1 Readings

Benenti, Casati, and Strini:
Classical circuits and computation Ch. 1.2, 2.6
Quantum Gates Ch. 3.2-3.4

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 $\mathbb{C}^2$,

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

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 columns of $U$ form an orthonormal basis.
- $U$ preserves inner products, i.e. $(\vec{v},\vec{w}) = (U\vec{v},U\vec{w})$. Indeed, $(U\vec{v},U\vec{w}) = (U|\vec{v}\rangle)^\dagger U|\vec{w}\rangle = \langle \vec{v}|U^\dagger U|\vec{w}\rangle = \langle \vec{v}|\vec{w}\rangle$. 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

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

3 Schrödinger’s Equation

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

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H |\psi\rangle.$$
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 $\lambda_i$: $H|\phi_i\rangle = \lambda_i|\phi_i\rangle$.

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 $H$:

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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

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

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.
  
  \[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]

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

  \[ H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \]

  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 \( \pi \) about the axis \( (1/\sqrt{2}, 0, 1/\sqrt{2}) \) (Benenti, p. 111).

  Note the action of \( H \) on larger number of qubits:

  \[ H \otimes H |00\rangle = H^\otimes 2 |00\rangle = |00\rangle + |01\rangle + |10\rangle + |11\rangle \]

  \[ H^\otimes n |00...0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \]

  Thus \( H^\otimes n \) produces an equal superposition of all computational basis states.

- Rotation Gate. This rotates in the complex plane by \( \theta \).

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

- 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 \( Z|-\rangle = |+\rangle \).

- General Phase Gate, \( R_x(\delta) \).

  \[ R_x(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \]

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

  \[ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \pi/8 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix} \]
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

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

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

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

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

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.,

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

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

$X, Y, Z$ (Euler rotations)