Quantum Computing

Muchang Bahng

Spring 2024

Contents

1 Introduction

In quantum mechanics we usually work in a Hilbert space V over field $\mathbb{C}$. A **ket** is of the form $|v\rangle$, which mathematically denotes a vector v in V. A **bra** is of the form $\langle f|$, which denotes a covector $f \in V^*$, the dual space. With the usual construction of the canonical isomorphism between a Hilbert space and its dual, we say if $|m\rangle$ defines a column vector in $\mathbb{C}^n$, then $\langle m|$ is its conjugate transpose. Furthermore, let us write the shorthand notation for the classical bit as such:

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

When can represent a set of classical bits as the tensor product, which is realized as simply the outer product. For a system of two bits, we have

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

We can take our familiar logic gates and represent them as matrix operations. For example, the `NOT` gate, which flips the state of the bit, can be represented as

$$N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and the `CNOT` gate, which takes gate, which takes two bits and flips the state of the second bit if the first is a $|0\rangle$ and does nothing otherwise, can be represented as

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \implies \begin{cases} C\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = C \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |01\rangle \\ \ldots \\ C\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = C \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |10\rangle \end{cases}$$

We describe the basic postulates of quantum mechanics, which provide a connection between the physical world and the mathematical formalism of quantum mechanics.

Theorem 1.1. The first postulate:

- *Associated to any isolated physical system is a Hilbert space (a complex inner product space) known as the* ***state space*** *of the system. The system is completely described by its* ***state vector****, which is a unit vector in the system's state space.*

This postulate is quite intuitive, since in Lagrangian mechanics we use the familiar configuration manifold to model the state of a system, and by Whitney's embedding theorem every manifold can be embedded in a sufficiently high-dimensional vector space. But QM does not tell us what the state space of that system is, nor does it tell us what the state vector of that system is. Figuring it out for a specific system is done independently with rules that physicists have developed. The simplest quantum mechanical system is the qubit, which has a two complex-dimensional state space (the unit sphere in $\mathbb{C}^2$) with $|0\rangle, |1\rangle$ forming an orthonormal basis for that state space. We also have the normalization condition that $\langle \psi | \psi \rangle = 1$, i.e. $|\psi\rangle$ is a unit vector.

Theorem 1.2. The second postulate comes in two forms: The first form describes how the quantum states of a closed system at two different times are related. The second form is a refinement and a generalization of the first which describes the evolution of a quantum system in continuous time.

- *The evolution of a closed quantum system is described by a unitary transformation in $U(n)$. That is, the state of the system $|\psi\rangle$ at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2.*

  $$|\psi'\rangle = U\,|\psi\rangle$$

- *The time evolution of a closed quantum system is described by the* ***Schrodinger equation***

  $$i\hbar \frac{d|\psi\rangle}{dt} = \hat{H}|\psi\rangle,$$

  an ordinary differential equation with solution $|\psi\rangle(t)$ ($|\psi\rangle : \mathbb{R}_t \longrightarrow \mathbb{C}^n$, the Hilbert space). Where $\hbar$ is Planck's constant and $\hat{H}$ is a fixed Hermitian operator called the **Hamiltonian** of the closed system. Note that because H is self-adjoint, it has the spectral decomposition

  $$H = \sum_E E\,|E\rangle\langle E|$$

  with eigenvalues E and corresponding normalized eigenvectors $|E\rangle$. The eigenvectors $|E\rangle$ are called **energy eigenstates** with the energy of the state being E. The minimum energy and energy eigenstate is known as the **ground state energy** and **ground state**, respectively.

Abstractly, we can visualize the evolution of a quantum system as a point traversing through a unit sphere in some complex vector space. In general finding out the Hamiltonian of a system is a very difficult problem, but we will assume that it is given in our context. Furthermore, for systems that are under the experimentalist's control and which may be changed, a **time-varying Hamiltonian** may be used to describe the quantum system. The connection between these two forms can be seen when writing down the solution to Schrodinger's equation (with initial time value t_1 and its initial state vector $|\psi(t_1)\rangle$), which is easily verified to be:

$$\begin{aligned} |\psi(t_2)\rangle &= \exp\left(\frac{-i\hat{H}(t_2 - t_1)}{\hbar}\right)|\psi(t_1)\rangle \\ &= U(t_1, t_2)\,|\psi(t_1)\rangle \end{aligned}$$

We can see that $\frac{-i\hat{H}(t_2-t_1)}{\hbar}$ is in the Lie algebra $\mathfrak{u}(2)$, which is mapped to the Lie group $\mathrm{U}(2)$ through the exponential map $\exp : \mathfrak{u}(2) \longrightarrow \mathrm{U}(2)$. In other words we are describing a homotopy: smoothly changing t_2 smoothly changes $U(t_1, t_2)$ within $\mathrm{U}(2)$, which itself is a function $|\psi(t_1)\rangle \mapsto |\psi(t_2)\rangle$ from one state to another.

Theorem 1.3. We have postulated that closed quantum systems evolve according to unitary evolution. The evolution of systems which don't interact with the rest of the world is all very well, but there must also be times when the experimenter and their experimental equipment (i.e., an external physical system) observe the system to find out what is going on inside the system. This observation is an interaction with the system, making the system not closed, and thus not subject to unitary evolution. The effects of measurements done on quantum systems can be described with postulate 3, and in here let us remind the reader that a measurement outcome is *different* than the state of a quantum system (e.g., the state space of a qubit is the complex 2-sphere, while the measurement outcomes can be 0 or 1).

- *Let the total number of measurement outcomes of a quantum system be parameterized by m. Then, a quantum measurement is described by a collection $\{M_m\}$ of* ***measurement operators*** *(acting on the state space) satisfying the completeness equation*

  $$\sum_m M_m^\dagger M_m = I$$

If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability that result m occurs is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

Immediately after this measurement outcome m, the state of the system then becomes

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$$

Note that clearly, the completeness equation implies

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle$$

A point to make: Measuring devices are quantum mechanical systems, so the quantum system being measured and the measuring device together are part of a larger, isolated, quantum mechanical system which, according to postulate 2, undergoes evolution through a unitary operator. Whether postulate 3 can be derived by postulate 2 is debated today. As an example, suppose that we have the simple quantum system consisting of a single qubit that has the state $|\psi\rangle = a|0\rangle + b|1\rangle$ immediately before measurement

$$\{M_0, M_1\} = \left\{ \begin{pmatrix} 0.8 & 0 \\ 0 & 0.6 \end{pmatrix}, \begin{pmatrix} 0.6 & 0 \\ 0 & 0.8 \end{pmatrix} \right\}$$

which clearly satisfies the completeness equation $M_0^\dagger M_0 + M_1^\dagger M_1 = I$, has probabilities

- $p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = 0.64a^2 + 0.36b^2$ chance of a measurement outcome of 0
- $p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = 0.36a^2 + 0.64b^2$ chance of a measurement outcome of 1

If we observe a measurement of 0 in the system, then the state vector of the quantum system would be

$$\frac{M_0|\psi\rangle}{\sqrt{\langle\psi|M_0^\dagger M_0|\psi\rangle}} = \frac{1}{\sqrt{0.64a^2 + 0.36b^2}} \begin{pmatrix} 0.8a \\ 0.6b \end{pmatrix} = \frac{0.8a}{\sqrt{0.64a^2 + 0.36b^2}}|0\rangle + \frac{0.6b}{\sqrt{0.64a^2 + 0.36b^2}}|1\rangle$$

and if we observe an outcome of 1, then the state vector of the system would be

$$\frac{M_1|\psi\rangle}{\sqrt{\langle\psi|M_1^\dagger M_1|\psi\rangle}} = \frac{1}{\sqrt{0.36a^2 + 0.64b^2}} \begin{pmatrix} 0.6a \\ 0.8b \end{pmatrix} = \frac{0.6a}{\sqrt{0.36a^2 + 0.64b^2}}|0\rangle + \frac{0.8b}{\sqrt{0.36a^2 + 0.64b^2}}|1\rangle$$

A following theorem is that a composition of measurements, e.g., $\{L_l\}$ followed by a separate $\{M_m\}$ is physically equivalent to a single measurement defined by measurement operators $\{N_{lm}\}$ with the representation $N_{lm} = M_m L_l$.

Projective Measurements

We have defined a measurement as a collection $\{M_m\}$ of operators satisfying the completeness equation. The majority of cases that we will be interested in are **projective measurements**. To introduce this, recall a few facts from linear algebra:

1. Every Hermitian (self-adjoint) operator M has an eigendecomposition of orthogonal eigenspaces

   $$M = \sum_m \lambda_m P_m$$

   where each P_m is an orthogonal projection operator, and the λ_m is the eigenvalue corresponding to the mth eigenspace of M. The eigenspaces may have multiple dimensions, but M can be diagonalized, i.e., decomposed into a collection of 1-dimensional eigenspaces (some having the same eigenvalue).

2. A projection map P is a linear map if and only if $P = P^2$.
3. If P is a projection map, it is an orthogonal projection if and only if P is Hermitian (self-adjoint).
4. If $\{|u_1\rangle, |u_2\rangle, \ldots, |u_n\rangle\}$ are an orthonormal basis for $\mathbb{C}^n$, then

$$A = \sum_i |u_i\rangle\langle u_i| = I_n$$

since $A|u_i\rangle = |u_i\rangle$ for each i and therefore by linearity it must be the identity.

Now, we can state postulate 3 in terms of projective measurements. The following statements are all equivalent:

- A projective quantum measurement is described by a collection $\{P_m\}$ of measurement operators that are orthogonal/Hermitian projectors satisfying the completeness equation (which can be simplified using the linear algebra properties above):

$$\sum_m P_m^\dagger P_m = \sum_m P_m^2 = \sum_m P_m = I$$

- A projective quantum measurement is described by an **observable** M, a Hermitian operator on the state space with the spectral decomposition

$$M = \sum_m m P_m$$

such that the P_m's satisfy the completeness equation.

- A quantum measurement "in an orthonormal basis $|m\rangle$" means to conduct a projective measurement with projectors $P_m = |m\rangle\langle m|$. This is equivalent to the two above because given two orthonormal vectors $|m\rangle, |m'\rangle$, we have

$$P_{m'} P_m = |m'\rangle\langle m'|m\rangle\langle m| = \begin{cases} 0 & m' \neq m \\ |m\rangle\langle m| = P_m & m' = m \end{cases}$$

which implies that P_m is projective. Since P_m is the outer product of two identical vectors it is clearly Hermitian, and therefore P_m is an orthogonal projection. Furthermore, by the linear algebra result above we can see that the $P_m = |m\rangle\langle m|$ satisfies the completeness equation.

This formulation simplifies calculations. Upon measuring the state $|\psi\rangle$, the probability of getting result m is

$$p(m) = \langle\psi|P_m^\dagger P_m|\psi\rangle = \langle\psi|P_m|\psi\rangle$$

Given that outcome m occurred, the state of the quantum system immediately after measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$$

When we conduct a measurement of some quantum system, we can interpret M in two very similar and connected ways:

- M, the observable, is a Hermitian operator that decomposes into the projectors P_m that determines the probabilities $p(m)$ of result m occurring.
- M is a random variable that generates an m representative of an element in the outcome space, following some multinomial probability density $p(m)$ when we measure the system.

Interpreting M as this random variable, the expected measurement outcome is:

$$\begin{aligned}\mathbb{E}(M) &= \sum_m m\, p(m) \\ &= \sum_m m\langle\psi|P_m|\psi\rangle \\ &= \langle\psi|\bigg(\sum_m mP_m\bigg)|\psi\rangle \\ &= \langle\psi|M|\psi\rangle \equiv \langle M\rangle\end{aligned}$$

with variance

$$\begin{aligned}\big(\Delta(M)\big)^2 &= \langle(M-\langle M\rangle)^2\rangle \\ &= \langle M^2\rangle - \langle M\rangle^2\end{aligned}$$

For example, let us have a 1-qubit quantum system that is in the state

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}$$

and we (projectively) observe it with the Pauli-Z operator. We can calculate it to have eigenvalue $+1$ with eigenvector $|0\rangle$ and eigenvalue -1 with eigenvector $|1\rangle$. The decomposition of Z into its projective maps is

$$\begin{aligned}Z &= (+1)\,P_{+1} + (-1)\,P_{-1} \\ &= (+1)\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + (-1)\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\end{aligned}$$

and so the probability of getting a measurement of $+1$ or -1 is

$$\begin{aligned}p(+1) = \langle\psi|P_{+1}|\psi\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{2} \\ p(-1) = \langle\psi|P_{-1}|\psi\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix} = \frac{1}{2}\end{aligned}$$

Distinguishing Quantum States

One interesting property of measurements arises when **distinguishing quantum states**. In short, it turns out that if we are trying to find out whether a quantum system is in state A or state B, it is possible to find out by measuring it if and only if A and B are orthogonal (i.e., orthonormal since state vectors are unit vectors). Elaborating on this, let us have a quantum system with some mystery state vector that is chosen from a set of states $\{|\psi_i\rangle\}_{i=1}^n$. For the sake of explanation, we will say that this mystery state vector is $|\psi_k\rangle$, with $1 \leq i = k \leq n$ (but remember that this is not actually known). Is it possible to measure the system so that we can correctly identify the correct state $|\psi_k\rangle$ from the $|\psi_i\rangle$'s, i.e., find the value $i = k$?

- If all the $|\psi_i\rangle$'s are orthonormal, then this is possible. We define measurement operators $M_i \equiv |\psi_i\rangle\langle\psi_i|$ for $i = 1, \ldots, n$, a final operator

  $$M_0 = \sqrt{I - \sum_{i\neq 0}|\psi_i\rangle\langle\psi_i|}$$

  These operators $\{M_i\}$ satisfy the completeness equation, and since

  $$p(i) \equiv \langle\psi_k|M_i|\psi_k\rangle = \langle\psi_k|\psi_i\rangle\langle\psi_i|\psi_k\rangle = \begin{cases}1 & i = k\\ 0 & i \neq k\end{cases}$$

  all we have to do is observe the system according to set $\{M_i\}$, which will give the outcome $i = k$ with probability 1.

- If the $|\psi_i\rangle$'s aren't orthonormal, then there is some nonzero probability that the system may be in another state, and we cannot determine for sure the index k of $|\psi_k\rangle$.

POVM Measurements

The measurement postulate involves two elements: the probabilities of the measurement outcomes and the post-measurement state of the system. When we are concerned with only the probabilities (e.g., in the case of an experiment where the system is measured only once), it is useful to employ the POVM formalism. Suppose a measurement described by measurement operators M_m is performed upon a quantum system in the state $|\psi\rangle$. Then, the probability of outcome m is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle.$$

We now define

$$E_m \equiv M_m^\dagger M_m$$

to be the **POVM elements** associated with the measurement, and the complete set $\{E_m\}$ to be the **POVM**. Some linear algebra reveals that E_m must be positive-definite, the POVM is sufficient to completely determine the probabilities of the different measurement outcomes.

For a projective measurement described by measurement operators P_m, we can see that they are equal to the POVM elements since $E_m \equiv P_m^\dagger P_m = P_m$.

We have seen that the existence of a set of measurement operators $\{M_m\}$ satisfying the completeness equation automatically implies the existence of the POVM $\{E_M\}$ consisting of positive operators satisfying $\sum_m E_m = I$:

$$\{M_m\} \longrightarrow \{E_m\}.$$

Going backwards, we claim that the existence of an arbitrary set of positive operators $\{E_M\}$ satisfying $\sum_m E_m = I$ implies the existence of measurement operators $\{M_m\}$ defining a measurement described by the POVM. We simply define $M_m \equiv \sqrt{E_m}$, which we can do since E_m is positive (define a new linear map with the same eigenspaces but square root of eigenvalues; more info here).

$$\{M_m\} \longleftrightarrow \{E_m\}.$$

The applicability of POVMs is demonstrated in the following example: Suppose a qubit is in one of two states: $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = (|0\rangle + |1\rangle)/2$. Since these qubits are not orthonormal, we cannot determine the state with 100% accuracy. However, it is possible for us to perform a measurement that distinguishes the states sometimes, but never makes an error of identification. We can construct a POVM of three elements as such:

$$\begin{aligned}
E_1 &\equiv \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1| = \frac{\sqrt{2}}{1+\sqrt{2}}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \\
E_2 &\equiv \frac{\sqrt{2}}{2+2\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \\
E_3 &\equiv I - E_1 - E_2.
\end{aligned}$$

It can be checked that these sum up to I and are positive definite. If the actual state of the system was $|\psi_1\rangle$, then we have

$$\begin{aligned}
p(1\,|\,|\psi_1\rangle) &= \langle\psi_1|E_1|\psi_1\rangle = 0, \\
p(2\,|\,|\psi_1\rangle) &= \langle\psi_1|E_2|\psi_1\rangle = \frac{\sqrt{2}}{2+2\sqrt{2}}, \\
p(3\,|\,|\psi_1\rangle) &= \langle\psi_1|E_3|\psi_1\rangle = \frac{2+\sqrt{2}}{2+2\sqrt{2}}.
\end{aligned}$$

And if the actual state of the system was $|\psi_2\rangle$, then we have

$$\begin{aligned} p(1\,|\,|\psi_2\rangle) &= \langle\psi_2|E_1|\psi_2\rangle = \frac{\sqrt{2}}{2+2\sqrt{2}}, \\ p(2\,|\,|\psi_2\rangle) &= \langle\psi_2|E_2|\psi_2\rangle = 0, \\ p(3\,|\,|\psi_2\rangle) &= \langle\psi_2|E_3|\psi_2\rangle = \frac{2+\sqrt{2}}{2+2\sqrt{2}}. \end{aligned}$$

Clearly, we can see that if the measurement outcome yields 1, then the actual state of the system must have been $|\psi_2\rangle$, and if it yields 2, then the actual state must have been $|\psi_1\rangle$. In the case where the outcome is 3, then we would not know, but at least there is no risk of misinterpreting.

Theorem 1.4 (Postulate 4: Composite Systems)**.** If we are interested in a composite quantum system made up of two (or more) distinct physical systems, the states of the composite system can be described as stated in postulate 4:

- *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. That is, if we have systems* $1, \ldots, n$ *with the state vector of the* i*th system being* $|\psi_i\rangle$*, then the joint state of the total system is*

$$\bigotimes_i |\psi_i\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle.$$

A further property of the tensor product of Hilbert spaces is the induced inner product. That is, if H_1 and H_2 are Hilbert spaces with inner products $\langle\cdot,\cdot\rangle_1$ and $\langle\cdot,\cdot\rangle_2$, respectively, then $H_1 \otimes H_2$ is a Hilbert space with an induced inner product

$$\langle v_1 \otimes v_2, w_1 \otimes w_2\rangle \equiv \langle v_1, w_1\rangle_1 \, \langle v_2, w_2\rangle_2$$

for $v_1, w_1 \in H_1,\ v_2, w_2 \in H_2$.

We can now talk about entanglement. A state $|\psi\rangle$ of a composite system that cannot be written as the tensor product of the states of its component systems is said to be in an **entangled state**. A classic example is the 2-qubit entangled state

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle,$$

which cannot be written down as the following product

$$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} &\neq \big(\alpha|0\rangle + \beta|1\rangle\big) \otimes \big(\alpha'|0\rangle + \beta'|1\rangle\big) \\ &= \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle \end{aligned}$$

since this must mean that one of α or β' must be 0. If $\alpha = 0$, then the $|00\rangle$ amplitude must be 0 and if $\beta' = 0$, then the $|11\rangle$ amplitude must be 0, leading to a contradiction.

Heisenberg Uncertainty Principle

Suppose A and B are two Hermitian operators, and $|\psi\rangle$ is a quantum state. Then, by the properties of self-adjoint/Hermitian operators and the skew-symmetricity of the inner product, we have

$$\begin{aligned} \langle\psi|[A,B]|\psi\rangle &= \langle\psi|AB - BA|\psi\rangle \\ &= \langle\psi|AB|\psi\rangle - \langle\psi|BA|\psi\rangle \\ &= \langle\psi|AB|\psi\rangle - \langle A^\dagger B^\dagger \psi|\psi\rangle \\ &= \langle\psi|AB|\psi\rangle - \langle AB\psi|\psi\rangle \\ &= \langle\psi|AB|\psi\rangle - \overline{\langle\psi|AB|\psi\rangle} \\ \langle\psi|\{A,B\}|\psi\rangle &= \langle\psi|AB + BA|\psi\rangle \\ &= \langle\psi|AB|\psi\rangle + \overline{\langle\psi|AB|\psi\rangle} \end{aligned}$$

where $[\cdot,\cdot]$ and $\{\cdot,\cdot\}$ are the commutator and anti-commutator, respectively. Therefore,

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2.$$

By combining the Cauchy-Schwarz inequality

$$|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$$

with the equation above, along with dropping the nonnegative term $|\langle\psi|\{A,B\}|\psi\rangle|^2$, we have

$$|\langle\psi|[A,B]|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle.$$

Suppose C and D are two observables. Substituting $A = C - \langle C\rangle$ and $B = D - \langle D\rangle$ into the last inequality gives **Heisenberg's Uncertainty Principle**, formally stated:

$$\Delta(C)\,\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}.$$

A common misinterpretation of the uncertainty principle is that measuring an observable C to some "accuracy" $\Delta(C)$ causes the value of D to be "disturbed" by an amount $\Delta(D)$ satisfying the inequality above. While it is true that measurements in quantum mechanics cause disturbance to the system being measured, this is not what it states.

The correct interpretation of the uncertainty principle is that if we prepare a large number of quantum systems in identical states $|\psi\rangle$ and then perform measurements of C in some of those systems and of D in others, then the standard deviation $\Delta(C)$ of the C results times the standard deviation $\Delta(D)$ of the results for D will satisfy the inequality.

Qubits & Quantum Circuits

Superposition

The state space of a classical bit is $\{0,1\}$. On the other hand, the state of a **quantum bit**, or a **qubit**, is the 3-dimensional unit sphere in $\mathbb{C}^2$. More specifically, the state of the qubit can be parameterized by two **complex amplitudes** α,β defining a complex unit linear combination, or **superposition**, of the 0 and 1 vectors

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \qquad \alpha,\beta\in\mathbb{C},\ |\alpha|^2+|\beta|^2 = 1.$$

That is, the state of a qubit is a vector in a two-dimensional complex vector space, with the special states $|0\rangle$ and $|1\rangle$ known as **computational basis states** and form an orthonormal basis for this vector space. Quantum mechanics tells us that upon observing this qubit, its state will "collapse" onto a state of 0 or 1, with probabilities determined by **Born's rule**: Given qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$,

$$\begin{aligned}\mathbb{P}(\text{collapse to } 0) &= |\alpha|^2,\\ \mathbb{P}(\text{collapse to } 1) &= |\beta|^2.\end{aligned}$$

Note that this isn't a special "rule" at all. If we make a projective measurement of $M = I$, having decomposition

$$M_1 = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \quad M_2 = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},$$

on this single qubit system with state vector $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we get

$$\begin{aligned}p(0) &= \langle\psi|M_0^\dagger M_0|\psi\rangle = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \overline{\alpha}\alpha = |\alpha|^2,\\ p(1) &= \langle\psi|M_1^\dagger M_1|\psi\rangle = \begin{pmatrix}\overline{\alpha} & \overline{\beta}\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \overline{\beta}\beta = |\beta|^2.\end{aligned}$$

Note again that this strange property of the qubit "being" in a continuum of states until it is observed runs counter to our intuition. Despite this, qubits are decidedly real, and different physical systems can be used to realize qubits.

Measurements With Respect to Other Computational Bases

So far, we have described quantum measurements of a single qubit in the state $\alpha\,|0\rangle + \beta\,|1\rangle$ as yielding the result 0 or 1 and leaving the qubit in the corresponding state $|0\rangle$ or $|1\rangle$ with respective probabilities $|\alpha|^2$ and $|\beta|^2$. However, we can choose another orthonormal computational basis state for a qubit.
For example, we can convert $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in terms of the basis $|+\rangle, |-\rangle$ as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}\,|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|-\rangle$$

with

$$\begin{aligned}\mathbb{P}\big(\text{collapse to } |+\rangle\big) &= \frac{|\alpha+\beta|^2}{2},\\ \mathbb{P}\big(\text{collapse to } |-\rangle\big) &= \frac{|\alpha-\beta|^2}{2}.\end{aligned}$$

More generally, given any orthonormal basis states $|a\rangle, |b\rangle$, it is possible to express an arbitrary state as a linear combination

$$\alpha|a\rangle + \beta|b\rangle$$

of those states, and we can **perform a measurement with respect to the $|a\rangle, |b\rangle$ basis**, giving result a with probability $|\alpha|^2$ and b with probability $|\beta|^2$.

Bloch Sphere: Global & Relative Phase

The unit sphere in $\mathbb{C}^2$ captures the state space of the single qubit in full generality. However, for the sake of visualization and for simplicity, we can reduce it to a quotient space by defining an equivalence relation. Given a quantum system with state vector $|\psi\rangle$ that we observe with measurements $\{M_m\}$, we can see that

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle.$$

Given any $\delta \in \mathbb{R}$, if the state vector is $e^{i\delta}|\psi\rangle$, then we have

$$\begin{aligned}p(m) &= \langle e^{i\delta}\psi|M_m^\dagger M_m|e^{i\delta}\psi\rangle,\\ &= \langle\psi|e^{-i\delta}M_m^\dagger M_m e^{i\delta}|\psi\rangle,\\ &= \langle\psi|M_m^\dagger M_m|\psi\rangle.\end{aligned}$$

Therefore, from an observational point of view, these two states $|\psi\rangle$ and $e^{i\delta}|\psi\rangle$ are identical.
Let's go back to the main discussion. Since $\mathbb{C}^2$ is isomorphic to $\mathbb{R}^4$, we can construct an equivalent representation of $|\psi\rangle$ as a real 3-manifold parameterized as below:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = e^{i\gamma}\bigg(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\bigg), \quad \gamma, \varphi, \theta \in \mathbb{R}.$$

But since $|\psi\rangle$ and $e^{i\delta}|\psi\rangle$ are observationally equivalent, we can construct an equivalence class defined as

$$|\psi\rangle \sim |\phi\rangle \text{ if } \exists\delta \in \mathbb{R} \text{ s.t. } |\psi\rangle = e^{i\delta}|\phi\rangle,$$

which allows us to disregard the **global phase factor** $e^{i\gamma}$ and write $|\psi\rangle$ as

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\,\sin\frac{\theta}{2}\,|1\rangle.$$

This describes the parameterization of a unit 2-sphere, known as the **Bloch sphere**. The other kind of phase is known as the **relative phase factor**. Given two states

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ and } |\psi^*\rangle = \alpha^*|0\rangle + |\beta^*\rangle,$$

if $|\alpha| = |\alpha^*|$ or $|\beta| = |\beta^*|$, then we say that **the amplitudes differ by a relative phase**. Furthermore, two states $|\psi\rangle, |\psi^*\rangle$ are said to **differ by a relative phase in some basis** if each of the amplitudes in that basis is related by such a phase factor.
It is clear that due to Born's rule on this one-qubit system, $|\alpha| = |\alpha^*| \iff |\beta| = |\beta^*|$, and so, all we have to do is check the magnitudes of the $|0\rangle$ amplitudes of two state vectors. Visualizing this on the Bloch sphere, we can see that the θ is the only parameter capable of changing the $|0\rangle$ amplitude. The global phase factor $e^{i\gamma}$ is merely a rotation map and also cannot change the $|0\rangle$. Therefore, we can see that two state vectors differ by a relative phase if and only if they have the same θ value, i.e. if the two points on the Bloch sphere are on the same "latitude."

Notice that if two states are differ by a relative phase, then these phases are observationally equivalent, and so must be similar to the global phase factor. However, the relative phase is basis-dependent and so may produce different probability densities depending on the computational basis, while the global one is basis-independent.

Multiple Qubit Systems

By applying postulate 4, a two-qubit system can be represented in tensor product notation. Let us have qubits $\psi_0 = \alpha_0 |0\rangle + \beta_0 |1\rangle$ and $\psi_1 = \alpha_1 |0\rangle + \beta_1 |1\rangle$. Then, the tensor product notation of the two qubits can be represented as

$$|\psi_0 \psi_1\rangle = \begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix} \otimes \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix},$$

with the important property that

$$|\alpha_0\alpha_1|^2 + |\alpha_0\beta_1|^2 + |\beta_0\alpha_1|^2 + |\beta_0\beta_1|^2 = 1,$$

where

$$\begin{aligned} \mathbb{P}(\text{collapse to } |00\rangle) &= |\alpha_0\alpha_1|^2, \\ \mathbb{P}(\text{collapse to } |01\rangle) &= |\alpha_0\beta_1|^2, \\ \mathbb{P}(\text{collapse to } |10\rangle) &= |\beta_0\alpha_1|^2, \\ \mathbb{P}(\text{collapse to } |11\rangle) &= |\beta_0\beta_1|^2. \end{aligned}$$

But since this tensor product space has the basis

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; |10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

we can represent the two-qubit system more concisely as

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

with the measurement result $x(= 00, 01, 10, 11)$ occurring with probability $|\alpha_x|^2$.

Quantum Logic Gates

Quantum logic gates can be interpreted as matrices that modify the state of qubits. This is similar to those of classical gates, but one key difference between quantum logic gates and classical ones is that quantum gates are always **reversible**, while some classical gates like NAND are irreversible (e.g., if the output of a NAND gate is 1, we don't know if the input is $00, 01$, or 10). We can divide them into classes depending on how many arguments they take, but as we will see, the general form of a quantum gate taking in n input qubits is some unitary matrix in $U(2^n)$.
Three fundamental such gates are precisely the **Pauli matrices** (recall that they are Hermitian and unitary):

- The Pauli X, also called the NOT gate, is simply a rotation by π radians around the x-axis of the Bloch sphere.
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \iff X\big(\alpha|0\rangle + \beta|1\rangle\big) = \beta|0\rangle + \alpha|1\rangle,$$
with normalized eigenvectors
$$\psi_{x+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \psi_{x-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$
which we call the **eigenstates** of the X-gate.

- The Pauli Y is a rotation of π radians around the y-axis.
$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \iff Y\big(\alpha|0\rangle + \beta|1\rangle\big) = -\beta i|0\rangle + \alpha i|1\rangle,$$
with eigenstates
$$\psi_{y+} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad \psi_{y-} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

- The Pauli Z is a rotation of π radians around the z-axis.
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \iff Z\big(\alpha|0\rangle + \beta|1\rangle\big) = \alpha|0\rangle - \beta|1\rangle,$$
with eigenstates
$$\psi_{z+} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \psi_{z-} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$
which is why the Z gate doesn't have any effect on a qubit in either the $|0\rangle$ or $|1\rangle$ state.

These three matrices are very important because it turns out that
$$\frac{1}{2}iX, \frac{1}{2}iY, \frac{1}{2}iZ$$
forms the basis for the Lie algebra $\mathfrak{u}(2)$, which exponentiates to the unitary group $\mathrm{U}(2)$. Therefore, by exponentiating each Pauli matrix, we have

$$\begin{aligned} e^{-i\beta X/2} &= \cos\frac{\beta}{2} I - i \sin\frac{\beta}{2} X = \begin{pmatrix} \cos\frac{\beta}{2} & -i\sin\frac{\beta}{2} \\ -i\sin\frac{\beta}{2} & \cos\frac{\beta}{2} \end{pmatrix}, \\ e^{-i\gamma Y/2} &= \cos\frac{\gamma}{2} I - i \sin\frac{\gamma}{2} Y = \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix}, \\ e^{-i\delta Z/2} &= \cos\frac{\delta}{2} I - i \sin\frac{\delta}{2} Z = \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}. \end{aligned}$$

and so every rotation matrix $U \in \mathrm{U}(2)$, which represents single qubit operations, can be decomposed as the following products for real values of β, γ, δ:
$$U = \begin{pmatrix} \cos\frac{\beta}{2} & -i\sin\frac{\beta}{2} \\ -i\sin\frac{\beta}{2} & \cos\frac{\beta}{2} \end{pmatrix} \begin{pmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}.$$

The next set of single input quantum logic gates are common ones, but remember that these are just special cases of some combination of the exponentiated Pauli matrices.

- The **Hadamard gate** H takes in $|0\rangle$ or $|1\rangle$ and puts it into exactly equal superposition.

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

  That is, $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. This can be thought of as a rotation around the Bloch vector $(1, 0, 1)$.

- The **Phase gate** S is the square root of the Pauli-Z gate.

  $$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

- The $\pi/8$ **gate** T is the square root of the Phase gate.

  $$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

The next set consists of multiple qubit gates. Recall that any function of bits can be computed from the composition of NAND gates alone, which is known as a **universal gate**. The multi-qubit universal quantum gate is actually the control-not gate.

- The **controlled-NOT** gate has the matrix representation:

  $$U_{CNOT} = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

  and transforms the quantum state:

  $$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \mapsto a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle,$$

  also written

  $$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} \implies U_{CNOT} \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\beta_2 \\ \beta_1\alpha_2 \end{pmatrix}.$$

  Notice how unlike the swap gate, the output 4-vector of the CNOT gate is not always guaranteed to decompose into a tensor product $|\psi_1\rangle \otimes |\psi_2\rangle$ of vectors (more on Bell states later). Its circuit is represented in the given image.

- The **controlled-U** gate is a generalization of controlled-NOT. Let us have a control bit and n target bits. If the control bit is set to $|0\rangle$, then the target qubits are left alone. If the control qubit is set to $|1\rangle$, then the states/spins of the n target qubits are changed by some unitary matrix $U \in \mathrm{U}(2^n)$.

  $$U_{CU} = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

  Its circuit is represented in the given image.

- The **swap** gate simply swaps the states of the two qubits.

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

and transforms the quantum state

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \mapsto a|00\rangle + c|01\rangle + b|10\rangle + d|11\rangle,$$

also written

$$\begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} \implies U_{SWAP} \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 \\ \beta_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \otimes \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}.$$

Its circuit is represented in the given image.

- The **Toffoli** gate is similar to a CNOT but with two control qubits and 1 target qubit. If the control qubits are set to $|11\rangle$, then the target qubit is flipped.

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

and transforms the quantum state

$$\begin{aligned} a|000\rangle &+ b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle \\ &\mapsto a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + h|110\rangle + g|111\rangle. \end{aligned}$$

Its circuit is represented in the given image.