International Journal of Theoretical Physics, Vol. 38, No. 3, 1999

Error Symmetrization in Quantum Computers

Asher Peres[1]

Received September 1, 1998

Errors in quantum computers are of two kinds: sudden perturbations to isolated qubits, and slow, random drifts of all the qubits. Isolated errors can be corrected by using quantum codewords that represent a logical qubit in a redundant way, by several physical qubits. On the other hand, slow drifts can be reduced, but not completely eliminated, by means of symmetrization, namely by using many replicas of the computer, and forcing their joint quantum state to be completely symmetric. Several symmetrization strategies are examined and analyzed.

A computer is a physical system, subject to the ordinary laws of nature. No error ever occurs in the application of these laws. What we call an error is a mismatch between what the computer does and what we wanted it to do. This may be caused by incorrect programming (software errors, which I shall not consider here), or by imperfect hardware. The computer engineer's problem is to design the hardware in such a way that common flaws, which are unavoidable, will almost never cause errors in the final output (namely, in the relevant parts of the final state of the computer).

In *classical* computers, logical bits, having values 0 or 1, are implemented in a highly redundant way by bistable elements, such as magnetic domains. The bistability is enforced by coupling the physical bits to a dissipative environment. Errors may then occur because of thermal fluctuations and other hardware imperfections. To take care of these errors, various correction methods have been developed (Welsh, 1989, Chapter 4), involving the use of redundant bits (which are implemented by additional bistable elements).

In *quantum* computers, the situation is more complicated: in spite of their name, the logical "qubits" (quantum binary digits) are not restricted to the discrete values 0 and 1. Their value can be represented by any point on

[1] Department of Physics, Technion—Israel Institute of Technology, 32 000 Haifa, Israel, e-mail: peres@photon.technion.ac.il.

0020-7748/99/0300-079 9$16.00/0 © 1999 Plenum Publishing Corporation

the surface of a Poincaré sphere. Moreover, any set of qubits can be in an *entangled* state: none of the individual qubits has a pure quantum state, it is only the state of all the qubits together that is pure (Peres, 1993, Chapter 5). The continuous nature of qubit states implies that there can be no intrinsic stabilizing mechanism, and error control becomes critical.

Here, a distinction must be made between quantum computers of the Benioff type (Benioff, 1980; Feynman, 1986), where quantum hardware is used for implementing classical logic, and computers that are fundamentally quantal (Deutsch, 1985), and can do more than just mimic classical computation. In the former case, there are instants of time at which all the qubits ought to represent definite values, 0 or 1. They are not then in a quantum superposition, and error correction can be done as for a classical computer (Peres, 1985). On the other hand, a computer of the Deutsch type usually is an entangled state of all the qubits, and classical methods of error correction are not applicable. What can be done then depends on the nature of the anticipated errors.

In general, we may write the Hamiltonian of the computer as $H = H_0 + H_1$, where H_0 is the Hamiltonian of an ideal error-free computer and H_1 represents the influence of the environment. The latter is unknown to the computer designer, except statistically. That Hamiltonian acts on a Hilbert space which is the tensor product of those representing the computer and the environment. The designer's problem is to distill, from the computer's variables, a subset giving with probability close to 1 the correct result of the computation, irrespective of the unknown form of H_1 and of the initial state state of the environment. Two different types of errors ought to be considered: accidental large disturbances to isolated qubits (e.g., a residual gas molecule may hit one of them), and small, random, uncorrelated drifts of all the qubits.

The first type of error can be corrected by codewords (Shor, 1995; Steane, 1996a, b) that represent a logical qubit by means of several physical qubits. The latter are in a highly entangled state chosen in such a way that, if any one of the qubits gets entangled with an unknown environment, there still is enough information stored in the other qubits to restore the codeword and to unitarily disentangle it from the environment (Peres, 1998).

However, continuous random drifts of all the qubits cannot be eliminated by using codewords. They can be reduced by symmetrizing the joint quantum state of several identical computers (Berthiaume *et al.*, 1994; Barenco *et al.*, 1997). The purpose of this paper is to discuss this symmetrization method and some possible variants.

In its original version, the symmetrization method involved the use of R identical replicas of the entire computer. At preset times, the joint quantum state of the R computers is projected onto the symmetric subspace of their common Hilbert space (for example, by measuring whether or not the state is symmetric, and aborting the computation if the answer is negative). As shown below, if *small* errors randomly affect all the qubits, this projection reduces the average error by a factor R. On the other hand, symmetrization gives poor results if a single qubit goes completely astray: we then have a nonsymmetric state that is almost orthogonal to the symmetric subspace, and the computation is almost always aborted. Indeed, if one of the computers has a state orthogonal to that of all the others, the probability is only $1/R$ that the joint state will be projected onto the symmetric subspace; in that case, the error is not eliminated, but rather uniformly spread over all the R computers.

There is, however, a more efficient protocol for error correction by symmetrization. The R computers can be arranged in pairs, and each one of the $R/2$ pairs symmetrized separately. The process can then be repeated with different pairing arrangements if we wish to further improve the symmetry. With such a pairwise symmetrization, if a computer accidentally gets into a state orthogonal to that of all the other ones, there is a 50% chance that the pair containing the bad computer will be eliminated, and a 50% chance that the error will be equally shared by the two computers. Repeating this process many times, so that each computer has many partners, ultimately leads to the elimination of a bad computer, together with one good one. There still are $R - 2$ good computers available for continuing the work.

A more complicated (and probably more realistic) model would be to assume that any computer may occasionally fail when one of the logical steps is executed. This event must be rare enough so that the total probability of failure of any given computer during the entire computation is less than 1/2. Pairwise symmetrizations are performed between any two logical steps (the pairs are chosen in such a way that each computer is compared with many others during the complete computation). Most errors are then eliminated, and the surviving computers contain, on average, less than one defective result. In this theoretical model, an "error" means a state that is orthogonal to the correct one. This notion has to be generalized to the case of less radical errors. It is plausible that repeated pairwise symmetrizations are in general preferable to a single overall symmetrization, but a formal proof is still needed.

The poor efficiency of the symmetrization method in the case of large, isolated errors is due to frequent negative answers to the symmetry tests: when a test fails, we must discard a pair of computers, if not the entire process. However, there is no need of testing anything in order to force a quantum state to stay in a symmetric subspace. A "quantum measurement" is not a supernatural event. It is an ordinary dynamical process, and any error correction that may result from it should also be obtainable as a consequence of a unitary evolution, governed by ordinary dynamical laws. Indeed, a much simpler method for enforcing symmetry of the quantum state is to impose on the R computers an extra static potential that vanishes in the symmetric subspace and has a very large value in all the orthogonal (asymmetric) states. Effectively, in the R computers, any R homologous physical qubits behave as if they were R bosons. Likewise, if the qubits of a codeword have an internal symmetry, such as the cyclic symmetry of the codewords of Bennett *et al.* (1996), we may protect their cyclic subspace by erecting around it a high potential barrier.

The result of such a symmetrizing potential is analogous to a continuous Zeno effect (Peres, 1993, pp. 392–400). To test its effectiveness, consider the simple example of two computer memories, each one consisting of a single qubit, initially in the state $\binom{\alpha}{\beta}$, which is unknown. We want these computer memories to be stable: there should be no evolution of the two qubits. The problem is to protect them against random fluctuations of the environment. Let us use for this discussion the terminology and notations appropriate to spin-1/2 particles. A symmetric state of the pair belongs to the triplet ($J = 1$) representation, while the singlet ($J = 0$) is antisymmetric.

Consider the Hamiltonian

$$H_0 = (1 - \mathbf{J}^2/2)\,\Omega \tag{1}$$

where Ω is a large, positive constant. Since $\mathbf{J}^2 = J(J + 1)$, this potential vanishes in the triplet state, and is equal to Ω for a singlet. As a simple model of perturbation, let a phase error be generated by

$$H_1 = \mu\sigma_{Az} + \nu\sigma_{Bz} \tag{2}$$

where μ and ν are constant coefficients much smaller than Ω, and the subscripts A and B refer to the two qubits. This can also be written as

$$H_1 = \epsilon\,(\sigma_{Az} + \sigma_{Bz}) + \eta\,(\sigma_{Az} - \sigma_{Bz}) \tag{3}$$

where $\epsilon = (\mu + \nu)/2$ and $\eta = (\mu - \nu)/2$. The ϵ term in H_1 is symmetric, it commutes with H_0, and therefore this kind of perturbation cannot be eliminated by symmetrization. Indeed, the evolution of the qubit state $\binom{\alpha}{\beta}$ is given (if we ignore the η term, for simplicity) by $\alpha(t) = \alpha(0)e^{-i\epsilon t}$ and $\beta(t) = \beta(0)e^{i\epsilon t}$. If there were R qubits, instead of just two, the symmetric part of the perturbation (which cannot be eliminated by symmetrization) would have as its coefficient the arithmetic average of the individual perturbations. If the latter are random and independent, that average is expected to be smaller than the r.m.s. perturbation by a factor $\sqrt{R}$, and therefore the error probability is reduced by a factor R. No further improvement can be expected.

On the other hand, the error due to the antisymmetric part of H_1 can be considerably reduced. Written with the Bell basis (Braunstein *et al.*, 1992), the initial state of the pair is

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\frac{\alpha^2+\beta^2}{\sqrt{2}}\,\Phi^+ + \frac{\alpha^2-\beta^2}{\sqrt{2}}\,\Phi^- + \sqrt{2}\alpha\beta\Psi^+ \tag{4}$$

where Φ^+, Φ^-, and Ψ^+ are the triplet states corresponding to $J_x = 0$, $J_y = 0$, and $J_z = 0$, respectively. The antisymmetric part of the perturbation has matrix elements given by

$$(\sigma_{Az} - \sigma_{Bz})\,\Phi^{\pm} = 0 \tag{5}$$

and

$$(\sigma_{Az} - \sigma_{Bz})\,\Psi^{\pm} = \Psi^{\mp} \tag{6}$$

where Ψ^- is the singlet state. The nontrivial part of the Hamiltonian thus involves only the $\Psi^{\pm}$ subspace. We can write (ignoring for simplicity the ϵ contribution, which is symmetric)

$$H = H_0 + H_1 = \begin{pmatrix}0 & \eta\\ \eta & \Omega\end{pmatrix} \tag{7}$$

It is easy to find the eigenvalues and eigenvectors of this Hamiltonian. The initial state (4) can be written as a linear combination of these two eigenstates, and its time evolution obtained explicitly: the $\Phi^{\pm}$ terms have constant amplitudes, and, for $\eta \ll \Omega$, the Ψ^+ term in (4) evolves as

$$\Psi^+ \to e^{i\eta^2 t/\Omega}\,\Psi^+ + (\eta/\Omega)\,(e^{-i\Omega t} - 1)\,\Psi^- \tag{8}$$

where terms of order $(\eta/\Omega)^2$ have been neglected. If we could make the potential energy Ω arbitrarily large (as we do in an ideal "quantum measurement" context, where the interaction with the measuring apparatus is assumed arbitrarily strong), then the Ψ^+ term in the state vector would be perfectly stabilized, and the Ψ^- term (which is antisymmetric) would never appear. For large, but finite Ω, the amplitude of the Ψ^- term, initially zero, always remains small. On the other hand, the Ψ^+ term undergoes a slow secular drift, which definitely is an error, but is nevertheless compatible with the symmetry constraint. The same kind of drift also occurs for repeated discrete symmetrization (Berthiaume *et al.*, 1994) because the symmetric state obtained at each step may contain a small residual error, and these errors gradually accumulate.

These considerations can now be generalized from two to R computers, each one having many qubits. It may seem that a global potential is required, involving all of them at once, a proposal that would be a technological nightmare. Fortunately, this is not necessary: it is enough to take $R(R-1)/2$ identical potentials, one for each pair of computers. If any two computers are in a symmetric state, then all R computers are in a symmetric state, by definition. The comparison of two computers cannot be done bitwise: the states of the complete computers have to be compared. However, this can be achieved by means of a coherent sequence of two-qubit interactions, as shown by Barenco *et al.* (1997).

Finally, let us note that the symmetrization method can also be applied to individual codewords if the latter have an internal symmetry. For example, the codewords of Bennett *et al.* (1996) are invariant under cyclic permutations of their five qubits. These codewords have the property that if any four qubits are correct, it is always possible to restore the remaining defective qubit. However, the codeword error correction procedure definitely requires four qubits to be correct, and it cannot cope with small drifts of all five qubits, or even two of them. Therefore, it is helpful to test once in a while the cyclic symmetry of the codeword: successful tests will reduce the amplitude of small errors. Unfortunately, just as in the case of intercomputer symmetrization, an unsuccessful test leads to an asymmetric state, and forces us to completely discard the incorrect codeword. One of the logical qubits is then missing, and the computation can proceed only if there is enough redundancy among the logical qubits themselves (not only in their representation by physical qubits), for example, if they are parts of higher order codewords.

Instead of continually testing the symmetry of a codeword, it is also possible to force its physical qubits to respect that symmetry by introducing a high potential barrier that prevents access to asymmetric states, as in Eq. (1):

$$H_0 \to H_0 + \Omega\,(1 - P_0 - P_1) \tag{9}$$

where P_0 and P_1 are projection operators on the codewords that represent the logical 0 and 1, respectively. In this way, an error that turns a codeword state into a new quantum state lying in the orthocomplement of the legal subspace can be produced only by investing a large amount of energy, Ω. All corrigible errors are of this type, and are therefore prevented. However, an incorrigible error, namely one that creates a state that is not orthogonal to both codewords, cannot be prevented by the additional potential in Eq. (9). Incorrigible errors remain uncorrected, of course. At most, their probability of occurrence can be reduced.

ACKNOWLEDGMENTS

This work was supported by the Gerard Swope Fund and the Fund for Encouragement of Research. Part of it was done during a visit to the Institute of Theoretical Physics, University of California, Santa Barbara, whose hospitality is gratefully acknowledged.

REFERENCES

Barenco, A., Berthiaume, A., Deutsch, D., Ekert, A., Jozsa, R., and Macchiavello, C. (1997). *SIAM Journal of Computation*, **26**, 1541.

Benioff, P. A. (1980). *Journal of Statistical Physics*, **22**, 563.

Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K. (1996). *Physical Review A*, **54**, 3824.

Berthiaume, A., Deutsch, D., and Jozsa, R. (1994). The stabilisation of quantum computation. In *Proceedings of the Workshop on Physics and Computation, PhysComp '94*, IEEE Computer Society Press.

Braunstein, S. L., Mann, A., and Revzen, M. (1992). *Physical Review Letters*, **68**, 3259.

Deutsch, D. (1985). *Proceedings of the Royal Society (London) A*, **400**, 97.

Feynman, R. P. (1986). *Foundations of Physics*, **16**, 507.

Peres, A. (1985). *Physical Review A*, **32**, 3266.

Peres, A. (1993). *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht.

Peres, A. (1998). *Superlattices and Microstructures*, **23**, 373.

Shor, P. W. (1995). *Physical Review A*, **52**, 2493.

Steane, A. M. (1996a) *Physical Review Letters*, **77**, 793.

Steane, A. M. (1996b). *Proceedings of the Royal Society (London) A*, **452**, 2551.

Welsh, D. (1989). *Codes and Cryptography*, Oxford University Press, Oxford.