Quantum Gates

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

Pauli-X $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

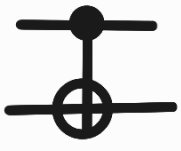
Pauli-Y $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

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

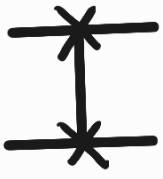
Phase $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

$\frac{\pi}{8}$ $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

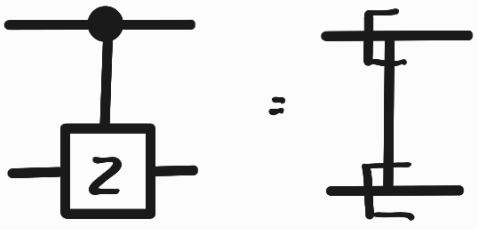
Circuit symbol



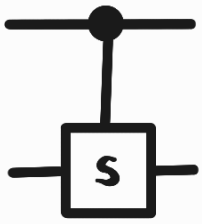
controlled-NOT $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$



swap $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

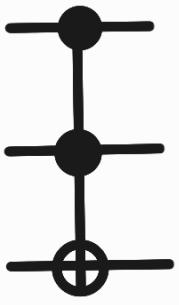


controlled-Z $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$



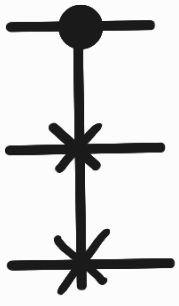
controlled-phase

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$



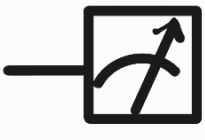
Toffoli

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$



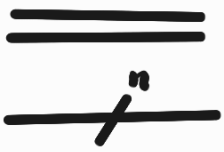
Fredkin
(controlled-swap)

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



measurement — Projection onto $|0\rangle$ and $|1\rangle$

qubit — wire carrying a single qubit (time goes left to right)



classical bit — wire carrying a single classical bit

n qubits — wire carrying n qubits

Notation

$|\psi\rangle$ is a vector of a vector space V (Ket)

$\langle\psi|$ is a vector dual to $|\psi\rangle$ (bra)

$\langle\varphi|\psi\rangle$ is an inner product of $|\varphi\rangle$ and $|\psi\rangle$

$|\varphi\rangle \otimes |\psi\rangle$ is a tensor product of $|\varphi\rangle$ and $|\psi\rangle$. We may abreviate to $|\varphi\rangle|\psi\rangle$

0 is the zero vector, such that $|\psi\rangle + 0 = |\psi\rangle$

$|0\rangle$ is a 0 qubit $\begin{bmatrix}1\\0\end{bmatrix}$

$|1\rangle$ is a 1 qubit $\begin{bmatrix}0\\1\end{bmatrix}$

z^* is a conjugate of z, with $z \in \mathbb{C}$

A^* is a conjungate of a matriz A, with $A \subseteq C^n$

A^T is a transpose of A

$A^\dagger$ is a Hermition conjugate or adjoint of A, such that $A^\dagger = (A^T)^*$

$\langle\psi|A|\psi\rangle$ inner product between $|\psi\rangle$ and $A|\psi\rangle$, equivalently, inner product between $A^\dagger|\psi\rangle$ and $|\psi\rangle$

- A **spanning set** for a vector space is a set of vectors $|v_1\rangle, \dots, |v_n\rangle$, such that any vector $|v\rangle$ in the vector space V can be written as a linear combination $|v\rangle = \sum_i a_i |v_i\rangle$
- A **linear operator** is a function $A: V \longrightarrow W$, such that

$$A\left(\sum_i \alpha_i |v_i\rangle\right) = \sum_i \alpha_i A|v_i\rangle$$

- $I_V\ |v\rangle \equiv |v\rangle$ is the identity operator
  to indicates the vector space we are referring to.
- A **composition** BA is a function composition defined as

$$BA|v\rangle = B(A|v\rangle)$$

Notice that for V, W, X being vector spaces, $A: V \longrightarrow W$ and $B: W \longrightarrow X$. This is important to consider when we make a composition of functions.

- Suppose $A: V \longrightarrow W$, $(|v_1\rangle, \dots, |v_m\rangle)$ a basis for V and $(|w_1\rangle, \dots, |w_n\rangle)$

a basis for W. Then, lets define

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle$$

- The **Pauli Matrices** are important transformations to know about:

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Probability Theory

- A **random variable** X may take one of a number of values x with probabilities $p(X=x)$.

$p(x) \equiv p(X=x)$ (implicit)

- The **conditional probability** that $Y=y$ given that $X=x$ is defined by

$$p(Y=y|X=x) = \frac{p(X=x, Y=y)}{p(X=x)},$$

in which $p(X=x, Y=y)$ is the probability of $X=x$ and $Y=y$. It is important to note that when $p(X=x) \neq 0$, $p(Y=y|X=x) \neq 0$.

- Random variables X and Y are said to be **independent** if $p(X=x, Y=y) = p(X=x)p(Y=y)$, $\forall x, y$

It follows that $p(y|x) = p(y)$

- **Bayes' rule** relates the conditional probabilities for y given X to those for X given Y, such that

$$p(x|y) = p(y|x)\frac{p(x)}{p(y)}$$

• the law of total probability states that for any partion $\{B_1, \dots, B_n\}$ of a sample space Ω, and for any event A in Ω,

$$p(y) = \sum_x p(y|x)p(x)$$

• The expectation, average or mean of a random variable X is defined by

$$E(X) \equiv \sum_x p(x)x$$

A.1.3?

$\exists x \geq E(x) \quad p(x) > 0$

Let X be a random variable , such that $0 \leq p(x_i) \leq 1$ and

$E(X) = x_1 p(x_1) + \dots + x_n p(x_n)$

By definition, $\sum p(x_i) = 1$, with $i \in [1, n]$. So, for every $x_i \; p(x_i) \leq x_i$

Then,

$x_1 p(x_1) + x_2 p(x_2) + \dots + x_n p(x_n)$

Suppose $p(x_n) = 1$, then $p(x_i)$, with $i \in [1, n)$ is equal 0, then

$x_n p(x_n) \leq x_n$

If $0 \leq p(x_n) \leq 1$

$x_1 p(x_1) + \dots + x_n p(x_n) \leq$

A.1.6.?

• $E(XY) = \sum x_i y_i \; p(x_i, y_i)$

$= \sum x_i y_i \; p(x_i) \cdot p(y_i)$

$= x_1 y_1 \; p(x_1) p(y_1) + \dots + x_n y_n \; p(x_n) p(y_n)$

$(x_1 p(x_1) + \dots + x_n p(x_n)) (y_1 p(y_1) + \dots + y_n p(y_n))$

Groups

A group $(G, \cdot)$ is non-empty set G with a binary group multiplication operation '$\cdot$', such that:

1. Closure $g_1 \cdot g_2 \in G, \; \forall g_1, g_2 \in G$

2. Associativity $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$, $\forall g_1, g_2, g_3 \in G$

3. Identity $\exists e \in G$, $\forall g \in G$ $g \cdot e = e \cdot g = g$.

4. Inverses $\forall g \in G$, $\exists g^{-1} \in G$, $g \cdot g^{-1} = e$ e $g^{-1} \cdot g = e$.

* A group is Abelian if $g_1 g_2 = g_2 g_1$, $\forall g_1, g_2 \in G$.

Example:

finite

Z_n is the group of integers modulo n.

Abelian group

- A group G is finite if the number of elements in G is finite.
- The order of a finite group G is the number of elements it contains, denoted as $|G|$.
- The order of an element $g \in G$ is the smallest positive integer r such that g^r (g multiplied with itself r times) equals the identity element e.
- A Subgroup H of G is a subset of G which forms a group under the same group multiplication operation as G.

Theorem: If H is a subgroup of a finite group G then $|H|$ divides $|G|$. (Lagrange's theorem)

G, H

↳ $g_1 \cdot g_2 \in G$, $\forall g_1, g_2 \in G$

↳ $(g_1 \cdot g_2) g_3 = g_1 (g_2 g_3)$, $\forall g_1, g_2, g_3 \in G$

↳ Identity, $\exists e \in G : g \cdot e = e g = g$, $\forall g \in G$

↳ Inverse, $\exists g^{-1} \in G : g g^{-1} = g^{-1} g = e$, $\forall g \in G$

divide? inversion of $\cdot$?

$|G|$ → order

$|H| = 0 \pmod{|G|}$ ✓

$\exists p \in G : p \cdot |H| = |G|$

• In finite dimensional complex vector spaces, a Hilbert space is the same thing as an inner product space.

• Let $|v\rangle$ and $|u\rangle$ be vectors in the vector space V. They are orthogonal if their inner product is zero.

• A norm of a vector $|v\rangle$ in V is defined as

$$\||v\rangle\| \equiv \sqrt{\langle v|v\rangle}$$

$\langle \cdot | \cdot \rangle \rightarrow$ inner product

• An unit vector is a vector $|v\rangle$ such that $\||v\rangle\| = 1$

• We can normalize a non-zero vector $|v\rangle$, diving it by its norm, that is, $\frac{|v\rangle}{\||v\rangle\|}$

• A set $|i\rangle$ of vectors with index i is orthonormal if each vector is a unit vector, and distinct vectors in the set are orthogonal, that is, $\langle i|j\rangle = \delta_{ij}$, with i and j chosen from the index set.

• An eigenvector of a linear operator A on a vector space is a non-zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$, in which v is a complex number known as the eigenvalue of A corresponding to $|v\rangle$.

* Use the characteristic function, defined to be

$\rightarrow$ determinant function

$$c(\lambda) = \det|A - \lambda I|$$

$\rightarrow$ root

The solutions to the equation, that is, $c(\lambda) = 0$ give us the eigenvalues of the operator A.

• A diagonal representation for an operator A on a vector space V is a representation $A = \sum_i \lambda_i |i\rangle\langle i|$, where the vectors $|i\rangle$ form an orthonormal set of eigenvectors for A, with corresponding eigenvalues λ_i.

* Diagonal representations are sometimes also known as orthonormal decompositions.

* When an eigenspace is more than one dimensional we say that it is degenerate.

• Let A be a linear operator on a Hilbert space V. There exist a

unique linear operator A^* on V such that for all vectors $|v\rangle, |w\rangle \in V$

$$(|v\rangle, A|w\rangle) = (A^*|v\rangle, |w\rangle)$$

We call A^* adjoin or Hermitian conjugate

Attention: $|v\rangle^* = \langle v|$

- An operator A is said to be normal if $AA^* = A^*A$.
  - An Hermitian operator is also normal
- An operator A on a complex inner product space is called Hermitian if for every vector u and v in the inner product space

$$\langle Au, v\rangle = \langle u, Av\rangle^*$$ → complex conjugate

- A inner product space is a vector space V over the field of complex numbers, such that there is a function $\langle \cdot, \cdot \rangle$, which satisfies
  1. $\forall u, v, w \in V, \langle \alpha u + \beta v, w\rangle = \alpha \langle u, w\rangle + \beta \langle v, w\rangle$
  2. $\forall u, v \in V, \langle u, v\rangle = \langle v, u\rangle^*$
  3. $\forall u \in V, \langle u, u\rangle \geq 0$
  4. $\forall v \in V$, if $\langle u, v\rangle = 0$, then $u = 0$
- A matrix U is said to be unitary if $U^*U = I$.

An operator A

- For an operator A, if A is unitary $A^*A = AA^* = I$, then A is normal and has spectral decomposition.

Theorem: (Spectral decomposition) Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.

- the tensor product of $V \otimes W$ ("V tensor W") is an mn dimensional vector space.

Notation: $|v\rangle|w\rangle$, $|v, w\rangle$ or $|vw\rangle$ for abbriviation of $v \otimes w$

It satisfies the following properties:

1. For every scalar z, $|v\rangle$ of V and $|w\rangle$ of W

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle)$$

2. For every $|v_1\rangle$ and $|v_2\rangle$ in V and $|w\rangle$ in W

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

3. For every $|v\rangle$ in V and $|w_1\rangle$ and $|w_2\rangle$ in W

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

Quantum circuits

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S := \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad T := \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}$$

↳ π/8 gate

* $H = \frac{(X+Z)}{\sqrt{2}}$ and $S = T^2$

• A qubit $|\varphi\rangle = a|0\rangle + b|1\rangle$ can be visualized as a point (θ, φ) on the unit sphere, which $a = \cos(\theta/2)$ $b = e^{i\varphi}\sin(\theta/2)$

↳ Bloch sphere

↳ real