

How Peter Shor Changed Physics



1994: “These algorithms take a number of steps **polynomial in the input size**, for example, the number of digits of the integer to be factored.”

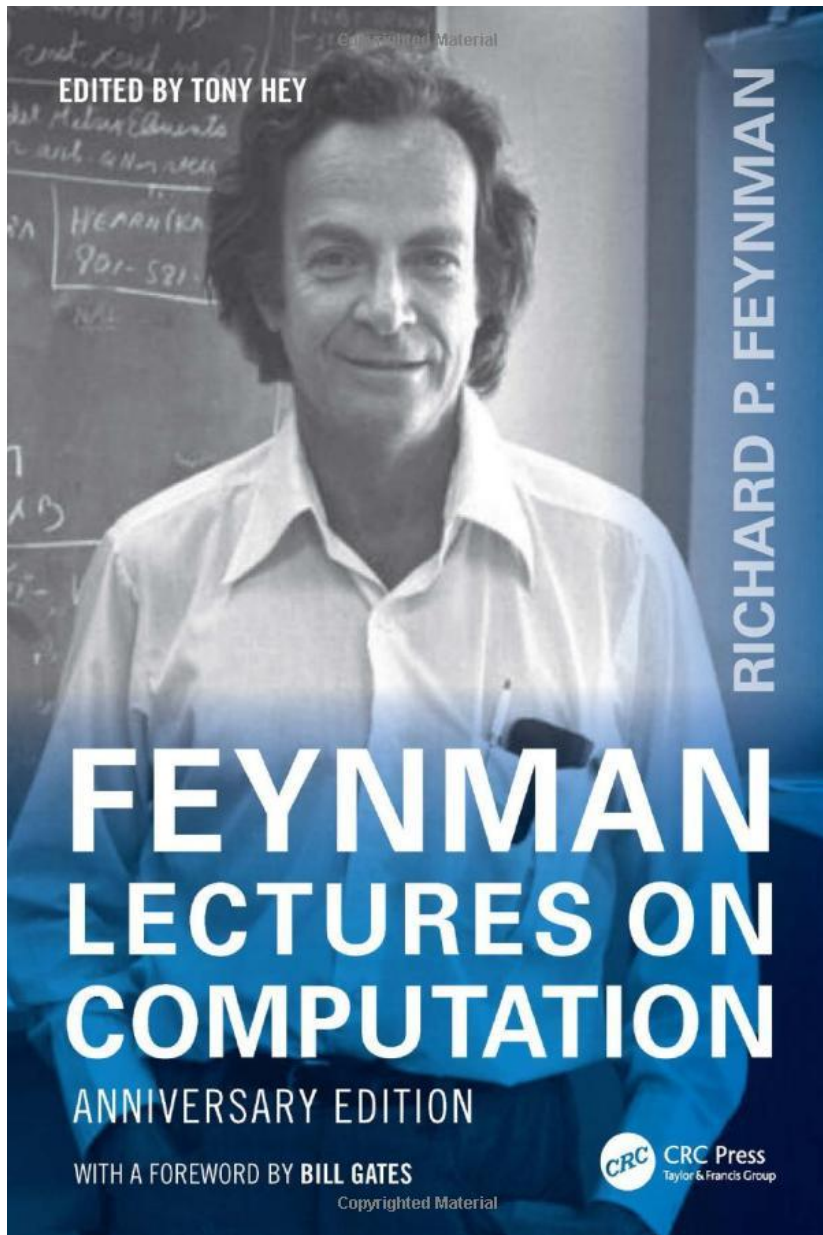
1995: “It is shown how to **reduce the effects of decoherence** for information stored in quantum memory, assuming that the decoherence process acts independently on each of the bits stored in memory.”

1996: “This paper shows both how to **correct errors in encoded qubits using noisy gates** and also how to compute on these encoded qubits without ever decoding the qubits.”

The underlying physical laws necessary for the mathematical theory of a large part of physics and the whole of chemistry are thus completely known, and the difficulty is only that **the exact application of these laws leads to equations much too complicated to be soluble.**

Paul A. M. Dirac, Quantum Mechanics of Many-Electron Systems, Proceedings of the Royal Society, 1929





Richard Feynman (1981)

“You can simulate this with a quantum system, with quantum computer elements. It’s not a Turing machine, but a machine of a different kind.”

Simulating Physics with Computers

Transcript of a talk at the Conference on the Physics of Computation, MIT 1981

Google Scholar > 12,000 citations (> 1100 in 2023)

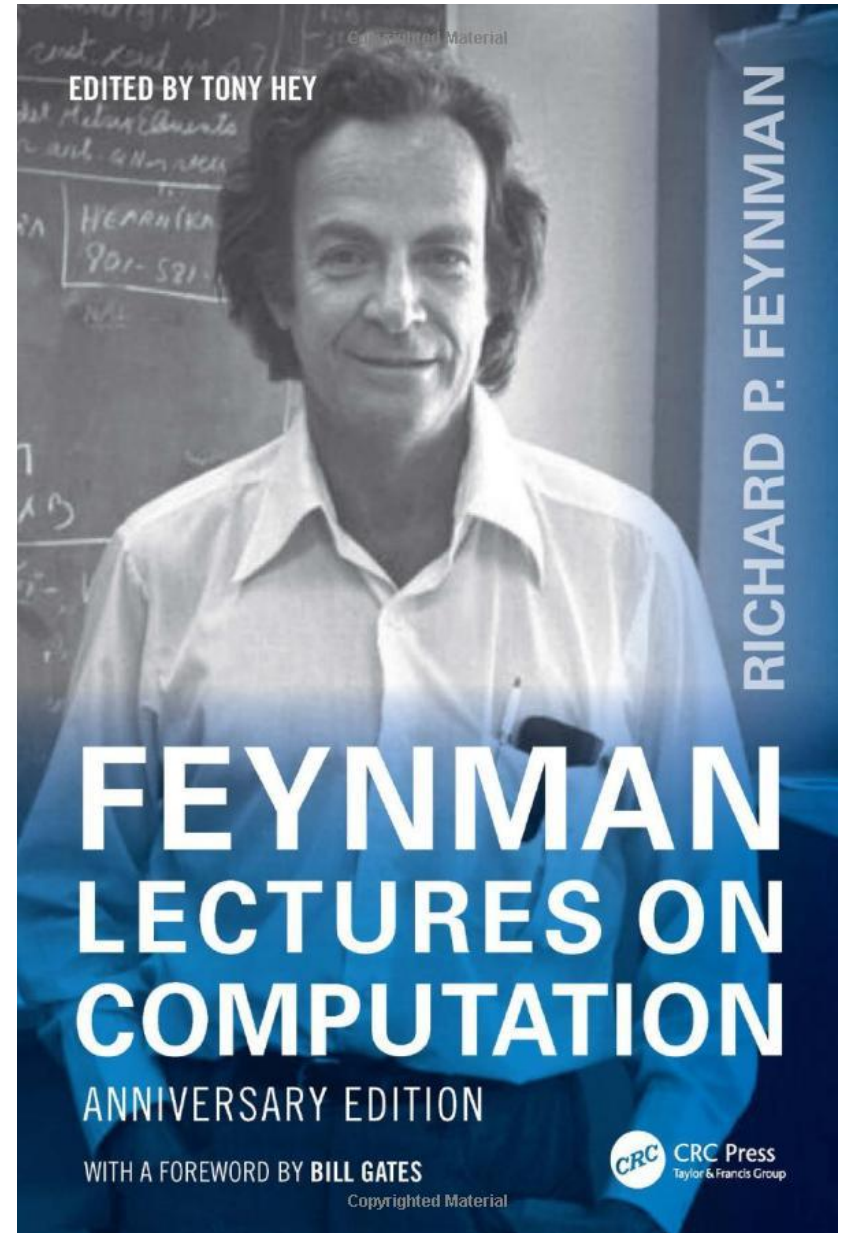
The goal: The rule of simulation that I would like to have is that **the number of computer elements required to simulate a large physical system is only to be proportional to the space-time volume of the physical system.**

Complexity: Now I explicitly go to the question of how we can simulate with a computer ... the quantum mechanical effects ... But the full description of quantum mechanics for a large system with R particles is given by a function which we call the amplitude to find the particles at x_1, \dots, x_R , and therefore because it has too many variables, ***it cannot be simulated with a normal computer.***

Quantum computing: Can you do it with a new kind of computer --- a quantum computer? Now it turns out, as far as I can tell, that **you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind.**

“Nature isn’t classical, dammit, and if you want to make a simulation of Nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem because it doesn’t look so easy.”

Richard Feynman
Simulating Physics with Computers
May 1981



Yuri Manin (1937-2023), *Computable and Uncomputable* (1980)

Translated from the Russian by Victor Albert

These objects [quantum automata] may show us mathematical models of deterministic processes with highly unusual features. One of the reasons for this is because **the quantum phase space is much bigger than classical**: where classical space has N discrete levels, a quantum system allowing their superposition will have c^N Planck cells. In a union of two classical systems, their sizes N_1 and N_2 multiply, but in the quantum case we have $c^{N_1+N_2}$.

These heuristic calculations point to a much larger potential complexity of the behavior of a quantum system when compared to its classical imitator.

Paul Benioff (1930-2022), *J. Stat. Phys.* 22, 563-591 (1980)

“These considerations suggest that it may be impossible even in principle to construct **a quantum mechanical Hamiltonian model of the computation process**. The reason is that any such model evolves as an isolated system with a constant total energy. The point of this paper is to suggest, by construction of such models, that this may not be the case.”

Note: Unlike Manin, Benioff was not concerned with quantum complexity. Rather, he mainly focused on the question whether a quantum computer can operate *without dissipation* (as did Feynman in his 1984 CLEO/IQEC talk on “Quantum Mechanical Computers”).



David Deutsch (1985)

“I describe the universal quantum computer, which is capable of perfectly simulating every finite, realizable physical system.



Umesh Vazirani

(1993)

“The study of the computational power of quantum Turing Machines gives a method of demonstrating, in a quantifiable way, **the inherent difference between the model proposed by quantum physics and *any* classical model.**”



Peter Shor

(1994)

“These algorithms take a number of steps polynomial in the input size, for example, the number of digits of the integer to be factored.”



Vazirani

I didn't think about quantum computing again until 1992, when Umesh Vazirani gave a talk at Bell Labs about his paper with Ethan Bernstein on quantum Turing machines ... I was really intrigued by that talk, and I probably understood it better than other computer scientists because of the amount of physics I'd taken in college.

I gave a talk [at Bell Labs] on how to solve discrete logarithms on a quantum computer, and it went well. Later that week, I was able to solve the factoring problem as well.



Shor

That weekend, when I was at home with a bad cold, Umesh Vazirani called me up and said “I hear that you can factor efficiently with a quantum computer.” This was surprising ... the talk had been about the discrete log algorithm, but by the time the rumors reached Umesh, they had changed into factoring ... But luckily, I had solved the factoring problem in the meantime ...

After that, the news spread like wildfire ...

Peter Shor, The early days of quantum computation, arXiv:2208.09964

Unruh, Physical Review A, Submitted June 1994

PHYSICAL REVIEW A

VOLUME 51, NUMBER 2

FEBRUARY 1995

Maintaining coherence in quantum computers

W. G. Unruh*

*Canadian Institute for Advanced Research, Cosmology Program, Department of Physics,
University of British Columbia, Vancouver, Canada V6T 1Z1*

(Received 10 June 1994)

The effects of the inevitable coupling to external degrees of freedom of a quantum computer are examined. It is found that for quantum calculations (in which the maintenance of coherence over a large number of states is important), not only must the coupling be small, but the time taken in the quantum calculation must be less than the thermal time scale $\hbar/k_B T$. For longer times the condition on the strength of the coupling to the external world becomes much more stringent.

PACS number(s): 03.65.-w

“The thermal time scale thus sets a (weak) limit on the length of time that a quantum calculation can take.”

Landauer, Philosophical Transactions, Published December 1995

THE ROYAL SOCIETY
PUBLISHING

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A

MATHEMATICAL, PHYSICAL AND ENGINEERING SCIENCES

[Home](#)

[Content](#)

[Information for](#)

[About us](#)

[Sign up](#)

[Propose an issue](#)



[Is Quantum Mechanics Useful?](#)

Rolf Landauer

Published 15 December 1995. DOI: 10.1098/rsta.1995.0106

“...small errors will accumulate and cause the computation to go off track.”

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-197, 600 Mountain Avenue, Murray Hill, New Jersey 07974

(Received 17 May 1995)

Combining repetition codes for bit flips and phase errors (Shor code).

PHYSICAL REVIEW LETTERS

VOLUME 77

29 JULY 1996

NUMBER 5

Error Correcting Codes in Quantum Theory

A. M. Steane

Clarendon Laboratory, Parks Road, Oxford, OX1 3PU, England

(Received 4 October 1995)

A quantum version of the classical Hamming code (Steane code).

Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels

Charles H. Bennett,^{1,*} Gilles Brassard,^{2,†} Sandu Popescu,^{3,‡} Benjamin Schumacher,^{4,§}
John A. Smolin,^{5,||} and William K. Wootters^{6,¶}

¹*IBM Research Division, Yorktown Heights, New York 10598*

²*Département IRO, Université de Montréal, C.P. 6128, Succursale centre-ville, Montréal, Québec, Canada H3C 3J7*

³*Physics Department, Tel Aviv University, Tel Aviv, Israel*

⁴*Physics Department, Kenyon College, Gambier, Ohio 43022*

⁵*Physics Department, University of California at Los Angeles, Los Angeles, California 90024*

⁶*Physics Department, Williams College, Williamstown, Massachusetts 01267*

(Received 24 April 1995)

Two separated observers, by applying local operations to a supply of not-too-impure entangled states (e.g., singlets shared through a noisy channel), can prepare a smaller number of entangled pairs of arbitrarily high purity (e.g., near-perfect singlets). These can then be used to faithfully teleport unknown quantum states from one observer to the other, thereby achieving faithful transmission of quantum information through a noisy channel. We give upper and lower bounds on the yield $D(M)$ of pure singlets ($|\Psi^-\rangle$) distillable from mixed states M , showing $D(M) > 0$ if $\langle \Psi^- | M | \Psi^- \rangle > \frac{1}{2}$.

PACS numbers: 03.65.Bz, 42.50.Dv, 89.70.+c

Entanglement purification and teleportation for faithful transmission of quantum information through noisy channels.

Good quantum error-correcting codes exist

A. R. Calderbank and Peter W. Shor
AT&T Research, 600 Mountain Avenue, Murray Hill, New Jersey 07974
(Received 12 September 1995)

**Multiple-particle interference and
quantum error correction**

BY ANDREW STEANE

*Department of Atomic and Laser Physics, Clarendon Laboratory,
Parks Road, Oxford OX1 3PU, UK*
a.steane@physics.oxford.ac.uk

Proceedings of the Royal Society A, Received 27 November 1995, Published 8 November 1996

[Calderbank-Shor-Steane \(CSS\) Codes: the first family of good quantum codes.](#)

Author: Steane

Title: Multiple particle interference and quantum error correction

Manuscript Number: 95PA342

This paper is a major contribution to quantum information theory, one of the most significant in recent years. It contains deep and surprising new results, and it is clearly written. Without question, it is worthy of publication in the Proceedings.

Class of quantum error-correcting codes saturating the quantum Hamming boundDaniel Gottesman^{*}*California Institute of Technology, Pasadena, California 91125*

(Received 29 April 1996)

I develop methods for analyzing quantum error-correcting codes, and use these methods to construct an infinite class of codes saturating the quantum Hamming bound. These codes encode $k=n-j-2$ quantum bits (qubits) in $n=2^j$ qubits and correct $t=1$ error. [S1050-2947(96)09309-2]

PACS number(s): 03.65.Bz, 89.80.+h

Quantum Error Correction and Orthogonal GeometryA. R. Calderbank,¹ E. M. Rains,² P. W. Shor,¹ and N. J. A. Sloane¹¹*AT&T Labs—Research, Murray Hill, New Jersey 07974*²*Institute for Defense Analyses, Princeton, New Jersey 08540*

(Received 9 May 1996; revised manuscript received 3 July 1996)

A group theoretic framework is introduced that simplifies the description of known quantum error-correcting codes and greatly facilitates the construction of new examples. Codes are given which map 3 qubits to 8 qubits correcting 1 error, 4 to 10 qubits correcting 1 error, 1 to 13 qubits correcting 2 errors, and 1 to 29 qubits correcting 5 errors. [S0031-9007(96)02177-1]

**Quantum stabilizer codes:
the quantum analogue of additive classical codes.**

Fault-tolerant quantum computation

Peter W. Shor (AT&T Research)

(Submitted on 13 May 1996 (v1), last revised 5 Mar 1997 (this version, v2))

Recently, it was realized that use of the properties of quantum mechanics might speed up certain computations dramatically. Interest in quantum computation has since been growing. One of the main difficulties of realizing quantum computation is that decoherence tends to destroy the information in a superposition of states in a quantum computer, thus making long computations impossible. A further difficulty is that inaccuracies in quantum state transformations throughout the computation accumulate, rendering the output of long computations unreliable. It was previously known that a quantum circuit with t gates could tolerate $O(1/t)$ amounts of inaccuracy and decoherence per gate. We show, for any quantum computation with t gates, how to build a polynomial size quantum circuit that can tolerate $O(1/(\log t)^c)$ amounts of inaccuracy and decoherence per gate, for some constant c . We do this by showing how to compute using quantum error correcting codes. These codes were previously known to provide resistance to errors while storing and transmitting quantum data.

Comments: Latex, 11 pages, no figures, in 37th Symposium on Foundations of Computing, IEEE Computer Society Press, 1996, pp. 56-65

Fault-tolerant syndrome measurement,
using encoded ancillas, verified offline.

Universal gates acting on encoded quantum data,
using “magic states” verified offline.

Threshold Accuracy for Quantum Computation

E. Knill, R. Laflamme, W. Zurek

(Submitted on 8 Oct 1996 (v1), last revised 15 Oct 1996 (this version, v3))

We have previously ([quant-ph/9608012](#)) shown that for quantum memories and quantum communication, a state can be transmitted over arbitrary distances with error ϵ provided each gate has error at most $c\epsilon$. We discuss a similar concatenation technique which can be used with fault tolerant networks to achieve any desired accuracy when computing with classical initial states, provided a minimum gate accuracy can be achieved. The technique works under realistic assumptions on operational errors. These assumptions are more general than the stochastic error heuristic used in other work. Methods are proposed to account for leakage errors, a problem not previously recognized.

Fault Tolerant Quantum Computation with Constant Error

Dorit Aharonov (Physics and computer science, Hebrew Univ.), Michael Ben-Or (Computer science, Hebrew univ.)

(Submitted on 14 Nov 1996 (v1), last revised 15 Nov 1996 (this version, v2))

Recently Shor showed how to perform fault tolerant quantum computation when the error probability is logarithmically small. We improve this bound and describe fault tolerant quantum computation when the error probability is smaller than some constant threshold. The cost is polylogarithmic in time and space, and no measurements are used during the quantum computation. The result holds also for quantum circuits which operate on nearest neighbors only. To achieve this noise resistance, we use concatenated quantum error correcting codes. The scheme presented is general, and works with all quantum codes that satisfy some restrictions, namely that the code is "proper".

Scalable
quantum
computing
using recursive
simulations.

Haroche and Raimond, Physics Today, Published August 1996

QUANTUM COMPUTING: DREAM OR NIGHTMARE?

The principles of quantum computing were laid out about 15 years ago by computer scientists applying the superposition principle of quantum mechanics to computer operation. Quantum computing has recently become a hot topic in physics, with the recognition that a two-level system can be pre-

Recent experiments have deepened our insight into the wonderfully counterintuitive quantum theory. But are they really harbingers of quantum computing? We doubt it.

Serge Haroche and Jean-Michel Raimond

two interacting qubits: a “control” bit and a “target” bit. The control remains unchanged, but its state determines the evolution of the target: If the control is 0, nothing happens to the target; if it is 1, the target undergoes a well-defined transformation.

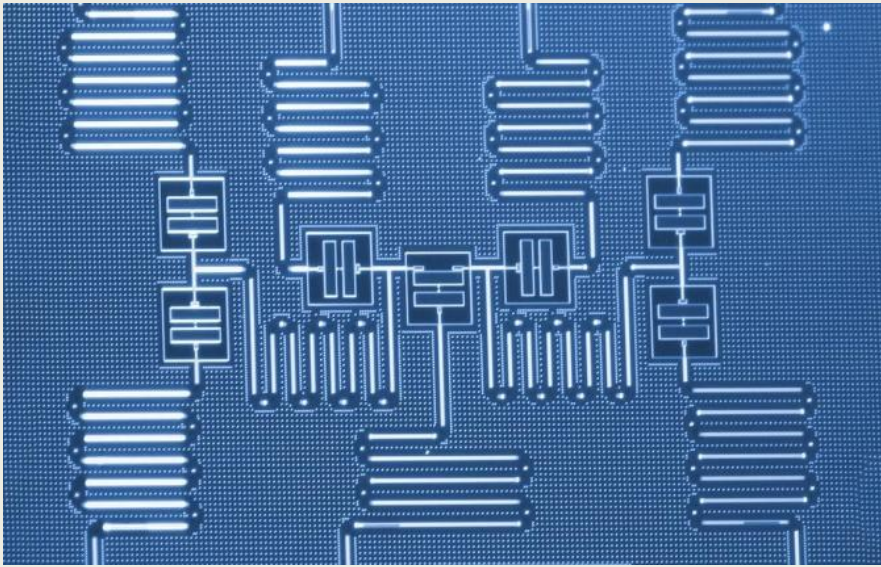
Quantum mechanics admits additional options. If

Therefore we think it fair to say that, unless some unforeseen new physics is discovered, the implementation of error-correcting codes will become exceedingly difficult as soon as one has to deal with more than a few gates. In this sense the large-scale quantum machine, though it may be the computer scientist's dream, is the experimenter's nightmare.

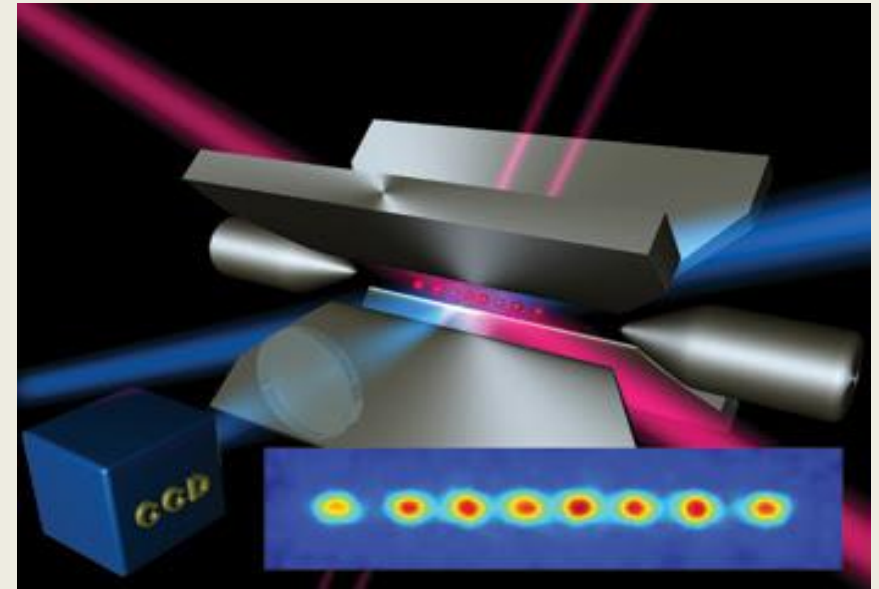


Alexei Kitaev (1997)

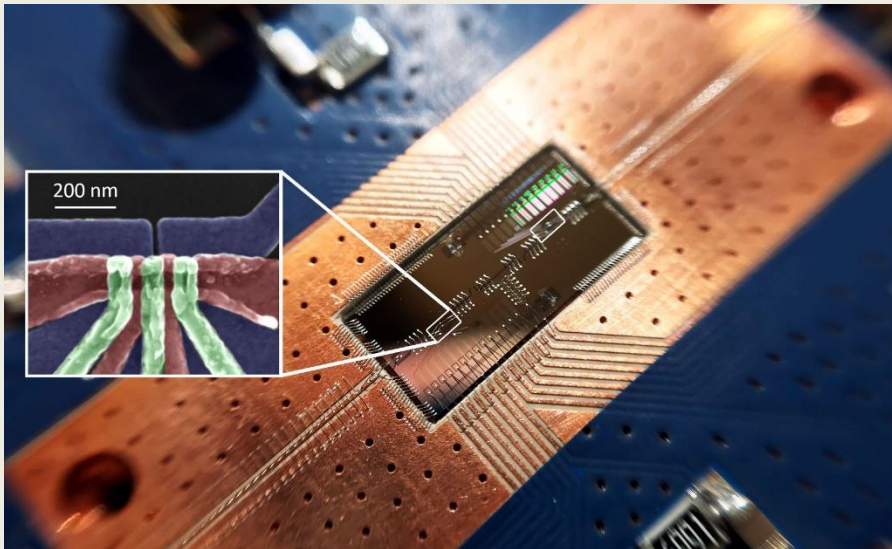
“Such computation is
fault-tolerant by its
physical nature.”



superconducting qubits



trapped atoms/ions



spin qubits



photonics

Open Questions

How will we scale up to quantum computing systems that can solve hard problems?

What are the important applications for science and for industry?

Applications: Looking ahead

Optimization, finance, and machine learning. Typical quantum speedups are at best quadratic. Quantum advantage kicks in for very large problem instances and deep circuits.

Quantum many-body physics: Chemistry and materials. Hundreds of logical qubits, hundreds of millions of logical gates or more.

Quantum fault tolerance needed to run these applications. High cost in physical qubits and gates.

Logical gate speed is also important. Run time on the wall clock.

Overcoming noise in quantum devices

Quantum error mitigation. Used effectively in current processors. Asymptotic overhead cost scales exponentially.

Quantum error correction. Asymptotic overhead cost scales polylogarithmically. Not yet effective in current processors.

What we need. Better two-qubit gate fidelities, *many* more physical qubits, and the ability to control them. Also fast gates, mid-circuit readout, feed-forward, reset.

An exciting time for Rydberg atom arrays!

May lead the progress in quantum error correction for the next few years, if two-qubit gate fidelities continue to improve.

Thousands of qubits, movement of atoms enables geometrically nonlocal operations and syndrome measurements [*Harvard/MIT/QuEra*].

Further improvement from erasure conversion [*Princeton/Caltech*].

Repeated syndrome measurement yet to be demonstrated.

Continuous loading of fresh atoms will be needed.

Atomic movement and readout are relatively slow.

Quantum Information Physics

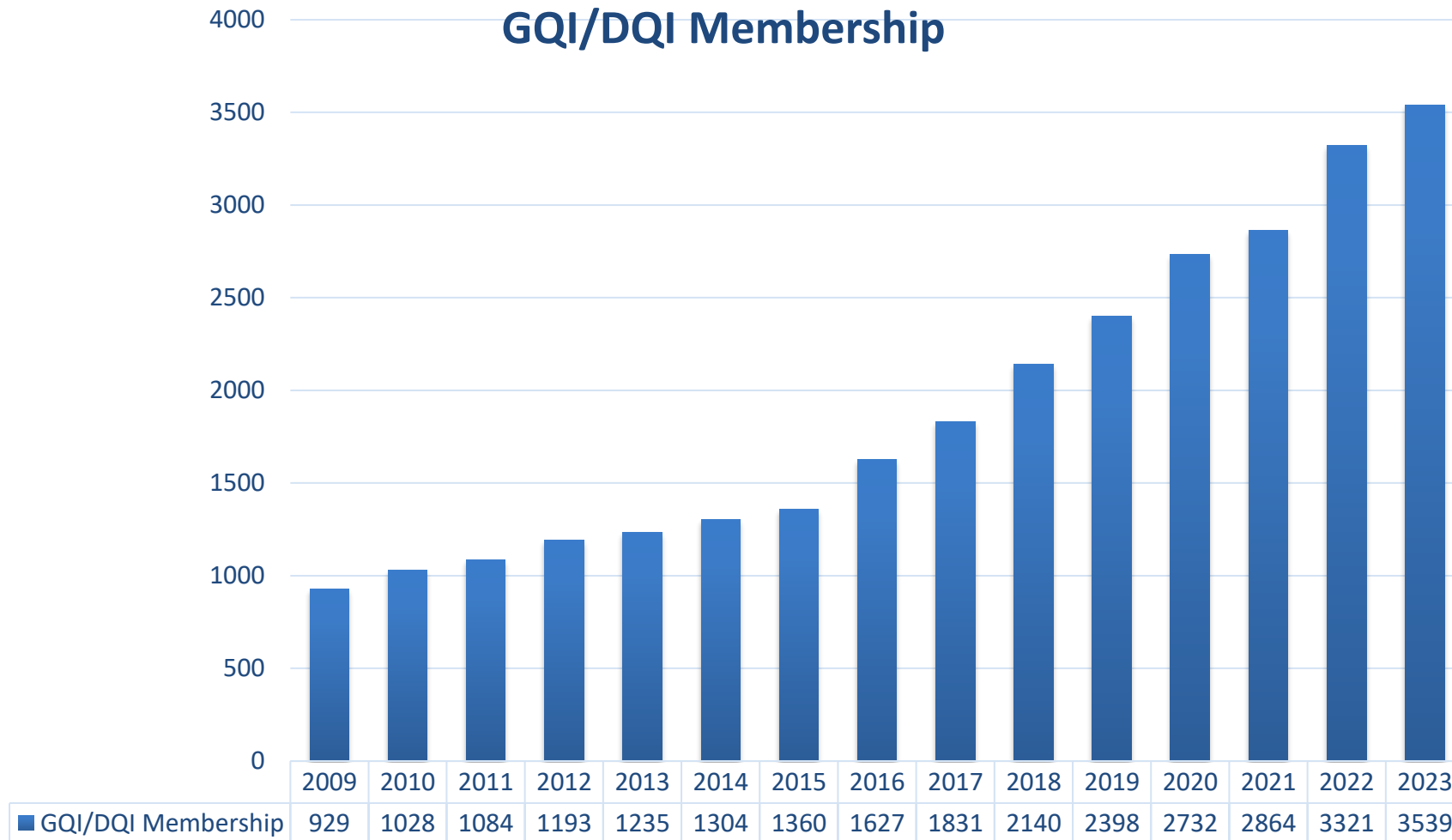
Information scrambling: quantum circuits, chaotic dynamics, black holes, ...

Quantum error correction: scalable computing, topological phases of matter, holographic correspondence.

Computational complexity: hardness of computational problems, preparing quantum phases of matter, geometry of the black hole interior.

Lots more.

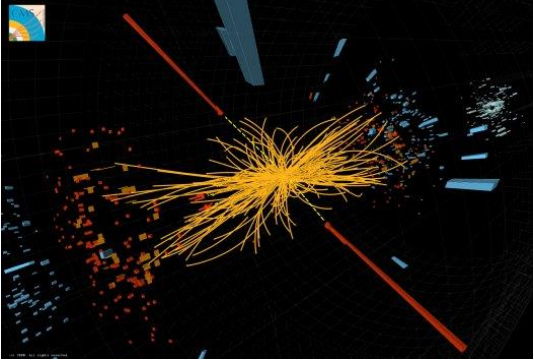

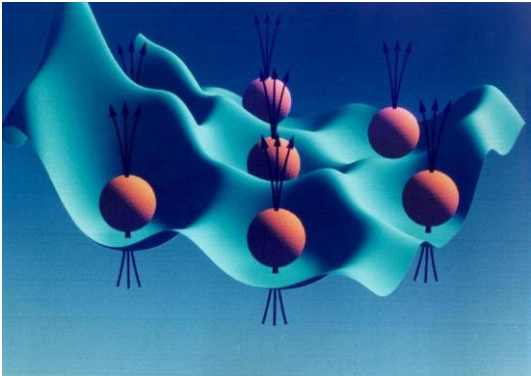
APS Division of Quantum Information



<http://www.aps.org/membership/units/statistics.cfm>

(Founded 2005. Now 7.1% of APS. **Membership is 57% students.**)

Frontiers of Physics

short distance	long distance	complexity
		
<p>Higgs boson</p> <p>Neutrino masses</p> <p>Supersymmetry</p> <p>Quantum gravity</p> <p>String theory</p>	<p>Large scale structure</p> <p>Cosmic microwave background</p> <p>Dark matter</p> <p>Dark energy</p> <p>Gravitational waves</p>	<p>“More is different”</p> <p>Many-body entanglement</p> <p>Phases of quantum matter</p> <p>Quantum computing</p> <p>Quantum spacetime</p>

How Peter Shor Changed Physics



1994: “These algorithms take a number of steps **polynomial in the input size**, for example, the number of digits of the integer to be factored.”

1995: “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.”

1996: “This paper shows both how to **correct errors in encoded qubits using noisy gates** and also how to compute on these encoded qubits without ever decoding the qubits.”