

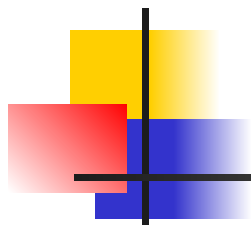


Quantum Computation and Information

Chap 1 Intro and Overview: p 1-28

Dr. Charles Tappert

The information presented here, although greatly condensed, comes almost entirely from the course textbook: *Quantum Computation and Quantum Information* by Nielsen & Chuang



1.1 Global Perspectives

- This chapter develops in broad brushstrokes a picture of the field of quantum computation and quantum information
 - Detail comes in later chapters
- Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems



1.1.1 History

- Early 1920s – creation of the modern theory of quantum mechanics
 - Quantum mechanics is the math framework or set of rules for the construction of physical theories
 - The rules are simple but can be counterintuitive
- Early 1980s – idea of signaling faster than light hinged on cloning an unknown quantum state
 - No-cloning theorem showed this not possible



1.1.1 History (cont)

- 1970s – interest started in obtaining complete control over single quantum systems
 - Modest success to date
 - Small quantum computers capable of doing dozens of operations on a few quantum bits (or qubits)
 - Experimental prototypes were demonstrated for doing quantum cryptography, secret communication over long distances



1.1.1 History (cont)

- Modern incarnation of computer science
 - 1936 – Alan Turing’s paper on an abstract idea of a programmable computer, *Universal Turing Machine*
 - Church-Turing thesis – any algorithmic process can be simulated using a Turing machine
 - Electronic component von Neumann machines
 - 1947 – transistor invention increased development
 - Vacuum tubes, transistors, integrated circuits
 - 1960s – Moore’s law: computing power doubles every two years



1.1.1 History (cont)

■ Modern incarnation of computer science

- Efficient (polynomial time) versus inefficient (super-polynomial, usually exponential) algorithm
- Strong Church-Turing thesis: any algorithmic process can be simulated efficiently using a Turing machine
- Mid 1970s – the Solovay-Strassen randomized algorithm for testing whether an integer is prime
- Stronger Church-Turing thesis: any algorithmic process can be simulated efficiently using a probabilistic Turing machine



1.1.1 History (cont)

- In 1985, trying to further extend the Church-Turing thesis, David Deutsch tried to define a computational device capable of simulating efficiently an arbitrary physical system
 - Because the laws of physics are ultimately quantum mechanical he thought of quantum devices
 - At this time, it is not clear whether Deutsch's notion of a Universal Quantum Computer is correct
 - He did show that quantum computers might have computing powers greater than classical computers



1.1.1 History (cont)

- In 1994, Peter Shor showed that two important problems could be solved efficiently on a quantum computer
 - Finding prime factors and the 'discrete logarithm'
 - Giving further indication that quantum computers are more powerful than classical computers
- In 1995, Lov Grover found another problem that could be sped up on a quantum computer
 - Search through some unstructured search space



1.1.1 History (cont)

- At this time, mid 1990s, many came to believe Richard Feynman's 1982 idea that computers could be based on quantum mechanics
- But designing good quantum algorithms is hard
 - Human intuition is rooted in the classical world
 - To be interesting, the algorithm must be better than any existing classical algorithm



1.1.1 History (cont)

- Switching topics, in 1948 Claude Shannon created modern information theory
- Quantum information theory followed
 - In 1995, Ben Schumacher provided an analog to Shannon's noiseless coding theorem
 - Although no analog exists to Shannon's noisy channel coding theorem, we do have a class of quantum error-correcting codes (CSS codes, after the 1996 inventors Calderbank, Shor, and Steane)



1.1.1 History (cont)

- Transmitting classical information using a quantum channel
 - In 1992 Charles Bennett and Stephen Wiesner explained how to transmit two bits with one qubit
 - Called **superdense coding** (more in chapter 2)
- Networked information theory is a rich subject
 - But networked quantum information theory is in its infancy



1.1.1 History (cont)

- Networked quantum information theory

- Sending quantum information from Alice to Bob through a noisy quantum channel with zero capacity for quantum information is impossible
- However, with two copies of the channel and reversing the direction of one of the channels, non-zero transmission capacity is possible (Fig. 1.1)

1.1.1 History (cont)

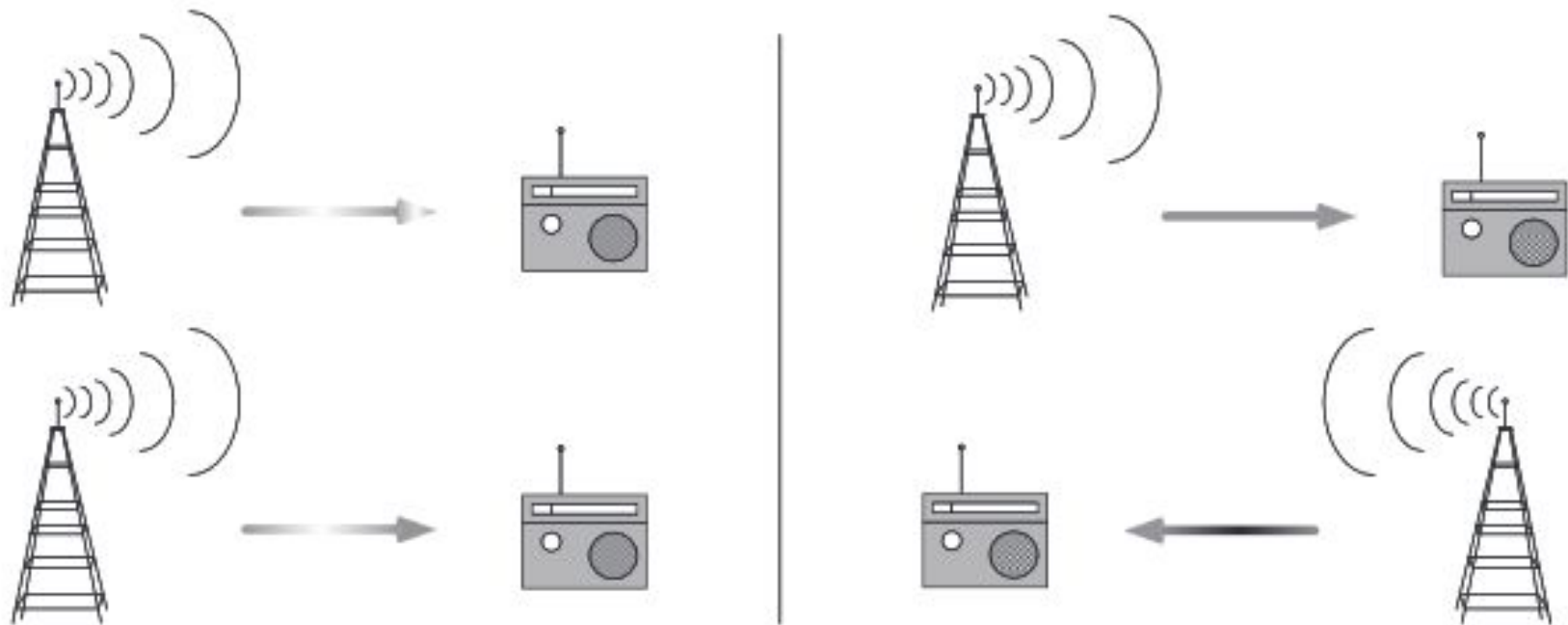


Figure 1.1. Classically, if we have two very noisy channels of zero capacity running side by side, then the combined channel has zero capacity to send information. Not surprisingly, if we reverse the direction of one of the channels, we still have zero capacity to send information. Quantum mechanically, reversing one of the zero capacity channels can actually allow us to send information!



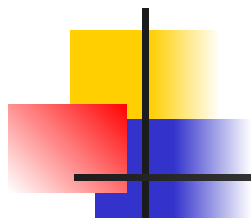
1.1.1 History (cont)

- Switching topics again, now to cryptography
 - We have public and private key cryptosystems
 - A fundamental problem with private key cryptosystems is distributing the key
 - Quantum key distribution solves this problem (1984)
 - Now used in limited-scale real-world applications
 - The problem with public key systems, like RSA, is that they depend on the difficulty of certain math problems like the factoring of large integers
 - But quantum computing may soon speed up factoring



1.1.1 History (cont)

- We have looked at the historical antecedents for quantum computation and information
- But, as the field has grown, it has sprouted its own subfields of research in the quantum arena
 - Perhaps the most striking is quantum entanglement
 - Many researchers believe that further study of quantum entanglement will lead to new applications



1.1.2 Future Directions

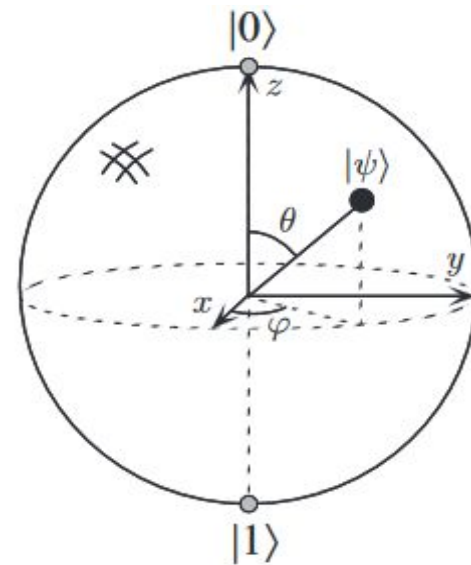
- Notions we learned may yield future results
 - Think physically about computation
 - Any physical theory, not just quantum mechanics, could be the basis for information processing and communication
 - Also, we should think computationally about physics

1.2 Quantum Bits or Qubits

■ **Qubit** = basic concept of quantum computing

- Qubits are abstract mathematical objects
- A qubit has two possible states, $|0\rangle$ and $|1\rangle$
- And superpositions $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
 - where α and β are complex numbers, and $\alpha^2 + \beta^2 = 1$
- Also $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$

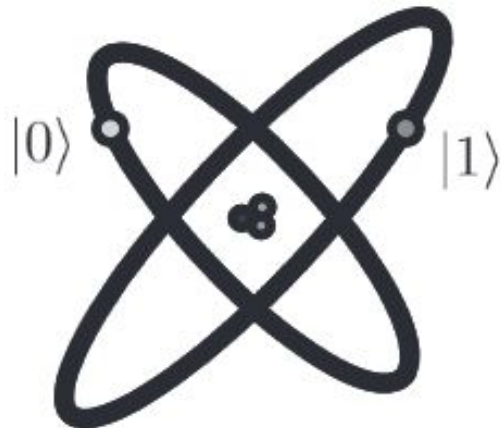
Bloch sphere
representation of a qubit
as a point on a sphere





1.2 Quantum Bits or Qubits

- Many physical systems realize qubits, and their existence and behavior validated by experiment
 - Two different polarizations of a photon
 - Nuclear spin alignment in a uniform magnetic field
 - Two states of an electron orbiting an atom



ground state $|0\rangle$ and excited state $|1\rangle$
and a 50%-50% state denoted $|+\rangle$
that is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$



1.2.1 Multiple Qubits

- A two qubit system has four **computational basis states** denoted $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- A pair of qubits can exist in superpositions of these four states with complex coefficients called **amplitudes**

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- And the possible measurement results occur with probabilities $|\alpha_x|^2$



1.2.1 Multiple Qubits

- An important two qubit state is the **Bell state** or **EPR pair** (for Einstein, Podolsky, and Rosen)

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

- Measured results are unexpectedly correlated
 - Measuring the 2nd qubit gives the same result as 1st
- These strange measurement correlations are stronger than could exist in classical systems



1.2.1 Multiple Qubits

- Consider a system of n qubits

- The computational basis states are $|x_1 x_2 \dots x_n\rangle$
- And a quantum state is specified by 2^n amplitudes
- So, for $n=500$, this number of amplitudes is larger than the number of atoms in the universe
- This enormous potential computing power is something we would like to exploit



1.3 Quantum Computation

- Classical computer built from electrical circuit
 - Containing wires and logic gates
- Quantum computer built from quantum circuit
 - Wires and quantum gates to carry around and manipulate the quantum information



1.3.1 Single Qubit Gates

- Classical computers have only one non-trivial single bit gate
 - The NOT gate
- Quantum computers can have infinitely many single qubit gates
 - Each described by a **unitary** two-by-two matrix U
 - Unitary means $U^\dagger U = I$ where U^\dagger is the *adjoint* of U obtained by transposing and then complex conjugating U

1.3.1 Important Single Qubit Gates

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

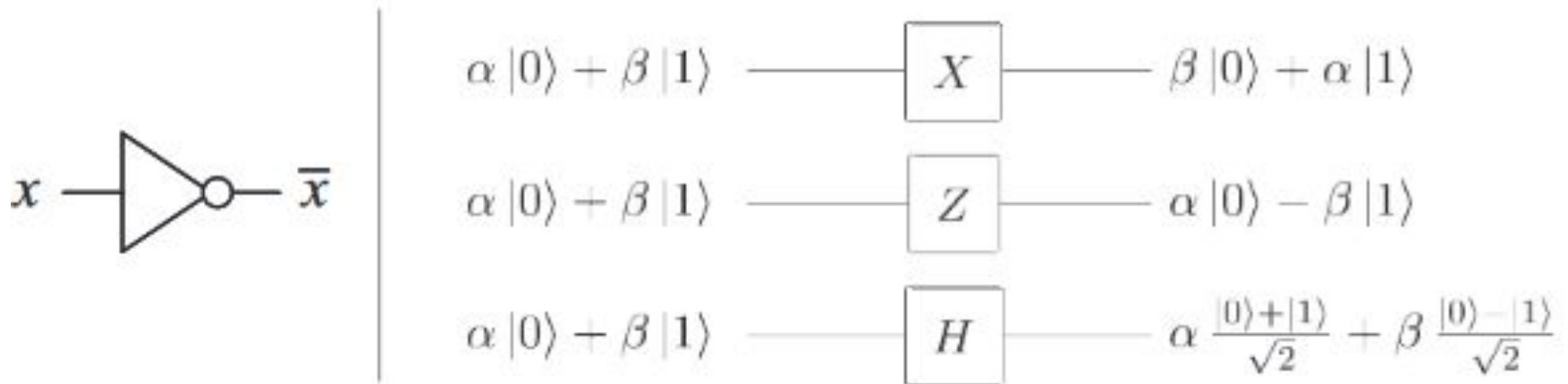
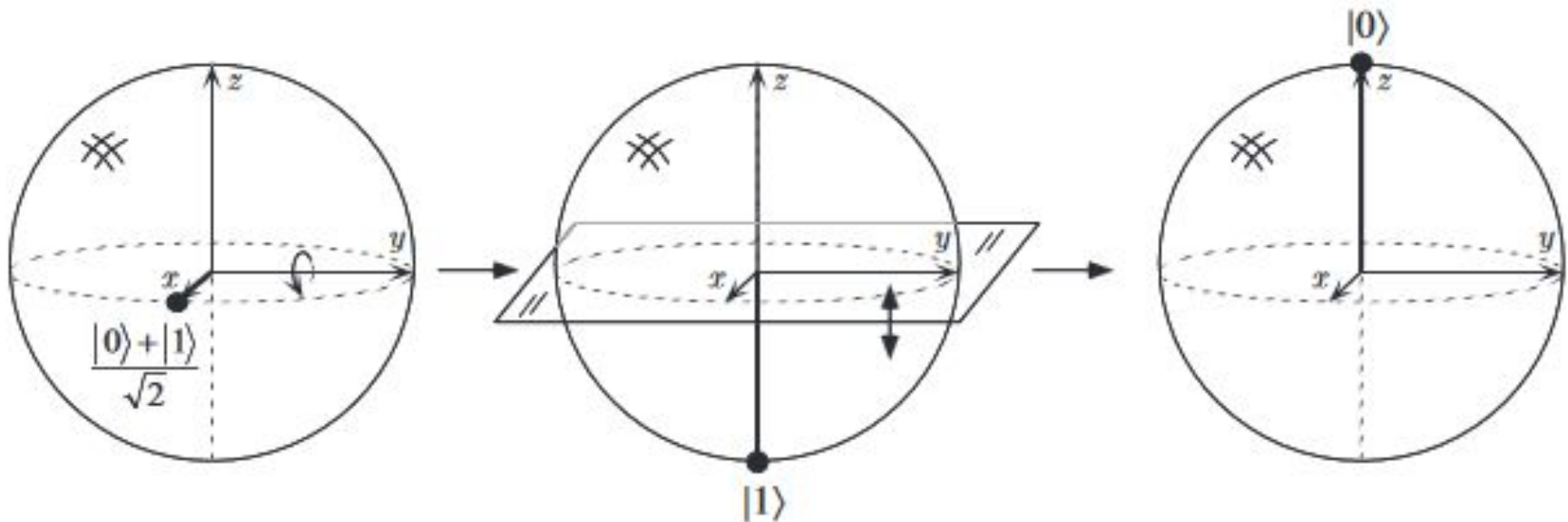


Figure 1.5. Single bit (left) and qubit (right) logic gates.

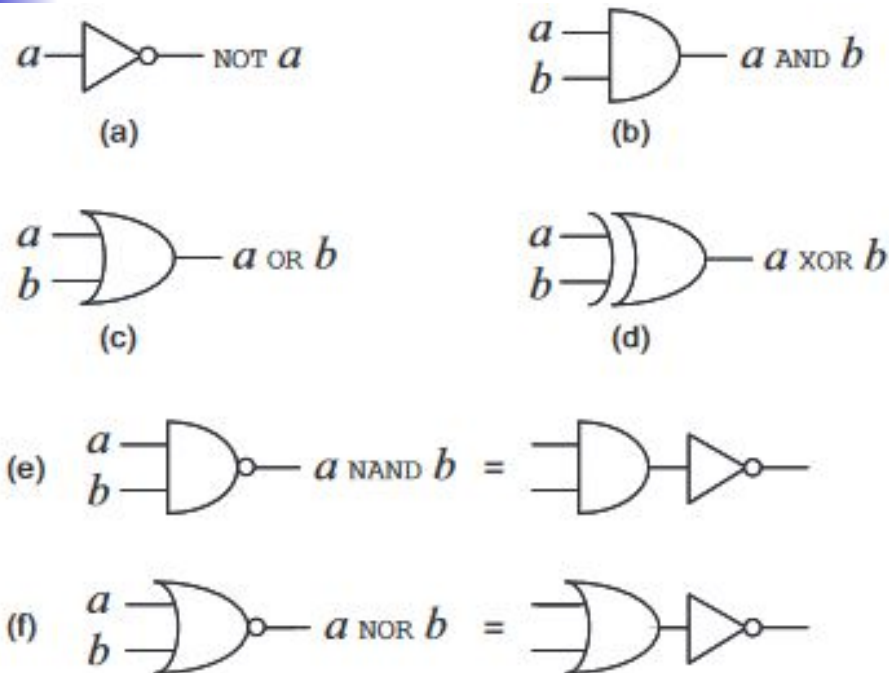
1.3.1 Hadamard (H) Single Qubit Gate

- Hadamard operation = rotation about y axis by 90° , followed by rotation about x axis by 180°

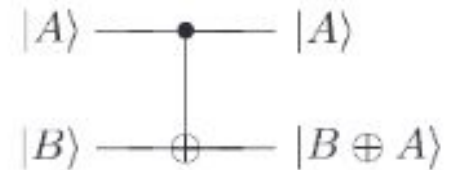


1.3.2 Multiple Qubit Gates

Classical (left), Quantum (right)



controlled-NOT



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 1.6. On the left are some standard single and multiple bit gates, while on the right is the prototypical multiple qubit gate, the controlled-NOT. The matrix representation of the controlled-NOT, U_{CN} , is written with respect to the amplitudes for $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, in that order.



1.3.2 Multiple Qubit Gates

- Prototypical quantum **controlled–NOT** gate
 - Two input qubits: control qubit and target qubit
 - If the control qubit is set to 0, target qubit is left alone
 - If the control qubit is set to 1, target qubit is flipped

$$|00\rangle \rightarrow |00\rangle; |01\rangle \rightarrow |01\rangle; |10\rangle \rightarrow |11\rangle; |11\rangle \rightarrow |10\rangle$$

$|A, B\rangle \rightarrow |A, B \oplus A\rangle$, where \oplus is addition modulo two, which is exactly what the **XOR** gate does.



1.3.2 Multiple Qubit Gates

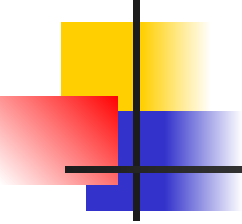
- Classical NAND gate is **universal** – any function on bits can be computed from only NAND gates
- A similar **quantum universality** result – any multiple qubit logic gate can be composed from controlled-NOT and single qubit gates



1.3.2 Multiple Qubit Gates

- Classical versus quantum gates

- All quantum gates are reversible because the inverse of a unitary matrix is also unitary
- However, many classical gates, like NAND and XOR, are irreversible or non-invertible because it is not possible to determine what the inputs were
 - Thus, an irretrievable loss of information occurs
- Understanding how to do classical logic in this reversible way will be crucial in understanding how to harness the power of quantum computing



1.3.3 Measurements in Bases Other Than the Computational Basis

- So far, a qubit in a state $\alpha|0\rangle + \beta|1\rangle$ has been described using the basis states $|0\rangle$ and $|1\rangle$
- Other bases can be used, and its importance is to describe experimental results (section 2.2.3)

1.3.4 Quantum Circuits

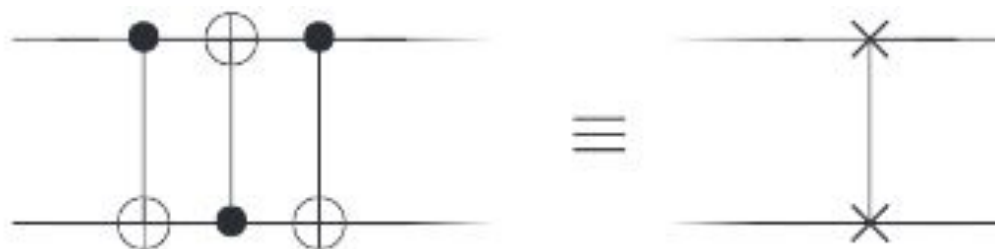


Figure 1.7. Circuit swapping two qubits, and an equivalent schematic symbol notation for this common and useful circuit.

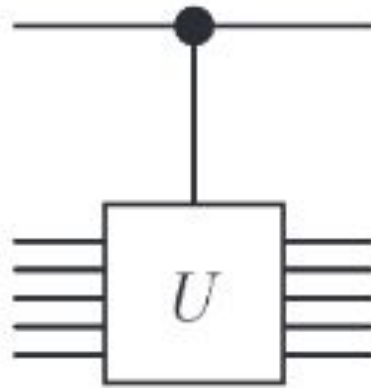
$$\begin{aligned} |a, b\rangle &\longrightarrow |a, a \oplus b\rangle && \text{additions are modulo 2} \\ &\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \\ &\longrightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle, \end{aligned}$$



1.3.4 Quantum Circuits

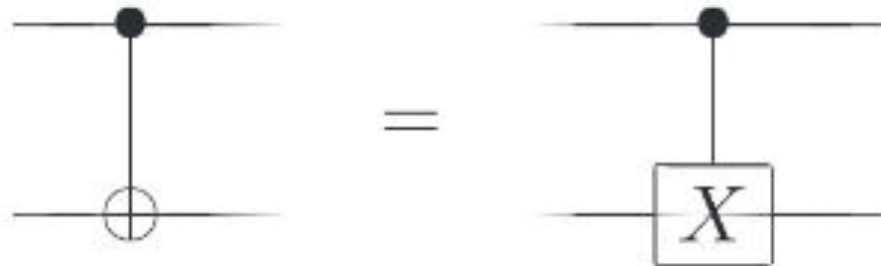
- Classical circuits **not** present in quantum circuits
 - Loops – therefore, quantum circuits are acyclic
 - Fan-in – wires joined together
 - Fan-out – produces copies of a bit

1.3.4 Quantum Circuits



Top line is control qubit
 U = any unitary matrix

Figure 1.8. Controlled- U gate.



Matrix X =
quantum not gate

Figure 1.9. Two different representations for the controlled-NOT.

1.3.4 Quantum Circuits

■ Quantum measurement circuit

- Converts qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a bit M
 - Result = 0 with probability α^2 , 1 with probability β^2

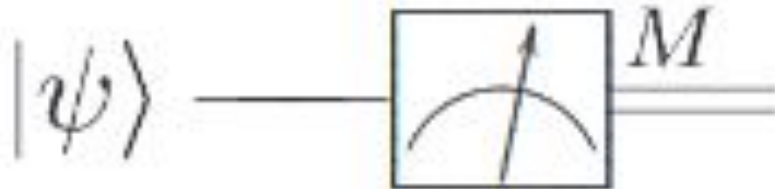


Figure 1.10. Quantum circuit symbol for measurement.



1.3.5 Qubit Copying Circuit?

- This section shows that qubits can't be copied
- This is known as the *no-cloning theorem*
- This is a key difference between quantum and classical information

1.3.6 Example: Bell States

In	Out
$ 00\rangle$	$(00\rangle + 11\rangle)/\sqrt{2} \equiv \beta_{00}\rangle$
$ 01\rangle$	$(01\rangle + 10\rangle)/\sqrt{2} \equiv \beta_{01}\rangle$
$ 10\rangle$	$(00\rangle - 11\rangle)/\sqrt{2} \equiv \beta_{10}\rangle$
$ 11\rangle$	$(01\rangle - 10\rangle)/\sqrt{2} \equiv \beta_{11}\rangle$

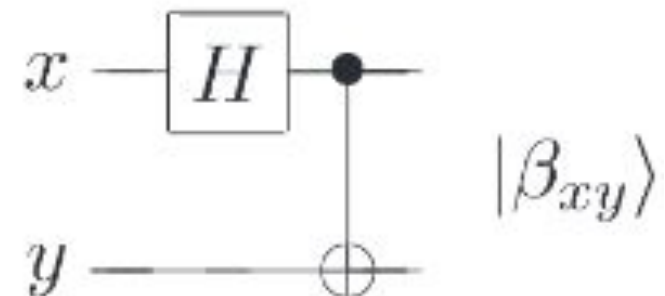


Figure 1.12. Quantum circuit to create Bell states, and its input–output quantum ‘truth table’.

1.3.7 Example: Quantum Teleportation

Quantum teleportation is a technique for moving quantum states around

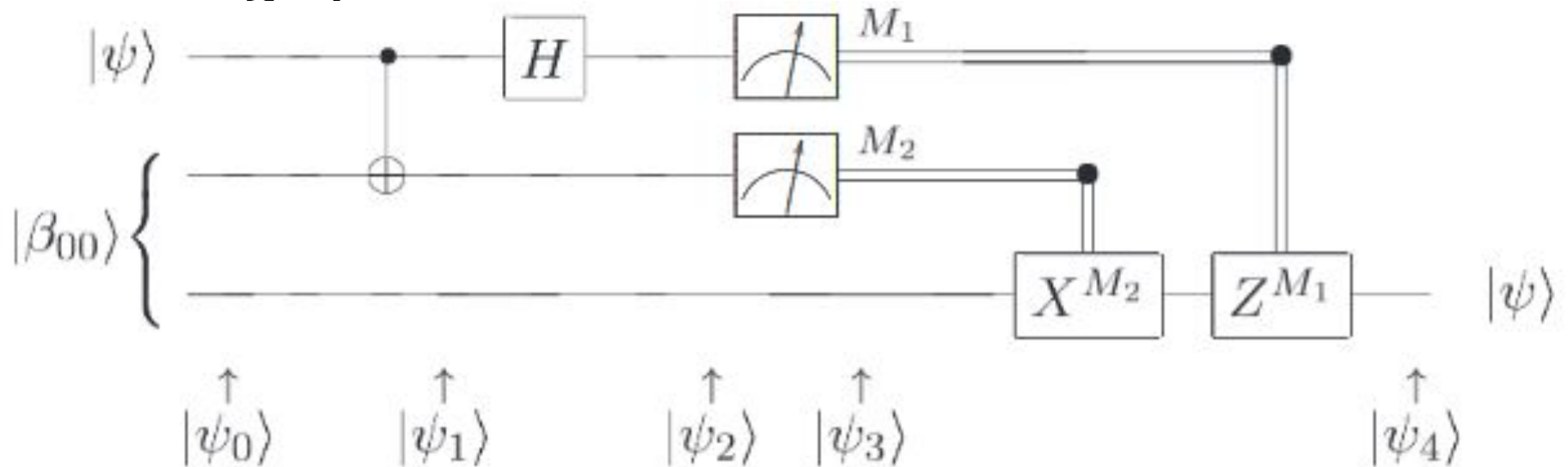


Figure 1.13. Quantum circuit for teleporting a qubit. The two top lines represent Alice's system, while the bottom line is Bob's system. The meters represent measurement, and the double lines coming out of them carry classical bits (recall that single lines denote qubits).



1.3.7 Example: Quantum Teleportation

- Quantum teleportation has interesting features
 - It emphasizes the different quantum resources
 - In particular, chap 10 explains how it is used to build quantum gates resistant to noise, and chap 12 explains how it is connected with properties of quantum error-correcting codes
 - However, it does not
 - Enable faster-than-light communication
 - And does not violate the no-cloning theorem