The Stabilisation of Quantum Computations

André Berthiaume
Département IRO
Université de Montréal
Montréal, Québec

David Deutsch
Wolfson College
University of Oxford,
Oxford UK

Richard Jozsa
School of Mathematics and Statistics
University of Plymouth
Plymouth UK

1 Introduction

A *quantum computer* ([5], [2] and [3]) is a device capable of performing computational tasks that depend on characteristically quantum mechanical effects, in particular coherent quantum superposition. Recently it has been shown ([4], [1], [7] and [6]) that such devices can efficiently perform classes of computation, e.g. factorisation, which are believe to intractable on any classical computer. This makes it highly desirable to construct such devices. In this paper we address the last remaining theoretical obstacle to such a construction, namely, the problem of stability, or error correction.

This problem is more substantial in quantum computation than in classical computation because of the delicate nature of the interference phenomena on which quantum computation depends. In all classical computers, stability is achieve by using great redundancy. That is, one represents the computational variables redundantly, using many more physical degrees of freedom than are logically required, and then takes the average, or the majority vote, to be the answer. This error-correction process is applied many times during a computation and at each application all the redundant copies are reset to the accepted result. The probability of error can be shown to fall exponentially with the degree of redundancy, efficiently stabilising the computation.

However, all such classical methods depend in effect on *measuring* the computational state before the computation has finished. In quantum computation this is impossible, because any such measurement would create quantum correlations between the computer and the outside physical objects, thus destroying the coherence.

In this paper we present a new, purely quantum mechanical method of error correction, which has no classical analogue, but can serve to stabilise coherent quantum computations. Like the classical methods, it utilises redundancy, but it does not depend on measuring intermediate results of the computation.

2 Classical Error-Correction: Redundancy and Majority Voting

Consider a classical computer that performs each computational step inaccurately, having a probability $\frac{1}{2}+\varepsilon$ of producing the correct answer.

If we use R such computers the probability E that a majority will give the wrong results at any step is less than $2^{-\frac{2\epsilon^2 R}{\ln 2}}$. This decreases exponentially with the degree of redundancy R. Suppose a polynomial-time computation runs for M steps and majority voting is used after each step. The probability that the final answer will be correct is then greater the $(1-E)^M$. Thus any desired success probability $1-\delta$ can be achieved using a degree of redundancy $R = \mathrm{O}(\log M/\delta)$.

Unfortunately no such method can be applied in the quantum case - quantum mechanics does not allow one to identify the state of a given object or indeed even to clone an unidentified state. Thus the technique of majority voting cannot even get off the ground, as we can neither determine what state is in the majority nor reset the remaining copies to that state.

3 Quantum Error-Correction: The Symmetric Subspace

Suppose that we have R copies of a quantum computer. If there were no errors then at time t during the computation the joint state would have the form

$$|\Psi(t)\rangle = \overbrace{|\psi(t)\rangle|\psi(t)\rangle\ldots|\psi(t)\rangle}^{R} \in \mathcal{H}^R \qquad (1)$$

where $\mathcal{H}$ is the Hilbert space of states of one computer. In the presence of errors the states of the R computers will evolve wrongly, and, in general differently. They will have a joint state of the form

$$|\psi_1(t)\rangle|\psi_2(t)\rangle\ldots|\psi_R(t)\rangle \qquad (2)$$

or more generally a (mixture of) superpositions of such states. The fundamental reason that majority voting

0-8186-6715-X/94 $4.00 © 1994 IEEE

cannot be applied is the quantum mechanics forbids the identification of the component states $|\psi_i(t)\rangle$.

Consider the set of all possible error-free joint states i.e. states of the form for arbitrary $|\psi(t)\rangle$. The subspace spanned by this set is known as the *symmetric subspace*, S, of $\mathcal{H}^R$. It is thus the smallest Hilbert space containing all possible error-free states. S may alternatively be defined as the space of all states in $\mathcal{H}^R$ which are invariant under interchange of any two computers. For fixed $\mathcal{H}$ the dimension of S increases only polynomially with R whereas the dimension of $\mathcal{H}^R$ increases exponentially. For example if $\mathcal{H}$ is 2-dimensional then S is an $(R+1)$-dimensional subspace of the 2^R-dimensional space $\mathcal{H}^R$.

Thus, since all possible error-free states lie in a tiny subspace S of the full Hilbert space $\mathcal{H}^R$, we might hope that projecting a slightly erroneous state into S would serve to remove a large proportion of its erroneous component. For example, suppose that the R computers are subject to random errors. Their joint state may be written as the sun of an error-free component proportional to (1) and a remainder. Because of the randomness of the error this remainder lies in a random direction in $\mathcal{H}^R$ and hence is expected to have only an exponentially small component in S. The error-free component, by contrast, lies wholly in S.

4 Projecting into the Symmetric Subspace

The projection operator $\hat{P}$ into the subspace S is (like any projection operator) an observable with eigenvalues 0 and 1. We shall now show how this observable on $\mathcal{H}^R$ may be efficiently measured.

We first show how to project a product state of the form (2) into S. The same method must, by linearity of quantum mechanics, do the same for a general state in $\mathcal{H}^R$. We first append an *ancilla*, i.e. an auxiliary system, with an $R!$-dimensional state space $\mathcal{A}$, initially in a standard state $|\mathbf{0}\rangle$. We then apply to the ancilla a unitary transformation U whose effect is

$$U|\mathbf{0}\rangle = \frac{1}{\sqrt{R!}}\sum_{i=0}^{R!-1}|i\rangle$$

where the states $|i\rangle$ form an orthonormal basis for $\mathcal{A}$. This can be performed in a number of steps that is polynomial in R. Next we perform a unitary operation on $A \otimes \mathcal{H}^R$, which applies the i'th permutation to the R computers if the ancilla is in the state $|i\rangle$. Each permutation can be performed with $\mathbf{O}(R\log R)$ transposition. Next, we perform the transformation U^{-1}, an operation that involves only the ancilla, and can again be performed in a number of steps that is polynomial in R.

If the state of the R computers was initially in S, then each of the permutation left that state unchanged, and the ancilla would therefore have returned to the state $|\mathbf{0}\rangle$. Since U transforms

$|\mathbf{0}\rangle$ into an equal-amplitude superposition, it follows that U^{-1} will transform each $|i\rangle$ to $|\mathbf{0}\rangle$ with equal amplitude. Thus if we measure the ancilla in the basis $\{|i\rangle\}$, and the outcome is zero, the relative state of the R computers must be the projection into S of its original form. If the outcome is not zero, then our symmetrization has failed, and the computation must be re-started from the beginning.

It is therefore desirable to maximise the probability of successful symmetrization.

The cumulative probability that a sequence of symmetrizations will all succeed can be made arbitrarily close to 1 by performing them sufficiently frequently. This is the well-known quantum watchdog effect. We are measuring the observable $\hat{P}$, hoping for outcome 1. If we do obtain that outcome the relative state of the system is an eigenstate of $\hat{P}$ with eigenvalue 1. During the interval between symmetrizations, the state will evolve away from such an eigenstate, with an evolution of the form $\cos(\omega t)|\mathbf{1}\rangle + \sin(\omega t)|\mathbf{0}\rangle$, where ω is some characteristic frequency of the system. If symmetrization is performed N times during the period T of the computation and if $\omega T/N$ is small then the probability of any particular symmetrization failing will be

$$\sin^2\left(\frac{\omega T}{N}\right) \approx \frac{\omega^2 T^2}{N^2}$$

The probability that all N symmetrizations will succeed is therefore

$$\left(1-\frac{\omega^2T^2}{N^2}\right)^N \approx 1-\frac{\omega^2T^2}{N}$$

Thus the probability of having to restart the computation is inversely proportional to N.

5 The Stabilisation of Quantum Computations

The above arguments suggest the following strategy for stabilising quantum computers. Based on an estimate of the length M of the computation and a desired lower bound $1-\mu$ on the probability that an outcome be correct, we can choose a redundancy R and a number N of symmetrization operations that will achieve the desired bound. R will be polynomial in $\log(M/\mu)$. N will be chosen to satisfy the condition that $\omega T/N$ be small.

References

[1] E. Berstein and U. Vazirani, *Quantum Complexity Theory*, Proc. 25th ACM·Symp. on the Theory of Computation 11-20 (1993)

[2] D. Deutsch, *Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer*, Proc. R. Soc. Lond., **A400** 96-117 (1985)

[3] D. Deutsch, *Quantum Computational Networks*, Proc. R. Soc. Lond., **A425** 73-90 (1989).

[4] D. Deutsch and R. Jozsa, *Rapid Solution of Problems by Quantum Computation*, Proc. R. Soc. Lond., **A439** 553-558 (1992)

[5] R. Feynman, *Simulating Physics with Computers*, Int. J. Theor. Phys., **21** 6/7 467-448 (1982)

[6] P.W. Shor, *Algorithms for Quantum Computation: discrete Log and Factoring* (1994 preprint).

[7] D. Simon, *On the power of Quantum Computation* (1994 preprint)