

DAC 2003: Session 51.1

Tutorial: Basic Concepts in Quantum Circuits

John P. Hayes

Advanced Computer Architecture Laboratory
EECS Department
University of Michigan,
Ann Arbor, MI 48109, USA





Outline

- Motivation
- · Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- Physical Implementation





- Motivation
- · Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- Physical Implementation





Computational Limits

- Some important computational problems seem to be permanently intractable
 - > Their complexity grows exponentially with problem size, e.g. factoring large numbers—the basis for "unbreakable" Internet codes
- Performance improvements in "classical" computer circuits may be approaching a limit
 - > This is described by Moore's Law



Computational Limits

 Question: Is there a faster and more compact way to compute?

• Answer: Yes!

Quantum mechanics can form the basis for an entirely new type of computation—

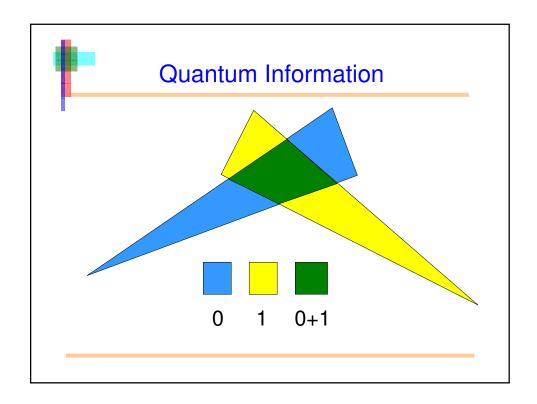
quantum computing — It some huge practical implementation problems can be solved



Quantum Information

- A classical logic state can be 0 or 1, but not both
- A quantum state can be 0 and 1 at the same time!
- More precisely, a quantum state is a superposition of the zero and one states called a $\frac{\text{qubit}}{c_0|0\rangle + c_1|1\rangle}$

The coefficients c_0 and c_1 are complex numbers called (probability) amplitudes





Quantum Information

The Good News

> N qubits can store 2^N binary numbers simultaneously, suggesting massive parallelism

$$N$$
 = 2: $|\Psi\rangle=c_0|00\rangle+c_1|01\rangle+c_2|10\rangle+c_3|11\rangle$ or, in general,

$$|\Psi\rangle = \sum_{i=0}^{2^{n}-1} c_{i} |b_{i,n-1}b_{i,n-2}...b_{i,0}\rangle$$

 Quantum states have wavelike properties that allow powerful nonclassical operations (interference, entanglement)



Quantum Information

The Good News

> N qubits can store 2^N binary numbers simultaneously, suggesting massive parallelism

$$N=2$$
: $|\Psi\rangle=c_0|00\rangle+c_1|01\rangle+c_2|10\rangle+c_3|11\rangle$ or, in general,

$$|\Psi\rangle = \sum_{i=0}^{2^{n}-1} c_{i} |b_{i,n-1}b_{i,n-2}...b_{i,0}\rangle$$

> Quantum states have wavelike properties that allow powerful nonclassical operations (interference, entanglement)



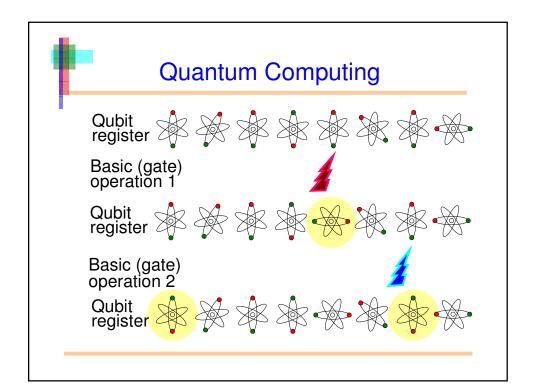
Quantum Information

The Bad News

- > Measurement yields just one of the 2^N superimposed numbers $|b_{i,n-1} b_{i,n-2}...b_{i,0}\rangle$ and destroys the superposition
- > Quantum states are very fragile due to
 - Tiny (nano) scale and low energy levels
 - Interaction with the environment (decoherence)

Implications

- > Physical quantum circuits are extremely hard to build
- > Fault-tolerant design is believed to be essential





A Little History

- 1982: Richard Feynman suggested quantum mechanics could provide an exponential speed-up in simulation
- 1985: David Deutsch described a simple algorithm exhibiting quantum parallelism
- 1994: Peter Shor showed how to factor integers into primes in polynomial time using quantum methods, thus "breaking" RSA encryption
- 1996-now: First quantum computing devices built at LANL, Oxford, etc. employing a few (≤ 10) qubits



- Motivation
- Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- The Future





Classical Logic Circuits

- Behavior is governed implicitly by classical physics: no restrictions on copying or measuring signals
- Signal states are simple bit vectors, e.g. X = 01010111
- Signal operations are defined by Boolean algebra
- Small well-defined sets of universal gate types exist, e.g. {NAND}, {AND, OR, NOT}
- Circuits use fast, scalable and macroscopic technologies such as transistor-based CMOS integrated circuits



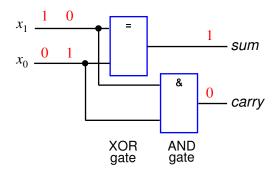
Quantum Circuits

- Behavior is governed by quantum mechanics
- Signal states are qubit vectors
- Operations are defined by linear algebra over Hilbert space and represented by unitary matrices
 - > Gates and circuits must be reversible (information-lossless)
 - > Number of output lines = Number of input lines
 - > States cannot be copied so fan-out ("cloning") is not allowed
- Many universal gate sets and physical implementation technologies exist (the best ones are not obvious)



Classical vs. Quantum Circuits

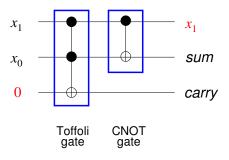
- Example: Classical Half Adder
 - > Compute the sum and carry for two bits x_1, x_0





Classical vs. Quantum Circuits

- Example: Quantum Half Adder
 - > Compute the sum and carry for two qubits x_1, x_0





Outline

- Motivation
- Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- Physical Implementation





Quantum Gates

- One-Input gate: NOT
 - > Input state: $c_0|0\rangle + c_1|1\rangle$
 - > Output state: $c_1|0\rangle + c_0|1\rangle$
 - > Graphic symbol:



> Basic states $|0\rangle$ and $|1\rangle$ are mapped thus:

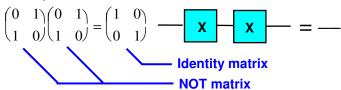
$$|0\rangle \rightarrow |1\rangle$$

$$|1\rangle \rightarrow |0\rangle$$



Quantum Gates

- NOT gate (contd.)
 - > Vector notation for states: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
 - > Matrix notation for gate operation: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
 - > Gate connection corresponds to matrix multiplication:





Quantum Gates

Hadamard Gate

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad - \boxed{\mathbf{H}}$$

> Maps $|0\rangle \rightarrow 1/\sqrt{2} |0\rangle + 1/\sqrt{2} |1\rangle$ and $|1\rangle \rightarrow 1/\sqrt{2} |0\rangle - 1/\sqrt{2} |1\rangle$ so it "randomizes" the basic states

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



Quantum Gates

Phase-Shift Gate

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$



- > Maps $|0\rangle \to |0\rangle$ and $|1\rangle \to e^{i\phi}|1\rangle$ so it "twists" the 1 state by an angle ϕ
- > If = π , it maps $|1\rangle \rightarrow -|1\rangle$
- > Note that the entries of a gate matrix can be complex numbers



Quantum Gates

Two-Input Gate: Controlled NOT (CNOT)

> CNOT maps

$$|x\rangle|0\rangle \to |x\rangle||x\rangle$$

and

$$|x\rangle|1\rangle \rightarrow |x\rangle||\mathsf{NOT}(x)\rangle$$



Quantum Gates

"Standard" Universal Gate Set



- Motivation
- Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- Physical Implementation





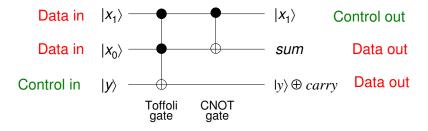
Quantum Circuits

- A quantum "circuit" is a sequence of quantum "gates"
- The signals (qubits) may be static while the gates are dynamic
- The circuit has fixed "width" corresponding to the number of qubits being processed
- Logic design (classical and quantum) attempts to find circuit structures for needed operations that are
 - > Functionally correct
 - > Independent of physical technology
 - > Low-cost, e.g. uses the minimum number of qubits or gates



Quantum Circuits

- Example 1: Quantum Half Adder
 - > Compute the sum and carry for two qubits x_1, x_0

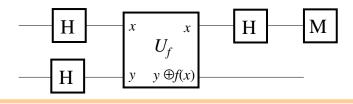




Quantum Circuits

Example 2: Implementing Deutsch's Algorithm

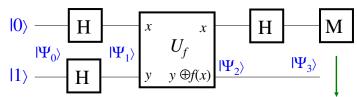
- Problem: Determine whether a one-variable Boolean function f(x) is constant, i.e. f(0) = f(1), or balanced, i.e. f(0) ≠ f(1).
- Classical algorithms require two evaluations of f.
- This algorithm uses just one quantum evaluation by, in effect, computing f(0) and f(1)simultaneously
- Circuit:





Quantum Circuits

• Deutsch's Algorithm (contd.)

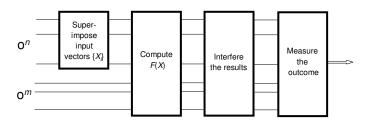


- Initialize with $|\Psi_0\rangle = |01\rangle$
- $|0\rangle$ = constant; $|1\rangle$ = balanced
- Create superposition of x states using the first Hadamard (H) gate. Set y control input using the second H gate
- Compute f(x) using the special unitary circuit U_f
- Interfere the $|\Psi_2\rangle$ states using the third H gate
- Measure the x qubit



Quantum Computation

Generic Structure to Compute F(X)





- Motivation
- Quantum vs. Classical
- Quantum Gates
- Quantum Circuits
- Physical Implementation





Physical Implementation

Main Contenders

- Nuclear magnetic resonance (NMR)
- lon traps
- Semiconductor quantum dots
- Optical lattices etc.

Main Deficiency

Poor scalability

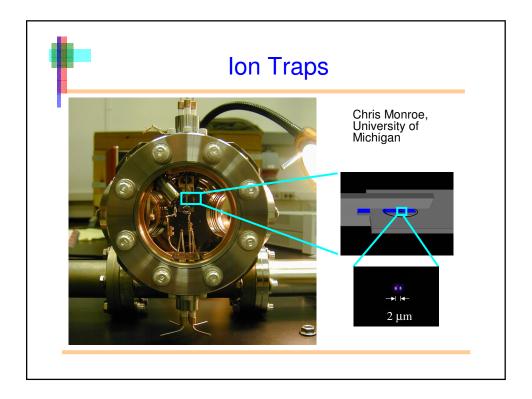


Ion Traps

 String of charged particles is trapped by a combination of static and oscillating electric fields in a high-vacuum device



- Each ion has two long-lived electrical states representing |0> and |1>
- The individual ions can be addressed by laser beams
- Means exist for initializing (optical pumping and laser cooling) and measuring the quantum state





Summary: State of the Art

- Quantum circuits can solve some important problems with exponentially fewer operations than classical algorithms
- Small quantum circuits have been demonstrated in the lab using various physical technologies
- Quantum cryptography has been demonstrated over long distances
- Current technologies are fragile, and appear to be limited to tens of qubits and hundreds of gates
- Big gaps remain in our understanding of quantum circuit and algorithm design, as well as the necessary implementation techniques