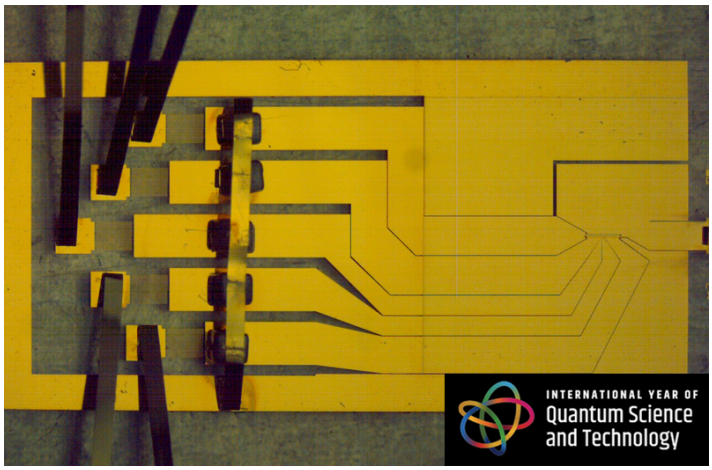
Quantum Milestones, 1995: Correcting Quantum Computer Errors

Researchers proposed methods to preserve the integrity of quantum bits—techniques that may become the key to practical quantum computing on a large scale.

By **David Lindley**

For the International Year of Quantum Science and Technology, we are republishing stories on the history of quantum physics from the archives of Physics Magazine *and* APS News*. The original version of this story was published in* Physics Magazine *on June 10, 2016.*

Quantum computers were dreamed up long before any practical demonstration became possible. In the mid-1990s, two researchers working independently showed theoretically how to get around one major difficulty that some thought insurmountable [**1**, **2**]. They devised error-correction methods that would protect the fragile quantum states essential to the inner workings of a quantum computer. The discovery inspired fault-tolerant designs that could make large-scale quantum computers feasible, as well as methods to preserve information transmitted by quantum-mechanical means.

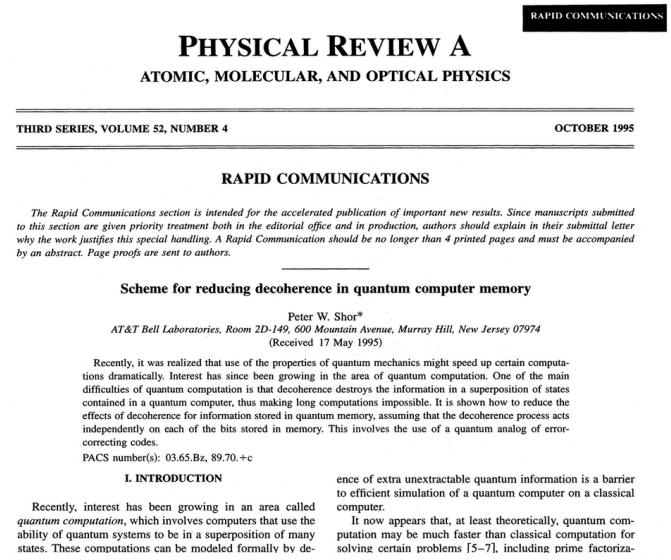


This arrangement of gold electrodes on a chip can hold up to twelve magnesium ions 40 μm above the surface while laser light cools them, enabling the ions to functions as qubits. Error-correction techniques that allow qubits to recover from unwanted disturbances will be a crucial part of any large-scale quantum computer.
Credit: S. Seidelin and J. Chiaverini/NIST

The idea of quantum computing is often credited to Richard Feynman, who gave a talk in 1981 arguing that quantum combinations, or "superpositions," of two distinct states could form the elements of a computer. Instead of 1s and 0s, the quantum bits (qubits) could be in states that were partially 1 and partially 0—a more versatile system [**3**]. In 1994, Peter Shor of AT&T Bell Labs in Murray Hill, New Jersey, showed that such a device could rapidly find the factors of large numbers, a task that is prohibitively time-consuming using conventional computers [**4**].

But doubts also arose about the feasibility of quantum computing. A qubit can maintain its identity only as long as it is kept strictly isolated from disturbances that would knock it out of its quantum superposition and force it to become either a 1 or a 0. Some researchers argued that it would be impossible to preserve qubits long enough to perform a calculation [**5**].

Shor addressed this concern in 1995 by coming up with a way to



RAPID COMMUNICATIONS

PHYSICAL REVIEW A

ATOMIC, MOLECULAR, AND OPTICAL PHYSICS

THIRD SERIES, VOLUME 52, NUMBER 4 OCTOBER 1995

RAPID COMMUNICATIONS

The Rapid Communications section is intended for the accelerated publication of important new results. Since manuscripts submitted to this section are given priority treatment both in the editorial office and in production, authors should explain in their submittal letter why the work justifies this special handling. A Rapid Communication should be no longer than 4 printed pages and must be accompanied by an abstract. Page proofs are sent to authors.

Scheme for reducing decoherence in quantum computer memory

Peter W. Shor*

AT&T Bell Laboratories, Room 2D-149, 600 Mountain Avenue, Murray Hill, New Jersey 07974

(Received 17 May 1995)

Recently, it was realized that use of the properties of quantum mechanics might speed up certain computations dramatically. Interest has since been growing in the area of quantum computation. One of the main difficulties of quantum computation is that decoherence destroys the information in a superposition of states contained in a quantum computer, thus making long computations impossible. It is shown how to reduce the effects of decoherence for information stored in quantum memory, assuming that the decoherence process acts independently on each of the bits stored in memory. This involves the use of a quantum analog of error-correcting codes.

PACS number(s): 03.65.Bz, 89.70.+c

I. INTRODUCTION

Recently, interest has been growing in an area called *quantum computation*, which involves computers that use the ability of quantum systems to be in a superposition of many states. These computations can be modeled formally by de-

ence of extra unextractable quantum information is a barrier to efficient simulation of a quantum computer on a classical computer.

It now appears that, at least theoretically, quantum computation may be much faster than classical computation for solving certain problems [5–7], including prime factoriza-

Credit: P. W. Shor [**1**]

test whether a qubit has been disturbed and, if so, correct it. The problem is that any direct test of a qubit amounts to a measurement that destroys its superposed state. Shor explained how to create, from a single qubit, a state of nine qubits that are connected through quantum entanglement and that encode the original superposition. The nine-qubit state is a set of three groups containing three qubits each, all of which are identical at the start. If one qubit out of the nine is disturbed, then the triplet it belongs to will become different from the other two. The two identical triplets, however, retain an accurate record of the original qubit state.

To assess the condition of the triplets without destroying the relevant information, Shor made use of measurements that reveal only one aspect of an entangled state. For example, with qubits based on quantum spins, a certain measurement of an entangled qubit pair will show whether their spins point in the same or opposite directions, without indicating what those directions are. Shor constructed a sequence of such operations on the three triplets that would indicate whether one of them had changed and that would allow another sequence of operations to reconstruct the original qubit from the unchanged triplets.

The next year, Andrew Steane of the University of Oxford, UK, published an analysis in the same vein, except that his error-correction method needed only seven qubits. Both his and Shor's methods were, at the time, theoretical proposals. As Steane observed, "the experimental production of such states…is a demanding task which remains to be addressed."

"Shor's work was revelatory," says David DiVincenzo, now at Aachen University in Germany. At the time he was at IBM Research in Yorktown Heights, New York, working with colleagues on issues arising from the 1993 discovery of quantum teleportation (see **Special Feature: Quantum Milestones, 1993: Teleportation Is Not Science Fiction**). In teleportation, two observers at different locations share an entangled state, and a problem analogous to error correction arises in that the connection between the observers will typically be subject to disturbances that can disrupt the entanglement. The IBM group was studying this problem when Shor's work appeared, and it influenced their research on how to guarantee accurate teleportation through a noisy channel [**6**].

Theoretical work blossomed rapidly, says DiVincenzo. It quickly emerged that infinitely many error-correction codes exist, classifiable using group theory, and connections with statistical mechanics and phase transitions became apparent. The first demonstration of an error-correction method came in 1998 [**7**]. But the experimental work is difficult, and progress continues to be "more plodding," as DiVincenzo puts it. So far, working quantum computers have involved only a handful of qubits that can be protected from disturbance, and quantum error-correction has been demonstrated only for single qubits. For large-scale quantum computing to become practical, however, fault-tolerant methods originating in Shor's and Steane's work will be a necessary design element.

David Lindley is a freelance science writer, now retired. His most recent book is ***The Dream Universe: How Fundamental Physics Lost Its Way*** (Penguin Random House, 2020).

REFERENCES

1. P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," **Phys. Rev. A 52, R2493 (1995).**
2. A. M. Steane, "Error correcting codes in quantum theory," **Phys. Rev. Lett. 77, 793 (1996).**
3. R. P. Feynman, "Simulating physics with computers," **Int. J. Theor. Phys. 21, 467 (1982).**
4. P. W. Shor, "Algorithms for quantum computation," **Proc. 35th**

Ann. Symp. Foundation of Computer Science (IEEE Computer Society Press, Los Alamitos, 1994), p. 124; P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," **SIAM J. Comput. 26, 1484 (1997).**

5. R. Landauer, "Is quantum mechanics useful?" **Philos. Trans. R. Soc., A A353, 367 (1995).**
6. C. H. Bennett *et al.*, "Purification of noisy entanglement and faithful teleportation via noisy channels," **Phys. Rev. Lett. 76, 722 (1996).**
7. D. G. Cory *et al.*, "Experimental quantum error correction," **Phys. Rev. Lett. 81, 2152 (1998).**