Chapter 3

Quantum Computing Tools

The purpose of this chapter is to prepare some basic tools useful for quantum computation.

- Bits vs. Qubits
- Reversible Operations
- Measurement and the Born rule
- Basic Logic Gates vs. Quantum Gates
- Circuit Design
- Non-cloning Theorem

3.1 Quantum Computer

- A quantum computer is one that executes operations by exploiting certain special transformations of its internal state.
- In a quantum computer, the physical systems encoding the individual logical bits must not have any physical interactions with whatever that are not under the complete control of the intended program.
  - ◇ These common interactions matters not in a conventional computers:
    - ▷ Air molecules bouncing off the physical systems.
    - ▷ Absorption of minute amounts of ambient radiant thermal energy.
    - ▷ Coexistent features within the same system that cause interference phenomena between what matters for the computation and what does not.
  - ◇ But, they introduce potentially catastrophic disruptions into the operation of a quantum computer.
- How to maintain isolation is a challenge!
  - ◇ In general a quantum computer cannot be encoded in physical systems of macroscopic size.
  - ◇ Bits are encoded in a small number of states of a system of atomic size.
    - ▷ Extra internal features require extraordinarily high energies to come into play.

Bits versus Qubits

- On a classical computer, a *bit* (binary digit) is the basic unit of digital representation.
  - ◇ Each digit, 0 or 1, is realized by a specific physical quantity, say, the on-or-off of an electronic flow.
  - ◇ Numbers are represented by strings of 0's and 1's.
  - ◇ Binary arithmetic converts numbers into other numbers.
  - ◇ Most machines have finite precision and limited memory.
- On a quantum computer, a *qubit* (quantum bit) is the basic unit of quantum information.
  - ◇ A qubit is a two-state quantum mechanical system, denoted by $|0\rangle$ or $|1\rangle$.
  - ◇ A qubit is the quantum version of the classical bit physically realized with a two-state device.
- The fundamental difference is
  - ◇ In a classical system, a bit would have to be in one state or the other.
  - ◇ In a quantum mechanics, the qubit is to be in a coherent superposition of both states simultaneously.

Representing an n-Qubit

- Any integer $x \in [0, 2^n)$ has a unique binary representation:

$$x \equiv (x_{n-1} \dots x_0)_2 := \sum_{j=0}^{n-1} x_j 2^j. \tag{3.1}$$

  - ◇ Each x_j is either 0 or 1.
  - ◇ We say that x is composed by n bits.
  - ◇ Count the indices from right to left.

- We can mimic a similar notion by thinking x as an n-dimensional vector $\mathbf{x}$ where

$$\mathbf{x} = |x\rangle_n := |x_{n-1}\rangle \otimes |x_{n-1}\rangle \otimes \dots |x_0\rangle\,. \tag{3.2}$$

  - ◇ In this way, we properly identify $|x\rangle_n$ with the standard basis in $\mathbb{C}^n$.

$$|5\rangle_3 = |101\rangle_3 = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}.$$

- In Section 2.3, we represent a 2-Qubit element $|\boldsymbol{\psi}\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ by a 2×2 matrix. Now we can represent it by a vector in $\mathbb{C}^4$.

$$|\boldsymbol{\psi}\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}.$$

n-Qubit in $\mathbb{C}^{2^n}$

- An n-qubit $|\boldsymbol{\psi}\rangle \in \mathbb{C}^{\otimes n}$ should be an order-n tensor.
- The preceding notion can be generalized

$$|\boldsymbol{\psi}\rangle = \sum_{0 \leq x < 2^n} \alpha_x \, |x\rangle_n \, . \tag{3.3}$$

  ◇ $|x\rangle_n$ is the x-th standard basis in $\mathbb{C}^{2^n}$. (Starting from 0)

  ◇ $\sum_{0 \leq x < 2^n} |\alpha_x|^2 = 1$.

  ◇ A general state in the n-partite system $\mathbb{C}^{2^n}$ resides in a 2^n-dimensional complex vector space.

- Recall the notation of separability and entanglement.

  ◇ Not all vectors $\mathbf{c} \in \mathbb{C}^4$ can be separated as $\mathbf{c} = \mathbf{a} \otimes \mathbf{b}$ with $\mathbf{a}, \mathbf{b} \in \mathbb{C}^2$.

  ◇ What is the necessary condition that a vector $\mathbf{c} \in \mathbb{C}^{2^n}$ is separable?

    ▷ $2^n >> 2n$ when n is large. So, most quantum states are entangled.

Multistate Systems

- An integer can be expressed in an arbitrary base.
  - ◇ $(11)_{10} = (12)_9 = (102)_3 = (111)_2$.
- Likewise, a quantum system can admit three different states, each is called a *qutrit*.
  - ◇ In general, if a system takes d different states, then each state is called a *qudit*.
- Maybe it is of interest for theoretical consideration only. However, just in case it becomes useful, how to derive the general representation? (Recall that IBM machines use base 16.)

3.2 Reversible Operations

- A crucial and necessary feature in quantum computing is that all but one operations must be *reversible*. That is, when transforming an initial state of the final form, only processes whose action can be inverted are employed.
  - ◇ Why is this concept of reversibility so important?
- The one single irreversible component to the operation of a quantum computer is measurement.
  - ◇ Measurement is the only way to extract useful information.
    - ▷ In a classical computer, the extraction of information from the state of the bits is natural and conceptually straightforward.
    - ▷ In a quantum machine, the measurement after the state has acquired its final form destroys the state.

Some Irreversible Operators

- **ERASE** is irreversible. (not feasible on quantum machines)
  - ◇ It nullifies every state.
  - ◇ There is no way to recover the initial state.
- **AND** is irreversible.
  - ◇ **AND** returns a high output $|1\rangle$ only if all inputs are high.

Input		Output
A	B	A $\wedge$ B
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$

  - ◇ Suppose its output is $|0\rangle$. Can we infer what its inputs were?
- **XOR** is irreversible.
  - ◇ **XOR** is an exclusive **OR** that returns a true output results if one and only one of the inputs is true.

Input		Output
A	B	A $\oplus$ B
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

  - ◇ Why is this operation irreversible?

Some Reversible Operations

- **NOT**, denoted by $\mathbf{X}$, is reversible.
  - ◇ It exchanges two states.
  - ◇ $\mathbf{X}(|0\rangle) = |1\rangle$; $\mathbf{X}(|1\rangle) = |0\rangle$.
  - ◇ $\mathbf{X}^2 = I$.
  - ◇ Can think of $\mathbf{X}$ as
$$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{3.4}$$
- **SWAP**, denoted by $\mathbf{S}_{ij}$, is reversible.
  - ◇ $\mathbf{S}_{ij}$ swaps the ith and the jth qubits.
  - ◇ Over a bipartite system, $\mathbf{S}_{01}\,|0\rangle_2 = |0\rangle_2$, $\mathbf{S}_{01}\,|1\rangle_2 = |2\rangle_2$, $\mathbf{S}_{01}\,|2\rangle_2 = |1\rangle_2$, $\mathbf{S}_{01}\,|3\rangle_2 = |3\rangle_2$.
  - ◇ Can think of $\mathbf{S}_{ij}$ as
$$\mathbf{S}_{01} = \mathbf{S}_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{3.5}$$
- **Theorem:** Any Boolean function $f : \{0,1\}^n \to \{0,1\}^n$ is computable by a Boolean circuit C using just **AND**, **OR**, and **NOT** gates.
  - ◇ Gates **AND**, **OR**, and **NOT** are *universal*.
  - ◇ See if you can prove the above theorem.
  - ◇ A related question is, if a circuit can be built, how to build it with the shortest length?

Why Is Reversibility Necessary?

- Quantum computers work by applying quantum gates to quantum states.
  - ◇ Quantum gates are the basic building blocks of quantum circuits, like logic gates are for classical digital circuits.
  - ◇ The quantum circuits realize certain functions for quantum computations, to help evolving the quantum system to reach some desired ultimate goal.
- One major difference between quantum gates and classical logic gates is the reversibility.
  - ◇ Quantum gates are reversible, i.e. suppose $\mathbf{A}$ is a certain quantum gate. Then $\mathbf{A}\,|X\rangle = |Y\rangle$ if and only $\mathbf{A}\,|Y\rangle = |X\rangle$, ensuring no information loss.
  - ◇ Classical gates are not reversible.
    - ▷ A typical arithmetic operation is irreversible.
    - ▷ The loss of "information" is a huge problem. (What information?)
- Major challenge:
  - ◇ An operation on a classical computer is extendable to a quantum computer must be reversible.

Preserving Quantum Properties

- The evolution of quantum states must preserve property of quantum mechanics.
  - ◇ Keep the sum-to-one of probabilities of all possible outcomes.
  - ◇ Preserve the set of density matrices.
- Suppose not. Then
  - ◇ Begin with two entangled states.
  - ◇ Go through some gates that are irreversible.
  - ◇ The above properties are lost.
  - ◇ Where would we stand? No information can be retrieved.
- The quantum gates should be reversible primarily because of energy efficiency.
  - ◇ Notice the cooling problem in any classical computer (even battery-based).
  - ◇ Can calculate energy produced for every bit of information lost due to an irreversible computation.
- Unitary transformation can preserve quantum properties.
  - ◇ Thus, any quantum gate is to be implemented as a unitary operator.
  - ◇ A unitary transformation is always reversible.

3.3 Logic Gates vs. Quantum Gates

- In classical systems, binary values are stored in classical memory, passed through logic gates, altered and modified along the way, and finally, produce some output.
  - ◇ Gates ⇒ Circuits ⇒ Algorithms.
- The same goes for quantum systems.
  - ◇ Superpose states in a quantum memory
  - ◇ Applying quantum gates maps that superpose to another state.
  - ◇ Take measurement to produce some meanful output.
- Similar ideas, but different way to build a gate.
  - ◇ In classical systems, any classical gate can be represented using Boolean algebra.
  - ◇ In quantum systems, the any quantum gate should be described as a unitary matrix.
- Major challenge:
  - ◇ How to convert an irreversible Boolean algebra to a reversible unitary matrix?
- In quantum systems, if the gate acts on n input qubits, the unitary matrix will be of size $2^n \times 2^n$ to produce n output qubits.

cNOT Gate

- The controlled-NOT operation **cNOT** plays a significant role in quantum computing.
  - ◇ $\mathbf{C}_{ij}$ flips the jth qubit (target) if and only if the ith qubit (control) is $|1\rangle$.

Before		After	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

    - ▷ The states are enumerate from right to left.
      - ✓ $\mathbf{C}_{10}\,|xy\rangle$ means that x is the control.
      - ✓ $\mathbf{C}_{01}\,|xy\rangle$ means that y is the control.
- Over a bipartite system, $\mathbf{C}_{10}\,|0\rangle_2 = |0\rangle_2$, $\mathbf{C}_{10}\,|1\rangle_2 = |1\rangle_2$, $\mathbf{C}_{10}\,|2\rangle_2 = |3\rangle_2$, $\mathbf{C}_{10}\,|3\rangle_2 = |2\rangle_2$. (Work out what $\mathbf{C}_{01}$ does?)
  - ◇ Can think of $\mathbf{C}_{01}$ and $\mathbf{C}_{10}$ as

$$\mathbf{c}_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \mathbf{c}_{01} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

  - ◇ Can also write

$$\begin{aligned} \mathbf{C}_{ij}\,|x_i\rangle\,|y_j\rangle &= |x_i\rangle\,|y_j \oplus x_i\rangle \\ \mathbf{C}_{ji}\,|x_i\rangle\,|y_j\rangle &= |x_i \oplus y_j\rangle\,|y_j\rangle\,. \end{aligned}$$

    - ▷ $\oplus$ is the addition modulo 2.
- See the similarity between **XOR** and **cNOT**? (Why needed?)

$\mathbf{Z}$ Gate

- A useful single qubit $\mathbf{n}$ operator:
  - ◇ For $x = 0$ or 1, define

$$\begin{cases} \mathbf{n}\,|x\rangle & := \; x\,|x\rangle\,, \\ \widetilde{\mathbf{n}}\,|x\rangle & := \; (1-x)\,|x\rangle\,. \end{cases} \tag{3.6}$$

  - ◇ Can represent

$$\mathbf{n} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}; \quad \widetilde{\mathbf{n}} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}.$$

  - ◇ Enjoy basic properties such as

$$\begin{cases} \mathbf{n}^2 = \mathbf{n}; \quad \widetilde{\mathbf{n}}^2 = \widetilde{\mathbf{n}}; \quad \mathbf{n}\widetilde{\mathbf{n}} = \widetilde{\mathbf{n}}\mathbf{n} = 0; \quad \mathbf{n} + \widetilde{\mathbf{n}} = I_2; \\ \mathbf{n}\mathbf{X} = \mathbf{X}\widetilde{\mathbf{n}}; \quad \widetilde{\mathbf{n}}\mathbf{X} = \mathbf{X}\mathbf{n}. \end{cases}$$

- Let $\mathbf{n}_j$ and $\mathbf{X}_j$ denote their applications to the jth qubit. Then

$$\mathbf{C}_{ij} = \widetilde{\mathbf{n}}_i + \mathbf{X}_j\mathbf{n}_i.$$

  - ◇ The proof would be a good exercise.

- The $\mathbf{Z}$ gate has no physical meaning, but is a useful intermediator.

$$\mathbf{Z} := \widetilde{\mathbf{n}} - \mathbf{n} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{3.7}$$

  ◇ Trivially,

$$\mathbf{n} = \frac{1}{2}(I - Z); \quad \widetilde{\mathbf{n}} = \frac{1}{2}(I + Z).$$

  ◇ Also,

$$\mathbf{X}_i \mathbf{Z}_j = \begin{cases} \mathbf{Z}_i \mathbf{X}_j, & \text{if } i \neq j \\ -\mathbf{Z}_i \mathbf{X}_j, & \text{if } i = j, \end{cases} \tag{3.8}$$

  ◇ Can write

$$\begin{aligned} \mathbf{C}_{ij} &= \frac{1}{2}(I_2 + \mathbf{Z}_i) + \frac{1}{2}\mathbf{X}_j(I_2 - \mathbf{Z}_i) \\ &= \frac{1}{2}(I_2 + \mathbf{X}_j) + \frac{1}{2}\mathbf{Z}_i(I_2 - \mathbf{X}_j). \end{aligned}$$

Hadamard Gate $\mathbf{H}$

- Hadamard gate is another critically important operation.

$$\mathbf{H} = \frac{1}{\sqrt{2}}(\mathbf{X} + \mathbf{Z}) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{3.9}$$

  ◇ Observe these effects:

$$\begin{aligned} \mathbf{H}\,|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ (\mathbf{H} \otimes \mathbf{H})(|0\rangle \otimes |0\rangle) &= \mathbf{H}\,|0\rangle \otimes \mathbf{H}\,|0\rangle \qquad (3.10) \\ &= \frac{1}{2}(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2), \\ \mathbf{H}^{\otimes n}\,|0\rangle_n &= \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} |x\rangle_n . \qquad (3.11) \end{aligned}$$

    ▷ This is an equally weighted superposition of all possible n-qubits.

      ✓ A good starting point for any quantum evolution.

      ✓ Consider the case $n = 100$. Apply the Hadamard gate to the trivial state $|0\rangle_{100}$. Then the final state will contain the results of all $2^{100} \approx 10^{30}$ states. This is the amazing power *quantum parallelism*.

- Verify the following general formula:

$$\mathbf{H}^{\otimes n}\,|z\rangle_n = \sum_{0 \le x < 2^n} \frac{(-1)^{x \cdot z}}{\sqrt{2^n}} |x\rangle_n . \tag{3.12}$$

  ◇ If $|x\rangle_n = |x_{n-1} \dots x_0\rangle_2$ and $|z\rangle_n = |z_{n-1} \dots z_0\rangle_2$, then

$$x \cdot z := x_{n-1}z_{n-1} \oplus \dots \oplus x_0 z_0. \tag{3.13}$$

The EPR Pairs

- Consider the combined effect

$$\left|\boldsymbol{\psi}_{xy}\right\rangle := \mathbf{C}_{10}\mathbf{H}_1 \left|xy\right\rangle . \tag{3.14}$$

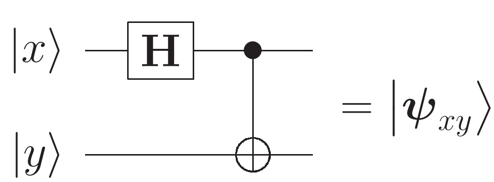
  - ◇ Read as applying $\mathbf{H}$ to the qubit x, followed by the **cNOT** using the first qubit to control the qubit y.

$$\begin{aligned}
\left|\boldsymbol{\psi}_{00}\right\rangle &= \mathbf{C}_{10}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \left|\Phi^{+}\right\rangle \\
\left|\boldsymbol{\psi}_{01}\right\rangle &= \mathbf{C}_{10}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \left|\Psi^{+}\right\rangle \\
\left|\boldsymbol{\psi}_{10}\right\rangle &= \mathbf{C}_{10}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \left|\Phi^{-}\right\rangle \\
\left|\boldsymbol{\psi}_{11}\right\rangle &= \mathbf{C}_{10}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|1\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \left|\Psi^{-}\right\rangle
\end{aligned}$$

  - ◇ Can be represented by the matrix multiplication

$$\mathbf{C}_{10}(\mathbf{H} \otimes I_2) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}.$$

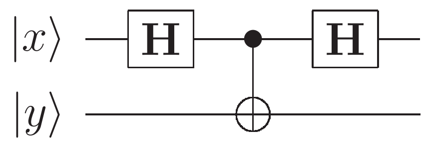
- A quantum circuit that produces the orthonormal entangled Bell states $\left|\boldsymbol{\psi}_{xy}\right\rangle$ from untangled 2-qubit states $|xy\rangle$.



  - ◇ • denotes a control point.
  - ◇ □ denotes a gate.
  - ◇ ⊕ denotes a target.

More Exercises

- What is the output of this circuit?

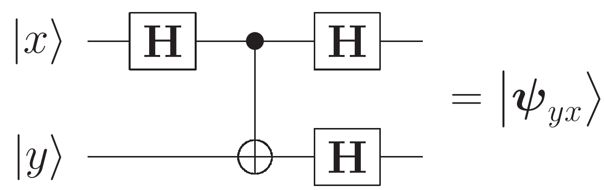


  ◇ Work out the qubit analysis step by step and show that

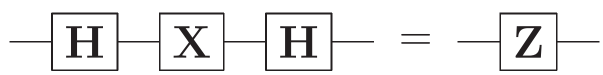
$$(\mathbf{H}\otimes I_2)\mathbf{C}_{10}(\mathbf{H}\otimes I_2) = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$

- Prove the following results:

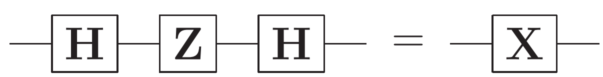
  ◇



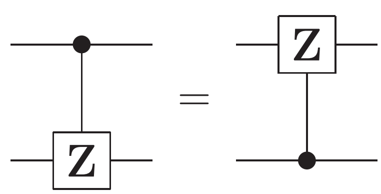
  ◇



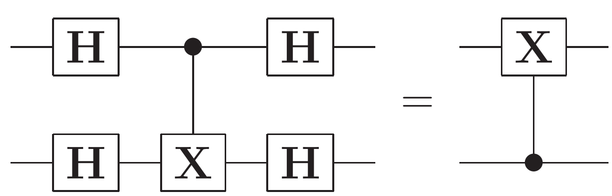
  ◇



  ◇



  ◇



Toffoli Gate **T**

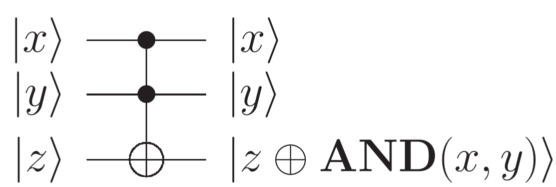
- It has been known that to build up all arithmetical operations on a reversible classical computer it is necessary (and sufficient) to use at least one classically irreducible 3-qubit gate. (Why?)
- Consider the Toffoli gate **T**.
  - ◇ It is a **ccNOT** gate where the third (target) qubit is flipped if and only if the first two (control) qubits are $|1\rangle$.

Before		After	
Control	Target	Control	Target
$\|00\rangle$	$\|0\rangle$	$\|00\rangle$	$\|0\rangle$
$\|00\rangle$	$\|1\rangle$	$\|00\rangle$	$\|1\rangle$
$\|01\rangle$	$\|0\rangle$	$\|01\rangle$	$\|0\rangle$
$\|01\rangle$	$\|1\rangle$	$\|01\rangle$	$\|1\rangle$
$\|10\rangle$	$\|0\rangle$	$\|10\rangle$	$\|0\rangle$
$\|10\rangle$	$\|1\rangle$	$\|10\rangle$	$\|1\rangle$
$\|11\rangle$	$\|0\rangle$	$\|11\rangle$	$\|1\rangle$
$\|11\rangle$	$\|1\rangle$	$\|11\rangle$	$\|0\rangle$

  - ◇ Can write

$$T\,|x\rangle\,|y\rangle\,|z\rangle = |x\rangle\,|y\rangle\,|z \oplus xy\rangle\,. \tag{3.15}$$

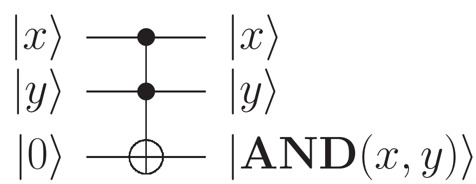
  - ◇ Can draw



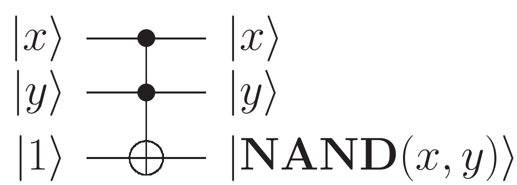
- One can use Toffoli gates to build systems that will perform any desired Boolean function computation in a reversible manner, i.e., the Tofolli gate is universal. (More to think about!)
- A Toffoli gate can be constructed from eight **cNOT** gates.

AND and **NAND** Gates

- The logical **AND** and **NAND** gates are not reversible.
  - ◇ To make them usable for quantum computation, we have to build some equivalent gates.
  - ◇ The notion of Tofolli gate can be applied.
- $\mathbf{AND}(x, y) = \mathbf{T}\,|xy0\rangle$.
  - ◇



- $\mathbf{NAND}(x, y) = \mathbf{T}\,|xy1\rangle$.
  - ◇

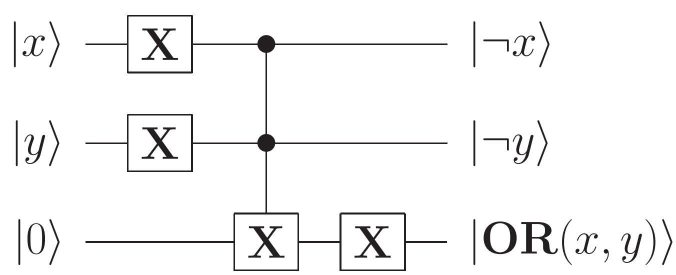


OR Gate

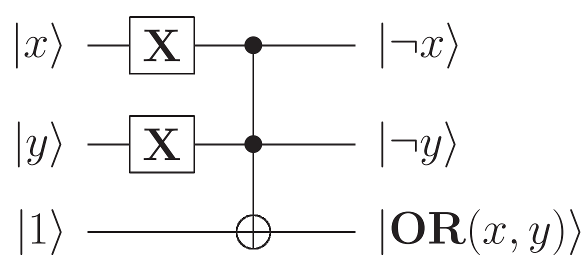
- **OR**(x, y) is much harder to reverse.
- Consider the equivalence

Input		Output	Input		Output
$\|x\rangle$	$\|y\rangle$	$\|x\rangle \vee \|y\rangle$	$\|\neg x\rangle$	$\|\neg y\rangle$	$\|\neg x\rangle \wedge \|\neg y\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$

◇



◇ Does this work?



3.4 Circuits

- As in the usual sense of computation, a suitably programmed quantum computer should act on a number x to produce another number $f(x)$ for some specified function f.
  - ◇ Properly interpreted, will assume x is an integer represented in an n-qubit integer.
- Different from the classical computation, quantum computers must operate reversibly to perform their magic, except for measurement gates.
  - ◇ They are generally designed to operate with both input and output registers.
    - ▷ Sometimes the algorithm has to be designed in a fairly nonclassical way.
  - ◇ Need to view the function f as a unitary transformation.
    - ▷ We have see how **AND** and **OR** are treated.

Registers

- Suppose $f : \{0,1\}^n \to \{0,1\}^m$.
  - ◇ Represent $(x; f(x))$ in at least $n+m$ Qbits.
    - ▷ The first n-qubits are called the input register, representing x.
    - ▷ The last m-qubits are called the output register, representing $f(x)$.
  - ◇ Sometimes additional qubits might be needed. (Why?)
- A standard protocol for quantum computation of $f(x)$:

$$\mathbf{U}_f(|x\rangle_n |y\rangle_m) := |x\rangle_n |f(x) \oplus y\rangle_m . \tag{3.16}$$

  - ◇ $\oplus$ is the modulo-2 bitwise addition (without carrying).
  - ◇ $\mathbf{U}_f(|x\rangle_n |0\rangle_m) := |x\rangle_n |f(x)\rangle_m$.
- The operator $\mathbf{U}_f$ is reversible.

$$\begin{aligned}\mathbf{U}_f\mathbf{U}_f(|x\rangle_n |y\rangle_m) &= \mathbf{U}_f(|x\rangle_n |f(x) \oplus y\rangle_m) \\ &= |x\rangle_n |f(x) \oplus f(x) \oplus y\rangle_m = |x\rangle_n |y\rangle_m .\end{aligned}$$

Quantum Parallelism and Weirdness

- Recall (3.11).

$$\mathbf{H}^{\otimes n} |0\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} |x\rangle_n .$$

- Observe

$$\begin{aligned} \mathbf{U}_f(\mathbf{H}^{\otimes n} \otimes I_m)(|0\rangle_n |0\rangle_m) &= \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} \mathbf{U}_f(|x\rangle_n |0\rangle_m) \\ &= \frac{1}{\sqrt{2^n}} \sum_{0 \le x < 2^n} |x\rangle_n |f(x)\rangle_m . \end{aligned} \tag{3.17}$$

  - ◇ This relationship reveals that all 2^n calculations of $f(x)$ are done in parallel! We have done nothing fancy on the left side of (3.17) to the n qubits, but the mathematics tells that the quantum computation has "somehow" divided the computational task among 2^n of parallel worlds. This simultaneity is where the quantum computation achieves its power.
  - ◇ However, we have no way to learn the state since they all appear with equal probability.

- The conventional notion that the selection of x was made before $f(x)$ was evaluated is as wrong as as asserting that a superposed qubit is actually in any of its basis states.
  - ◇ The so called "quantum weirdness" is that the random selection of the x, for which $f(x)$ can be learned, is made only after the computation has been carried out, quite possibly long after the computation has been finished.

Non-Cloning Theorem

- One possible remedy for the quantum weirdness is to "remember" the experimental results. That is, make copies of the output state before running the whole computation over again.
  - ◇ But such copying is impossible. There is no quantum procedure that can do duplication. (Why?)
  - ◇ We can copy if the cloning is limited to the basis states.
- **Theorem:** There is no unitary transformation that can take the state $|\psi\rangle_n |0\rangle_n$ into the state $|\psi\rangle_n |\psi\rangle_n$ for arbitrary $|\psi\rangle_n$.
  - ◇ Suppose that a unitary operator $\mathbf{U}$ clones a quantum system.
  - ◇ Let $|\psi\rangle$ and $|\phi\rangle$ be two linear independent states. Then
$$\mathbf{U}(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle ; \quad \mathbf{U}(|\phi\rangle |0\rangle) = |\phi\rangle |\phi\rangle .$$
  - ◇ By linearity,
$$\begin{aligned} \mathbf{U}(\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) |0\rangle) &= \frac{1}{\sqrt{2}}(\mathbf{U}(|\psi\rangle |0\rangle) + \mathbf{U}(|\phi\rangle |0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|\psi\rangle |\psi\rangle + |\phi\rangle |\phi\rangle). \end{aligned}$$
  - ◇ On the other hand,
$$\begin{aligned} \mathbf{U}(\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) |0\rangle) &= \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)\frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle) \\ &= \frac{1}{2}(|\psi\rangle |\psi\rangle + |\psi\rangle |\phi\rangle + |\phi\rangle |\psi\rangle + |\phi\rangle |\phi\rangle). \end{aligned}$$
- Over $\mathbb{C}^2$, describe the non-cloning theorem in linear algebra terms.

No Approximate Cloning

- Is it possible to approximately cloning to a reasonable degree?
- Approximate copy is not possible.
  - ◇ Suppose $\mathbf{U}$ is capable of doing

$$\mathbf{U}(|\psi\rangle\,|0\rangle) \approx |\psi\rangle\,|\psi\rangle\,; \quad \mathbf{U}(|\phi\rangle\,|0\rangle) \approx |\phi\rangle\,|\phi\rangle\,.$$

  - ◇ Since a unitary transformation preserves length and angles,

$$\begin{aligned}\langle \mathbf{U}(|\psi\rangle\,|0\rangle)|\mathbf{U}(|\phi\rangle\,|0\rangle)\rangle &= \langle(|\psi\rangle\,|0\rangle)|(|\phi\rangle\,|0\rangle)\rangle \\ &\approx \langle(|\psi\rangle\,|\psi\rangle)|(|\phi\rangle\,|\phi\rangle)\rangle\end{aligned}$$

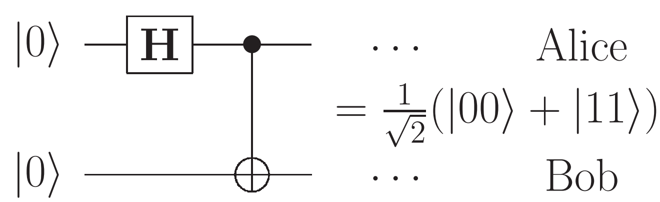
  - ◇ Need to satisfy

$$\langle\psi|\phi\rangle \approx (\langle\psi|\phi\rangle)^2.$$

  - ◇ Cannot be true for arbitrary $|\psi\rangle$ and $|\phi\rangle$.

3.5 Applications of Entanglement

- Dense coding and quantum teleportation are two simple but illustrative applications of qubits and quantum gates.
  - ◇ A common setting for both cases is the entanglement.
- Assume the game players are Alice and Bob.
  - ◇ Assume that both of them have had in hand the same EPR pair, say, the Bell state $|\Phi^+\rangle$:



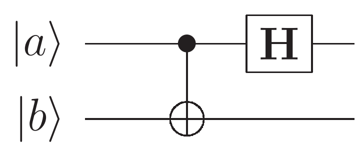
  - ◇ Assume that Alice has the first bit qubit information and Bob has the second bit qubit information.

Dense Coding

- Suppose that Alice wants to send a 2-bit message to Bob.
- Depending on the message $00, 01, 10, 11$, Alice applies the Pauli matrices $I_2, \sigma_x, \imath\sigma_y, \sigma_z$, respective, to her (first) qubit in $|\Phi^+\rangle$.

message	transformation U on $\|\Phi^+\rangle$	state sent
$0 = 00$	$I_2 \otimes I_2$	$\|\psi_0\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
$1 = 01$	$\sigma_x \otimes I_2$	$\|\psi_1\rangle = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
$2 = 10$	$\imath\sigma_y \otimes I_2$	$\|\psi_2\rangle = \frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
$3 = 11$	$\sigma_z \otimes I_2$	$\|\psi_3\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

- Alice sends her joint spin over to Bob.
- Bob applies the gate



to the state he received from Alice.

state received	after **cNOT**	after **H**
$\|\psi_0\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\|00\rangle$
$\|\psi_1\rangle$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\|01\rangle$
$\|\psi_2\rangle$	$\frac{1}{\sqrt{2}}(\|01\rangle - \|11\rangle)$	$\|11\rangle$
$\|\psi_3\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\|10\rangle$

What is significant?

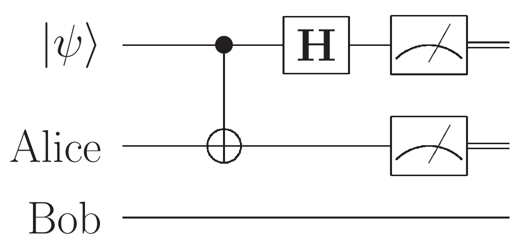
- Alice simply needs to prepare her single 1-qubit in $|\Phi^+\rangle$, by which she can sent 2-bit information.
- Bob can fully decode the single tangled state for the original message.
  - ◇ Look at the second qubit.
    - ▷ $|0\rangle \Rightarrow 00$ or 11.
    - ▷ $|1\rangle \Rightarrow 01$ or 10.
  - ◇ Look at the he first qubit.
    - ▷ $|0\rangle \Rightarrow 00$ or 01.
    - ▷ $|1\rangle \Rightarrow 10$ or 11.
- The only thing in common is that they share a tangled state.
  - ◇ Try a few other Bell states.
  - ◇ Does the ordering $\{I_2, \sigma_x, \imath\sigma_y, \sigma_z\}$ matter?
- We just see the result, but what is the mathematics behind?

Teleportation

- Consider the scenario that
  - ◇ Alice has a qubit $|\psi\rangle = \alpha_1 |0\rangle + \alpha_1 |1\rangle$ that she want to send to Bob.
  - ◇ Alice is at far distance away from Bob.
  - ◇ Alice cannot learn what α_0 and α_1 are without performing a measurement, which would cause her to lose $|\psi\rangle$ entirely. (Collapse!!!)
  - ◇ Even if Alice knew about α_0 and α_1, it would need infinitely many bits to maintain the precision.

Alice's Tasks

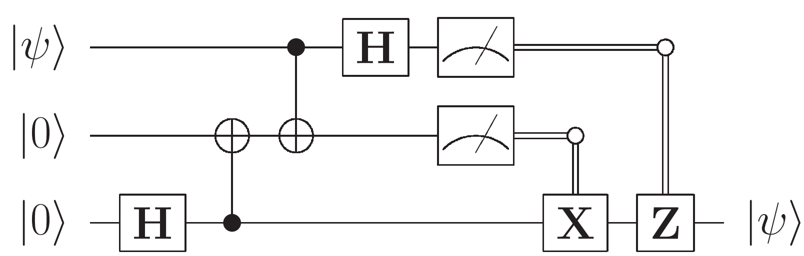
- Prepare a 3-qubit state
$$|\psi\rangle \otimes \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(\alpha_0 |000\rangle + \alpha_0 |011\rangle + \alpha_1 |100\rangle + \alpha_1 |111\rangle).$$
- Apply the quantum gate



  ◇ Before the measurement, Alice has this state in hand:
  $$\frac{1}{2}(\alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_1 |010\rangle + \alpha_0 |011\rangle + \alpha_0 |100\rangle - \alpha_1 |101\rangle - \alpha_1 |110\rangle + \alpha_0 |111\rangle .$$
  ◇ Suppose Alice's measures her two qubits. The probability of every state in $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ is always $\frac{1}{4}$. (Why?)
  ◇ After measurement, the 3-qubit state collapses to
  $$\begin{aligned} &|00\rangle \otimes (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \\ &|01\rangle \otimes (\alpha_1 |0\rangle + \alpha_0 |1\rangle) \\ &|10\rangle \otimes (\alpha_0 |0\rangle - \alpha_1 |1\rangle) \\ &|11\rangle \otimes (-\alpha_1 |0\rangle + \alpha_0 |1\rangle) \end{aligned}$$
    ▷ The above expression is only for bookkeeping.
      ✓ Alice only has two classical bits in hand.
      ✓ Alice no long has a copy of the state $|\psi\rangle$. (Non-cloning theorem!)
    ▷ The third qubit will be Bob's state from which he needs to recover $|\psi\rangle$.

Bob's Tasks

- Alice "calls" Bob to inform him her partial measurement which will be two classical bits.
  - ◇ These two classical bits tell Bob what transform is to be applied to the third qubit to recover the original $|\psi\rangle$.
  - ◇ Since the "call" is needed, the teleportation is still subject to the speed of light.
- How?
  - ◇ If Alice says 00, then Bob's qubit is precisely $|\psi\rangle$.
  - ◇ If Alice says 01, then Bob applies $\mathbf{X}$ to get $|\psi\rangle$.
  - ◇ If Alice says 10, then Bob applies $\mathbf{Z}$ to get back $|\psi\rangle$.
  - ◇ If Alice says 11, then Bob applies $\imath\sigma_y = XZ$ to retrieve $|\psi\rangle$.
- The overall teleportation procedure can be described in the circuit:



  - ◇ We use ∘ to denote the controlled operator.