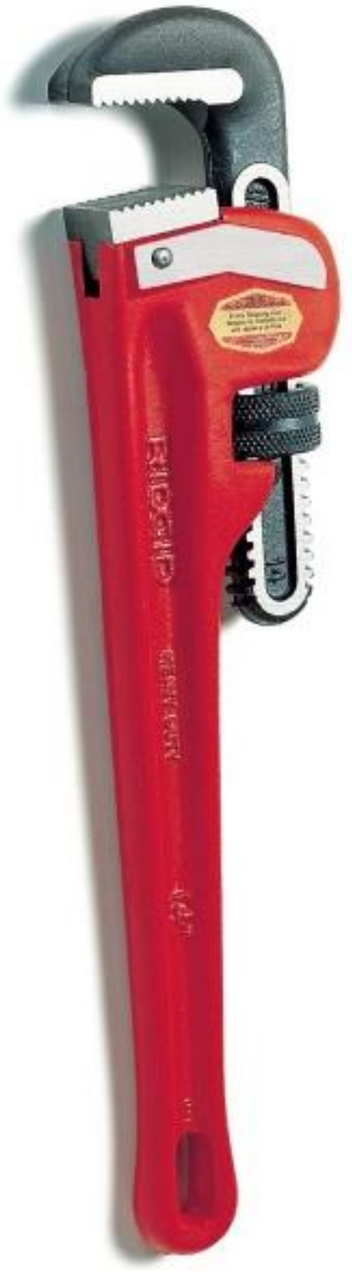
Introduction to **Quantum Computation**

Daniel Nagaj

universität wien



ICTP-VAST-APCTP winter school
Hanoi, 12/2013

0 Review: algorithms

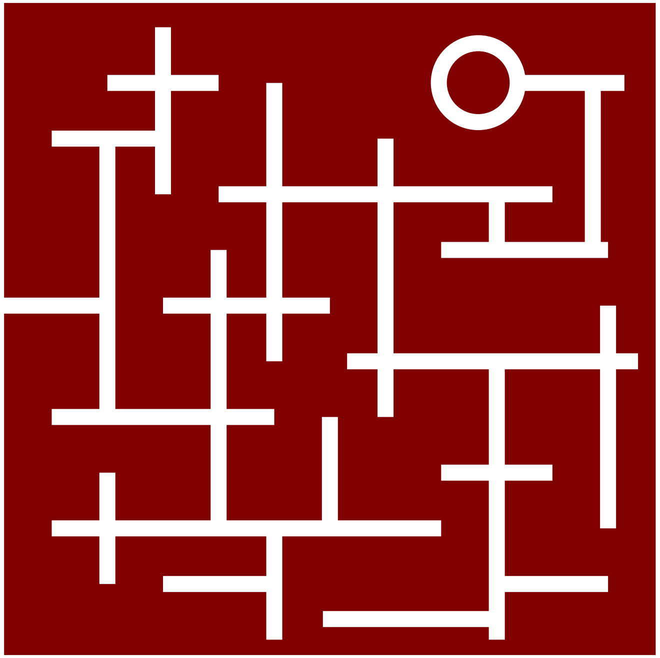
- quantum information/computing is good for ...

- quantum computation essentials

superposition

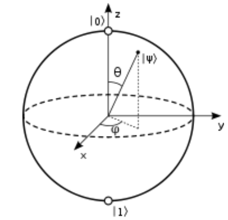
interference

entanglement



1 **we need a qubit**

and we can use it

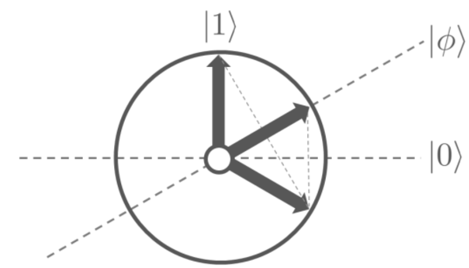


2 **EPR pairs**

give us cool 2-qubit protocols

3 **the algorithms**

that make quantum computing tick

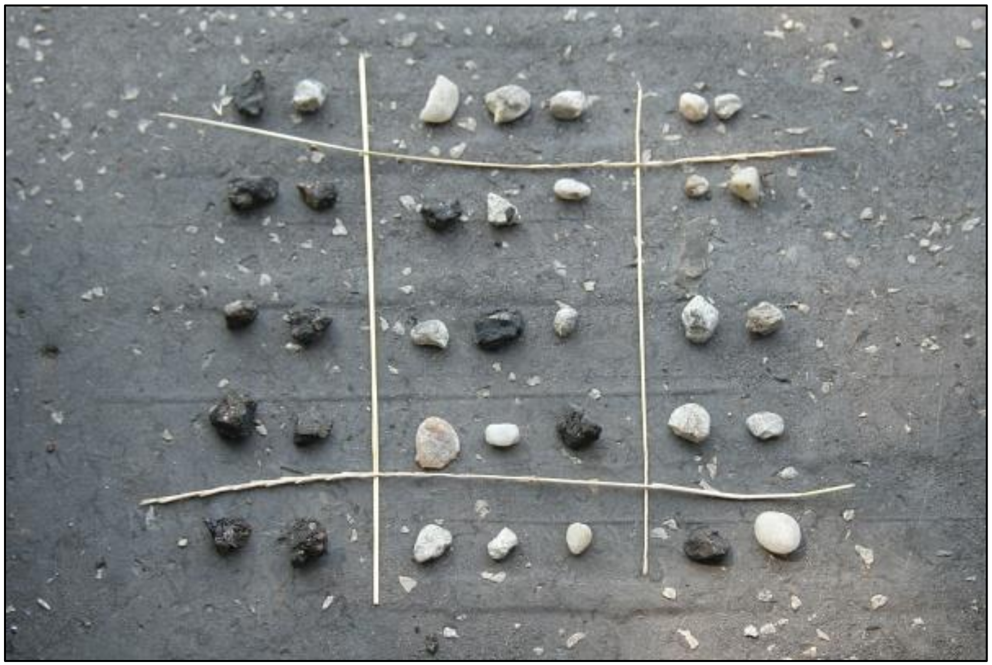


4 **error correction**

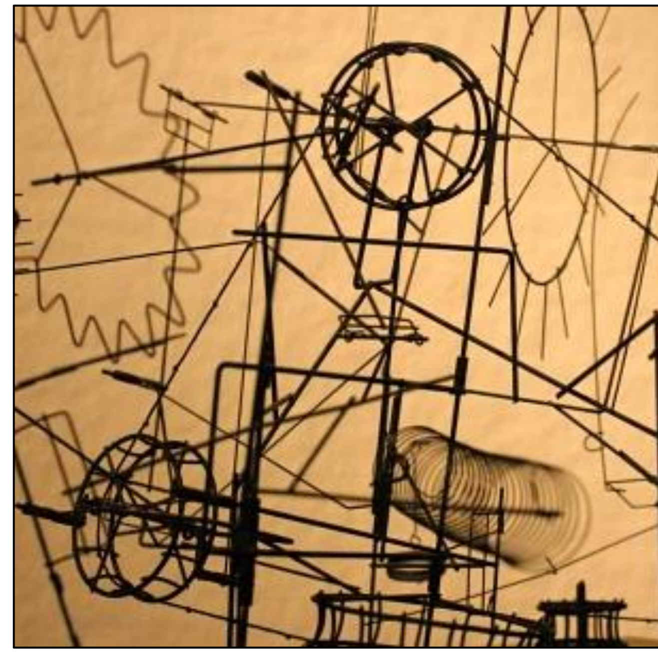
can we really scale up this stuff?


PHỐ
G BUỒM

What/how does nature allow us to compute?



Won't it quickly break down?



Exact computation with imprecise elements in a noisy environment?

1 Quantum computation & qubits

- qubits instead of bits

  statest in a Hilbert space

$$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

- time evolution

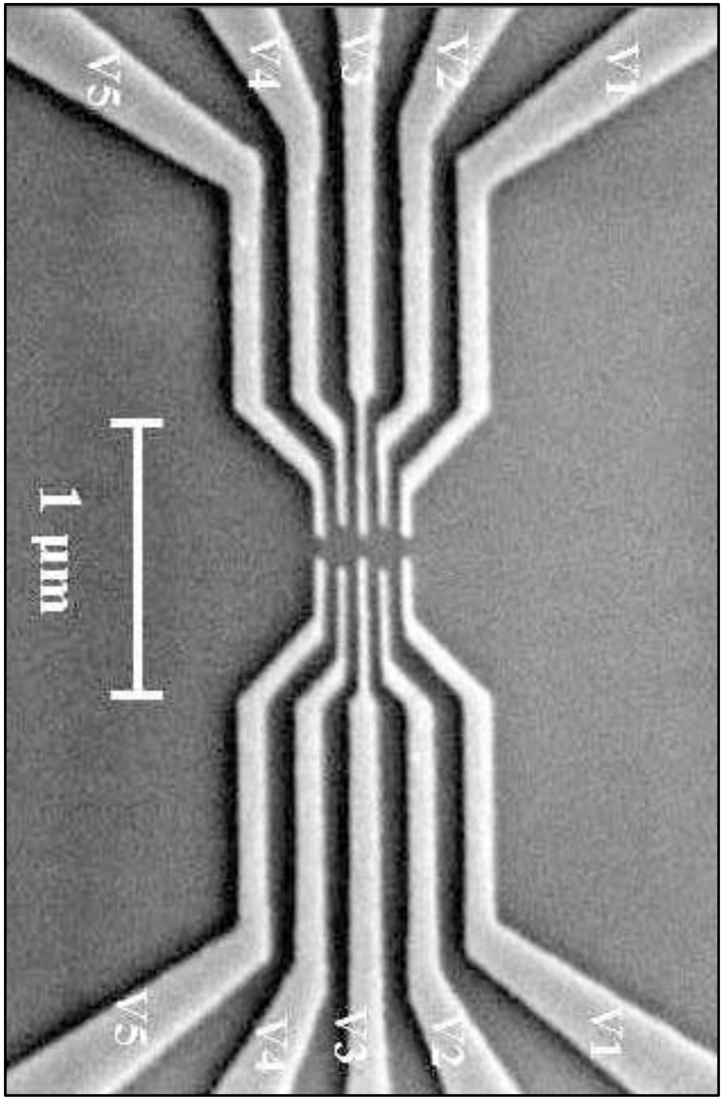
  Schrödinger equation

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

  unitarity

$$|\psi(t)\rangle = U_{t,0}|\psi(0)\rangle$$

- a final measurement



[a quantum dot, Purdue University]

1 Quantum computation & qubits

- qubits instead of bits

  statest in a Hilbert space

$$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}$$

- time evolution

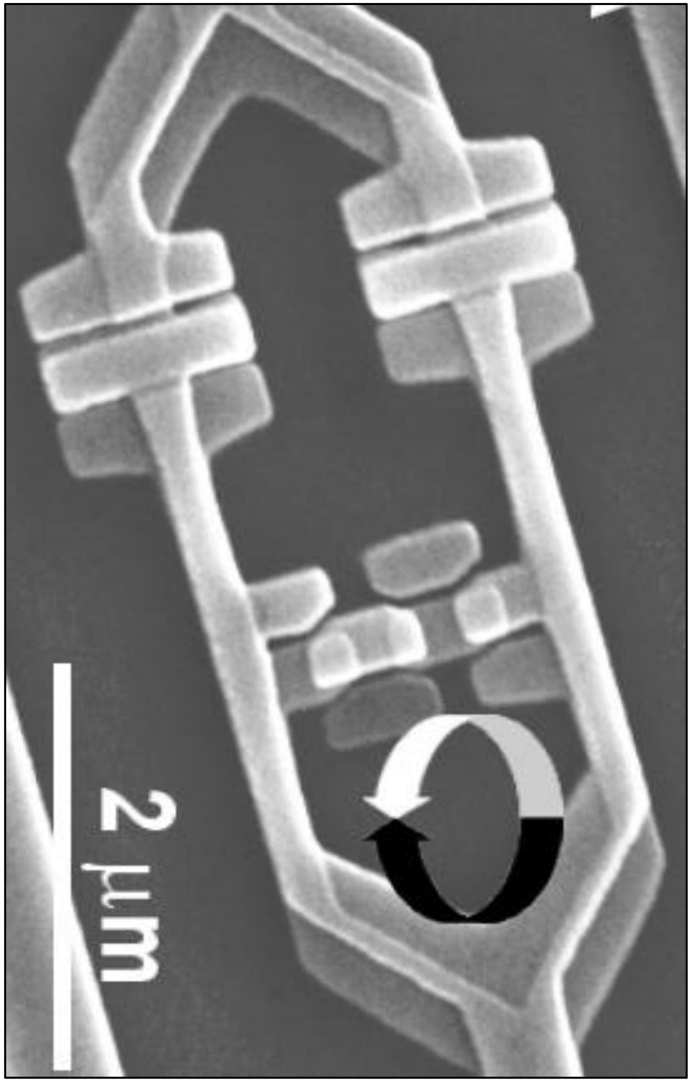
  Schrödinger equation

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

  unitarity

$$|\psi(t)\rangle = U_{t,0}|\psi(0)\rangle$$

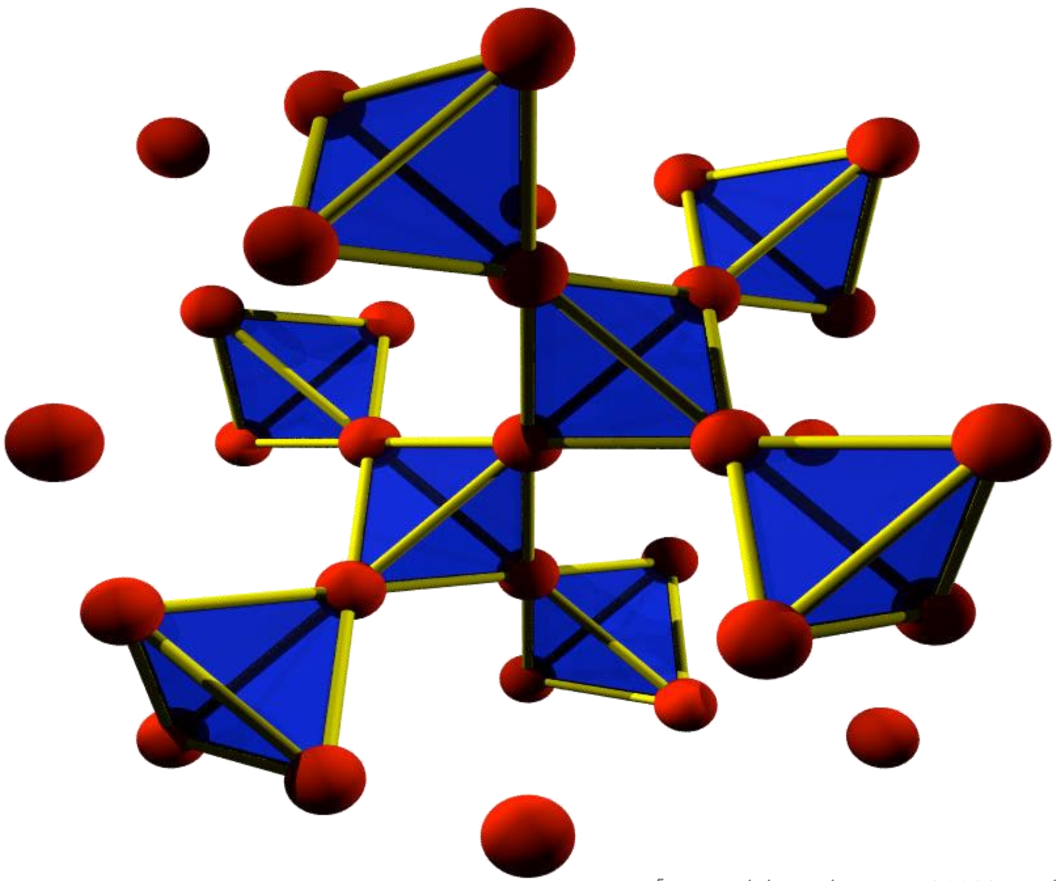
- a final measurement



[a superconducting flux qubit, Florida State Uni.]

1 Quantum computation & qubits

- *N* qubits



[pyrochlore lattice, U Waterloo]

$$2^N$$

ground state?

evolution?

control?

1 Quantum circuits

- single-qubit operations

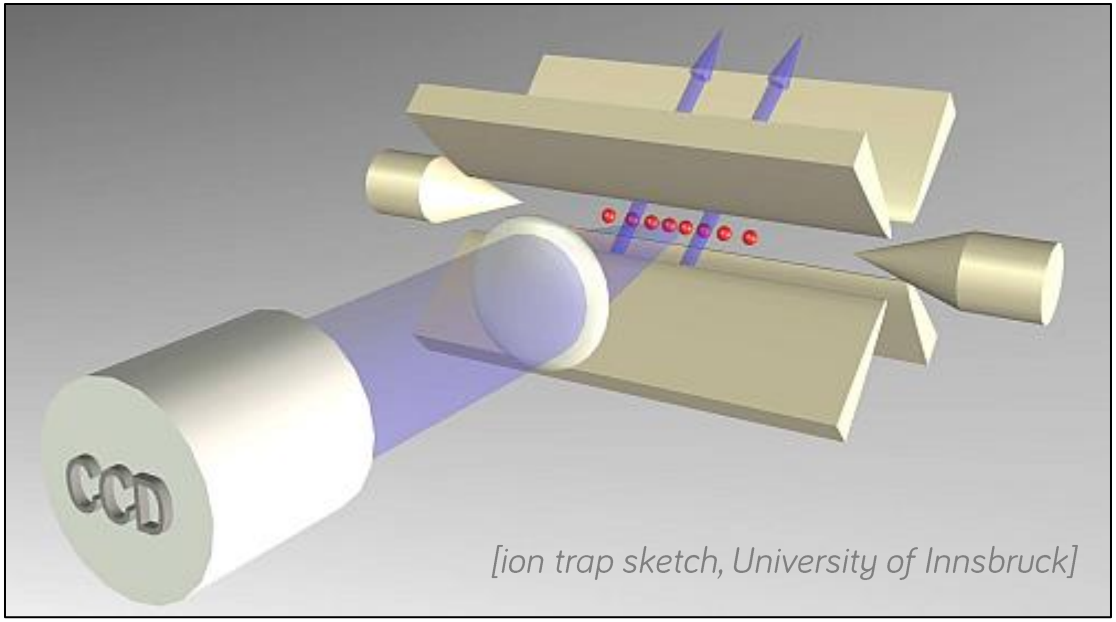
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

controlled 2-qubit gates

$$\begin{aligned} \text{CNOT} &= |0\rangle\langle 0|_1 \otimes \mathbb{I}_2 \\ &+ |1\rangle\langle 1|_1 \otimes \sigma_2^x \end{aligned}$$

- output
  Z-basis
  measurements

- reality:
  decoherence
  imprecise control



[ion trap sketch, University of Innsbruck]

1 DiVincenzo criteria for quantum computation

- well-defined qubits

$$|0\rangle \quad |1\rangle$$

- (pure-state) initialization

$$|000\cdots 0\rangle$$

- universal gate set

$$R_x^\varphi, R_Z^\varphi, \mathrm{CNOT}$$

- comp. basis measurement

$$|0\rangle\langle 0|, |1\rangle\langle 1|$$

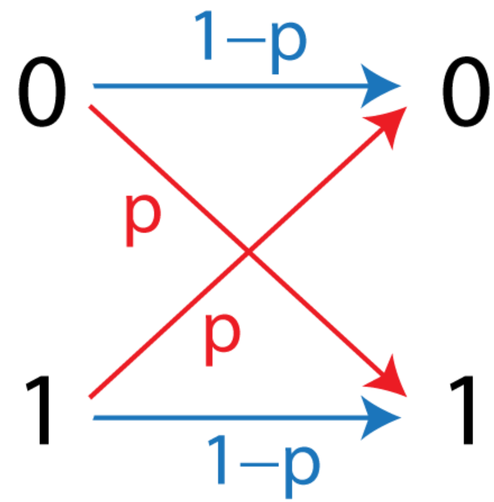
- long coherence times

$$\left(|0\rangle + |1\rangle\right)/\sqrt{2}$$

+ scalability
+ (flying qubits)

1 Simple (classical) error correction: repetition

- a bit-flip error



- redundant information

$$0 \longrightarrow 000$$
$$1 \longrightarrow 111$$

- majority voting

$$0 \longleftarrow 000, 001, 010, 100$$
$$1 \longleftarrow 011, 101, 110, 111$$

- post-correction error probability

$$3p^2(1-p) + p^3 = O(p^2)$$

1 A quantum no-go: QM is linear … no-cloning

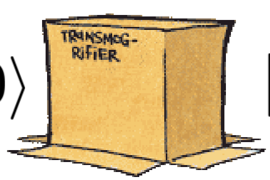
- we can copy orthogonal (classical) states

$$|0\rangle \qquad |1\rangle \qquad\qquad \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

- non-orthogonal states? $|0\rangle \qquad \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

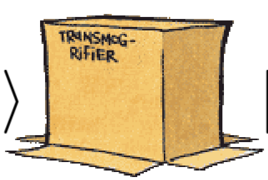
- let's have a cloning machine

$|0\rangle\,|0\rangle$



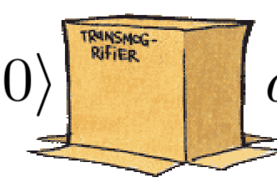
$|0\rangle\,|0\rangle$

$|1\rangle\,|0\rangle$



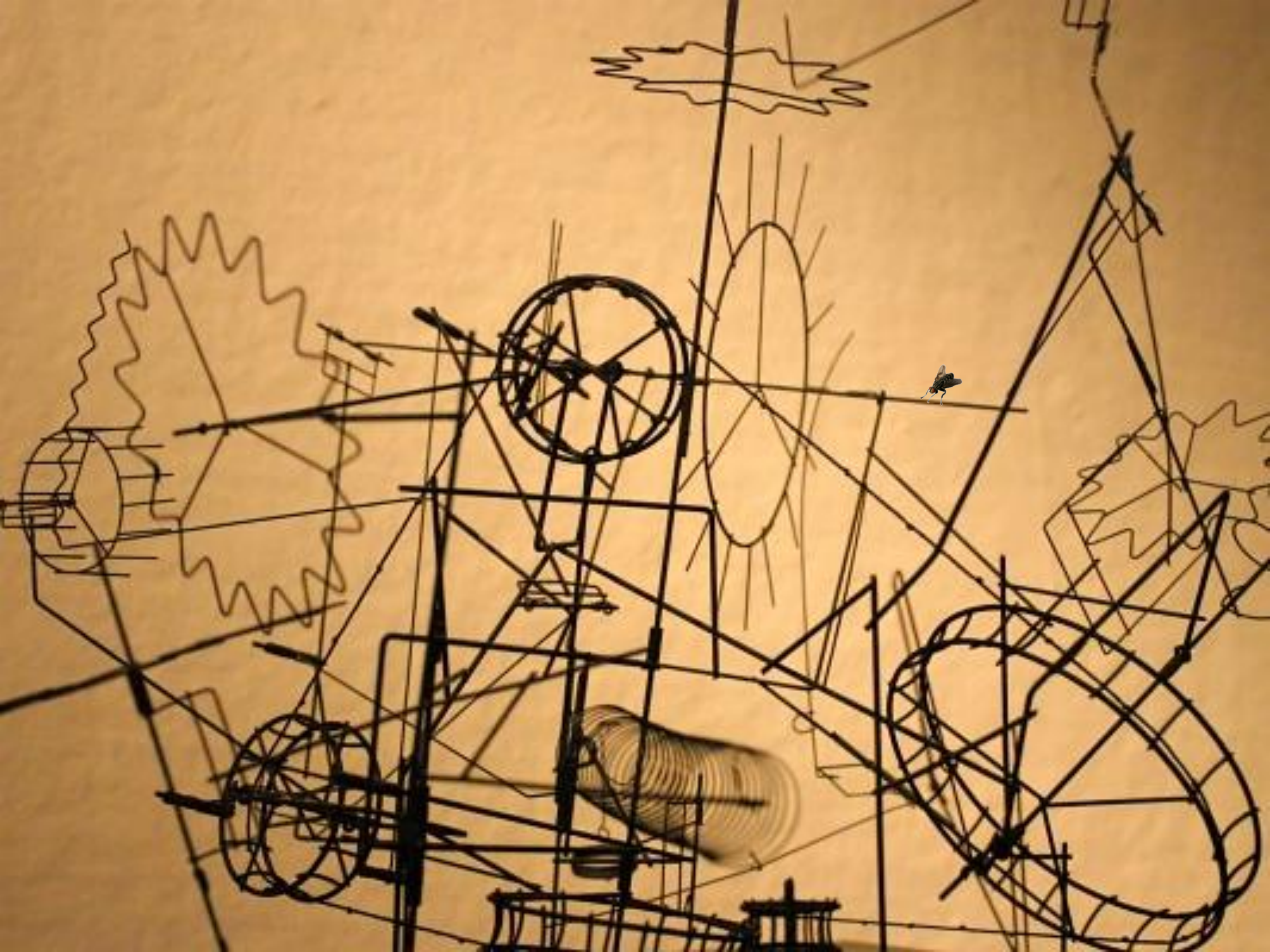
$|1\rangle\,|1\rangle$

$(a\,|0\rangle + b\,|1\rangle)\,|0\rangle$



$a\,|00\rangle + b\,|11\rangle$

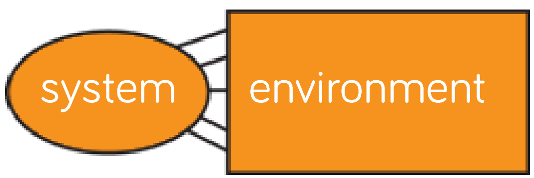
It doesn't work!



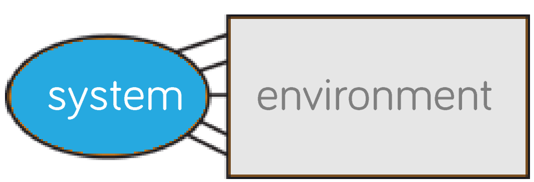
2 Quantum computing & decoherence

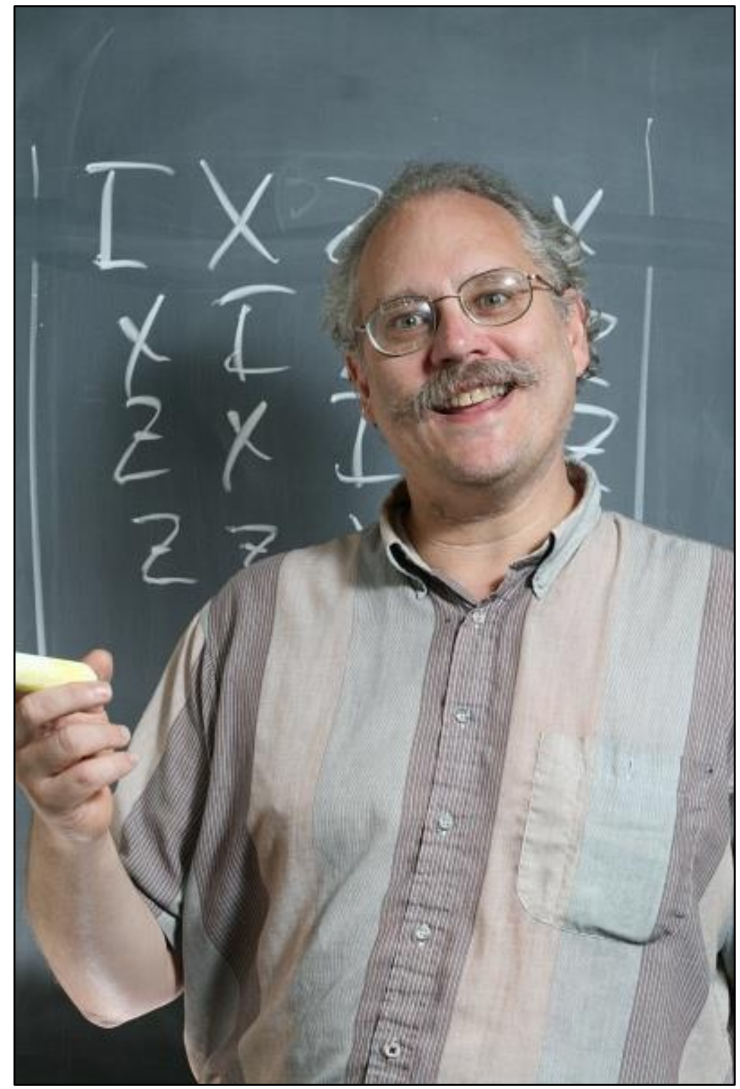
- a perfect computer
  from faulty parts?

$$|\varphi_t\rangle = U_t U_{t-1} \ldots U_2 U_1 |\varphi_0\rangle$$



ρ  $\sum_i E_i \rho E_i^\dagger$





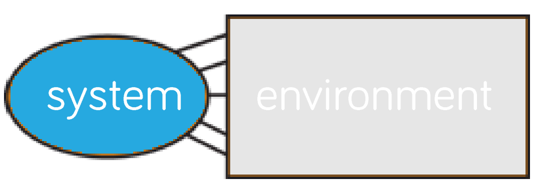
2 Quantum computing & decoherence

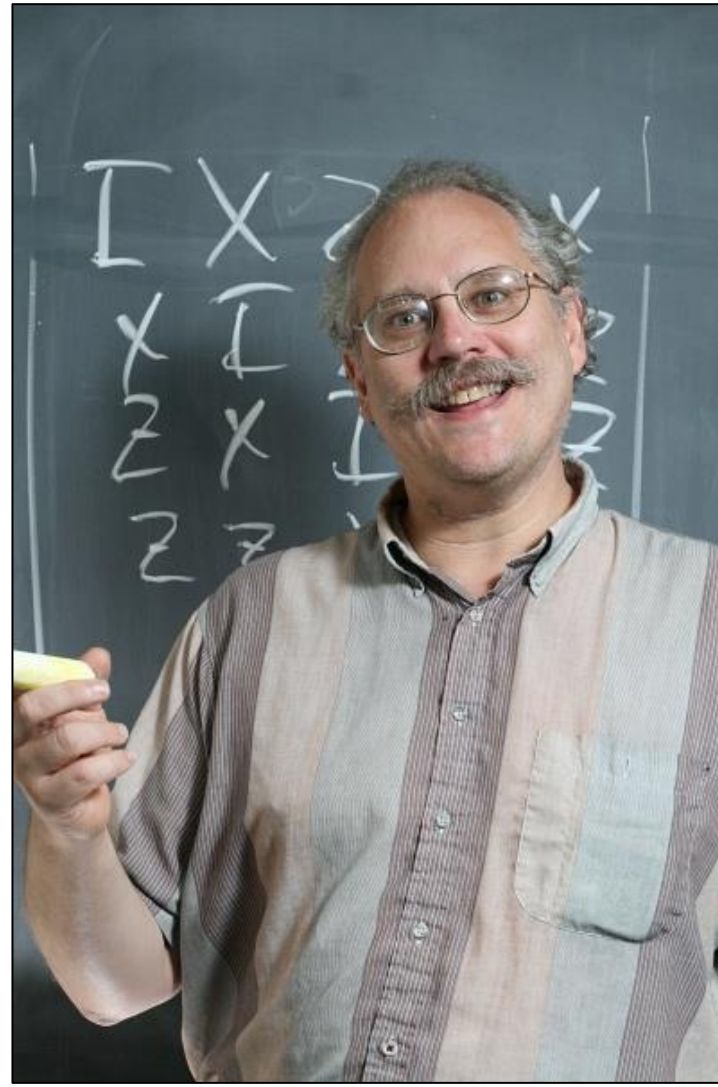
- a perfect computer from faulty parts?

$$|\varphi_t\rangle = U_t U_{t-1} \dots U_2 U_1 |\varphi_0\rangle$$

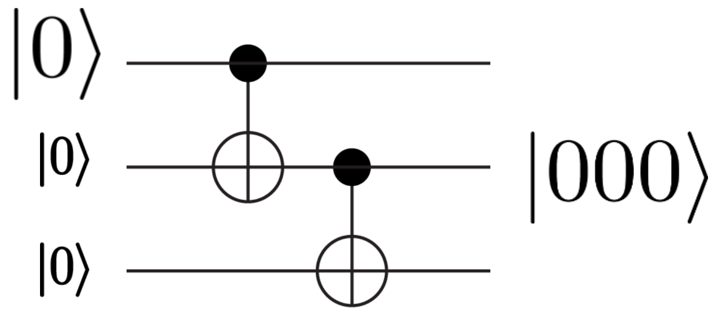
- error correction codes
  [CSS: Calderbank, Shor, Steane]

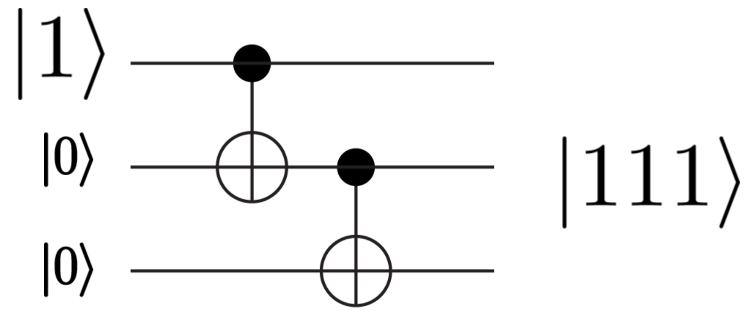
ρ  $\sum_i E_i \rho E_i^\dagger$

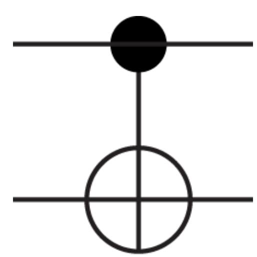




2 The quantum bit-flip code

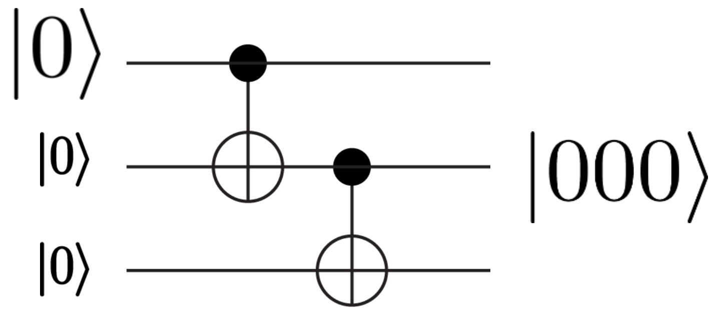


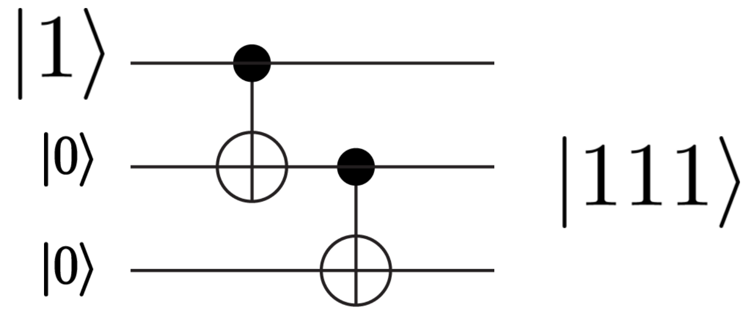


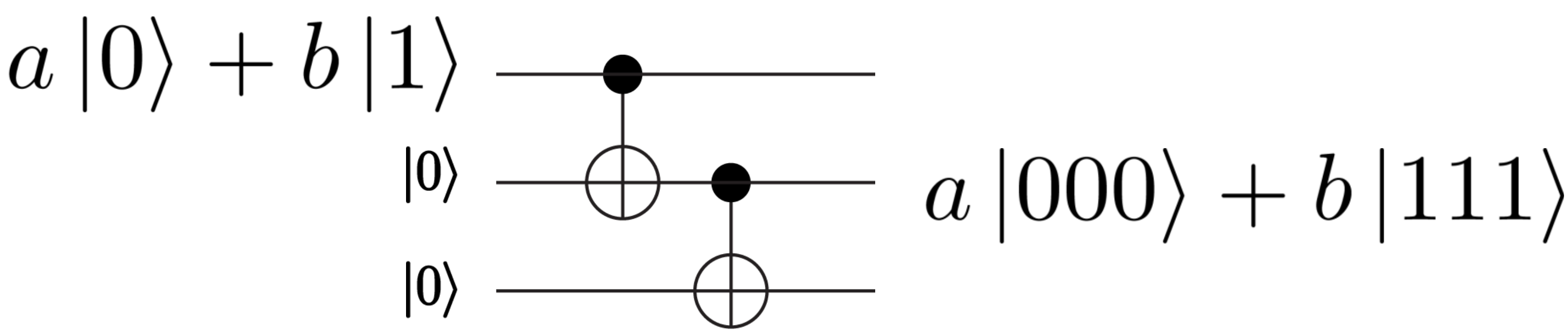


$$
\begin{aligned}
|00\rangle &\rightarrow |00\rangle \\
|01\rangle &\rightarrow |01\rangle \\
|10\rangle &\rightarrow |11\rangle \\
|11\rangle &\rightarrow |10\rangle
\end{aligned}
$$

2 The quantum bit-flip code







2 The quantum bit-flip code

$a|000\rangle + b|111\rangle$

$$a|000\rangle + b|111\rangle$$
$$a|100\rangle + b|011\rangle$$
$$a|010\rangle + b|101\rangle$$
$$a|001\rangle + b|110\rangle$$
$$a|110\rangle + b|001\rangle$$
$$a|101\rangle + b|010\rangle$$
$$a|011\rangle + b|100\rangle$$
$$a|111\rangle + b|000\rangle$$

- how to detect what happened without disturbing the data?
- are there unitaries that leave the code alone?

2 The quantum bit-flip code

- measure: Z_1Z_2 & Z_1Z_3
- nothing: I
  errors: X_1, X_2, X_3

let's repair it … how?

+	+	$a\|000\rangle + b\|111\rangle$
−	−	$a\|100\rangle + b\|011\rangle$
−	+	$a\|010\rangle + b\|101\rangle$
+	−	$a\|001\rangle + b\|110\rangle$
Z_1Z_2	Z_1Z_3	

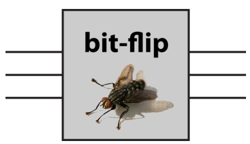
$\downarrow X_3$

$a|000\rangle + b|111\rangle$

2 The quantum bit-flip code

- measure: Z_1Z_2 & Z_1Z_3

- nothing: I
  errors: X_1, X_2, X_3



Z_1Z_2	Z_1Z_3	corrected
+	+	$a\|000\rangle + b\|111\rangle$
−	−	$a\|100\rangle + b\|011\rangle$
−	+	$a\|010\rangle + b\|101\rangle$
+	−	$a\|001\rangle + b\|110\rangle$

$a|110\rangle + b|001\rangle$

$a|101\rangle + b|010\rangle$

$a|011\rangle + b|100\rangle$

$a|111\rangle + b|000\rangle$

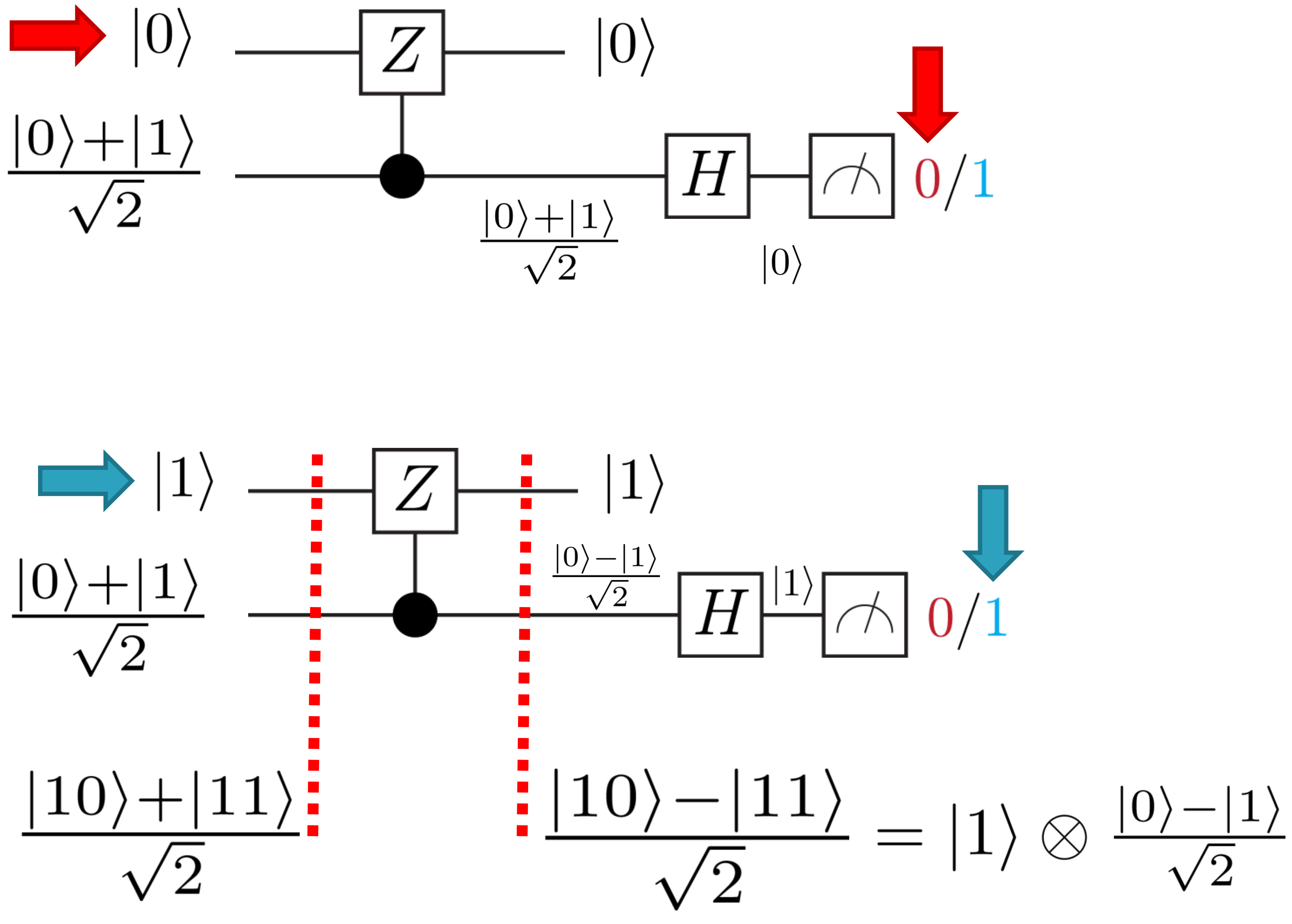
messed up

- post-correction error probability

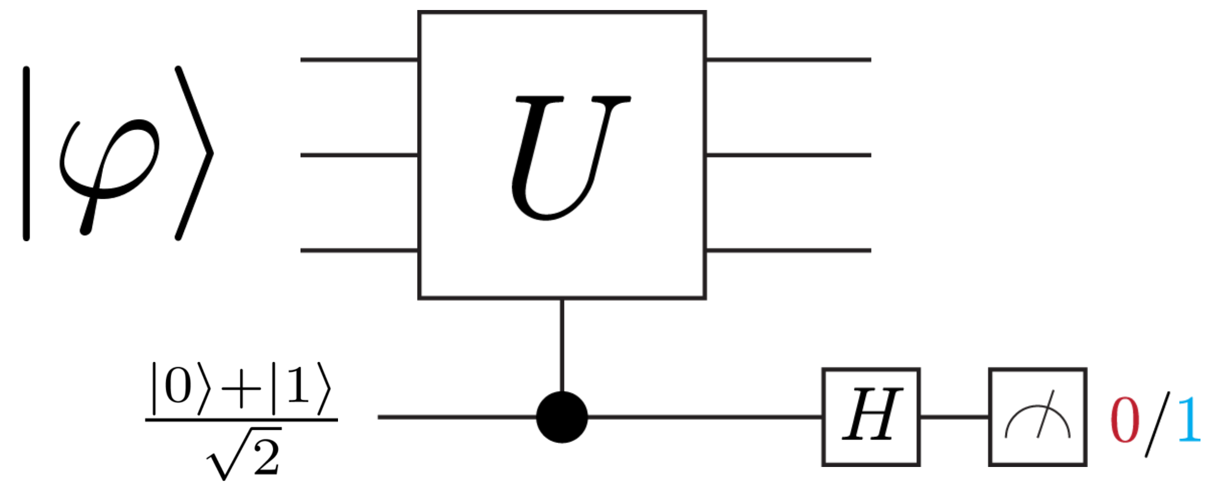
$$3p^2(1-p) + p^3 = O(p^2)$$

- how can we measure Z_1Z_2?

2 Measuring in the eigenbasis of the operator Z



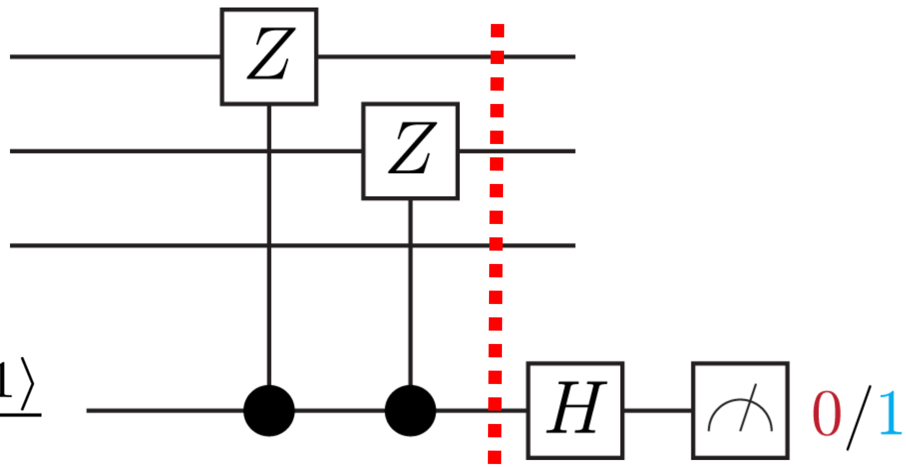
2 Measuring in the eigenbasis of an operator U



2 Measuring in the eigenbasis of the operator Z_1Z_2

$$|\varphi\rangle = a\,|00\alpha\rangle + b\,|11\beta\rangle + c\,|01\gamma\rangle + d\,|10\delta\rangle$$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

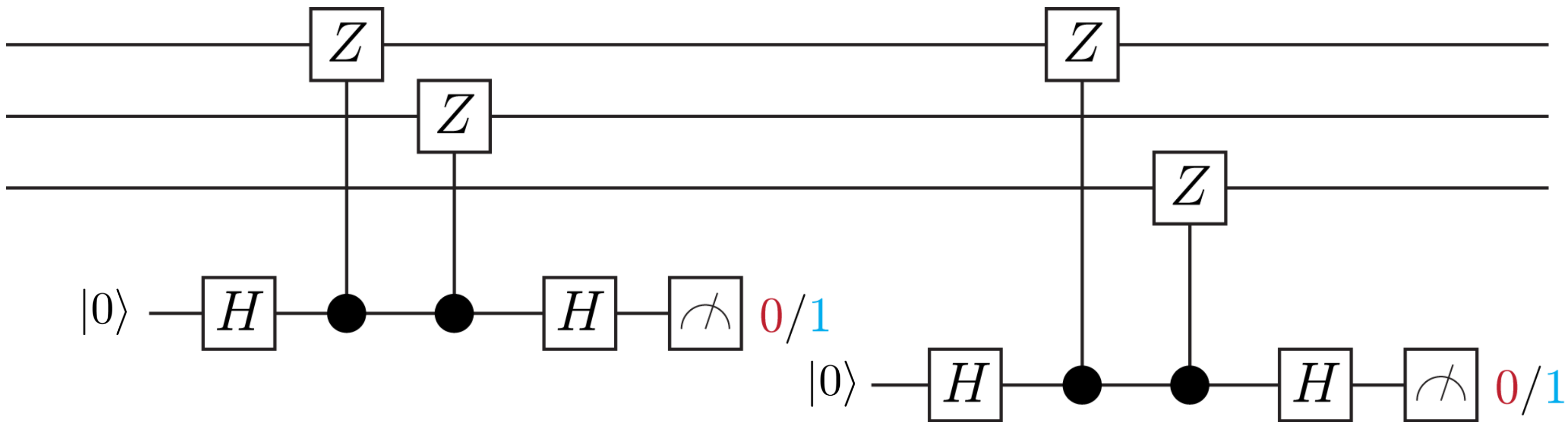


$$(a\,|00\alpha\rangle + b\,|11\beta\rangle) \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} + (c\,|01\gamma\rangle + d\,|10\delta\rangle) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

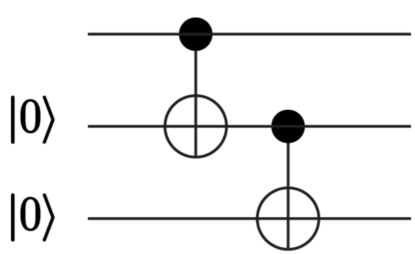
- a projective measurement in the eigenbasis of Z_1Z_2

2 The quantum bit-flip code

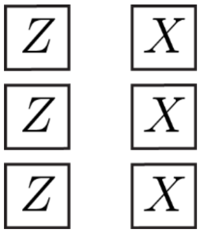
- measure the error, not the data …



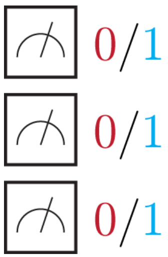
- project into ZZ eigenstates … enforce a scenario … repair
- encoding



operations



decoding



2 Shor's 9-qubit code

- repair 1 bit flip and/or 1 phase flip …

$$|0\rangle \Rightarrow \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \Rightarrow \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

- bit-flip detection (X_k) $Z_1Z_2, Z_1Z_3, Z_4Z_5, Z_4Z_6, Z_7Z_8, Z_7Z_9$
- phase-flip detection (Z_k) $X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$
- 1-qubit Pauli errors
  can be decomposed into
  bit/phase flips: I_k, X_k, Z_k, Y_k ($= iZ_kX_k$)

2 Shor's 9-qubit code

- repair 1 bit flip and/or 1 phase flip …

$$a\,\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+b\,\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

- bit-flip detection (Z_k) Z_1Z_2, Z_1Z_3, Z_4Z_5, Z_4Z_6, Z_7Z_8, Z_7Z_9
- phase-flip detection (X_k) $X_1X_2X_3X_4X_5X_6$, $X_4X_5X_6X_7X_8X_9$
- 1-qubit Pauli errors
  can be decomposed into
  bit/phase flips: I_k, X_k, Z_k, Y_k ($= iZ_kX_k$)

2 Shor's 9-qubit code

- repair 1 bit flip and/or 1 phase flip …

$$a\frac{i(|010\rangle-|101\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$+b\frac{i(|010\rangle+|101\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

- bit-flip detection (Z_k) Z_1Z_2, Z_1Z_3, Z_4Z_5, Z_4Z_6, Z_7Z_8, Z_7Z_9
- phase-flip detection (X_k) $X_1X_2X_3X_4X_5X_6$, $X_4X_5X_6X_7X_8X_9$
- 1-qubit Pauli errors can be decomposed into bit/phase flips: I_k, X_k, Z_k, Y_k ($= iZ_kX_k$)

2 Shor's 9-qubit code

- repair 1 bit flip and/or 1 phase flip ...

$$|0\rangle \Rightarrow \frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \Rightarrow \frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$$

- bit-flip detection (Z_k) $Z_1Z_2, Z_1Z_3, Z_4Z_5, Z_4Z_6, Z_7Z_8, Z_7Z_9$
- phase-flip detection (X_k) $X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$

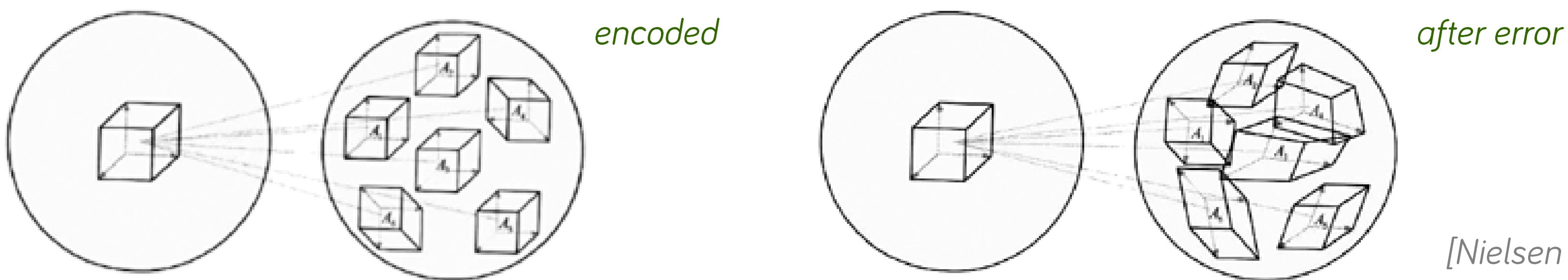
- **repair any 1-qubit error**
  (error discretization)

$$\rho \longrightarrow \sum_i E_i \rho E_i^\dagger$$

3 Stabilizer codes

- a group of n-k stabilizers
  (don't change the code, detect errors)

$$S = \langle g_1, g_2, \ldots, g_{n-k} \rangle$$



[Nielsen & Chuang]

- a Pauli error up to weight $2t$ anticommutes with at least one of the stabilizers

$$\langle x| E(|y\rangle) |x\rangle = \langle x| E_i |y\rangle \langle y| E_i |x\rangle = 0$$

… no codeword overlap after the error

- k logical qubits in n physical ones, repair up to t errors

3 The 5-qubit code

[Knill et al., PRL 86, 5811 (2001)]

- stabilizer & operations

M_1	σ_x	σ_z	σ_z	σ_x	I
M_2	I	σ_x	σ_z	σ_z	σ_x
M_3	σ_x	I	σ_x	σ_z	σ_z
M_4	σ_z	σ_x	I	σ_x	σ_z
$\overline{X}$	σ_x	σ_x	σ_x	σ_x	σ_x
$\overline{Z}$	σ_z	σ_z	σ_z	σ_z	σ_z

n = 5, k = 1, t = 1

possible 1-qubit errors: $1 + 5 \times 3 = 16$

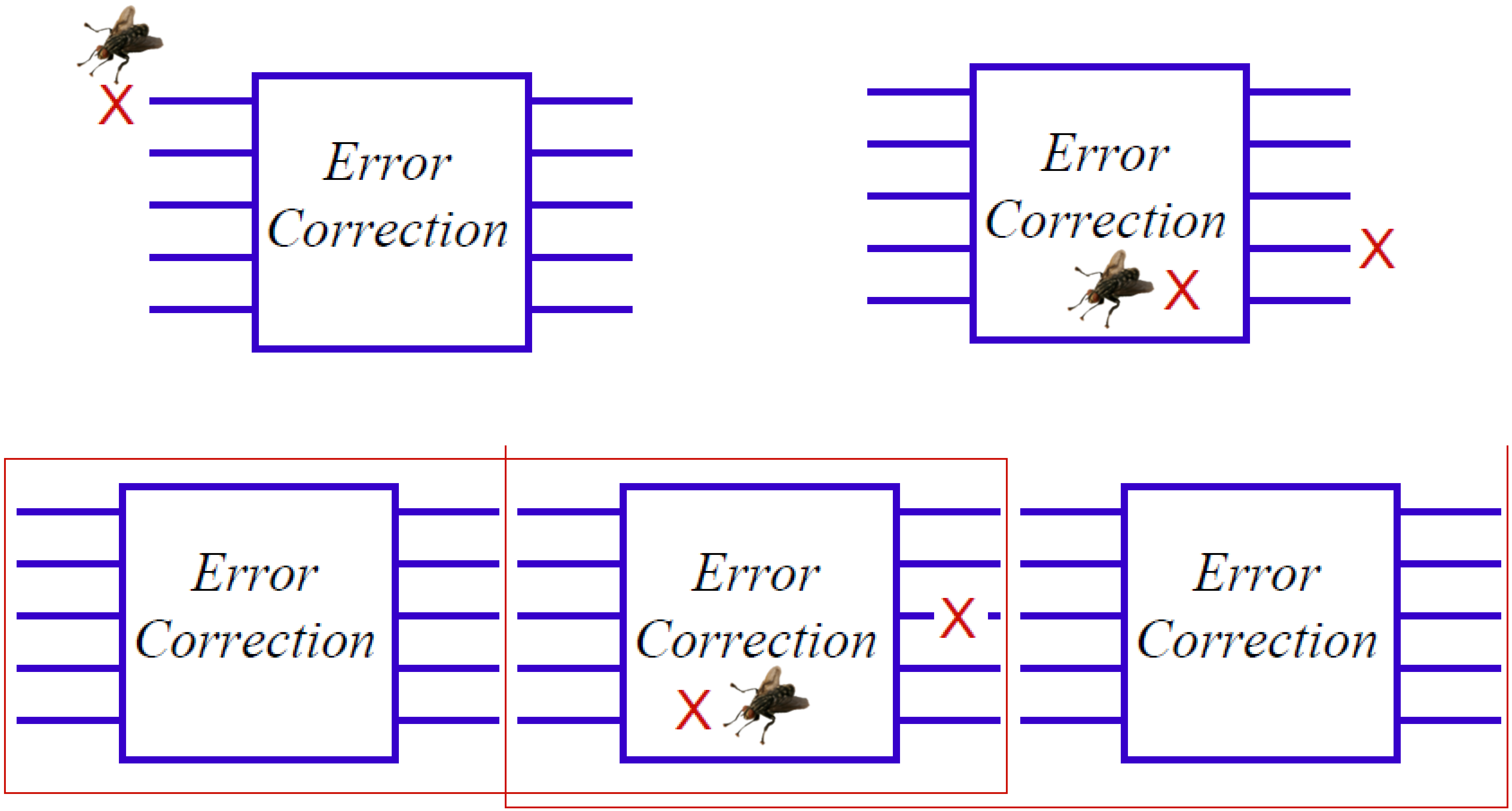
- codewords

$$\begin{aligned}|\overline{0}\rangle = \; & |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ & + |01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ & - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ & - |10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle\end{aligned}$$

$$\begin{aligned}|\overline{1}\rangle = \; & |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle \\ & + |10101\rangle - |00100\rangle - |11001\rangle - |00111\rangle \\ & - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle \\ & - |01110\rangle - |10011\rangle - |01000\rangle + |11010\rangle\end{aligned}$$

4 stabilizers detect 16 possibilities

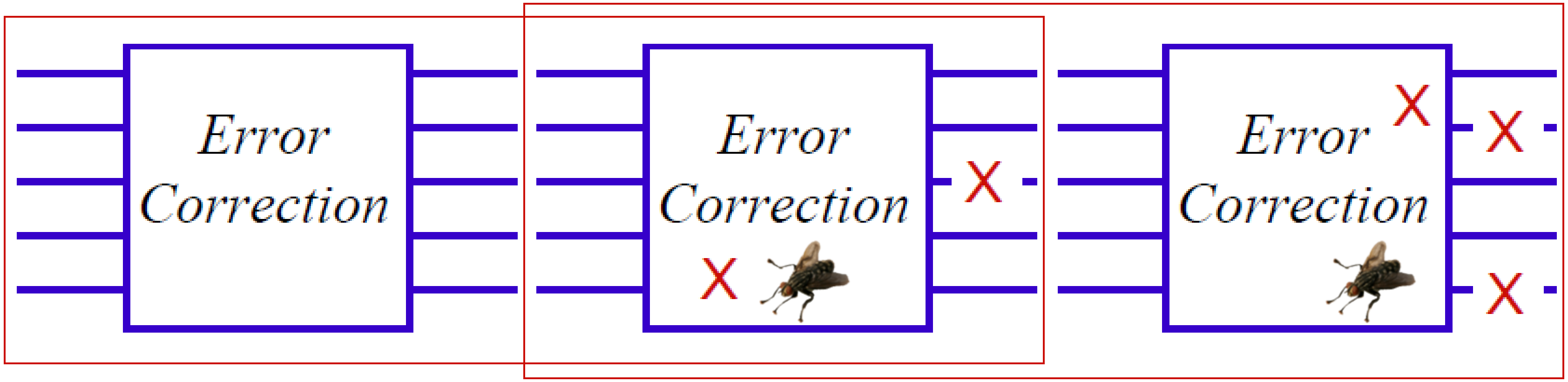
4 Fault tolerance ... ensuring errors don't propagate



[J. Preskill]

4 Fault tolerance … ensuring errors don't propagate

- 2 errors within a rectangle = trouble



[J. Preskill]

independent errors

error probability ε

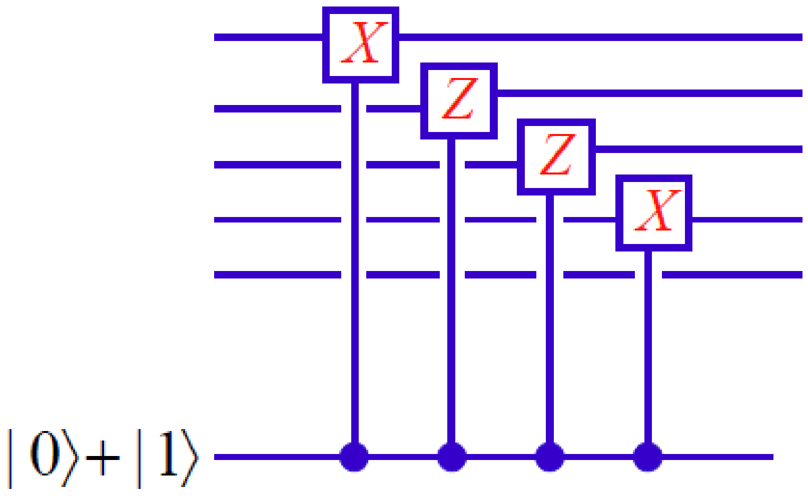
tolerate T errors

A rectangle overlaps

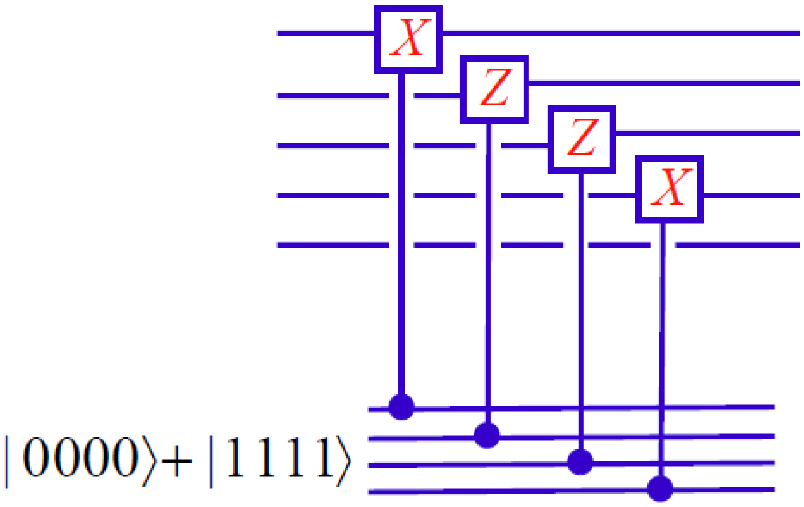
$$P_{\text{fail}} \leq TA\varepsilon^2$$

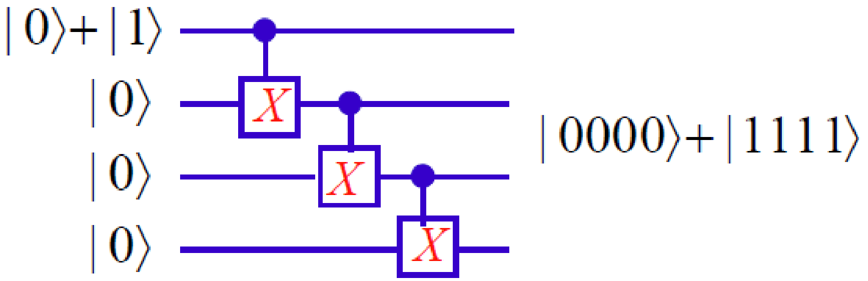
4 Fault tolerant measurement

This is *bad:*



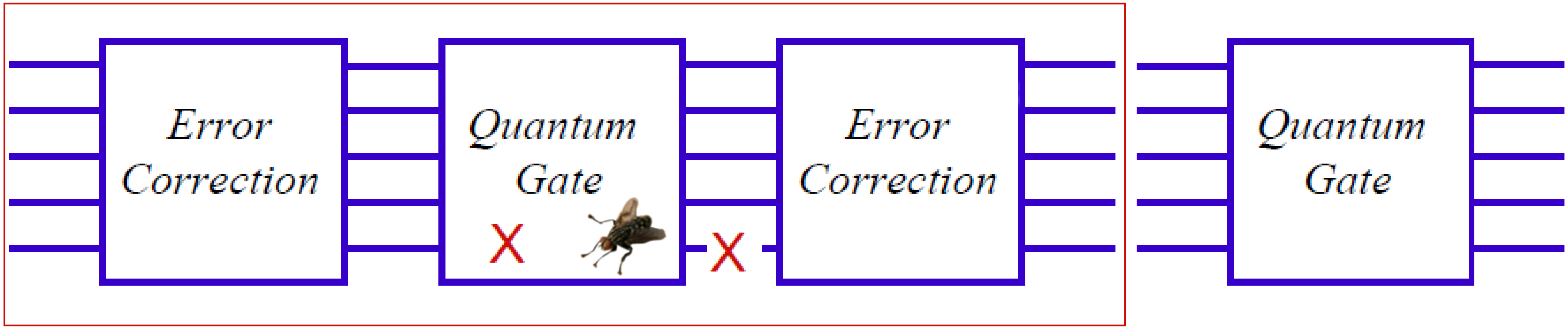
This is *better:*



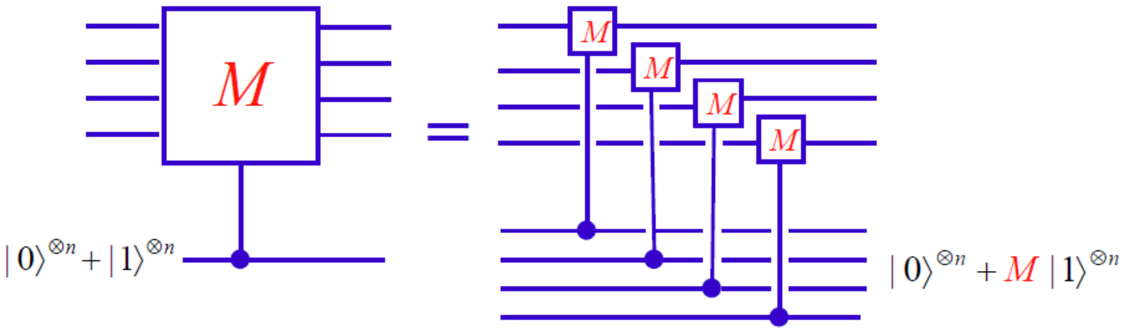


[J. Preskill]

4 Fault tolerant gates



- transversal gates



[J. Preskill]

4 Fault tolerance

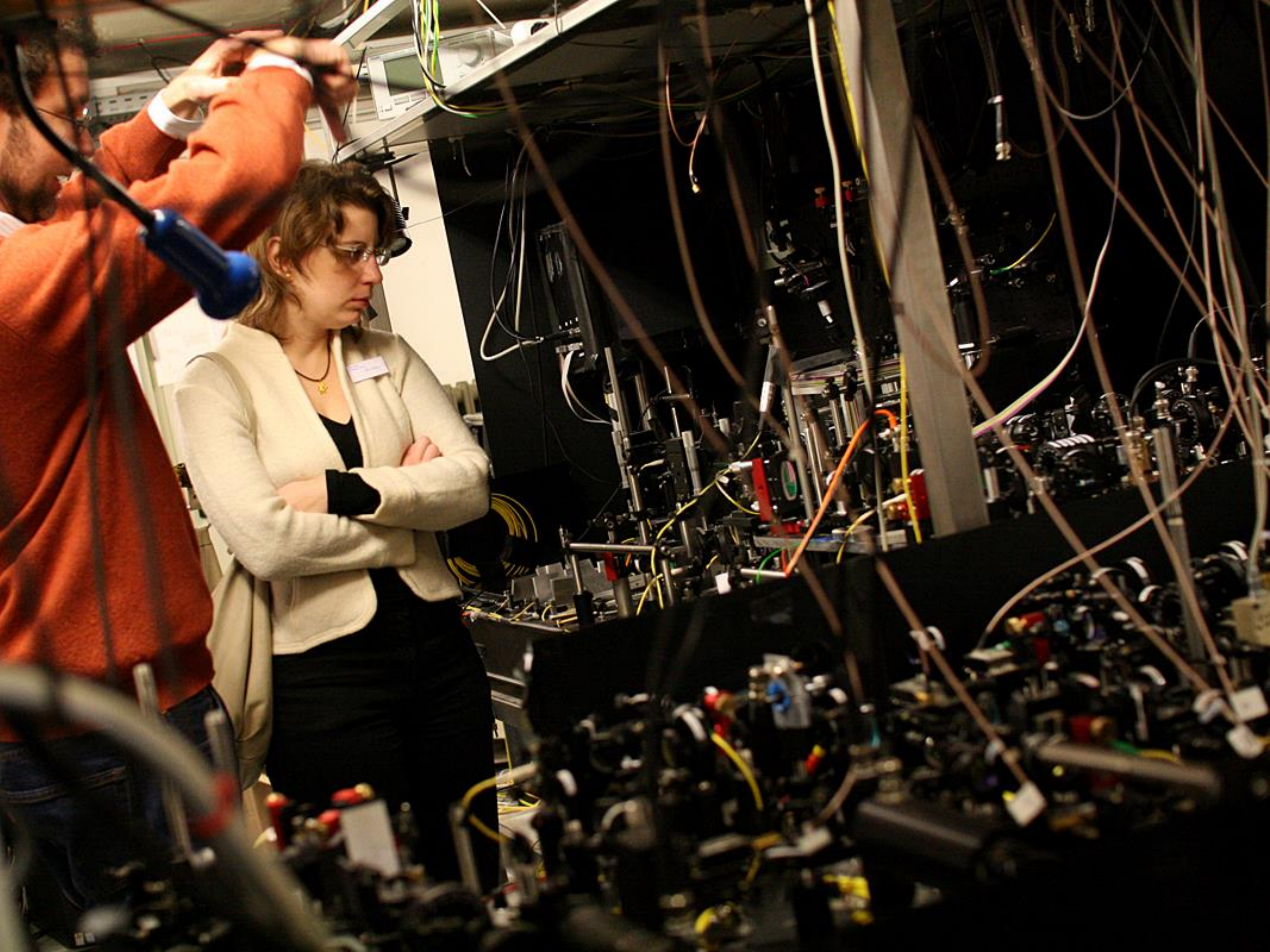
Quantum Accuracy Threshold Theorem: Suppose that faults occur independently at the locations within a quantum circuit, where the probability of a fault at each location is no larger than ε. Then there exists $\varepsilon_0 > 0$ such that for a fixed $\varepsilon < \varepsilon_0$ and fixed $\delta > 0$, any circuit of size L can be simulated by a circuit of size L^* with accuracy greater than 1-δ, where, for some constant c,

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

- the Steane [7, 1, 3] code $\varepsilon_0 > 2.73 \times 10^{-5}$

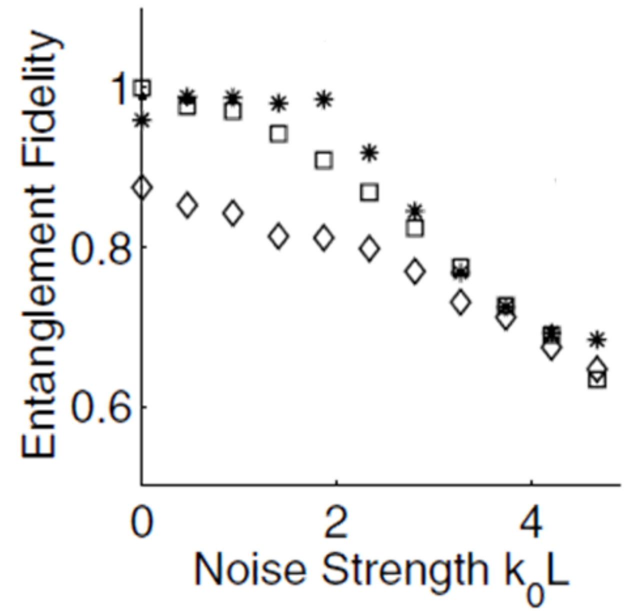
  adversarial, independent, stochastic noise

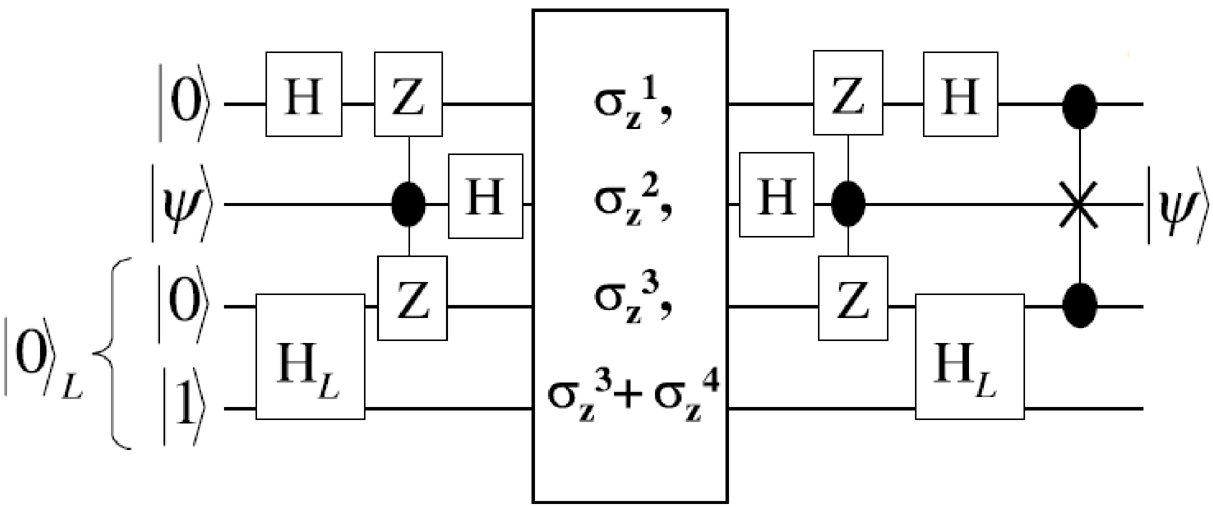
- require: fast measurement & processing, fresh ancillas, non-local gates, parallelism



4 The road towards fault tolerance: NMR

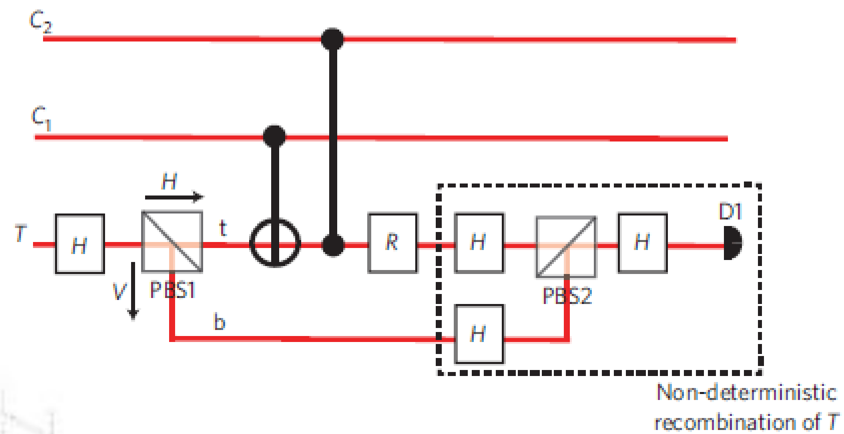
- correcting phase errors in a labeled ^{13}C system
  [Boulant et al. PRL 94, 130501 (2005)]

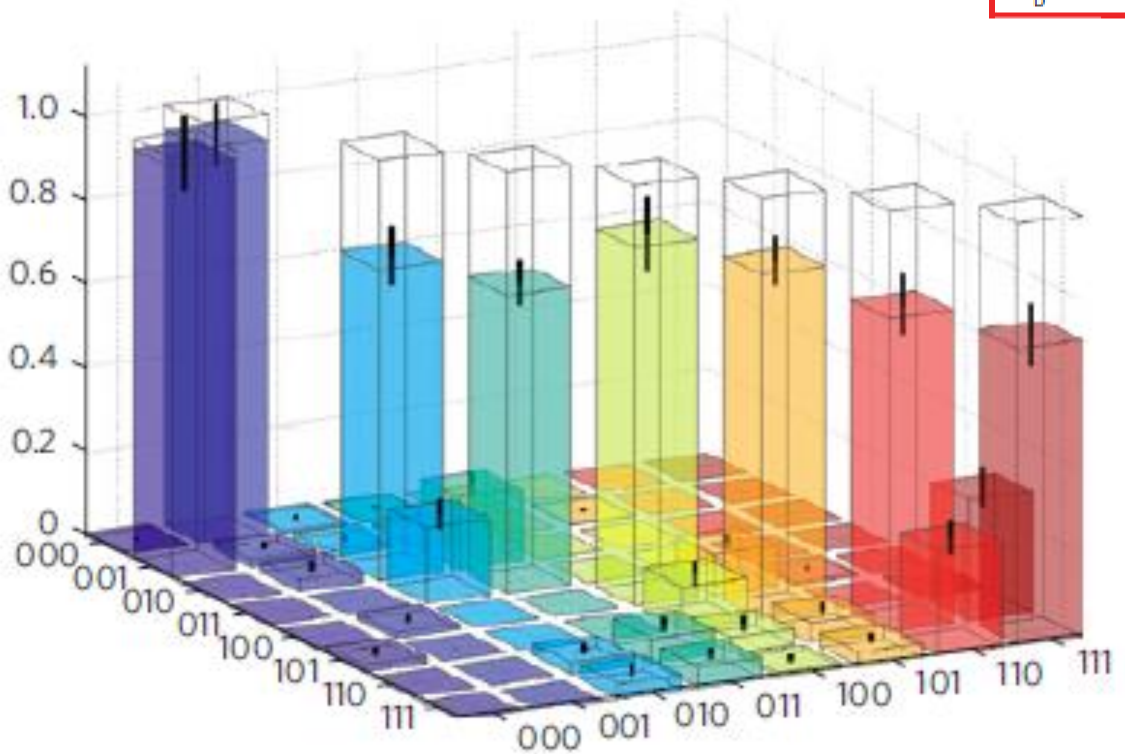




4 The road towards fault tolerance: linear optics

- Toffoli gate with qudits
  [Lanyon et al., Nature Photonics 5, 134-140 (2009)]

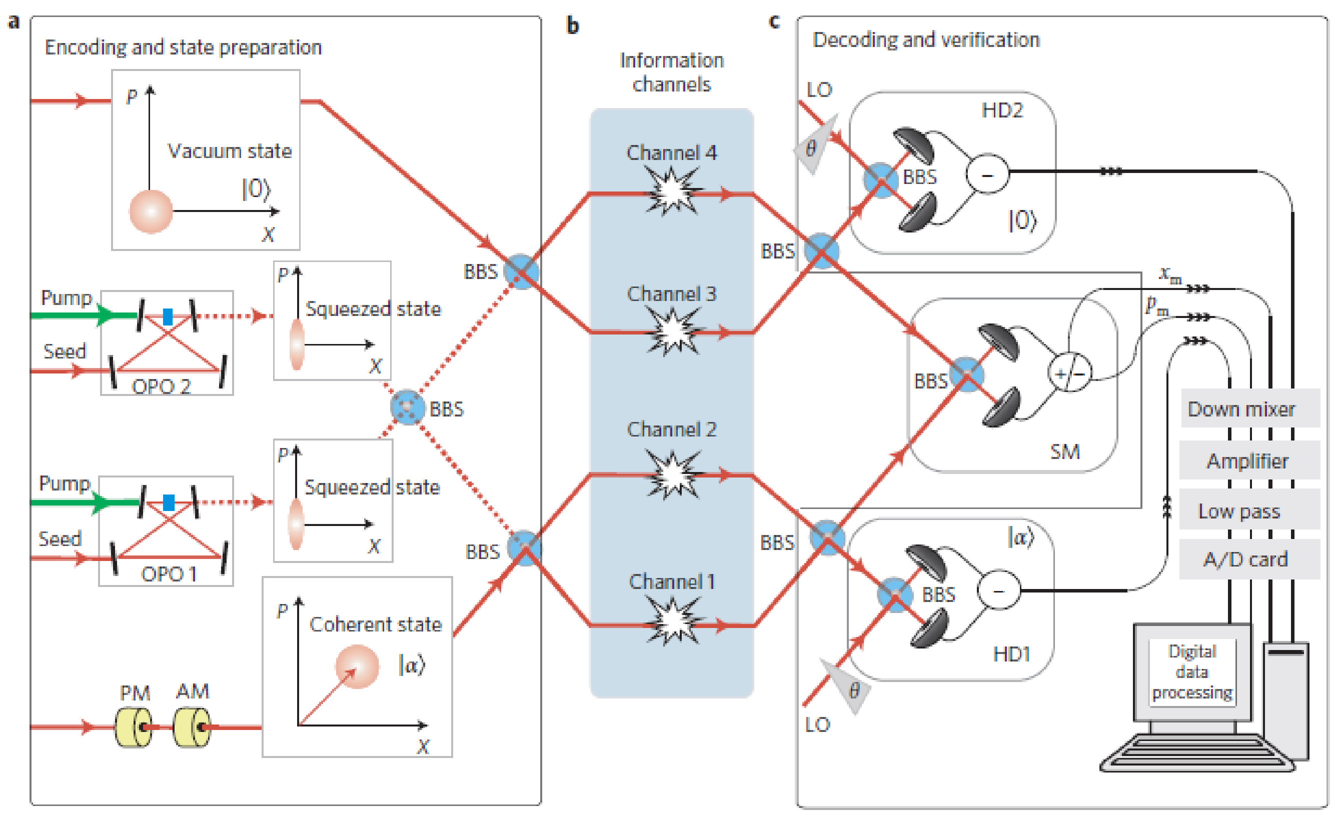




4 The road towards fault tolerance: linear optics

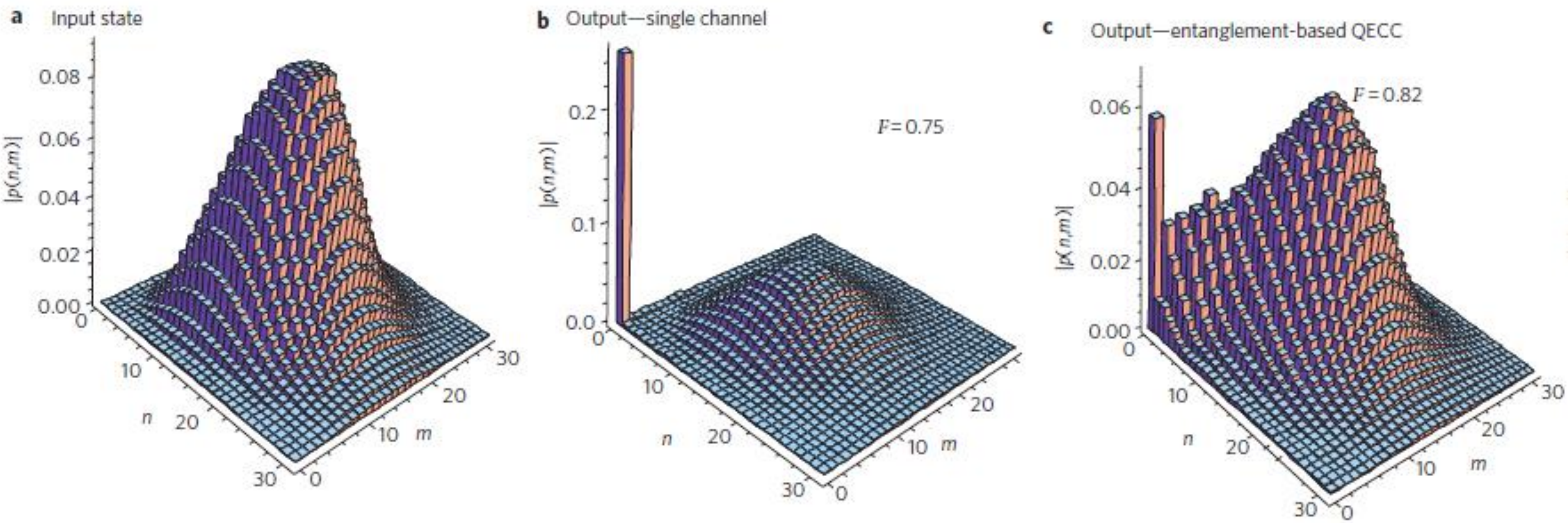
- error correction for communication
  [Braunstein, Nature 394, 47-49 (1998)]

- photon losses, 4 mode squeezed states
  [Lassen et al., Nature Photonics 4, 700-705 (2010)]

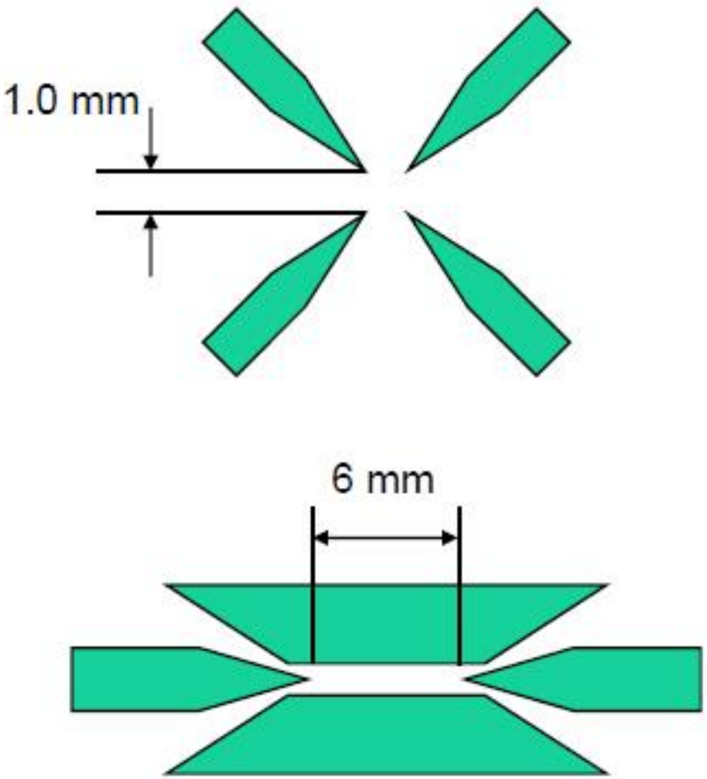


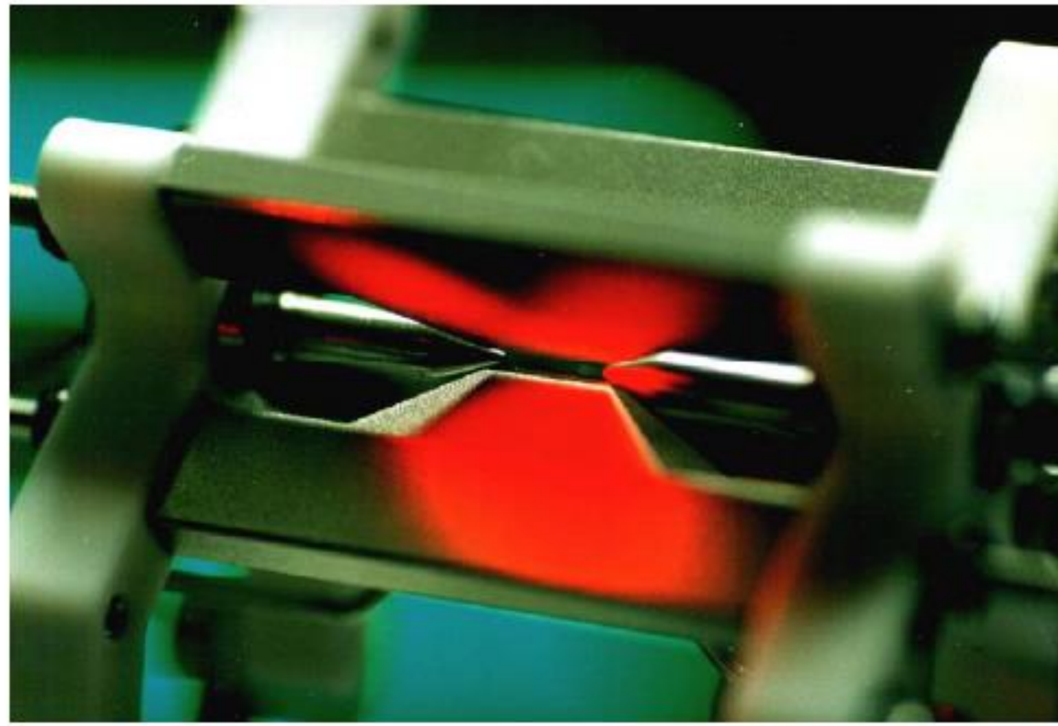
4 The road towards fault tolerance: linear optics

- error correction for communication
  [Braunstein, Nature 394, 47-49 (1998)]
- photon losses, 4 mode squeezed states
  [Lassen et al., Nature Photonics 4, 700-705 (2010)]



Innsbruck linear ion trap (2000)





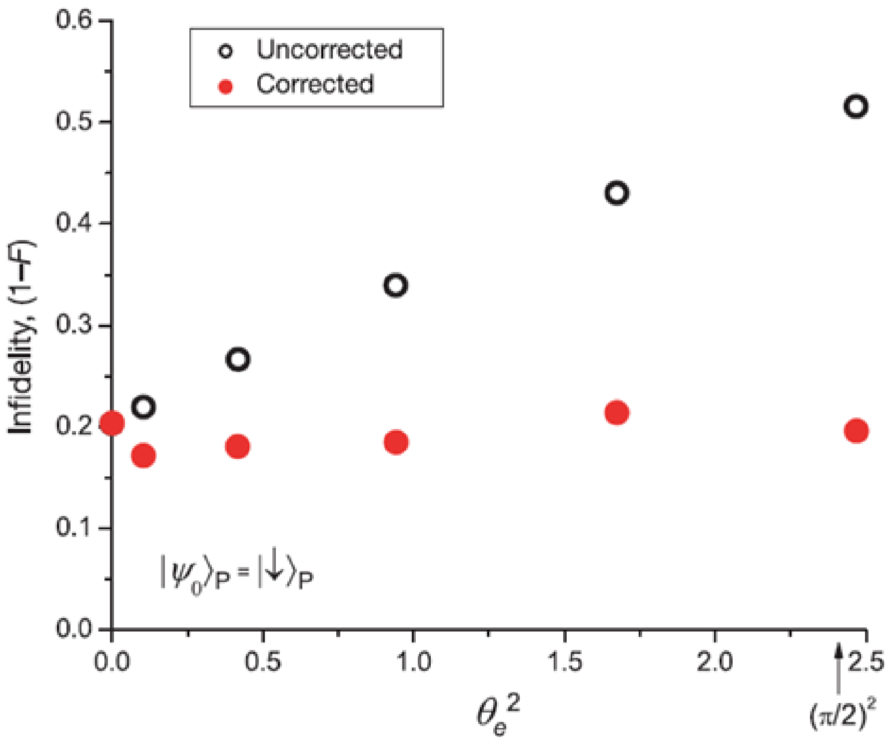
$$\omega_z \approx 0.7 - 2\,\mathrm{MHz} \qquad \omega_{x,y} \approx 1.5 - 4\,\mathrm{MHz}$$

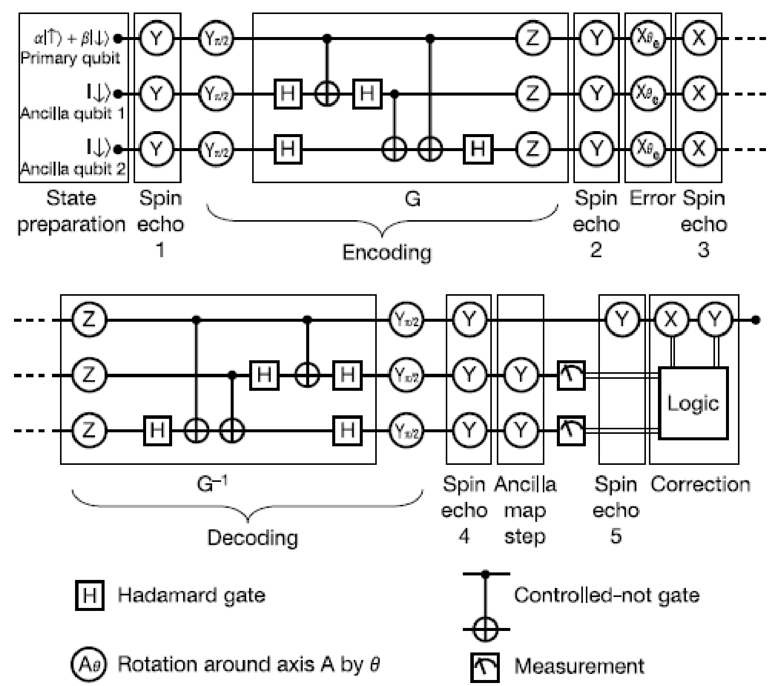
[Reiner Blatt, Innsbruck]

4 The road to fault tolerance: ion traps

- spin flip errors
  3 beryllium ions

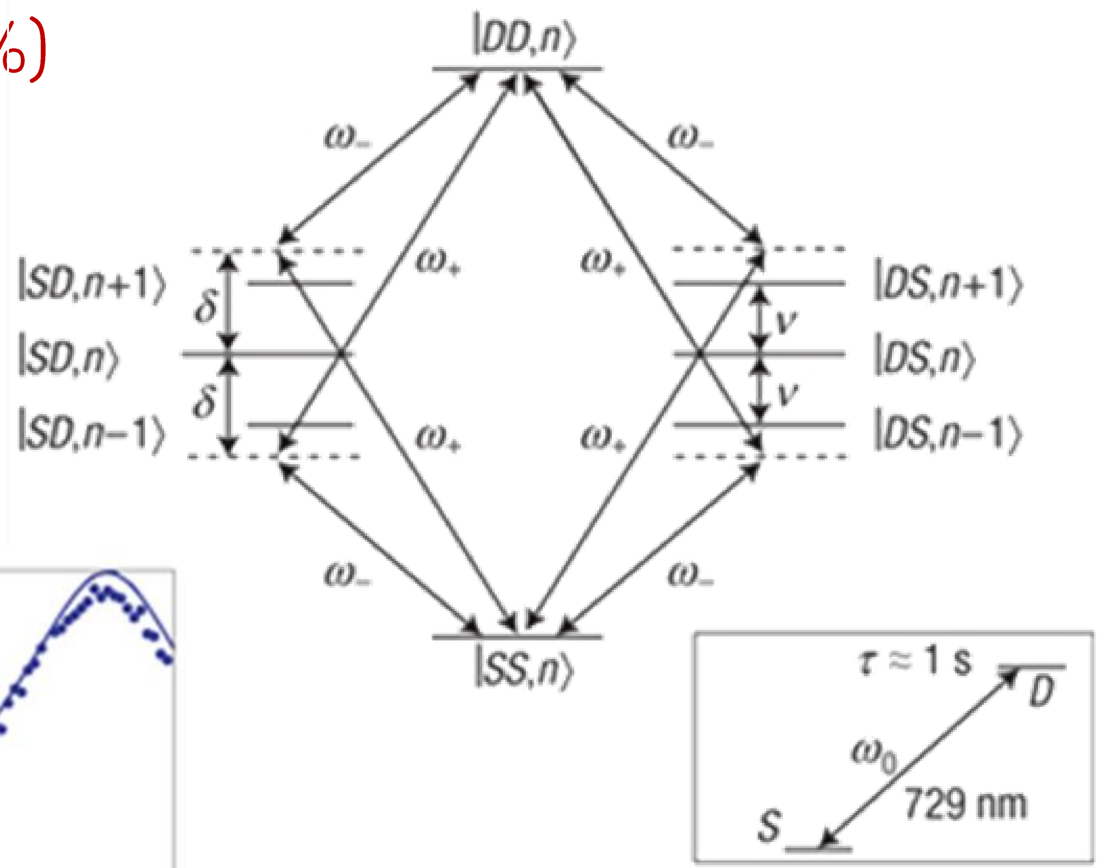
[Chiaverini et al., Nature 432, 602-605 (2004)]

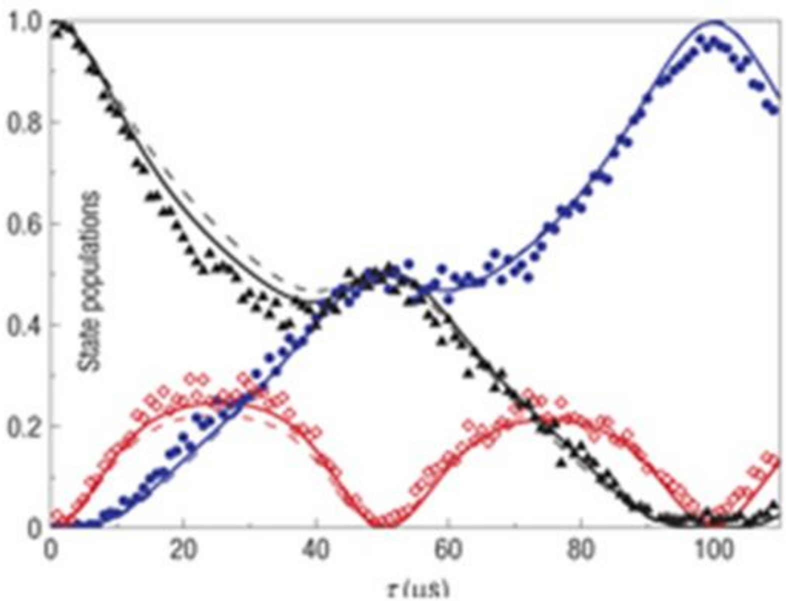




4 The road to fault tolerance: ion traps

- a high-fidelity (99%) 2-qubit gate

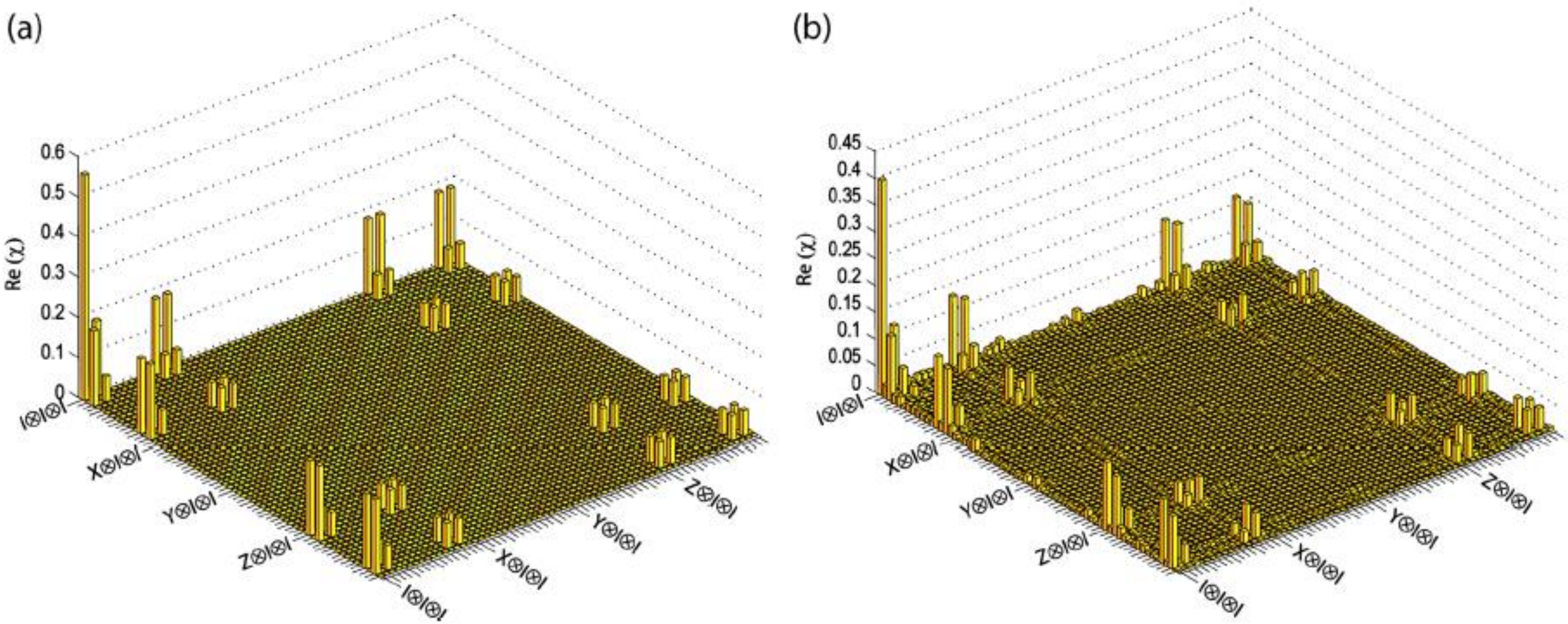




[Benhelm et al., Nature Physics 4, 463-466 (2008)]

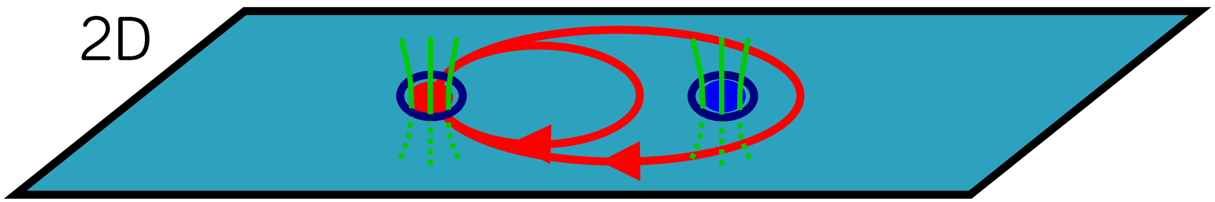
4 The road to fault tolerance: ion traps

- a high-fidelity (99%) 2-qubit gate — *[Benhelm et al., Nature Physics 4, 463 (2008)]*
- a 700μs Toffoli gate (71%) — *[Monz et al., PRL 102, 040501 (2009)]*



4 The road to fault tolerance: topological

- anyonic qubits



$$|\Psi\rangle \rightarrow e^{i2\varphi}|\Psi\rangle$$
$$|\Psi\rangle \rightarrow U|\Psi\rangle$$

[Jiannis Pachos]

- operations: braiding
- Kitaev's toric code: 2D lattice, torus, ground-state of a (4-local) Hamiltonian (XXXX , ZZZZ)
- error correction: local errors detected by stabilizers
- a topological barrier against "bad" errors
- implementation: fractional quantum Hall systems?

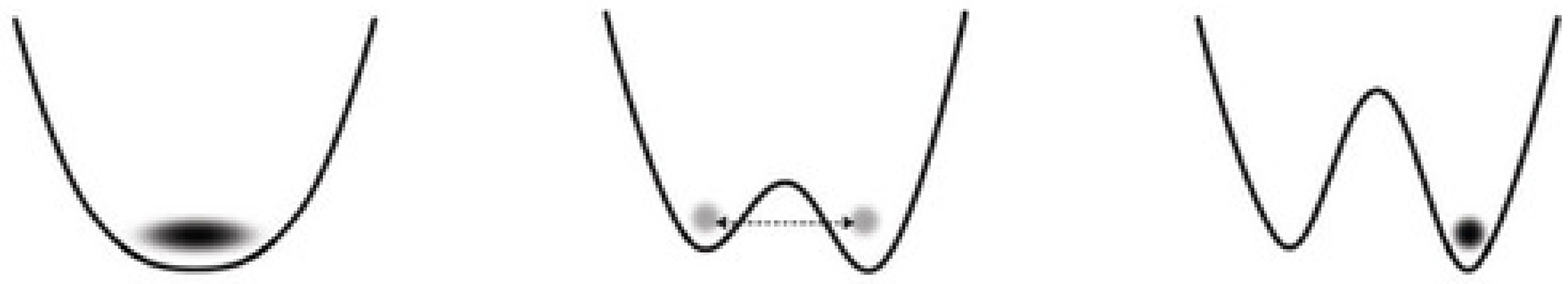
4 Adiabatic quantum optimization

- find a ground state: minimize a cost function

$$H_P\,|z\rangle = h(z)\,|z\rangle$$

- adiabatic quantum optimization *[Farhi et al.]* with a time-dependent slowly changing Hamiltonian

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \frac{t}{T} H_P$$



4 Adiabatic quantum optimization

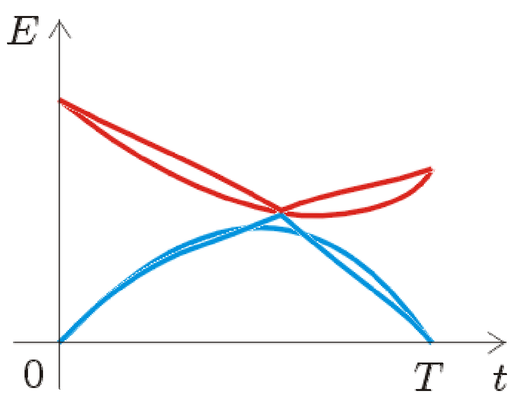
- find a ground state = minimize a cost function

$$H_P \left|z\right\rangle = h(z) \left|z\right\rangle$$

- adiabatic quantum optimization *[Farhi et al.]*
  with a time-dependent
  slowly changing Hamiltonian

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \frac{t}{T} H_P$$

- the adiabatic theorem:
  start in a ground state
  … end up in a ground state
- how slow is "slow enough"?
- gap scaling down with system size
- error correction for AQC?



4 Adiabatic quantum computation

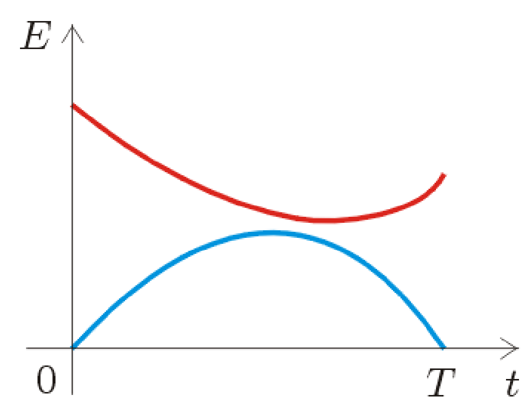
- universal for quantum computing … with a quantum final Hamiltonian

$$H_P$$

- adiabatic quantum optimization *[Farhi et al.]* with a time-dependent slowly changing Hamiltonian

$$H(t) = \left(1 - \frac{t}{T}\right) H_B + \frac{t}{T} H_P$$

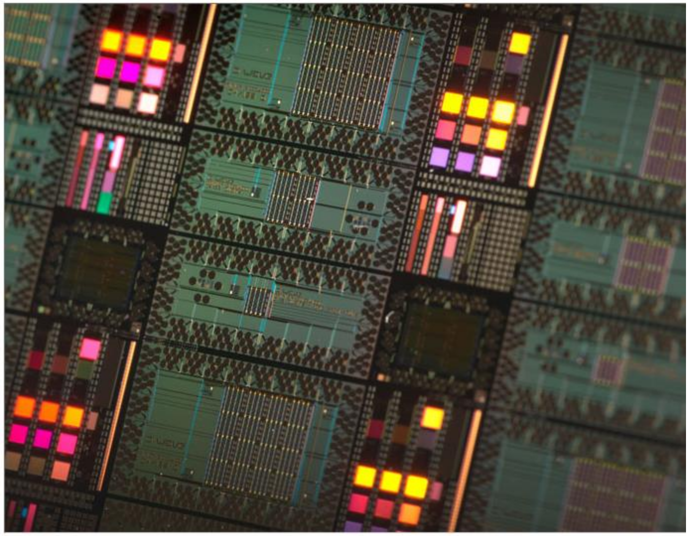
- the adiabatic theorem: start in a ground state … end up in a ground state
- how slow is "slow enough"?
- gap scaling down with system size
- error correction for AQC?



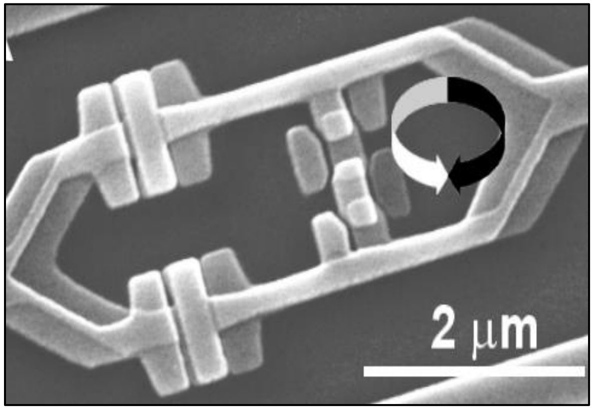
D-Wave sells first commercial quantum computer to Lockheed Martin

By Sean Hollister posted May 29th 2011 2:02AM

Who found ten million dollars to drop on the first commercially available quantum computer? Lockheed Martin, it seems, as the aerospace defense contractor has just begun a "multi-year contract" with the quantum annealing experts at D-Wave to develop... nothing that they're ready or willing to publicly discuss at this time.



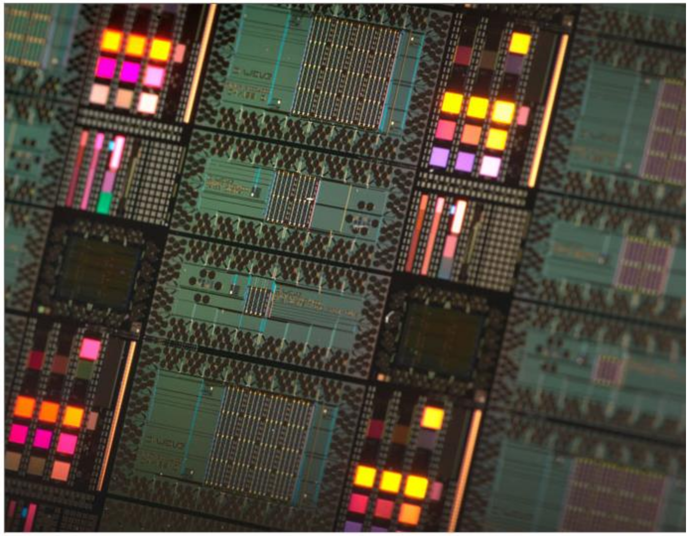
D-Wave's processors on wafer (Courtesy: D-Wave).



[FSU]

superconducting qubits

D-Wave's Geordie Rose in front of the firm's D-Wave One system (Courtesy: D-Wave).



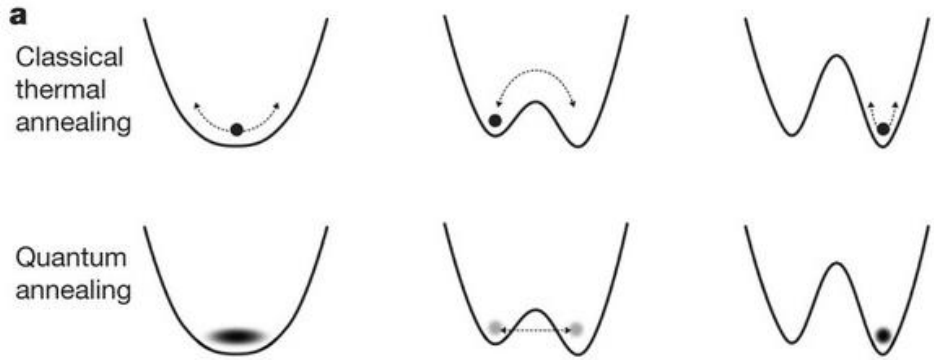
D-Wave's processors on wafer (Courtesy: D-Wave).

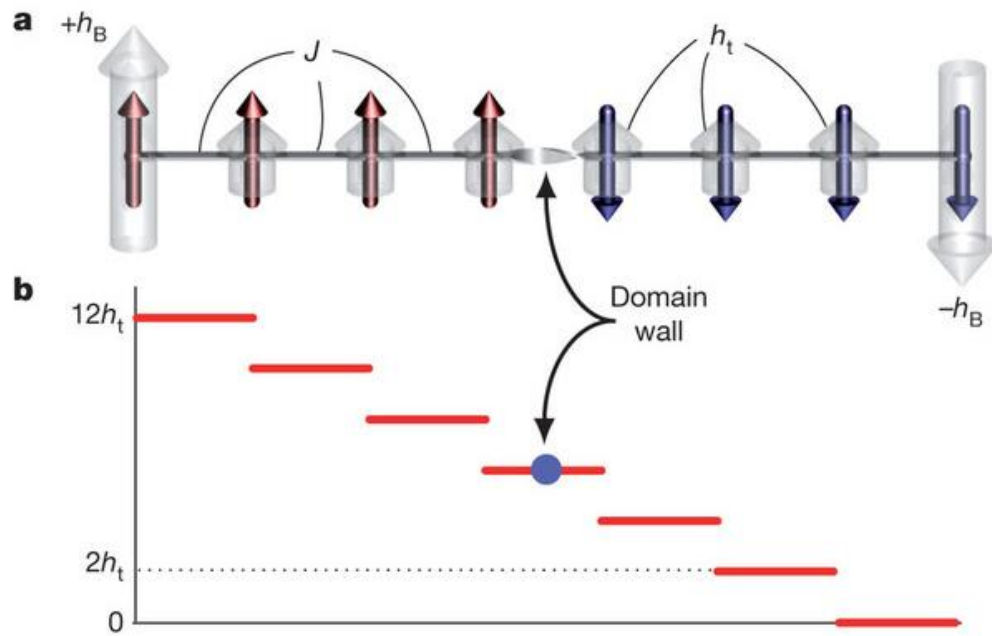
M.W.Johnston et al.

Quantum annealing with manufactured spins

Nature 473, 194–198 (2011)

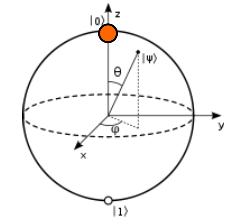
a frustrated 8-spin chain, quantum annealing confirmed





1 we need a qubit

but what can one do with it?

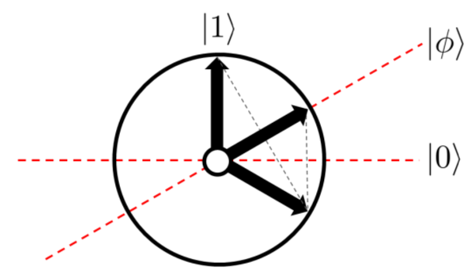


2 EPR pairs

give us cool 2-qubit protocols

3 the algorithms

that make quantum computing tick



4 error correction

can we really scale up this stuff?

5

Quantum Computation conclusions & discussion

- What's the point?
- Where are the problems?
- How are we doing?