Robust solutions to hard problems

John Preskill

Twenty-first century computers could achieve astonishing speed by exploiting the principles of quantum mechanics. New techniques of quantum error correction will be essential to prevent those machines from crashing.

According to the classical theory of computation, it is possible for a computing system to be fault tolerant — it can be designed so that it is sure to get the right answer even though its components occasionally fail. Now Emanuel Knill, Raymond Laflamme and Wojciech Zurek of Los Alamos National Laboratory have reported a similar result for quantum computers[1]. They show that a properly designed quantum computer can achieve arbitrarily high reliability, provided that its components operate within a specified tolerance. Along with other recent developments in quantum error correction, this work has bolstered the hope that large-scale quantum computers will someday be realized.

Whereas ordinary classical computers process information encoded in bits, a quantum computer processes information encoded in quantum states — such as the internal electronic states of individual atoms, the polarization states of photons, or the spin states of atomic nuclei. Interest in quantum computation grew explosively a few years ago when it was recognized that a quantum computer, by exploiting the exotic properties of quantum information, can make many attempts to solve a hard problem all at the same time. A quantum computer exploits a kind of massive parallelism that can never be approached by any conceivable conventional digital computer. Therefore it can, in principle, solve certain hard problems far faster than any foreseeable digital device.

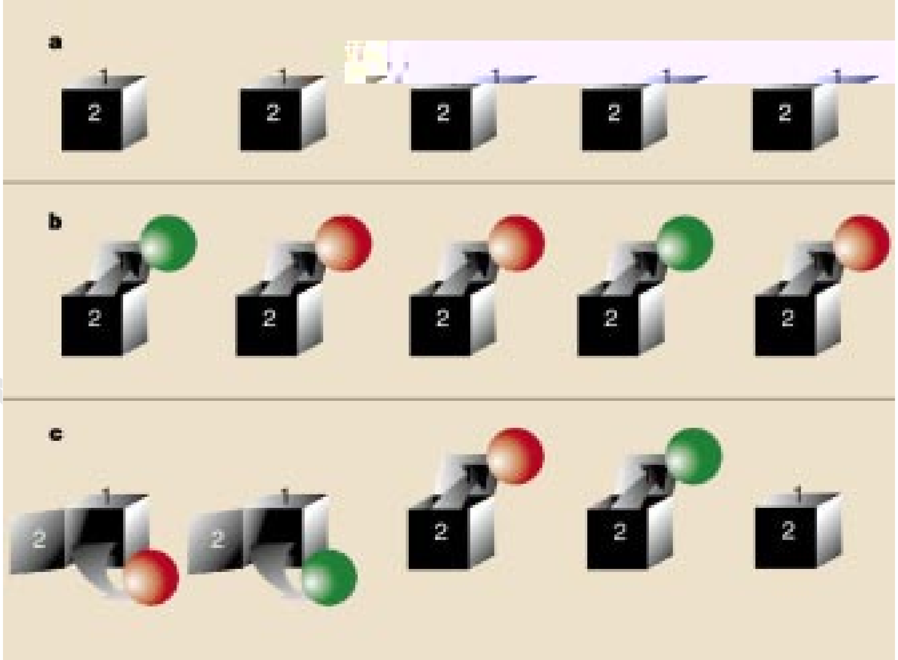

Figure 1 **A simple quantum error correcting code.** a, **A quantum bit ('qubit') of information can be envisaged as a box with an object inside (here a ball). The object can be one of two colours, and the box can be opened through one of two doors; the doors might represent two different ways to measure the polarization of a photon. In the code portrayed here, one qubit of information is encoded in correlations among five different boxes. As shown in** b, **we can measure the encoded qubit by opening door 1 on all five boxes, and observing whether the number of green balls is even or odd. But to operate a quantum computer reliably, we need to be able to correct errors without measuring or otherwise disturbing the encoded qubit. An error occurs when the environment opens a door and switches the colour of the ball; different types of errors modify the correlations among the boxes in distinguishable ways.** c, **We can diagnose the error by opening door 1 of two boxes and door 2 of two other boxes — if the number of green balls is odd, then an error has been detected. Four such measurements of four boxes each suffice to identify which box is damaged and what action will repair it.**

An example of a hard problem is factoring — finding the prime factors of a composite number. Nowadays, with the best hardware and algorithm, it is barely possible to find the 65-digit prime factors of a 130-digit number in a few months. The difficulty escalates sharply as the number of digits increases: with the same hardware and algorithm, we would need about the age of the Universe (10 billion years) to factor a 400-digit number. But with a quantum computer that could factor a 130-digit number in a month (which doesn't exist, of course, at least not yet), we would be able to factor a 400-digit number in just a few years, using an algorithm discovered in 1994 by Peter Shor[2]. So at least for certain classes of hard problem, the time needed to find a solution scales much more favourably with the size of the problem if we use a quantum computer rather than a conventional computer.

This development may have profound implications for the foundations of computer science, but what of the implications for technology? When will we have quantum computers on our desktops? The hardware is still in its infancy (quantum logic gates were successfully demonstrated for the first time less than three years ago[3,4]), so it seems safe to predict that practical and large-scale quantum computers will not be manufactured for at least several decades. But even in the longer term, one may wonder whether useful quantum computing devices will ever be feasible.

A fundamental problem is that quantum computers are far more susceptible to making errors than conventional digital computers. Complicated quantum systems are notoriously unstable; they inevitably interact with their surroundings, causing their stored information to decay — a process called decoherence. No matter how the hardware of future quantum computers is constructed, it is nearly certain that some type of error control will be needed to prevent the machines from crashing.

Error correction is a routine part of modern digital communication, but extending the classical ideas about error correction and fault tolerance to quantum devices required new ideas. The prospects for quantum computing received a tremendous boost in 1995 when Shor[5] and Andrew Steane[6] independently discovered that quantum error correction really is possible. If quantum information is cleverly encoded, then suitable measurements — such as those portrayed in Fig. 1 — can digitize the errors that afflict the information. If the errors are small, then most of the time the measurement projects the quantum system back to an undamaged state; rarely, the measurement projects the system to a state with a particular type of error that can be diagnosed and reversed. Only much more rarely is the error so serious that faithful recovery is impossible.

If we want to perform a reliable quantum computation, we must do more than merely store quantum information with high fidelity; we must also be able to process the encoded information accurately. The central principles of fault-tolerant quantum computation were formulated in 1996 by Shor[7]; now Knill, Laflamme and Zurek have invoked these ideas to show that, despite the debilitating effects of decoherence and other sources of noise, a quantum computer can carry out an arbitrarily long computation successfully, as long as the components of the machine are not too noisy. Similar results have been obtained by others[8–10] but Knill *et al.*[1] analyse a more general and realistic class of error models.

The principles of fault tolerance can be adapted to realistic laboratory situations[11], and small-scale experimental demonstrations of quantum error correction are now feasible. Still, the gap between current technology and what will be needed in the future is vast, and the challenge of devising large-scale quantum computers remains formidable[12]. Fresh ideas will be needed to bridge this gap. Although the new principles of fault tolerance have nourished the hope that quantum computers can overcome the menace of decoherence, a broad effort from physicists, computer scientists and engineers will be needed if quantum computers are to fulfil their destiny as the world's fastest computing devices.

If, as is indicated by efficient quantum algorithms, quantum computers can perform tasks that are beyond the grasp of foreseeable classical computers, then realizable quantum systems may have far greater potential than we now suspect to surprise, baffle and delight us. Yet this potential will never be fulfilled if we can't protect such systems from the destructive effects of noise and decoherence. Thus the discovery of fault-tolerant methods for quantum error recovery and quantum computation may have exceptionally deep implications, both for the future of experimental physics and for the future of technology. The theoretical advances have illuminated the path towards a future in which intricate quantum systems may be persuaded to do our bidding. □

John Preskill is in the Division of Physics, Mathematics, and Astronomy, California Institute of Technology, Pasadena, California 91125, USA.
e-mail: preskill@theory.caltech.edu

1. Knill, E., Laflamme, R. & Zurek, W. H. *Proc. R. Soc. Lond. A* **454,** 365–384 (1998); *Science* **279,** 342–345 (1998).
2. Shor, P. *Proc. 35th Annu. Symp. Fundamentals of Computer Science* 124–134 (IEEE Press, Los Alamitos, CA, 1994).
3. Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M. & Wineland, D. J. *Phys. Rev. Lett.* **75,** 4714–4717 (1995).
4. Turchette, Q. A., Hood, C. J., Lange, W., Mabuchi, H. & Kimble, H. J. *Phys. Rev. Lett.* **75,** 4710–4713 (1995).
5. Shor, P. *Phys. Rev. A* **52,** R2493–R2496 (1995).
6. Steane, A. M. *Phys. Rev. Lett.* **77,** 793–797 (1996).
7. Shor, P. *Proc. Symp. Foundations of Computer Science* preprint quant-ph/9605011 at xxx.lanl.gov
8. Aharonov, D. & Ben-Or, M. *Proc 29th Annu. ACM Symp. Theory of Computing* preprint quant-ph/9611025 at xxx.lanl.gov
9. Kitaev, A. Yu. *Russian Math. Surv.* No. 6 (1997).
10. Preskill, J. *Proc. R. Soc. Lond. A* **454,** 385–410 (1998).
11. Van Enk, S. J., Cirac, J. I. & Zoller, P. *Science* **279,** 205–208 (1998).
12. Preskill, J. *Proc. R. Soc. Lond. A* **454,** 469–486 (1998).

Evolutionary biology

Eyes viewed from the skin

Heinz Arnheiter

Many vertebrates and invertebrates have cells in the skin which react to light by dispersing or aggregating intracellular pigment granules. Even in a dish, such cells act like chameleons and change their shading according to the light[1].

A study by Provencio *et al.*, published last month in *Proceedings of the National Academy of Sciences*[2], now shows that light-sensitive pigment cells in frog skin, called melanophores, express a molecule, melanopsin, which is similar to the rhodopsins used to detect light in the eye. Melanopsin is also expressed in several other cell types known or thought to be light-sensitive in the frog, including cells in the iris, non-image-forming photoreceptor cells in the retina, and hypothalamic neurons which may be involved in controlling responses to day/night cycles. All this is hardly unexpected. Rather, the real surprise comes in Provencio and colleagues' finding that melanopsin is more closely related to the rhodopsins in invertebrate eyes (particularly of scallop, squid and octopus) than to those in vertebrate eyes, including the frog's own eyes. This is an observation that raises several intriguing issues.

Members of the rhodopsin family are built on the principle that, when hit by photons, a chromophore related to vitamin A can flip its conformation and impart conformational changes on a seven-transmembrane G-protein-coupled receptor (opsin). Phylogenetic analyses suggest that an ancestral opsin gene was duplicated during, or even before, the split of animals into vertebrates and higher invertebrates, and then diverged to give rise to the two main branches of vertebrate and invertebrate opsins[3]. The main differences between members of these two opsin branches include the type of chromophore regeneration after photoactivation and the type of G-protein used for signal transduction. For instance, in vertebrate photoreceptor cells, the chromophore is released from opsin and regenerated in neighbouring cells; in invertebrate photoreceptor cells, the chromophore is retained and available for repeated photochemical interconversions.

This difference depends on a particular residue in the third transmembrane helix of the G-protein-coupled receptor, which in vertebrate opsins is acidic but in most invertebrate opsins (and in melanopsin) is aromatic[4] (Fig. 1). It is likely, therefore, that melanopsin, like invertebrate opsins, is more self-sufficient in chromophore regeneration. As Provencio and colleagues point out, this feature may be important for cells such as melanophores which, because they are dispersed over much of an animal's surface, may not be able to establish a firm relationship with specialized neighbouring cells capable of providing fresh chromophore.

G proteins are used in all sorts of biological signalling systems, and some of the variety in their properties stems from differences in the amino-acid composition of their α-subunits. In the case of rhodopsin action, in most invertebrate opsins coupling is with the q-type α-subunit; in vertebrate opsins with the t (or transducin) type. One of the opsin domains implicated in this difference is the third cytoplasmic loop[4]. Melanopsin's predicted third cytoplasmic loop shows very limited sequence similarities with the corresponding loops of either vertebrate or invertebrate opsins, although its length is similar to the longer loops of invertebrate opsins (Fig. 1). This sequence dissimilarity may reflect the fact that the melanophore's pigment redistribution can be mimicked by hormones whose action is mediated through receptors that stimulate different G proteins[1]. Perhaps melanopsin interacts with these G proteins and may thus allow the pigment cells to integrate the light and hormone responses.

Melanopsin's close similarities with scallop SCOP-1, and squid and octopus opsins, are not restricted to the above-mentioned functionally important domains but extend over much of the transmembrane and loop regions. They include a long cytoplasmic tail characteristic of these opsins, and clearly place melanopsin phylogenetically with invertebrate opsins. Melanopsin is thus one of the most highly divergent of a long list of opsins in vertebrates which includes other divergent opsins such as catfish parapinopsin (expressed in the parapineal and pineal gland)[5] and vertebrate ancient opsin of salmon[6]. These opsins are also likely to be involved in non-image-forming tasks of photodetection, but are still more closely related to vertebrate ocular opsins than to melanopsin. Although convergent evolution cannot be ruled out, it can hardly