Multiple-particle interference and quantum error correction

By Andrew Steane

Department of Atomic and Laser Physics, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, UK

a.steane@physics.oxford.ac.uk

The concept of *multiple-particle interference* is discussed, using insights provided by the classical theory of error correcting codes. This leads to a discussion of error correction in a quantum communication channel or a quantum computer. Methods of error correction in the quantum regime are presented, and their limitations assessed. A quantum channel can recover from arbitrary decoherence of x qubits if K bits of quantum information are encoded using n quantum bits, where K/n can be greater than $1-2H(2x/n)$, but must be less than $1-2H(x/n)$. This implies exponential reduction of decoherence with only a polynomial increase in the computing resources required. Therefore quantum computation can be made free of errors in the presence of physically realistic levels of decoherence. The methods also allow isolation of quantum communication from noise and evesdropping (quantum privacy amplification).

1. Introduction

The concepts of quantum interference, correlations and entanglement are at the heart of quantum mechanics. A quantum interference between two parts a system's evolution is prevented when the system interacts with another so as to produce an entangled state. In such situations, properties of the two entangled systems are correlated, and correlations of this type are subject to the Bell inequalities (Bell 1964), which shows that they are non-local in character. Whereas for many quantum mechanical effects a model can be given which relies only on classical concepts, this non-locality is a feature of quantum mechanics which is alien to the very structure of other (classical) theories. (Many texts are available as an introduction to this broad subject, for example that of Shimony (1989).)

One way of shedding light on the nature of quantum mechanics is to pose the question 'to what extent can quantum mechanical behaviour be modelled in classical terms?' To make this slightly vague question more concrete, it can be posed thus: 'to what extent can quantum mechanical behaviour be simulated by means of a universal computer operating according to the laws of classical mechanics?' Such a 'universal' computer is universal in the sense of a universal Turing machine: it can simulate the behaviour of any other computer in the set of all possible computers (Turing 1936). However, as long as the set of 'possible' computers includes only those operating by classical laws of physics, then the non-local correlations which arise in the real world cannot be simulated, as was discussed by Feynman (1982). To simulate

Proc. R. Soc. Lond. A (1996) **452**, 2551–2577
Printed in Great Britain

TEX Paper

them, the computer must be allowed to operate according to the laws of quantum mechanics. Hence one introduces the concept of the quantum, as opposed to classical, computer (see Deutsch 1985; Ekert 1995; Ekert & Jozsa 1996), and the question under consideration can be rephrased: 'to what extent can a quantum computer perform calculations which are beyond the computing abilities of a classical computer?' For the physicist, this question addresses fundamental questions concerning the nature of our most basic physical theory. However, the answer is also of considerable practical interest because computing ability is an extremely useful kind of ability.

The theoretical analysis of quantum computers has by now passed some important milestones, among them the demonstration of how to construct a universal quantum computer (Deutsch 1985), the discovery of simple universal quantum gates (Deutsch *et al.* 1995; Barenco 1995; DiVincenzo 1995), and the presentation of algorithms for idealized quantum computers which surpass the computing ability of known algorithms for classical computers, and which appear to surpass even what is in principle possible classically (Deutsch & Jozsa 1992; Bernstein 1993; Shor 1994; Simon 1994). It has been obvious from the outset that quantum computation is different from classical computation precisely because of the possibility of quantum interference and entanglement. However, this entanglement is itself sensitive to a problem which is unavoidable in the quantum context, namely, *decoherence* of the state of the computer (Zurek 1993; Landauer 1995). The useful algorithms just mentioned were initialy proposed under the assumption of the idealized case that this decoherence, or generally any process involving loss of quantum information, is negligible. However, it can be argued that the possibility of decoherence is itself just as fundamental a feature of quantum mechanics as the interference and entanglement of which a quantum computer takes advantage. Such decoherence must be considered, for example, in any discussion of the 'Schrödinger's cat' paradox (Schrödinger 1935; for a textbook treatment see, for example, Peres 1993). The cat in Schrödinger's thought-experiment corresponds here to the quantum computer itself. Hence, the idealization in which decoherence is taken to be negligible is not merely a limit on the practical application of the theory of quantum computation, it is in fact an 'idealization too far', since it involves neglecting a basic aspect of quantum theory, as has been emphasized by Landauer (1995).

This paper discusses both the nature of quantum interference involving many particles, and also the question of decoherence in quantum computers. It is shown that both questions are intimately concerned with the issue of error correction which arises in classical information theory. Unruh (1995) and Palma *et al.* (1996) calculated the sensitivity of a 'bare' quantum computer to thermal decoherence. Here, we are concerned with the different question of how to add redundancy to such a 'bare' computer in order to stabilise it against all error processes, including decoherence. The classical theory of error correction which is invoked is a well-founded body of knowledge involving some beautiful mathematical concepts, and we can take advantage of this knowledge in our quest to understand quantum mechanics more fully. This paper does not assume much familiarity with classical error correction, however. At the risk of alienating experts, concepts from classical information theory are introduced for the most part with sufficient explanation to allow readers unfamiliar with this material to follow the argument. The readily available textbooks such as MacWilliams & Sloane (1977) and Hamming (1986) give further explanation.

In § 2 a general theory of interference involving many particles is presented. It is shown that an interesting class of entanglements involving many particles (or other

simple quantum systems) can be understood by appealing to the known theory of classical error correcting codes. In § 3 the same concepts are applied to the problem of error correction in a set of two-state systems ('quantum bits'). Coding and correction methods are presented which allow the problem of decoherence in a quantum computer to be circumvented. The same methods allow privacy in quantum cryptography to be enhanced (for a review and references to this subject, see, for example, Hughes *et al.* (1995) and Phoenix & Townsend (1995).) In § 4 the limitations of these coding methods are estimated, by a calculation reminiscent of Shannon's main theorem for communication through a noisy channel. A full quantum equivalent to Shannon's theorem is not found, and this is a limitation of the present work, but the ideas presented here suggest ways of tackling this more general question. The conclusions of the present discussion are hopeful, however, in that they suggest that error-free quantum computation is possible using resources (numbers of quantum bits and of operations) that are only a polynomial factor greater than those required by an ideal quantum computer. Indeed, the judicious use of redundency and error correction allows the probability of decoherence to *fall exponentially* with the amount of redundency. This is a conclusion which has commonly been imagined to be ruled out for quantum systems. The implementation of the error correction procedure to be described, without introducing excessive extra decoherence, remains a severe technological challenge, however.

2. Multiple-particle interference and parity checks

(*a*) *Single parity check*

Consider a two-state quantum system. Its two-dimensional Hilbert space is spanned by two orthogonal states which will be written $|0\rangle$ and $|1\rangle$. These states may for example be different states of motion of a spinless particle of no internal structure, or they may be different internal states, such as those of a two-level atom. The simple concept of quantum interference arises when such a system is in a state such as $(|0\rangle + \exp(\mathrm{i}\phi)|1\rangle)/\sqrt{2}$, and measurements are performed which project the state onto $(|0\rangle \pm |1\rangle)/\sqrt{2}$. Now, what happens if this system interacts with another two-state system, such that the total state of the pair is the entangled state $(|0\rangle \otimes |0\rangle + \exp(\mathrm{i}\phi)|1\rangle \otimes |1\rangle)/\sqrt{2}$? In this case, measurements on either subsystem alone (hereafter called a 'particle') will not reveal any interference effect (any dependence on the value of ϕ). If both particles are measured in the $(|0\rangle \pm |1\rangle)/\sqrt{2}$ basis, on the other hand, and *the results of the measurements on each particle pair are compared*, then a correlation is observed which is sensitive to ϕ. The probability that the particles are found in the same state is equal to $\cos^2 \phi/2$. Whereas before we had a single particle interference effect, we now have a *two-particle interference*, in the sense that no measurements on individual particles reveal the interference phase ϕ, while combining measurements on both particles makes the interference 'fringe' $\cos^2 \phi/2$ observable.

The above argument was extended by Greenberger *et al.* (1990), so that one speaks of an 'n-particle interference,' meaning a state of n particles in which *no* measurements on *any* subset of the n particles (containing 1, 2 or any number up to $n-1$ particles) will suffise to reveal an interference, but once all n are measured (in the correct basis), and correlations established between the results, the interference be-

comes apparent. Such an n-particle interference is the state

$$|n,\phi\rangle = (|000\overset{n}{\cdots}0> + \exp(\mathrm{i}\phi)|111\overset{n}{\cdots}1>)/\sqrt{2}, \tag{2.1}$$

where there are n zeroes or ones in the ket labels, and the usual convention has been followed of writing product states $(|0\rangle \otimes |0\rangle \otimes \cdots)$ by the notation $|00\cdots\rangle$. When $n = 2$ the correlations are subject to the most simple type of Bell inequality. When $n = 3$ we have the 'GHZ' state of Greenberger, Horne and Zeilinger (1989), in which correlations can be found which are both non-local and which occur with certainty. Also, Zurek (1981) stressed that three particles are sufficient and necessary to establish a 'preferred' basis for inter-particle correlations. For larger n, Mermin (1990) derived a Bell-type inequality which becomes more and more severe as n grows.

Is there a simple way of seeing that the state $|n,\phi\rangle$ is an n-particle interference? Clearly, a 'which path' argument will suffice. If any set of less than n particles is measured, the remaining unmeasured two-state system could in principle be measured in the $\{|0\rangle,|1\rangle\}$ basis, thus indicating which of the two 'paths' $|000\overset{n}{\cdots}0\rangle$ or $|111\overset{n}{\cdots}1\rangle$ the whole system followed, which prevents any interference between those paths†.

In the case that all n particles are measured so as to observe a ϕ-dependent result, it is instructive to examine how such interference can come about, it being a property of all n particles, and not of any subset. To this end, a simple notation will be introduced. The pair of states $\{|0\rangle,|1\rangle\}$ will be referred to as 'basis 1', and written using standard (unbarred) labels. The states $|\overline{0}\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$, and $|\overline{1}\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$, will be referred to as 'basis 2', and distinguished from basis 1 by using bars over the ket symbols. (The two bases are related by a rotation in Hilbert space through 45°.)

Consider the three-particle interference $|3,\phi\rangle = (|000\rangle + \exp(\mathrm{i}\phi)|111\rangle)/\sqrt{2}$. To observe the interference, measurements must be carried out in basis 2 on all the particles. Therefore, it is useful to write the state $|3,\phi\rangle$ in terms of basis states of basis 2:

$$\begin{aligned}|3,\phi\rangle \equiv{}& (1+\mathrm{e}^{\mathrm{i}\phi})(|\overline{000}\rangle + |\overline{011}\rangle + |\overline{101}\rangle + |\overline{110}\rangle)/4 \\ &+(1-\mathrm{e}^{\mathrm{i}\phi})(|\overline{111}\rangle + |\overline{100}\rangle + |\overline{010}\rangle + |\overline{001}\rangle)/4.\end{aligned} \tag{2.2}$$

Measurements carried out in basis 2 will collapse the state onto one of the 8 product states $|\overline{000}\rangle, |\overline{001}\rangle \cdots |\overline{111}\rangle$. Examining equation (2.2), one finds that *the probability of obtaining an even number of 1s* is equal to $\cos^2\phi/2$. In other words, the information on the value of ϕ is contained in the *parity check* of the total state in basis 2. We are using the word 'parity' in the sense of the parity check for binary communication channels.

With this insight in terms of parity, a new way of explaining the n-particle inteference arises. For, to learn the parity of a string of n bits, it is obvious that one must know the value of all n bits. No subset of the bits contains this information. It is important to note that when $\phi = 0$, *all* the 4 possible product states of even parity appear, and when $\phi = \pi$, all the 4 possible product states of odd parity appear. If this were not the case, then sometimes a subset containing less than 3 bits

† If this description in terms of 'following a path' is felt to be too reliant on an assumption of wavefunction collapse, it can always be stated more elaborately in terms of entanglements with external measuring devices, and the same conclusion is obtained.

would define the parity. For example, if we know from the outset that the product state $|\overline{111}\rangle$ is not present in the final superposition, then whenever measurements of the first two bits both yield 1, we know immediately that the overall parity is even, without measuring the third bit.

The parity check argument is true for any n (this was shown by Steane (1996) and will also be demonstrated below). The parity check is a two-valued quantity, and thus can store a single bit of information. It may be imagined as a single bit stored symmetrically among all the n bits.

(*b*) *Multiple parity checks*

Once the n-particle interference has been understood as a parity check in basis 2, the concept of multiple-particle interference can be generalized. For, an overall parity check is the simplest example of *error detection* in a classical communication channel. More advanced types of error detection and correction are associated with more complicated types of n-particle interferences. To understand the details, we make use of theorems 1 to 3 of Steane (1996), which are reproduced below. Before they are presented, a few notations will be introduced.

First, the two-state systems which have so far been referred to as 'particles' will hereafter be called qubits†. The product states in either of bases 1 or 2 (e.g. $|0010\rangle$ or $|\overline{01101}\rangle$) will be referred to as *words*, since each such state is identified by a unique string of bits when written in the relevent basis. A superposition of product states defines a set of words. A set of words is called a *code*, following standard nomenclature in the theory of error correcting codes. When writing superposition (entangled) states, the overall normalization factor will often be omitted, since it is not important to the main argument, and can always be reintroduced easily if necessary. The theorems derived in Steane (1996) are as follows.

Theorem 2.1. *The word* $|000\cdots0\rangle$ *consisting of all zeros in basis* 1 *is equal to a superposition of all* 2^n *possible words in basis* 2, *with equal coefficients.*

Theorem 2.2. *If the* j*th bit of each word is complemented* $(0 \leftrightarrow 1)$ *in basis* 1, *then all words in basis* 2 *in which the* j*th bit is set (is a* $\bar{1}$*) change sign.*

Theorem 2.3. *When the quantum state of the system forms a linear code* C *in basis* 1, *in a superposition with equal coefficients, then in basis* 2 *the words appearing in the superposition are those of the dual code* $C^{\perp}$.

Theorems 2.1 and 2.2 are easy to prove, while theorem 2.3 requires further comment. A *linear* code C is any set of n-bit words for which if the bitwise EXCLUSIVE-OR (addition modulo 2) operation $\oplus$ is carried out between any two words in the code, then the resulting word is also in the code. Such codes can be expressed in terms of an $(n \times k)$ *generator matrix* G, whose k rows are n-bit words. The code consists of all linear combinations (by bitwise EXCLUSIVE-OR) of the rows of G. This produces 2^k different words in the code. It can be shown that any linear code is also fully defined by its $(n \times (n-k))$ *parity check matrix* H. The code consists of all words u for which $H_j \cdot u$ has even parity, for all rows H_j of H, where the dot indicates the bitwise AND operation. When $H_j \cdot u$ has even parity, we say that 'u satisfies the parity check H_j'.

† The word 'qubit' for 'quantum bit' is now a standard term for a two-state system.

In other words, H_j singles out a subset of the bits of u, and it is the parity of this subset which is 'checked' when we ascertain the parity of $H_j \cdot u$.

If C is a linear code, then the dual code $C^\perp$ is defined to be the set of all words v for which $v \cdot u$ has even parity for all $u \in C$. If $C^\perp$ is the dual of C, then C is the dual of $C^\perp$. The only property of dual codes which will interest us for the moment is that *the generator matrix of a code C is the parity check matrix of the dual code $C^\perp$*. (This property is used in the derivation of theorem 2.3 (see Steane 1996).)

Using the formalism, it is possible to generalize the concept of multiple-particle (or multiple-qubit) interference. It is necessary first to extend slightly the definition of the generator matrix. We associate with each row G_j of the matrix a phase factor $\exp \mathrm{i}\phi_j$, and when different rows are combined, these factors multiply:

$$G_j \oplus G_k = \mathrm{e}^{\mathrm{i}(\phi_j+\phi_k)}(|G_j| \oplus |G_k|), \qquad (j \neq k), \tag{2.3}$$

where $|G_j|$ signifies the jth row with phase factor set to 1. If a row is combined with itself, the resulting phase factor is defined to be 1, so that the zero word is produced: $G_j \oplus G_j = 000\cdots0$. One may regard the words as vectors in a discrete n-dimensional vector space (Hamming space), and the phase factors as scalars.

The generalized multiple-particle interference is defined through the following theorem.

Theorem 2.4. *If G generates the state in basis 1, then the probability that the parity check $|G_j|$ is satisfied in basis 2 varies as* $\cos^2 \phi_j/2$.

Proof. This is closely related to the proof of theorem 2.3. To find the effect of the jth row of G, first consider the state $|G'\rangle$ generated by G' in basis 1, where G' consists of all rows of G except the jth, with all phase factors set to 1. By theorem 2.3, for this state, all the parity checks of G' are satisfied in basis 2. Now complement, in basis 1, the qubits specified by the jth row of G. Call the resulting state $|G''\rangle$. By repeated applications of theorem 2.2, this has the effect that all words change sign in basis 2 which do not satisfy the parity check $|G_j|$. Now form

$$\tfrac{1}{2}(1+\mathrm{e}^{\mathrm{i}\phi_j})(|G'\rangle + |G''\rangle) + \tfrac{1}{2}(1-\mathrm{e}^{\mathrm{i}\phi_j})(|G'\rangle - |G''\rangle) \equiv |G'\rangle + \mathrm{e}^{\mathrm{i}\phi_j}|G''\rangle. \tag{2.4}$$

The left-hand side of this equivalence shows that the probability that the jth parity check is satisfied in basis 2 is proportional to $\cos^2 \phi_j/2$, since if $|G'\rangle$ and $|G''\rangle$ are added (subtracted), all words which satisfy (respectively fail to satisfy) the parity check $|G_j|$ disappear in basis 2. The right-hand side of the equivalence is the state generated by G' with the row G_j added to it, since the selective bit-complementing operation which was carried out is in fact the EXCLUSIVE-OR operation. By applying this argument successively to all the rows of G, the theorem is proved. ∎

Theorem 2.4 is more easily understood in terms of an example, which will now be provided. Consider the generator matrix

$$G_s = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\phi_1} & \mathrm{e}^{\mathrm{i}\phi_2} & \mathrm{e}^{\mathrm{i}\phi_3} \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \tag{2.5}$$

This equation is to be understood as a 3-column matrix of phase factors multiplying a 3-row matrix of 7-bit words. G_s generates the state

$$\begin{aligned} |G_s\rangle = {} & |0000000\rangle + \mathrm{e}^{\mathrm{i}\phi_3}|1010101\rangle + \mathrm{e}^{\mathrm{i}\phi_2}(|0110011\rangle + \mathrm{e}^{\mathrm{i}\phi_3}|1100110\rangle) \\ & + \mathrm{e}^{\mathrm{i}\phi_1}\{|0001111\rangle + \mathrm{e}^{\mathrm{i}\phi_3}|1011010\rangle + \mathrm{e}^{\mathrm{i}\phi_2}(|0111100\rangle + \mathrm{e}^{\mathrm{i}\phi_3}|1101001\rangle)\}. \end{aligned} \tag{2.6}$$

This code, appearing in basis 1, is well known in classical coding theory. It is called the simplex code, since the 8 words define the 8 vertices of a regular simplex in 7-dimensional space (see, for example, MacWilliams & Sloane 1977). In the quantum mechanical context, the code appears in $|G_s\rangle$ as a 7-particle entanglement containing three 4-particle interferences. Each phase ϕ_j is associated with a multiple-particle correlation among all those qubits which are selected by the jth row of G_s. Thus, by examining the matrix G_s (equation (2.5)), one sees that for this example case there are 3 correlations, each involving a different 4-member subset of the 7 qubits. These correlations can be revealed by measuring the qubits in basis 2, and calculating the relevent parity checks. I conjecture that such correlations satisfy Bell-type inequalities similar to those deduced by Mermin (1990), though a demonstration is beyond the scope of the present work. One may regard the linear codes as a generalization to many qubits of the 2-qubit 'Bell basis' $\{|00\rangle \pm |11\rangle, |01\rangle \pm |10\rangle\}$.

This concludes the discussion of multiple-particle interference *per se*. The concepts introduced make a natural introduction to the following sections, which will provide more information on these interferences, such as a method for their generation, while discussing other issues.

3. Error correction for qubits

The set of n qubits which we have been discussing may be considered to be a quantum computer (Deutsch 1985). In the course of a computation, entangled states involving many qubits at once are produced, and one of the fundamental problems of quantum computation is that such entanglements are highly sensitive to decoherence. 'Decoherence' refers (cf. Zurek 1993) to one class of departures of the quantum state of the computer from the state which it ought to have. We will not assume that decoherence is the only type of error process, however. Rather, we seek to correct the computer (or quantum channel) in the presence of completely general unknown departures from the state the computer ought to have (that produced purely by evolution under error-free computing operations)

An erroneous state of the whole computer will in general require correction methods operating on the whole computer at once in order to correct it. A method of this type was presented by Berthiame *et al.* (1994). Some types of error can be corrected through a bit-by-bit method, on the other hand, in which operations only on small subsets of the qubits are required. Shor (1995) proved that 9 qubits can be used to protect a single bit of quantum information against single errors, and Steane (1996) introduced a 7-qubit scheme, and a general method for correcting many errors, while discussing limitations to robust encoding of a single qubit. The approach adopted in the latter work is generalized in this paper to enable robust encoding of a whole computer. Also, the method of how to carry out error correction without disrupting the unitary evolution of the computation process is given.

The philosophy pursued in this paper is to adopt methods suggested by the classical theory of error correction, and then to consider afterwards what types of error can be corrected by such methods. It will be argued that realistic physical systems can be found which are subject primarily to the type of error whose correction we discuss. The general scenario is that of a computer undergoing its normal computing operations, and interspersed among these are error correction operations. The qubits are assumed to decohere and generally change their state in an unpredictable

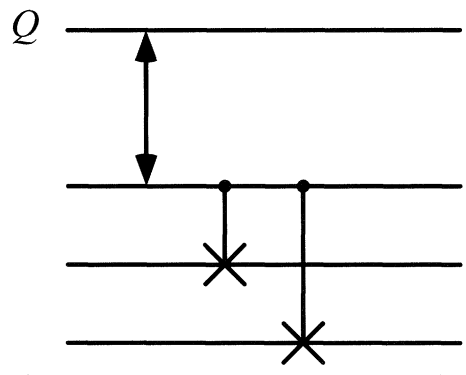

Figure 1. Encoding for simplest error correction scheme. Initially Q is the qubit to be encoded, and the three 'encoding' qubits are in the state $|\overline{000}\rangle$. Symbols: $\updownarrow$= state swapping; $\curlywedge$ = controlled not in basis 2.

manner. The word 'error' will sometimes refer to a rotation of a qubit through $\pi/2$ radians about a given axis in Hilbert space, which mimics the classical 'error' where a bit is complemented, but in general the word will refer to any departure of a qubit from the state it ought to be in.

A general error of a qubit can be considered as made up of phase error in basis 1 (a rotation around the axis of the Poincaré or Bloch sphere) plus an amplitude error in basis 1 (a rotation to different latitude on the sphere), plus a contribution due to entanglement with external systems, which, once those external degrees of freedom are traced over, causes the qubit's state to become mixed rather than pure. We will consider first the case of phase error alone, then a restricted class of external entanglements, and then more general errors.

(*a*) *Simplest case*

Let us begin by considering the case that the qubits randomly dephase but never entangle with the environment, and never flip in basis 1. This is the simplest non-trivial case, and is practically interesting because it may be possible to approximate it experimentally. In this simple situation, the only errors are phase errors in basis 1.

The errors are modelled by rotating the jth qubit using an operator

$$\begin{pmatrix} \mathrm{e}^{\mathrm{i}\epsilon\phi_j/2} & 0 \\ 0 & \mathrm{e}^{-\mathrm{i}\epsilon\phi_j/2} \end{pmatrix}, \tag{3.1}$$

where the matrix has been written in basis 1. The angles ϕ_j are independent, and ϵ is a parameter used to indicate the typical magnitude of the errors, $0 < \epsilon \leqslant 1$. If the single qubit state $a|0\rangle + b|1\rangle$ is subject to such errors, its density matrix becomes

$$\rho = \begin{pmatrix} |a|^2 & \alpha ab^* \\ \alpha^* a^* b & |b|^2 \end{pmatrix}, \tag{3.2}$$

$$\text{where } \alpha = \mathrm{e}^{\mathrm{i}\epsilon\phi}. \tag{3.3}$$

Since $\exp(\mathrm{i}\epsilon\phi) = 1 + O(\epsilon)$, the error in the off-diagonal elements is of order ϵ.

Phase errors in basis 1 can be corrected as follows. Each qubit in the quantum computer is 'encoded' using a set of three physical qubits, by the encoding method shown in figure 1. This set is then 'corrected' from time to time by the correction

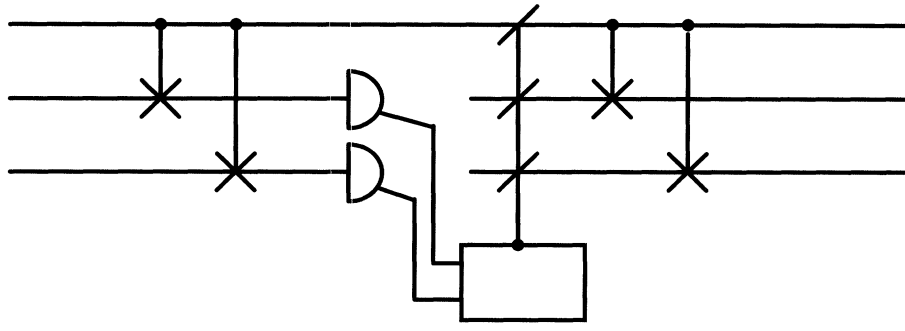

Figure 2. Simplest error correction scheme. All operations take place in basis 2. After two CNOT operations, the lower two qubits are measured in basis 2. The results are fed to a classical 'box' which then complements (NOT operation) one or more of the qubits, depending on the measurement results. The two final CNOT's reencode the state (see text).

method shown in figure 2. Computing operations, when required, can be carried out by a network equivalent to one which first 'decodes', then carries out the relevent operation, then encodes again. The decoding operation is the inverse of the encoding one.

To understand the error-correction scheme, one notes that it is based on the simplest classical error correction code, the $n = 3$ repetition code, operating in basis 2. This is because phase errors in basis 1 cause amplitude errors in basis 2, so we employ a scheme which corrects amplitude errors in basis 2. A general single-qubit state $a|0\rangle + b|1\rangle$ is encoded by two controlled not (CNOT) operations in basis 2,† acting on an initial state $(a|0\rangle + b|1\rangle) \otimes |\overline{00}\rangle$ (see figure 1). The state thus encoded using three qubits is

$$\begin{aligned} a(|000\rangle + |011\rangle + |101\rangle + |110\rangle) + b(|111\rangle + |100\rangle + |010\rangle + |001\rangle) \\ = (a+b)|\overline{000}\rangle + (a-b)|\overline{111}\rangle. \end{aligned} \tag{3.4}$$

Therefore the only 'legal' states are $|\overline{000}\rangle$ and $|\overline{111}\rangle$ or linear combinations of these.

The random phase errors in basis 1 cause departures from the subspace spanned by $|\overline{000}\rangle$ and $|\overline{111}\rangle$. As long as the errors are small, the component which was $|\overline{000}\rangle$ is likely to remain in the region of Hilbert space spanned by $\{|\overline{000}\rangle, |\overline{001}\rangle, |\overline{010}\rangle, |\overline{100}\rangle\}$ while the component which was $|\overline{111}\rangle$ is likely to remain in the region spanned by $\{|\overline{111}\rangle, |\overline{110}\rangle, |\overline{101}\rangle, |\overline{011}\rangle\}$. As long as only such 'single errors' occur, they can be corrected.

The error corrector shown in figure 2 works as follows. First, two CNOT operations carry out parity checks. The checks required are those given by the parity check matrix for the $\{000, 111\}$ repetition code:

$$H_{\mathrm{rep}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \tag{3.5}$$

After these checks, the 'control' qubit contains the state to be corrected, and the other two 'target' qubits (hereafter called parity qubits) contain the error syndrome. The two parity qubits containing the syndrome are now measured. The syndrome

† CNOT in basis 1 is $(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)$ where the first qubit is the control, the second is the target. CNOT in basis 2 (as here) is the operator having the same form, but with 0 and 1 replaced by $\bar{0}$ and $\bar{1}$.

indicates which qubit is to be complemented. That is, if the measurements give 11 then the NOT operation is carried out on the control qubit.‡ Whatever the result of the measurements, the parity qubits are reset to $|\overline{00}\rangle$. After this, the three qubits are in the decoded state. The final part of the error corrector reencodes the state.

The effect of the above transformations can easily be calculated. Once the encoding has been carried out, yielding the state given by equation (3.4), all three bits are subjected to errors given by the operator (3.1) with independent unknown ϕ_0, ϕ_1, ϕ_2. The resulting erroneous state is to be corrected. The two CNOT operations are applied, and measurements are modelled by projection operators. This yields 4 different density matrices for the 4 different measurement outcomes. The NOT operation is carried out on the relevent qubit or bits as indicated by the syndrome associated with each density matrix. The resulting four density matrices are added with weights given by the probabilities of obtaining them. Now we are at the stage just before the final reencoding. If instead of reencoding, we simply extract the density matrix of the control qubit, the result is equation (3.2) with

$$\begin{aligned}\alpha = \tfrac{1}{2}\{&\cos(\epsilon\phi_0) + \cos(\epsilon\phi_1) + \cos(\epsilon\phi_2)\\ &- \cos(\epsilon\phi_0)\cos(\epsilon\phi_1)\cos(\epsilon\phi_2)\\ &- i\sin(\epsilon\phi_0)\sin(\epsilon\phi_1)\sin(\epsilon\phi_2)\}.\end{aligned} \tag{3.6}$$

When only one of the three angles ϕ_j is non-zero (that is, one qubit is erroneous), the state is restored exactly, and when all three are non-zero, the error term is of order ϵ^3 instead of order ϵ, as a Taylor expansion of the trigonometric functions will show ($\alpha = 1 + O(\epsilon^3)$). The corresponding properties of classical single-error correction are that single errors are corrected exactly, and error probabilities of order p become of order p^2 after correction. Since in this case the qubit error term goes directly to $O(\epsilon^3)$ rather than $O(\epsilon^2)$, the correction is efficient. In the next section a case which mimics the classical behaviour more closely will be discussed.

It has been assumed throughout that the process of encoding and correcting does not itself introduce more errors than it corrects.

The discussion so far only demonstrates a modest correction ability. However, the concepts can be generalized, enabling the limitations of the method to be derived. We turn to this in later sections. The main result so far is to show that unitary evolution of a qubit can be preserved, while information about error processes is nevertheless gathered and used to correct the qubit. Next it will be shown that the general methods discussed in this paper are not limited to the correction of unitary errors, but can enable the quantum computer to recover from relaxation caused by erroneous coupling to its environment.

(*b*) *Simplest purity amplification*

The single error correction in basis 2 discussed in the previous section with regard to unitary phase errors in basis 1 is also sufficient to correct a restricted class of relaxation errors (i.e. errors caused by coupling to external systems). The restricted class is relaxation which does not cause amplitude errors in basis 1. One can model such relaxation either as a decay in the off-diagonal density matrix elements of each qubit in basis 1, or as an entanglement with the environment introduced by operators

‡ NOT in basis 1 is the operator $|0\rangle < 1| + |1\rangle < 0|$. NOT in basis 2 (as here) is $|\overline{0}\rangle < \overline{1}| + |\overline{1}\rangle < \overline{0}|$.

of the type

$$W_j = \begin{matrix} |0\rangle_j \otimes |\psi_{1j}\rangle \\ |0\rangle_j \otimes |\psi_{2j}\rangle \\ |1\rangle_j \otimes |\psi_{1j}\rangle \\ |1\rangle_j \otimes |\psi_{2j}\rangle \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1-\epsilon_j & \sqrt{2\epsilon_j - \epsilon_j^2} \\ 0 & 0 & -\sqrt{2\epsilon_j - \epsilon_j^2} & 1-\epsilon_j \end{pmatrix}. \tag{3.7}$$

Here, $|\psi_{1j}\rangle$ and $|\psi_{2j}\rangle$ are orthogonal states of the environment, and the product states on the left of the operator matrix indicate the basis in which the matrix is written. The (real) parameter ϵ_j, bounded by $0 < \epsilon_j \leqslant 1$, indicates the strength of the entanglement with the environment. The entanglement can be imagined as an imperfect ($\epsilon < 1$) or perfect ($\epsilon = 1$) measurement of the qubit in basis 1. Such entanglements, when perfect, have the effect of making the 'interference phase' between the two parts $|0\rangle$ and $|1\rangle$ of qubit's state unobservable, as a straightforward analysis will show. No amplitude error is introduced in basis 1, which is the clue that the 'simplest possible' error-correction procedure introduced in the previous section will be sufficient to correct errors having this form.

The effect of the entanglement W_j on a single qubit is calculated by operating W_j on the joint qubit–environment state $(a|0\rangle + b|1\rangle) \otimes |\psi_1\rangle$, and then obtaining the reduced density matrix of the qubit by tracing over the environment variables. The result is a density matrix as in equation (3.2), with

$$\alpha = 1 - \epsilon. \tag{3.8}$$

This is clearly a mixed state when $\epsilon > 0$, and the error term is of $O(\epsilon)$.

When we examine the density matrix in basis 2, this error appears partly as an amplitude error, and it can be corrected by the encoding and correcting procedure described in the previous section (figures 1 and 2). To calculate the effects, first the general single-qubit state $(a|0\rangle + b|1\rangle)$ is encoded using three qubits, then each of the three undergoes entanglement with the environment, described by three operators W_0, W_1, W_2 defined by equation (3.7). The overall state then involves 8 different environment states, associated with 8 different 3-qubit states. The error correction procedure is carried out next. In the calculation, it appears as a set of eight independent corrections on each of the eight 3-qubit states. The final 'corrected' 3-qubit density matrix is then taken to be the weighted sum of the eight 3-qubit density matrices associated with different states of the environment. The density matrix of the control qubit is extracted, yielding the form (3.2) with

$$\alpha = 1 - \tfrac{1}{2}(\epsilon_0\epsilon_1 + \epsilon_0\epsilon_2 + \epsilon_1\epsilon_2) + \tfrac{1}{2}\epsilon_0\epsilon_1\epsilon_2. \tag{3.9}$$

This result shows that when only a single qubit decoheres (i.e. only one of the entanglement terms ϵ_j is non-zero), the state is corrected exactly ($\alpha = 1$), and when all three undergo errors, the error term is of $O(\epsilon^2)$ instead of $O(\epsilon)$. The corresponding properties of classical single-error correction are that single errors are corrected exactly, and error probabilities of order p become of order p^2 after correction.

The fact that the corrected density matrix is nearer to 'pure state' conditions than the original density matrix (when $\epsilon = \epsilon_j < 1$), is an example of a general phenomenon called 'quantum privacy amplification' in the context of a quantum communication channel (Bennett *et al.* 1995; Deutsch *et al.* 1996), and which will be referred to here as 'purity amplification'. The ability to implement purity amplification is an

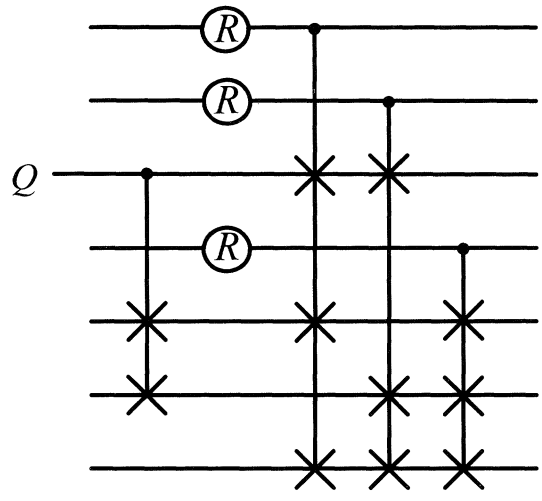

Figure 3. Encoder for the simplest scheme enabling single error correction in both bases. The multiple CNOT symbols mean successive CNOT operations carried out between the single control qubit and each of the target qubits. The initial state is $|00Q0000\rangle$. The first two CNOT operations prepare for the generation of a superposition of the simplex code and its complement. The rest generates the code from this preparatory state. The symbol Ⓡ means the rotation $|0\rangle \rightarrow |\overline{0}\rangle$, $|1\rangle \rightarrow |\overline{1}\rangle$.

important part of the general problem of error correction in quantum communication channels and computers. This section has shown that the approach to error correction adopted in this paper is capable of handling purity amplification. Indeed, the 'quantum privacy amplification' protocol described by Deutsch *et al.* (1996) can be understood as an implementation of single-error *detection* in basis 1 and basis 2 simultaneously, by means of a single parity check in each basis. The fact that it is a detection rather than correction scheme explains why non-useful pairs of bits have to be thrown away.

(*c*) *General single error correction*

Suppose now the type of error is completely general—there is an arbitrary change in the state of a qubit, including possible relaxation. To correct this, the method is to implement single error correction in both bases simultaneously. For this, the encoding used in the previous section is not sufficient, since there single errors in basis 1 could not be corrected. To understand the encoding requirements, the concept of *minimum distance*, introduced by Hamming (1950), is employed. The Hamming distance between two words is equal to the number of bits which must be complemented in order to convert one word into the other. The minimum distance d of a code is the minimum Hamming distance between any two words in the code. A code of minimum distance $d > 2x$ is necessary if x errors are to be corrected, since only if fewer than $d/2$ errors occur can the codeword which gave rise to the erroneous word can be identified unambiguously as the only codeword within distance $d/2$ of the erroneous word. In what follows, the standard notation $[n, k, d]$ will be employed to refer to a linear code using n bits, having 2^k codewords and minimum distance d.

To correct for a general single error, we require an encoding allowing minimum distance 3 in both basis 1 and basis 2. A method to do this was presented by Steane (1996), as follows. We seek a code C having the following properties: its dual code

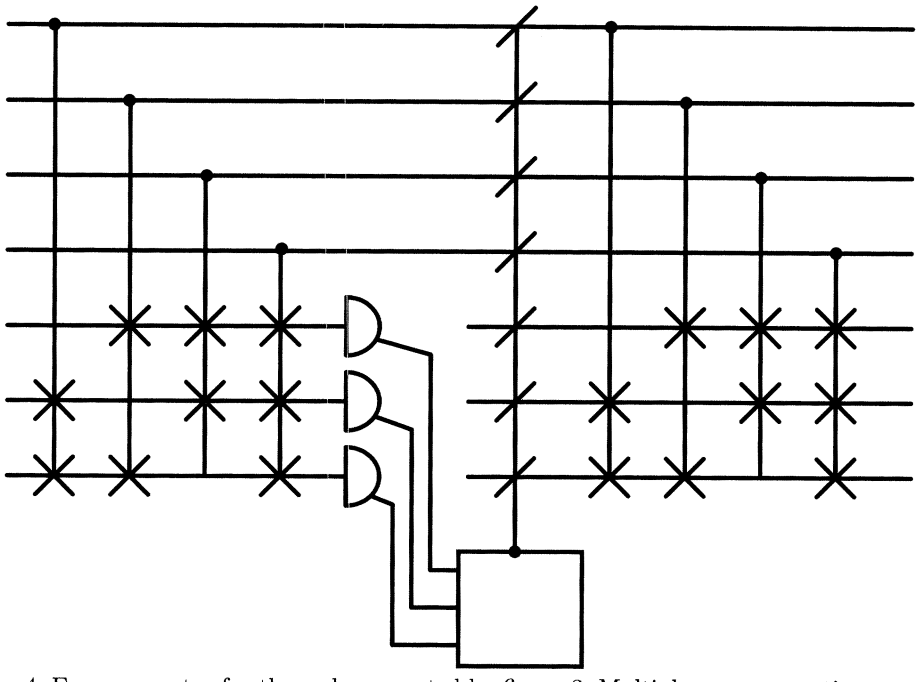

Figure 4. Error corrector for the code generated by figure 3. Multiple CNOT operations perform parity checks. The lower three qubits are measured, and the results used to determine which qubits undergo a NOT operation. The scheme is first applied in basis 1, then in basis 2 (see text).

$C^{\perp}$ has minimum distance 3, and it is itself a subcode of a of code C^{+} of minimum distance 3. The reasoning behind this is best demonstrated by means of an example.

The $[7,3,4]$ simplex code presented in § 2 *b* has the properties required. Its dual code is the $[7,4,3]$ Hamming code which has minimum distance 3, and it is a subcode of the $[7,4,3]$ punctured Reed–Muller code, also of minimum distance 3. $n = 7$ is the smallest number of bits for which a code can be found with these properties. The encoding and correcting procedure is shown in figures 3 and 4, and explained as follows.

The encoding method is based on the generator matrix of the $[7,3,4]$ simplex code, given by equation (2.5) with $\phi_1, \phi_2, \phi_3 = 0$. The simplex code thus generated will be called $|C\rangle$. It is the state $|G_s\rangle$ shown in equation (2.6) with all phase angles set to zero. The essential idea is that a qubit state $|0\rangle$ is encoded as $|C\rangle$, while a qubit state $|1\rangle$ is encoded as $|\neg C\rangle$, which is $|C\rangle$ with the NOT operation carried out on all the qubits, i.e. the coset $|C \oplus 1111111\rangle$. It is easy to deduce that when the qubit Q to be encoded is in the state $|0\rangle$, the encoder shown in figure 3 places the 7 qubits in the state $|C\rangle$. To see that $|1\rangle$ becomes encoded as $|\neg C\rangle$, consider the parity check matrix of $|C\rangle$:

$$H_C = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{3.10}$$

Now, $|\neg C\rangle$ fails all those parity checks for which there is an odd number of 1s in the relevent row of H_s, and passes the others. Hence, the operations which generate

$|C\rangle$ when starting from $|0000000\rangle$, will generate $|\neg C\rangle$ when starting from $|0010110\rangle$, since the complemented qubits ensure that the final state will pass and fail the checks in H_C in the way appropriate for $|\neg C\rangle$. This initial complementing of qubits is the job of the first two CNOT operations in the encoder. The encoder therefore encodes a general single qubit state $(a|0\rangle + b|1\rangle)$ as $(a|C\rangle + b|\neg C\rangle)$.

Now, $|C\rangle$ and $|\neg C\rangle$ are subcodes (strictly, cosets) of the $[7,4,3]$ punctured Reed–Muller code C^+ whose parity check matrix is

$$H_{C+} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}. \tag{3.11}$$

All legal encoded states satisfy this parity check matrix, and this is the basis of the corrector shown in figure 4. The operation of the corrector is similar to that of the corrector presented in the previous section (figure 2). Multiple CNOT operations are used to carry out parity checks, the parity qubits are measured, and the state corrected by means of NOT operations on qubits identified by the measured syndrome. Finally, the state is reencoded.

So far, error correction has been carried out in basis 1. However, the coding was carefully selected in such a way that only words in the $[7,4,3]$ Hamming code $C^\perp$ should appear in basis 2. Therefore, error correction can also be carried out in basis 2. The corrector is based on the parity check matrix of the $[7,4,3]$ Hamming code, which is equal to the generator matrix of its dual, the matrix G_C given in equation (2.5). Now, it so happens that the $[7,4,3]$ Hamming code is the same as the $[7,4,3]$ punctured Reed–Muller code (this is not always true for higher order codes), as can be seen by the fact that G_C and H_{C+} are equal (one can be converted to the other by linearly combining rows). Therefore, the corrector in basis 2 is once again given by figure 4, only now all the operations are carried out in basis 2.

The correction scheme described will tend to keep the encoded state confined to the region of Hilbert space spanned by the two state vectors $\{|C\rangle, |\neg C\rangle\}$. This is a two-dimensional subspace within the 128-dimensional total Hilbert space. The subspace is also spanned by the state vectors $\{|\overline{H,e}\rangle, |\overline{H,o}\rangle\}$ defined by the even and odd parity subcodes of the $[7,4,3]$ Hamming code in basis 2, since theorem 2.4 implies that $|C\rangle + |\neg C\rangle \equiv |\overline{H,e}\rangle$ and $|C\rangle - |\neg C\rangle \equiv |\overline{H,o}\rangle$, up to a normalization factor. If an arbitrary single-qubit state is encoded as $(a|C\rangle + b|\neg C\rangle)$, and then any one (but only one) of the 7 qubits is allowed to change state and entangle with the environment in an arbitrary manner, the error corrector described in this section will return the 7 qubits exactly to the error-free state $(a|C\rangle + b|\neg C\rangle)$. This will be proved below as part of the more general theorem 3.3. If more than one qubit is allowed to undergo errors, then error terms which would be of order ϵ in the density matrix of an uncorrected qubit become of order ϵ^2 or higher when encoding and correction is employed.

(*d*) *Multiple correction of multiple qubits*

The previous sections have introduced almost sufficient insights to enable the general problem of multiple error correction of many qubits to be addressed. The final ingredient is theorem 3.1 below. Before it is presented, we remark that just as in classical information theory, it is necessary to distinguish between the amount of information k and the number of bits n used in a $[n,k,d]$ code, it will be necessary here

to distinguish between the number K of independent quantum bits of information we wish to keep free of errors, and the number n of qubits used to do this. Thus, in § 3 *a* a single qubit was encoded, $K = 1$, by means of $n = 3$ encoding qubits, and in § 3 *c* a single qubit $K = 1$ was encoded by means of $n = 7$ encoding qubits.

Theorem 3.1. *To encode K qubits with minimum distance d_1 in one basis, and minimum distance d_2 in the other, it is sufficient to find a linear code C^{+K} of minimum distance d_1, whose Kth order subcode C is the dual of a distance d_2 code.*

Corollary 3.2. *Finding such a code is sufficient not only to demonstrate that the encoding is possible, but also to make self-evident the physical procedures for encoding and correction.*

A Kth order subcode of C^{+K} is a code obtained by adding K rows to the parity check matrix of C^{+K}.

Proof. The general insight is that whereas in classical theory, information is encoded using different *words* of a code, in the quantum mechanical case, information is encoded using different *cosets* of a code. Thus in § 3 *c*, cosets of the $[7, 4, 3]$ punctured Reed–Muller code, were used, and in § 3 *a*, the even parity and odd parity codes in basis 1 were cosets of the $[n, n, 1]$ code of all possible words.

To encode K qubits, we require 2^K cosets. If these are all non-overlapping cosets in a distance d_1 code, then clearly they are all separated from one another by at least d_1. That is, all words in one coset are at least d_1 from all words in another coset. We can ensure the cosets do not overlap by defining them as follows. K new rows are added to the parity check matrix of C^{+K}. The new rows are linearly independent of each other and of all the other rows. (If this is not possible then n must be increased and the argument restarted). Each of the K new parity checks can either be satisfied or not satisfied. This allows 2^K different possibilities, each of which produces a coset which has no words in common with any of the other cosets. Hence the cosets are non-overlapping.

Suppose the first coset C is a code having a dual $C^{\perp}$. To obtain one of the other $2^K - 1$ cosets from C, it is sufficient to complement in basis 1 whichever parity qubits implement a parity check which C satisfies but the new coset does not. The effect in the other basis is to change the sign of some of the words (by theorem 2.2). (Equivalently, it is sufficient to change the sign of the relevent rows of the parity check matrix in basis 1, which is the generator matrix in basis 2, by theorem 2.4.) Therefore, each coset in basis 1 produces the words of $C^{\perp}$ in basis 2, with signs depending on the coset. Hence, for any superposition of the cosets in basis 1, all words appearing in basis 2 are in the code $C^{\perp}$. Therefore, if we require minimum distance d_2 in basis 2, it is sufficient that $C^{\perp}$ should be a distance d_2 code, and the theorem is proved. ■

The coding method of theorem 3.1 uses a 2^K-dimensional subspace to store the quantum information, within a total Hilbert space of dimension 2^n. The subspace is spanned by the 2^K cosets of C^{+K} in basis 1, and by 2^K cosets of $C^{\perp}$ in basis 2. The encoding and correcting operations are deduced directly from the parity check matrices of the relevant linear codes, in the manner illustrated by figures 1 to 4. An alternative approach to error correction is illustrated by figure 5. To implement correction in basis 1 (basis 2), a set of $n - k_1$ (respectively $n - k_2$) ancillary qubits is introduced, and the error syndrome is stored into this ancilla by means of multiple

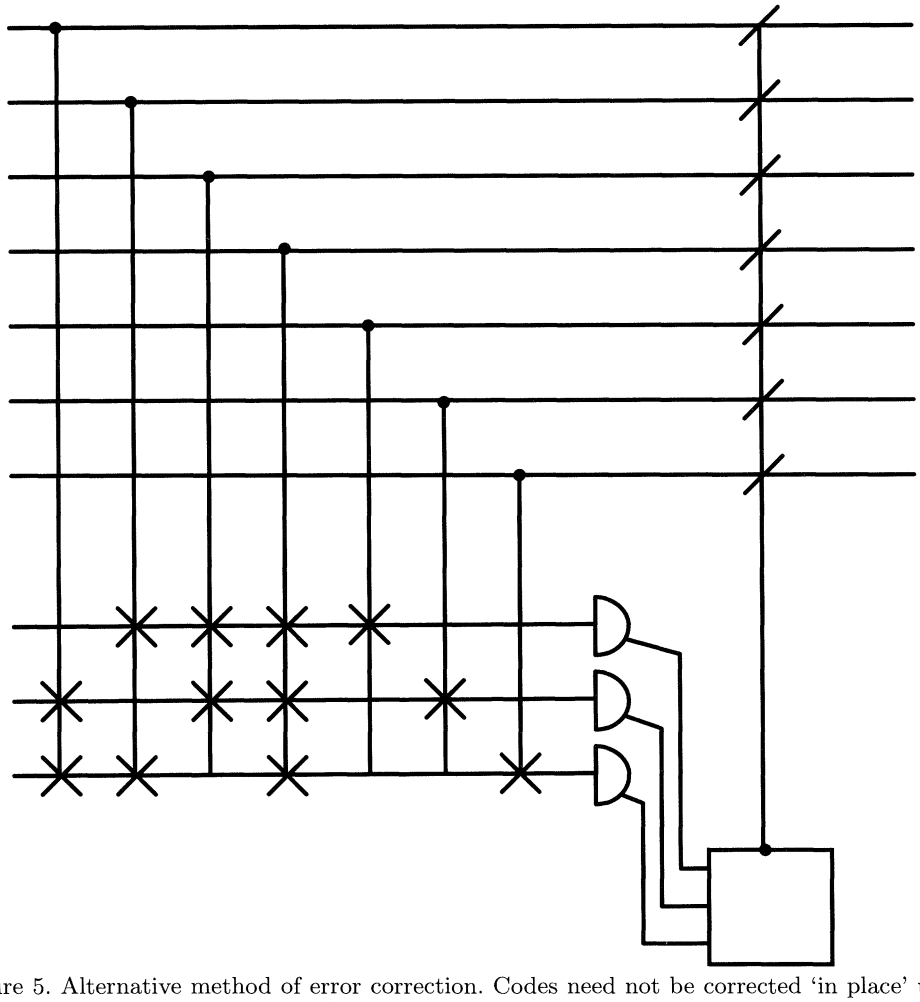

Figure 5. Alternative method of error correction. Codes need not be corrected 'in place' using the qubits of the computer itself (as in the previous figures). It may be more convenient to establish the error syndrome using a set of ancillary qubits. The example shown here carries out the same correction as the corrector of figure 4.

CNOT operations. The operations required are exactly those specified by the parity check matrix of C^{+K} (respectively $C^{\perp}$), which proves the corollary to theorem 3.1. The ancilla is measured (in the relevent basis), and the result used to calculate which qubits in the quantum computer are to undergo a NOT operation.

(*e*) *Error correction in two bases is sufficient*

This section is dedicated to the proof of the following theorem.

Theorem 3.3. *Error correction in basis 1 followed by error correction in basis 2 is sufficient to restore the quantum computer after arbitrary errors of a small enough subset of its qubits. Specifically, if x qubits undergo errors, then correction is successful if at least x errors can be corrected in both basis 1 and basis 2.*

This theorem shows that the correction methods described in this paper are not limited to the correction of simple 'qubit complementing' errors, but can handle any

error process, as long as it only affects a subset of the n qubits in the computer. To keep a clear distinction, the word *flip* is reserved in this section to refer to error processes of the form either $|0\rangle \leftrightarrow |1\rangle$ ('a flip in basis 1') or $|\overline{0}\rangle \leftrightarrow |\overline{1}\rangle$ ('a flip in basis 2'). Completely general erroneous changes in the state of a qubit, including entanglement with the environment, will be referred to as *defection*†.

The following notations will be used.

$$\begin{aligned}
|Ci\rangle &= \text{the } i\text{th coset of } |C^{+K}\rangle.\\
|Ci_j\rangle &= \text{the } j\text{th coset of } |Ci\rangle.\\
|Ci_j/{}^1S_k\rangle &= |Ci_j\rangle \text{ subject to flips in basis 1 whose error syndrome is } S_k\\
|Ci/{}^2S_l\rangle &= |Ci\rangle \text{ subject to flips in basis 2 whose error syndrome is } S_l\\
|e_n\rangle &= \text{ a state of the environment.}
\end{aligned}$$

As an example of the above, consider the state $|Ci\rangle = |0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle$. One pair of possible cosets is $|Ci_0\rangle = |0000\rangle + |0011\rangle$ and $|Ci_1\rangle = |1100\rangle + |1111\rangle$. Suppose the error syndrome for the case of no errors is S_0, then $|Ci_j/{}^1S_0\rangle = |Ci_j\rangle$. If a single error in the last bit produces the syndrome S_1, then $|Ci_0/{}^1S_1\rangle = |0001\rangle + |0010\rangle$; $|Ci_1/{}^1S_1\rangle = |1101\rangle + |1110\rangle$; $|Ci/{}^2S_1\rangle = |0000\rangle - |0011\rangle + |1100\rangle - |1111\rangle$.

In what follows, we will require the following result:

$$|Ci_j\rangle = \sum_{l=0}^{2^x-1} |Ci/{}^2S_l\rangle(-1)^{\mathrm{wt}(j\cdot l)} \tag{3.12}$$

where the notation $\mathrm{wt}(j \cdot l)$ means the Hamming weight‡ of $j \cdot l$, and the dot indicates the bitwise AND operation carried out between j and l. The result holds for a particular type of coset Ci_j, which will be identified shortly.

It is obvious that a code can be written as the sum of its cosets: $|Ci\rangle = \sum_j |Ci_j\rangle$. The content of (3.12) is the inverse result, that a coset $|Ci_j\rangle$ can be written as a sum of (erroneous) codes. The flips in basis 2 cause sign changes amongst the basis 1 words of $|Ci\rangle$ in such a way that when the sum in equation (3.12) is carried out, all words in $|Ci\rangle$ which do not belong to $|Ci_j\rangle$ cancel, so the result is $|Ci_j\rangle$.

Proof of equation (3.12). If Ci_j is an xth order coset of Ci, then the parity check matrix for Ci_j consists of the parity check matrix of Ci, plus x extra rows. We consider the case that each of these extra rows contains all zeros apart from a single 1. For example, for $x = 3$, $n = 10$, the 8 cosets might be counted by the values of the fourth, sixth and tenth qubits in basis 1, in which case the parity check matrix in basis 1 is

$$|Ci_j\rangle \rightarrow \left(\begin{array}{c} H_i \\ \hline (-1)^{\mathrm{wt}(j\cdot 001)}\,0000000001 \\ (-1)^{\mathrm{wt}(j\cdot 010)}\,0000010000 \\ (-1)^{\mathrm{wt}(j\cdot 100)}\,0001000000 \end{array}\right), \tag{3.13}$$

† Random unitary changes (rotations) of a qubit are caused by defects in the quantum computer; to entangle randomly with the environment is to form a treacherous alliance with an enemy of successful quantum computation.

‡ The Hamming weight of a bit string x is the number of 1s in x.

where H_i is the parity check matrix of $|Ci\rangle$. The jth coset passes or fails these extra parity checks according as the bits of the binary value of j are zero or one. This pass/fail property is indicated by the sign (power of -1) in front of each row of the matrix.¶ Thus, Ci_0 is the set of words of Ci for which the 4th, 6th and 10th bits are zero, Ci_5 is the set of words of Ci for which the 4th and 10th bits are one, and the 6th is zero, since decimal 5 is binary 101, and so on.

In general, the type of coset for which equation (3.12) holds is one consisting of all words in $|Ci\rangle$ for which a chosen set of x qubits has the value j in basis 1.

Since the matrix in equation (3.13) is the parity check matrix of $|Ci_j\rangle$ in basis 1, it is the generator matrix in basis 2 of the same quantum state (theorem 2.4). But, such a generator matrix will generate the code Ci plus $2^x - 1$ erroneous copies of Ci, where a given copy will have flips of just the bits selected by those extra rows of the generator matrix which were used to generate that copy. Hence, equation (3.12) is proved.

We now pass on to the question of general errors and their correction. A general defection of a single qubit can be written

$$\left.\begin{aligned} |0\rangle|e_0\rangle &\rightarrow |0\rangle|e_1\rangle + |1\rangle|e_2\rangle, \\ |1\rangle|e_0\rangle &\rightarrow |0\rangle|e_3\rangle + |1\rangle|e_4\rangle, \end{aligned}\right\} \tag{3.14}$$

where no assumptions are made about the environment states $|e_i\rangle$—they may or may not be orthogonal, and they may include arbitrary (complex) coefficients (they are not normalized). A general defection of x qubits is

$$|j\rangle|e_0\rangle \rightarrow \sum_{k=0}^{2^x-1} |j/\,{}^1S_k\rangle|e_{jk}\rangle, \tag{3.15}$$

where $|j\rangle$ is any one of the 2^x possible x-qubit words.

Now, suppose that in some state $|Ci\rangle$, a subset of the qubits defect. The subset contains x qubits positioned anywhere among the n qubits of the total system. A state $|Ci\rangle$ (i.e. before defection) can be written $|Ci\rangle = \sum_{j=0}^{2^x-1} |Ci_j\rangle$ where the jth coset consists of all words in $|Ci\rangle$ for which the subset of x bits has the value j in basis 1. A general defection among the x defecting qubits is the process indicated by equation (3.15), with the $n - x$ unchanged qubits acting as spectators, and with j indicating the initial values of the decohering qubits. Therefore, the effect of defection on $|Ci_j\rangle$ is

$$|Ci_j\rangle|e_0\rangle \rightarrow \sum_{k=0}^{2^x-1} |Ci_j/\,{}^1S_k\rangle|e_{jk}\rangle. \tag{3.16}$$

Note that the state of the environment after defection is independent of i in this equation. This is because we selected the cosets $|Ci_j\rangle$ in such a way as to bring exactly this property about. The environment does not 'care' about the state of the spectator qubits, so its final state is not sensitive to which code $|Ci\rangle$ gave rise to the coset $|Ci_j\rangle$.

We now have enough results to prove theorem 3.3.

Proof. Using the encoding method of theorem 3.1, a general state of a computer

¶ This sign is an example of the phase factor introduced in § 2 *b* to generalize the use of such matrices in the quantum mechanical as opposed to classical context (cf. theorem 2.4).

before defection can be written

$$|QC\rangle = \sum_{i=0}^{2^K-1} c_i |Ci\rangle. \tag{3.17}$$

Expanding each state $|Ci\rangle$ as a set of cosets, this is

$$|QC\rangle = \sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} |Ci_j\rangle, \tag{3.18}$$

where we choose the set of cosets identified by the 2^x possible values in basis 1 of the x qubits which now defect. Using equation (3.16), the effect of defection is

$$|QC\rangle|e_0\rangle \to \sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} \sum_{k=0}^{2^x-1} |Ci_j/\,{}^1S_k\rangle|e_{jk}\rangle. \tag{3.19}$$

Now apply error correction in basis 1. As long as $x < d_1/2$, this has the result that

$$|Ci_j/\,{}^1S_k\rangle|{}^1m_0\rangle \to |Ci_j\rangle|{}^1m_k\rangle, \tag{3.20}$$

where $|{}^1m_k\rangle$ indicates a state of the measuring apparatus used for correction (cf. figure 5). Therefore the total state of the quantum computer, environment and measuring apparatus becomes

$$\sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} \sum_{k=0}^{2^x-1} |Ci_j\rangle|{}^1m_k\rangle|e_{jk}\rangle \tag{3.21}$$

$$= \sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} |Ci_j\rangle \left(\sum_{k=0}^{2^x-1} |{}^1m_k, e_{jk}\rangle \right). \tag{3.22}$$

Note that the error correction has corrected all 2^x cosets $|Ci_j\rangle$ in parallel. The correction is not yet complete because each coset is entangled with a different state of the environment.

Using equation (3.12), the total state given by (3.22) can be written

$$\sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} \sum_{l=0}^{2^x-1} |Ci/\,{}^2S_l\rangle (-1)^{\mathrm{wt}(j\cdot l)} \left(\sum_{k=0}^{2^x-1} |{}^1m_k, e_{jk}\rangle \right). \tag{3.23}$$

Now apply error correction in basis 2. As long as $x < d_2/2$, this has the result that

$$|Ci/\,{}^2S_l\rangle|{}^2m_0\rangle \to |Ci\rangle|{}^2m_l\rangle, \tag{3.24}$$

where $|{}^2m_l\rangle$ indicates a state of the measuring apparatus using for correction in basis 2. Therefore the total state of the quantum computer, environment and both measuring apparati becomes

$$\sum_{i=0}^{2^K-1} c_i \sum_{j=0}^{2^x-1} \sum_{l=0}^{2^x-1} |Ci\rangle|{}^2m_l\rangle (-1)^{\mathrm{wt}(j\cdot l)} \left(\sum_{k=0}^{2^x-1} |{}^1m_k, e_{jk}\rangle \right) \tag{3.25}$$

$$= \left(\sum_{i=0}^{2^K-1} c_i |Ci\rangle \right) \sum_{j=0}^{2^x-1} \sum_{l=0}^{2^x-1} |{}^2m_l\rangle (-1)^{\mathrm{wt}(j\cdot l)} \left(\sum_{k=0}^{2^x-1} |{}^1m_k, e_{jk}\rangle \right) \tag{3.26}$$

$$= |QC\rangle \otimes |{}^2m, {}^1m, e\rangle. \tag{3.27}$$

Hence, the quantum computer becomes completely disentangled from its environment, and is returned to its initial state. Therefore, error correction in basis 1 and basis 2 is sufficient to restore the quantum computer after arbitrary errors of $x < d_1/2$, $d_2/2$ qubits, and theorem 3.3 is proved. ■

4. Error rate limitations

We now turn to the question of whether errors can be supressed sufficiently to enable useful computations to be carried out on a quantum computer. This may also be regarded as a problem of communication over a noisy quantum channel. The method is to establish the limitations implicit in the coding method described by theorems 3.1 and 3.3.

The fundamental problem of the theory of classical error correcting codes is to find codes of length n (i.e. n is the length of the words) and minimum distance d which contain the maximum possible number of codewords. Let this maximum possible number of codewords be $A(n, d)$. Although $A(n, d)$ is not known in general, a number of upper and lower bounds have been established. In what follows, we will make use of two simple bounds. The first is the Hamming or sphere-packing bound introduced by Hamming 1950. In the limit of large n, it takes the form

$$\frac{\log_2(A(n,d))}{n} \leqslant \left(1 - H\left(\frac{d}{2n}\right)\right), (1-\zeta), \tag{4.1}$$

where $\zeta \to 0$ as $n \to \infty$, and $H(x)$ is the entropy function

$$H(x) \equiv x \log_2 \frac{1}{x} + (1-x) \log_2 \frac{1}{1-x}. \tag{4.2}$$

There are no codes of length n and distance d which have more words than this upper limit, and usually the upper bound itself cannot be achieved. This is the 'bad news'. The good news is that useful codes do exist. The Gilbert–Varshamov bound (Gilbert 1952; Varshamov 1957; see also MacWilliams & Sloane 1977) is a sufficient but not necessary condition for the existence of a $[n, k, d]$ code. In the limit of large n, it takes the form

$$k/n \geqslant (1 - H(d/n))(1-\zeta), \tag{4.3}$$

where $\zeta \to 0$ as $n \to \infty$. It can be shown (MacWilliams & Sloane 1977) that there exists an infinite sequence of $[n, k, d]$ linear codes satisfying inequality (4.3) with $d/n \geqslant \delta$ if $0 \leqslant \delta < 1/2$.

Theorem 3.1 states that to encode K qubits with minimum distances d_1 and d_2 in bases 1 and 2, we require codes C^{+K}, C, $C^{\perp}$ related as follows:

$$[n, x+K, d_1] \overset{\text{subcode}}{\longrightarrow} [n, x, y] \overset{\text{dual}}{\longleftrightarrow} [n, n-x, d_2]. \tag{4.4}$$

This implies that the codes $C^{+K} = [n, k_1, d_1]$ and $C^{\perp} = [n, k_2, d_2]$ have sizes k_1, k_2 related by

$$k_1 + k_2 = n + K. \tag{4.5}$$

Since all codes satisfy the Hamming bound (4.1), both C^{+K} and $C^{\perp}$ do so. Substituting in equation (4.5), this implies

$$K/n \leqslant 1 - H(d_1/2n) - H(d_2/2n), \tag{4.6}$$

where the factors $(1-\zeta)$ have been dropped for clarity (this will not affect the argument).

Now, provided the parameters $[n, k_1, d_1]$ satisfy the Gilbert–Varshamov (GV) bound (4.3), then it is certainly possible to find a code C^{+K} having size k_1 and minimum distance d_1. What is the condition that such a code will have associated with it a Kth order subcode C whose dual $C^{\perp}$ has minimum distance d_2? I conjecture that it is sufficient that $C^{\perp}$ also satisfy the GV bound. I have not been able to prove this, but the conjecture seems reasonable since it is known that there is an infinite series of self-dual codes which satisfy (4.3). Therefore in the set

$$\{C^{+K} \leftrightarrow C \leftrightarrow C^{\perp}\} = \{[n, n/2+K, d_1] \leftrightarrow [n, n/2, d_2] \leftrightarrow [n, n/2, d_2]\},$$

both C and $C^{\perp}$ can satisfy the GV bound simultaneously. In passing from C to C^{+K} in this case, one does not expect the minimum distance to fall especially rapidly, so it is reasonable to suppose that C^{+K} can also be found satisfying the GV bound.

NB. Since submitting this manuscript I have learnt that Calderbank & Shor (1996) have proved the above conjecture for the case $d_1 = d_2$, by proving that the GV bound is a sufficient condition for the existence of a *weakly* self-dual code, i.e. one containing its dual. These authors have reported an independent derivation of the most important result (theorems 3.1 and 3.3 combined) of the present work.

It will be assumed, then, that a sufficient condition for K qubits to be encoded with minimum distances d_1, d_2, is that C^{+K} and $C^{\perp}$ both satisfy the GV bound. Substituting this bound (4.3) in equation (4.5) leads to

$$K/n \geqslant 1 - H(d_1/n) - H(d_2/n). \tag{4.7}$$

Inequalities (4.6) and (4.7) are closely related to Shannon's main theorem in the classical regime. The classical regime corresponds to the limit $d_2/n \to 0$, $d_1 = d$, in which case we obtain $1 - H(d/2n) \geqslant K/n \geqslant 1 - H(d/n)$. The context in which we have been working throughout corresponds classically to a binary symmetric channel, having capacity $C(p) = 1 - H(p)$ where p is the error probability. Shannon's theorem states that the rate K/n can be arbitrarily close to capacity, while allowing error-free transmission. This implies $K/n \sim 1 - H(p)$ is possible for a code of average distance $\bar{d} = 2np(1+\zeta)$ with ζ arbitrarily close to zero. The averaging employed here involves various technicalities which are discussed in standard texts; a good introduction is given by Hamming (1986). For our present purposes, we note simply that Shannon's theorem gives $K/n \sim 1 - H(\bar{d}/2n)$. Comparing this with inequality (4.6), one sees that classically the Hamming bound gives a good guide to the limits of what is possible for an average distance between codewords, even though the *minimum* distance cannot not reach the upper limit of the Hamming bound, and indeed more restrictive bounds are known (see MacWilliams & Sloane 1977). This suggests that the Hamming bound is a useful indicator in general, i.e. that codes which 'approach' it in an average way do exist.

Returning to the quantum regime, let us consider for simplicity the case $d_1 = d_2 = d$. This is the type of coding one would choose if the probabilities of errors in bases 1 and 2 were equal. If they are not equal, one can always choose d sufficiently large to allow correction in the most error-prone basis, then it will also be more than sufficient for correction in the other basis. For $d_1 = d_2 = d$, inequalities (4.6) and (4.7) give

$$H(d/n) \geqslant \tfrac{1}{2}(1 - K/n) \geqslant H(d/2n), \tag{4.8}$$

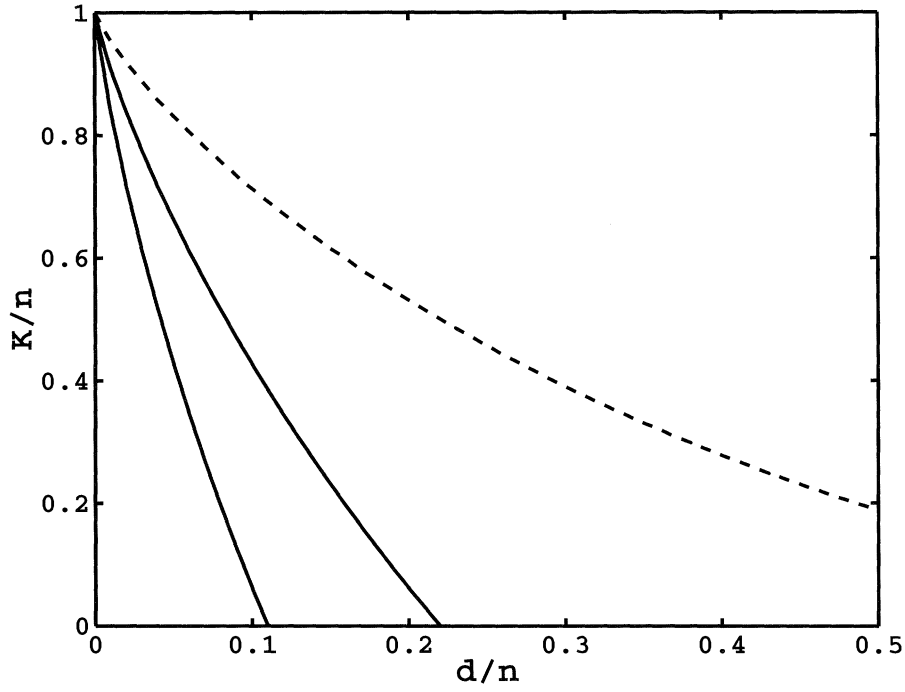

Figure 6. Asymptotic bounds, in the limit of large n, on the rate of a quantum code. Full curves: inequalities (4.8); dashed curve: Hamming bound for a classical code (i.e. quantum case with phase errors only). The upper full curve is an upper (Hamming) bound for the codes discussed in the text, the lower full curve is a sufficient (Gilbert–Varshamov) condition for the existence of the codes discussed.

which, in the case $n \gg K$, implies

$$H^{-1}(\tfrac{1}{2}) \leqslant d/n \leqslant 2H^{-1}(\tfrac{1}{2}). \tag{4.9}$$

The inverse entropy function $H^{-1}(x)$ is defined for $0 < x \leqslant 1/2$ by $H^{-1}(x) = y$ iff $x = H(y)$. Using $H^{-1}(1/2) \simeq 0.110028$, we find that encoding K qubits using $n \gg K$ allows d/n to be greater than 0.11, while d/n is certainly less than 0.22006. These limits are shown on figure 6.

At this point, a complete discussion would introduce the notion of the capacity of a noisy quantum channel. The capacity would be limited by error rates, and one would investigate whether error-free transmission is possible at rates close to capacity, as in Shannon's theorem. However, the capacity of a noisy quantum channel is not yet understood, and the present author has not developed a satisfactory definition. The equivalent of Shannon's noiseless coding theorem has been developed for the quantum regime by Schumacher (1995), and it is found that the number K of qubits is a useful measure of 'amount of information' in the quantum case, as one would hope. To understand the effect of noise (i.e. errors) in the quantum regime, I conjecture that it is useful to model errors in a way analagous to that employed in classical information theory. That is, we *assume* that decoherence, relaxation and so on in a real quantum computer or information channel can be *modelled* by a stochastic treatment, in which, between two defined times, each qubit either defects (undergoes an arbitrary error), or follows the error-free evolution governed by the known parts of the system Hamiltonian. Which of these two occurs for any given qubit during

any given time interval is a random decision, the defection occuring with probability p. This model is somewhat akin to the 'quantum jump' or 'quantum Monte Carlo' models of dissipative processes in quantum mechanics introduced by several authors in different contexts (Carmichael 1991; Dalibard *et al.* 1992; Dum *et al.* 1992; Gisin 1984; Mølmer *et al.* 1993, and references therein). This similarity suggests that the model can provide a realistic description of a large class of real error processes†. In fact the assumption we make is not that error processes can be *fully* modelled in this way, but merely that a scheme which can correct this assumed type of error will be able to correct satisfactorily the errors in a real physical computer.

With our stochastic model of errors, an argument using the law of large numbers can be employed to show that the probability that uncorrectable errors occur falls to zero when codes of long enough minimum distance are employed, just as in classical information theory. Thus, in the stochastic model, the probability that exactly x errors (defections) occur among n qubits is given by the binomial distribution, if we assume that errors in different qubits are independent. The probability that any number up to x qubits defect is

$$F(x) = \sum_{i=0}^{x} \binom{n}{i} p^i (1-p)^{n-i}, \tag{4.10}$$

where p is the probability of defection of a single qubit, during some defined interval of time $t \rightarrow t + \Delta t$. When $n, np \gg 1$, this can be approximated using the error function: $F(x) \simeq \mathrm{erf}((x-\mu)/\sigma\sqrt{2})$ where $\mu = np$, $\sigma = \sqrt{np(1-p)}$. If an x-error correction scheme is implemented (using a code of distance $d = 2x+1$), then $F(x)$ is the probability that the code can be corrected successfully. When the correction is successful, the state of the quantum computer is *exactly* what it should be (the assumptions of the stochastic model permit this 'unphysical' conclusion).

If the whole computation requires a total number T of time steps, each of duration Δt, and error correction is carried out at the end of each time step, then the probability that the whole computation is free of errors is

$$P(n, p, d, T) = (F(x = \lfloor (d-1)/2 \rfloor))^T. \tag{4.11}$$

In the case of the binomial distribution, the law of large numbers is expressed by the fact that once the number of correctable errors $x = \lfloor (d-1)/2 \rfloor$ becomes larger than the mean number of errors $\mu = np$, the error function $F(x)$ becomes arbitrarily close to 1 as n is increased. To see just how close, we use the asymptotic expansion $1 - \mathrm{erf}(z) \simeq (\exp(-z^2)/2\sqrt{\pi})(1 - 1/2z^2 + \cdots)$, for $z \gg 1$, which gives

$$\begin{aligned} P(\text{recover successfully after one timestep}) &\simeq F(x = d/2) \\ &\simeq 1 - \frac{1}{2\sqrt{\pi}} \exp\left(\frac{-n(d/2n - p)^2}{2p(1-p)} \right), \end{aligned}$$

where

$$d/2n \sim H^{-1}((1 - K/n)/2)$$

† Note, however, that the occurence of a random defection is not to be identified exactly with a quantum jump occuring in the quantum Monte Carlo method of Dalibard *et al.* (1992) and Mølmer *et al.* (1993), since in that method an error term still appears in the state when no quantum jump occurs, due to the non-Hermitian part of the Hamiltonian employed during the periods of evolution between jumps. The quantum Monte Carlo method has exactly the stochastic form we require when only phase relaxation occurs in one basis ('relaxation of type T_2', cf. § 3 *b*).

using inequalities (4.8). The probability that the computer cannot recover from errors falls exponentially with n, as long as codes are used which keep close to the maximum possible correction ability (i.e. Hamming distance), and as long as p is below an upper bound which does not depend on n or K. It has been supposed that such exponential stabilisation would be impossible for a quantum computer. Indeed, it is a surprising result which goes right against the usual conclusion of the Schrödinger cat paradox, in which macroscopic superpositions appear to be inherently unstable, and unstabilizable. However, using inequalities (4.9) (cf. figure 6), we find that error-free computation is guaranteed to be be possible if $p <\sim 0.055$. Error-free computation is impossible if $p >\sim 0.11003$ if correction is attempted using the type of coding method derived in this paper. However, we have not ruled out the possible existence of more powerful correction methods which would allow this upper limit on p to be increased.

As an example, consider a computer requiring $K = 1000$ qubits, which are encoded using a set of $n = 10000$ qubits. Inequalities (4.8) allow $d_1 = d_2 = 939$. Suppose the error (i.e. defection) probability during each time step is $p = 0.04$, and $T = 10000$ time steps are required. During each step, on average 400 errors occur, and the standard deviation of the error distribution is about 20. The probability of error-free computation is, from equation (4.11), $P(n, p, d, T) \simeq 0.01$. If p is reduced to $p = 0.03$, on the other hand, then $F(x) \simeq 1 - 4 \times 10^{-23}$ and error-free computation is almost certain for any reasonable length T of the calculation.

5. Concluding remarks

The error correction methods which have been presented involve many two-qubit CNOT operations each time correction is carried out, and the whole process only works if these operations can be performed without introducing too many extra errors. The number of 1's in the parity check matrix of a $[n, k, d]$ code is about kd, since each message bit must be associated with at least $d - 1$ parity checks. Therefore, the error corrector of such a code involves of the order of kd two-qubit operations. For the case $d_1 = d_2$ one uses coding with $k_1 = k_2 \simeq n/2$, and correction is carried out in both bases. Therefore the total number of operations for one complete correction is of order $nd \simeq 2n^2p$. A logical choice would be to correct the whole computer every time an elementary computing operation is performed. Therefore, the introduction of error correction causes the total number of two-qubit operations to be multiplied by $2n^2p$. This is a modest extension of the resources necessary to complete a computation, since n itself does not increase faster than the number K of bits of quantum information employed. The great gains in computing power associated with 'quantum parallelism' are retained in the corrected noisy computer.

It may come as a surprise that the condition for error-free computation derived above is simply an upper bound $p < H^{-1}(1/2) \simeq 0.11$ on the error probability, rather than a scaling law for n as a function of K and p. However, this is in the nature of the approach we have adopted, since when $np \gg 1$, the number of errors that actually occur during any one time step is almost certainly very close to the average number np, so the whole battle is won or lost on the ability to correct this number of errors. The corresponding limit in the classical regime is $p < H^{-1}(1) = 1/2$, above which error-free communication is impossible and the channel capacity falls to zero. Indeed, if the only errors that occur in the quantum case are phase errors in one of the bases

(say basis 1), then we can afford to use $d_1 = 1$, and the coding problem reduces to the classical one, so p can approach $H^{-1}(1)$ once again. The factor $1/2$ rather than 1 appearing in the inverse entropy function arose because it was assumed just before inequalities (4.8) that arbitrary unknown errors will require correction in both basis 1 and basis 2. It is here that the difference between a qubit and a classical bit enters: the extra degrees of freedom associated with the qubit mean that we do not know, in general, in which basis to correct it, so we are forced to correct it in two mutually rotated bases. By theorem 2.3, this means that both a code and its dual must be capable of correcting the expected error rate, so both k/n and $1 - k/n$ are limited by Shannon's theorem. The classical and quantum cases can be compared thus:

Classical		Quantum		
k/n	$< 1 - H(p)$	k/n	$< 1 - H(p)$	$(n \gg K)$
k/n	> 0	$1 - k/n$	$< 1 - H(p)$	
$\Rightarrow$	$H(p) < 1$	$\Rightarrow$	$H(p) < 1/2$	

It should be stressed that the left-hand side of this comparison represents a well-founded body of knowledge, while the right-hand side involves some assumptions which remain to be investigated further.

The whole argument has assumed that the process of error correction does not itself introduce defection (i.e. decoherence, etc.). However, this is an unrealistic assumption, since the error correction procedure is itself a special kind of quantum computation. Clearly, the probability of error during one time step must be reckoned to increase with the number of operations needed to implement error correction. However, such errors can be corrected during the next time step, provided that they affect sufficiently few qubits. The analysis of this in detail is an important avenue for future work.

In conclusion, the main contribution of this paper, and of Calderbank & Shor (1996), has been to show how to adapt the classical methods of error correction to the quantum regime. Theorems 3.1 and 3.3 are central. The sections leading up to them introduced the ideas, and those following examined the implications. The theorems show that a macroscopic quantum system can be stabilised by a judicious use of unitary operations and dissipative measurements. This is a type of feedback loop or 'quantum servo-control'. Among the results gained along the way are a useful taxonomy of types of multiple-particle (or multiple-qubit) interference, and a general insight into how to perform quantum purity amplification. These are basic properties of quantum theory, the former showing how information can be embodied in many qubits simultaneously, and the latter showing how quantum communication can be isolated from noise and evesdropping. The linear codes we have discussed constitute a generalization of the 'Bell basis' to many qubits.

The obvious need now is for a fuller understanding of the capacity of a noisy quantum channel. In particular, it would be useful to find out whether a stochastic model for errors in a quantum channel is sufficient to enable the error rate for many qubits to be estimated. Also, the effect of noise during the error correction process needs to be investigated. On the experimental side, an implementation of the simplest error correction schemes using 3 or 7 qubits would be a significant step forward.

I thank members of the Oxford Quantum Information group for commenting on the manuscript. The author is supported by the Royal Society.

References

Barenco, A. 1995 A universal two-bit gate for quantum computation. *Proc. R. Soc. Lond.* A **449**, 679–683.

Bell, J. S. 1964 On the Einstein–Podolsky–Rosen paradox. *Physics* **1**, 195–200. (Reprinted in Bell, J. S. 1987 *Speakable and unspeakable in quantum mechanics,* pp. 14–21. Cambridge University Press.)

Bennett, C. H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J. & Wootters, W. K. 1995 Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725.

Bernstein, E. & Vazirini, U. 1993 Quantum complexity theory. In *Proc. 25th Annual ACM Symp. on the Theory of Computing*, pp. 11–20. New York: Association for Computing Machinery.

Berthiaume A., Deutsch D. & Jozsa, R. 1994 The stabilisation of quantum computation. In *Proc. Workshop on Physics and Computation, PhysComp 94*, pp. 60–62. Los Alamitos: IEEE Computer Society Press.

Carmichael, H. J. 1991 An open systems approach to quantum optics. Lectures presented at l'Université Libre de Bruxelles, Bruxelles, Belgium, autumn 1991.

Cirac, J. I. & Zoller, P. 1995 Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091–4094.

Dalibard, J., Castin, Y. & Mølmer, K. 1992 Wave-function approach to dissipative processes in quantum optics *Phys. Rev. Lett.* **68**, 580–583.

Deutsch, D. 1985 Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond.* A **400**, 97–117.

Deutsch, D. & Jozsa, R. 1992 Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond.* A **439**, 553–558.

Deutsch, D., Barenco, A. & Ekert, A. 1995 Universality in quantum computation. *Proc. R. Soc. Lond.* A **449**, 669–677.

Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S. & Sanpera, A. 1996 Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.* **77**, 2818–2821.

DiVincenzo, D. P. 1995 Two-bit gates are universal for quantum computation. *Phys. Rev.* A **51**, 1015–1022.

Dum, R., Zoller, P. & Ritsch, H. 1992 *Phys. Rev.* A **45**, 4879.

Ekert, A. 1995 In *Atomic Physics 14* (ed. D. J. Wineland, C. E. Wieman & S. J. Smith). New York: AIP Press.

Ekert, A. & Jozsa, R. 1996 *Rev. Mod. Phys.* **68**, 733–753.

Feynman, R. P. 1982 Simulating physics with computers. *Int. J. Theor. Phys.* **21**, 467–488.

Gilbert, E. N. 1952 A comparison of signalling alphabets. *Bell Syst. Tech. J.* **31**, 504–522.

Gisin, N. 1984 *Phys. Rev. Lett.* **52**, 1657; *Helvetica Phys. Acta* **62**, 363 (1989).

Greenberger, D. M., Horne, M. A. & Zeilinger, A. 1989 Going beyond Bell's theorem. In *Bell's theorem, quantum theory, and conceptions of the universe* (ed. M. Kafatos), pp. 73–76. Dordrecht: Kluwer Academic Press.

Greenberger, D.M., Horne, M. A., Shimony, A. & Zeilinger, A. 1990 Bell's theorem without inequalities. *Am. J. Phys.* **58**, 1131–1143.

Hamming, R. W. 1950 Error detecting and error correcting codes. *Bell Syst. Tech. J.* **29**, 147–160.

Hamming, R. W. 1986 *Coding and information theory*, 2nd edn. Englewood Cliffs: Prentice-Hall.

Hughes, R. J., Alde, D. M., Dyer, P., Luther, G. C., Morgan, G. L. & Schauer, M. 1995 *Contemp. Phys.* **36**, 149–163.

Landauer, R. 1995 *Phil. Trans. R. Soc. Lond.* A **353**, 367.

MacWilliams, F. J. & Sloane, N. J. A. 1977 *The theory of error-correcting codes.* Amsterdam: North Holland.

Palma, M. G., Suominen, K.-A. & Ekert, A. K. 1996 *Proc. R. Soc. Lond.* A **452**, 567–584.

Mermin, N. D. 1990 Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.* **65**, 1838–1840.

Mølmer, K., Castin Y. & Dalibard, J. 1993 Monte Carlo wave-function method in quantum optics. *J. Opt. Soc. Am.* B **10**, 524–538.

Peres, A. 1993 *Quantum theory: concepts and methods.* Dordrecht: Kluwer Academic Press.

Phoenix, S. J. D. & Townsend, P. D. 1995 Quantum cryptography: how to beat the code breakers using quantum mechanics. *Contemp. Phys.* **36**, 165–195.

Schrödinger, E. 1935 *Naturwiss.* **23**, 807. (Translated in *Quantum theory and measurement* (ed. J. A. Wheeler & W. H. Zurek). Princeton University Press 1983.)

Schumacher, B. 1995 Quantum coding. *Phys. Rev.* A **51**, 2738–2747.

Shimony, A. 1989 Conceptual foundations of quantum mechanics. In *The new physics* (ed. P. Davies) pp. 373–395. Cambridge University Press.

Shor, P. W. 1994 Algorithms for quantum computation: discrete logarithms and factoring. In *Proc. 35th Annual Symp. on Foundations of Computer Science* (ed. S. Goldwasser), pp. 124–134. Los Alamitos: IEEE Computer Society Press.

Shor, P. W. 1995 Scheme for reducing decoherence in quantum computer memory. *Phys. Rev.* A **52**, R2493–R2496.

Simon, D. 1994 On the power of quantum computation. In *Proc. 35th Annual Symp. on Foundations of Computer Science* (ed. S. Goldwasser), pp. 116–123. Los Alamitos: IEEE Computer Society Press.

Steane, A. M. 1996 Error correcting codes in quantum theory. *Phys. Rev. Lett.* **77**, 793–797.

Turing, A. M. 1936 *Proc. Lond. Math. Soc.* 2 **43**, 544.

Unruh, W. G. 1995 Maintaining coherence in quantum computers. *Phys. Rev.* A **51**, 992–997.

Varshamov, R. R. 1957 Estimate of the number of signals in error correcting codes. *Dokl. Akad. Nauk. SSSR* **117**, 739–741.

Zurek, W. H. 1981 Pointer basis of quantum apparatus: into what mixture does the wave packet collapse? *Phys. Rev.* D **24**, 1516–1525.

Zurek, W. H. 1993 Preferred states, predictability, classicality and the environment-induced decoherence. *Prog. Theor. Phys.* **89**, 281–312; see also Zurek, W. H. 1991 Decoherence and the transition from quantum to classical, *Physics Today* **44** October, 36.

Received 27 November 1995; accepted 11 April 1996