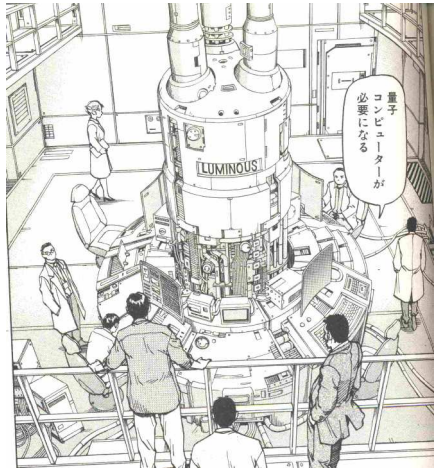
Quantum Computing *Systems*: State of the Art, Summer 2005

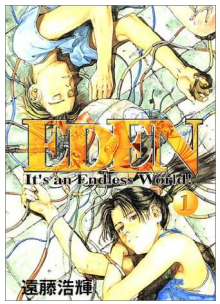
Rodney Van Meter, Keio University
rdv@tera.ics.keio.ac.jp
http://www.tera.ics.keio.ac.jp/person/rdv/

August 25, 2005
@CMU
Systems Design and Implementation Seminar Series

Goal: Design the Fastest, Most Scalable Quantum Computer Possible

One Like This?

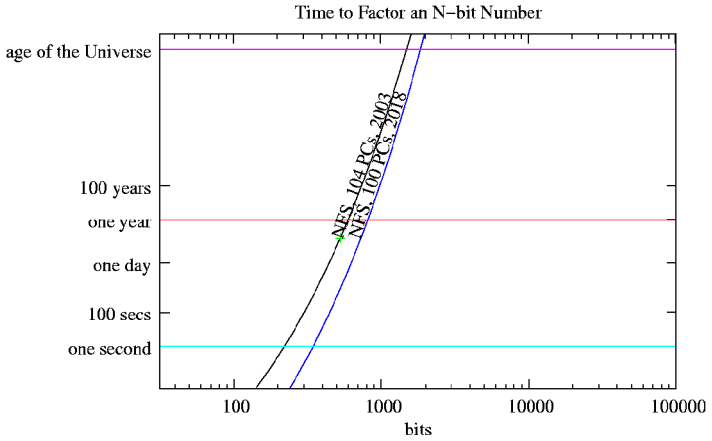




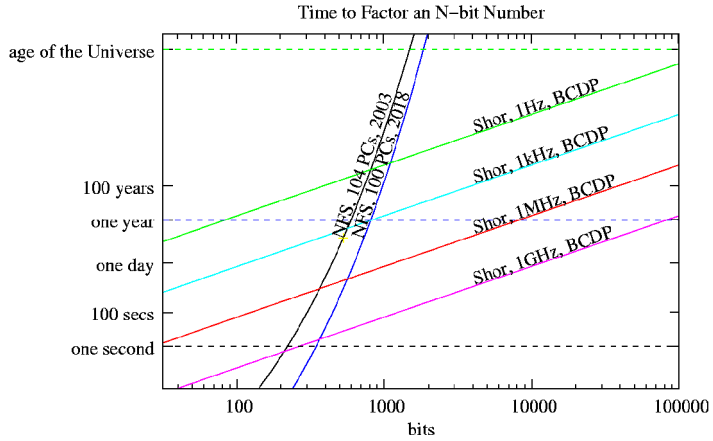
What's a Quantum Computer?

- Uses quantum mechanical effects to accelerate computation
- Can calculate a function on all possible input values at the same time
- Getting a useful answer out is the hard part!
- Most famous result is Shor's algorithm for factoring large numbers

Factoring Larger Numbers



Factoring Larger Numbers



The Challenge

- How do we build *real, non-abstract, usable* quantum computing *systems?*
- More immediately, how do we find the problems and establish a *program* to build these systems?

Outline

- Review principles & power of QC
- Taxonomy of QC technologies
- Recent results (planet-wide)
- My research
  - quantum arithmetic
  - a quantum multicomputer
- Open problems

What is Quantum Computing?

- Uses several important quantum characteristics:
  - Superposition
  - Entanglement
  - Phase (analog)
  - Interference of waveforms
- Input to quantum algorithm is superposition of all possible inputs
- Algorithms run to force interference to eliminate wrong answers

What's It Used For?

- Shor's algorithm for factoring large numbers impacts public-key cryptography
- Other mathematical hidden subgroup problems
- Grover's algorithm for "database search" (really a misnomer)
- Quantum Key Distribution (QKD) for sharing cryptographic keys (requires authenticated, untamperable classical channel)

How Fast Is It?

- Intuitively would hope for exponentially faster, since runs on all inputs
- Most general-purpose algorithm (Grover) is only O(sqrt(N)) to search N items (N = 2^L, for L-bit search space)
- Only special cases get exponential speedup

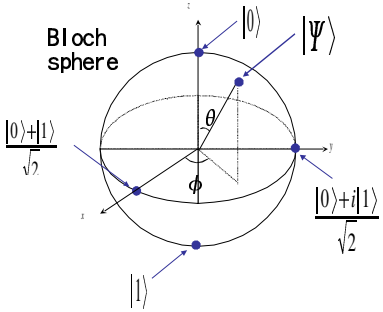
Why Study QC?

- If successful, payoff is revolutionary
- Even if "failure":
  - New physics is being learned
  - Understanding of computational complexity is deepening
  - Engineers must deal with quantum effects and thermodynamic reversibility as devices shrink

1-qubit state and Bloch sphere (Phase)

1-qubit basis states

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix} \quad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$$



superposition

$$|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle=\begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

$$|\alpha|^2+|\beta|^2=1 \quad (\alpha,\beta\in C)$$

$$|\Psi\rangle=e^{i\gamma}\left[\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right]$$

global phase has no effect

$$|\Psi\rangle=\cos\frac{\theta}{2}|0\rangle+e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

relative phase

Measurement and Decoherence

- When a qubit is measured, a result of 0 or 1 is always returned
- Superposition collapses to a single state
- Because the superposition is critical for correct functioning, measurement usually done at end of algorithm
- Accidental measurement is one cause of decoherence, or loss of state, resulting in failure of the algorithm

Acceptable Quantum Phenomena

- Electron spin (up or down)
- Photon polarization (horizontal/vertical)
- Spin of atomic nucleus
- Current in a superconducting loop
- Presence/absence of a particle
- etc., etc., etc....

Problems

- Coherence time
  - nanoseconds for quantum dot, superconducting systems
- Gate time
  - NMR-based systems slow (100s of Hz to low kHz)
- Gate quality
  - generally, 60-70% accurate
- Interconnecting qubits
- Scaling number of qubits
  - largest to date 11 qubits, most 1 or 2

Summary: Characteristics of QC

- Superposition brings massive parallelism
- Phase and amplitude of wave function used
- Entanglement
- Unitary transforms are gates
- Measurement both necessary and problematic when unwanted

So, can we surpass a classical computer with a quantum one?

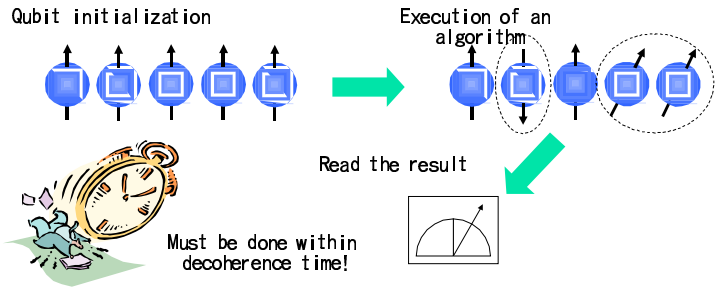
Depends on discovery of quantum algorithms and development of technologies

Outline

- Review principles & power of QC
- Taxonomy of QC technologies
- Recent results (planet-wide)
- My research
  - quantum arithmetic
  - a quantum multicomputer
- Open problems

DiVincenzo's Criteria

1. Well defined extensible qubit array
2. Preparable in the "000…" state
3. Long decoherence time
4. Universal set of gate operations
5. Single quantum measurements



Quantum Computer Taxonomy

- flying or sedentary qubits?
- single v. ensemble
- concurrent gate support
- addressing
- natural gates ("instruction set")
- logical encoding

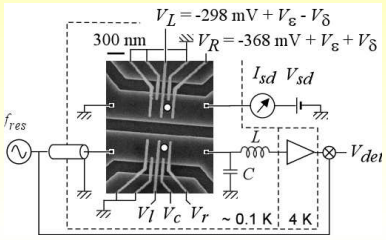
Quantum Computer Taxonomy (2)

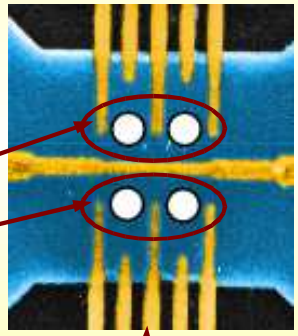
- internal topology
- quantum I/O
- time: clock speed v. decoherence
- timing: jitter and skew control
- programmability
- operating temperature
- measurement time v. gate time

Example: Layout (Internal Interconnect, Measurement)

- Quantum dots as example
- Leads to dots require space
- Double-dot structure limits layout
- Measurement device requires space (fit with every qubit? probably not)

Two-Quantum-Dot Qubits





Qubit 1

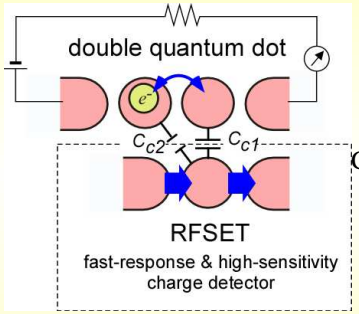
Qubit 2

Measurement device not included in this one! (see next slide)

Where will you put qubit 3?

Control leads

Toward single shot measurement



Bandwidth ~ 100 MHz

Sensitivity ~ 3×10^{-6} $eHz^{-1/2}$

$(C_{c1} - C_{c2})/C_\Sigma = 0.01 - 0.03$

Charge detection time: ~ 10 - 100 ns

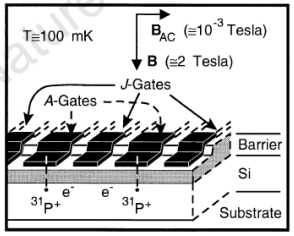
(optimistic expectation)

(T_1 = 10 ns – 1 μs – ?)

A. Aassime et al., Phys. Rev. Lett. 86, 3376 (2001).
S. Gardelis et al., Phys. Rev. B 67, 073302 (2003).
J. Elzerman et al., Phys Rev B 67, R161308 (2003).
L. C. L. Hollenberg et al., Phys. Rev. B 69, 113301 (2004).
L. DiCarlo et al., cond-mat/0311308.

Kane Solid-State NMR

Qubits are stored in the spin of the nucleus of phosphorus atoms embedded in a zero-spin silicon substrate. Standard VLSI gates on top control electric field, allowing electrons to read nuclear state and transfer that state to another P atom.



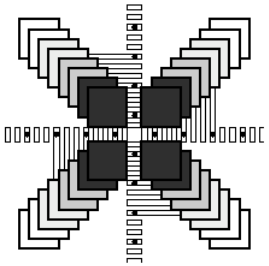
Kane, Nature, 393(133), 1998

Recent advances in manufacturing: can register individual P atoms in the Si lattice (Clark *et al.*, Phil. Trans. R. Soc. London A, 2003)

Kane/Oskin Lattice

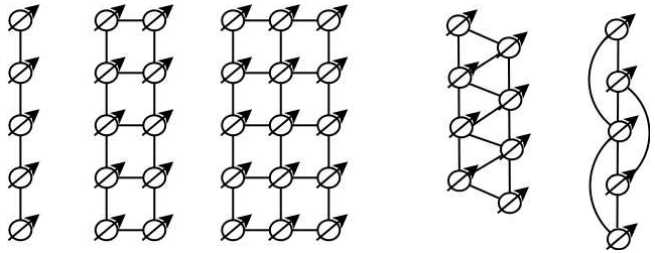
Black dots are location of P atoms. Small rectangles are quantum-scale leads. Large squares are standard-size VLSI leads.

Fitting it all in is tough! This is the role of system architecture...



Oskin et al., ISCA, 2003

Desirable 2D Layouts



1D chain | 2xN | 3xN | Triangular ladder | Next-nearest-neighbor (same as trilad)

Even achieving scalable form of any of these will be an accomplishment!

Layout and Error Correction

- QEC requires execution of gates
- Swapping data to execute gates, requires gates
- Threshold gets worse if lots of swapping required
- QEC proven to work for linear next-nearest-neighbor layout
- QEC not known to work for linear nearest neighbor layout (as far as I know)

Layout and Architecture

- We have the basic technologies
- Choosing number and relationship of elements will build up larger blocks
- Constructing systems from blocks is domain of architecture
- Needs of quantum error correction are critical

Outline

- Review principles & power of QC
- Taxonomy of QC technologies
- Recent results (planet-wide)
- My research
  - quantum arithmetic
  - a quantum multicomputer
- Open problems

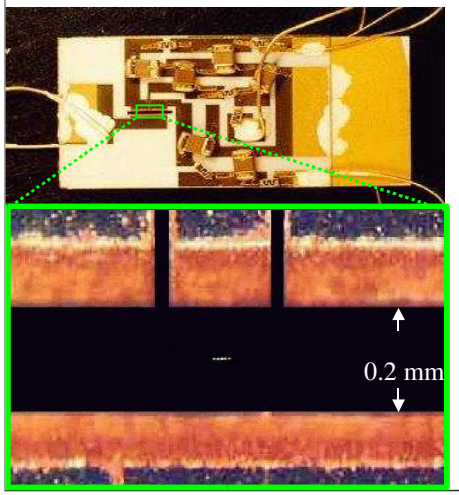
Advanced Architecture: Scalable Ion Trap

One of the few architectures that separates storage space from action space; that is, memory and CPU.

Main group is Wineland group at NIST (USA); Monroe group at Michigan, Chuang group at MIT also making excellent progress.

(Other groups including Oxford also doing small-scale ion trap.)

Trapped-Ion QIP



- Accomplishments:
  - Deutsch-Josza algorithm
    - Blatt group
    - Guide, Nature 421, 48 (2003)
  - 4 qubit entanglement
    - Wineland group
    - Monroe, AIP Conf. Proc. 551 (2001)
  - Ballistic transport
    - Wineland group
    - Rowe, Quantum Information and Computation 2, 257 (2002)
  - **3-qubit QFT**
    - **Chiaverini et al., Science 308 (2005)**

Scalable Ion Trap QC: Architecture?

- Scaling: mictrotraps

(Wineland/NIST)

- **Large-scale QC?**
  - **Teleportation can be used for wiring & code conversion**
  - **Gate errors ~ O(10^{-4}) possible**

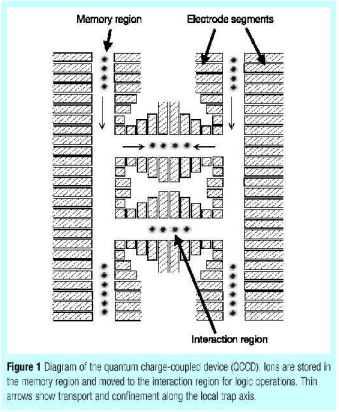
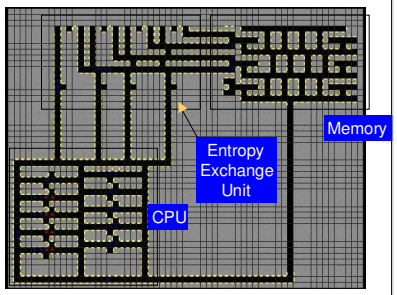


Figure 1 Diagram of the quantum charge-coupled device (QCCD). Ions are stored in the memory region and moved to the interaction region for logic operations. Thin arrows show transport and confinement along the local trap axis.

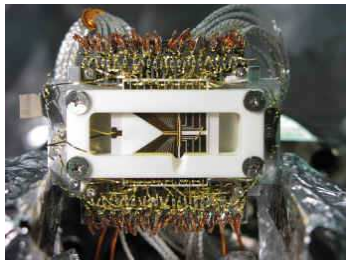
Kielpinski et al, Nature v417, p 709, 2002

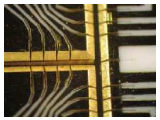
General Quantum Architecture

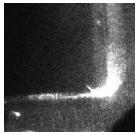
- Processing Units and Memory
- Preparation and Initialization Units
- Communication Strategies
  - Quantum Teleportation Channels
  - Swap Channels



Ion Control: Around a Corner!



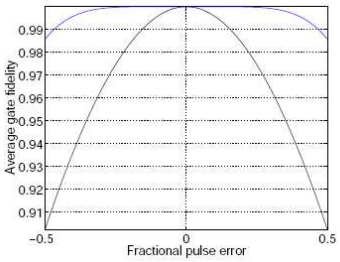




Hensinger *et* al., arxiv.org/quant-ph/0508097
Christopher Monroe's lab, U. Michigan, 2005

Error Control: Analog Gate Accuracy

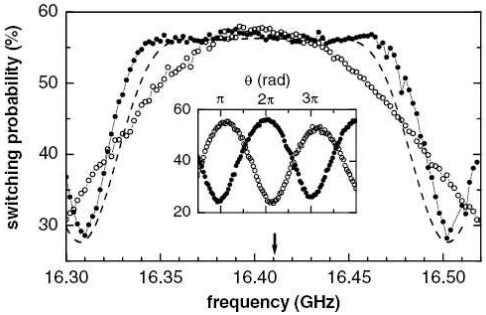
Rotations are analog; QEC can't correct for over- or under-rotation, so NMR sequences used to reduce sensitivity to $O(\epsilon^6)$



Vandersypen & Chuang, Rev. Mod. Phys. **76**, 1037 (2004)

NMR-like Composite Pulses

In Josephson junction; also, Rigetti *et al.* (PRL 94, 2005),
1K gates in liquid NMR

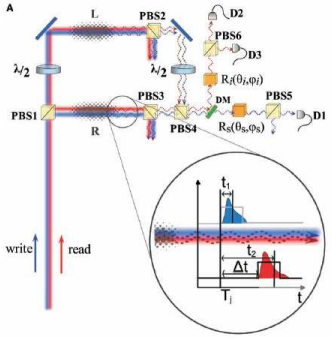


Collin *et al.*, PRL **93** (2004)

Qubit Transfer

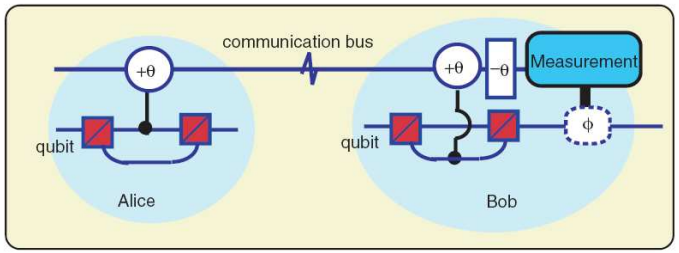
Qubits can (and *must*) be transferred from e.g. nuclear spin to electron spin to photon and back again.

Matsukevich & Kuzmich, Science **306** (2004), executed w/ fidelity ~0.75.



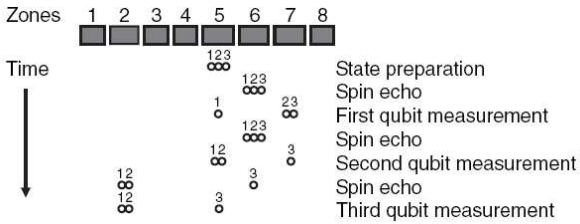
(Various other groups working on this for various technologies; Childress *et al.* quant-ph/0502112, Mehring *et al.* PRL **90** (2003), Jelezko *et al.* PRL **93** (2004).)

Weak Non-Linearity Optical



Uses macro laser phenomenon interacting with single photon at each end to determine parity of two qubits – creates entanglement.
Munro, Nemoto, Spiller, NJP **7** (2005).

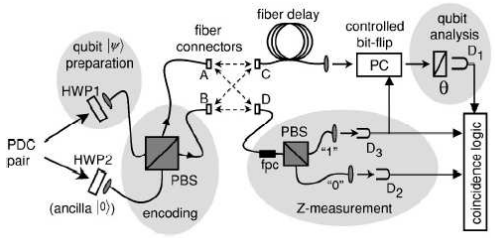
QFT Implementation



3-qubit quantum Fourier transform (QFT) on beryllium ions
Moved ions around, chaining & separating, measuring
Took ~3.5 msec
Fidelity depended on input state – off by 8-29% from expected probability
Chiaverini, *Science*, **308** (2005)

QEC Implementation

Both ion trap and optical demonstrating error-measure-correct cycle



optical: Pittman *et al.*, PRA **71** (2005)
ion trap: Roos *et al., Science*, **304** (2004)

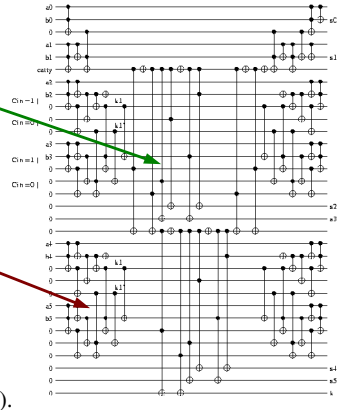
Outline

- Review principles & power of QC
- Taxonomy of QC technologies
- Recent results (planet-wide)
- My research
  - quantum arithmetic
  - a quantum multicomputer
- Open problems

Conditional-Sum Adder

O(log n) latency when long-distance gates are easy. O(n) when swap required (NTC architecture) -- with a big constant!

Better use of concurrent gates (total still O(n) or larger).



(Carry-save and carry-lookahead are other types that reach O(log n). See quant-ph/9808061, quant-ph/0406142.)

Conditional-Sum Adder (AC)

O(log n) latency when long-distance gates are easy. O(n) when swap required (NTC architecture) -- with a big constant!

Better use of concurrent gates (total still O(n) or larger).

(Carry-save and carry-lookahead are other types that reach O(log n). See quant-ph/9808061, quant-ph/0406142.)

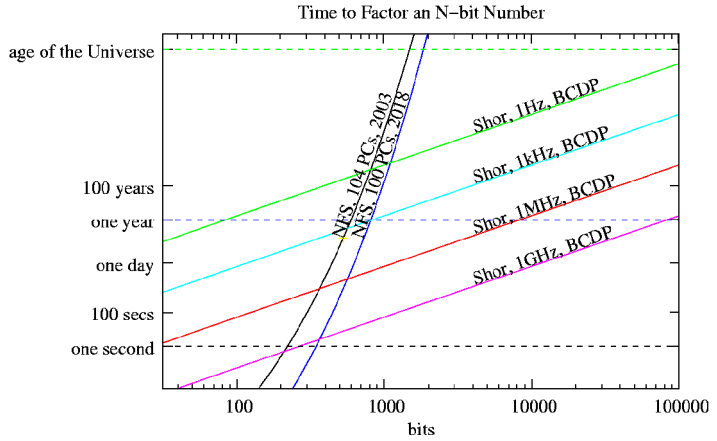
Conditional-Sum Adder (NTC)

O(log n) latency when long-distance gates are free. O(n) when swap required (NTC architecture) -- with a big constant!

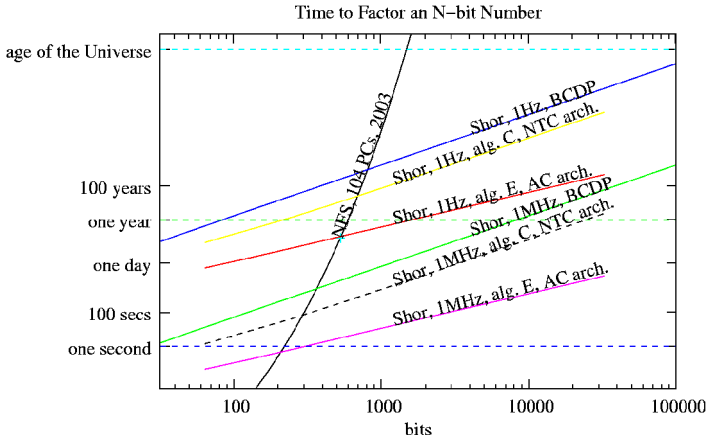
Better use of concurrent gates (total still O(n) or larger).

(Carry-save and carry-lookahead are other types that reach O(log n). See quant-ph/9808061, quant-ph/0406142.)

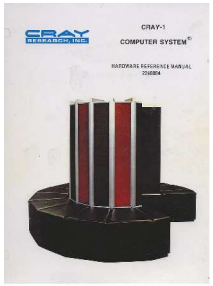
Factoring Larger Numbers



Factoring Larger Numbers

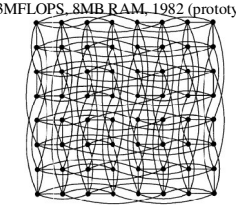


Two Paths to Scalability



Cray 1, 80MFLOPS, 8MB RAM, $9M, 1976

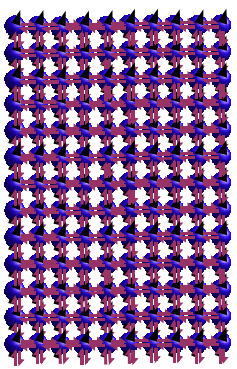
Caltech Cosmic Cube, 64 processors (8086/7) 3MFLOPS, 8MB RAM, 1982 (prototype)

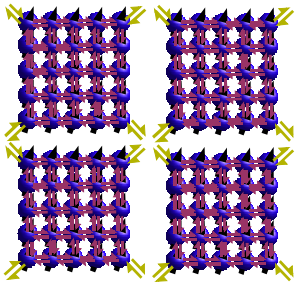


Two choices:

Make it bigger, or figure out how to connect more than one smaller unit hopefully achieving both *speed* and *storage capacity* increases

Two Paths to Scalability





Two choices:
Make it bigger, or figure out how to connect more than one smaller unit hopefully achieving both *speed* and *storage capacity* increases

Outline

- Review principles & power of QC
- Taxonomy of QC technologies
- Recent results (planet-wide)
- My research
  - quantum arithmetic
  - a quantum multicomputer
- Open problems

Summary: Technology

- Liquid NMR: 13 qubits, but limited
- Scalable ion trap promising
- Solid-state (JJ, qdot, NMR) has hurdles
- Optics making advances
- Anything else: dark horse

Summary: Error Control

- Many types of errors & techniques:
  - bit flip, phase flip: QEC
  - error propagation: FT
  - collective decoherence: DFS
  - gate accuracy: NMR composite pulses
- Theoretical grounding solid
- Next step is realistic combinations & conditions (e.g., larger block sizes, matching to technology)

Summary: Algorithm Building Blocks

- QFT well understood
- Arithmetic fundamentals advanced in last year
  - carry-lookahead, conditional-sum, better carry-ripple adders
  - higher level could still use work (multiply, divide, etc.)
- More work on mapping to realistic architectures to be done

Open Problems

Obviously, each technology has its problems to solve; decoherence times, ion movement, gate accuracy, noise, fabrication...

The **big** issue is **scalability**, but just saying that is trite and not very informative...

I would say that scalability requires **heterogeneity**, and the demands of heterogeneity are poorly understood.

Specific Problems

- Distance
- Implementation of QEC, FT, etc.
  - choice of algorithm, block size, mapping to specific technology & architecture
- Compilers & language tools
  - finding efficient gate sequence for given unitary transform
  - optimizing qubit motion

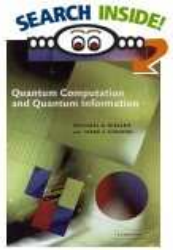
Specific Problems

- Control structures
  - Integrating into systems (for lithographic-based technologies) (can't cram arbitrary # of wires into a dilution fridge!)
  - Does every qubit need a measurement device?
- Balancing classical and quantum portions of a system and a computation (see my MS+S2004 paper)
- Understanding performance

Quantum Multicomputer Problems

- Reliable transfer protocol built on unreliable basis
  - What will performance be?
- Distributed control
  - Clock, sequencing
- Determining minimum node size
  - How will QEC work?
- Possibly, heterogeneous qubit technologies
- Node-to-node network topology

References



- Nielsen & Chuang, Quantum Computation and Quantum Information (esp. Chapter 1)
- Williams, Ultimate Zero and One
- Preskill's lecture notes http://www.theory.caltech.edu/people/preskill/ph229/
- http://www.qubit.org/
- My intro class: http://www.soi.wide.ad.jp/class/20050012/
- http://www.tera.ics.keio.ac.jp/person/rdv/

News/Current Research

- quant-ph mailing list: http://arXiv.org/
- Virtual Journal of Quantum Information (covers PRA, PRB, PRL, etc.)
- Qubit News http://quantum.fis.ucm.es/
- Quantum Pontiff http://dabacon.org/pontiff/
- Science and Nature almost every week...
- QIC, IJQI