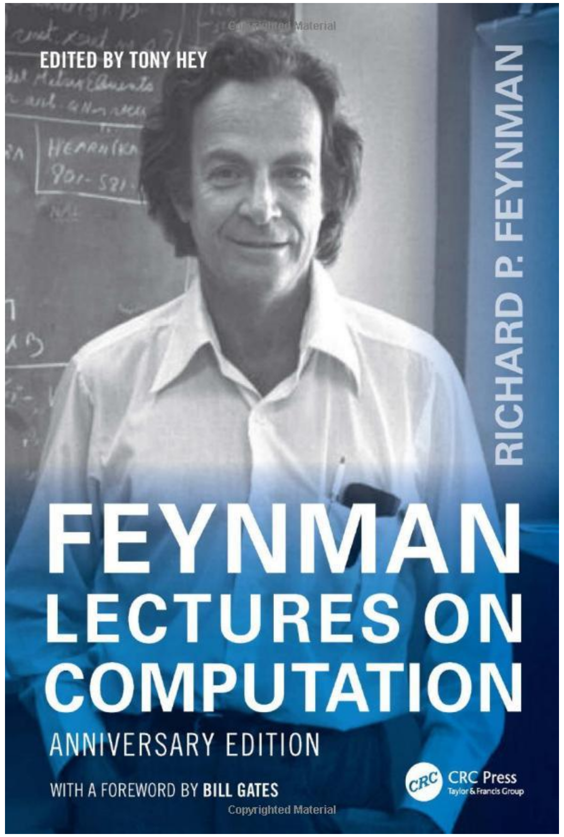
Quantum Computing 44 years later

Feynman in 1984

Richard Feynman, May 1981:
"By golly it's a wonderful problem because it doesn't look so easy."



aws

IQIM
INSTITUTE FOR QUANTUM INFORMATION AND MATTER

John Preskill

Qiskit Global Summer School

8 July 2025

CALIFORNIA INSTITUTE OF TECHNOLOGY 1891

@preskill

Quantum computing 40 years later

John Preskill

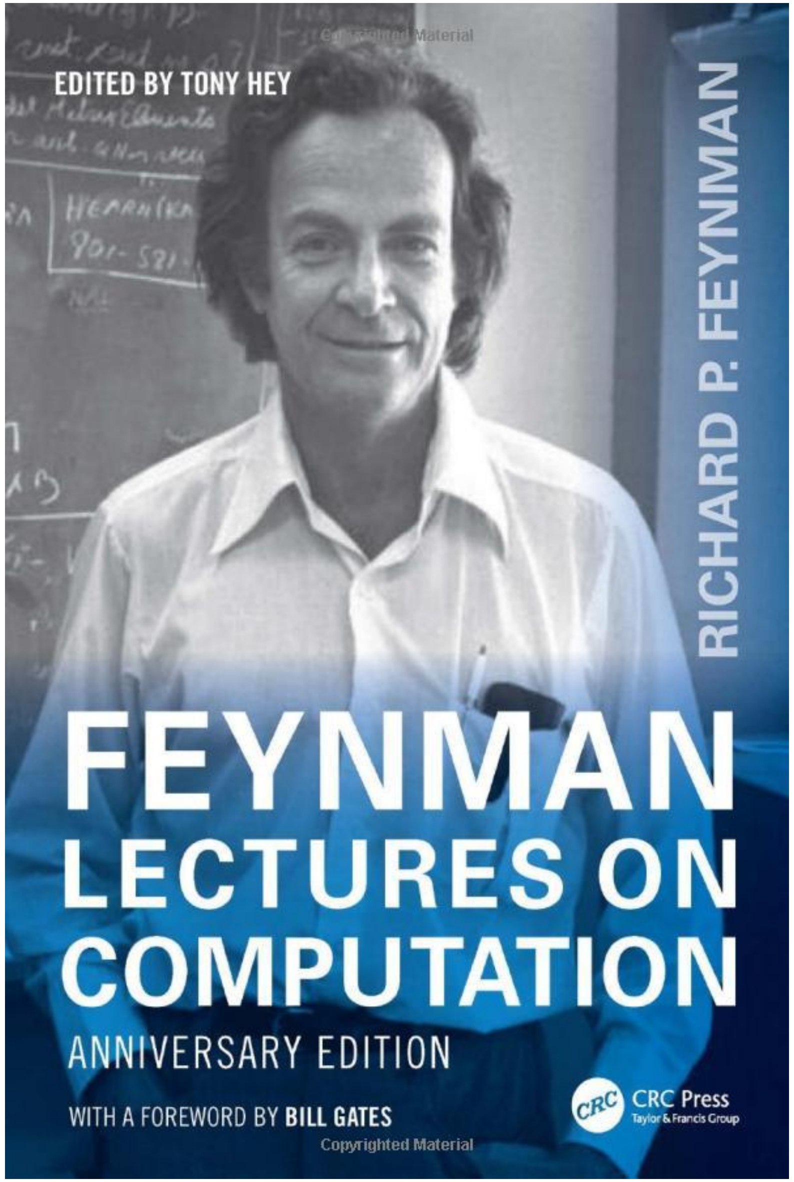
Institute for Quantum Information and Matter
California Institute of Technology, Pasadena CA 91125, USA
AWS Center for Quantum Computing, Pasadena CA 91125, USA

6 June 2021

Abstract

Forty years ago, Richard Feynman proposed harnessing quantum physics to build a more powerful kind of computer. Realizing Feynman's vision is one of the grand challenges facing 21st century science and technology. In this article, we'll recall Feynman's contribution that launched the quest for a quantum computer, and assess where the field stands 40 years later. To appear in *Feynman Lectures on Computation, 2nd edition*, published by Taylor & Francis Group, edited by Anthony J. G. Hey.

arXiv:2106.10522
In Feynman Lectures on Computation
2nd Edition



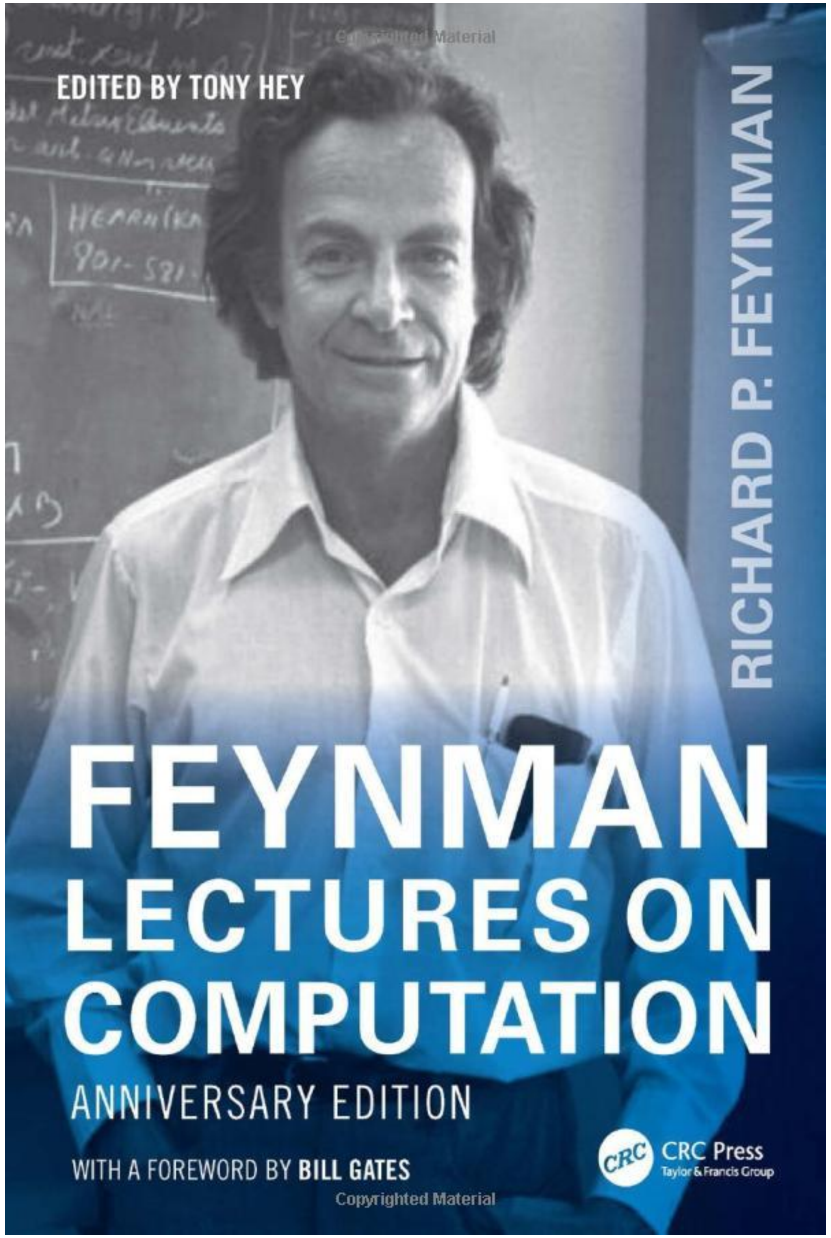
On June 6, 1925, a swollen-faced, stuffy-nosed Werner Heisenberg, then 23 years old and suffering from hay fever, left his home in central Germany for the fresh air of the North Sea island of Helgoland, hoping for relief. There, he had a breakthrough, becoming the first to articulate a mathematical framework of quantum mechanics and resolve the then-glaring contradictions of quantum theory.

APS News, 1 July 2025

Heisenberg in the 1920s

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 > 14,000 citations (> 1400 in 2024)

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 $x_1, \ldots, x_R$, 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.

Simulating Physics with Computers

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

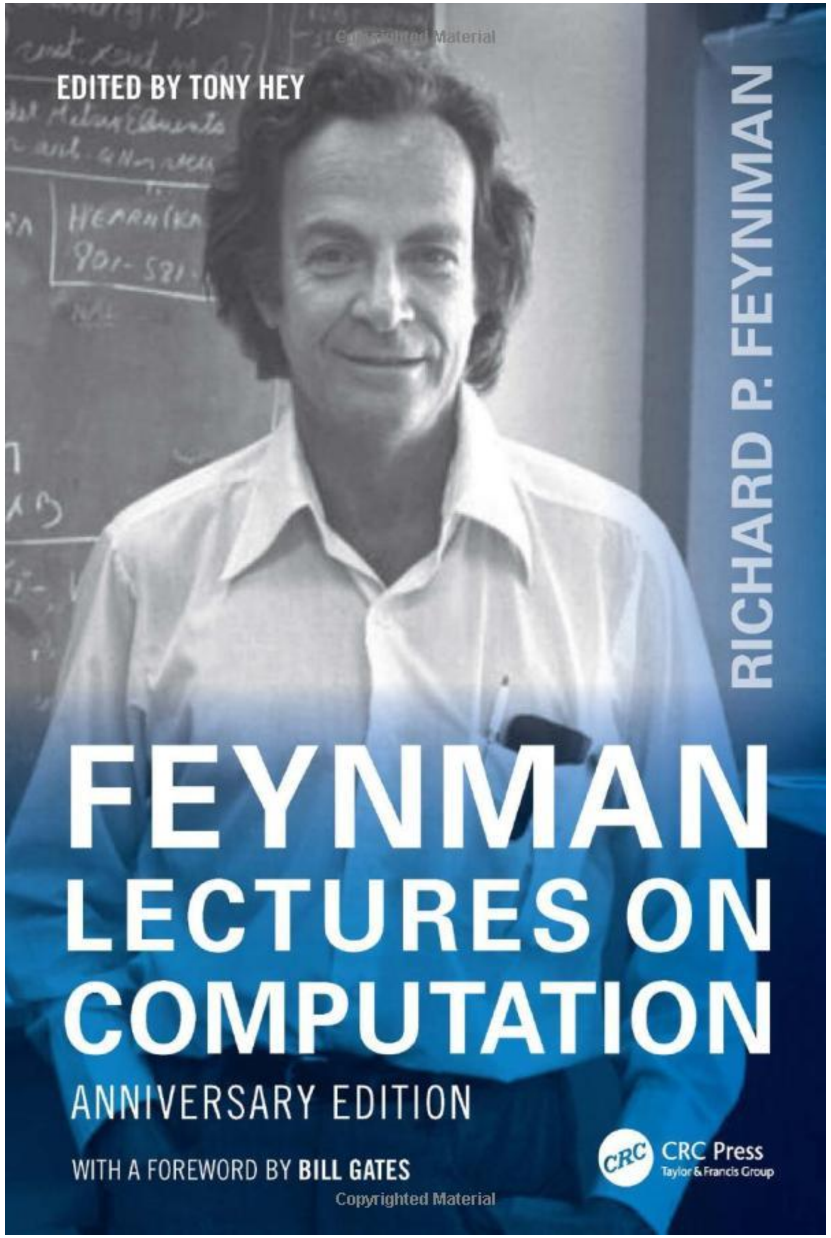
Much of the talk addresses the question: Can Quantum Systems be Probabilistically Simulated by a Classical Computer?

“If you take the computer to be the classical kind I’ve described so far (not the quantum kind described in the last section) and there’re no changes in any laws, and there’s no hocus-pocus, the answer is certainly, “No!” This is called the hidden variable problem: It is impossible to represent the results of quantum mechanics with a classical universal device.”

There follows a lucid discussion of Bell inequalities and the experimental evidence that they are violated. There are no references, and Bell is never mentioned!

“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^{N1+N2}.

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").

There's Plenty of Room at the Bottom

Transcript of a talk at the APS Annual Meeting, Caltech 1959

(Google Scholar ~ 7700 citations)

Future computers: If they had millions of times as many elements, they could make judgements … In many ways, they would have new qualitative features … There is nothing that I can see in the physical laws that says computer elements cannot be made enormously smaller than they are now. In fact, there may be certain advantages.

Atom-by-atom assembly: All our devices can be mass produced so that they are absolutely perfect copies of one another … The principles of physics, as far as I can see, do not speak against the possibility of maneuvering things atom by atom.

David Deutsch

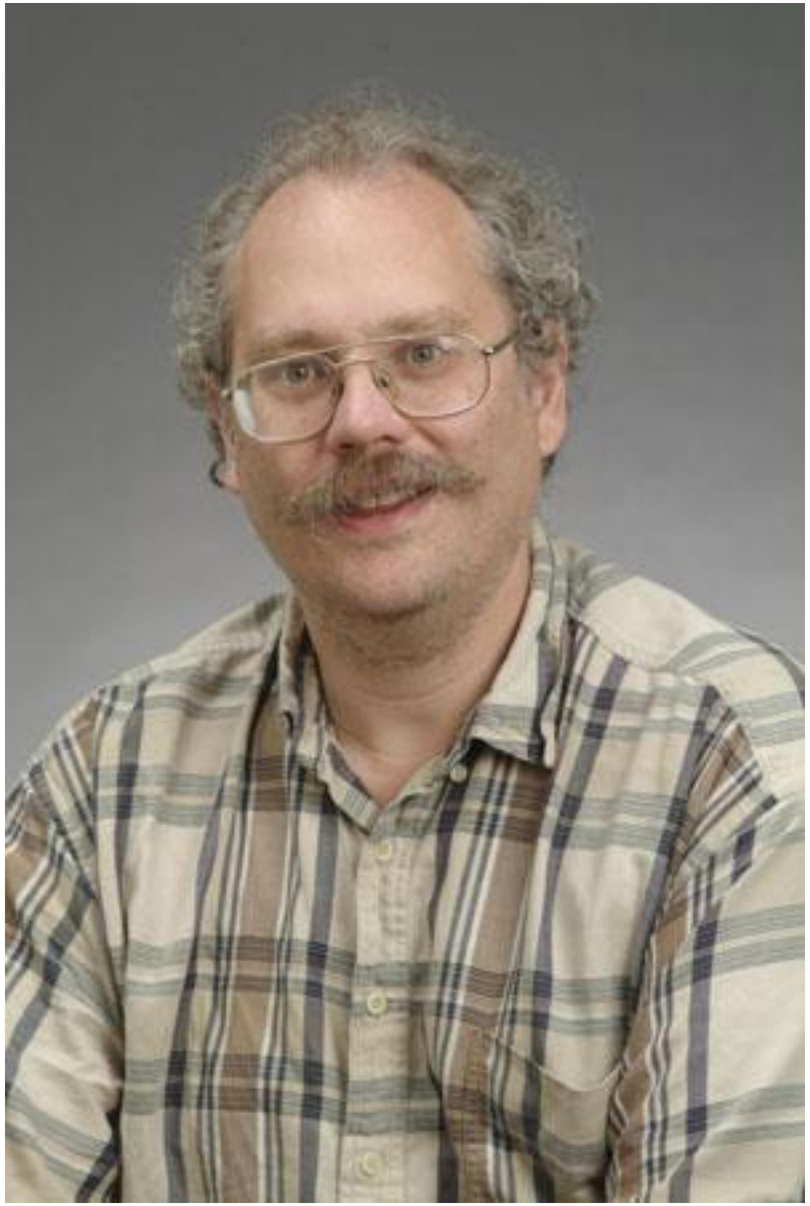
(1985)

“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 …

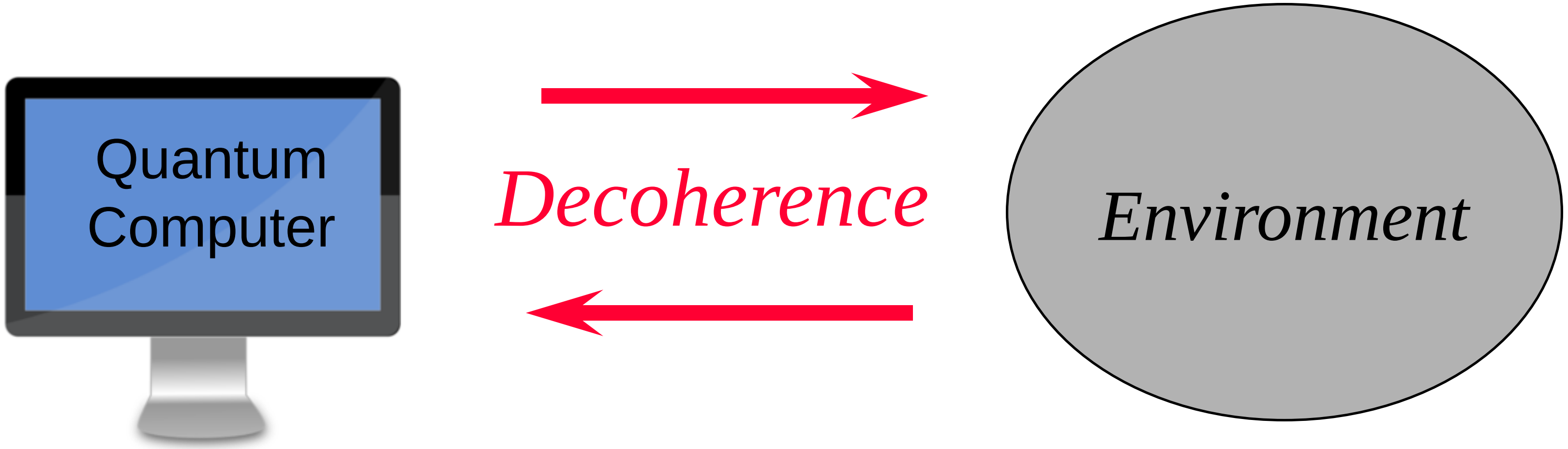
Peter Shor, The early days of quantum computation, arXiv:2208.09964

Why quantum computing is hard

We want qubits to interact strongly with one another.

We don’t want qubits to interact with the environment.

Except when we control or measure them.



ERROR!

To resist decoherence, we must prevent the environment from "learning" about the state of the quantum computer during the computation.

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

CrossMark
click for updates

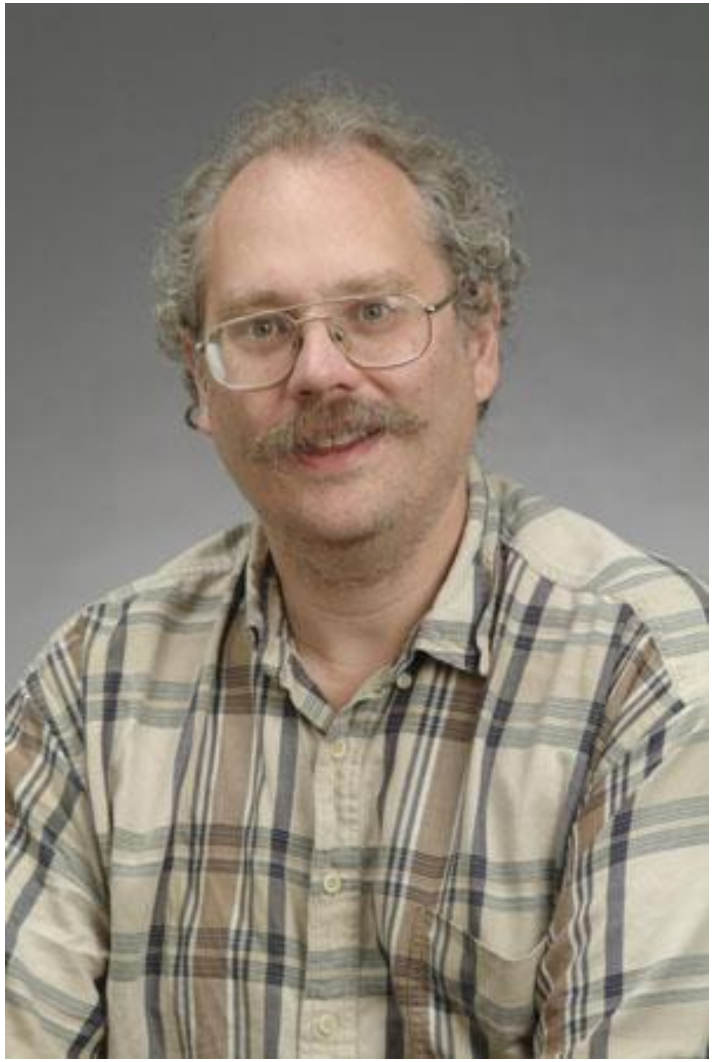
Is Quantum Mechanics Useful?

Rolf Landauer

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

"…small errors will accumulate and cause the computation to go off track."

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.”

PHYSICAL REVIEW A VOLUME 54, NUMBER 2 AUGUST 1996

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.

arXiv.org > quant-ph > arXiv:quant-ph/9610011

Search or

Quantum Physics

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.

arXiv.org > quant-ph > arXiv:quant-ph/9611025

Search or A

Quantum Physics

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.

"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."

Aharonov and Ben-Or, 1996

Haroche and Raimond, Physics Today, Published August 1996

QUANTUM COMPUTING: DREAM OR NIGHTMARE?

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

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-

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

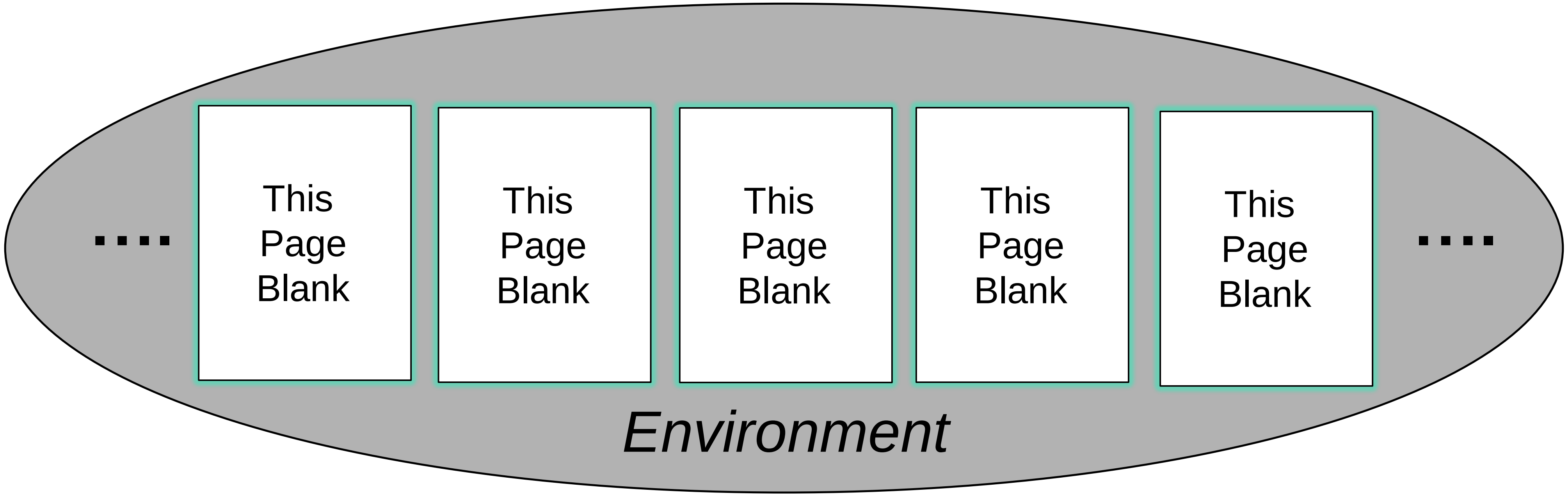
Therefore we think it fair to say that, unless some unforeseen new physics is discovered, the implementation of error-correcting codes will become exceedingly difficult as soon as one has to deal with more than a few gates. In this sense the large-scale quantum machine, though it may be the computer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

Alexei Kitaev

(1997)

"Such computation is fault-tolerant by its physical nature."

Quantum error correction



The protected "logical" quantum information is encoded in a highly entangled state of many physical qubits.

The environment can't access this information if it interacts locally with the protected system.

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

Quantumly easy.

Classically hard.

Useful.

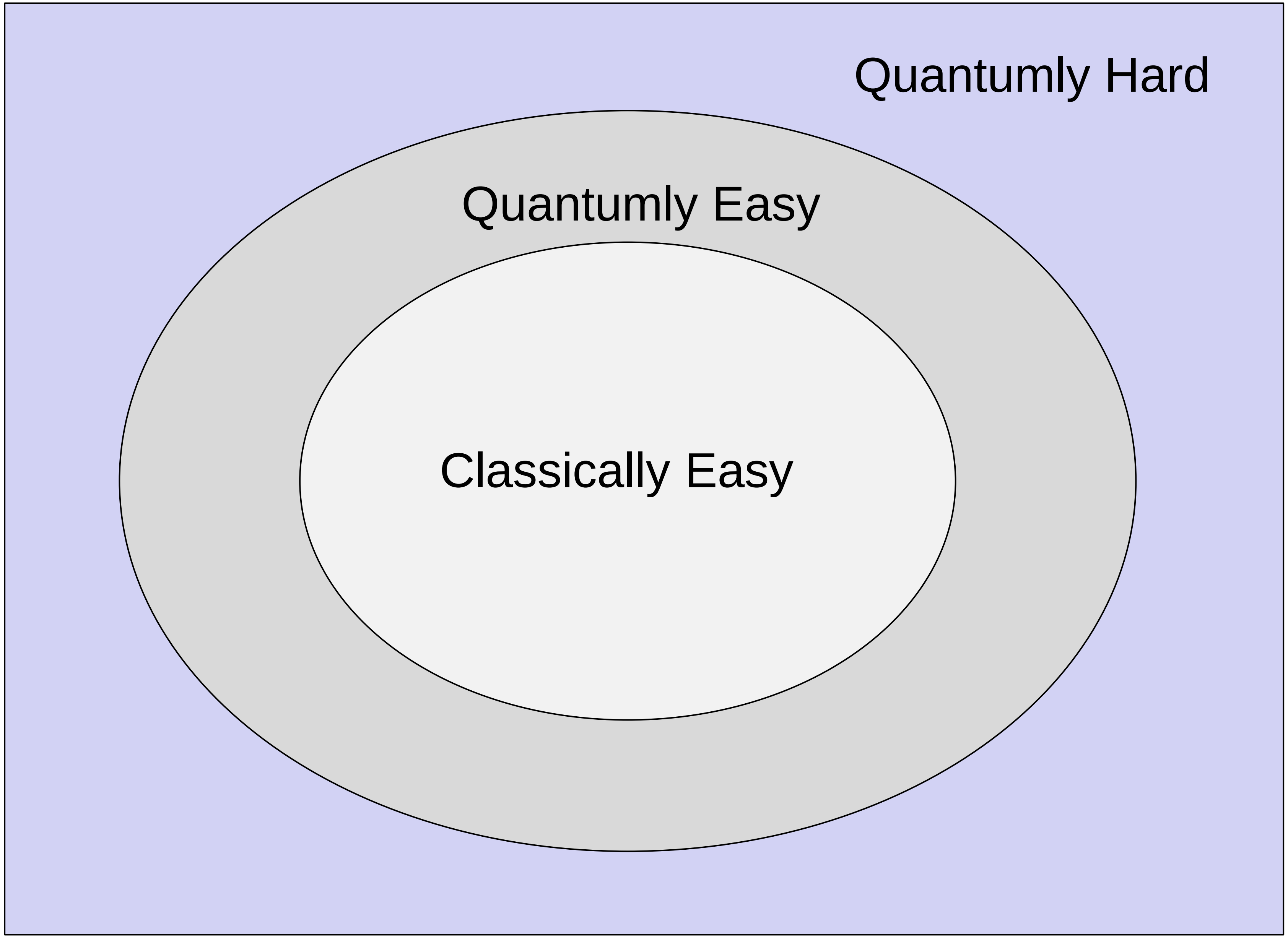
Scaling

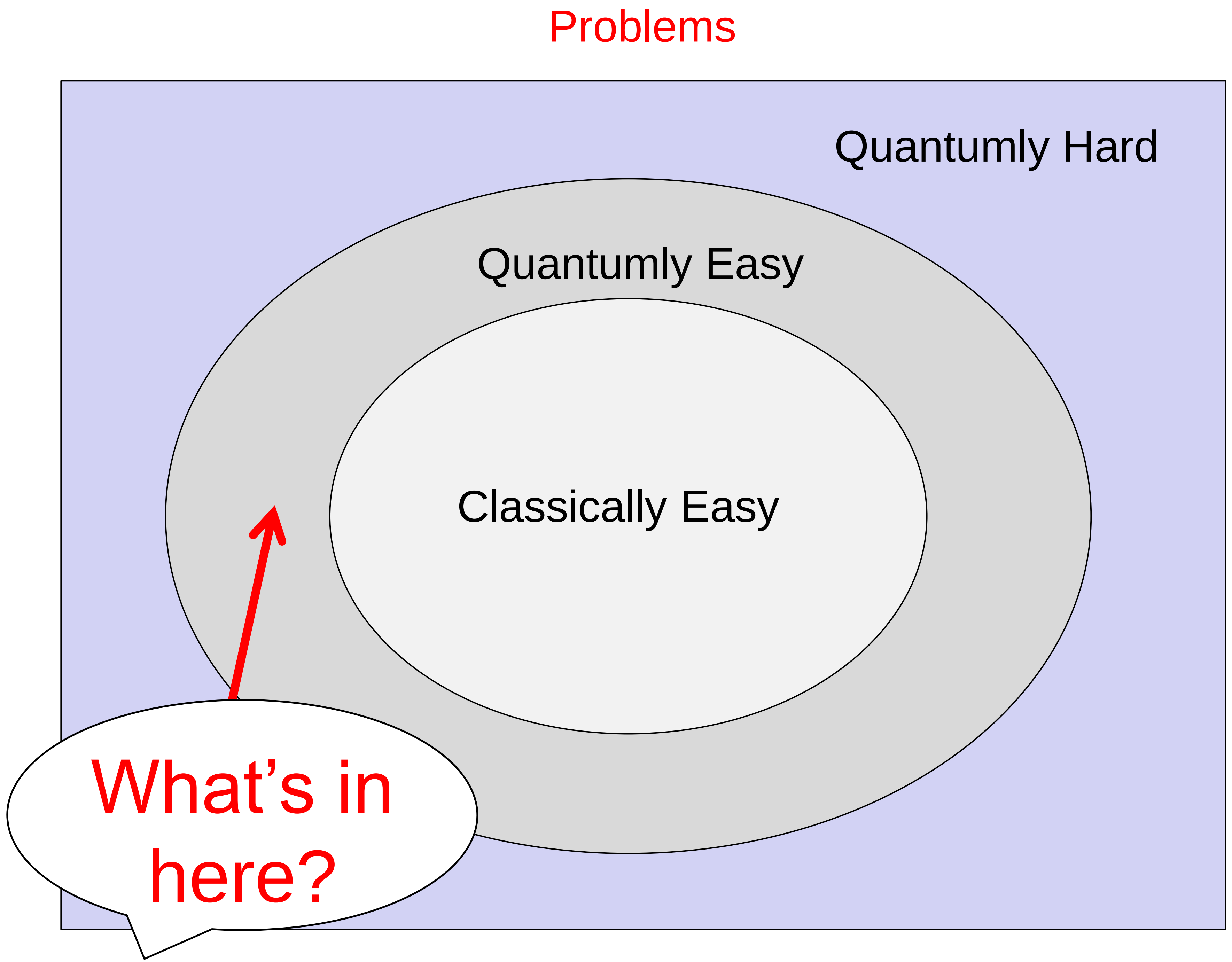
Devices.

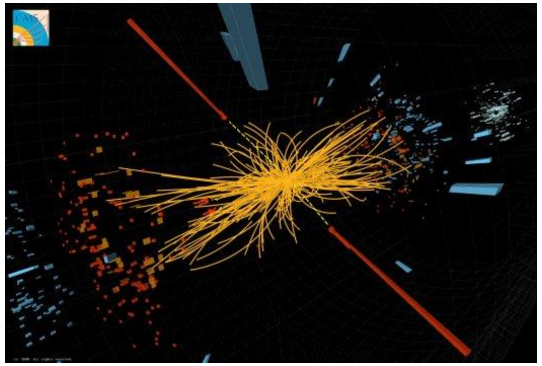
Error correction.

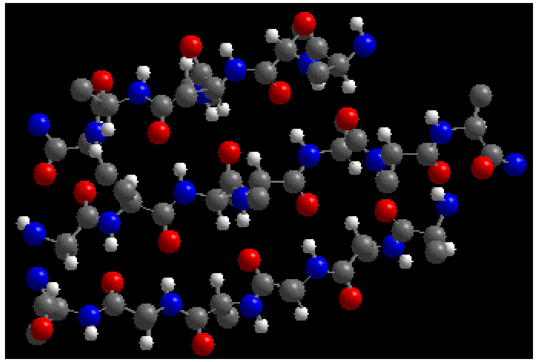
Systems engineering.

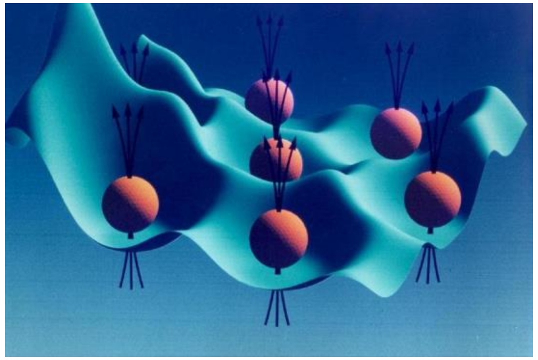
Problems



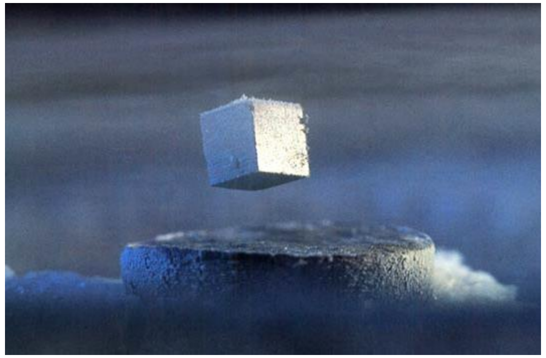

Problems
Quantumly Hard
Quantumly Easy
Classically Easy
What’s in here?

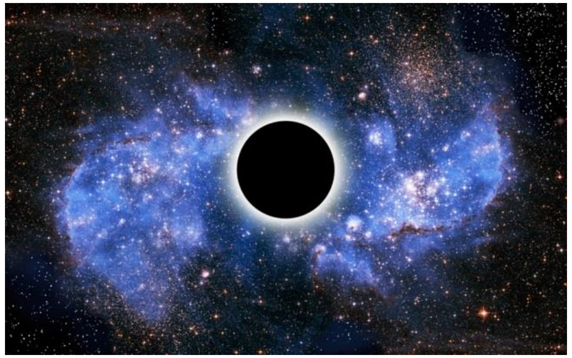

particle collision


molecular chemistry

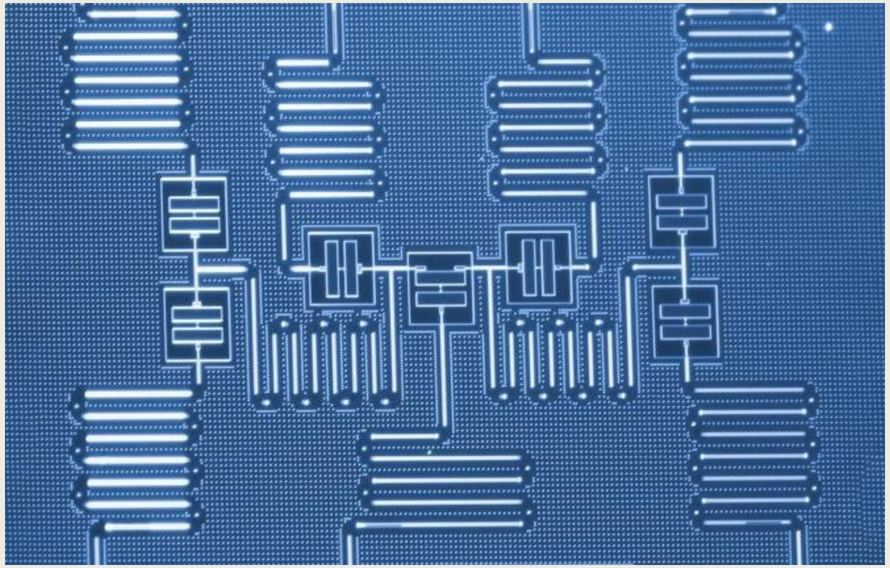

entangled electrons

(We expect that) a quantum computer can simulate efficiently any physical process that occurs in Nature.

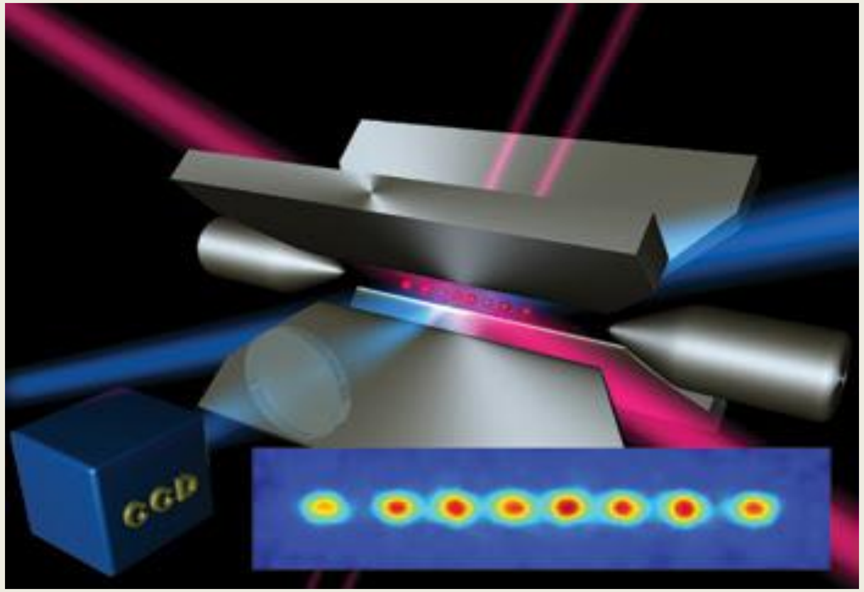

superconductor


black hole

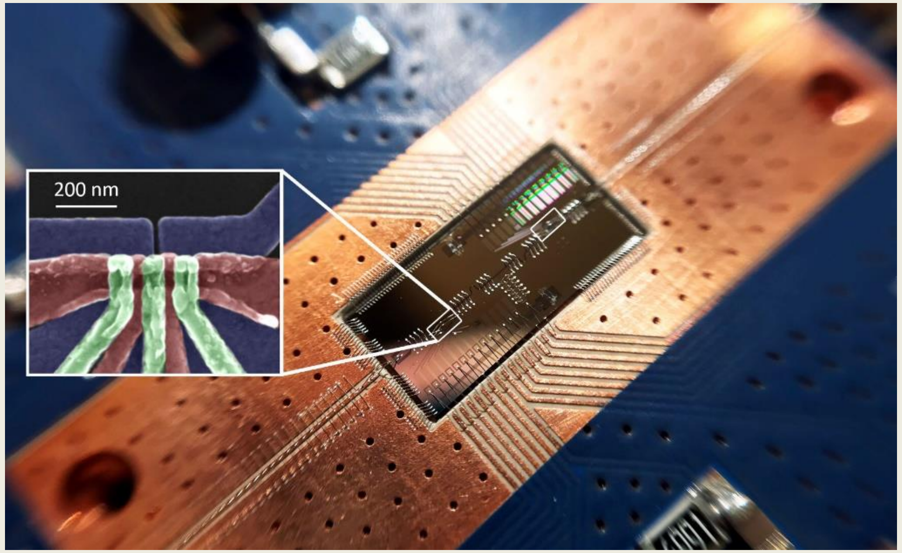

early universe



superconducting qubits



trapped atoms/ions



silicon spin qubits

photonics

Atomic Ions

Tens of qubits in a (linear) trap.

Stable laser → state preparation, single-qubit gates, readout.

Manipulate normal modes of vibration → two-qubit gates, all-to-all coupling (tens of microseconds).

Scaling: modular traps with optical interconnects or ion shuttling.

Superconducting Circuits

~ 100 qubits in a two-dimensional array with nearest-neighbor coupling.

Transmons: artificial atoms, carefully fabricated and frequently calibrated.

Microwave resonator for readout, microwave pulses for single-qubit gates.

Two-qubit gates via tunable frequency, tunable couplers, or cross-resonance drive (tens of nanoseconds).

Scaling: modular devices, microwave control lines, materials, fabrication, alternative qubit designs.

Neutral Atoms

100s to 1000s of atoms in optical tweezer arrays. Highly excited Rydberg states for entangling operations.

Atoms are movable, hence no geometrical constraints.

Global control, move to processing zones for local gates.

Atomic movement and readout are relatively slow.

Continuous loading of fresh atoms under development.

Noisy Intermediate Scale Quantum (NISQ) Era

What we have now.

NISQ is valuable for scientific exploration. But there is no proposed application of NISQ computing with *commercial* value for which quantum advantage has been demonstrated *when compared to the best classical hardware running the best algorithms for solving the same problems*.

What we can reasonably foresee.

Nor are there persuasive theoretical arguments indicating that commercially viable applications will be found that do *not* use quantum error-correcting codes and fault-tolerant quantum computing.

Fault-tolerant Application Scale Quantum (FASQ) Era

What we want to have.

-- Quantum computers running a wide variety of useful computations.

-- Machines that can execute of order 10^{12} quantum operations ("teraquop machines").

-- This requires improving quantum gate error rates by about 9 orders of magnitude beyond the current state of the art.

-- Quantum error correction and will be essential for crossing the chasm from NISQ to FASQ. We may need devices with millions of physical qubits.

When will we have it?

No one knows. It might take decades.

Quantum computing for chemistry and materials

Dirac (1929): "… equations much too complicated to be soluble."

Yet, heuristic classical algorithms are often very successful, and these methods are continually improving.

Quantum computing targets the relatively small "strongly correlated" corner of chemistry and materials science, where such methods falter.

How useful are quantum computers in physically relevant situations that are beyond the reach of classical methods?

Artificial intelligence may drive future progress in (strongly correlated) chemistry and materials science. Eventually, quantum computers can accelerate progress by providing abundant training data.

Simulating quantum dynamics

Classical computers are especially bad at simulating quantum *dynamics*. Quantum computers will have a big advantage.

But …

Many-body localized (MBL) systems, which equilibrate slowly, are only slightly entangled, and *might* therefore be easy to simulate classically.

Systems with strong quantum chaos become highly entangled and are therefore hard to simulate classically. But they might be boring – perhaps they quickly converge to thermal equilibrium and after that "nothing interesting" happens.

If we ask the right questions, scientifically informative surprises should be expected (quantum many-body scars, diabatic evolution in quantum spin liquids, …)

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. Limited effectiveness 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.

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 $P_{\text{physical}} = 10^{-4}$.)

Quantum error correction below the surface-code threshold

[*Google 2024*]

105 qubit Willow processor. Improved transmon lifetime, measurement error, leakage correction.

Millions of rounds of surface-code error syndrome measurement, each lasting ~1 microseconds (600 nanosecond measurement time).

Logical error rate for quantum memory improves by $\Lambda \approx 2$ when code distance increases by 2 (from 3 to 5 to 7).

Accurate *real-time* decoding of error syndromes for distance 3 and 5.

Repetition code: $\Lambda \approx 8.4$ up to d = 29.

Looking ahead: Better Λ, larger codes, high-fidelity logical two-qubit gates.

Other error correction progress

Movable qubits for all-to-all coupling.

Harvard + MIT + QuEra: Circuit sampling with 48 logical qubits on a 280-qubit device. CCZ gates within an [[8,3,2]] code block.

Atom Computing + Microsoft: Bernstein-Vazirani algorithm with 28 logical qubits in a 256-qubit device. [[4,1,2]] subsystem code.

Quantinuum + Microsoft. Preparation of a cat state with 12 logical qubits on a 56-qubit device. CNOT within a [[16,4,4]] block and transversal between blocks.

Caveats: Few rounds of syndrome measurement and unscalable postselection.

Can movement be much faster?

Error correction and fault tolerance

Surface code. High error threshold, 2D layout, good enough decoders (?), high overhead cost.

High-rate quantum low-density parity-check (LDPC) codes. Geometrically nonlocal, better decoders needed, complex logical operations.

System design. Trade time for space to reduce local control requirements.

General principles. Space and time should be treated in a unified framework, logical operations performed via code deformations.

Megaquop Machine

Logical gate error rate ~ 10^{-6}. Not achievable without QEC.

Error mitigation will continue to be useful in the Megaquop era and beyond.

Beyond classical, NISQ, or analog. E.g., depth 10K and 100 (logical) qubits.

Tens of thousands of high-quality physical qubits.

When will we have it? Less than 5 years? What modality? Rydberg atoms?

What will we do with it? Quantum dynamics?

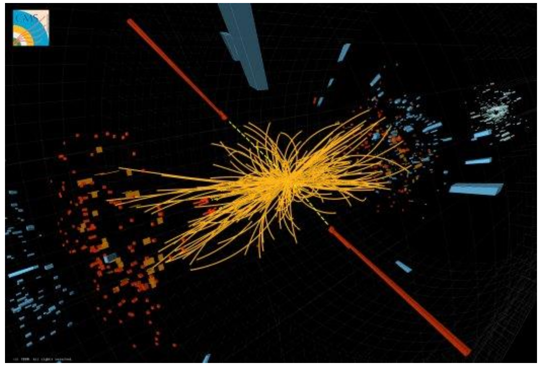
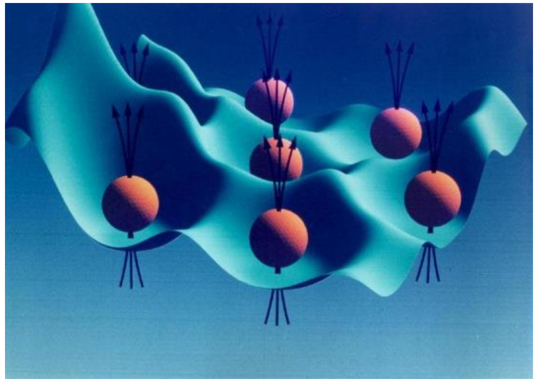
Commercial as well as scientific applications? [arXiv:2502.17368]

Co-design

Adapt the application and the error correction protocol to the hardware.

Adapt the hardware to the application and the error-correcting code.

Frontiers of Physics

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

Prospects for the next 5 years

Encouraging progress toward scalable fault-tolerant quantum computing.

Scientific insights enabled by programmable quantum simulators and circuit-based quantum computers.

Advances in quantum metrology from improved control of quantum many-body systems.

Prospects for the next 100 years

Past 100 years:

The relatively simple quantum behavior of weakly correlated particles like electrons, photons, etc.

Next 100 years:

The extraordinarily complex quantum behavior of many profoundly entangled particles.