Introduction to Quantum Computing
量子計算入門

Rod Van Meter
rdv@tera.ics.keio.ac.jp

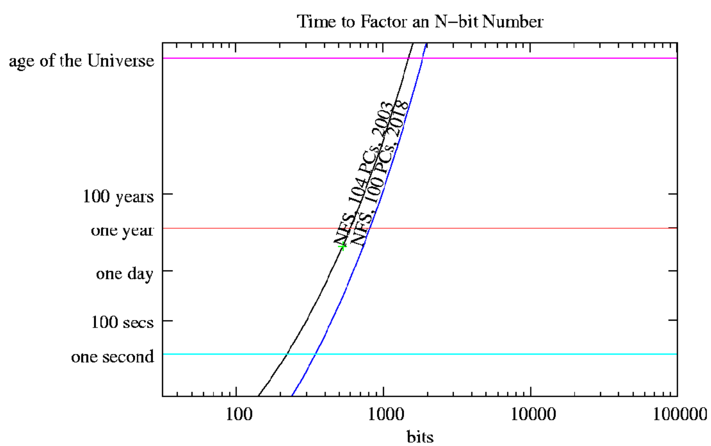
Sept. 28-30, 2004
@会津大学 (U. Aizu)

with help from
伊藤公平 (K. Itoh), 阿部英介 (E. Abe)
and slides from
BBN, Reagan Moore (SDSC), 藤沢 (T. Fujisawa, NTT)

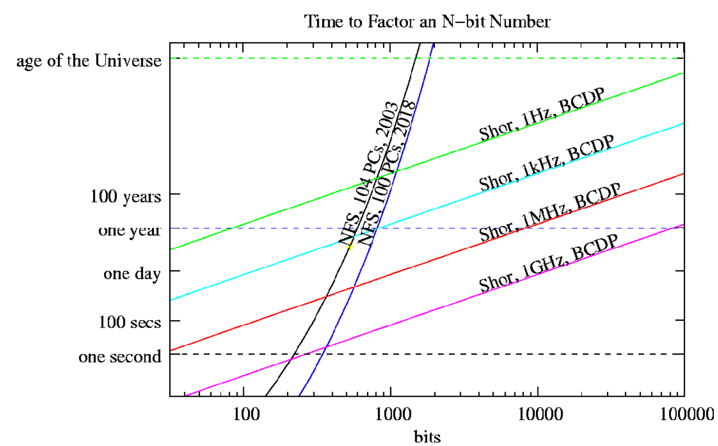
What's a Quantum Computer?

- 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



Course Outline

- Lecture 1: Introduction
- Lecture 2: Quantum Algorithms, Quantum Computational Complexity Theory
- Lecture 3: Devices and Technologies
- Lecture 4: Quantum Computer Architecture
- Lecture 5: Quantum Networking, Wrapup

Today's Outline

- Introductions
- What's Hot: the world we live in (or, why quantum computing is interesting)
- What's a Qubit?
- Reversible computing and unitary transforms
- What's quantum computing (QC) good for?
  - intro to algorithms, technologies, networking

What's Hot

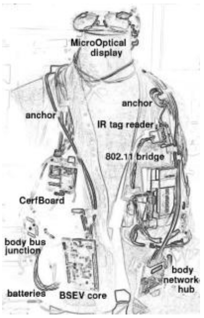
- Mobile & ubiquitous computing
- Robotics
- Supercomputing
- (Computer systems)
- Quantum computing!

Mobile Phones



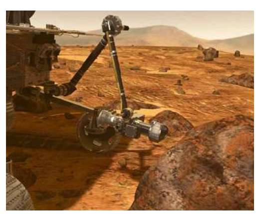


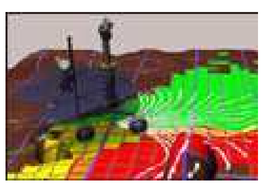
Wearable Computers



Honda's ASIMO

Mars Rovers





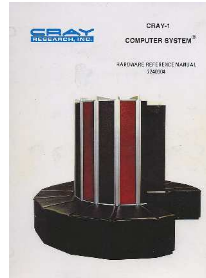
Parallels w/ QC

- Seductive, science fiction-like topic
- Long time between vision and reality
- Convergence of many technologies necessary
- Reality might not look like original vision
- Very big impact when successful

Supercomputing

- A Quantum Computer is a type of Supercomputer
- Today, more about Big Data than Big Processors

Two Paths to Scalability

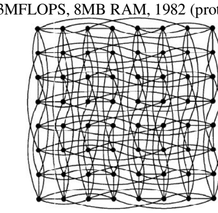


Cray 1, 80MFLOPS, 8MB RAM, $9M, 1976

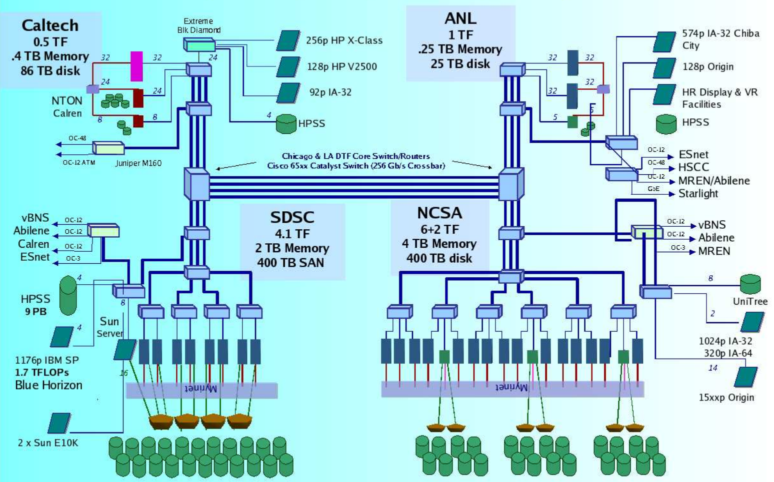
Caltech Cosmic Cube, 64 processors (8086/7) 3MFLOPS, 8MB RAM, 1982 (prototype)

Two choices:

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

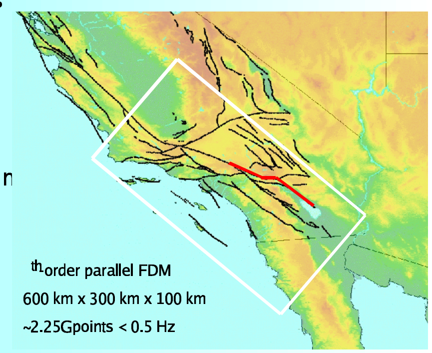


TeraGrid (Aug. 2004): 13.6 TFLOPS, 6.8 TB memory, 900 TB network disk, 10 PB archive (courtesy Reagan Moore, SDSC)



TeraShake Simulation Area

- Rectangular region parallel to San Andreas fault containing:
  - Los Angeles,
  - San Diego,
  - Mexicalli,
  - Tijuana,
  - Ventura Basin,
  - Southern San Joaquin Valley,
  - Catalina Island,
  - Ensenada



th order parallel FDM

600 km x 300 km x 100 km

~2.25Gpoints < 0.5 Hz

TeraShake Simulation Parameters

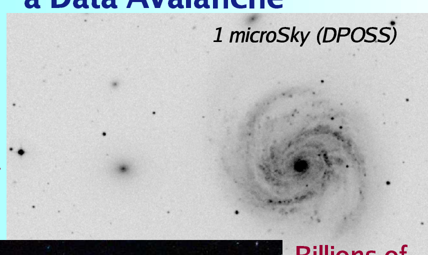
- 600km x 300km x 100km
- Spatial resolution d_x = 200m
- Mesh Dimensions
  - 3000 x 1500 x 500 = 2.25 Gpoints
- Temporal Resolution d_t = 0.01s
- Maximum Frequency = 0.5 Hz
- Simulated time = 200s
- Number of time steps = 20,000

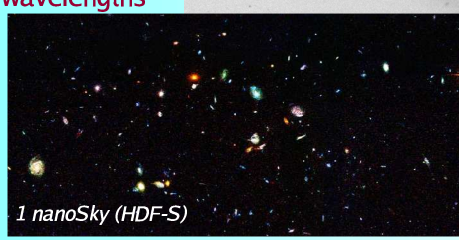
TeraShake Simulation Output

- 4D WaveField
  - Each mesh snapshot 27GBytes
  - 20,000 time steps potentially 540TBytes
  - Run at SDSC DataStar, planned for August
    - Output 2,000 time steps or ~ 60TBytes in 20 hours
    - Digital Library registration and archival with SDSC Storage Resource Broker
- Surface Data for Synthetic Seismograms
  - 1 TByte

Astronomy is Facing a Data Avalanche

Multi-Terabyte (soon: multi-Petabyte) sky surveys and archives over a broad range of wavelengths





Billions of detected sources, hundreds of measured attributes per source

Supercomputing is Big Data

Supercomputing today is not about processing power *per se*. It is about turning enormous amounts of raw data into useful information.

Quantum computing will, indeed, *must*, open new fields of applications, mostly heavily mathematical. QC will probably be of minimal use on existing SC applications.

量子計算とは?

- ひとつの量子は同時に二つの所にある。
  - 誰も見ていない時だけ!
  - 有名なgedankenexperiment: Schroedinger's cat
  - Superposition (重ね合わせ)
- その重ね合わせを使って、ちょう並列計算できるようになっている。

量子計算は何に使えるか?

- 素因数分解(Shor's algorithm):
  量子計算すると : O(L^3) for L-bit number
  古典的な計算方法だと : O(2^L)
- 検索(Grover's algorithm):
  O(sqrt(N)) to search N items (N=2^L)
- Quantum Key Distribution:
  物理学のせいで、絶対セキュア

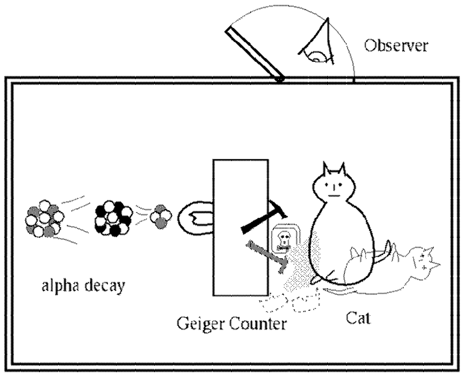
アウトライン

- 量子計算とは?
- 量子計算の基本
- 量子計算のアルゴリズム
- 具体的な実験/技術
- 量子ネットワーク
- 量子コンピューターシステム研究

量子計算の基本

- Superposition, phase, and the ket notation
- Entanglement
- 1 and 2-qubit gates
- Measurement and decoherence

Schroedinger's Cat



Schroedinger's Cat

- If an atom decays, poison is released and the cat dies
- Set up so that probability of atom decaying is 50%
- Is the cat dead or alive?
- When observed, the wave function collapses and the cat "chooses" to be either dead or alive

Superposition（重ね合わせ）and ket Notation

- Qubit state is a vector
  - two complex numbers
- |0> means the vector for 0;
  |1> means the vector for 1;
  |00> means two bits, both 0;
  |010> is three bits, middle one is 1;
  etc.
- A qubit may be partially both!
  (just like the cat, but stay tuned for measurement...)
  complex numbers are wave fn amplitude;
  square is probability of 0 or 1

1-qubitの状態とBloch球（Phase）

1-qubitの状態の標準基底

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

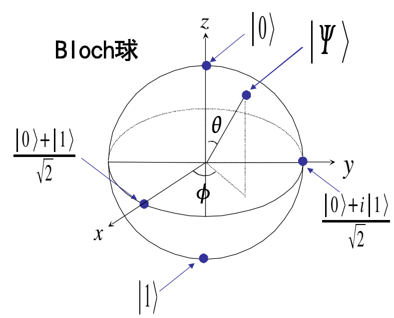
任意の重ね合わせ状態

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

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

複素2変数ー1束縛条件＝実3変数

Bloch球



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

測定結果に影響しない

実2変数（物理的要請）

相対位相

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

Entanglementとは?
絡み付き

- 二つのqubitのvalue (0,1)は相手次第である

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$$

どちらかを測定すると、
相手のvalueは決まる。
0でも1でもの確率は50%だが、
(0,1)と(1,0)の確率は0!

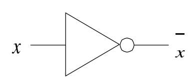
Bit0	Bit1	
0	0	50%
0	1	0%
1	0	0%
1	1	50%

Measurement and Decoherence
(測定と位相緩和)

- Qubitを測定すると、重ね合わせがなくなります。必ず1か0かどちらかの結果になります。
- その重ね合わせは計算に大事なので、計算がおわってから測定する。
- 偶然に測定されると、decoherence(位相緩和)と呼ぶ。この場合は、計算は失敗である。

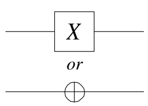
1-qubitの演算の例, Pauli行列

古典回路における1-bit演算 ⇒ NOTのみ



量子演算版NOT = Pauli-X ゲート

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



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

$$\left\{\begin{array}{l} X|0\rangle=|1\rangle \\ X|1\rangle=|0\rangle \end{array}\right. \Leftrightarrow X\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}, X\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}$$

$$X=\begin{bmatrix}\boxed{0} & \boxed{1}\\ \boxed{1} & \boxed{0}\end{bmatrix}$$

$|1\rangle=\begin{bmatrix}0\\1\end{bmatrix}$ がどの状態になるかを表す

$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix}$ がどの状態になるかを表す

Pauli-Y,Z
ゲート

$$Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;—\boxed{Y}—\; -i\beta|0\rangle+i\alpha|1\rangle$$

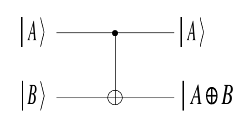
$$Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \qquad \alpha|0\rangle+\beta|1\rangle \;—\boxed{Z}—\; \alpha|0\rangle-\beta|1\rangle$$

2-qubitの量子演算の例

例1. 制御NOTゲート

$$C_{AB}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

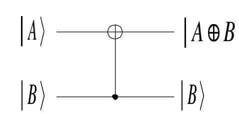
AB
$|00\rangle\to|00\rangle$
$|01\rangle\to|01\rangle$
$|10\rangle\to|11\rangle$
$|11\rangle\to|10\rangle$



mod 2 の足し算

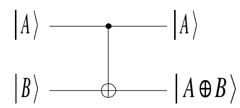
$$C_{BA}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}$$

AB
$|00\rangle\to|00\rangle$
$|01\rangle\to|11\rangle$
$|10\rangle\to|10\rangle$
$|11\rangle\to|01\rangle$



制御NOT, Entanglement

必ずしも，「上のレールがqubit A，下のレールがqubit Bの情報を運んでいる」わけでは**ない**ことに注意



$$|1\rangle_A \otimes \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]_B \xrightarrow{C_{AB}} |1\rangle_A \otimes \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]_B$$

「上のレールが $|1\rangle_A$，下のレールが $(|0\rangle_B+|1\rangle_B)/\sqrt{2}$ の状態」と言ってもよさそう

$$\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]_A \otimes |0\rangle_B \xrightarrow{C_{AB}} \frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}$$

Bell state or EPR state

qubit Aの情報とqubit Bの情報は不可分

Unitary演算

Schrödinger equation

$$\frac{\partial|\Psi\rangle}{\partial t} = -iH|\Psi\rangle \qquad \begin{cases} \hbar = 1 & \text{(Planck定数)} \\ H & \text{(系のHamiltonian)} \end{cases}$$

状態ベクトルの時間発展

$$|\Psi\rangle \to \exp(-iHt)|\Psi\rangle = U|\Psi\rangle$$

U: unitary演算子 $\quad UU^\$ = U^\$ U = 1$

Sorry, not "dagger" but "dollar"!

$$(AB)^\$ = B^\$ A^\$ \qquad (U|\Psi\rangle)^\$ = \langle\Psi|U^\$$$

1-qubitの量子状態の変化

$$|\Psi\rangle = {}_0|0\rangle + {}_0|1\rangle \vec{U}_1 \; {}_1|0\rangle + {}_1|1\rangle \vec{U}_2 \; {}_2|0\rangle + {}_2|1\rangle \vec{U}_3 \cdots$$

$$U_n \cdots U_2 U_1 |\Psi\rangle$$

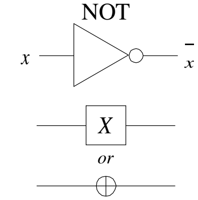
Time ←

In Layman's Terms

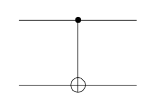
- "Unitary" implies "reversible"
- Necessary to preserve quantum state
- Deleting information requires energy, creates entropy
- Reversible computing also making inroads in classical computing
- Same number of outputs as inputs

Reversible Gates

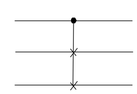
NOT



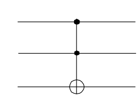
Control-NOT



Control-SWAP
(Fredkin gate)



Control-Control-NOT
(Toffoli gate)



Hadamardゲート

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

$—\boxed{H}—$

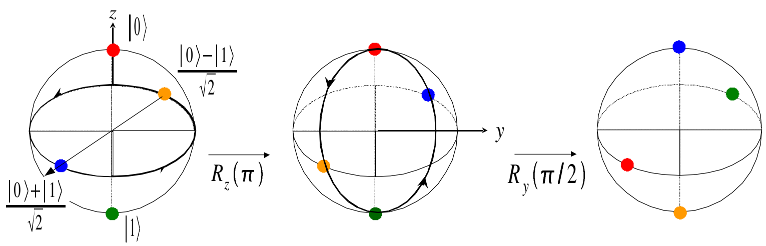
$$HH^{\$}=I$$

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

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

$$R_y(\pi/2)\,R_z(\pi)=-iH \qquad R_y(\pi/2)=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix} \qquad R_z(\pi)=\begin{bmatrix}-i & 0\\ 0 & i\end{bmatrix}=-iZ$$

Time



測定

通常，「測定」は「標準基底による測定」を指す

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

確率 ¿$|\alpha|^2$¿で，“0” を得る

確率 ¿$|\beta|^2$¿で，“1” を得る

現実の測定では，他の基底でしか測定できないことがありうる

$\{|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2},\ |-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$ の基底で測定すると $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle=\frac{\alpha+\beta}{\sqrt{2}}|+\rangle+\frac{\alpha-\beta}{\sqrt{2}}|-\rangle$ なので，

$|\psi\rangle$ ±¿

確率 ¿$|\alpha+\beta|^2/2$ で，“+” を得る

確率 ¿$|\alpha-\beta|^2/2$ で，“−” を得る

基底の変換

$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ $—\boxed{H}—$ $|\psi\rangle=\alpha|+\rangle+\beta|-\rangle$ ±¿

確率 ¿$|\alpha|^2$¿で，“+ ”

確率 ¿$|\beta|^2$¿で，“− ”

量子計算の特徴

- 状態の重ね合わせによる量子並列性
- 振幅と位相の非局所性
- Entanglement
- Unitary変換による多様な演算
- 測定による状態の収縮

古典計算機をしのぐ高速計算の可能性?

量子アルゴリズムの発明

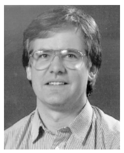
アウトライン

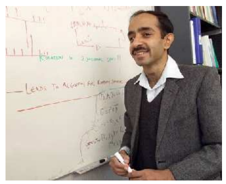
- 量子計算とは?
- 量子計算の基本
- 量子計算のアルゴリズム
- 具体的な実験
- 量子ネットワーク
- 量子コンピューターシステム研究

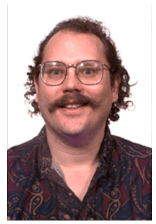
量子アルゴリズム

- Deutsch-Jozsa(D-J)のアルゴリズム
  - Proc. R. Soc. London A, 439, 553 (1992)
- Groverの検索アルゴリズム
  - Phys. Rev. Lett., 79, 325 (1997)
- Shorの素因数分解アルゴリズム
  - SIAM J. Comp., 26, 1484 (1997)


D. Deutsch


R. Jozsa

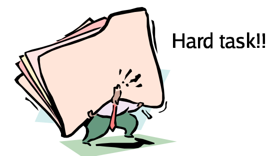

L. K. Grover

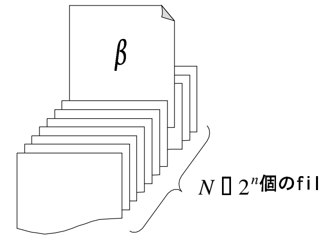

P. W. Shor

Groverの検索アルゴリズム

$N=2^n$ 個のfileの中から，所望のfile “β” を検索する

古典的には，順番にfileを調べて，平均N/2回程度の操作が必要





Groverのアルゴリズムでは，N 個のfile(状態)の重ね合わせから，出発して $\sqrt{N}$ 回程度のunitary演算G を実行することで，ほぼ所望のfileに到達

$$|\Psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle \longrightarrow ¿ \approx |\beta\rangle$$

Shorの素因数分解アルゴリズム

$$66554087 =?\ 6703 \times 9929$$

古典的な方法では，指数オーダーの時間を要する素因数分解アルゴリズムしか知られていない

古典的には、O(2^L)

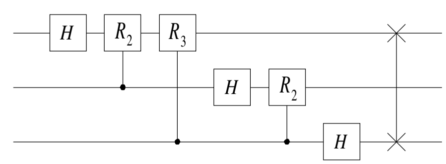
量子Fourier変換を使って、O(L^3)

一番有名な量子計算のアルゴリズム

量子Fourier変換

FFTの量子計算版 $|j\rangle \xrightarrow{QFT_N} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp(2\pi ijk/N)|k\rangle$

例 QFT_8を実行する量子回路



$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{bmatrix}$$

QFT_8の行列表示

$$QFT_8 = \frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

$$\omega = \exp(2\pi i/8) = \sqrt{i}$$
$$\omega^i + \omega^{i+4} = 0$$

アウトライン

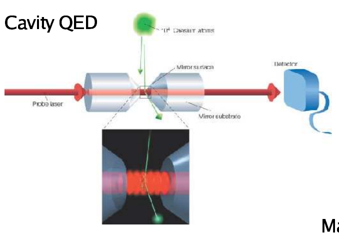
- 量子計算とは?
- 量子計算の基本
- 量子計算のアルゴリズム
- 具体的な実験（慶應を含めて）
- 量子ネットワーク
- 量子コンピューターシステム研究

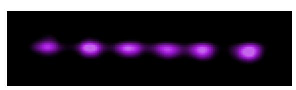
量子計算の実行

- IBM, Stanford, Berkeley, MIT (solution NMR)
- NEC (Josephson junction charge)
- Delft (JJ flux)
- 慶應 (silicon NMR, quantum dot)
- Caltech, Berkeley (quantum dot)
- Australia (ion trap, linear optics)
- Many others (cavity QED, Kane NMR, ...)
- All schemes so far have drawbacks

Physical Realization

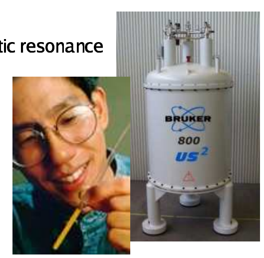
Cavity QED

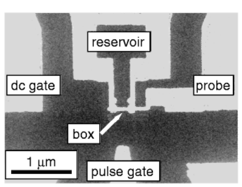




Ion trap

Magnetic resonance

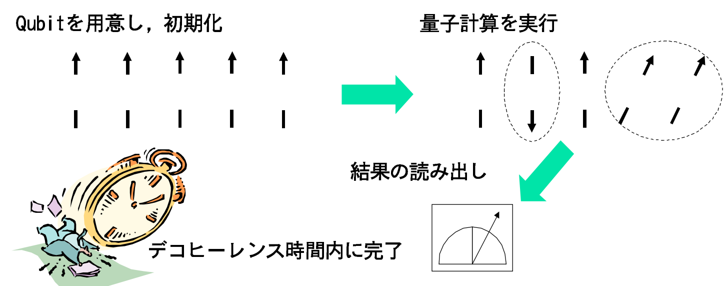




Superconductor

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



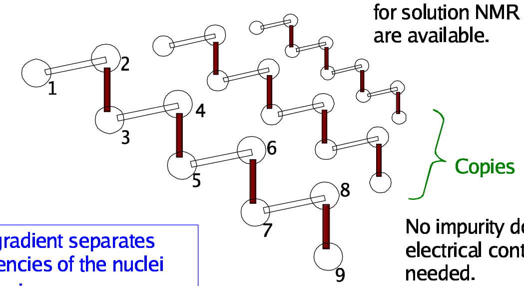
Problems

- 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 7 qubits, most 1 or 2

All-Silicon Quantum Computer

10^5 ^{29}Si atomic chains in ^{28}Si matrix work like molecules in solution NMR QC.

Many techniques used for solution NMR QC are available.

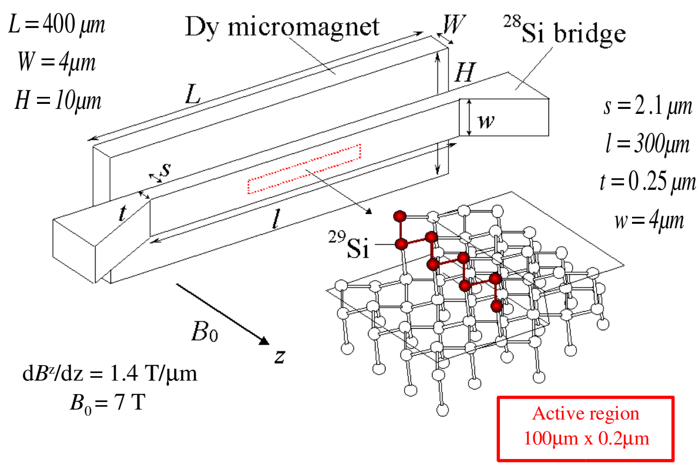


A large field gradient separates Larmor frequencies of the nuclei within each chain.

No impurity dopants or electrical contacts are needed.

T.D.Ladd *et al.*, Phys. Rev. Lett. **89**, 017901 (2002)

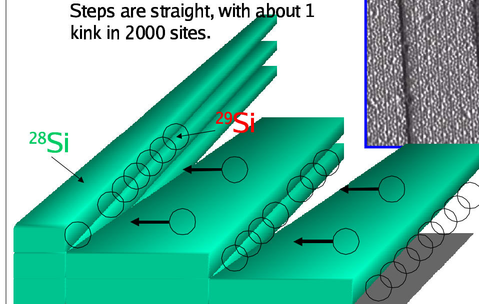
Overview

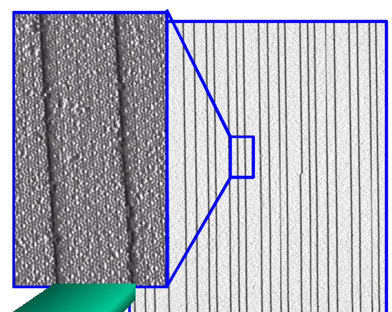


Fabrication: ^{29}Si Atomic Chain

Regular step arrays on slightly miscut ^{28}Si(111)7x7 surface (~1° from normal)

Steps are straight, with about 1 kink in 2000 sites.





STM image

J.-L.Lin *et al.*, J. Appl. Phys **84**, 255 (1998)

アウトライン

- 量子計算とは?
- 量子計算の基本
- 量子計算のアルゴリズム
- 具体的な実験
- 量子ネットワーク
- 量子コンピューターシステム研究

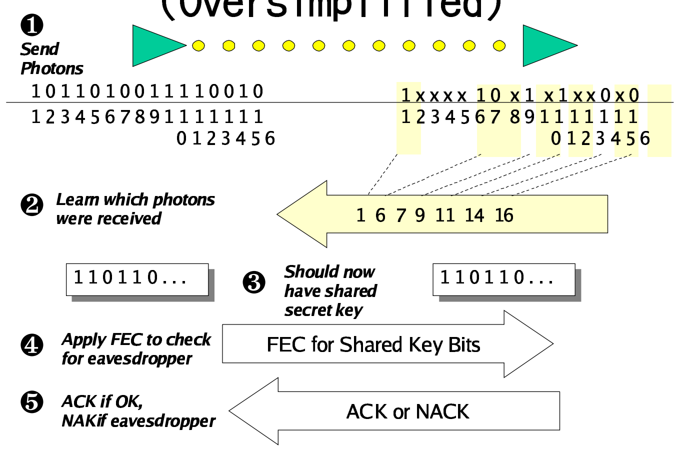
量子ネットワーク

- Quantum Key Distribution (QKD)
- Teleportation
- (Superdense coding)
- All discovered by Charles Bennett (IBM) & associates

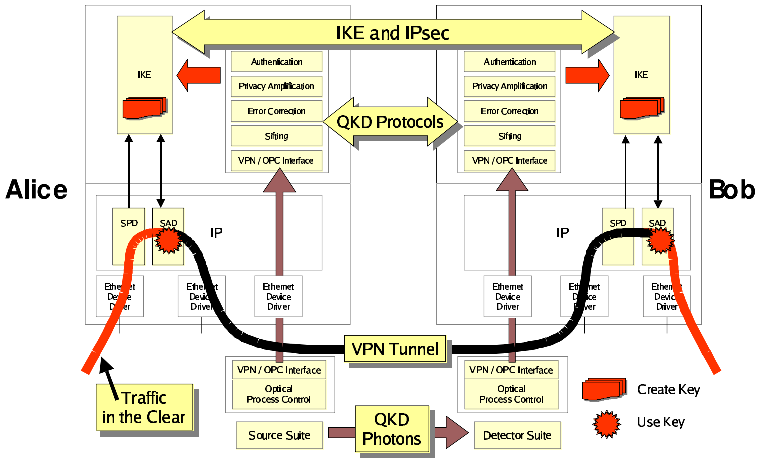
Quantum Key Distribution

- Bennett & Brassard, BB84 protocol
- Key distribution only, not data encryption
- Requires authenticated (not encrypted) classical channel to complete protocol
- Many, many places working on this!
  - BBN, Harvard, Boston U. for DARPA
  - MagiQ Technologies
  - CERN
  - 東大

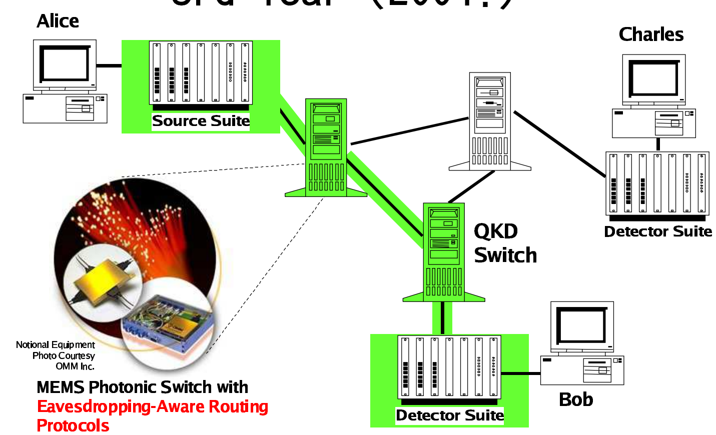
QKD Basic Idea (Oversimplified)



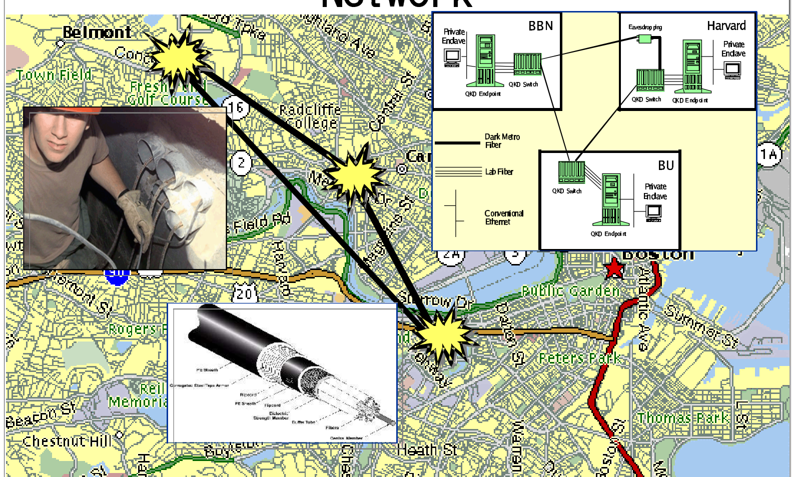
Putting It All Together



The DARPA Quantum Network – 3rd Year (2004?)



Building the DARPA Quantum Network



Teleportation

- 奇妙なことですが...
- 計算する前に、entangled pairをshareする
  - 一つを持って、一つを相手に送る
- 計算して（結果はAとよぶ）、持っているqubitにentangleして、測定して、古典的な結果を相手に送る
- 相手はその結果を使って、少し量子計算して、Aが出て来る。

アウトライン

- 量子計算とは?
- 量子計算の基本
- 量子計算のアルゴリズム
- 具体的な実験
- 量子ネットワーク
- 量子コンピューターシステム研究（私の研究を含めて）

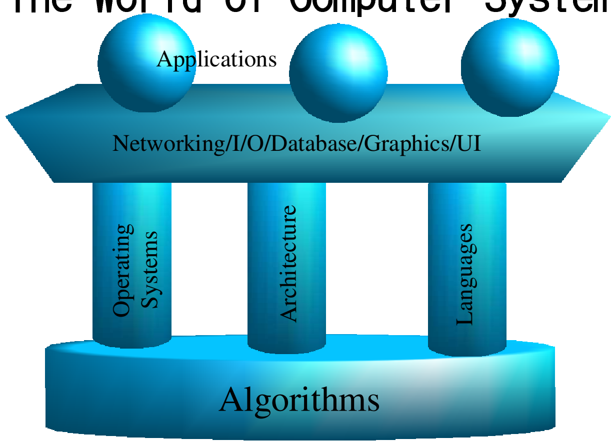
Quantum Computing Systems Research

- 本当の量子コンピュータを作る為に、研究すべきことがまだまだ沢山ある
- Berkeley, Oxford, NIST, MIT で研究されているが、研究所の数は少ない

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?

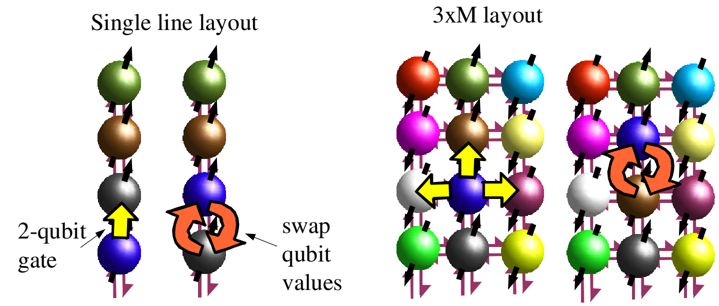
The World of Computer Systems



Systems Areas

- Logic/Analog
- Microarchitecture
- System Architecture
- Operating Systems
- Compilers/Languages
- Networking & I/O

Layout/Algorithm Efficiency



Neighbor only operations require swapping qubits

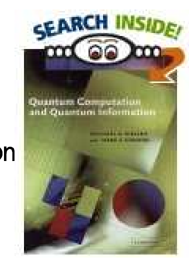
3xM layout roughly twice as efficient
3 new neighbors after each swap
= 2/3 reduction in swaps

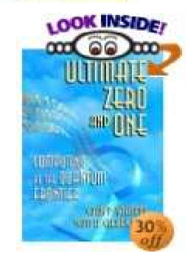
Wrap-Up

- Qubits: superposition, entanglement, and phase interference give great power
- Algorithms:
  - search (O(sqrt(N))
  - Factoring (O(L^3))
- Experiments: many kinds under way
- Networking: many experimental quantum key distribution (QKD) systems being built
- Systems: just beginning

References

- Nielsen & Chuang, Quantum Computation and Quantum Information (esp. Chapter 1)
- 林正人,
- Williams, Ultimate Zero and One
- 上坂、量子コンピュータの基礎数理





関東の研究所

- 慶應：
  - 伊藤：http://www.appi.keio.ac.jp/Itoh_group/
  - 江藤：http://www.phys.keio.ac.jp/staff/eto/eto-jp.html
- 東大：
  - ERATO 今井プロジェクト: http://www.qci.jst.go.jp/
  - 村尾： http://eve.phys.s.u-tokyo.ac.jp/indexj.htm
- RIKEN
- NEC/Tsukuba
- NTT/Atsugi (全ては50人!):
  - http://www.brl.ntt.co.jp/J/organization/psrl/psrl.html
  - http://www.brl.ntt.co.jp/cs/ninri-g/paradigm/index-j.html
- NII 国立情報科学研究所: 根本、松本

Tomorrow & Beyond

- Begin filling in details
- Algorithms (factoring, search)
- Technologies (ion traps and more)
- Architecture (how do you turn a technology into a system?)
- Networking (quantum key distribution, teleportation)