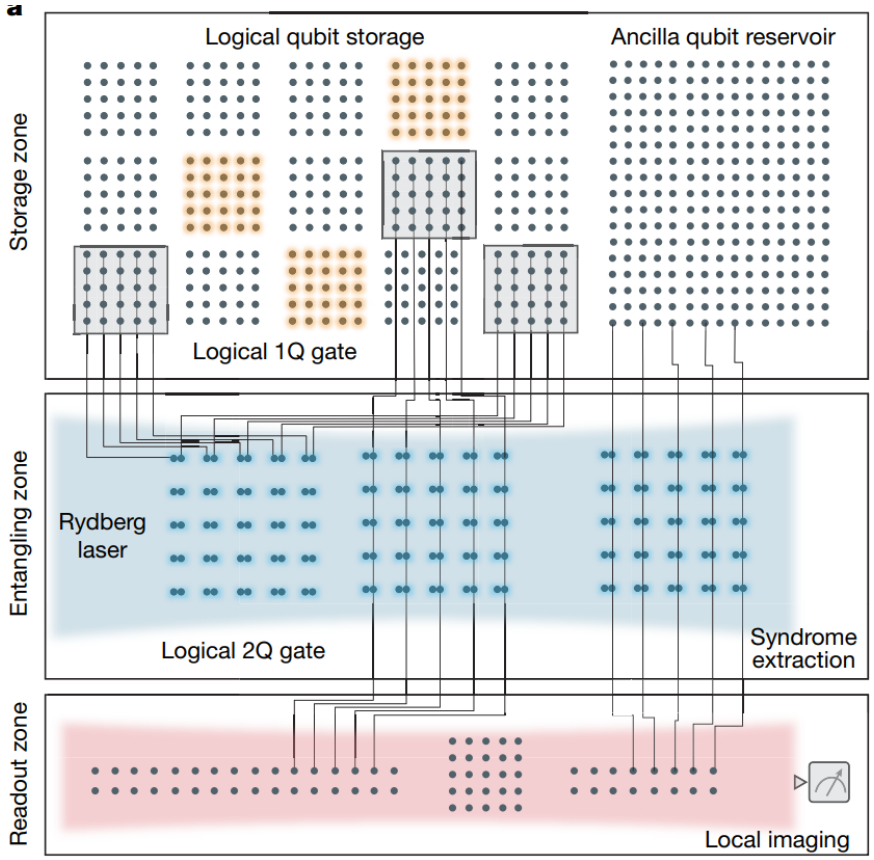
Quantum error correction gets real



Shor

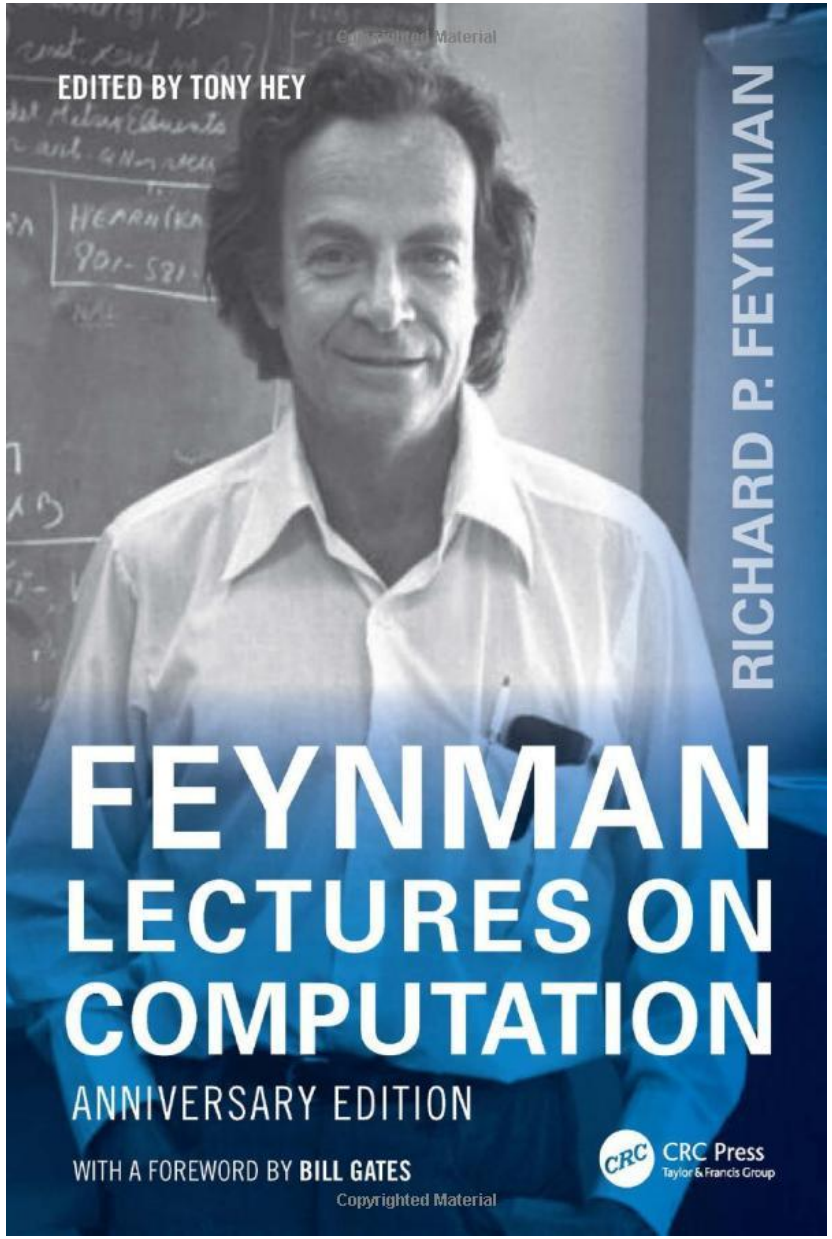
Steane

Kitaev

INSTITUTE FOR QUANTUM INFORMATION AND MATTER

John Preskill
Nobel Symposium
30 October 2026

Oratomic

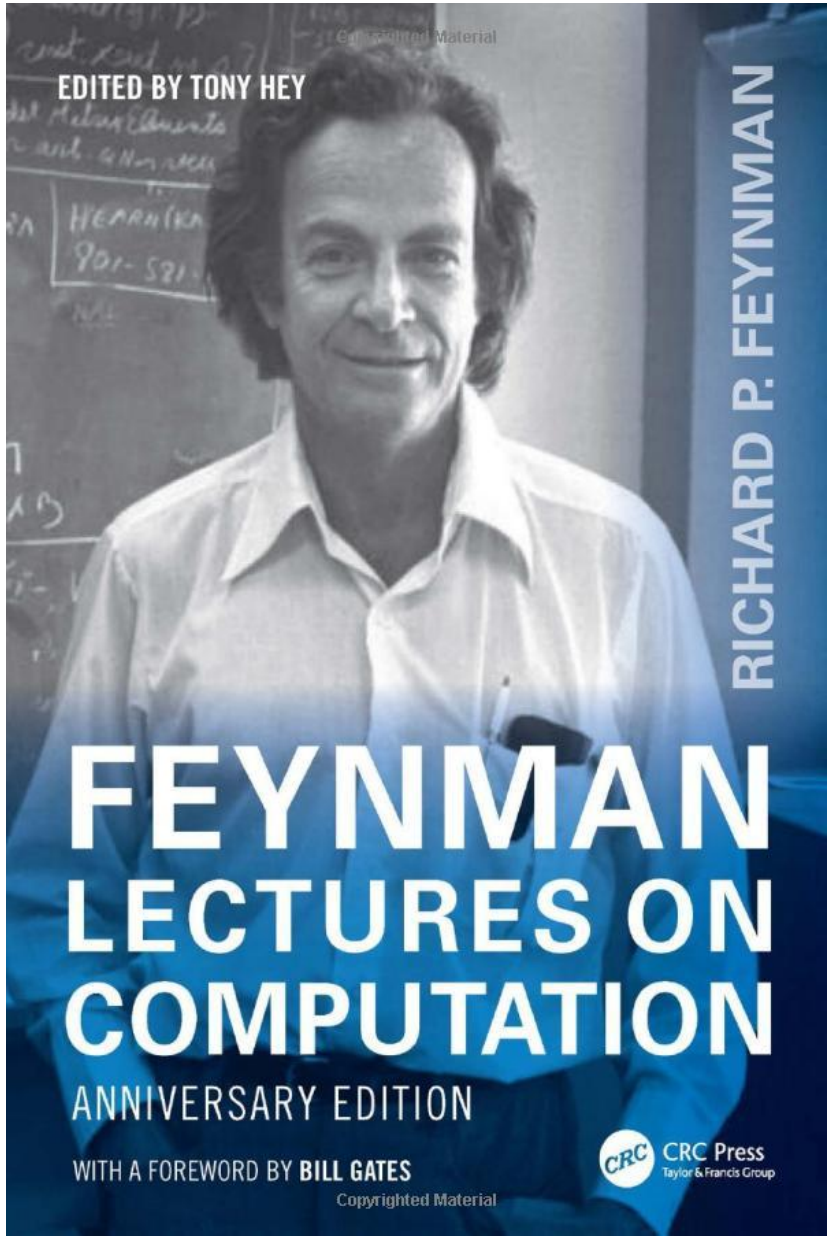


Richard Feynman
(1981)

"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

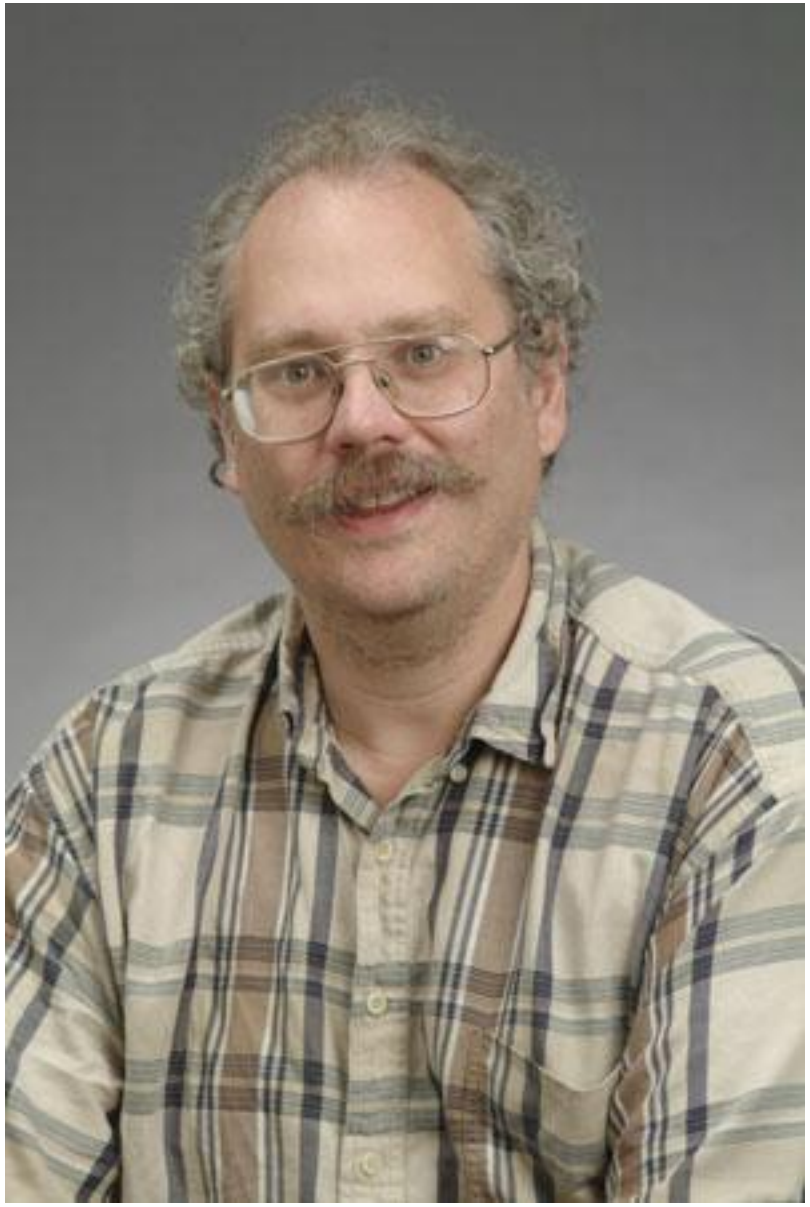


David Deutsch
(1985)

“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

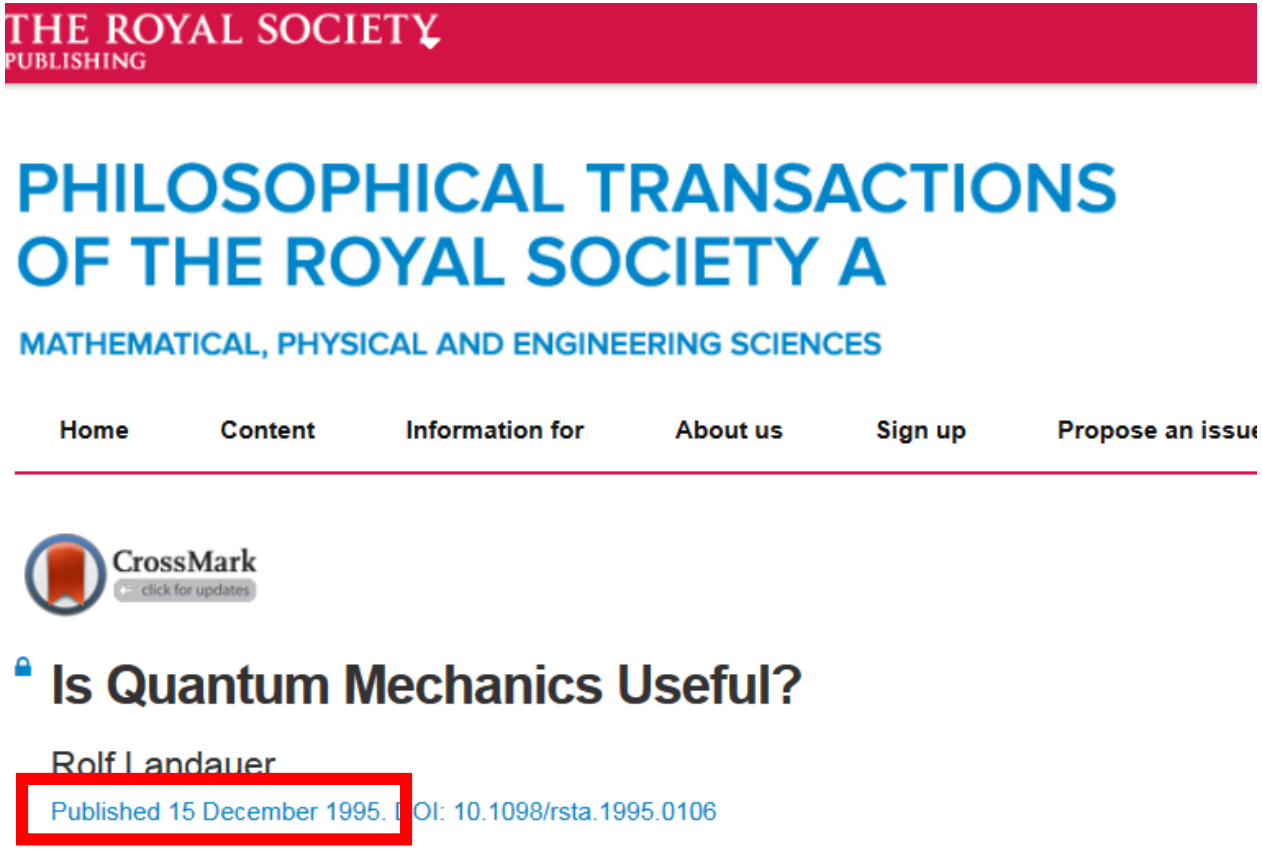
W. G. Unruh*
Canadian Institute for Advanced Research, Cosmology Program, Department of Physics, University of British Columbia, Vancouver, Canada V6T 1Z1
(Received 10 June 1994)

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 $\hbar/k_BT$. For longer times the condition on the strength of the coupling to the external world becomes much more stringent.

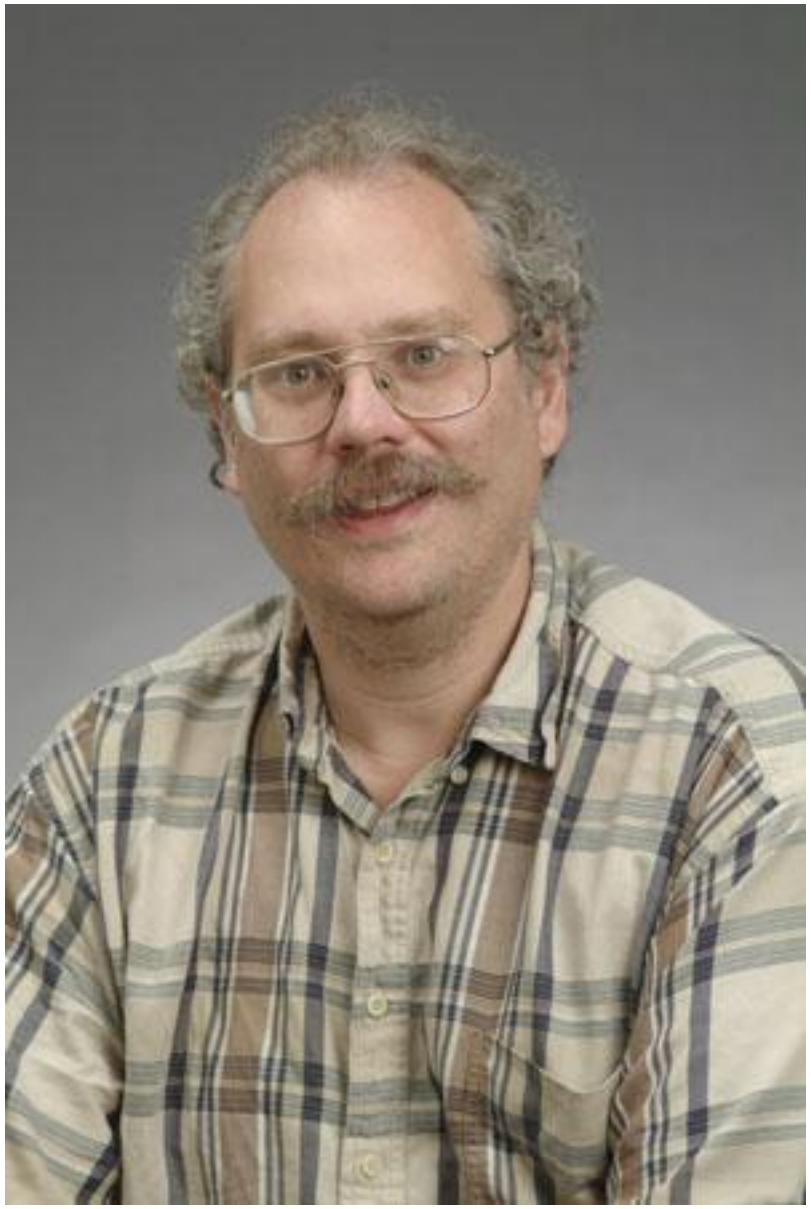
PACS number(s): 03.65.−w

"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



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



Peter Shor

Quantum error-correcting codes (1995)
Fault-tolerant syndrome measurement (1996)
Fault-tolerant universal quantum gates (1996)
Using QEC to prove security of QKD (2000)

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, R[illegible] 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.

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.

PHYSICAL REVIEW A VOLUME 54, NUMBER 3 SEPTEMBER 1996

Class of quantum error-correcting codes saturating the quantum Hamming bound

Daniel 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

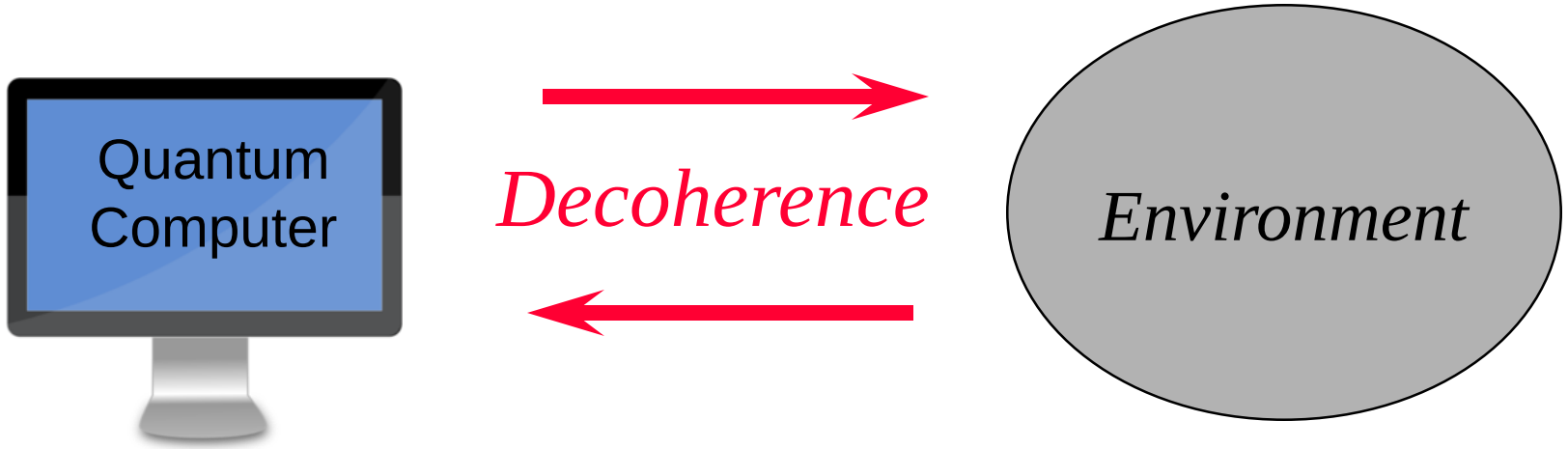
VOLUME 78, NUMBER 3 PHYSICAL REVIEW LETTERS 20 JANUARY 1997

Quantum Error Correction and Orthogonal Geometry

A. R. Calderbank,[1] E. M. Rains,[2] P. W. Shor,[1] and N. J. A. Sloane[1]
[1]*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]

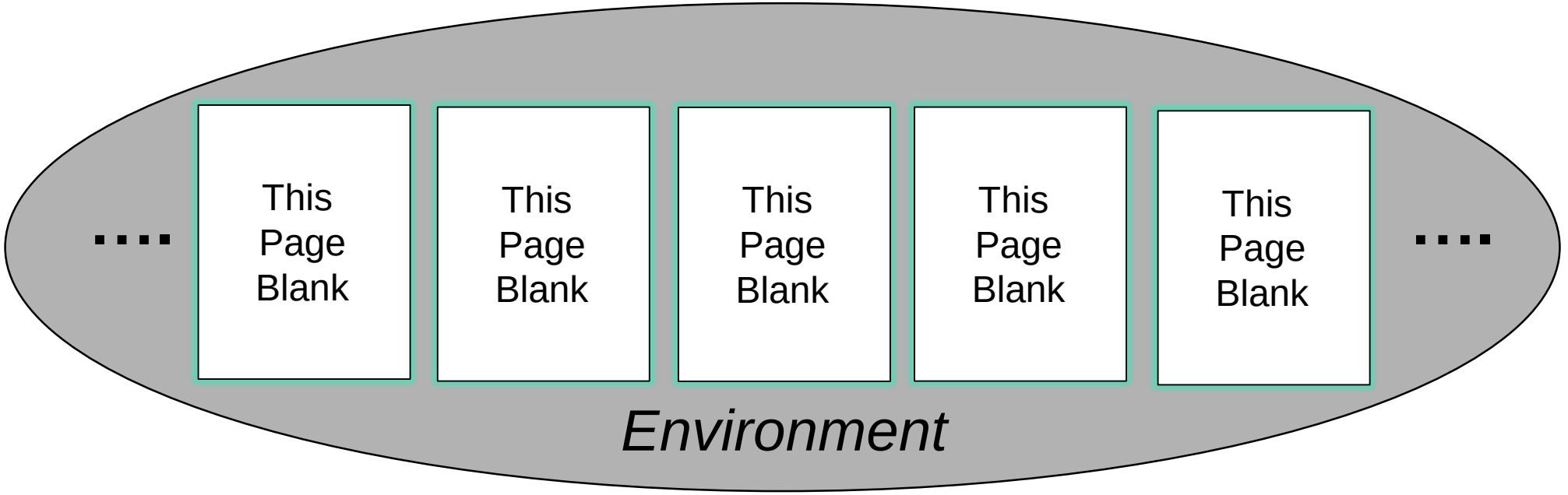
Quantum stabilizer codes:
the quantum analogue of additive classical codes.



ERROR!

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

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.

arXiv.org > quant-ph > arXiv:quant-ph/9605011

Search or

Quantum Physics

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 futher 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.

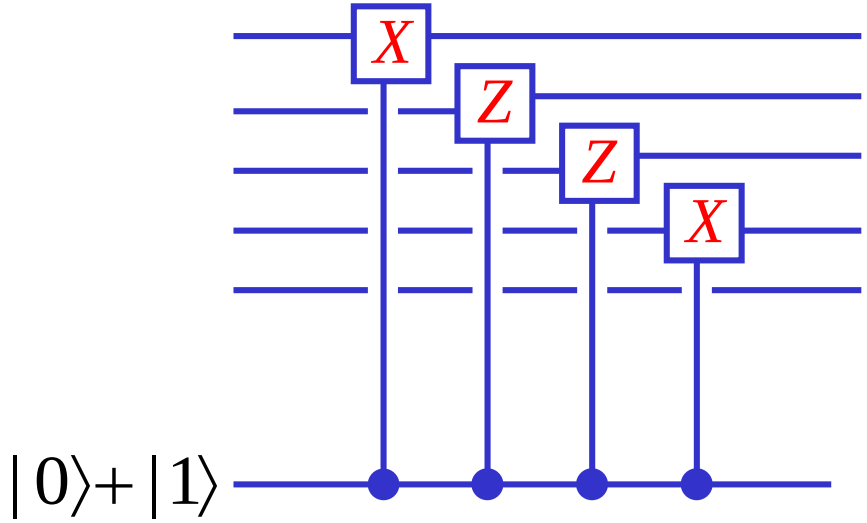
Comments: Latex, 11 pages, no figures, in 37th Symposium on Foundations of Computing, IEEE Computer Society Press, 1996, pp. 56-65

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

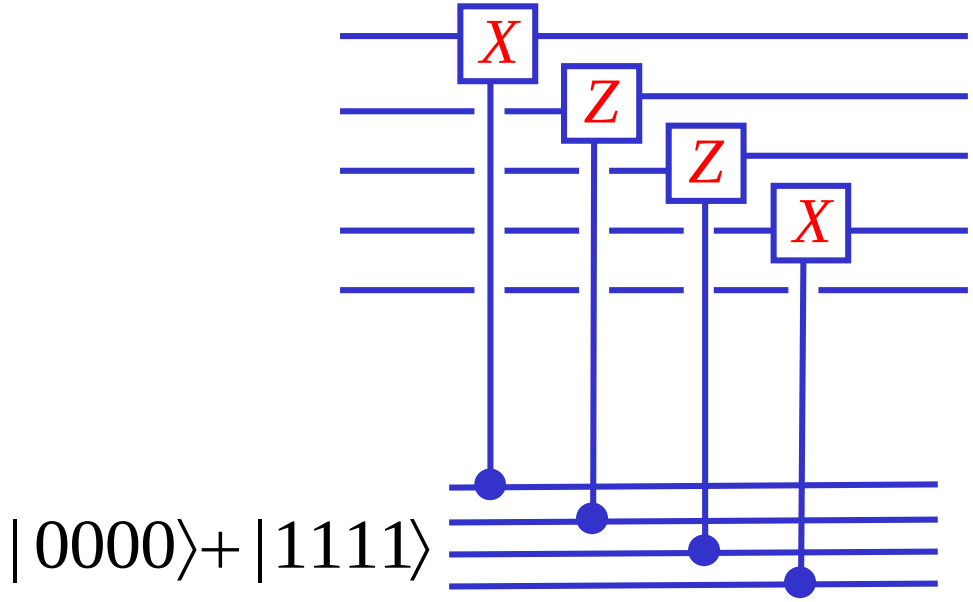
Universal gates acting on encoded quantum data, using “magic states” verified offline.

Fault-tolerant syndrome measurement

This is *bad:*



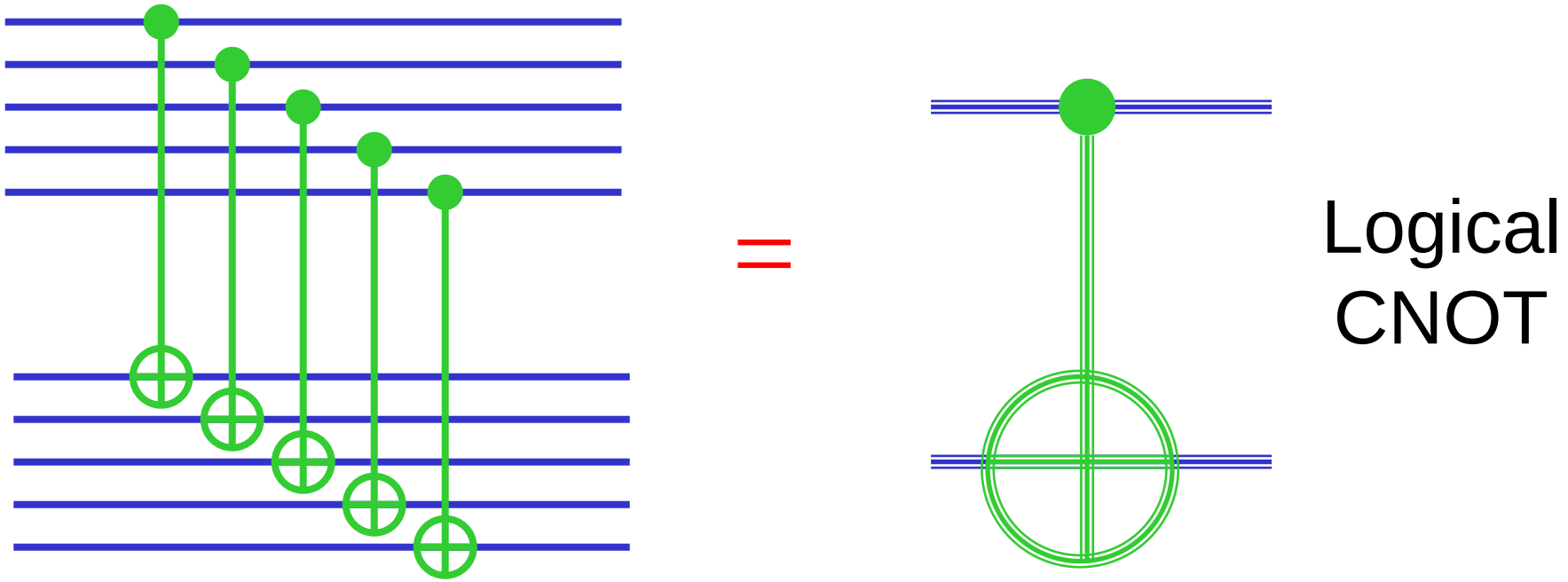
This is *better:*



*Prepare and verify an **encoded** ancilla for syndrome measurement.*

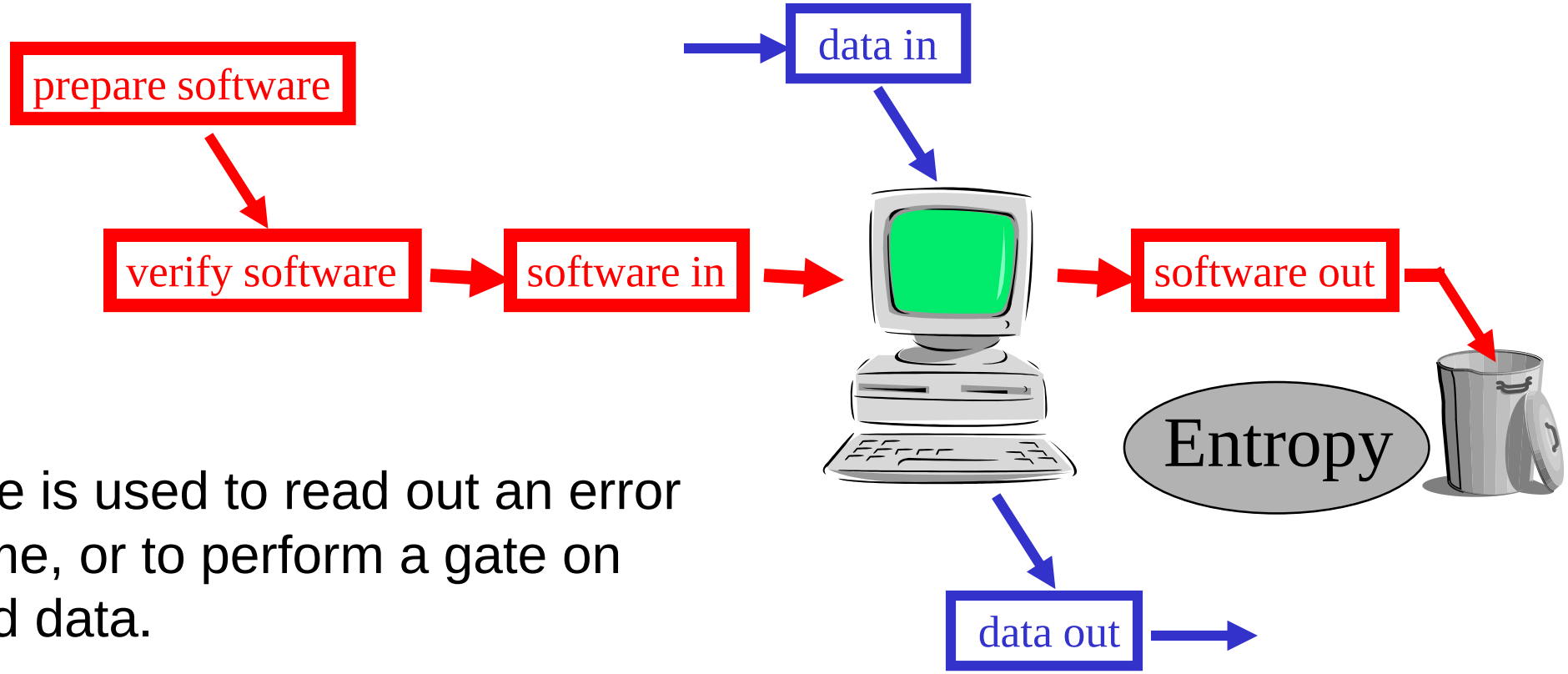
Repeat to protect against measurement errors.

Transversal gates are fault tolerant



Not all logical gates in a universal set can be realized transversally. Eastin and Knill 2009. To complete a universal fault-tolerant gate set, we must add to the transversal gates additional gates that are implemented by consuming *quantum software*.

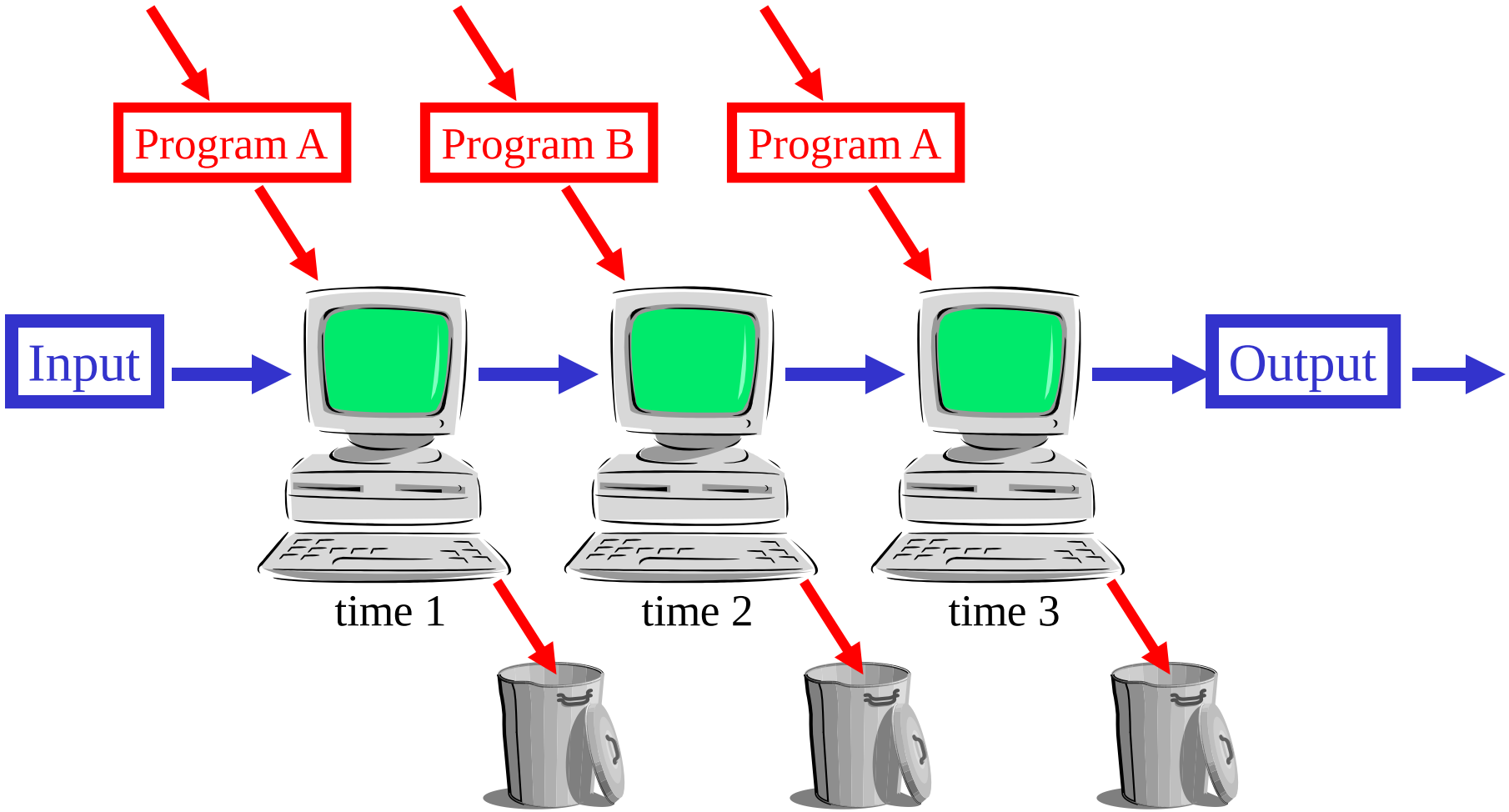
Preparation and consumption of *quantum software*



Software is used to read out an error syndrome, or to perform a gate on encoded data.

The software must be prepared and verified before it interacts with data. After a single use, the software is irreparably damaged and must be discarded.

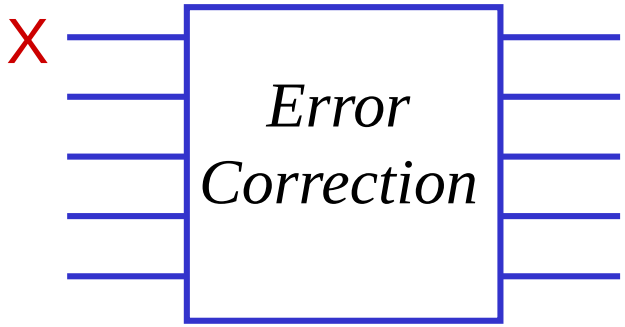
Consumption of *quantum software*



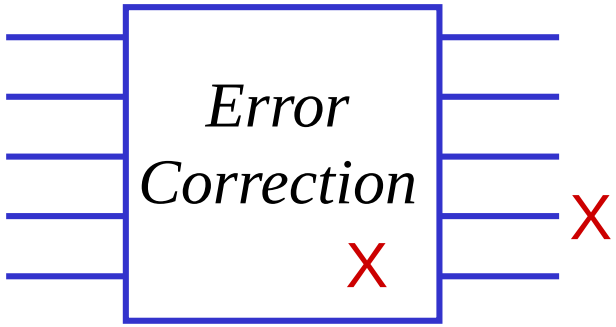
The software is prepared and verified, then discarded after use. To execute a quantum algorithm, the user prepares and consumes a particular program many times. Shor 1996, Gottesman and Chuang 1999, Bravyi and Kitaev 2005.

Fault-tolerant error correction

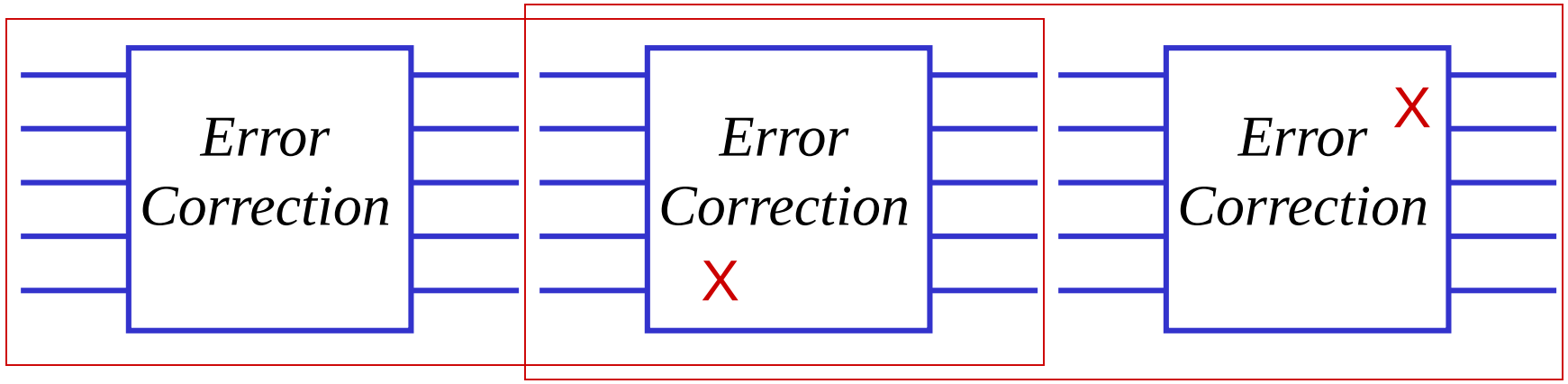
Fault: a location in a circuit where a gate or storage error occurs.
Error: a qubit in a block that deviates from the ideal state.



If input has at most one error, and circuit has no faults, output has no errors.

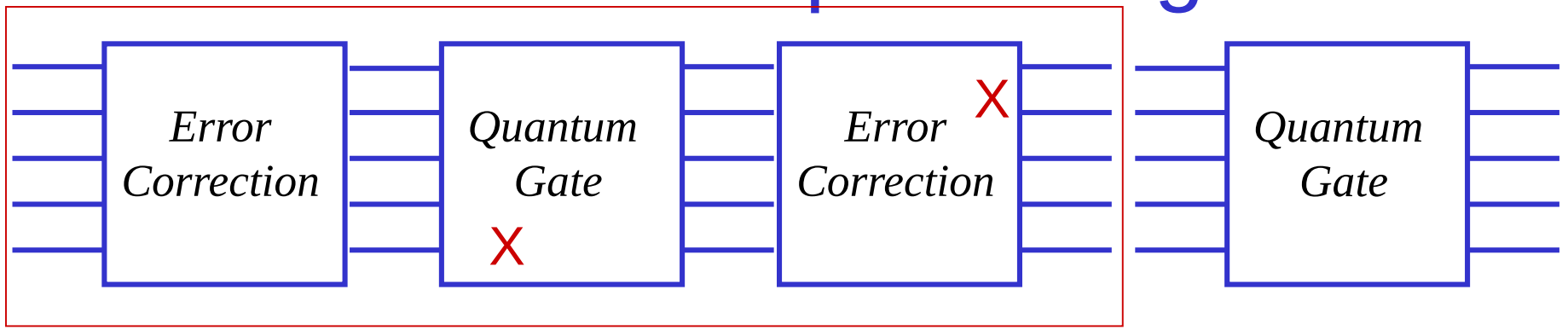


If input has no errors, and circuit has at most one fault, output has at most one error.



A quantum memory fails only if two faults occur in some “extended rectangle.”

Fault-tolerant quantum gates



Each gate is followed by an error correction step. The circuit simulation fails only if two faults occur in some “extended rectangle.”

If we simulate an ideal circuit with noisry quantum gates, and faults occur independently with probability ε at each circuit location, then the probability of failure per gate is

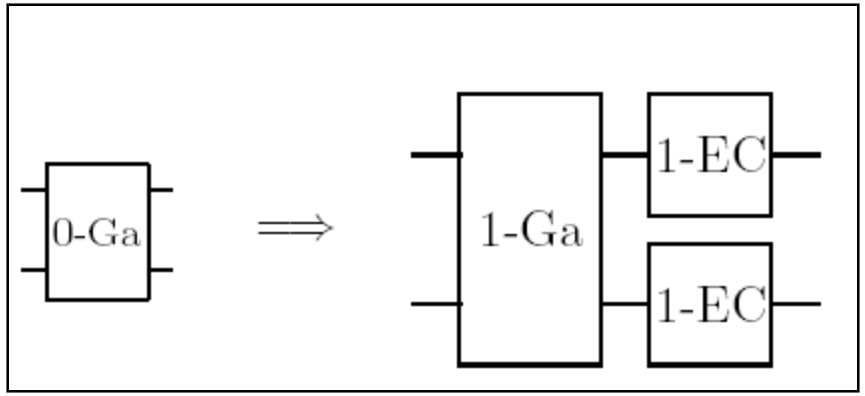
$$P_{\text{fail}} \leq A\varepsilon^2$$

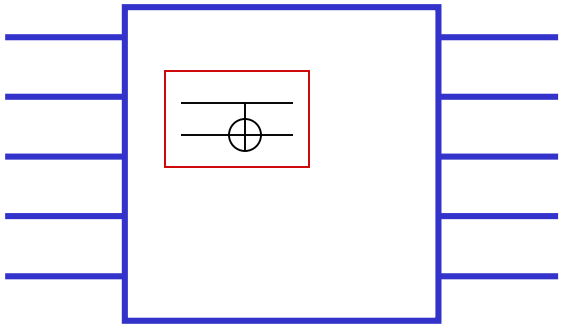
where A is the number of pairs of circuit locations in an extended rectangle.

Recursive simulation

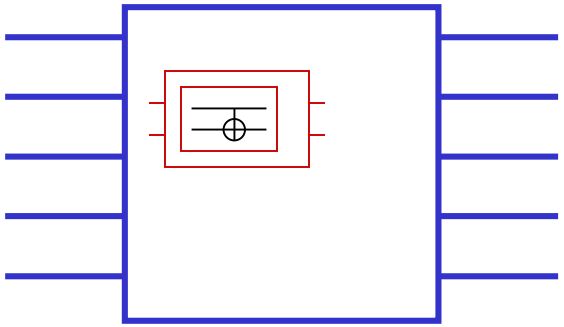
Replace each level-0 ideal gate by a *1-gadget*: level-1 gate gadget followed by level-1 EC.

Repeat k times → a level-k simulation: Each ideal gate replaced by a k-gadget.

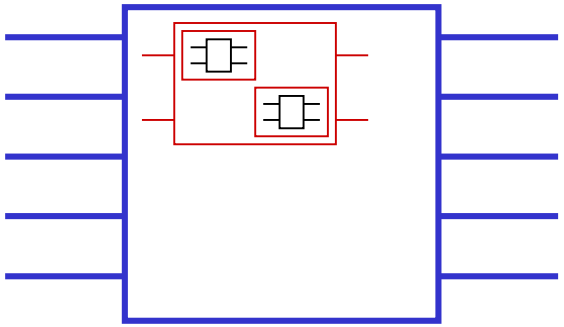




A *1-gadget* is built from quantum gates.



A *2-gadget* is built from 1-gadgets.



A *3-gadget* is built from 2-gadgets.

The effective noise for the level-1 gadget has a "renormalized" strength:

$$\varepsilon^{(1)} \le \varepsilon^2 / \varepsilon_0 = \varepsilon_0 (\varepsilon / \varepsilon_0)^2$$

At level k the renormalized noise strength is:

$$\varepsilon^{(k)} < \varepsilon_0 (\varepsilon / \varepsilon_0)^{2^k}$$

Scalable quantum computing

Quantum Accuracy Threshold Theorem: Consider a quantum computer subject to quasi-independent noise with strength ε. There exists a constant $\varepsilon_0 > 0$ such that for a fixed $\varepsilon < \varepsilon_0$ and fixed $\delta > 0$, any circuit of size L can be simulated by a circuit of size L^* with accuracy greater than $1-\delta$, where, for some constant c,

$$L^* = O\left[L (\log L)^c \right]$$

Aharonov, Ben-Or
Kitaev
Laflamme, Knill, Zurek
Aliferis, Gottesman, Preskill
Reichardt

assuming:

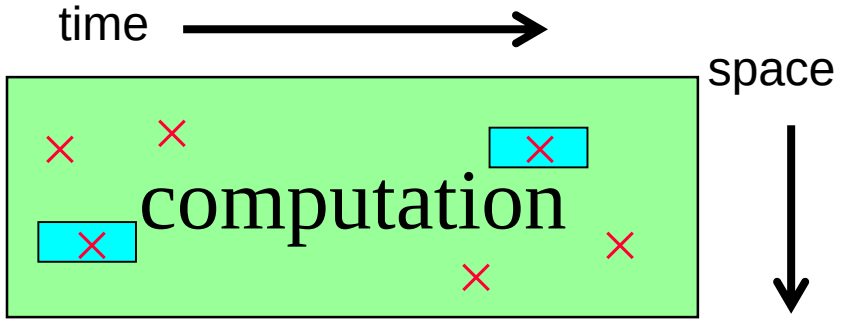
parallelism, fresh qubits (*necessary* assumptions)

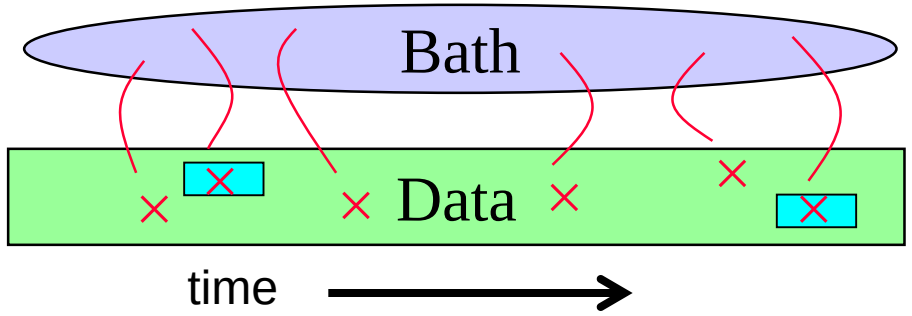
nonlocal gates, fast measurements, fast and accurate classical processing, no leakage (*convenient* assumptions).

Noise models

The threshold theorem applies to both stochastic and Hamiltonian noise models.

Quasi-independent noise. "Fault paths" are assigned *probabilities*. For any set of *r* gates in the circuit, the probability that all r of the gates have faults is no larger than ε^r. A useful caricature of noise in actual devices, and can be compared with simulations.



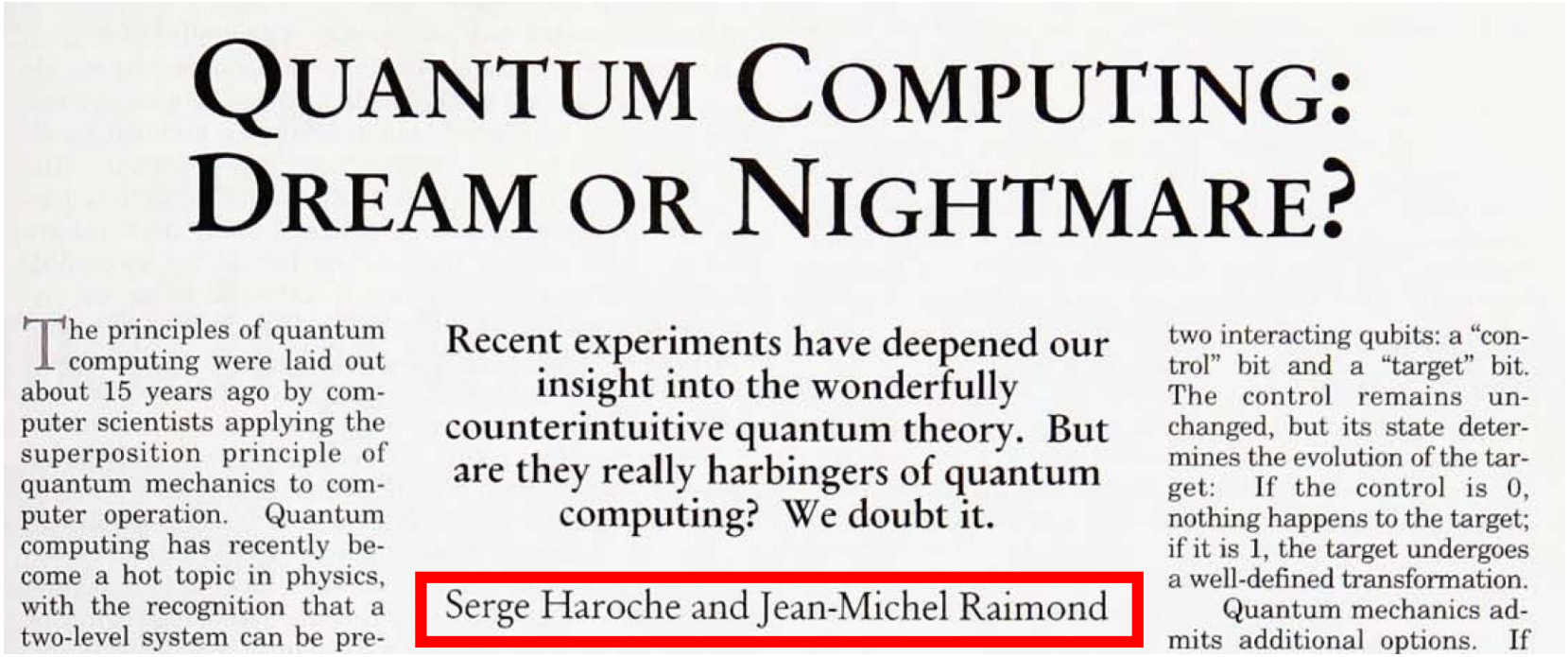


$$H = H_{System} + H_{Bath} + H_{System-Bath}$$

Bath coupled locally to system. Fault tolerance works if the system-bath coupling is sufficiently weak.

Terhal, Burkard 2005; Aliferis, Gottesman, Preskill 2006; Aharonov, Kitaev, Preskill 2006; Ng, Preskill 2009.

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.

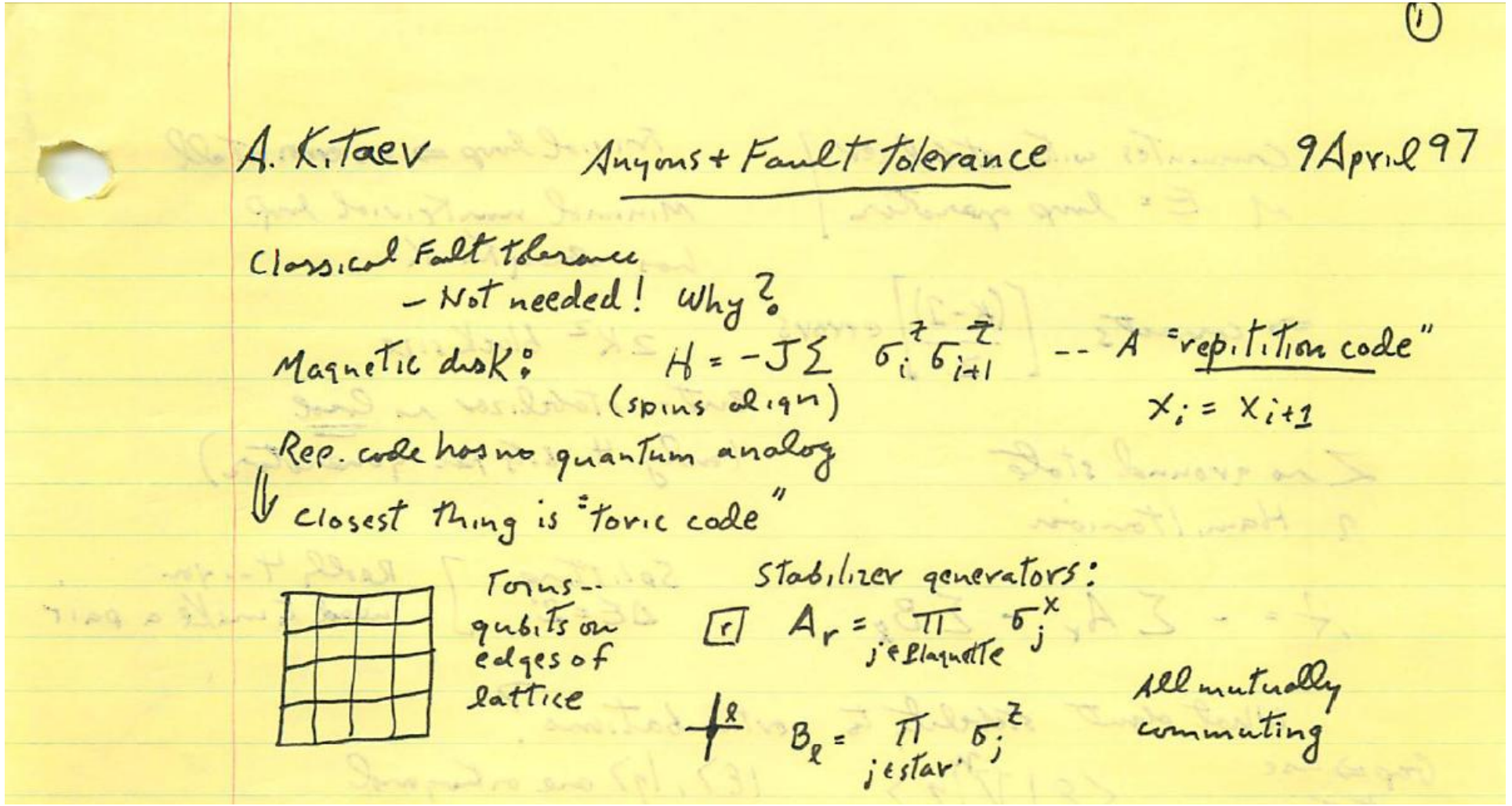
Alexei Kitaev
(1997)

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

Alexei Kitaev

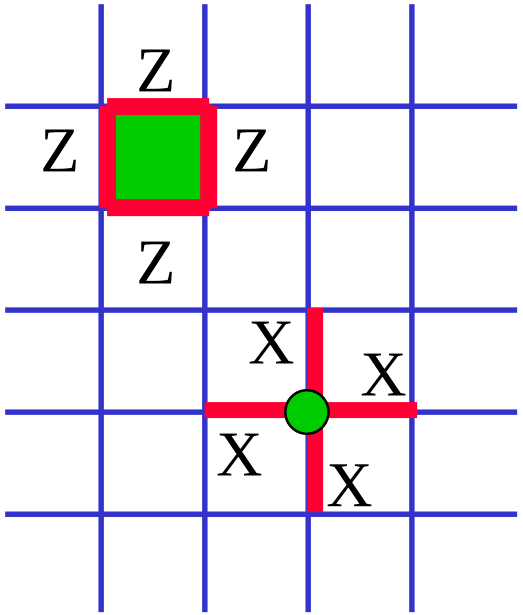
Topological quantum codes (1996)
Physically protected quantum computing (1997)
Computing with nonabelian anyons (1997)
Magic state distillation (1999-2004)
Majorana modes in quantum wires (2000)

And many others, of course: Steane, Knill, Laflamme, Aharonov, Ben-Or, Gottesman, …
Second-decade heroes: Bombin, Bravyi, Terhal, Poulin, Haah, …
Third decade: A new generation driving progress, especially in high-rate quantum codes!



9 April 1997 … An exciting day!

Toric / Surface code



Qubits on edges of a 2D square lattice.

Four-qubit check operators can be measured *locally*.

$$\prod_{+} X = 1, \qquad \prod_{\square} Z = 1,$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

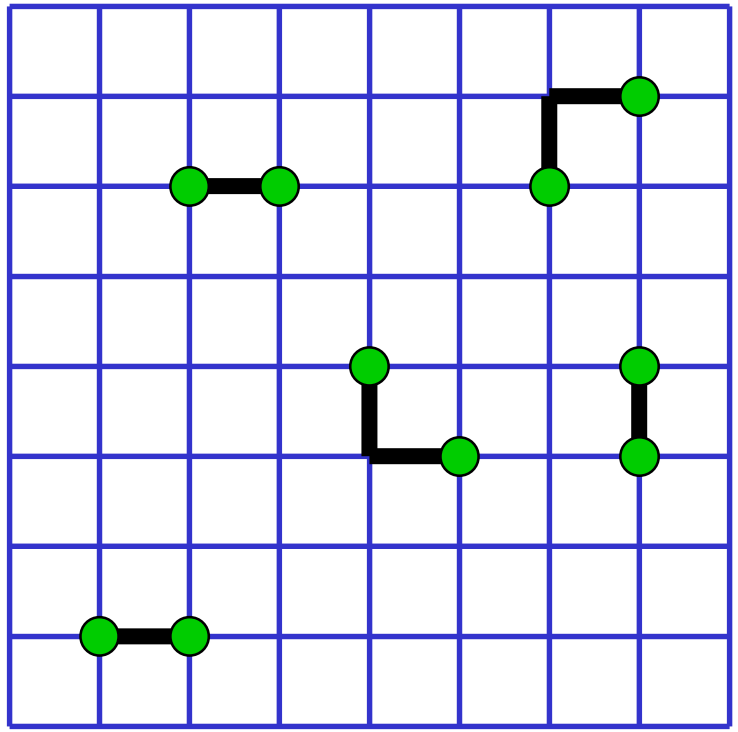
Check operators are mutually commuting (simultaneously diagonalizable).

Logical operators = strings extending across the lattice.

Compare Z_2 gauge theory --- site operators detect electric charges and plaquette operators detect Z_2 magnetic flux.

Kitaev 1996

Error Recovery



Low error rate: short error chains.

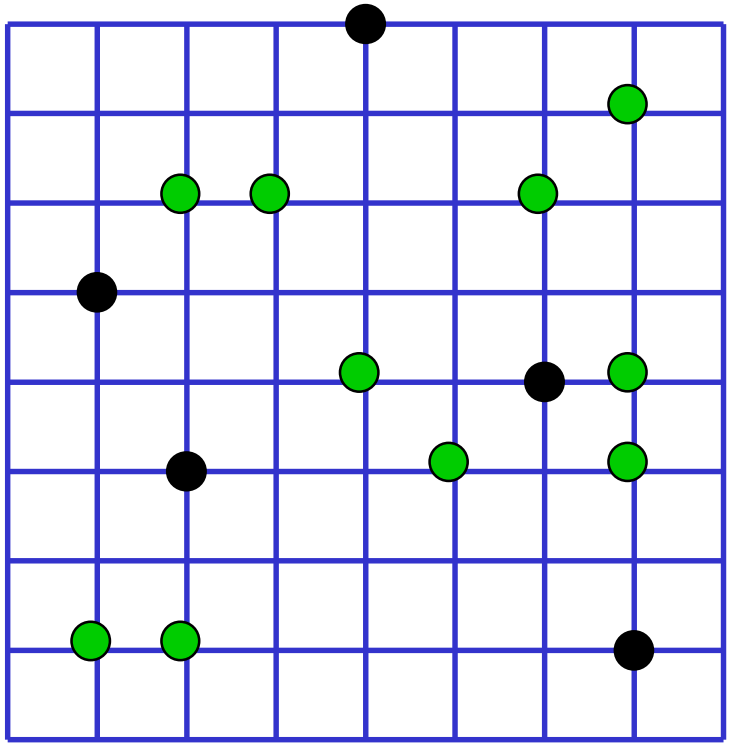
Easy to guess how to pair the defects without producing long strings.

Can tolerate a number of errors that scales linearly with the block size.

There is an accuracy threshold.

… assuming fast and accurate (poly-time) classical processing.

Fault-tolerant Recovery?



Genuine defect:

Ghost defect:

Measurement errors: some apparent defects are phony.

Repeat syndrome measurement O(d) times for a d x d lattice.

Threshold survives.

Weight-4 check operators, relatively large 2-qubit error rate is acceptable.

Dennis, Kitaev, Landahl, Preskill 2002

From NISQ to FASQ

What we have now:

-- *Noisy Intermediate-Scale Quantum (NISQ) machines*.

-- Capable of performing thousands of two-qubit operations.

-- Becoming useful for scientific exploration.

-- Limited commercial value.

What we want to have:

-- *Fault-Tolerant Application-Scale Quantum (FASQ) machines*.

-- Capable of performing billions or trillions of two-qubit operations.

-- Opening a wide variety of scientific and commercial applications.

-- Need to improve error rates by many orders of magnitude!

-- Quantum error correction is essential for crossing from NISQ to FASQ.

Quantum error correction: What we want

Repeated rounds of accurate error syndrome measurement.

Quantum memory times that improve sharply as codes increase in size.

Accurate *real-time* decoding of error syndromes, scalable control.

Scalable efficient logical universal gates with (much) higher fidelity than physical gates.

Logical gate fidelities that improve sharply as codes increase in size.

Acceptable overhead cost in space and time.

Speed matters! (Superconducting ~1000 time faster than ions.)

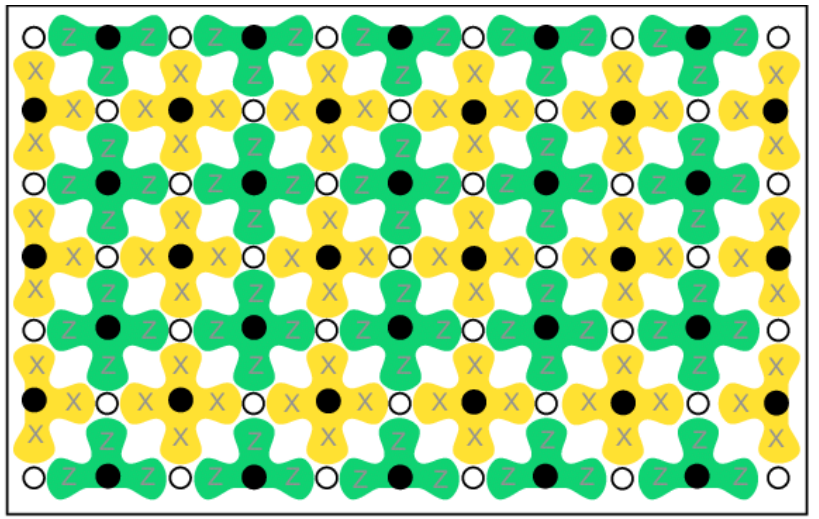
Overhead cost of fault tolerance

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

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

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



white = data
black = check

Quantum error correction below the surface-code threshold

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

Millions of rounds of surface-code error syndrome measurement, each lasting ~1 microsecond (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).

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

Google Quantum AI 2024

Quantum low-density parity-check codes

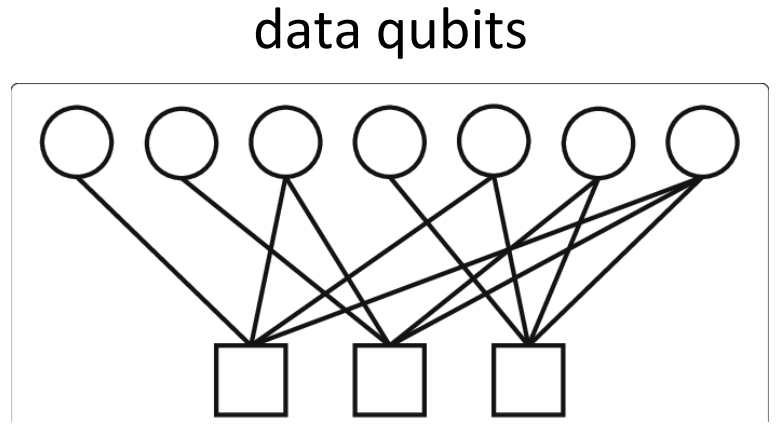
The *n* physical qubits obey *n*-*k* constraints ("checks"), leaving *k* "logical" qubits.

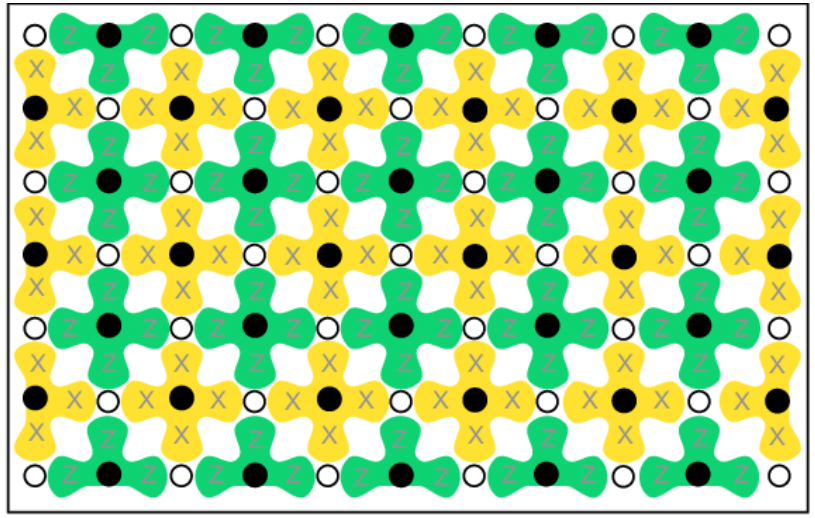
Each logical operator acts on at least *d* physical qubits ("distance" *d*).

Each constraint acts on few physical qubits, and each physical qubit is involved in few constraints.

Surface code: checks are geometrically local in 2 dimensions. *k*=1 logical qubits per block.

High-rate codes: large *k* and *d* via nonlocal connectivity.





surface code

The joy of nonlocal connectivity

Long-range connections might require complex fabrication in solid state devices.

More natural for movable qubits in ion traps and neutral atom arrays.

Higher encoding rates with quantum low-density parity-check (qLDPC) codes. Reduced number of physical qubits, high threshold, feasible decoders.

Universal gate gadgets for qLDPC codes with reduced spacetime cost.

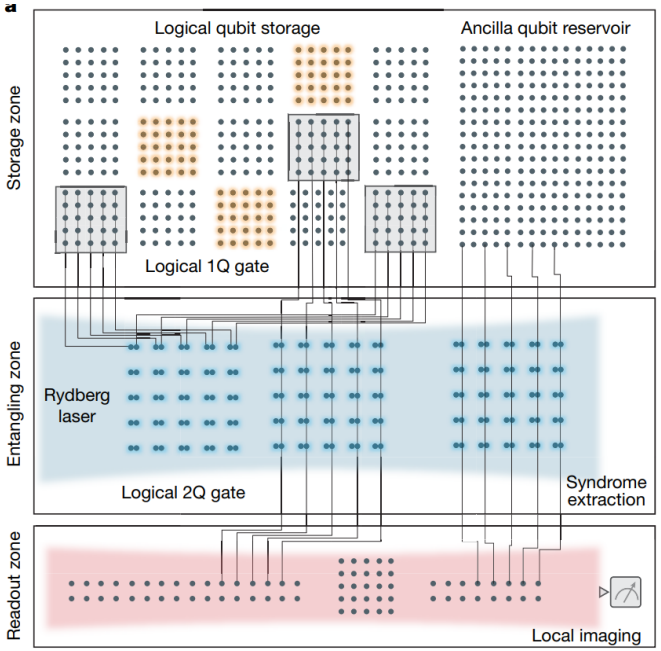
These advantages partially compensate for the slow clock speed.

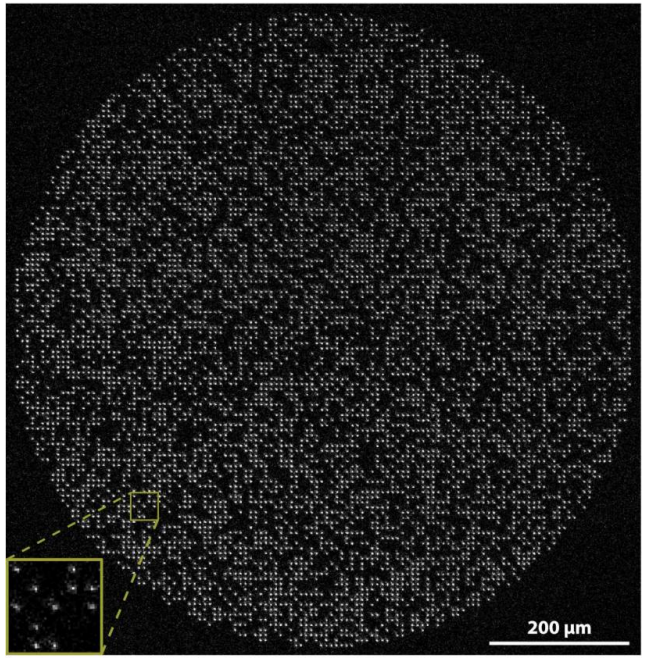
Neutral atoms in optical tweezer arrays

Traveling qubits for measuring nonlocal check operators.
Efficient logical operations on high-rate code blocks.
Pursued by companies, but so far universities have been leading innovation.
Likely to be the leading near-term quantum computing architecture.

Logical processor based on reconfigurable atoms arrays

Lukin Lab (Harvard)
Nature 2024





Tweezer array with 6100 highly coherent atomic qubits

Endres Lab (Caltech)
Nature 2025

What *are* these things?

Bivariate Bicycle (BB) Codes
Hypergraph Product (HGP) Codes
Quasi-Cyclic Lifted Product (LP) Codes
Quantum Tanner Codes
Syndrome decoding by Belief Propagation (BP)
Pauli-Based Computation (PBC)
Surgery
Algorithmic Fault Tolerance (AFT)
And lots of other stuff!

Quantum Physics

[Submitted on 9 Jun 2026]

Handbook of Error-Correcting Codes

Victor V. Albert, Philippe Faist

Barcode scans, clear phone calls, reliable data storage, satellite communication, and large-scale quantum computation are all made possible by error correction. We present a handbook version of The Error Correction Zoo, a curated reference of methods for protecting classical or quantum information from errors during storage and transmission. The handbook includes descriptions of these error-correcting codes and a classification according to the symbols they use. It also catalogues relations among codes and related objects such as sphere packings, lattices, designs, groups, and classical and quantum phases of matter. The collection is intended both as a rigorous reference and as a practical aid for tracing the web of code relationships and uncovering new connections.

Comments: 440 classical codes, 619 quantum codes, 15 c-q codes. Online zoo at this https URL. Notify zookeeper of errors or issue a pull request at this https URL

Subjects: **Quantum Physics (quant-ph)**; Strongly Correlated Electrons (cond-mat.str-el); Information Theory (cs.IT); Combinatorics (math.CO); Metric Geometry (math.MG)

https://preskill.caltech.edu/ph219/ph219_2026.html

Ph219/CS219
Quantum Computation
Spring 2026

Course description: Ph/CS 219C is the third term in a three-term course on quantum computation and quantum information science. Topics covered in 219A included density operators, quantum operations, quantum entanglement, quantum circuits, and quantum algorithms. Ph/CS 219B covered quantum error correction and fault-tolerant quantum computing.

Ph/CS 219C will build on 219B by covering additional topics related to error correction and fault tolerance as well as other topics to be decided. But the course should be accessible to students who did not take 219B.

Instructor:
John Preskill, 206 Annenberg, X-6691, email: preskill(at)caltech(dot)edu

Teaching assistants:
Kyle Gulshen, email: kgulshen(at)caltech(dot)edu
Preksha Naik, email: pnaik(at)caltech(dot)edu
TA Office hours: Tuesdays on weeks where problem sets are due. Tuesday 2-3pm in Downs 107. Please also feel free to email TAs any time to request additional office hours.

Class meetings:
Monday and Wednesday 2:30 – 3:55 pm in 269 Lauritsen, starting March 30. The lectures are in-person only and will not be recorded.
There will be no lecture on May 6.

Homework assignments and grading:
The course is graded pass-fail. Homework will be submitted, and graded homework will be returned, using Canvas.

You may receive partial credit if you describe a thoughtful approach to the problem, even if you are unable to solve it completely.

References:
The primary reference for most of the lectures will be these lecture notes (JP). Other useful books are *Quantum Computation and Quantum Information* by Nielsen and Chuang (NC), *Classical and Quantum Computation* by Kitaev, Shen, and Vyalyi (KSV), *Quantum Computing Since Democritus* by Aaronson, *The Theory of Quantum Information* by Watrous, and *Quantum Information Theory* by Wilde.
Other recommended lecture notes: John Watrous, Umesh Vazirani, Andrew Childs, Scott Aaronson, Ronald de Wolf
The first few weeks of the course will draw on material in Chapter 7 of the lecture notes. Notes and references for subsequent lectures will be posted.

Lectures:
March 30 and April 1: Lectures 1 and 2. Error correction review, erasure and correctability. 7.3, 7.10
April 6 and 8: Lectures 3 and 4. Cleaning lemma, bounds on local codes, string operators. 7.14, 7.19, 7.20
April 13: Lecture 5. Codes from circulant matrices and polynomials. Notes.
April 15: Lecture 6. Bivariate bicycle codes. Notes. Reference.
April 20: Lecture 7. Hypergraph product codes. Notes. Reference.
April 22: Lecture 8. Chain complexes and CSS codes. Notes.
April 27: Lecture 9. Lifted product codes. Notes. Reference.
April 29: Lecture 10. Syndrome decoding. Notes. Reference 1. Reference 2.
May 4: Lecture 11. Belief propagation. Notes.
May 6: No Lecture.
May 11: Lecture 12. Quantum computing by measurement. Notes.
May 13: Lecture 13. Pauli-based computation. Notes. Reference.
May 18: Lecture 14. One-way quantum computer. Notes.
May 20: Lecture 15. Lattice surgery. Notes. Reference 1. Reference 2.
May 27: Lecture 16. Gauging logical operators. Notes. Reference.
June 1: Lecture 17. Algorithmic fault tolerance. Notes. Reference 1. Reference 2.
June 3: Lecture 18. Clifford hierarchy. Notes. Reference.

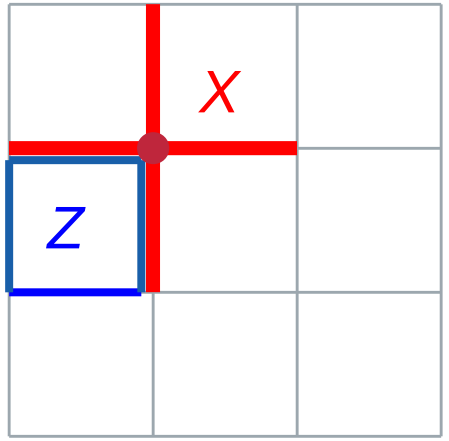
See here for notes and references

Calderbank–Shor–Steane (CSS) codes

A quantum code from two classical linear codes

H_X X-type checks

H_Z Z-type checks



Even overlap

Commuting checks

$$H_Z \, H_X^T = 0 = H_X \, H_Z^T$$

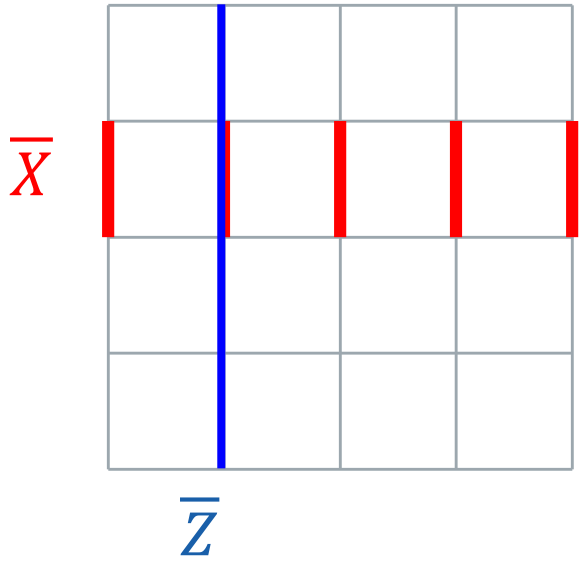
All matrix arithmetic is over $\mathbb{F}_2$.

Logical operators and distance

$$L_X = \ker(H_Z) \,/\, \mathrm{im}(H_X^T)$$

$$L_Z = \ker(H_X) \,/\, \mathrm{im}(H_Z^T)$$

Commute with every check.
Not a product of checks.



(Periodic B.C.)

Distance:

d_X Minimum weight of a nontrivial logical X.

d_Z Minimum weight of a nontrivial logical Z.

Cyclic symmetry

Translation symmetry as a permutation matrix

$$x = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$x^T = x^{-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1$

$1 \rightarrow 4 \rightarrow 3 \rightarrow 2 \rightarrow 1$

$x^n = I$ if *x* is an n x n matrix.

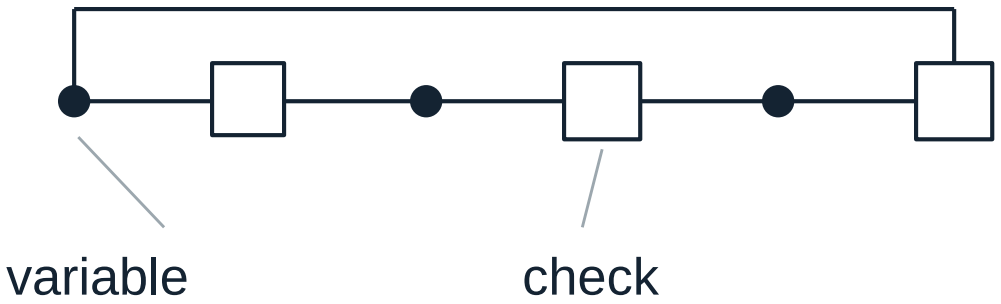
Circulant matrices as polynomials

$$A = c_0\, I + c_1\, x + c_2\, x^2 + \cdots + c_{n-1}\, x^{n-1}$$ determined by 1st row (or column).

$R = \mathbb{F}_2[x] \,/\, (x^n - 1)$ Ring of commuting circulant binary matrices.

Repetition code on a cycle

$$H = 1 + x = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$



Matrix multiplication becomes polynomial multiplication.

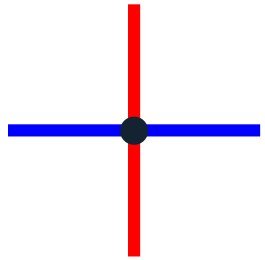
Toric code from polynomials

(L x M torus)

Two cyclic symmetries: x (hor) and y (vert). $x^L = 1 = y^M$

Register 1: vertical edges

Register 2: horizontal edges



Star: X check

$$H_X = (1 + y,\ 1 + x)$$

$$H_Z = (1 + x^{-1},\ 1 + y^{-1})$$

Plaquette: Z check

Checks commute:

$$H_X\, H_Z^T = (1 + y)(1 + x) + (1 + x)(1 + y) = 0$$

Haah 2013

Bivariate bicycle (BB) codes

Two cyclic symmetries. Two qubit registers.

$$H_X = (A(x,y), B^T(x,y))$$

$$H_Z = (B(x,y), A^T(x,y))$$

Checks commute:

$$H_X H_Z^T = AB^T + B^T A = 0$$

Check weight = number of polynomial terms

k logical qubits: number of independent relations among the checks

The Gross code

$[[n, k, d]] = [[144, 12, 12]]$ $x^{12} = 1 = y^6$ (12 x 6 torus)

$A' = y^{-1} A = 1 + y + y^{-1}x^3$

$(B')^T = x^{-1} B^T = 1 + x + x^{-1}y^3$

(Check weight 6)

Toric-code terms plus two more with longer reach:

X check includes:

Register 1	3 right, 1 down
Register 2	1 left, 3 up

Bravyi et al. (IBM) 2024

Hypergraph product (HGP) codes

A: $r_A \times n_A$ matrix (horizonal), B: $r_B \times n_B$ matrix (vertical)

$$H_X = (A \otimes I_{n_B}, I_{r_A} \otimes B^T) \qquad r_A\, n_B\ X\text{checks}$$

$$H_Z = (I_{n_A} \otimes B, A^T \otimes I_{r_B}) \qquad n_A\, r_B\ Z\text{checks}$$

Reg 1: $n_A\, n_B$ qubits Reg 2: $r_A\, r_B$ qubits

$$H_X\, H_Z^T = A \otimes B^T + A \otimes B^T = 0$$

Two registers: checks commute

Tillich, Zemor 2013

HGP rate and check weight

$$H_X = (A \otimes I_{n_B}, I_{r_A} \otimes B^T)$$

$$n = n_A\, n_B + r_A\, r_B$$

$$H_Z = (I_{n_A} \otimes B, A^T \otimes I_{r_B})$$

$$k \geq n - r_A\, n_B - n_A\, r_B = (n_A - r_A)(n_B - r_B) = \#\text{qubits - }\#\text{checks}$$

$$k = k_A\, k_B + k_{A^T}\, k_{B^T}$$ (Künneth formula)

HGP of high-rate classical codes = high-rate quantum code.

X-check weight = A-row weight + B-column weight

Z-check weight = B-row weight + A-column weight

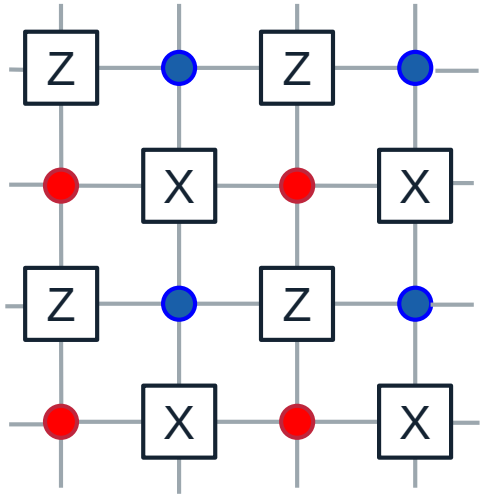
Low classical weight
yields low quantum weight

Toric code as HGP of classical repetition codes

Repetition code

Transpose code

Same code!



$$H_X = (A \otimes I, I \otimes B^T)$$ hor on Reg 1, vert on Reg 2

$$H_Z = (I \otimes B, A^T \otimes I)$$ hor on Reg 2, vert on Reg 1

Checks are weight 2 + 2 = 4. It's the toric code again, with $d_{\text{toric}} = d_{\text{rep}}$

Distance of HGP code

$d = \min(d_A, d_B, d_{A^T}, d_{B^T})$ For example, $d_{\text{toric}} = d_{\text{rep}}$

Suppose two classical codes have k= Θ(n) and d= Θ(n).

Their hypergraph product has high rate and square root distance:

$$k = \Theta(n) \qquad d = \Theta(\sqrt{n})$$

We may also consider “higher-dimensional” products.

Useful for non-Clifford gates and more robust syndrome extraction (“metachecks”).

Lifted product (LP) codes

$$H_X = (A \otimes I_{n_B}, I_{r_A} \otimes B^T) \qquad A \text{ is } r_A \times n_A$$

$$H_Z = (I_{n_A} \otimes B, A^T \otimes I_{r_B}) \qquad B \text{ is } r_B \times n_B$$

Keep the HGP structure. But replace entries by elements of polynomial ring:

$R = \mathbb{F}_2[x] \,/\, (x^\ell - 1)$ e.g., monomials: $x^m, m \in \{0, 1, 2, \ldots, \ell-1\}$

“Lift” the “seed matrices” *A* and *B* by adding a “fiber” above each point in a 2D “base space.”

Compared to the seed code, the number of qubits and the number of checks increases by the factor ℓ, without increasing the check weight if the entries are monomials.

Panteleev, Kalachev 2021

A lifted-product example

$$H_X = (A \otimes I_{n_B}, I_{r_A} \otimes B^T)$$

$$H_Z = (I_{n_A} \otimes B, A^T \otimes I_{r_B})$$

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & x^{14} & x^{19} & x^{11} & x^{26} \\ 1 & x^{13} & x^{2} & x^{15} & x^{21} \end{pmatrix}$$

$$A = B, \quad \ell = 33$$

$n = (5^2 + 3^2)33 = 1122$

5 × 3 × 33 = 495 checks of each type.

$k \geq 1122 - 2(495) = 132$

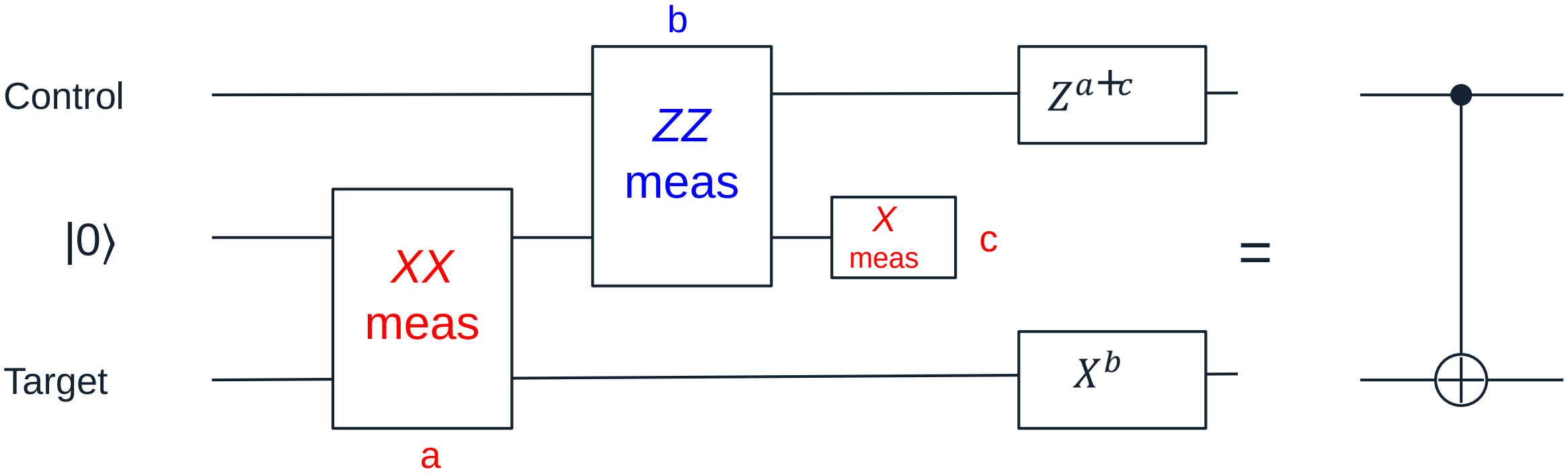
$k = 148$ $\quad$ $d \leq 20$

Check weight 5 + 3 = 8.

Very large matrices with a simple structure, admitting compact presentation.

Cain, Xu et al. 2026

CNOT by nondestructive measurement



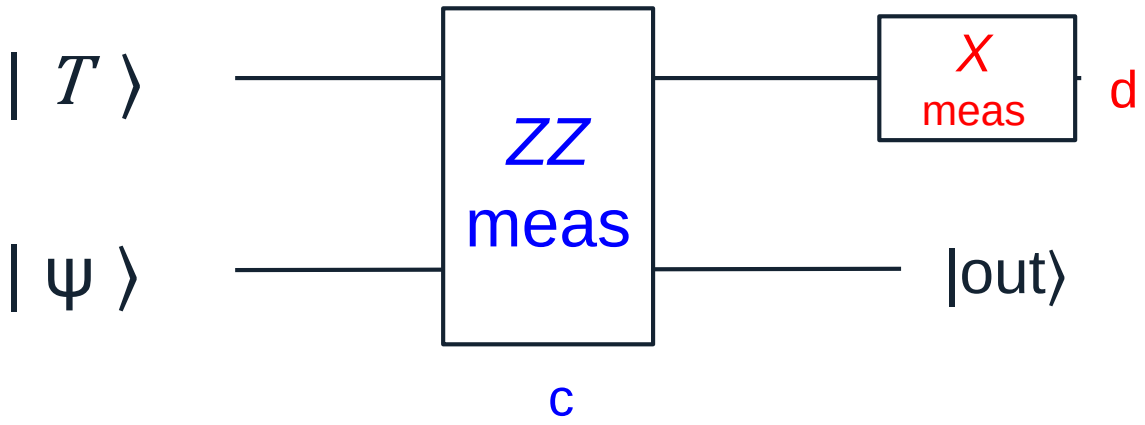
Measurement outcomes: $(-1)^a, (-1)^b, (-1)^c$

Track the corrections in the Pauli frame.

A T gate from a magic state

$T = \mathrm{diag}(1, e^{i\pi/4})$

$|T\rangle = (|0\rangle + e^{i\pi/4}|1\rangle) / \sqrt{2}$



$c = 0$: $T|\psi\rangle$

$c = 1$: $T^{-1}|\psi\rangle$

Up to a Pauli correction

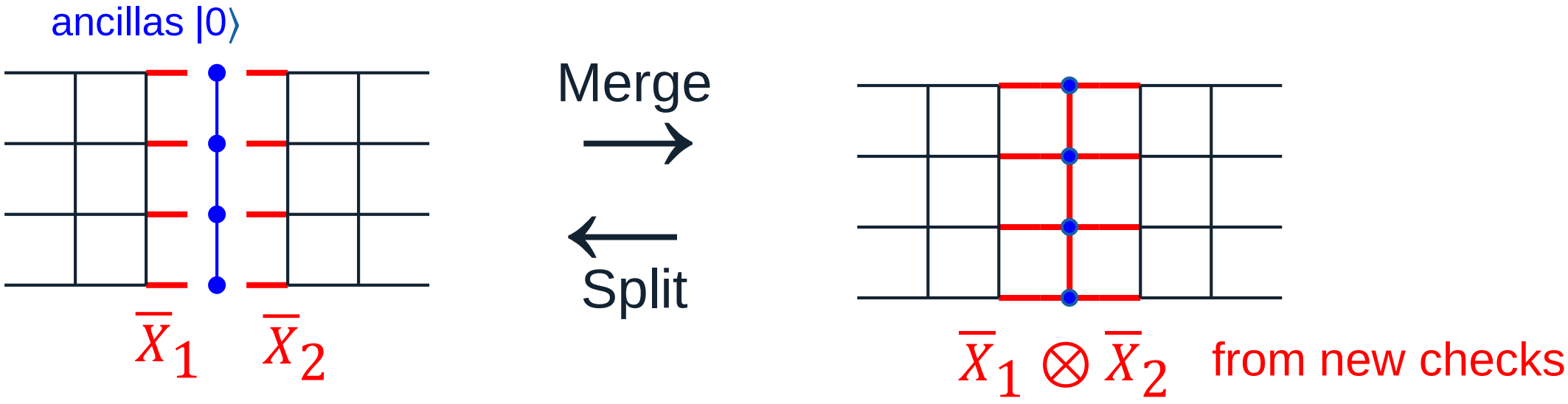
Conditional $S = T^2$ correction gives T in either case.

Magic-state prep + nondestructive Pauli-product measurement are all you need!

Bravyi, Smith, Smolin 2016

Pauli-product measurement by surgery

Measure $\overline{X}_1 \otimes \overline{X}_2$ for two surface code blocks.



Deform: the target logical Pauli product is a product of low-weight checks in deformed code.

Measure for O(d) rounds to determine checks robustly, then restore the original code.

Generalize: High-weight Pauli products in surface code.
Extend to deformations of high-rate codes.

Horsman, Fowler, Devitt, Van Meter 2012

What *are* these things?

Bivariate Bicycle (BB) Codes
Hypergraph Product (HGP) Codes
Quasi-Cyclic Lifted Product (LP) Codes
Quantum Tanner Codes
Syndrome decoding by Belief Propagation (BP)
Pauli-Based Computation (PBC)
Surgery
Algorithmic Fault Tolerance (AFT)
And lots of other stuff!

Prospects for the next few years

Encouraging progress toward scalable fault-tolerant quantum computing.

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

The most important applications of quantum computing are likely to be ones we have not yet imagined.

The most important ideas in physics in recent decades?

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 $n >> k$ 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.

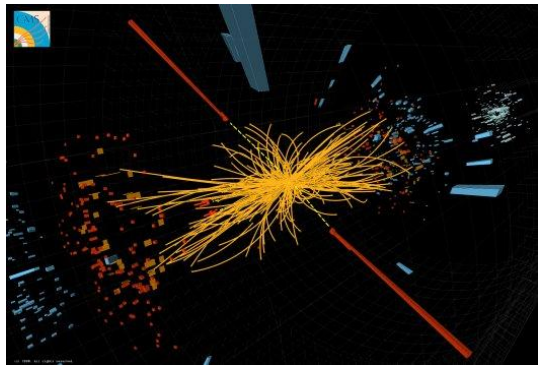
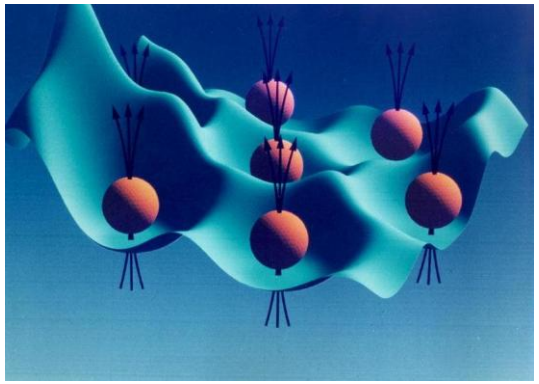
An electron in a topological phase can split into pieces, each carrying a fraction of the electron's charge.

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
		
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