

# Introduction to Quantum Computing 量子計算入門

Rod Van Meter  
rdv@tera.ics.keio.ac.jp  
September 28–30, 2004  
@Aizu U.

with help from  
伊藤公平  
阿部英介



and slides from many others

## Course Outline

- Lecture 1: Introduction
- Lecture 2: Quantum Algorithms
- Lecture 3: Quantum Computational Complexity Theory
- Lecture 4: Devices and Technologies
- Lecture 5: Quantum Computer Architecture
- Lecture 6: Quantum Networking
- **Lecture 7: Wrapup**

## 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。

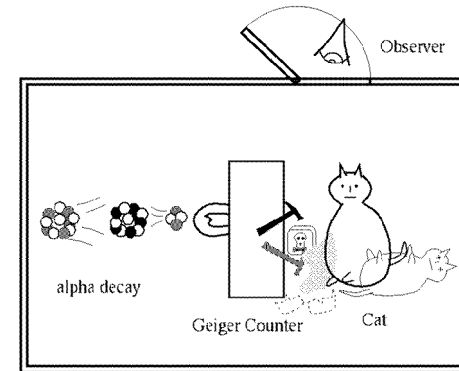
## 量子計算は何に使えるか?

- 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

## Superposition (重ね合わせ) and ket Notation

- Qubit state is a vector
- $|0\rangle$  means the vector for 0;  
 $|1\rangle$  means the vector for 1;  
 $|00\rangle$  means two bits, both 0;  
 $|010\rangle$  is three bits, middle one is 1;  
 etc.
- A qubit may be partially both!

## Schroedinger's Cat



## 1-qubitの状態とBloch球 (Phase)

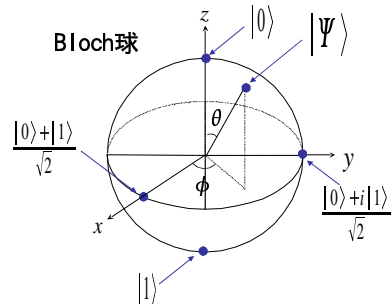
1-qubitの状態の標準基底

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

任意の重ね合わせ状態

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

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



$$\frac{|0\rangle + i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$$

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

## Entanglementとは? 絡み付き

- 二つのqubitのvalue (0, 1)は相手次第である

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} |00\rangle + 0 |01\rangle + 0 |10\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

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

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

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

## Collapsing the Superposition


$$\frac{1}{4}(|0\rangle+|4\rangle+|8\rangle+|12\rangle)|3\rangle +$$

$$\frac{1}{4}(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle)|1\rangle +$$

$$\frac{1}{4}(|0\rangle-|4\rangle+|8\rangle-|12\rangle)|7\rangle +$$


$$\frac{1}{4}(|0\rangle-i|4\rangle+|8\rangle+i|12\rangle)|0\rangle$$

Measure 2<sup>nd</sup> register,  
get e.g. 1



$$\frac{1}{2}(|0\rangle+i|4\rangle-|8\rangle-i|12\rangle)|1\rangle$$

Measure 1<sup>st</sup> register, get e.g. 4



$$|4\rangle|1\rangle$$

Measurements of *part* of the system cause the system to move to a state where the unmeasured parts of the system are consistent with the original superposition.

## 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

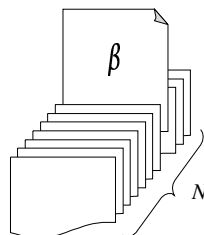
## Groverの検索アルゴリズム

$N = 2^n$  個のfileの中から、所望のfile “ $\beta$ ” 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



Hard task!!



$N \approx 2^n$  個のfile

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

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

## 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、 $O(L^3)$

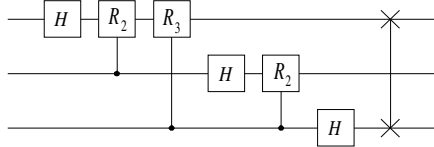
一番有名な量子計算のアルゴリズム

# 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<sub>8</sub>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<sub>8</sub>の行列表示

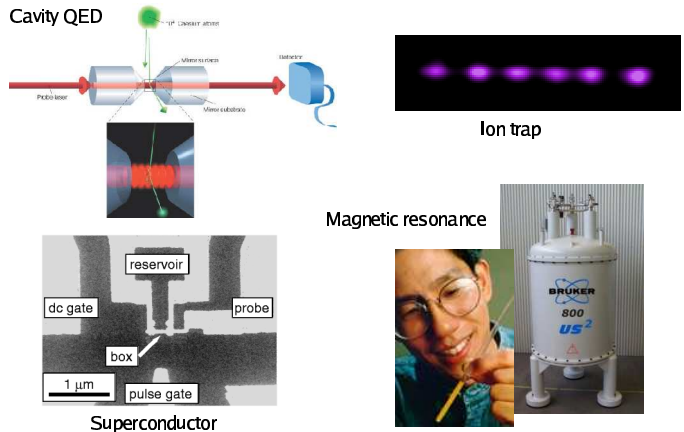
$$QFT_8 = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2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

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

# Algorithms

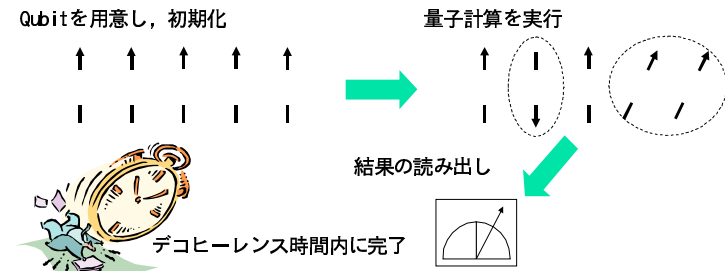
- Usually, run on superposition of all possible inputs
- Depend on analog/complex nature of phase
- Goal is to create interference (干渉) that pushes state toward the result we want

# Physical Realization



# 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



## Two-qubit operation for charge qubit

Two-qubit device  
(preliminary)

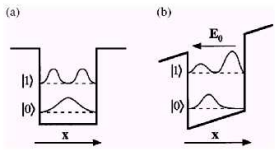
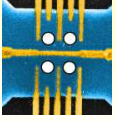


FIG. 1. Charge density in the quantum well in the direction  $x$  of the applied field. A dipole moment is induced when the electric field is turned on (b), but is zero without the electric field (a).

A. Barenco, D. Deutsch, A. Ekert, and R. Jozsa,  
Phys. Rev. Lett. 74, 4083 (1995).

c.f. Two-qubit CNOT gate in superconducting charge qubit.  
T. Yamamoto, Nature 425, 941 (2003).

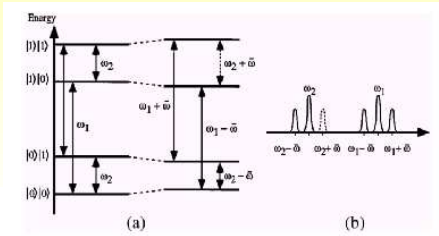


FIG. 2. (a) Energy levels of two quantum dots without and with the coupling induced by the presence of a static electric field  $E_0$ . (b) Resonance spectrum of the two quantum dots. The dotted line shows the wavelength for which the two dots act as a controlled-NOT gate, with the first dot being the control qubit and the second the target qubit.

## Scalable Ion Trap QC: Architecture?

- Scaling: microtraps



(Wineland/NIST)

- Large-scale QC?

- Teleportation can be used for wiring & code conversion
- Gate errors  $\sim O(10^{-4})$  possible

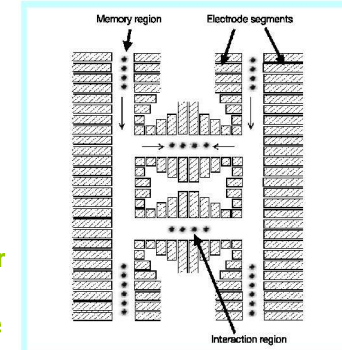


Figure 1 Diagram of the quantum charge-coupled device (QCCD). Ions are stored in the memory region and moved to the interaction region for logic operations. Thin arrows show transport and confinement along the local trap axis.

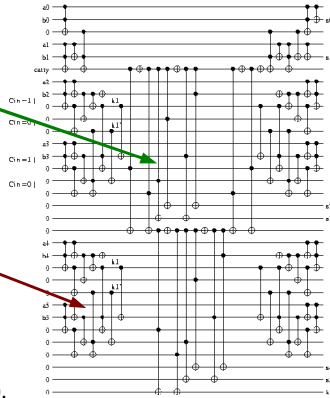
Kielipinski et al, Nature v417, p 709, 2002

## 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.)

## 量子ネットワーク

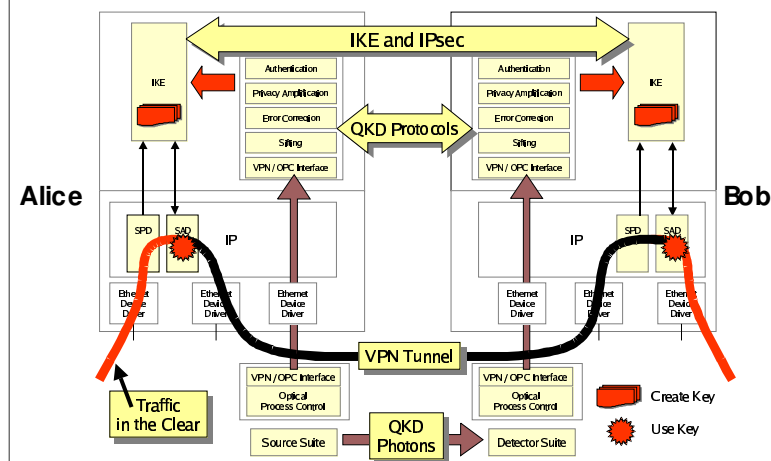
- Quantum Key Distribution (QKD)
- Teleportation
- (Superdense coding)
- All discovered by Charles Bennett (IBM) & associates



## 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

## Putting It All Together



## Teleportation

- 奇妙なことです...
- 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。

## Wrap-Up

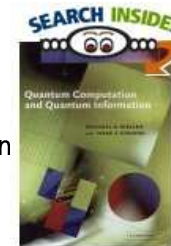
- Qubits: superposition, entanglement, and phase interference give great power
- Algorithms:
  - search ( $O(\sqrt{N})$ )
  - Factoring ( $O(L^3)$ )
- Experiments: many kinds under way
- Networking: many experimental quantum key distribution (QKD) systems being built
- Systems: just beginning

## Timeline

- Maybe 5 years to realistic multi-qubit systems (8-10 qubits?) on practical technology?
- Then start our own Moore's Law doubling?
  - Error correction and architecture begin to really "kick in"
  - Interesting machines in a decade, commercially viable ones will take longer
- Much work on every front to do!

## References

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



## Web Sites, Groups, Events

- 東大 ERATO project (今井先生)
- MIT Center for Bits and Atoms
- Caltech Institute for Quantum Information
- Oxford: <http://www.qubit.org>
- Stanford: Y. Yamamoto group
- Australia
- Okinawa summer school 2006?

## 関東の研究所

- 慶應：
  - 伊藤: [http://www.appi.keio.ac.jp/lttoh\\_group/](http://www.appi.keio.ac.jp/lttoh_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.br1.ntt.co.jp/J/organization/psr1/psr1.html>
  - <http://www.br1.ntt.co.jp/cs/ninri-g/paradigm/index-j.html>
- NII 国立情報科学研究所: 根本、松本

## Thank You for Material

- E. Abe, Keio
- K. Itoh, Keio
- R. Moore, SDSC
- T. Fujisawa, NTT
- (T. Metodiev, UC Davis)
- (BBN)
- NIST
- Oxford
- Honda
- JPL
- U. Arizona
- various publications