors is

<table>
<thead>
<tr>
<th>syndrome ( s^T )</th>
<th>compatible errors ( e^T )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(00)</td>
<td>{ (000), (111) }</td>
</tr>
<tr>
<td>(10)</td>
<td>{ (100), (011) }</td>
</tr>
<tr>
<td>(01)</td>
<td>{ (001), (110) }</td>
</tr>
<tr>
<td>(11)</td>
<td>{ (010), (101) }</td>
</tr>
</tbody>
</table>

Assuming a local error model, for either value of the syndrome vector \( s \), there is a clear favourite error to correct. For example, if the syndrome is \( (00)^T \), it is assumed that no error occurred, and no correction is performed. This decision is wrong with a probability \( p^3 \). Likewise, if the error syndrome is \( (01)^T \), the error \( (001)^T \) is corrected for. This choice is wrong with a probability \( (1 - p)p^2 \). Summing all the cases, the error correction fails with a probability of order \( p^2 \). Without encoding and error correction, the error probability is \( p \). Thus, for small values of \( p \), error correction helps us.

Parity-check matrices exist for a very large class of classical codes, not just for repetition codes. The defining property of the parity-check matrix is equation (3.3). By linearity, \( s = Pc \oplus Pe = Pe \). Thus, the error syndrome \( s \) reveals
information only about the error, but not about the encoded bit. This may be a side note for classical error correction, but for quantum error correction it is all important. In fact, it is the starting point for making the transition.

To be specific, let us first consider a quantum counterpart of the repetition code,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \longrightarrow |\bar{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle. \tag{3.4}$$

Therein, one qubit is encoded in three. Now, what is the quantum counterpart to the parity-check matrix? We can easily set up the correspondence between the rows of the parity-check matrix and certain Pauli operators,

$$[110] \leftrightarrow Z_1 \otimes Z_2 \otimes I_3 \quad \{ \text{and} \quad [011] \leftrightarrow I_1 \otimes Z_2 \otimes Z_3 \} \tag{3.5}$$

The Pauli operators to the r.h.s. of the above correspondence have the property that *every* state $|\bar{\psi}\rangle$ in the code space is an eigenstate of them, with eigenvalue +1. That is,

$$Z_1 \otimes Z_2 \otimes I_3 |\bar{\psi}\rangle = |\bar{\psi}\rangle, \quad \forall |\bar{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle \quad \{ \text{and} \quad I_1 \otimes Z_2 \otimes Z_3 |\bar{\psi}\rangle = |\bar{\psi}\rangle, \quad \forall |\bar{\psi}\rangle = \alpha|000\rangle + \beta|111\rangle. \tag{3.6}$$

The operators on the r.h.s. of equation (3.5) are called stabilizer operators because they pointwise stabilize the code space. They are Hermitian, and can thus be measured. Because property (3.6) holds for *all* states in the code space, measuring those operators does *not* collapse the state of the encoded qubit.

Then, what information do we learn from measuring the operators $Z_1Z_2$ and $Z_2Z_3$? Property (3.6) does not hold for all states in the three-qubit Hilbert space in which the code space is embedded. Thus, by measuring the earlier-mentioned operators, we find out whether the encoded state is still in the code space or not. Furthermore, if the state has left the code space, then we learn which operation must be applied to bring it back.

To illustrate this point, consider the example of an $X$ error affecting the encoded state on qubit 1, i.e. $|\psi\rangle = X_1|\bar{\psi}\rangle$. Using the commutation relations among Pauli operators, we find $Z_1Z_2|\psi\rangle = Z_1Z_2X_1|\bar{\psi}\rangle = -X_1Z_1Z_2|\bar{\psi}\rangle = -X_1|\bar{\psi}\rangle = -|\psi\rangle$. Likewise, $Z_2Z_3|\psi\rangle = +|\psi\rangle$. Thus, measuring the operators $Z_1Z_2$, $Z_2Z_3$ on $|\psi\rangle$ yields the eigenvalues $\lambda_{12} = -1$, $\lambda_{23} = +1$. There are two $X$-type errors compatible with this syndrome, namely $X_1$ and $X_2X_3$. The error-correction procedure cannot further discriminate between the two, and the underlying error model must tell which error is the more likely. Applying either $X_1$ or $X_2X_3$ will bring the three-qubit state back to the code space. However, correcting the error that did not occur results in an encoded error $\bar{X} = X_1X_2X_3$, which is subsequently undetectable and uncorrectable.

The stabilizer operators play a central role in our error-correction procedure. Let us identify the key properties required of them. First, they must pairwise commute. For otherwise, the measurement of one stabilizer operator would wipe out the information learned earlier in the measurement of another such operator. Second, quantum mechanical errors must leave a characteristic signature in the measured stabilizer eigenvalues, i.e. the syndrome.

*Phil. Trans. R. Soc. A (2012)*
Within this study, we confine our attention to stabilizer operators in the $n$-qubit Pauli group for arbitrary $n$. For concreteness, the one-qubit Pauli group is $P = \{i,I,X,Z\}$. The $n$-qubit Pauli group is $P_n = P \otimes P \otimes \cdots \otimes P$, with one factor of $P$ for each of the $n$ qubits. The class of admissible quantum codes is thereby constrained, but in exchange we arrive at a very powerful and efficient formalism for discussing these codes, the so-called stabilizer formalism [4]. For a start, we also restrict our error models to probabilistic Pauli channels such as the bit-flip channel equation (2.7) or the partially depolarizing channel equation (2.8). We will show later that the restriction to probabilistic Pauli errors can be lifted.

We now formally define the notions of the stabilizer group and stabilizer codes, which form the basis for our subsequent discussion.

**Definition 3.1 (Stabilizer group and stabilizer code).** A stabilizer group $S$ on $n$ qubits is an abelian subgroup of $P_n$ such that $-I \notin S$. The corresponding quantum code space $\mathcal{H}_{\text{code}}(S) \subset \mathcal{H}$ is

$$\mathcal{H}_{\text{code}}(S) = \{ |\psi\rangle \in \mathcal{H}, \text{ such that } g|\psi\rangle = |\psi\rangle \forall g \in S \}.$$  

Let us check the above-mentioned definition in the case of the repetition code equation (3.4). Here, the stabilizer group is $S = \{Z_1 Z_2, Z_2 Z_3\}$ (cf. equation (3.5)). Then, equation (3.6) is the condition equation (3.7) for the present special case.

Consider a stabilizer group with $s$ generators. Each generator commutes with all the other generators and squares to the identity. Therefore, $S$ has $2^m$ elements. To run an error-correction procedure, we need only to measure the generators rather than all elements of $S$. Because $g_1 |\psi\rangle = \lambda_1 |\psi\rangle, g_2 |\psi\rangle = \lambda_2 |\psi\rangle \implies g_2 g_1 |\psi\rangle = \lambda_2 \lambda_1 |\psi\rangle$, measuring beyond a set of stabilizer generators yields no additional information. Enforcing each stabilizer generator cuts the dimension of the code space in half. Therefore, the number $k$ of qubits encoded with a given stabilizer code with $s$ generators is $k = n - s$.

For each of the encoded qubits, we require encoded Pauli operators $\bar{X}_i$ and $\bar{Z}_i$, for $1 \leq i \leq k$. These operators must obey the usual Pauli operator commutation relations $\bar{X}_i \bar{Z}_i = (-1)^{b_{ij}} \bar{Z}_j \bar{X}_i$, and, when applied, must map the code space back onto itself (without necessarily mapping each state in the code space to itself, of course). Therefore, the encoded Pauli operators must commute with all stabilizer operators,

$$[\bar{X}_i, g] = 0, \quad [\bar{Z}_j, g] = 0, \quad \forall i, j = 1 \ldots k, \quad \forall g \in S.$$  

For the example of the quantum repetition code, $n = 3$ and $s = 2$, such that there is one encoded qubit. We can verify directly in equation (3.4) that $X_1 X_2 X_3$ acts as $\bar{X}$ and that $Z_1$ acts as $\bar{Z}$. Indeed, these operators satisfy the required commutation relations among themselves and with the stabilizer operators (cf. equation (3.8)).

How are Pauli errors identified through the measurement of the stabilizer generators? The previous discussion of the quantum repetition code generalizes to all stabilizer codes. Any Pauli error $E$ can commute or anti-commute only with any given stabilizer operator $g$. If it commutes, the eigenvalue obtained in the measurement of $g$ is $\lambda_g = +1$. If it anti-commutes, then the measured eigenvalue is $\lambda_g = -1$. Combining the measured eigenvalues for a set of stabilizer generators, the error syndrome $\text{Sy}(E)$ is obtained for an error $E$ that has occurred. Each possible Pauli error leaves a characteristic signature in the syndrome. Two errors $E_1$ and $E_2$ can be told apart by the error-correction procedure, if their
syndrome differs, $\text{Sy}(E_1) \neq \text{Sy}(E_2)$. In some cases, it is not necessary that the error-correction procedure can distinguish two errors $E_1$ and $E_2$, namely, when $E_2 = E_1 g$, for some $g \in S$. In that case, $E_1$ and $E_2$ act in the same way on the code space. If $E_1$ occurred, it causes no harm if $E_2 = E_1 g$ is corrected for. To formalize these observations, we make the following definition.

**Definition 3.2 (Set of correctable errors).** A set $A$ of Pauli errors is correctable for a given code with stabilizer $S$, if, for all $E_1, E_2 \in A$, either $\text{Sy}(E_1) \neq \text{Sy}(E_2)$, or $E_2 = E_1 g$ for some $g \in S$.

A quantum code suppresses errors if the set of correctable errors contains all likely errors, with respect to a given error model. The code distance is a quantitative measure for the capability of a code to correct increasingly unlikely errors. For quantum codes, the weight $w$ of an operator is the number of qubits on which it acts non-trivially. For example, the operator $Z_1 Z_2 I_3$ has weight 2. Now, the distance $d$ of a code is the least weight of a Pauli operator that maps the code space onto itself without mapping each state in the code space to itself, i.e. the least weight of an encoded Pauli operator that is not the encoded identity. Consider two non-overlapping Pauli errors $E_1$ and $E_2$ of weight $t$ such that $E_1 E_2 = \tilde{U} \neq \tilde{I}$. Then, $E_1$ and $E_2$ cannot be simultaneously corrected. Thus, the weight $t$ of correctable errors is bounded by $2t \leq d - 1$.

Note that the weight is useful as a measure for the likeliness of a probabilistic error only under the assumptions that errors are local and occur independently. Then, for the probability $p(E)$ of a probabilistic Pauli error $E$, $p(E) \sim p_{\text{local}}^{w(E)}$. Furthermore, the same weights are assigned to $X$, $Y$ and $Z$ errors, which fit with the local depolarizing channel equation (2.8).

We are now in the position to explicitly write down the recovery operation $\mathcal{R}$ that corresponds to a single round of quantum error correction. The physical procedure consists of two steps, namely first the measurement of the error syndrome, and, second, a correction operation conditioned on that syndrome. The total $n$-qubit Hilbert space $\mathcal{H}$ splits into a direct sum of orthogonal subspaces,

$$\mathcal{H} = \bigoplus_{\text{Sy}} \mathcal{H}(\text{Sy}), \quad (3.9)$$

where $\mathcal{H}(\text{Sy})$ is such that, for every state in $\mathcal{H}(\text{Sy})$, we measure the syndrome $\text{Sy}$. Denote by $P_{\text{Sy}}$ the projector onto $\mathcal{H}(\text{Sy})$, and $\mathcal{H}(0) = \mathcal{H}_{\text{code}}$. For every syndrome value $\text{Sy}$, there is a most likely error $E_{\text{max}}(\text{Sy})$ compatible with that syndrome. In accordance with the above, this error is corrected for when the syndrome value $\text{Sy}$ is measured. Thus, the recovery operation is

$$\mathcal{R}(\rho) = \sum_{\text{Sy} \in \mathbb{Z}_2^s} E_{\text{max}}(\text{Sy}) P_{\text{Sy}} \rho P_{\text{Sy}} E_{\text{max}}(\text{Sy})^\dagger$$

$$= \sum_{\text{Sy} \in \mathbb{Z}_2^s} P_{\text{code}} E_{\text{max}}(\text{Sy}) \rho E_{\text{max}}(\text{Sy})^\dagger P_{\text{code}}. \quad (3.10)$$

We note that the recovery operation equation (3.10) is again of Kraus normal form.
Examples. For the quantum repetition code, $\mathcal{A} = \{I, X_1, X_2, X_3\}$ is a set of correctable errors. Thus, for the bit-flip error-channel equation (2.7) applied to all three physical qubits, the repetition code is a good code. The set of errors occurring with probability $p$ or higher form a correctible set, leaving a failure probability of order $p^2$ as we have already observed.

If we change our error model from a spin flipping to a partially depolarizing channel equation (2.8) applied to all three physical qubits, then the quantum repetition code is no longer good. The Pauli operator $Z_1$, as noted earlier, acts as $\bar{Z}$ and thus has trivial error syndrome. $Z_1$ as an error is therefore indistinguishable from the identity operation $I$ (no error), and $I, Z_1$ cannot simultaneously belong to any given set of correctable errors. Both events are likely, however, and the quantum repetition code offers no protection against a local partially depolarizing error. In terms of code distance, the repetition code has distance 1, and hence can correct general Pauli errors up to weight 0 (the identity only).

Because the partially depolarizing error channel changes both amplitudes and phases, it is a way more realistic error model than the effectively classical bit-flip channel, which does not affect the phases. We need a quantum code that can correct both single spin and phase flips. To achieve this, the quantum repetition code needs only a bit of repair, resulting in the nine-qubit Shor code,

$$
|0\rangle = \left( \frac{|000\rangle + |111\rangle}{\sqrt{2}} \right) \otimes^3
$$

and

$$
|1\rangle = \left( \frac{|000\rangle - |111\rangle}{\sqrt{2}} \right) \otimes^3
$$

As can be easily checked, it inherits its protection against bit-flip errors $X_i$ from the quantum repetition code, $Z_1Z_2Z_3, Z_4Z_5, \ldots, Z_8Z_9 \in \mathcal{S}_{Shor}$. Now, how do we detect and correct a local phase-flip error? Consider the example of an error $Z_1$. It affects the phase $\pm$ encoded in the first three qubits $\left( |000\rangle \pm |111\rangle \right)/\sqrt{2}$. The operator which measures that phase is $X_1X_2X_3$. We cannot perform this measurement because it distinguishes between $|0\rangle$ and $|1\rangle$. However, we can compare the phases $\pm$ in the first and second code part, comprising the qubits $(1,2,3)$ and $(4,5,6)$, respectively. For all states in the code space, the product of the two phase factors is $+1$. This property can be measured by the operator $X_1X_2X_3X_4X_5X_6$, which is thus in the stabilizer of the nine-qubit Shor code. Analogously, $X_4X_5X_6X_7X_8X_9 \in \mathcal{S}_{Shor}$. In all, we thus have eight stabilizer generators for nine physical qubits, yielding one encoded qubit in agreement with equation (3.11).

With the earlier-mentioned definition, it is easily verified that

$$
\mathcal{A} = \{I, X_i, Y_i, Z_i, \text{for } i = 1 \ldots 9\}
$$

is a set of correctable errors for the nine-qubit Shor code. Thus, all errors of weight 1 can be corrected. Further, because $X_1X_2X_3 = \bar{Z}$, the code is of distance 3. For a partially depolarizing error channel equation (2.8), the set $\mathcal{A}$ in equation (3.12) is also the set of likely errors, comprising all errors of probability $\sim p$ and higher. The failure probability of the code is thus at most of order $p^2$, which improves upon not encoding.
(c) Concatenated quantum codes

In §3b, we have seen two examples for quantum codes that, given certain error models, suppress but not eliminate the error. The storage time for quantum information is thus prolonged with these codes, but it remains finite. Is it possible to store quantum information arbitrarily long? The answer is affirmative. For a fixed number of encoded qubits, the larger the code, the higher is the degree of error suppression. To guarantee a specific storage time, given a fixed error rate per time step, one needs to use a sufficiently large quantum code.

This statement can be proved by using a special family of codes, the so-called concatenated codes. Consider any stabilizer code that encodes one logical qubit in \( n \) physical qubits, for example, the nine-qubit Shor code from §3b, and apply the following procedure. First, the single logical qubit is encoded in \( n \) physical ones. Next, each of these physical qubits is by itself considered a logical qubit, and is again encoded in \( n \) qubits using the same code as before. Next, each of the now \( n^2 \) physical qubits is considered a logical qubit, and again encoded with the original code. Iterating this procedure, we obtain an infinite family of codes with \( n, n^2, n^3, n^4 \ldots \) qubits.

How are errors suppressed in concatenated codes? Consider such a code with \( L \) levels of concatenation. We begin at the lowest coding level, level 1. It corresponds to the last step of encoding. Assume a local error occurring with probability \( p \). Running error correction on all groups of \( n \) qubits, we remove all errors at the bare level and remain with errors at the coding level 1. The probability \( p_1 \) of this second-level error is reduced, \( p_1 = f(p) = cp^{l+1} + O(p^{l+2}) \), for a quantum code that corrects \( t \) local errors. Next, we perform error correction at the second level of concatenation, leaving errors at the second level. Again, the error probabilities \( p_1 \) and \( p_2 \) are related via \( p_2 = f(p_1) \). Generally, the error probability \( p_l \) at level \( l \) is related to the error probability \( p_{l-1} \) at level \( l-1 \) via \( p_l = f(p_{l-1}) \), such that at level \( L \), \( p_L = f(f(f \ldots f(p) \ldots )) \), where the function \( f \) is iterated \( L \) times. For an illustration, see figure 2.

The residual error probabilities \( p_L(p) \) at level \( L \), with varying \( L \), all intersect at a critical value \( p_{th} \) of \( p \), the error threshold. If the initial error is below the threshold, then \( p_L \) becomes smaller with an increasing level \( L \) of concatenation. If \( p \) is above the threshold, then \( p_L \) becomes larger with increasing \( L \). As \( L \) increases, the residual error probability \( p_L \) after error correction, plotted as a function of the physical error probability \( p \), approaches a step function changing its value at \( p = p_{th} \). This justifies the notion of an error threshold.

*Phil. Trans. R. Soc. A* (2012)
In fact, the behaviour just described is a precursor of the celebrated threshold theorem of fault-tolerant quantum computation. In the above, we have made two substantial simplifications. First, we allowed only for memory errors and assumed the error correction to be perfect. This is unrealistic because the error-correction procedure consists of quantum gates and is thus prone to error itself. Second, we considered only storage of quantum information rather than universal quantum computation. As we briefly review in §4, removing these two assumptions makes the analysis more involved, but the threshold result remains intact.

(d) Error discretization

In our analysis leading up to the error threshold for quantum codes, we have made a very special assumption, namely, that the environment of our quantum memory plays dice and then performs conditional Pauli flips on the quantum memory. This is a very special decoherence model. A very simple error that does not fit into this framework is, for example, the unitary transformation

$$U_l = e^{-ia/2X_l}$$

on qubit $l$, with $a$ a small rotation angle.

Does quantum error correction break down the moment we move away from probabilistic error models? This is fortunately not the case, due to the phenomenon of error discretization. Note the following lemma.

Lemma 3.3. If $E_1$ and $E_2$ are correctable errors with respect to a set $A$, then every linear combination $\alpha E_1 + \beta E_2$, with $\alpha, \beta \in \mathbb{C}$, is also a correctable error.

Lemma 3.3 is of great importance because it lifts the restriction to probabilistic Pauli errors. Pauli operators form a basis for operators on our $n$-qubit Hilbert space, and therefore, if a quantum code corrects all Pauli errors up to weight $w$, then it corrects all errors of weight up to $w$.

Proof of lemma 3.3. For a pair of correctable errors $E_1, E_2 \in A$, there are two cases, (I) $\text{Sy}(E_1) \neq \text{Sy}(E_2)$ and (II) $E_2 = E_1 g$ for some $g \in S$.

Case I: $\text{Sy}(E_1) \neq \text{Sy}(E_2)$. As noted earlier, the $n$-qubit Hilbert space splits into subspaces $\mathcal{H}(\text{Sy})$ corresponding to the different syndrome values $\text{Sy}$. Now, under the act of syndrome measurement and the subsequent conditional correction operation, the following happens:

$$(\alpha E_1 + \beta E_2) |\psi\rangle \xrightarrow{\text{Sy-M}} \begin{cases} E_1 |\psi\rangle, & \text{if } \text{Sy}(E_1) \text{ measured} \\ E_2 |\psi\rangle, & \text{if } \text{Sy}(E_2) \text{ measured} \end{cases} \xrightarrow{\text{Corr}} |\psi\rangle. \quad (3.13)$$

In the above sequence ‘Sy-M’ stands for syndrome measurement, and ‘Corr’ for correction operation conditioned on the syndrome value. By measuring the syndrome value, $\text{Sy}(E_i)$ corresponds to a projection $P_{\text{Sy}(E_i)}$ onto $\mathcal{H}(\text{Sy}(E_i))$. Therefore, $P_{\text{Sy}(E_i)} E_i |\psi\rangle = \delta_{ij} |\psi\rangle$, and the syndrome measurement does indeed act as described in equation (3.13). We thus remain with either the error $E_1$ or the error $E_2$ after the syndrome measurement. Because both errors are correctable by assumption, in either case, we return to the true encoded state $|\psi\rangle$ after error correction.

Case II: $E_2 = E_1 g$ for some $g \in S$. Then, the linear combination of $E_1$ and $E_2$ is equivalent to $E_1$, say, $(\alpha E_1 + \beta E_2) |\psi\rangle = (\alpha + \beta) E_1 |\psi\rangle$, and $E_1$ can be corrected by assumption.
We now assume that the rotation angle $f^{(2)}$ and keep terms only up to first order. Then, powers of $\sin(f)$ are affected by a local unitary Shor code. As the interested reader may verify, for example, with the nine-qubit discretization. The essential conclusion is not specific to this particular quantum error correction code and then discarded it because it could not correct any phase errors. However, the code is good enough to demonstrate the process of error correction. We consider a non-probabilistic error model in which each qubit is affected by a local unitary $U_i(\phi) = e^{-i\phi/2}X_i$. Post-selecting on the syndrome value $Sy$ (c.f. equation (3.13)), the initial state $|\Psi\rangle$ evolves under the unitary error $U(\phi) := U_1(\phi) \otimes U_2(\phi) \otimes U_3(\phi)$ and subsequent syndrome measurement as

$$|\Psi\rangle \langle \Psi | \rightarrow U(\phi) |\Psi\rangle \langle \Psi | U^\dagger(\phi) \rightarrow P(Sy) U(\phi) |\Psi\rangle \langle \Psi | U^\dagger(\phi) P(Sy).$$

We now assume that the rotation angle $\phi$ is small, such that we may expand in powers of $\sin(\phi/2)$ and keep terms only up to first order. Then,

$$U(\phi) = \cos^3(\phi/2) I - i \cos^2(\phi/2) \sin(\phi/2) (X_1 + X_2 + X_3) + O(\sin^2(\phi/2)). \quad (3.14)$$

As we may verify using definition 3.2, the errors $\{I, X_1, X_2, X_3\}$ on the r.h.s. of equation (3.14) form a correctable set. We now discuss what happens under the syndrome measurement for two values of the syndrome.

1. $Sy = (0,0)$. That is, for the measurement of both the stabilizer operators $Z_1Z_2$ and $Z_2Z_3$ have obtained the eigenvalue $+1$. This is the most likely case. Using the truncated expression equation (3.14) for $U$, the only remaining compatible error is $I$. To see this, note that e.g. $P(0)X_1|\Psi\rangle = P(0)X_1P(0)|\Psi\rangle = X_1P((1,0))P(0)|\Psi\rangle = 0$. Thus, up to first order in $\sin(\phi/2)$, if the outcome of the syndrome measurement is 0, then $|\Psi\rangle \langle \Psi | \rightarrow U(\phi) |\Psi\rangle \langle \Psi | U^\dagger(\phi) \rightarrow |\Psi\rangle \langle \Psi |$. The remaining error (none) is discrete.

2. $Sy = (1,0)$, i.e. $X_1X_2 = -1, \langle Z_2Z_3 \rangle = -1$. For the truncated expression equation (3.14) of $U$, the only compatible error is $X_1$, and thus $|\Psi\rangle \langle \Psi | \rightarrow U(\phi) |\Psi\rangle \langle \Psi | U^\dagger(\phi) \rightarrow X_1|\Psi\rangle \langle \Psi | X_1$. Again, the error is discrete (of Pauli type), and uniquely identified by the syndrome. The remaining two cases, $Sy = (0,1)$ and $Sy = (1,1)$, are analogous to case (II). The main observation is that, for all syndrome values, the syndrome measurement discretizes the error.

Next, we consider the general case with no restriction on the rotation angle $\phi$. Then, error discretization is only approximate. For example, if $Sy = (0,0)$, then the two errors $I$ and $X_1X_2X_3$ are compatible with the

*Phil. Trans. R. Soc. A (2012)*
Consider a system-bath Hamiltonian $H_{SB}$ acting on a factorized initial state $\rho_{\text{init}} = \rho_S \otimes \sigma_B$ for a time $\Delta$ between two error-correction steps. In general, the resulting state does not factorize, $e^{-iH_{SB}\Delta/h} \rho_S \otimes \sigma_B e^{iH_{SB}\Delta/h} \neq \rho_S' \otimes \sigma_B'$. However, to a high degree of accuracy, the state resulting from applying $e^{-iH_{SB}\Delta/h}$ and a subsequent error-correction operation $\mathcal{R}$ to $\rho_{\text{init}}$ does factorize. If error correction is successful, then $\mathcal{R} \circ e^{-iH_{SB}\Delta/h}(\rho_S \otimes \sigma_B) \approx \rho_S \otimes \sigma_B'$, if $\rho_S \in \mathcal{H}_{\text{code}}$.

To see this, consider a quantum code that encodes one qubit into $n$. Starting from a factorized initial state, after the unitary evolution $e^{-iH_{SB}\Delta/h}$, the entanglement entropy between quantum computer $S$ and bath $B$ will, in general, be extensive, $S_{\text{ent}} \sim n$. Then, the syndrome measurement during the recovery procedure projects the system $S$ into a two-dimensional subspace. The entanglement remaining is $S_{\text{ent}} \leq 1$—a drastic reduction! We are almost back to factorized initial conditions. However, because quantum error correction is all about the remaining ebit, the argument is not yet sufficient. To be more accurate, expand the unitary $e^{-iH_{SB}\Delta/h}$ in terms of correctable errors on the system side,

$$e^{-iH_{SB}\Delta/h} = \sum_{E_i \in \mathcal{A}} E_i S \otimes O_{i,B} + \tilde{L}_{AB},$$

with $\mathcal{A}$ a set of correctable errors and $\tilde{L}_{AB}$ a remainder. If all likely errors are correctable, then $\tilde{L}_{AB}$ has a small operator norm and can be neglected. Then, $\mathcal{R} \circ e^{-iH_{SB}\Delta/h}(\rho_S \otimes \sigma_B) \approx \rho_S \otimes \sigma_B'$, with $\sigma_B' = \sum_{E_i \in \mathcal{A}} O_{i,B} \sigma_B O_{i,B}^\dagger$. The system returns to factorized initial conditions after each completed cycle of error correction.

To summarize, syndrome measurement is a drastic intervention, disentangling the quantum register from the bath and suppressing memory effects. Using a Markovian noise model, equation (2.6) from the start may thus be justified as a first approximation. In a more detailed analysis, environments with algebraically decaying correlations are examined, e.g. Novais et al. [9]. It is found that if the decay of the correlation functions in time and space is sufficiently fast, then the noise is effectively stochastic.

(e) Resolving the puzzle

We now respond to the argument of §3a that quantum error correction cannot work. First, it was claimed that projective measurement in general destroys superposition, and therefore quantum information. This is not the case. While measurement does indeed destroy superposition states, not every superposition is used to store quantum information. Consider a code space embedded in a higher-dimensional Hilbert space. If, by the action of an error, the encoded state $|\psi\rangle$ is transformed into a superposition $a|\psi_1\rangle + b|\psi_2\rangle$ of a state $|\psi_1\rangle$ in the code space and a state $|\psi_2\rangle$ in the orthogonal complement, then the measurement of
the stabilizer generators destroys this superposition. But, as we have seen, it
does not destroy the encoded quantum information. Thus, if we use quantum
codes, there are measurements that do not cause any harm to the encoded
quantum information.

Second, it was argued in §3a that the amount of information gained in any
measurement on a finite-dimensional Hilbert space is finite, and can therefore not
single out a unique correction operation from infinitely many \textit{a priori} possible
ones. Not so. By the above-discussed phenomenon of error discretization, a
continuous set of errors is converted into a discrete set, and the finite amount
of information obtained from the syndrome measurement is sufficient to correct
for these remaining errors with high accuracy.

4. From error correction to fault-tolerant quantum computation

In previous sections, we have discussed what it takes to reliably store
quantum information. We now move on to the discussion of computing
with quantum information, which is a more complicated scenario.

This will also require us to revise the error model we have so far used.
Specifically, we assumed that errors occur while the qubits wait in memory.
Then, once in a while, an error-correction procedure is applied to remove any
errors that may have accumulated since the last error-correction step. The error-
correction procedure itself was assumed error free. This is inconsistent. Errors in
the error-correction procedure must be taken into account.

The assumptions on the decoherence processes for the remainder of this study
are the following. Decoherence processes are associated with quantum gates,
including the identity gate (memory) such that the following properties hold.

— \textit{Independence.} Decoherence processes belonging to different gates are
stochastically independent, and each erroneous gate is described by a
super-operator of form equation (2.6).

— \textit{Locality.} Decoherence processes act on the same qubits where the
corresponding gates act.

— \textit{Probabilistic error model.} Erroneous unitary gates and state preparations
are modelled by the perfect gates and preparations followed by a
probabilistic error channel. Erroneous measurements are modelled by
perfect measurements preceded by a probabilistic error channel.

Those basic assumptions exclude some potentially relevant physical phenomena.
For example, independence excludes memory effects, and independence and
locality combined exclude most types of spatially correlated decoherence. We
invoke the earlier-mentioned assumption nonetheless, to simplify the analysis.

To justify this simplification, it is important to note that all of the earlier-
mentioned assumptions can be relaxed. Threshold theorems have been derived for
certain types of non-Markovian noise [10,15], for spatially correlated errors [8] and
for non-probabilistic error models [15]. Furthermore, the presence of correlations
in the noise does not necessarily complicate error correction significantly. For
example, Aharonov \textit{et al.} [8] discusses a setting in which a Hamiltonian $H =
HS + HB + HSB$ couples a system (quantum computer) $S$ to a bath $B$, and perfect
error-recovery operations occur at time intervals $t_0$. $H_{SB}$ has the special form 
$$H_{SB} = \sum_{ij} H_{ij},$$
with $H_{ij}$ acting on qubits $i, j$ and on the bath $B$. The result is that if 
$t_0 \sum_j \| H_{ij} \| < \eta$ for all $i$ and a suitable constant $\eta$, then quantum information can 
be protected for arbitrarily long times. In particular, if the qubits are arranged on 
a $D$-dimensional grid and $\| H_{ij} \|$ falls off algebraically with a power $z > D$, $\| H_{ij} \| \sim |r_i - r_j|^{-z}$, then fault tolerance can be achieved. Thus, long-range correlated errors 
are compatible with fault tolerance.

(a) Error propagation

Consider an encoded unitary gate $\bar{U}$ acting on an encoded state $|\bar{\psi}\rangle$, 
$|\psi\rangle \rightarrow \bar{U}|\psi\rangle \in \mathcal{H}_{\text{code}}$, and the projector $P_{\text{code}}$ on the code space. Then, 
$$\bar{U}|\psi\rangle = \bar{U}P_{\text{code}}|\psi\rangle = (\bar{U}P_{\text{code}}\bar{U}^\dagger)\bar{U}|\psi\rangle.$$ 
Therefore, $\bar{U}$ is an encoded gate if and only if 
$$\bar{U}P_{\text{code}}\bar{U}^\dagger = P_{\text{code}}. \quad (4.1)$$

In addition, we require the encoded gates to operate fault tolerantly. This means 
that likely errors in or immediately before the encoded gate should not cause the 
subsequent error-correction procedure to fail. Consider the action of a unitary 
encoded gate $\bar{U}$ on a state $|\phi\rangle$ outside but ‘near’ the code space, namely, $|\phi\rangle = E|\bar{\psi}\rangle$ with $|\bar{\psi}\rangle \in \mathcal{H}_{\text{code}}$ and $E$ a correctable error. The action of $\bar{U}$ on $|\phi\rangle$ is $|\phi\rangle = E|\bar{\psi}\rangle \rightarrow \bar{U}E|\bar{\psi}\rangle = (\bar{U}E\bar{U}^\dagger)\bar{U}|\bar{\psi}\rangle$. Thus, the error $E$ is propagated by the gate $\bar{U}$,

$$E \rightarrow E' = \bar{U}E\bar{U}^\dagger. \quad (4.2)$$

That is, an error $E$ followed by a gate $\bar{U}$ is equivalent to the gate $\bar{U}$ followed 
by $E'$. It is $E'$, rather than $E$, which is seen by the next error-correction step. 

A priori, there is no guarantee that $E'$ is a correctable error such as $E$ was. Let us 
consider this in the simple example of a syndrome extraction circuit of figure 3.

Using the propagation relations for the CNOT gate,

$$\text{CNOT}(c,t)X_c C\text{NOT}(c,t)^\dagger = X_c X_t \quad \text{and}$$
$$\text{CNOT}(c,t)X_t C\text{NOT}(c,t)^\dagger = X_t,$$ \quad (4.3)

Phil. Trans. R. Soc. A (2012)
it is easily verified that the circuit displayed in figure 3a measures the stabilizer operator $X_1X_2X_3X_4$. However, it does not do so fault tolerantly. In this regard, consider a single spin-flip error $X$ occurring on the ancilla qubit after the second CNOT gate. Using the above propagation relations, after all four CNOTs have been applied, this error has propagated into $X_3X_4X_a$. The error $X_a$ is subsequently absorbed in the measurement of the ancilla qubit, without causing harm. But the error $X_3X_1$ remains. For most small codes, a two-local error is not correctable. Thus, by error propagation, a correctable local error was converted into a non-correctable one. The procedure described is thus not fault tolerant.

All circuit elements involved in fault-tolerant encoded gates, namely, transversal encoded gate operation and syndrome extraction, must be carefully designed to prevent a malicious spread of error.

(b) Transversal gates

We now need to think about how to perform encoded quantum gates fault tolerantly. First, here are two ways of performing encoded quantum gates that are not fault tolerant. (i) Decode a (set of) encoded qubit(s), perform the quantum gate on the bare qubits, and encode again. Clearly, during the decoded stage, the bare qubits are highly susceptible to error. Somewhat more interesting is the following procedure. (ii) Consider a unitary gate $U = e^{i\tau H}$, with $H$ Hermitian. Build the Hamiltonian $\tilde{H}$ (the encoded version of $H$), and evolve the system unitarily for a time $\tau$. Again, the procedure is not fault tolerant. The reason is that we may have evolved for a time $\tau' = \tau + \Delta \tau$. For $\Delta \tau \neq 0$, we have implemented an erroneous unitary, and have no way of detecting it.

Here is a way of acting on encoded states that does not propagate errors badly. For an $n$-qubit quantum code, consider as an example the unitary operation

$$U_Z(\alpha) = \bigotimes_{i=1}^{n} e^{i\alpha Z_i}. \quad (4.4)$$

Clearly, local errors are propagated into local errors under the gate $U_Z(\alpha)$, and errors that are introduced by the gate operation itself are also local. But is $U_Z(\alpha)$ at all an encoded gate? Clearly, it cannot be for all angles $\alpha$. For example, for codes of distance $d \geq 2$ and very small $\alpha$, $U_Z(\alpha)$ is an error rather than an encoded gate.

However, what at first looks like a problem is actually half of the solution. The earlier-mentioned discussion leaves open the possibility that there are angles $\alpha_m = \alpha_0 m$, with $m \in \mathbb{Z}$, $|\alpha_0| < \pi$, such that $U_Z(\alpha)$ is an encoded gate. Depending on the code considered, this possibility is indeed made use of, as we discuss later.

That $U_Z(\alpha)$ is an encoded gate only for a discrete set of rotation angles is a useful feature. Suppose that one wants to implement $\tilde{U} = U_Z(\alpha_0)$ but overshoots the rotation angle a bit, implementing $U_Z(\alpha_0 + \Delta \alpha) = U_Z(\Delta \alpha) U_Z(\alpha_0)$. If the initial state $|\psi\rangle$ is in the code space, so is $|\psi\rangle = U_Z(\alpha_0)|\psi\rangle$. The final state $U_Z(\Delta \alpha)|\psi\rangle$ then has a small component outside the code space, and error-correction will bring it back to the intended state $|\psi\rangle$. Thus, error correction is used to reset a rotation angle that was slightly off.

The above procedure can be generalized to multi-qubit gates. The requirement imposed is that each physical gate employed for the encoded gate acts on at most one physical qubit in each code block. Such an encoded gate is called transversal.

Phil. Trans. R. Soc. A (2012)
Example. The Steane code is described by the stabilizer group

\[ S_{\text{Steane}} = \left\{ X_4 X_5 X_6 X_7, X_2 X_3 X_6 X_7, X_1 X_3 X_5 X_7, Z_1 Z_5 Z_6 Z_7, Z_2 Z_3 Z_6 Z_7, Z_1 Z_3 Z_5 Z_7 \right\} \] (4.5)

and encoded Pauli operators

\[ \bar{X} = X_1 X_2 X_3 X_4 X_5 X_6 X_7 \] and

\[ \bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7. \] (4.6)

We now show that the encoded Hadamard gate is transversal for the Steane code, namely \( \bar{H} = \bigotimes_{i=1}^{7} H_i \). Analogous to \( P_{\text{code}} \), if the state vector changes \( |\psi\rangle \rightarrow \mathcal{V} |\psi\rangle \), the corresponding change on a stabilizer element \( g \) and an encoded Pauli operator \( \bar{\Sigma} \) are \( g \rightarrow \mathcal{V} g \mathcal{V}^\dagger \) and \( \bar{\Sigma} \rightarrow \mathcal{V} \Sigma \mathcal{V}^\dagger \). Using the relations \( HXH^\dagger = Z \), \( HZH^\dagger = X \), \( H^\dagger = H \) and equation (4.5), we easily verify that \( \bar{H} g \bar{H}^\dagger \in S \), for all \( g \in S \). Hence, \( \bar{H} P_{\text{Steane}} \bar{H}^\dagger = P_{\text{Steane}} \), and \( \bigotimes_{i=1}^{7} H_i \) is an encoded gate. Furthermore, with equation (4.6), \( \bar{H} \bar{X} \bar{H}^\dagger = \bar{Z} \), \( \bar{H} \bar{Z} \bar{H}^\dagger = \bar{X} \) is indeed the encoded Hadamard.

The Steane code has more transversal gates. By an argument analogous to the above, we can show that the encoded versions of the \( \pi/4 \) phase gate \( U_{Z}(\pi/4) \), the CNOT gate and the conditional phase gate \( A(Z) := e^{i\pi/2} |11\rangle \langle 11| \) are all transversal, namely,

\[ U_{Z}(\pi/4) = \bigotimes_{i=1}^{7} U_{Z,i} \left( -\frac{\pi}{4} \right), \quad \text{CNOT} = \bigotimes_{i=1}^{7} \text{CNOT}_i \quad \text{and} \quad A(Z) = \bigotimes_{i=1}^{7} A(Z)_i. \]

In the two-qubit gates of the above set, the CNOT and the conditional phase gate, each bare gate in the transversal implementation acts on exactly one qubit in each code block, and each physical qubit is acted on by exactly one gate.

The Steane code has a fairly large set of transversal gates—are they sufficient for universal quantum computation? The answer is, unfortunately, in the negative. All transversal encoded gates in the Steane code are the so-called Clifford gates, which means that they map all Pauli operators onto Pauli operators under conjugation. Indeed, we made use of this property above when explaining the action of the encoded gates. However, the group of Clifford gates is finite, and thus can not give rise to universal quantum computation.

Every universal set of gates needs a non-Clifford gate. In the universal set of equation (2.4), the non-Clifford gate was \( e^{i\pi/8} Z \). Now, the seven-qubit Steane code has a cousin, a 15-qubit stabilizer code based on the classical so-called punctured Reed–Muller code \( \mathcal{R}^*(1,4) \) [16] (the Steane code is based on \( \mathcal{R}^*(1,3) \)). For a list of properties of this quantum code and their derivation, we refer the reader to Bravyi & Kitaev [17]. A geometrical description of the code stabilizer is given in figure 4. The property of interest to us is that the 15-qubit code has a transversal
Review. Quantum error correction

U_{Z}(\pi/8) gate. The CNOT and conditional phase gates are also transversal, but the Hadamard gate is not! Again, we fail to achieve a universal set of encoded transversal gates. But the following construction helps out:

$$|\varphi\rangle \xrightarrow{X} |\varphi\rangle$$

This (bare) circuit takes as input an unknown state $|\phi\rangle$ and an ancilla $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, applies a conditional phase gate, followed by an $X$ measurement of the first qubit and a spin flip conditioned on the outcome of that measurement. It is easily checked that it outputs the state $H|\varphi\rangle$ on the unmeasured qubit.

For the 15-qubit code, all these operations can be performed in a transversal fashion, including the $X$ measurement. We have thus achieved a universal gate set that operates transversally but requires measurement as part of the procedure. The property of transversality is preserved under code concatenation. By concatenating the 15-qubit code, we can thus build large codes that suppress errors to an arbitrary degree.

Are there more clever quantum codes that provide us with a universal set of transversal encoded gates and get by without measurement gadgets such as the circuit in equation (4.7)? Unfortunately, this is not the case. It can be proved that no quantum code can provide a universal set of transversal gates implemented in a purely unitary fashion [18,19].

Phil. Trans. R. Soc. A (2012)
Figure 5. Concatenated, encoded gates for fault-tolerant quantum computation. (a) The fault-tolerant gate, comprising a transversal gate and an error correction (EC), is repeated at every coding level. (b) The rectangle consists of the transversal gate and a subsequent error correction. The extended rectangle contains the leading error correction in addition. Errors from within the extended rectangle can cause failure of the gate in the included rectangle. (Online version in colour.)

(c) The threshold theorem

We can now put the elements of the construction together. Figure 5a shows the recursive structure for a fault-tolerant-encoded gate at coding level $l$. It comprises a transversal gate and an error-correction circuit. Both parts are built of level $l - 1$ gates.

The mechanism for reducing the error rate per gate is the same that we have already come across in concatenated codes: the encoded gates are built in a self-similar fashion over a number of coding levels. For gate construction to fail at coding level $l$, at least, $t + 1$ gates must fail at level $l - 1$, and therefore the probabilities $p_l$, $p_{l-1}$ of gate failure at levels $l$ and $l - 1$ are related via

$$p_l = kp_{l-1}^{t+1}. \quad (4.8)$$

Therein, $k$ is the number of error combinations at level $l - 1$ of weight $t + 1$ that cause failure at level $l$ (the circuit can correct $t$ independent errors).

While intuitive, equation (4.8) turns out to be much harder to prove than its counterpart for concatenated codes. The reason is that for a threshold theorem of fault-tolerant quantum computation, we need to take into account errors in the error-correction procedure itself, not merely storage errors. This introduces a mismatch between the actual circuit element that is reproduced self-similarly at each coding level, and the circuit area where errors can cause failure of any given encoded gate. The circuit element that is nested with itself at all coding levels is, for each gate, called the ‘rectangle’ (figure 5). However, the errors that, if sufficient in number, can cause failure of the gate come from a larger region called the ‘extended rectangle’. The rectangle consists of a transversal encoded gate and a trailing error correction. The extended rectangle consists of the transversal gate, the trailing error correction plus a leading error correction. Errors that occur during the transversal gate operation and early in the subsequent error correction
affect the functioning of a gate at a given coding level. But these are not
the only error locations harmful for a given gate. Also, there will be errors in
any leading error correction that the error-correction procedure cannot detect
and thus passes on in the outputted state. These errors need to be included
in the analysis as well, which requires one to consider extended rectangles
(figure 5b).

Despite the complications that arise in the derivation, the end result is that, as
for code concatenation, the gate failure rate at successive coding levels follows a
recursive relation, equation (4.8). Therefore, if the error at the bare level is below
a critical value, then the residual error rapidly decreases with increasing coding
level. Errors can be suppressed to an arbitrary degree. A detailed analysis shows
that the overhead of fault tolerance is poly-logarithmic. If a perfect quantum
circuit comprises $S$ gates, then its fault-tolerant realization requires $S' \sim S \log^\gamma S$
imperfect gates. Therein, $\gamma = 2 \ldots 12$ for known constructions.

5. Suggestions for further reading

(a) Quantum coding theory

In this study, we focused exclusively on stabilizer codes because they follow
straight from classical codes and the construction of fault-tolerant universal gate
sets is a manageable task for them. However, many interesting families of quantum
codes exist outside the realm of stabilizer codes, such as the codeword-stabilized
quantum codes [20,21] and the general concatenated quantum codes [22]. These
codes often outperform stabilizer codes in purely coding-theoretical benchmarks.
Furthermore, many properties of quantum codes can be stated in full generality,
without any reference to a specific code family. For example, the important
notion of the ‘set of correctable errors’, which we introduced for stabilizer
codes in definition 3.2 has a compact definition that applies to all quantum
codes [23,24].

(b) The threshold theorem

The threshold theorem of fault-tolerant quantum computation is the capstone
result of the theory of quantum error correction. Even for the simplest
decoherence models, its proof is rather intricate and beyond the scope of this
introductory article. A threshold theorem is rigorously established in Aliferis
et al. [7] for quantum codes down to distance three, including the workhorse of
many fault-tolerance constructions—the seven-qubit Steane code. For a summary
of the argument in Aliferis et al. [7], see Gottesman [25]. For earlier versions of
the threshold theorem, see earlier studies [5,6].

(c) Error-correction pros and cons

Fault-tolerant quantum computation is backed by a rigorous mathematical
theorem, but do the assumptions of this theorem apply to realistic physical
systems? Room for debate remains because, to date, threshold theorems are
proven case by case, each time covering only a small family of decoherence models.
To chart the boundary between decoherence models that do and that do not
permit successful quantum error correction, the presence of long-range spatial
and temporal correlations among errors has been picked as a test case. **Pros:** in Aharonov et al. [8], it is shown that, for quantum registers laid out on a $d$-dimensional lattice, fault-tolerant quantum computation remains possible if an unwanted two-body interaction among the qubits falls off faster than $1/r^d$ (for related work, see earlier studies [9,10].). **Cons:** Klesse & Frank [26] consider a register of qubits coupled to a common bath of massless bosons, with spectral function $J(\omega) \sim \omega^s e^{-\omega/\Omega}$ ($\Omega$ cut-off). Under the pessimistic assumption that the time between two successive steps of perfect error correction is proportional to the linear spatial extension of the quantum register, it is shown that quantum error-correction fails if $s \leq 2$. This includes the Ohmic case of $s = 1$, which is typical for settings in quantum optics. Furthermore, in Alicki et al. [27], it is shown that two basic assumptions that often enter the analysis of fault tolerance, namely, (i) fast quantum gates and (ii) the availability of fresh ancilla states throughout the computation, in combination prevent the limits in which a Markovian master equation can be rigorously derived. Nevertheless, as pointed out in Alicki et al. [27], the Markovian approximation is often assumed simultaneously with (i) and (ii).

### (d) Value of the fault-tolerance threshold

After threshold theorems have been established for various decoherence models, what are the values of the corresponding error thresholds? If the thresholds came out to be $10^{-50}$, the threshold theorems would remain of fundamental interest, but have no technological implications. Fortunately, the thresholds for fault-tolerant quantum computation turn out to be much higher, of the order from $10^{-4}$ to $10^{-2}$. The highest threshold known to date is 3 per cent [28], meaning that one gate in 30 is allowed to fail. It is also of interest to investigate quantum computer architectures with realistic limitations in their interactions. One such scenario is a two-dimensional array of qubits in which only nearest neighbours are allowed to interact. It is of relevance for quantum computation with cold atoms in optical lattices or arrays of Josephson junctions. The thresholds achievable in this setting are 0.75 per cent [29] to 1.1 per cent [30]. A different scenario of interest is probabilistic heralded gates (they fail most of the time, but when they succeed, it becomes known). This model applies to quantum computation with photons [31], and a threshold of $10^{-4}$ [32,33] has been established.

### (e) Gadgets

Generally, fault-tolerant gate constructions can be made more robust and efficient, if part of the procedure is moved offline into the preparation and verification of special states that can be used to implement quantum gates via teleportation [34]. For example, the fault-tolerant implementation of an $e^{i\pi/8}Z$ gate as described in §4 has the weakest protection against decoherence among all gates, and consequently sets the threshold value. A much more robust and at the same time more efficient procedure for the same task—based on exactly the same quantum code—is ‘magic state distillation’ [17]. Finally, in many physical systems of interest for quantum computation, in particular condensed matter systems, the process of measurement is very slow. Does this mean that everything
decoheres before a single stabilizer measurement is completed? Not so. By a clever construction, slow measurements can be prevented from reducing the fault-tolerance threshold [35].

6. Conclusion

In this work, we have reviewed three important ideas in quantum error correction, namely, quantum codes, error discretization and transversal quantum gates. Along with others, they contribute the techniques and phenomena that allow to establish the core result in the area of fault-tolerant quantum computation: the threshold theorem.

At present, the theory of quantum error correction is way ahead of its experimental verification. After establishing the threshold theorem and pushing up the threshold value from an initial $10^{-8}$–$10^{-6}$ to a current 3 per cent, the task remaining for theory is the reduction of the significant operational overheads associated with quantum fault tolerance. On the side of experiment, various quantum error-correction protocols have to date been realized in nuclear magnetic resonance systems [36–38] and ion traps [39,40], among them being magic state distillation and error correction for phase or spin flips. The physical realization of a quantum error-correction procedure that can simultaneously correct spin- and phase-flip errors (e.g. based on the Steane code) does now seem in reach of near-future experiments.

The author thanks Philip Stamp, Ike Chuang and Luming Duan for discussions. This work is based on notes for the summer school ‘Frontiers of Quantum Information Science’ held at Tsinghua University, Beijing, China, in July 2011. This work was supported by NSERC, PIMS and CIFAR.

References


