Al Aho

aho@cs.columbia.edu

Quantum Computer Compilers

COMPUTER SCIENCE AT
COLUMBIA UNIVERSITY

Invited Talk, PLDI

Tucson, AZ, June 9, 2008

A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. What might a quantum computer look like?
3. What is a good model of computation for quantum computers?
4. What would make a good quantum programming language?
5. What are the issues in building quantum computer compilers?
6. When are we likely to see scalable quantum computers?

What the Physicists are Saying

"Quantum information is a radical departure in information technology, more fundamentally different from current technology than the digital computer is from the abacus."

William D. Phillips, 1997 Nobel Prize Winner in Physics

Shor's Integer Factorization Algorithm

Problem: Given a composite *n*-bit integer, find a nontrivial factor.

Best-known deterministic algorithm on a classical computer has time complexity $\exp(O(n^{1/3} \log^{2/3} n))$.

A quantum computer can solve this problem in $O(n^3)$ operations.

Peter Shor

Algorithms for Quantum Computation: Discrete Logarithms and Factoring
***Proc. 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124-134**

Integer Factorization: Estimated Times

Classical: number field sieve

- Time complexity: $\exp(O(n^{1/3} \log^{2/3} n))$
- Time for 512-bit number: 8400 MIPS years
- Time for 1024-bit number: 1.6 billion times longer

Quantum: Shor's algorithm

- Time complexity: $O(n^3)$
- Time for 512-bit number: 3.5 hours
- Time for 1024-bit number: 31 hours
  (assuming a 1 GHz quantum device)

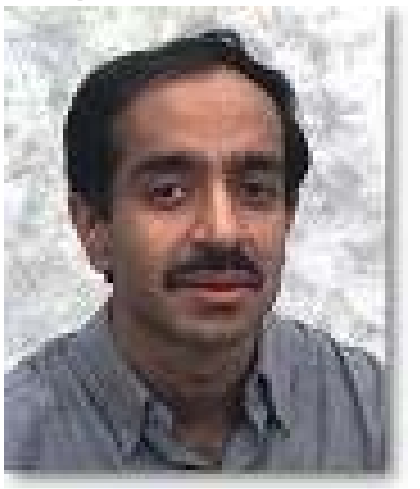
M. Oskin, F. Chong, I. Chuang
A Practical Architecture for Reliable Quantum Computers
IEEE Computer, 2002, pp. 79-87

Grover's Quantum Search Algorithm

Problem: Given a black box U_f for computing an unknown function $f : \{0,1\}^n \rightarrow \{0,1\}$, find an x in $\{0,1\}^n$ such that $f(x) = 1$.

Best-known deterministic algorithm on a classical computer requires 2^n operations.

A quantum computer can solve this problem in $\Theta(\sqrt{2^n})$ operations.



Lov Grover

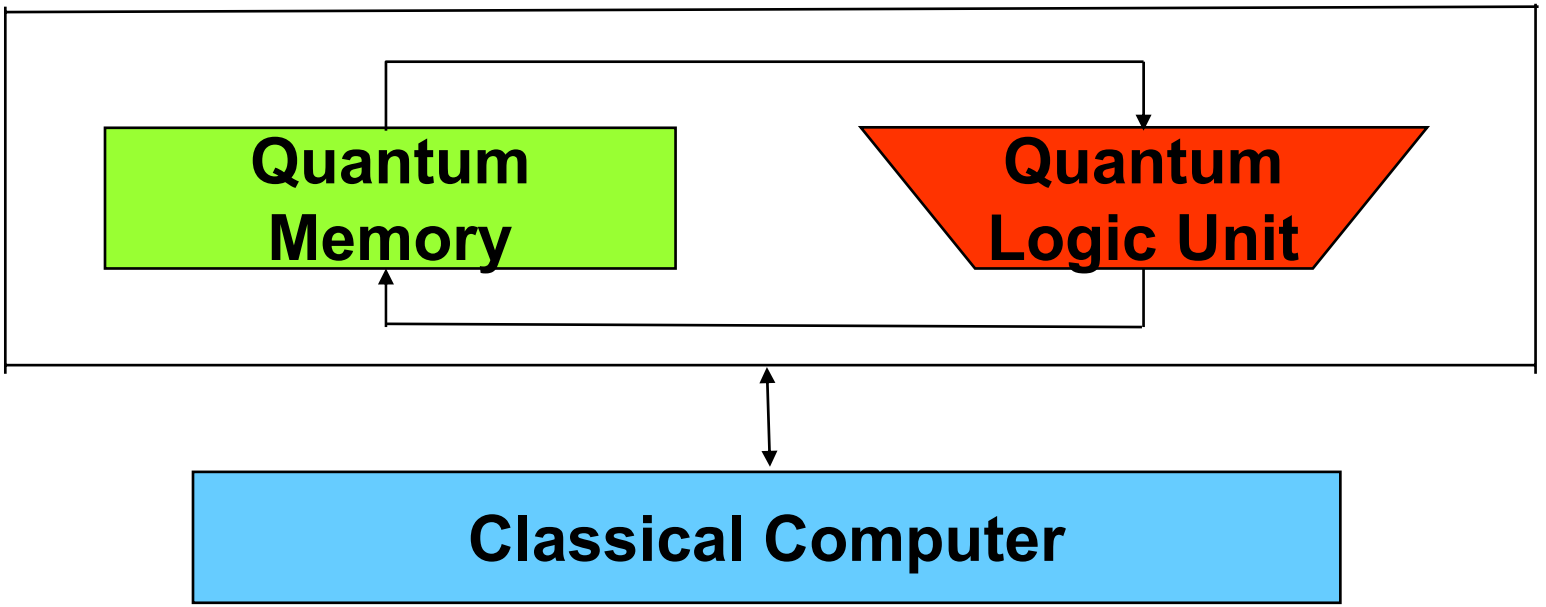
A Fast Quantum Mechanical Algorithm for Database Search

***Proc. 28th Annual ACM Symposium on the Theory of Computing*, 1996, pp. 212-219**

A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. **What might a quantum computer look like?**
3. What is a good model of computation for quantum computers?
4. What would make a good quantum programming language?
5. What are the issues in building quantum computer compilers?
6. When are we likely to see scalable quantum computers?

Quantum Computer Architecture



Knill [1996]: Quantum RAM, a classical computer combined with a quantum device with operations for initializing registers of qubits and applying quantum operations and measurements

Oskin, Chong, Chuang [2002]: fault-tolerant quantum computer architecture with quantum memory banks, quantum ALU, teleportation, and control by a classical microprocessor

DiVincenzo Criteria for a Quantum Computer

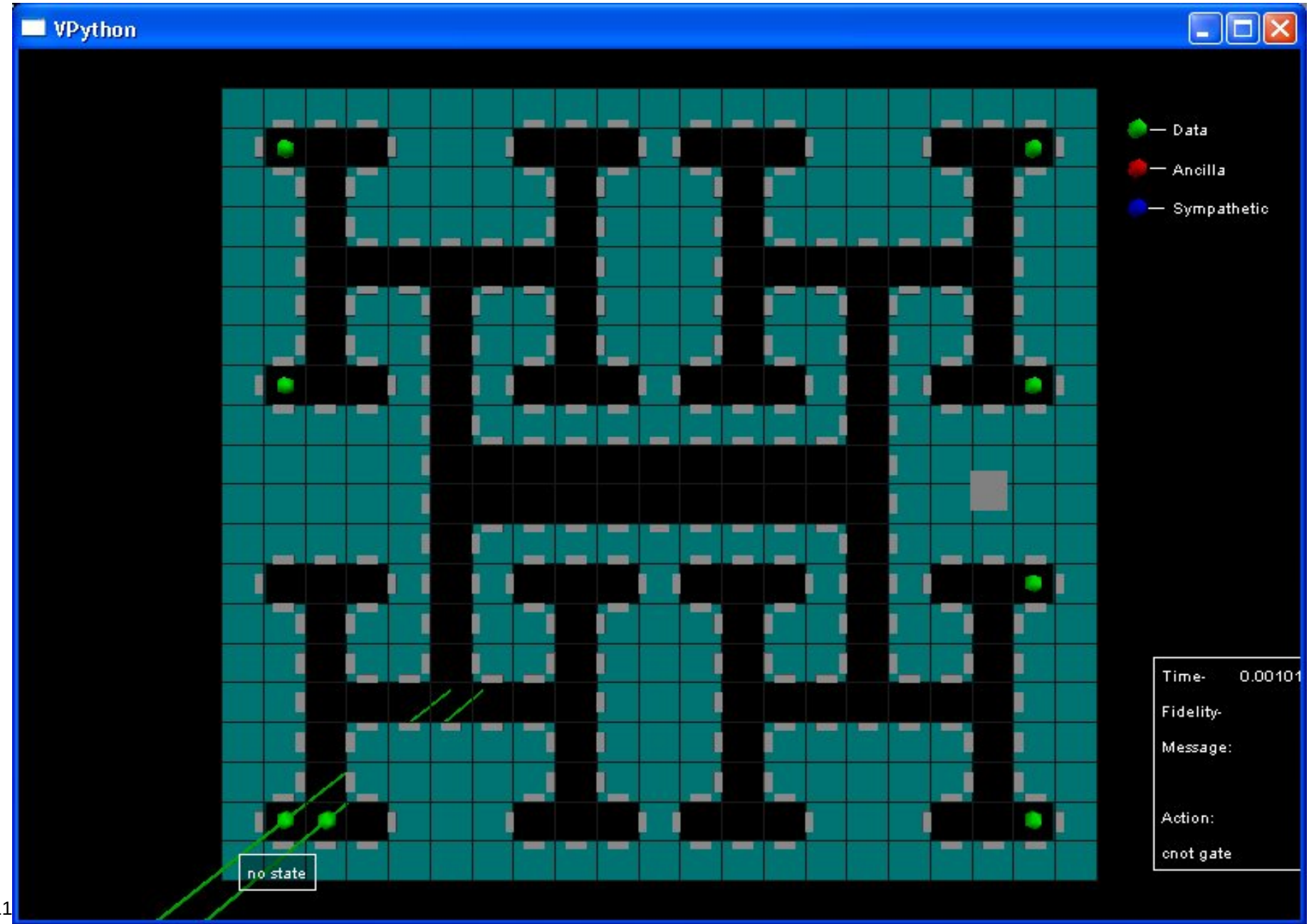
1. Be a scalable system with well-defined qubits
2. Be initializable to a simple fiducial state
3. Have long decoherence times
4. Have a universal set of quantum gates
5. Permit efficient, qubit-specific measurements

David DiVincenzo
Solid State Quantum Computing
http://www.research.ibm.com/ss_computing

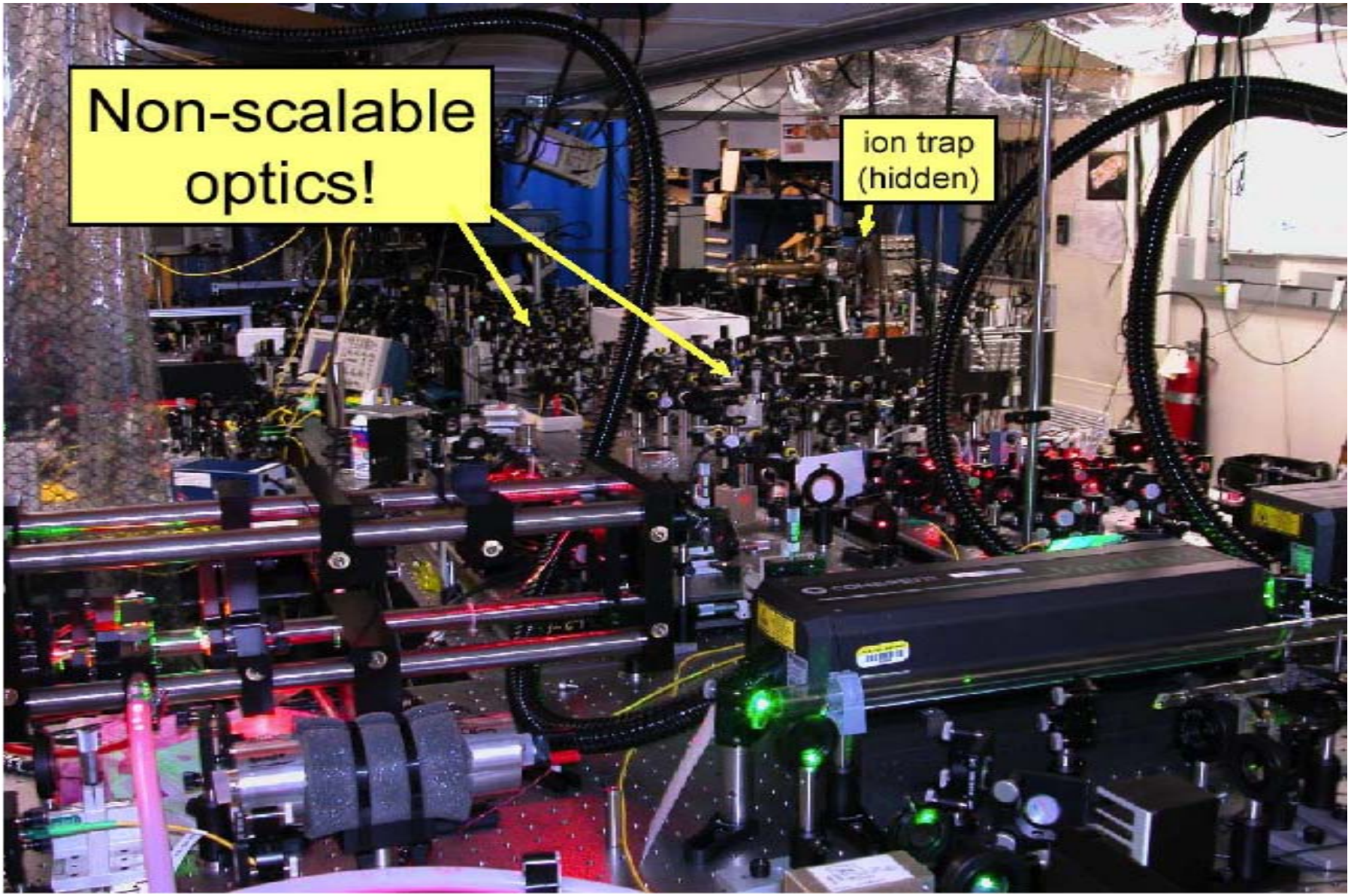
Possible Quantum Computing Device Technologies

- Ion traps
- Josephson junctions
- Nuclear magnetic resonance
- Optical photons
- Optical cavity quantum electrodynamics
- Quantum dots
- Nonabelian fractional quantum Hall effect anyons

MIT Ion Trap Simulator

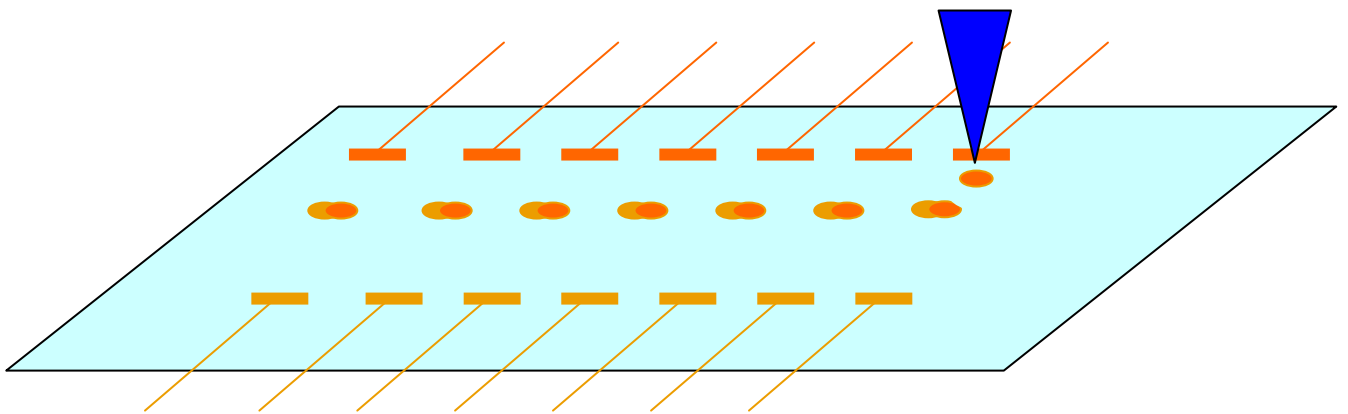


Ion Trap Quantum Computer: The Reality



Artist's Conception of Topological Quantum Device

Theorem (Simon, Bonesteel, Freedman… PRL05): In any topological quantum computer, all computations can be performed by moving only a single quasiparticle!



The Future of Quantum Hardware

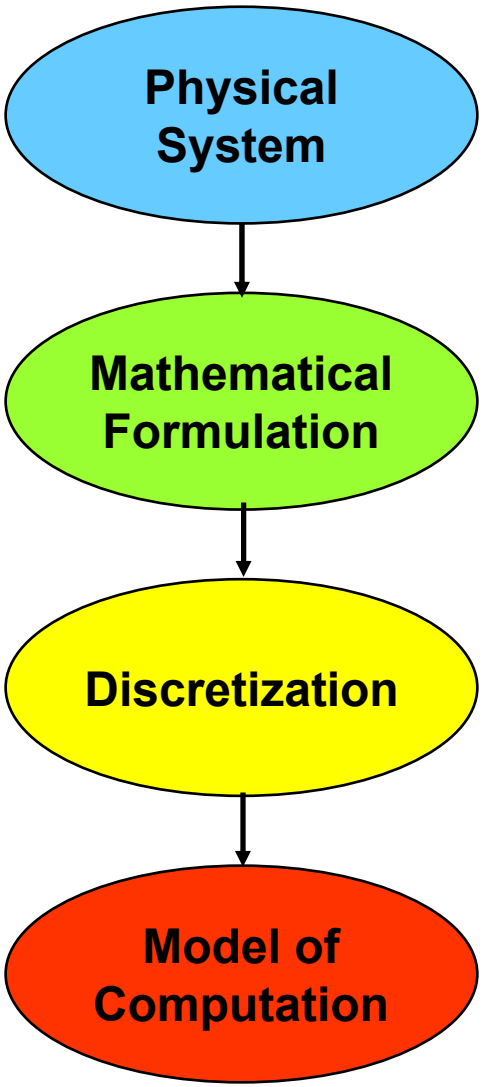
- The future does not necessarily belong to the ion trappers: for example, electron spins in quantum dots, superconducting qubits, ultracold neutral atoms are all making impressive progress.
- But ion traps have a head start, and some serious effort has been devoted to conceiving scalable architectures.
- "Ion trap chips look well placed to create useful computers before other methods."–Andrew Steane
- "There is progress, but it's still very slow."–Chris Monroe
- "I'd say almost any prediction about what a quantum computer will look like will, with high probability, be wrong. Ion trappers are encouraged because we can at least see a straightforward path to making a large processor, but the technical problems are extremely challenging. It might be fair to say that ion traps are currently in the lead; however, a good analogy might be that we're leading a marathon race, but only one meter from the start line."
  –Dave Wineland

John Preskill
Robust Quantum Computation
IPAM Conference on Topological Quantum Computing, 2007

A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. What might a quantum computer look like?
3. **What is a good model of computation for quantum computers?**
4. What would make a good quantum programming language?
5. What are the issues in building quantum computer compilers?
6. When are we likely to see scalable quantum computers?

Towards a Model of Computation for Quantum Computers



The Physical Underpinnings of Quantum Computing

The Four Postulates of Quantum Mechanics

M. A. Nielsen and I. L. Chuang
Quantum Computation and Quantum Information
Cambridge University Press, 2000

State Space Postulate

Postulate 1

The state of an isolated quantum system can be described by a unit vector in a complex Hilbert space.

Qubit: Quantum Bit

- **The state of a quantum bit in a 2-dimensional complex Hilbert space can be described by a unit vector (in Dirac notation)**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where *α* and *β* are complex coefficients called the amplitudes of the basis states $|0\rangle$ and $|1\rangle$ and

$$|\alpha|^2 + |\beta|^2 = 1$$

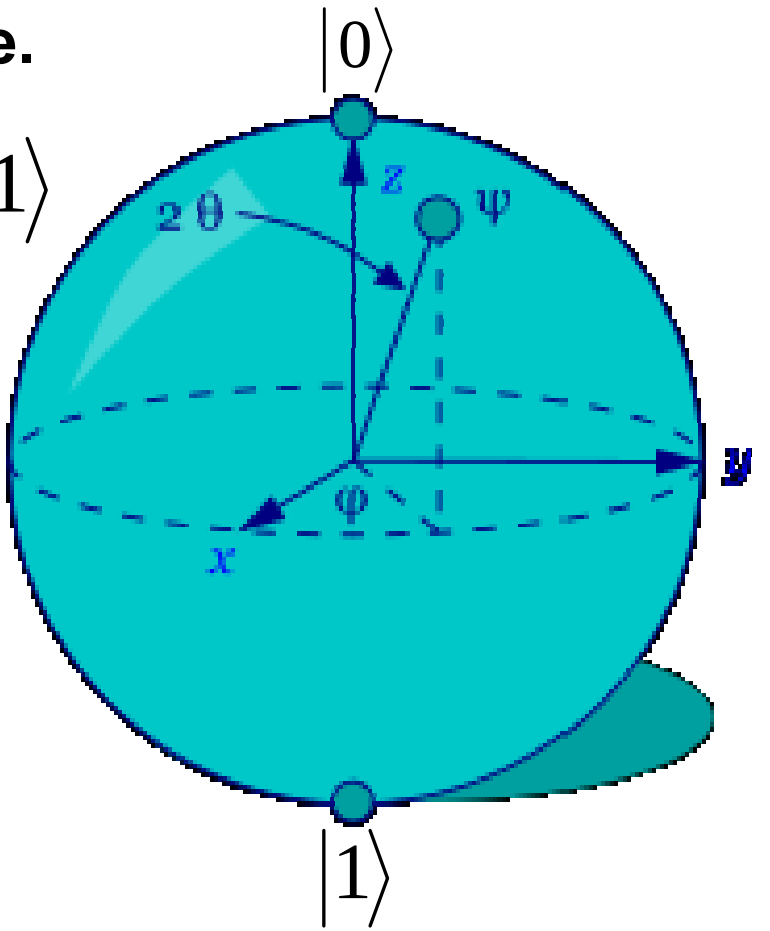
- **In conventional linear algebra**

$$\begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

State of a Qubit on the Bloch Sphere

The state vector of a qubit can be shown as a point on the surface of a 3-dimensional sphere called the Bloch sphere.

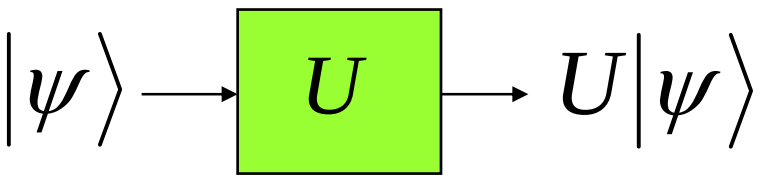
$$\left|\psi\right\rangle = \cos(\theta)\left|0\right\rangle + e^{i\varphi}\sin(\theta)\left|1\right\rangle$$



Time-Evolution Postulate

Postulate 2

The evolution of a closed quantum system can be described by a unitary operator U. (An operator U is unitary if $U^\dagger = U^{-1}$.)



state of the system at time t_1

state of the system at time t_2

Time-Evolution Postulate

Postulate 2′

The time evolution of the state of a closed quantum system can be described by Schrödinger's equation

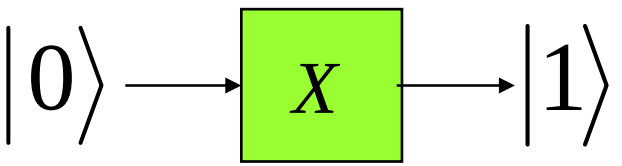
$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$$

H is a fixed Hermitian operator known as the Hamiltonian of the system.

Useful Quantum Operators: Pauli Operators

Pauli operators

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



In conventional linear algebra $X|0\rangle = |1\rangle$
is equivalent to

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

Useful Quantum Operators: Hadamard Operator

The Hadamard operator has the matrix representation

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

***H* maps the computational basis states as follows**

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Note that $HH = I$.

Composition-of-Systems Postulate

Postulate 3

The state space of a combined physical system is the tensor product space of the state spaces of the component subsystems.

If one system is in the state $|\psi_1\rangle$ and another is in the state $|\psi_2\rangle$, then the combined system is in the state $|\psi_1\rangle \otimes |\psi_2\rangle$.

$|\psi_1\rangle \otimes |\psi_2\rangle$ is often written as $|\psi_1\rangle|\psi_2\rangle$ or as $|\psi_1\psi_2\rangle$.

Tensor Product

Example

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$$

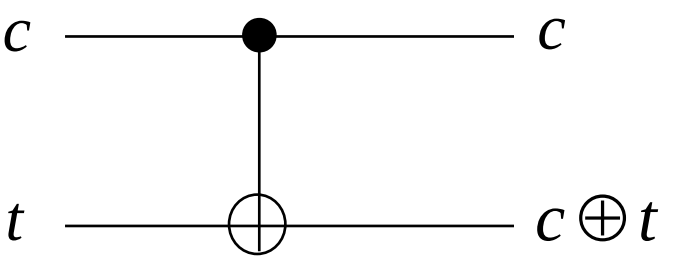
$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$

Useful Quantum Operators: the CNOT Operator

The two-qubit CNOT (controlled-NOT) operator:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

CNOT flips the target bit t iff the control bit c has the value 1:

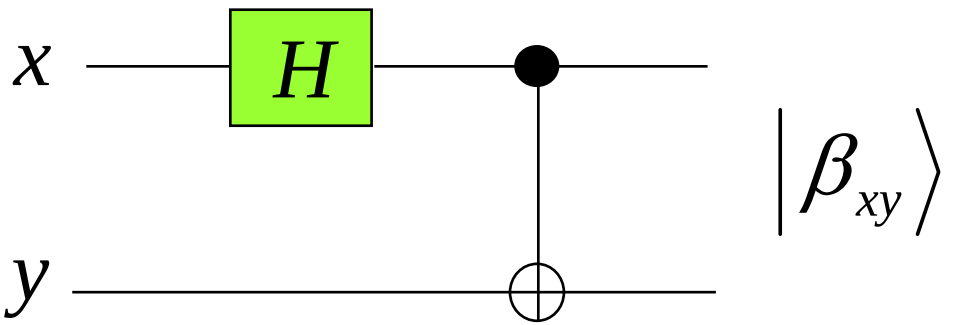


The CNOT gate maps

$$|00\rangle \mapsto |00\rangle, \quad |01\rangle \mapsto |01\rangle, \quad |10\rangle \mapsto |11\rangle, \quad |11\rangle \mapsto |10\rangle$$

Quantum Circuits

Quantum circuit to create Bell (Einstein-Podulsky-Rosen) states:



Circuit maps

$$|00\rangle \mapsto \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}, |01\rangle \mapsto \frac{(|01\rangle + |10\rangle)}{\sqrt{2}}, |10\rangle \mapsto \frac{(|00\rangle - |11\rangle)}{\sqrt{2}}, |11\rangle \mapsto \frac{(|01\rangle - |10\rangle)}{\sqrt{2}}$$

Each output is an entangled state, one that cannot be written in a product form. (Einstein: "Spooky action at a distance.")

Universal Sets of Quantum One-Qubit Gates

A set of gates is *universal* for one-qubit gates if any one-qubit gate can be approximated to arbitrary accuracy by a quantum circuit using gates from that set.

The $\pi/8$ gate T = $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Universal sets for one-qubit gates:

- **{ *H*, *T* }**
- **{ CNOT, *H*, *T* }**

Universal Sets of Quantum Gates

A set of gates is *universal for quantum computation* if any unitary operation can be approximated to arbitrary accuracy by a quantum circuit using gates from that set.

The phase-gate *S* = $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

Common universal sets of quantum gates:

- **{ *H*, *S*, CNOT, *T* }**
- **{ *H*, *I*, *X*, *Y*, *Z*, *S*, *T*, CNOT }**

CNOT and the single qubit gates are exactly universal for quantum computation.

Measurement Postulate

Postulate 4

Quantum measurements can be described by a collection $\{M_m\}$ of operators acting on the state space of the system being measured. If the state of the system is $|\psi\rangle$ before the measurement, then the probability that the result m occurs is

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

and the state of the system after measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

Measurement

The measurement operators satisfy the completeness equation:

$$\sum_m M_m^\dagger M_m = I$$

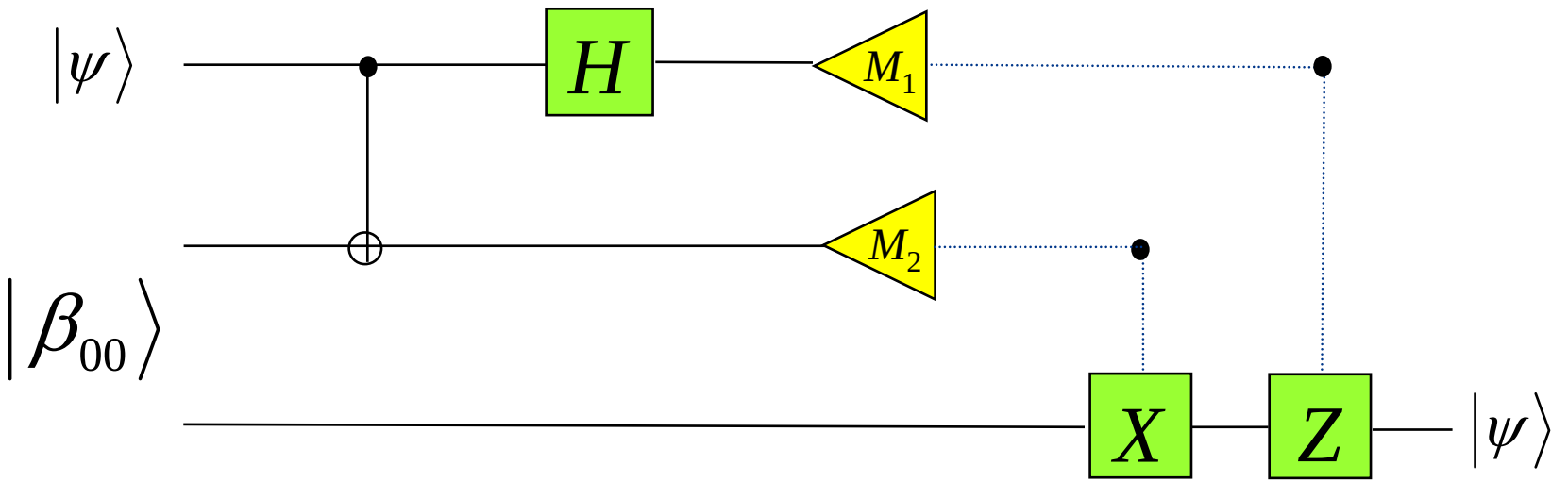
The completeness equation says the probabilities sum to one:

$$\sum_m p(m) = \sum_m \langle \psi | M_m^\dagger M | \psi \rangle = 1$$

Alice and Bob's Qubit-State Delivery Problem

- Alice knows that she will need to send to Bob the state of an important secret qubit sometime in the future.
- Her friend Bob is moving far away and will have a very low bandwidth Internet connection.
- Therefore Alice will need to send her qubit state to Bob cheaply.
- How can Alice and Bob solve their problem?

Alice and Bob's Solution: Quantum Teleportation!



- Alice and Bob generate an EPR pair.
- Alice takes one half of the pair; Bob the other half. Bob moves far away.
- Alice interacts her secret qubit $|\psi\rangle$ with her EPR-half and measures the two qubits.
- Alice sends the two resulting classical measurement bits to Bob.
- Bob decodes his half of the EPR pair using the two bits to discover $|\psi\rangle$.

Model of Computation for Quantum Computers

Quantum circuits!

A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. What might a quantum computer look like?
3. What is a good model of computation for quantum computers?
4. **What would make a good quantum programming language?**
5. What are the issues in building quantum computer compilers?
6. When are we likely to see scalable quantum computers?

Why Quantum Programming is Challenging

- States are superpositions
- Operators are unitary transforms
- States of qubits can become entangled
- Measurements are destructive
- No-cloning theorem: you cannot copy an unknown quantum state!

Quantum Algorithm Design Abstractions

- Phase estimation
- Quantum Fourier transform
- Period finding
- Eigenvalue estimation
- Grover search
- Amplitude amplification

Shor's Quantum Factoring Algorithm

Input: A composite number *N*

Output: A nontrivial factor of *N*

```
if N is even then return 2;
if N = a^b for integers a >= 1, b >= 2 then
 return a;
x := rand(1,N-1);
if gcd(x,N) > 1 then return gcd(x,N);
r := order(x mod N); // only quantum step
if r is even and x^(r/2) != (-1) mod N then
 {f1 := gcd(x^(r/2)-1,N);  f2 := gcd(x^(r/2)+1,N)};
if f1 is a nontrivial factor then return f1;
else if f2 is a nontrivial factor then return f2;
else return fail;
```

Nielsen and Chuang, 2000

The Order-Finding Problem

Given positive integers x and N, $x < N$, such that gcd(x, N) = 1, the order of x (mod N) is the smallest positive integer r such that $x^r \equiv 1 \pmod{N}$.

E.g., the order of 5 (mod 21) is 6.

The order-finding problem is, given two relatively prime integers x and N, to find the order of x (mod N).

All known classical algorithms for order finding are superpolynomial in the number of bits in N.

Quantum Order Finding

Order finding can be done with a quantum circuit containing

$$O((\log N)^2 \log\log(N) \log\log\log(N))$$

elementary quantum gates.

Best known classical algorithm requires

$$\exp(O((\log N)^{1/2} (\log\log N)^{1/2})$$

time.

Quantum Programming Languages

- Quantum pseudocode [Knill, 1996]
- Imperative: e.g., QCL [Ömer, 1998-2003]
  - syntax derived from C
  - classical flow control
  - classical and quantum data
  - interleaved measurements and quantum operators
- Functional: e.g., QFC, QPL, QML
  - Girard's linear logic
  - quantum lambda calculus

A Compiler Writer Looks at Quantum Computing

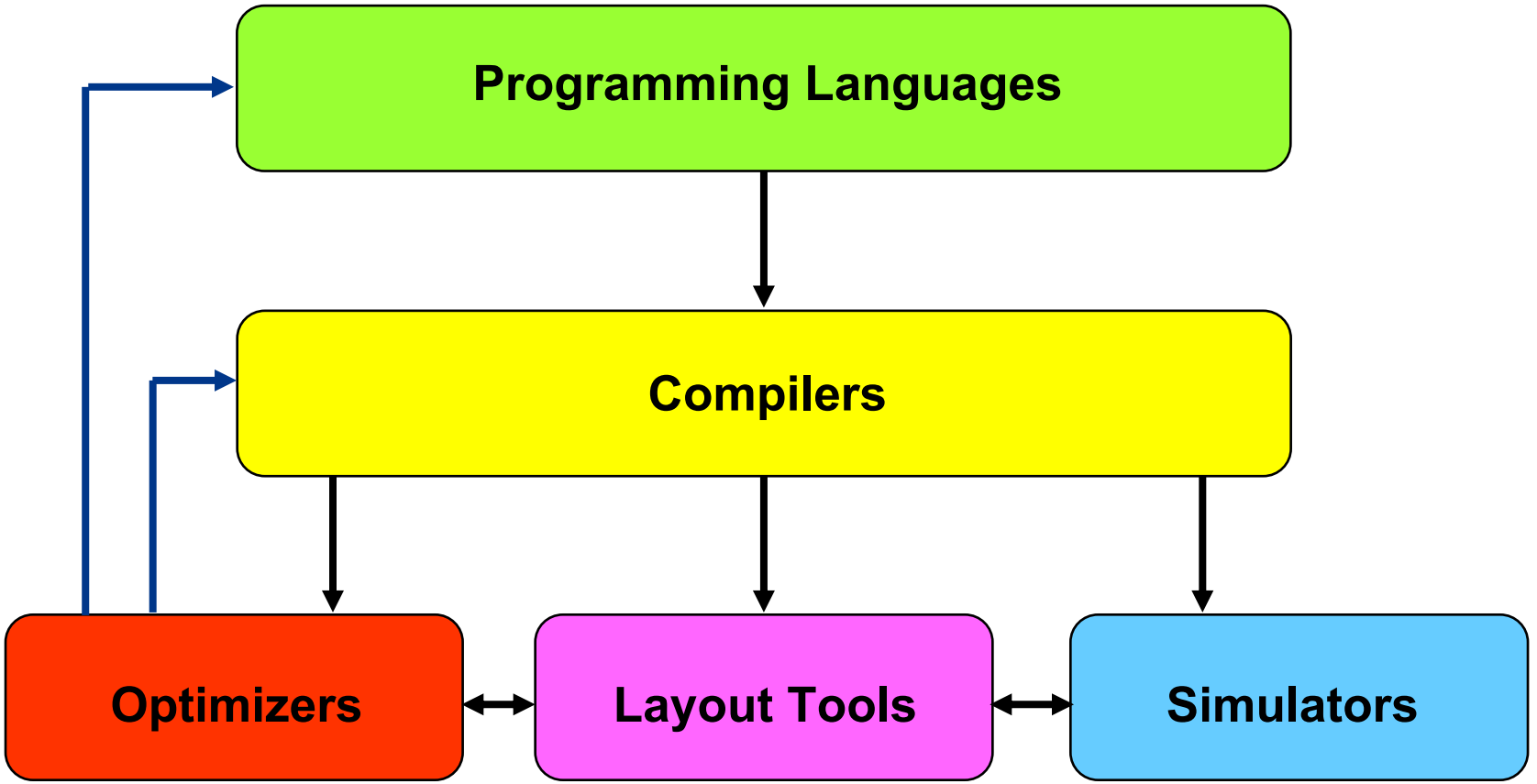
1. Why is there so much excitement about quantum computing?
2. What might a quantum computer look like?
3. What is a good model of computation for quantum computers?
4. What would make a good quantum programming language?
5. **What are the issues in building quantum computer compilers?**
6. When are we likely to see scalable quantum computers?

Desiderata

- A design flow that will map high-level quantum programs into efficient fault-tolerant technology-specific implementations on different quantum computing devices
- Languages, compilers, simulators, and design tools to support the design flow
- Well-defined interfaces between components
- Efficient methods for incorporating fault tolerance and quantum error correction
- Efficient algorithms for optimizing and verifying quantum programs

Quantum Design Tools Hierarchy

- **Vision: Layered hierarchy with well-defined interfaces**

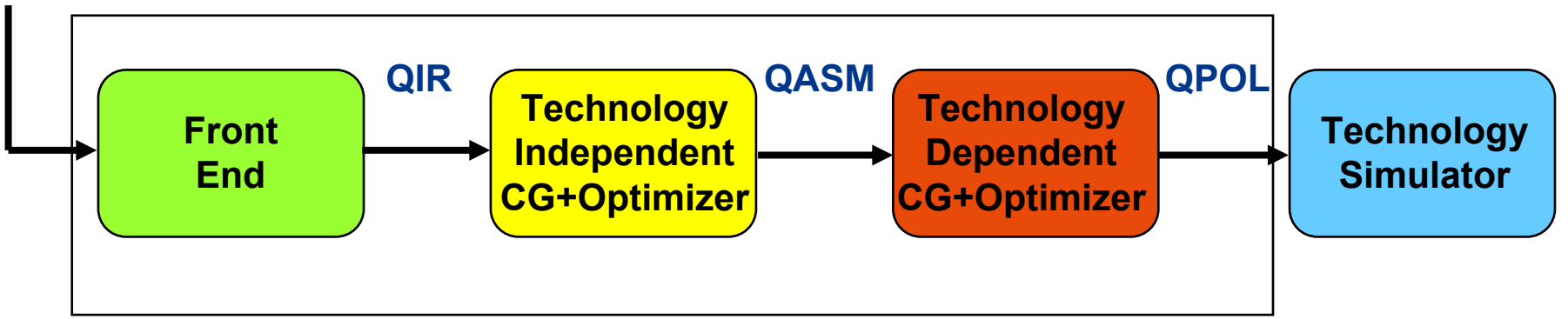


K. Svore, A. Aho, A. Cross, I. Chuang, I. Markov
A Layered Software Architecture for Quantum Computing Design Tools
***IEEE Computer*, 2006, vol. 39, no. 1, pp.74-83**

Languages and Abstractions in the Design Flow

quantum source program

QIR: quantum intermediate representation
QASM: quantum assembly language
QPOL: quantum physical operations language



Quantum Computer Compiler

ABSTRACTIONS

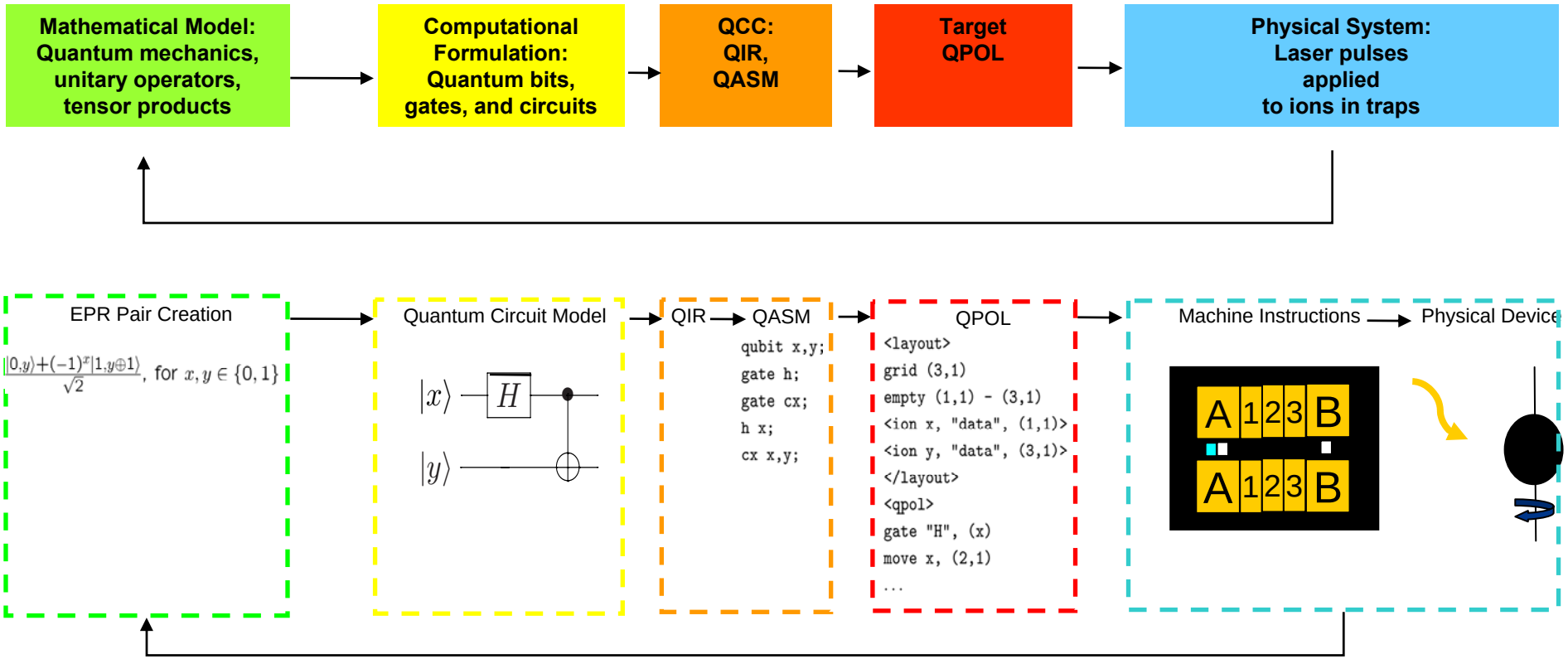
quantum mechanics

quantum circuit

quantum circuit

quantum device

Design Flow for Ion Trap

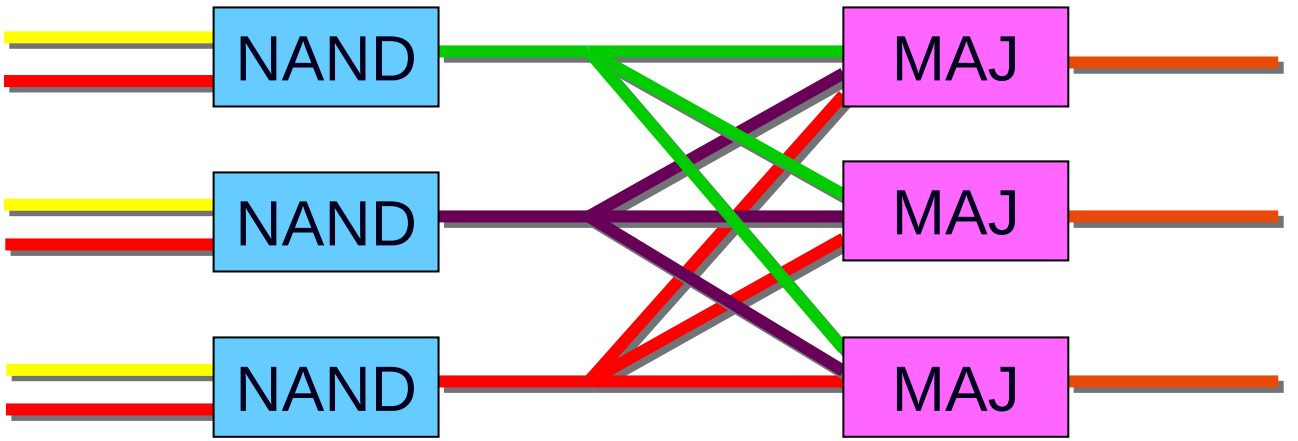


Fault Tolerance

- **In a fault-tolerant quantum computer, more than 99% of the resources spent will probably go to quantum error correction [Chuang, 2006].**

- **A circuit containing N (error-free) gates can be simulated with probability of error at most ε, using $N \log(N/\varepsilon)$ faulty gates, which fail with probability p, so long as $p < p_{th}$ [von Neumann, 1956].**

Fault-tolerant NAND



- Encode data: 0 → 000, 1 → 111
- Assume each gate fails with probability *p*
- Circuit fails only if 2 gates fail (6 possibilities)

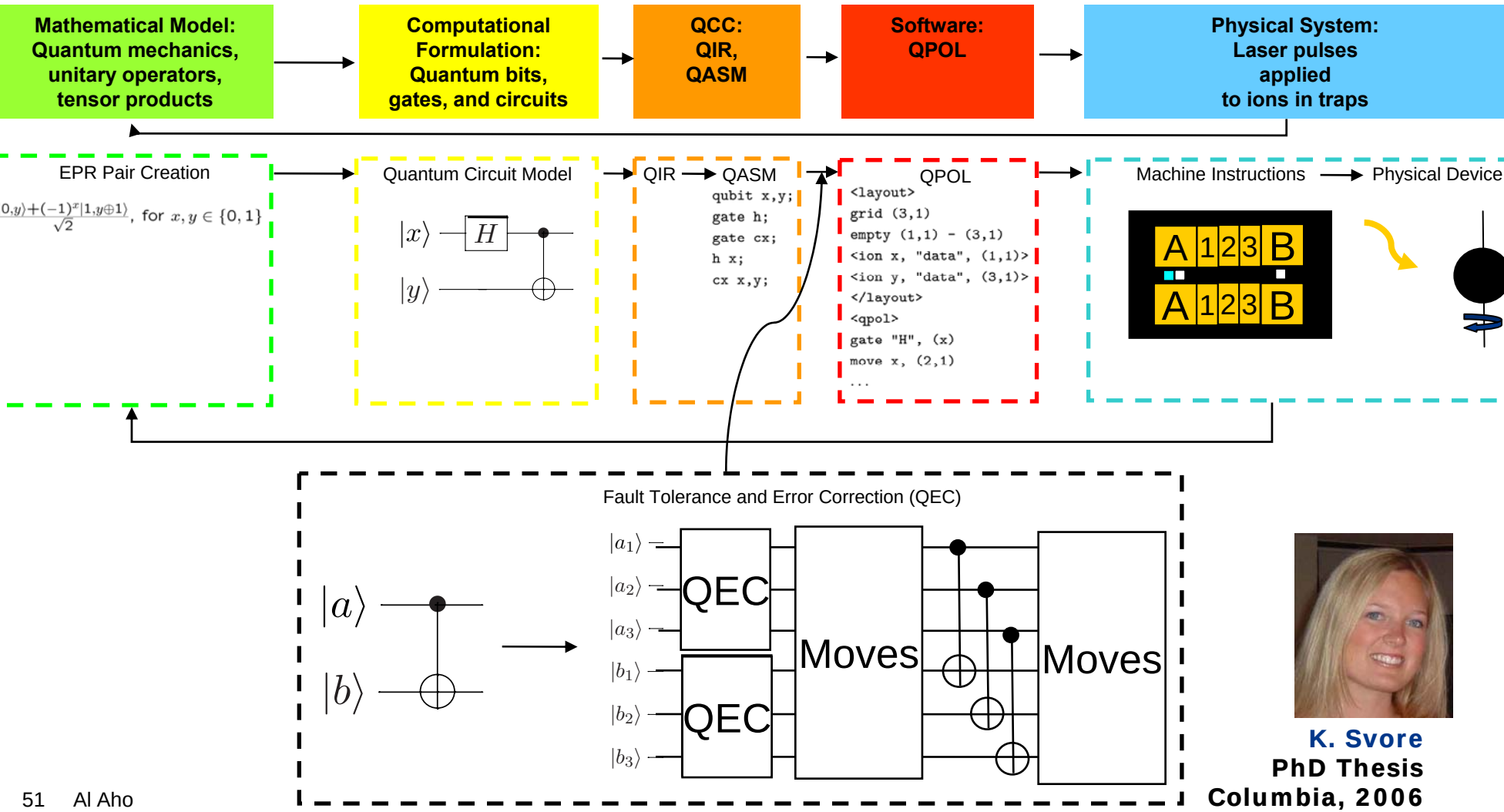
$$p_{fail} \leq 6p^2 \quad \Rightarrow \quad p \leq \frac{1}{6}$$

Fault Tolerance

- Obstacles to applying classical error correction to quantum circuits:
  - no cloning
  - errors are continuous
  - measurement destroys information

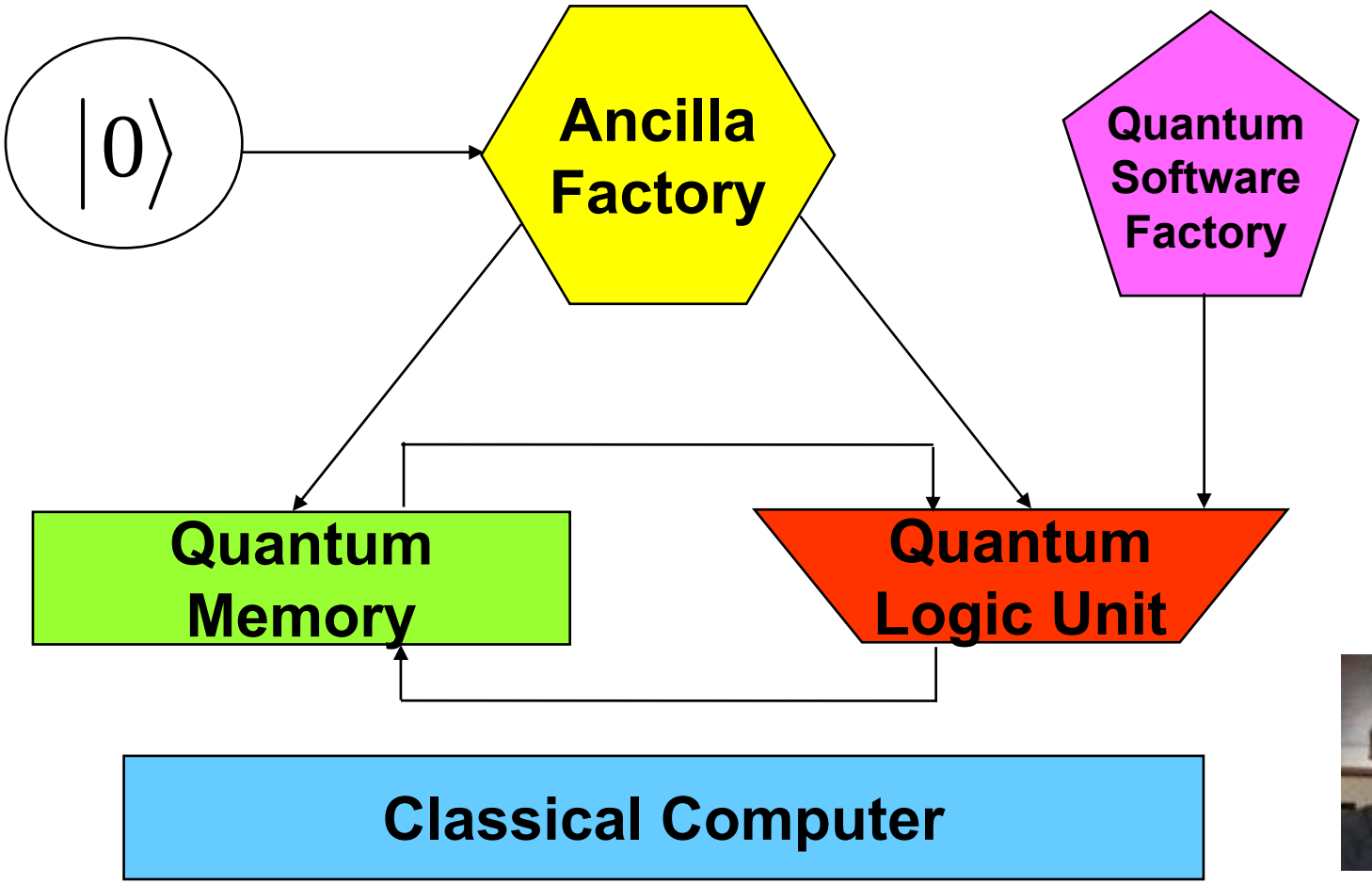
- Shor [1995] and Steane [1996] showed that these obstacles can be overcome with concatenated quantum error-correcting codes.

Design Flow with Fault Tolerance and Error Correction



K. Svore
PhD Thesis
Columbia, 2006

Cross's Fault-Tolerant Quantum Computer Architecture



Andrew W. Cross

Fault-Tolerant Quantum Computer Architectures Using Hierarchies of Quantum Error-Correcting Codes

PhD Thesis, MIT, June 2008

Optimization and Simulation of Quantum Circuits

- Optimizing and simulating quantum circuits on a classical computer is difficult
- The matrices for quantum gates and the vectors for qubit states grow exponentially with the number of qubits
- Quantum Information Decision Diagrams (QuIDDs), patterned after BDDs for classical circuits, exhibit polynomial growth for important classes of circuits
- QuIDDPro, a quantum computing simulator that uses QuIDDs, can be used to efficiently optimize and simulate important classes of quantum circuits

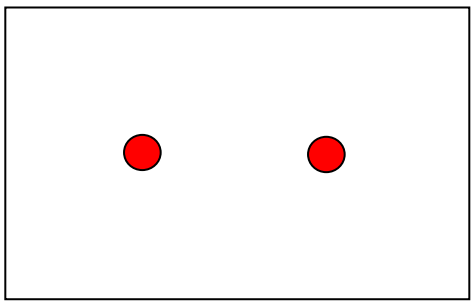
G. Viamontes, I. Markov, J. Hayes
Checking Equivalence of Quantum Circuits and States
Proc. 2007 IEEE/ACM ICCAD, 2007, pp. 69-74

Topological Quantum Computing

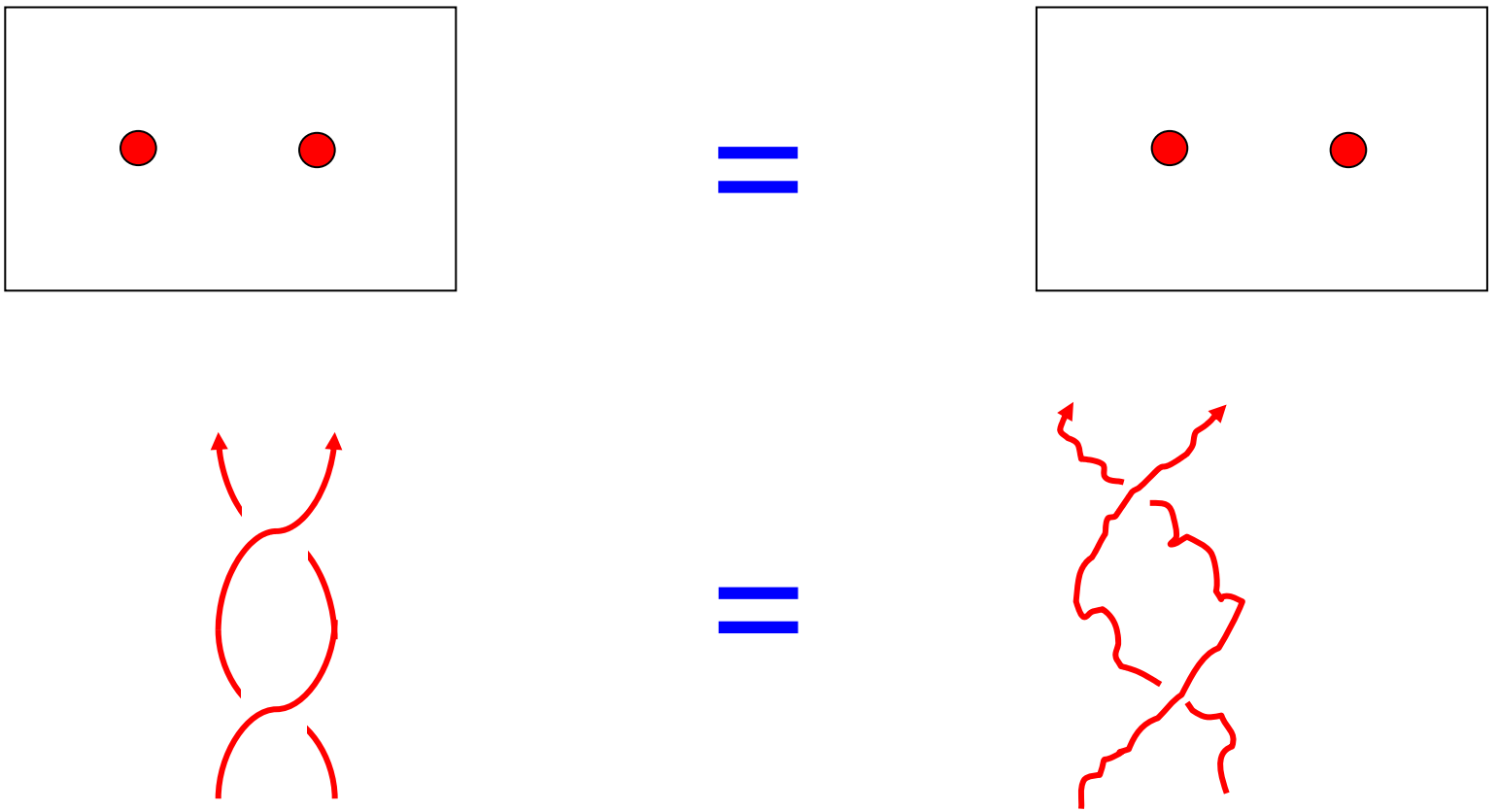
- **The simulation of topological quantum field theories by quantum computing**

- **The solution to quantum fault tolerance?**

Topological Robustness

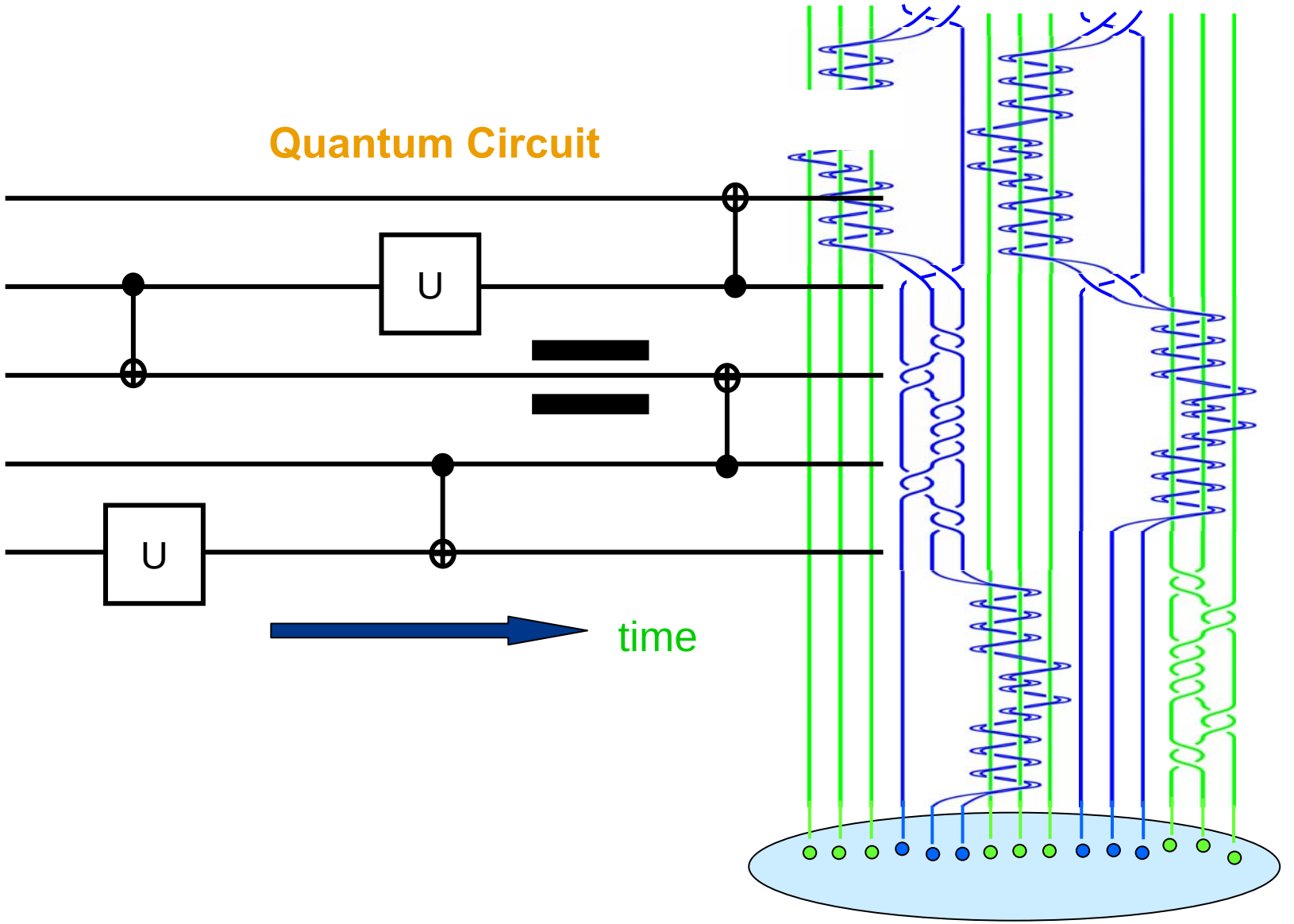


Topological Robustness



Bonesteel, Hormozi, Simon, … ; PRL 2005, 2006; PRB 2007

Braid



1. Degenerate ground states (in punctured system) act as the qubits

2. Unitary operations (gates) are performed on ground state by braiding punctures (quasiparticles) around each other.

   Particular braids correspond to particular computations.

3. State can be initialized by "pulling" pairs from vacuum
   State can be measured by trying to return pairs to vacuum

4. (Variants of these schemes 2,3 are possible)


Kitaev Freedman

Advantages:

- Topological Quantum "memory" highly protected from noise
- The operations (gates) are also topologically robust

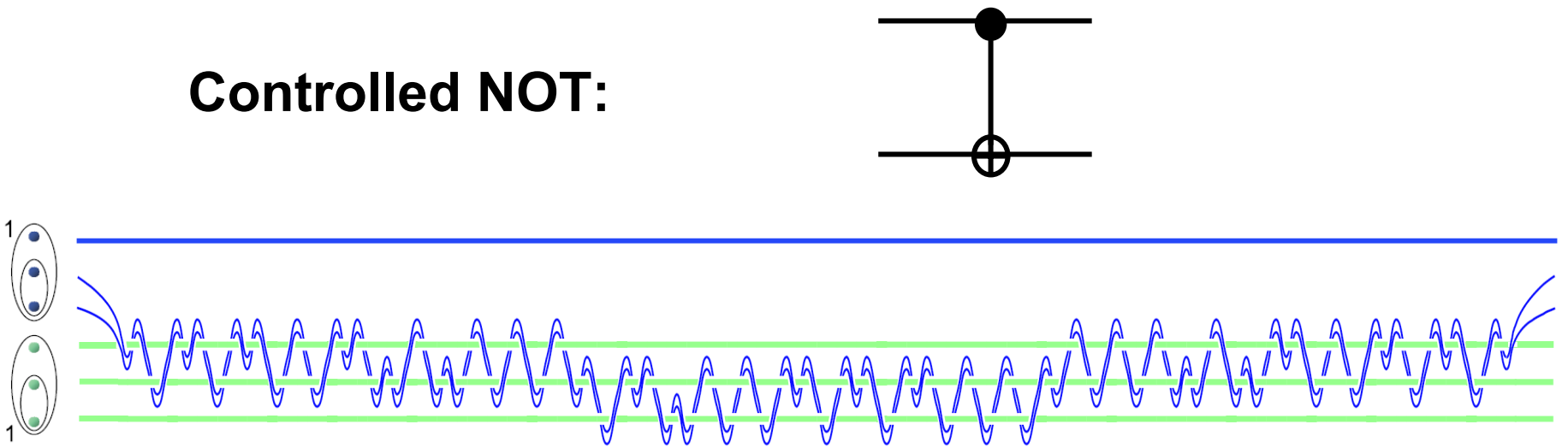
Ref: *Non-Abelian Anyons and Topological Quantum Computation*
C. Nayak, S.H. Simon, A. Stern, M. Freedman, S. DasSarma
Rev Mod Phys, June 2008

Universal Set of Topologically Robust Gates

(Bonesteel, Hormozi, Simon, 2005, 2006)

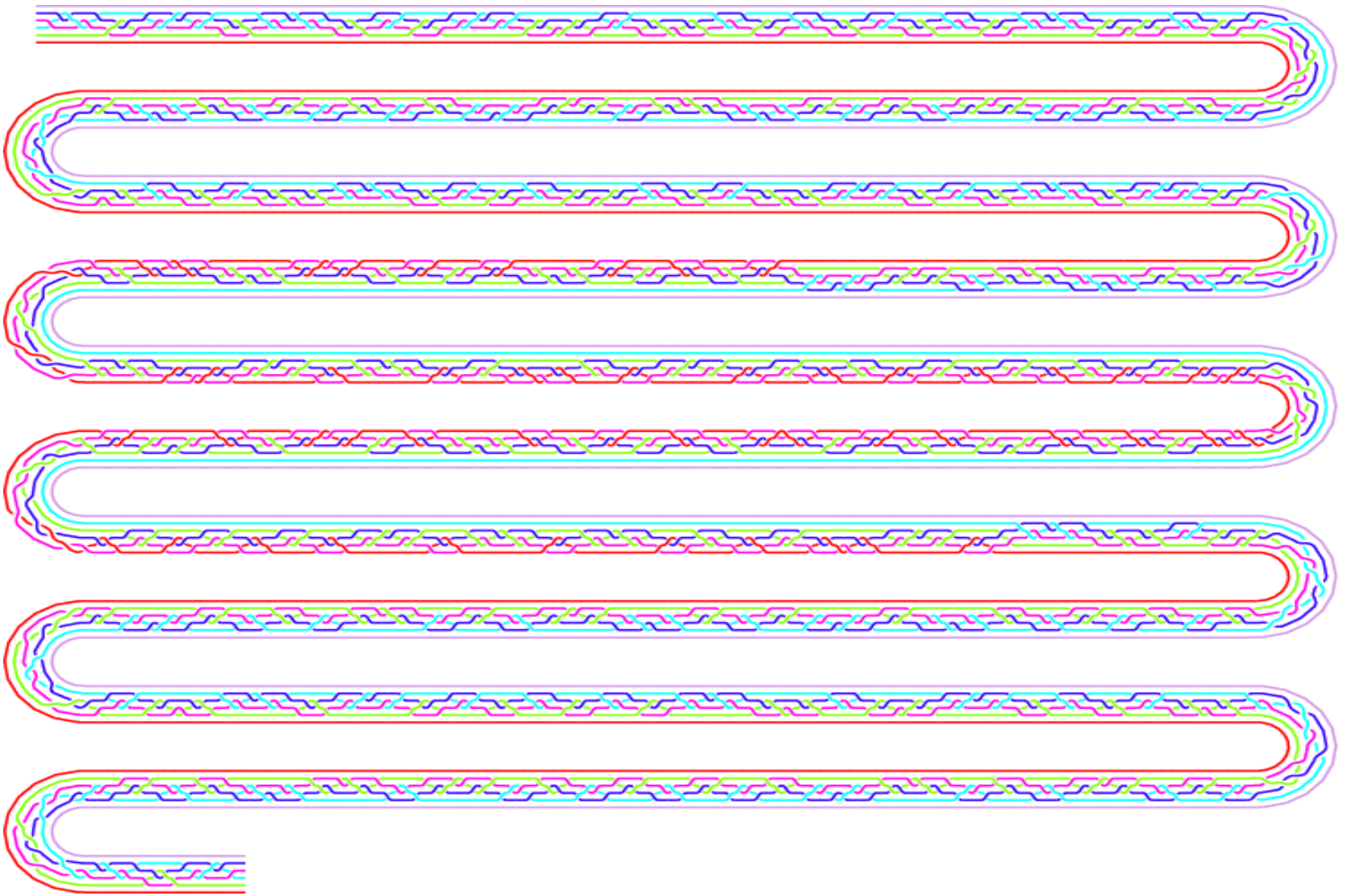
Single qubit rotations: $|\psi\rangle$ — $U_{\vec{\phi}}$ — $U_{\vec{\phi}}\,|\psi\rangle$

Controlled NOT:



Target Code Braid for CNOT Gate

with Solovay-Kitaev optimization



A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. What might a quantum computer look like?
3. What is a good model of computation for quantum computers?
4. What would make a good quantum programming language?
5. What are the issues in building quantum computer compilers?
6. **When are we likely to see scalable quantum computers?**

Press Release: EE Times February 28, 2007

EE Times: Design News
Quantum computer 'Orion' debuts

R. Colin Johnson
EE Times
(02/08/2007 7:32 PM EST)

PORTLAND, Ore. — Computing is poised for a quantum leap in speed and accuracy.

D-Wave Systems Inc. will demonstrate the world's first commercial quantum computer next week, a supercooled, superconducting niobium chip housing an array of 16 qubits.

To date, most quantum computing efforts have focused on communications or cryptography, but the D-Wave quantum computer, called "Orion," solves the most difficult problems—called "NP-Complete"—in a just a few cycles, compared to the thousands of cycles needed by conventional computers.

MIT Technology Review, June 6, 2007

Jason Pontin of MIT's *Technology Review*, interviews Geordie Rose, CTO D-Wave Systems

JP: Are you claiming that the Orion [D-Wave Systems recently announced commercial quantum computer] can solve NP-complete problems? …

GR: It solves them in the sense that it provides approximate solutions to things that are good enough in the sense that they meet the requirements of the user…

JP: … What about the PCP theorem that says that an approximate solution in these cases is as difficult as the best solution? …

GR: "Approximate" means something specific in computer science. It's not the way the term is used conventionally in business.

A Compiler Writer Looks at Quantum Computing

1. Why is there so much excitement about quantum computing?
2. How is a quantum computer different from a classical computer?
3. What is a good programming model for a quantum computer?
4. What would make a good quantum programming language?
5. What are the issues in making quantum computer compilers?
6. When are we likely to see scalable quantum computers?

Collaborators

Isaac Chuang
MIT

Andrew Cross
MIT
now SAIC

Igor Markov
U. Michigan

Krysta Svore
Columbia
now Microsoft Research

Topological Quantum Computing:
Steve Simon
Bell Labs
Alcatel-Lucent