

# Michael Ben-Or Corrects Errors



John Preskill, Caltech  
Workshop in Honor of Michael Ben-Or  
Simons Institute, 25 March 2024

In Dec 2002, Michael and I attended the QIP conference at MSRI in Berkeley. (We both spoke about the security of quantum key distribution.) We drove in my rental car to a dinner in San Francisco.

The car was equipped with a GPS navigation system, a novelty at that time. GPS was less reliable back then. I trusted the nav, but Michael was more cautious.

At one point, the nav directed me to drive off the road, into San Francisco Bay, and I obediently followed.

Michael, correcting my error, saved the day by crying “Stop!”

ChatGPT prompt: Create an image portraying John Preskill and Michael Ben-Or about to drive a car off the road and into San Francisco Bay. It is nighttime and both are terrified.



# The 31st Jerusalem Winter School in Theoretical Physics: Frontiers of Quantum Information Science

Mon, 30/12/2013 to Thu, 09/01/2014

## Frontiers of Quantum Information Science

All lectures will take place at the Israel Institute for Advanced Studies,  
at the Edmond J. Safra, Givat Ram Campus

**General Director:** David Gross, University of California at Santa Barbara

**Director:** John Preskill, Caltech

**Co-directors:**

Michael Ben-Or, The Hebrew University

Patrick Hayden, Stanford University

In 2005, Caltech's Institute for Quantum Information hosted a workshop that brought together classical and quantum cryptographers, which Michael attended.



Conversation between quantumists during a break:

A: What do you do when [classical cryptographer] X uses terminology you don't know?

B: I look it up on Google. What about you?

A: I ask Michael Ben-Or.

B: Yes! Michael is as good as Google.

A: He's better than Google!

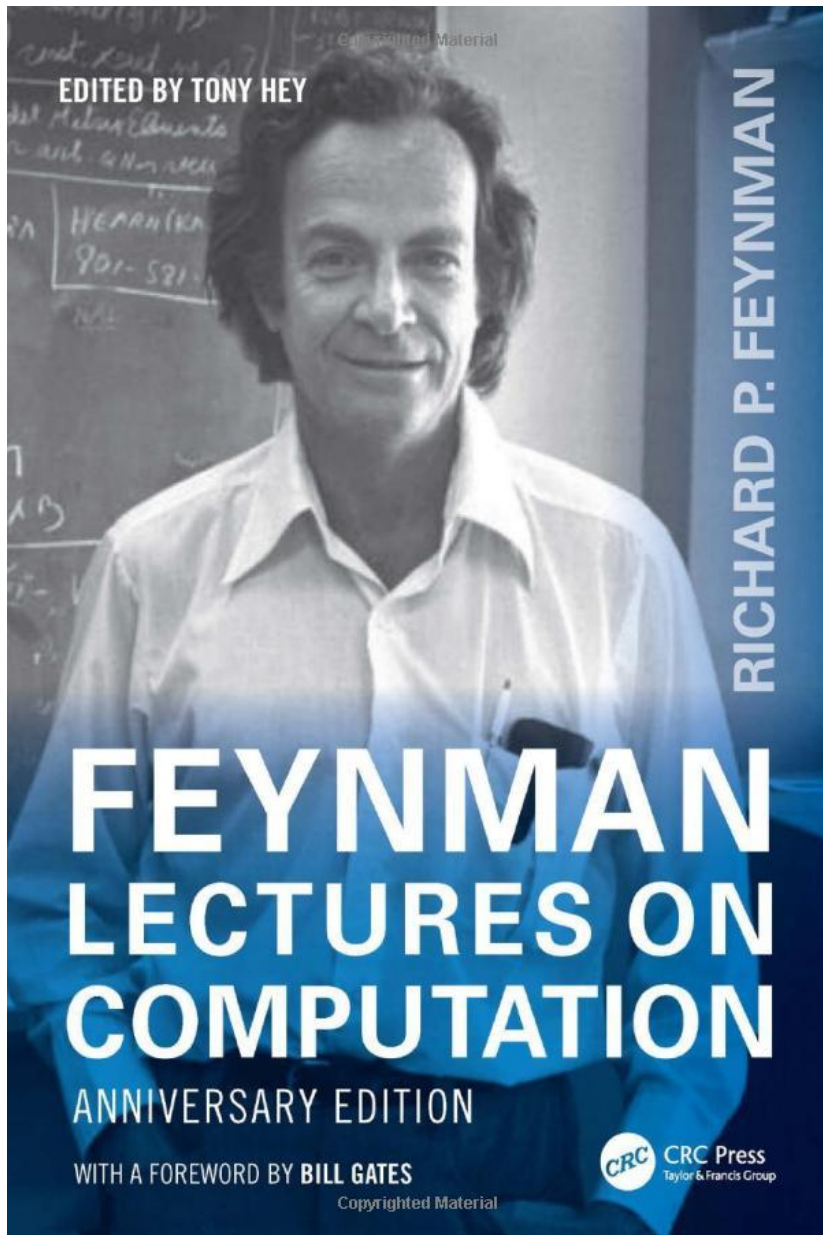
Michael (overhearing): I look up the answer using Google on my laptop.

(He is self-effacing, too.)

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*



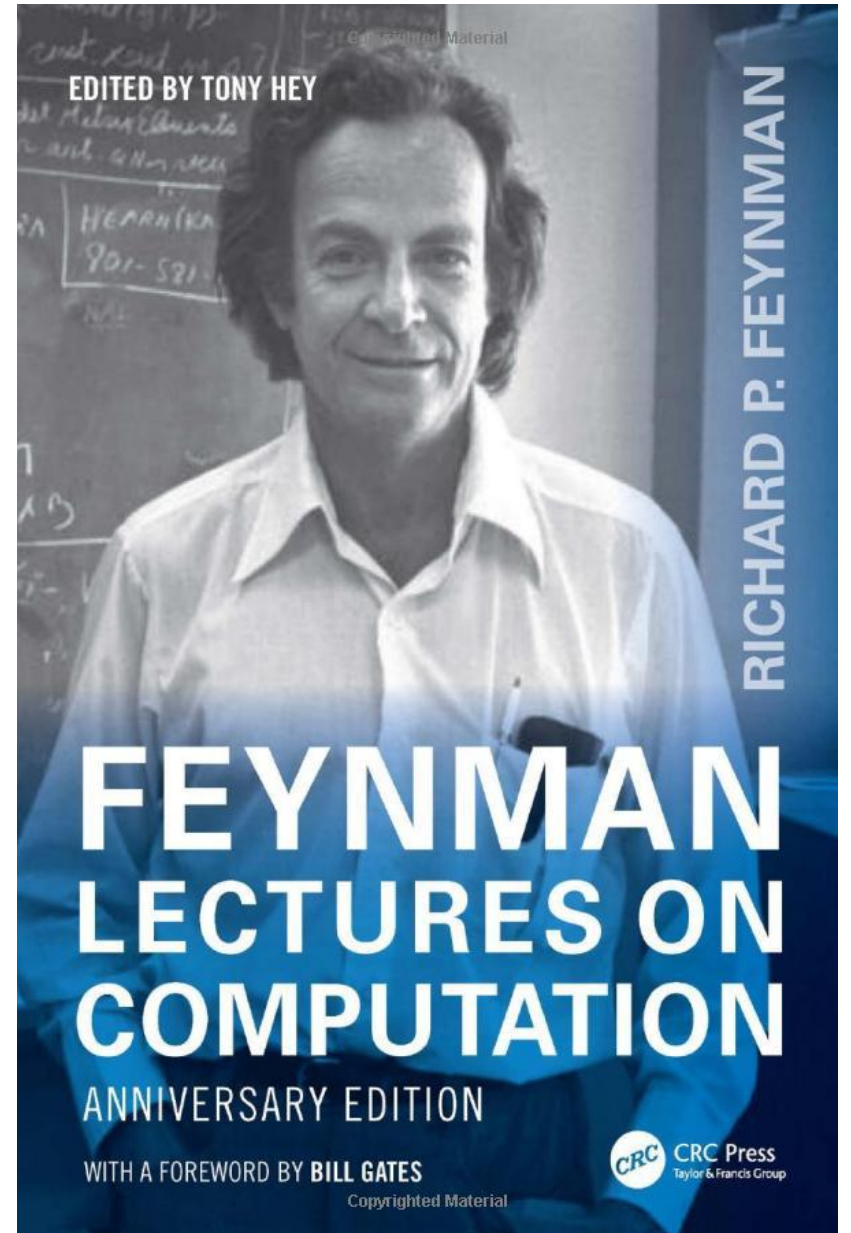


# Richard Feynman (1981)

“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.”

“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*





# 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.”



# 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-219, 600 Mountain View Road, 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,<sup>1,\*</sup> Gilles Brassard,<sup>2,†</sup> Sandu Popescu,<sup>3,‡</sup> Benjamin Schumacher,<sup>4,§</sup>  
John A. Smolin,<sup>5,||</sup> and William K. Wootters<sup>6,¶</sup>

<sup>1</sup>*IBM Research Division, Yorktown Heights, New York 10598*

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

<sup>3</sup>*Physics Department, Tel Aviv University, Tel Aviv, Israel*

<sup>4</sup>*Physics Department, Kenyon College, Gambier, Ohio 43022*

<sup>5</sup>*Physics Department, University of California at Los Angeles, Los Angeles, California 90024*

<sup>6</sup>*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 bound**Daniel Gottesman<sup>\*</sup>*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 Geometry**A. R. Calderbank,<sup>1</sup> E. M. Rains,<sup>2</sup> P. W. Shor,<sup>1</sup> and N. J. A. Sloane<sup>1</sup><sup>1</sup>*AT&T Labs—Research, Murray Hill, New Jersey 07974*<sup>2</sup>*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.

## Fault Tolerant Quantum Computation with Constant Error

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

Scalable quantum computing  
using recursive simulations.  
(Aharonov and Ben-Or, November 1996)

“This paper ... shows how to perform fault tolerant quantum computation when the error probability is smaller than some constant threshold. The cost is polylogarithmic in time and space.”

“Hopefully, this paper motivates a search for proper quantum codes with higher thresholds, at which point quantum computation becomes practical.”





# 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

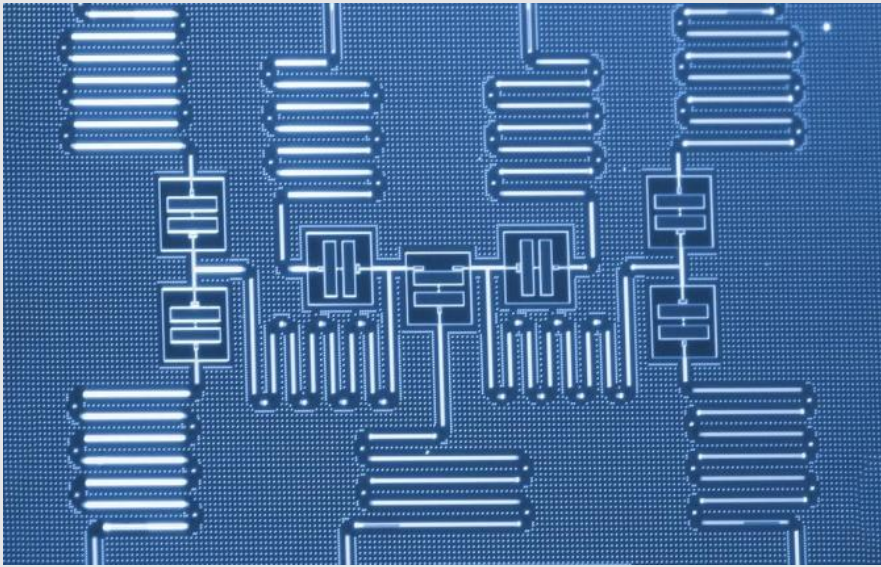
two interacting qubits: a “control” bit and a “target” bit. The control remains unchanged, but its state determines the evolution of the target: If the control is 0, nothing happens to the target; if it is 1, the target undergoes a well-defined transformation. Quantum mechanics admits additional options.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

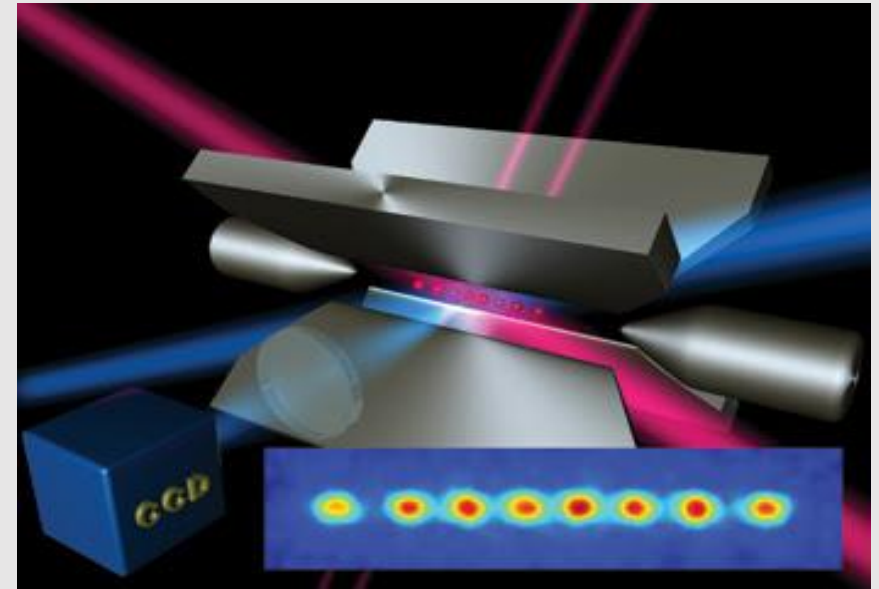


# Alexei Kitaev (1997)

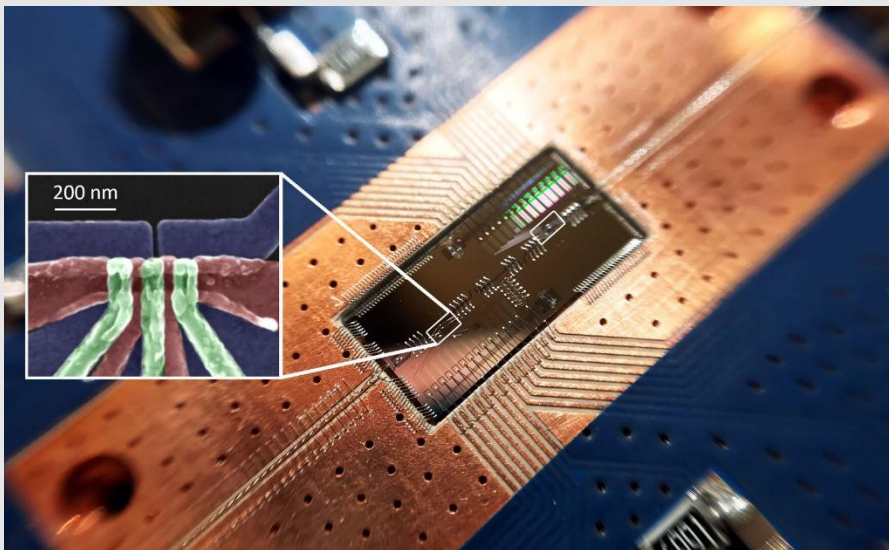
“Such computation is  
fault-tolerant by its  
physical nature.”



superconducting qubits



trapped atoms/ions



spin qubits



photonics

# Overhead cost of fault tolerance

$$P_{\text{logical}} \approx C \left( P_{\text{physical}} / P_{\text{threshold}} \right)^{(d+1)/2}$$

$$d = \sqrt{n}, \quad C \approx 0.1, \quad P_{\text{threshold}} \approx .01$$

Surface code

Suppose  $P_{\text{physical}} = .001, P_{\text{logical}} = 10^{-11}$

$\Rightarrow d = 19, n = 361$  physical qubits per logical qubit

(plus a comparable number of ancilla qubits for syndrome measurement). (Improves to  $d = 9$  for  $P_{\text{physical}} = 10^{-4}$ .)

# Progress toward QEC

**Erasure conversion.** Dominant errors occur at known locations, hence easier to correct.

**Biased noise.** Physical suppression of bit flips, error-correcting codes for the phase flips.

**More efficient codes.** But geometrically nonlocal syndrome measurements required.

**Co-design.** Adapt the coding to the hardware, adapt the hardware to the code.

# 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?

# The most important ideas in physics in the past 40 years?

1. The holographic principle (1994)
2. Topological quantum order (1989)
3. Quantum error correction (1995)

All three ideas are closely related!

The common thread: many-particle quantum entanglement.

# Quantum error correction

Quantum bits (qubits) tend to be very fragile, but  $k$  bits that are cleverly encoded in  $n \gg k$  qubits can be stored and processed reliably.

We can control the behavior of large-scale quantum systems, including powerful quantum computers.



# Topological Quantum Order

Quantum phases of matter that look identical when observed locally can be distinguished by their global properties.

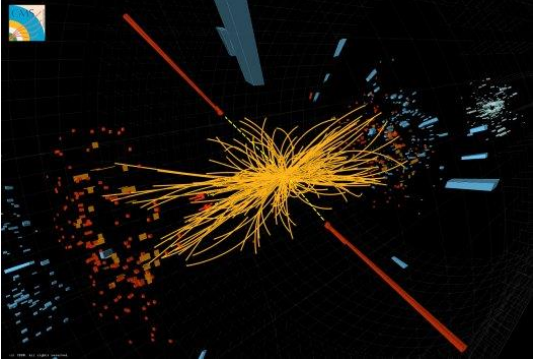

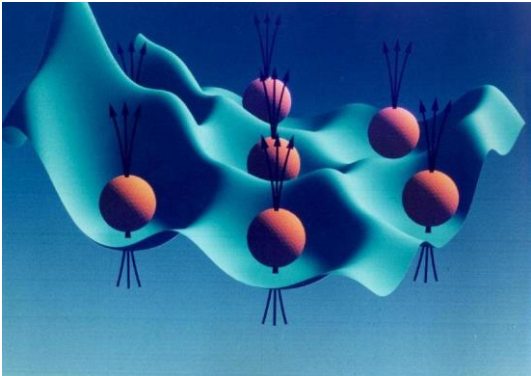
An electron in a topological phase can split into pieces, each carrying a fraction of the electron's charge.

# The Holographic Principle

All the information contained in a three-dimensional region of space is encoded on the two-dimensional boundary of the region.

Our most important clue about how to reconcile quantum mechanics with gravitational physics.

# 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>

# Michael Ben-Or Corrects Errors

