QUANTUM ERROR CORRECTION

Andrew M. Steane
Clarendon Laboratory, Oxford OX1 3PU, England.

The concept of *quantum information* is proving to be very useful in efforts to elucidate the nature of quantum mechanics. Both quantum communication and quantum information processing has been shown to be fundamentally different from its classical counterpart. Examples where this difference is highlighted are secure key distribution for cryptography, and the existence of fast algorithms for an idealised quantum computer. However, actual attempts to realise these possibilites run up against a further fundamental part of quantum mechanics: the problem of the instability of coherence.

All physical systems are subject to random fluctuations, including those degrees of freedom which may be described in terms of classical mechanics. However, classical degrees of freedom may be stabilised to a very high degree, either by making the ratio of system size to perurbation size very large (passive stabilisation), or by continuously monitoring the system and providing greatly enhanced 'inertia' against random fluctuation be means of feedback control (active stabilisation). Of these two possibilities, the former, that is passive stabilisation, can be applied in the quantum regime only by making the perturbations small rather than by making the system large, and stabilisation beyond a certain degree is in practice ruled out. It is not hard to show that this makes the experimental realisation of a quantum computer of useful computational power impossible by any currently attemptable method. The physics of quantum information processing remains interesting, one should add. It is simply that great computing power is not available.

The method of *active* stabilisation is extremely powerful in classical systems, and is at the heart of mechanical devices from early steam engines to the latest microchip processors. However, it is not obvious whether anything like active stabilisation is possible for a quantum system, since feedback control involves dissipation, and therefore is non-unitary. Hence one may frame the following question:

> *"Is active stabilisation of a quantum bit possible?"*

The idea of a quantum bit or qubit is introduced in order to emphasize that the aim is to stabilise a complete quantum state, not just a chosen observable. Also, we are concerned with the properties of the quantum state, not with the physical system expressing it. For example, a single qubit may be expressed by a system whose Hilbert space has many more than two dimensions. Among the possible changes such a system may undergo, some will affect the stored single qubit of quantum information, but others will not.

The surprising answer to our question is "yes," with some important *provisos* which depend on the type of stabilisation sought. The stabilisation is based on the classical theory of error correction, which provides a very powerful technique by which classical information can be transmitted without errors through the medium of a noisy channel[1]. Classical error correction operates by the judicious use of redundancy, that is, sending the same information many times. In this sense it is akin to making the system larger in order to make it more resistent to perturbations. However, the precise way in which the redundancy is introduced is very important. The type of redundancy, or *encoding*, employed must be carefully matched to the type of noise in the channel. Typically, one considers the case of random noise which affects different bits independently, but this is not the only possible case. The encoding enables the most likely errors in the information to be identified and corrected. This corrective procedure is akin to active stabilisation, and brings the associated benefits of powerful noise suppression.

To understand the application of these ideas to the quantum regime, it is best to start with a simple example. Thus, suppose we have a collection of spin-half particles, each of which is subject independently to random 'flips' or amplitude errors $|0\rangle \leftrightarrow |1\rangle$, but which otherwise is stable (in particular, the precession is free of phase error). Whenever such a flip occurs, the relevent two-state system may become entangled with its environment. In order to stabilise a single qubit, in the general state $a\,|0_L\rangle + b\,|1_L\rangle$, we express it by means of three two-state

systems, with the 'encoding' $|0_L\rangle \rightarrow |000\rangle$, $|1_L\rangle \rightarrow |111\rangle$. Thus the total initial state of the three spins is $a|000\rangle + b|111\rangle$. After a period of time, during which random flips may occur, the three-spin system is measured twice. The first measurement is a projection onto the two-state basis

$$\{|000\rangle + |111\rangle + |001\rangle + |110\rangle\,, \quad |010\rangle + |101\rangle + |100\rangle + |011\rangle\} \tag{1}$$

The second measurement is a projection onto the two-state basis

$$\{|000\rangle + |111\rangle + |010\rangle + |101\rangle\,, \quad |001\rangle + |110\rangle + |100\rangle + |011\rangle\} \tag{2}$$

Each measurement has two possible results, which we will call 0 and 1. Depending on which results R are obtained, an appropriate action is carried out: if $R = 00$, do nothing; if $R = 01$, flip the rightmost spin; if $R = 10$, flip the middle spin; if $R = 11$, flip the leftmost spin. If, during the time interval when the system was left to evolve freely, no more than one spin flipped, then this procedure will return the three-spin state to $a|000\rangle + b|111\rangle$. It is remarkable that this can be done without gaining information about the values of a and b and thus disturbing the stored quantum information. During the correction procedure, the entanglement between the system and its environment is transferred to an entanglement between the measuring apparatus and the environment. The qubit is actively isolated from its environment by means of this carefully controlled *entanglement transfer*.

The above error correction technique is based on the simplest classical error correcting code. More advanced techniques can be deduced from more advanced known classical codes, and the following striking results are obtained. First, completely general error processes can be corrected, including relaxation and entanglement with the environment, and to do this it is sufficient merely to be able to correct for spin flips (σ_x spin operator) and sign flips (σ_z spin operator)[2–5]. Second, a subset of the classical codes can be adapted directly to the quantum context[3–5]. Third, the probability of failure of the quantum error correction falls exponentially with the redundancy, in the limit of large redundancy, as long as the error rate is below a given level[4,5]. Finally, the degree of required redundancy and the complexity of the correction process rises only as a low-order polynomial function of the number of qubits to be corrected[5].

Note that we define the term 'error' to mean in general *any* contribution to the evolution of a quantum system which is unpredictable. Usually therefore the errors will be continuous rather than discrete, and will affect all the qubits rather than a subset. However, during

error correction the system is projected onto a subspace of its Hilbert space which contains only state vectors with a specific error syndrome. Therefore the continuous error process is rendered discrete (collapsed) by the projective measurement.

The main *proviso* to all the above is that the correction process can itself be carried out without errors. This is clearly a huge assumption. It is probably reasonable in the context of quantum communication[7,8], since there one eventually wishes to measure the communicated qubits, and the bulk of the error correction can be carried out on the classical information obtained *after* the qubits are measured. The context of quantum computing is another matter, however, and it remains to be seen whether quantum error correction can be made sufficiently robust against noise during the correction process itself. Thus quantum theory may still rule out the possibility of a powerful quantum computer.

The author is supported by the Royal Society.

1. MacWilliams F. J. & Sloane, N. J. A. 1977 *The Theory of Error-Correcting Codes.* Amsterdam: North Holland.
2. P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
3. A. M. Steane, submitted to Phys. Rev. Lett.
4. A. R. Calderbank and P. W. Shor, submitted to Phys. Rev. A.
5. A. M. Steane, submitted to Proc. Roy. Soc. A.
6. Related preprints now in circulation are those of I. L. Chuang and R. Laflamme; R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek; C. Macchiavello and A. Ekert.
7. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
8. A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera and W. K. Wootters, Oxford University preprint.

Résumé

Pour des systèmes classiques, les effets indésirables du bruit peuvent être contrôlés par une stabilisation active. Dans le cas des systèmes quantiques, pour lesquels une evolution unitaire doit être préservée, une telle stabilisation n'est pas possible. Ceci semble annéantir les espoirs que l'on fonde sur les possibilités d'un ordinateur qui fonctionnerait de manière quantique. Cependant, en adaptant des méthodes classiques de correction d'erreur, l'information quantique peut être stabilisée activement. La communication d'états quantiques en presence de bruit est ainsi rendue possible, et il est probable que l'élaboration de calculs au niveau quantique puisse bénéficier de ces nouvelles techniques.