



An Introduction to Quantum Computing

Edward Gerjuoy

University of Pittsburgh

What is a quantum computer?

- “While today’s digital computers process classical information encoded in bits, a quantum computer processes information encoded in quantum bits or qubits.”

-NSF Workshop Report NSF-00-101 (Oct. 28-29, 1999)

- What is a bit?
- $0 = \uparrow, 1 = \downarrow$
- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Normalized: $|\alpha|^2 + |\beta|^2 = 1$

Possible Realizations of Qubits

- Trapped ions in potential wells
- Trapped neutral atoms with electric dipole moments
- “Photons” interacting with single atom or ion in a resonant cavity
- Photons, either freely moving or bouncing between two resonant cavities
- Quantum dots containing a trapped electron
- Quantum dots which can contain an exciton
- Superconducting circuit at milli-Kelvin temperature
- Exotic qubits of various kinds, e.g. employing nonabelian fractional quantum Hall effect anyons

“A Quantum Information Science and Technology Roadmap Part 1: Quantum Computation,”
U.S. Army Advanced Research and Development Activity (ARDA) Report (April 2, 2004).

[*NMR, an aside*]

- Nuclear Magnetic Resonance: Each molecule can be a multi-qubit quantum computer
- Unlikely to succeed for non-trivial calculations
- See sources for more information

What's the minimum necessary?

- Must be able to:
 - Conveniently measure the state of a qubit
 - Conveniently express the wavefunction in terms of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
 - Be able to put the qubit in a desired state

Transitions

${}^9\text{Be}^+$ QUBITS:

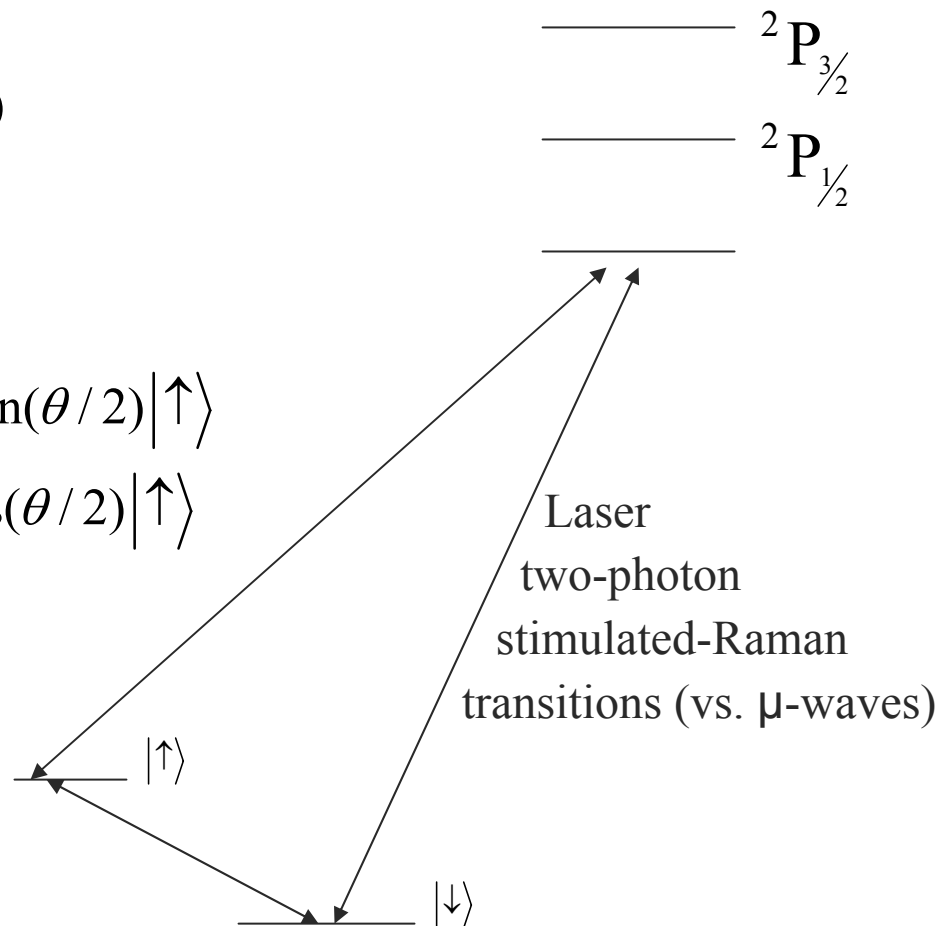
(${}^2\text{S}_{1/2}$ electronic ground state)

$$|\downarrow\rangle \equiv |F = 2, m_F = -2\rangle$$

$$|\uparrow\rangle \equiv |F = 1, m_F = -1\rangle$$

$$|\downarrow\rangle \rightarrow \cos(\theta/2)|\downarrow\rangle + -ie^{-i\phi} \sin(\theta/2)|\uparrow\rangle$$

$$|\uparrow\rangle \rightarrow -ie^{i\phi} \sin(\theta/2)|\downarrow\rangle + \cos(\theta/2)|\uparrow\rangle$$



[*Entanglement*]

- “Entanglement is *the* feature of the quantum world that distinguishes it from the classical world, saying that for a single pair of systems, a description of each system’s state is not sufficient to describe the entire state of the system...It is also the feature of quantum systems that makes exponential speedup of computations possible.”

Entanglement

$$\begin{aligned} \blacksquare \quad |\psi\rangle_{AB} &= \sum_{i=0}^1 \sum_{j=0}^1 c_{ij} |i\rangle_A |j\rangle_B = c_{00} |0\rangle_A |0\rangle_B + c_{01} |0\rangle_A |1\rangle_B \\ &\quad + c_{10} |1\rangle_A |0\rangle_B + c_{11} |1\rangle_A |1\rangle_B \end{aligned}$$

$$\blacksquare \quad \sum_{i,j} |c_{ij}|^2 = 1$$

■ If: $|\psi\rangle_{AB} = |u\rangle_A |v\rangle_B$, then unentangled. Otherwise, entangled.

Entanglement: Examples

■ Unentangled:

$$|\psi_\alpha\rangle_{AB} = |0\rangle_A |1\rangle_B; \quad i|\psi_\beta\rangle_{AB} = \left[\frac{1}{\sqrt{3}}|0\rangle_A + \sqrt{\frac{2}{3}}|1\rangle_A \right] \left[\frac{1}{2}|0\rangle_B - i\sqrt{\frac{3}{4}}|1\rangle_B \right]$$

■ Entangled:

$$|\psi_\gamma\rangle_{AB} = \frac{1}{\sqrt{2}} \left[|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B \right]$$

$$|\psi_\delta\rangle_{AB} = \frac{1}{\sqrt{5}} \left[|0\rangle_A |0\rangle_B + 2|0\rangle_A |1\rangle_B - 2|1\rangle_A |0\rangle_B \right]$$

Entanglement: Examples

- ?? $|\psi_t\rangle = \frac{1}{12} \left[-2|0\rangle_A |0\rangle_B - 5\sqrt{3}|1\rangle_A |1\rangle_B + \sqrt{5}|0\rangle_A |1\rangle_B + 2\sqrt{15}|1\rangle_A |0\rangle_B \right]$

- ?? $|\psi_\mu\rangle = \frac{1}{12} \left[2|0\rangle_A |0\rangle_B - 5\sqrt{3}|1\rangle_A |1\rangle_B + \sqrt{5}|0\rangle_A |1\rangle_B + 2\sqrt{15}|1\rangle_A |0\rangle_B \right]$

- Does $\begin{vmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{vmatrix} = 0$?

- If $|\psi\rangle_{AB\dots} = |u\rangle_A |v\rangle_B |w\rangle_C \dots$, unentangled.

Entanglement: Examples

- Unentangled:

$$|\psi_\alpha\rangle_{AB} = |0\rangle_A |1\rangle_B \quad i|\psi_\beta\rangle_{AB} = \left[\frac{1}{\sqrt{3}}|0\rangle_A + \sqrt{\frac{2}{3}}|1\rangle_A \right] \left[\frac{1}{2}|0\rangle_B - i\sqrt{\frac{3}{4}}|1\rangle_B \right]$$

- Entangled:

$$|\psi_\gamma\rangle_{AB} = \frac{1}{\sqrt{2}} \left[|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B \right]$$

- No-cloning theorem

Wootters and Zurek, Nature **299**, 802 (1982).

[

What is a quantum computer?

]

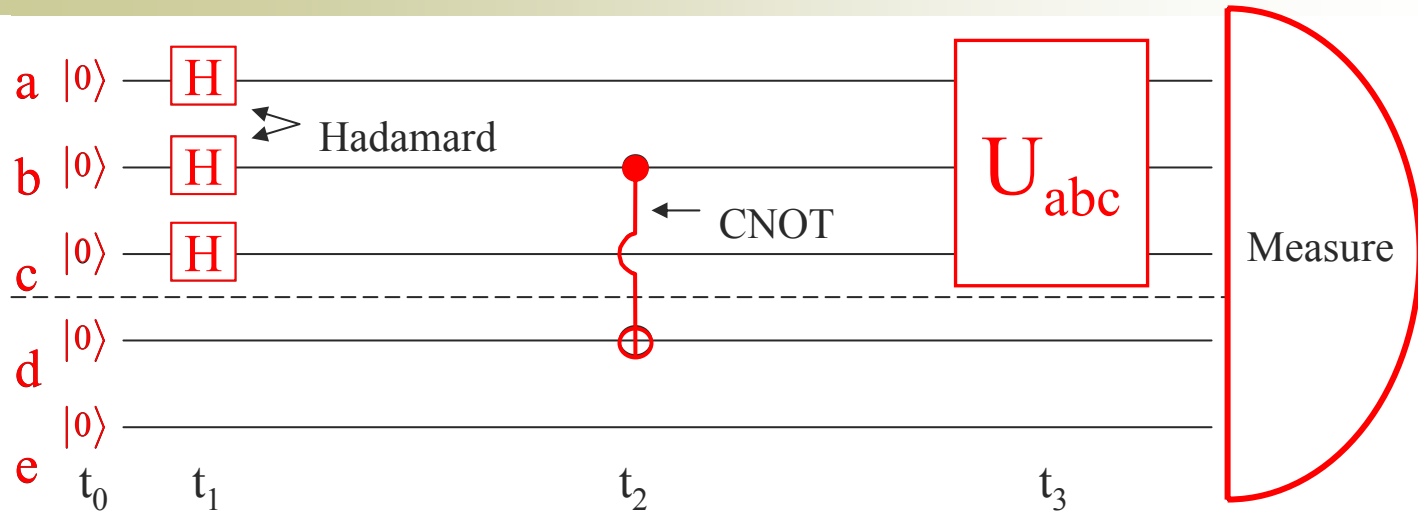
Permitted Quantum Computer Operations

- $i\hbar \psi = H\psi$ Let $\psi_i \equiv \psi(t = 0)$; $\psi_f \equiv \psi(t)$
- $\psi_f = e^{\frac{-iHt}{\hbar}} \psi_i \equiv U_1 \psi_i$, H is time-independent
- $\psi_f =$ time-ordered $e^{\frac{-i}{\hbar} \int_0^t H(t) dt} \psi_i \equiv U_2 \psi_i$,
 H time dependent
- In either case, whether U_1 or U_2 , U is unitary,
 $UU^t = U^tU = 1$

Definition of Quantum Computation

- Any particular quantum computation involves finding a sequence of unitary operations that will transform some chosen initial computer wave function into a final wave function wherein there is a non-negligible probability of measuring those combinations of qubit states that can be interpreted as yielding the outcome of the computation.

Circuit Model of Quantum Computation



$$t_0 : |\psi_0\rangle = |0\rangle_a |0\rangle_b |0\rangle_c |0\rangle_d |0\rangle_e \equiv [00000]_{abcde}$$

$$t_1 : |\psi_1\rangle = \frac{1}{2\sqrt{2}} [|0\rangle_a + |1\rangle_a] [|0\rangle_b + |1\rangle_b] [|0\rangle_c + |1\rangle_c] |0\rangle_d |0\rangle_e$$

$$= \frac{1}{2\sqrt{2}} \begin{bmatrix} 000 + 001 + 010 + 011 \\ +100 + 101 + 110 + 111 \end{bmatrix}_{abc} |0\rangle_d |0\rangle_e$$

$$t_2 : |\psi_2\rangle = \frac{1}{2\sqrt{2}} \begin{bmatrix} 0000 + 0010 + 0101 + 0111 \\ +1000 + 1010 + 1101 + 1111 \end{bmatrix}_{abcd} |0\rangle_e$$

$$t_3 : |\psi_3\rangle = U_{abc} |\psi_2\rangle$$

$$H|0\rangle = \frac{1}{\sqrt{2}} [|0\rangle + |1\rangle]$$

$$\text{CNOT}|00\rangle_{bd} = |00\rangle_{bd}$$

$$\text{CNOT}|01\rangle_{bd} = |01\rangle_{bd}$$

$$\text{CNOT}|10\rangle_{bd} = |10\rangle_{bd}$$

$$\text{CNOT}|11\rangle_{bd} = |11\rangle_{bd}$$

1-Qubit and 2-Qubit Gates

- Any unitary operator which is greater than 4×4 can be reduced to a succession of 2-qubit and 1-qubit operations.
- Not all 4×4 matrices are needed. There are so called universal gates. CNOT is one of them.
 - Any greater than 2×2 unitary operator can be reduced to the product of one qubit gates and CNOT gates.

What is Shor's Algorithm?

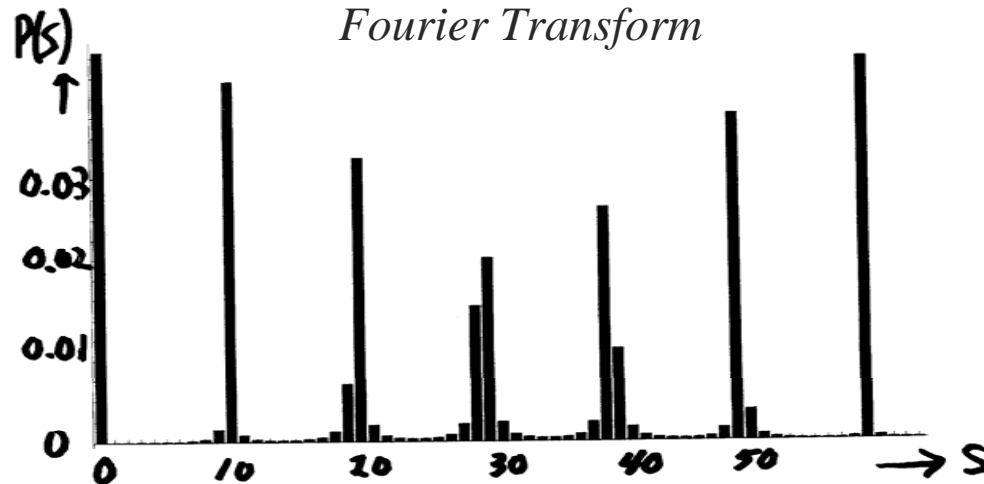
- Let $N=pq$, where p and q denote different odd primes. Then Shor's algorithm enables a quantum computer to find the prime factors p and q of N .
- Moreover, for very large N , the quantum computer using Shor's algorithm will factor N with less computational effort than a classical computer.
- However, the meaning of the phrase, "less computational effort" must be carefully defined.
- P.W. Shor, SIAM J. Comp. **26**, 1484 (1997).

"Progress in Quantum Algorithms" (Sept. 14, 2005). <http://www-math.mit.edu/~shor/>

E. Gerjuoy, "Shor's factoring algorithm...", Am. J. Phys. **73** (2005), p. 521.

Shor's Algorithm

Probability the first register will be in the state, S , after the Quantum Fourier Transform



- In this simulation, the first register is composed of 8 qubits, which can represent 256 different binary numbers S , with each S corresponding to a different state of the first register.
- The period $r = 26$. The probability $P(S)$ is plotted for $S = 0$ to about 60.
- The probabilities for larger S manifest similar peaks. Each peak occurs at the values of S which most nearly satisfies $S/256 = d/r$, where d is an integer $< r$.

Factoring $N=pq$ with a classical computer

- Crudest Attempt: Divide N by the sequence of integers 2, 3, 4, ..., up to \sqrt{N} . This must find one of the prime factors of N .
- Suppose N is a number of order 10^{100} , and that the average time to perform one of these divisions is 10^{-12} sec. Then the total time to find a factor of N will be $\sim 10^{-12} \times 10^{50} = 10^{38}$ sec.
- The age of the universe is only 12 billion years = 3.8×10^{17} sec.

Modern Developments

■ Other Models

- Measurement model, cluster model, graph state
- Adiabatic quantum computing
- Topological computer

[*Closing*]

- Counter-factual quantum computation

“The logic underlying the coherent nature of quantum information processing often deviates from intuitive reasoning, leading to surprising effects. Counterfactual computation constitutes a striking example: the potential outcome of a quantum computation can be inferred, even if the computer is not run...Here we demonstrate counterfactual computation, implementing Grover’s search algorithm with an all-optical approach.”

O. Hosten et al., *Nature*, **439**, 949 (2006). On counterfactual computation. See also J. Dowling, *Nature*, **439**, 919 (2006) and L. Vaidman, *Phys. Rev. Lett.* **98**, 160403 (4/25/07).