C/CS/Phys C191 Quantum Gates and Universality 9/22/05
Fall 2005 Lecture 8

1 Readings

Benenti, Casati, and Strini:

Classical circuits and computation Ch.1.2, 2.6

Quantum Gates Ch. 3.2-3.4

Universality Ch. 3.5-3.6

2 Unitary Operators

A postulate of quantum physics is that quantum evolution is unitary. That is, if we have some arbitrary quantum system U that takes as input a state $|\phi\rangle$ and outputs a different state $U|\phi\rangle$, then we can describe U as a *unitary linear transformation*, defined as follows.

If U is any linear transformation, the *adjoint* of U, denoted $U^\dagger$, is defined by $(U\vec{v},\vec{w}) = (\vec{v},U^\dagger\vec{w})$. In a basis, $U^\dagger$ is the conjugate transpose of U; for example, for an operator on $\mathscr{C}^2$,

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow U^\dagger = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} \quad .$$

We say that U is *unitary* if $U^\dagger = U^{-1}$. For example, rotations and reflections are unitary. Also, the composition of two unitary transformations is also unitary (Proof: U,V unitary, then $(UV)^\dagger = V^\dagger U^\dagger = V^{-1}U^{-1} = (UV)^{-1}$).

Some properies of a unitary transformation U:

- The rows of U form an orthonormal basis.
- The colums of U form an orthonormal basis.
- U preserves inner products, i.e. $(\vec{v},\vec{w}) = (U\vec{v},U\vec{w})$. Indeed, $(U\vec{v},U\vec{w}) = (U|v\rangle)^\dagger U|w\rangle = \langle v|U^\dagger U|w\rangle = \langle v|w\rangle$. Therefore, U preserves norms and angles (up to sign).
- The eigenvalues of U are all of the form $e^{i\theta}$ (since U is length-preserving, i.e., $(\vec{v},\vec{v}) = (U\vec{v},U\vec{v})$).
- U can be diagonalized into the form

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & e^{i\theta_d} \end{pmatrix}$$

3 Schrödinger's Equation

Schrödinger's equation is the equation of motion which describes the evolution in time of the quantum state.

$$i\hbar\frac{d\big|\psi(t)\big\rangle}{dt} = H\big|\psi\big\rangle \quad .$$

Here $\hbar$ is a constant (called Planck's constant – we'll usually assume $\hbar = 1$), and H is a linear *Hamiltonian* which is Hermitian, $H^\dagger = H$. Equivalently, H has an orthonormal set of eigenvectors $|\psi_i\rangle$, all with real eigenvalues λ_i: $H|\phi_i\rangle = \lambda_i|\phi_i\rangle$.

For those of you who are familiar with Schrödinger's equation, the unitarity restriction on quantum gates is simply the time-discrete version of the restriction that the Hamiltonian is Hermitian. This is a particular instance of the general relation between a unitary operator U and a Hermitian operator A

$$U = e^iA,$$

which follows from matrix algebra since $U^\dagger = exp(-iA^\dagger) = exp(-iA)$ and hence $UU^\dagger = 1$.

We will now prove explicitly that if the system satisfies Schrödinger's equation, then its evolution in discrete time is described by a unitary operator and determine this operator in terms of the eigenvalues of H. (We will assume that H is time independent.)

Write $|\psi(t)\rangle$ in the basis of eigenvectors of H:

$$|\psi(t)\rangle = \sum_j a_i(t)|\phi_j\rangle$$

$$\Downarrow$$

$$i\hbar\frac{d\Sigma a_j\big|\phi_j\big\rangle}{dt} = H\Sigma a_j\big|\phi_j\big\rangle = \Sigma a_j\lambda_j\big|\phi_j\big\rangle$$

$$\Downarrow$$

$$i\hbar\frac{da_j}{dt} = \lambda_j a_j$$

$$\Downarrow$$

$$a_j(t) = e^{-\frac{i}{\hbar}\lambda_j t}a_j(0)$$

$$\Downarrow$$

$$\big|\psi(t)\big\rangle = e^{-\frac{i}{\hbar}\lambda_j t}a_j(0)\big|\phi_j\big\rangle$$

We get that the change after a discrete time difference is unitary:

$$\big|\psi(t)\big\rangle = \begin{pmatrix} e^{-\frac{i}{\hbar}\lambda_1 t} & & 0 \\ & \cdot & \\ & & \cdot \\ 0 & & e^{-\frac{i}{\hbar}\lambda_d t} \end{pmatrix} \begin{pmatrix} a_0 \\ \cdot \\ \cdot \\ a_d \end{pmatrix} = U(t)\big|\psi(0)\big\rangle$$

In this basis, $U(t)$ is diagonal.

4 Quantum Gates

We already had some simple examples of unitary transforms, or "quantum gates". Here are most of the common ones you will encounter.

4.1 One-qubit gates:

- Hadamard Gate.

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

$$\begin{aligned} H|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= |+\rangle \\ H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= |-\rangle \end{aligned}$$

The Hadamard Gate is one of the most important gates. Note that $H^\dagger = H$ – since H is real and symmetric – and $H^2 = I$.

In the complex plane H can be visualized as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

On the Bloch sphere H can also be visualized in several ways. One is a rotation of $\pi/2$ about the y-axis, followed by reflection in the x-y plane (see Nielsen and Chuang, p.). Another is a rotation of π about the axis $(1/\sqrt{2}, 0, 1/\sqrt{2})$ (Benenti, p. 111).

Note the action of H on larger number of qubits:

$$\begin{aligned} H \otimes H|00\rangle \equiv H^{\otimes 2}|00\rangle &= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{\sqrt{2^2}} \\ H^{\otimes n}|00.....0_n\rangle &= \tfrac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned}$$

Thus $H^{\otimes n}$ produces an equal superposition of *all* computational basis states.

- Rotation Gate. This rotates in the complex plane by θ.

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- NOT Gate, also known as bit flip gate, or X (Pauli X). This flips a bit from 0 to 1 and vice versa.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip, also known as Z (Pauli Z).

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

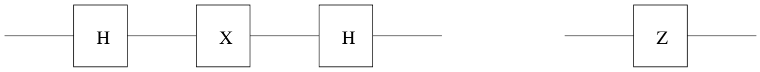
t


Figure 1: An X rotation conjugated by H gates is a Z rotation

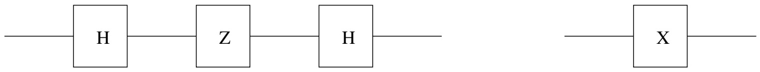
b


Figure 2: A Z rotation conjugated by H gates is an X rotation.

- General Phase Gate, $R_z(\delta)$.

$$R_z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix}$$

Clearly $Z = R_z(\pi)$. There are several other special phase gates that are commonly used: $S = R_z(\pi/2)$, $T =_z (\pi/4)$. The latter is sometimes referred to as the $\pi/8$ gate.

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T \equiv \pi/8 = \begin{pmatrix} 0 & 1 \\ 1 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

- Phaseflips and bitflips are related by conjugation

Conjugation of X by H means premultiplying X by H^{-1} and postmultiplying it by H. But $H = H^{-1}$.

Claim: $HXH = Z$. See Figure 1.

We can prove this by multiplying out the matrices, or by making use of the decomposition of H into an X and a Z gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left[\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right] = \frac{X+Z}{\sqrt{2}}$$

Then $\left(\frac{X+Z}{\sqrt{2}}\right) X \left(\frac{X+Z}{\sqrt{2}}\right) =$

$$\left[\frac{X+Z}{\sqrt{2}}\right] \left[\frac{X^2+XZ}{\sqrt{2}}\right] =$$

$$\left[\frac{X+Z}{\sqrt{2}}\right] \left[\frac{I+XZ}{\sqrt{2}}\right] =$$

$$\frac{XI+XXZ+ZI+ZXZ}{2} =$$

$$\frac{X+Z+Z+-X}{2} =$$

$$\frac{2Z}{2} = Z$$

Conversely, $HZH = X$ (Figure 2). Prove this for yourself.

- Any unitary operation on a single qubit can be constructed with various combinations of gates:

$H, R_z(\delta)$, e.g.,

$$R_z(\pi/2+\phi) H R_z(\theta) H |0\rangle = e^{i\theta/2} \left(\cos\theta/2 |0\rangle + e^{i\phi} \sin\theta/2 |1\rangle\right)$$

$H, X, T = R_z(\pi/4)$

X, Y, Z (Euler rotations)

4.2 Two-qubit gates:

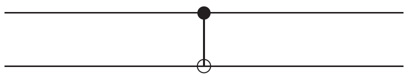
- Any one-qubit gate can be tensored with itself or another gate to make a two-qubit gate, as done above for $H \otimes H$. Such tensor products of one-qubit gates have no ability to generate entanglement and are referred to as 'local' gates.

- Controlled Not (CNOT).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

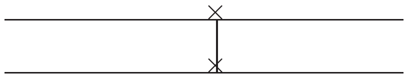
  The first bit of a CNOT gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

  The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



  Note that $(CNOT)^2 = 1$, i.e.,$CNOT^{-1} = CNOT$.

- SWAP



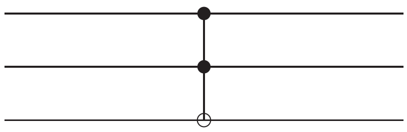
$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

4.3 n-qubit gates:

- local n-qubit gates formed as tensor products of one-qubit gates, e.g., $H^{\otimes n}$

- Toffoli gate

  This is a 3-qubit generalization of the CNOT gate. The third, target, qubit is flipped iff both the first and second qubits are in state 1. $Toff^2 = 1$.



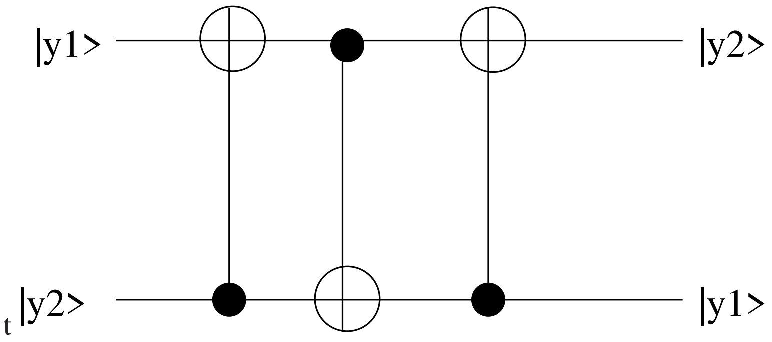
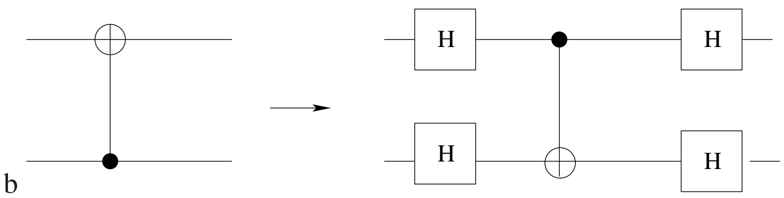


Figure 3: A *Swap* gate is three back to back *CNot* gates with control and target qubits alternating.



The Toffoli gate can be decomposed into a combination of one-qubit and two-qubit gates (Benenti, p. 121).

4.4 Useful gate equivalences

- Swap equals 3 x CNOT

  See Figure 3.

  Suppose we have two qubits in state $|y_2, y_1\rangle$:

  $$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix}$$
  $$= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$$

  Apply the first *CNot*:

  $$ac|00\rangle + ad|01\rangle + bd|10\rangle + bc|11\rangle$$

  Apply the second *CNot*:

  $$ac|00\rangle + bc|01\rangle + bd|10\rangle + ad|11\rangle$$

  Apply the third *CNot*:

  $$ac|00\rangle + bc|01\rangle + ad|10\rangle + bd|11\rangle$$
  $$= ca|00\rangle + cb|01\rangle + da|10\rangle + db|11\rangle$$
  $$= \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix}$$

  The resulting state is $|y_1, y_2\rangle$, i.e., the states of the two qubits have been swapped.

- Control and target of *CNOT* can be swapped by conjugating both qubits with *H*

  See Figure 4.

  Proof: see homework 2.

5 Universality of Gate Sets

5.1 Classical

The NAND gate is universal for classical computation.

For any boolean function $\{0,1\}^n \longrightarrow \{0,1\}$, there is a circuit built of NAND gates (possibly with fan-out = copy) for that function. Note that neither of these gates are reversible.

In general, the circuit may require an exponential number 2^n of gates. Functions which can be efficiently evaluated require only a polynomial number n^c gates. Complexity theory categorizes the scaling of the resources, esp. the number of gates, with the number of bits n. Provided the gate set is universal, the distinction between functions which require exponentially large circuits and those which can be computed with polynomial-size circuits does not depend on the chosen set of gates.

5.2 Quantum

A set G of quantum gates is called universal if for any $\varepsilon > 0$ and any unitary matrix U on n qubits, there is a sequence of gates $g_1, \ldots, g_l$ from G such that $\|U - U_{g_l} \cdots U_{g_2} U_{g_1}\| \leq \varepsilon$.

Here U_g is $V \otimes I$, where V is the unitary transformation on k qubits operated on by the quantum gate g, and I is the identity acting on the remaining $n-k$ qubits. The operator norm is defined by $\|U - U'\| = \max_{|v\rangle \text{unit vector}} \|(U-U')|v\rangle\|$. (Recall that for a vector w, $\|w\| = \sqrt{\langle w|w\rangle}$.)

Examples of universal gate sets include

- CNOT and all single qubit gates
- CNOT, Hadamard, and suitable phase flips
- CNOT, Hadamard, X and T ($\pi/8$)
- Toffoli and Hadamard