1 Introduction

This course, taught during the MIT January term over 11 classes of two hours each, aims to serve as a general introduction to the field of quantum computing. It is tailored to the motivated underclass undergraduate and assumes no background in either quantum mechanics or classical computing theory, though it is built on many of the simpler concepts in linear algebra. As such, the course begins with a general introduction to quantum mechanics, followed by a study of the formalism used in the quantum computing field. Then, we will cover fundamental quantum algorithms and their applications before diving into more complex topics such as quantum machine learning and the operational methods of currently researched quantum computing architectures.

These notes cover all topics presented in the lectures and cite applicable references in the field for the interested reader. By no means are they a fully comprehensive introduction to quantum computing, but they should, at minimum, lay a foundation for further investigation into the topic.

2 Introduction to Quantum Mechanics

Quantum mechanics is, in short, the theory which describes the workings of the entire universe but which only manifests itself in certain regimes where “classical” effects do not take over (namely at small lengths, low temperatures, low energies, high pressures, etc.). It presents various un-intuitive ideas as demonstrated by the Heisenberg Uncertainty Principle and Schrödinger’s cat. Yet, it describes with perfect accuracy numerous phenomena we experimentally observe at the microscopic level. Add to this the fact that we have yet to fully prove quantum mechanics, and one seriously doubts our current knowledge of the universe.

Clearly, quantum mechanics is not a trivial subject. But, we will cover the bare minimum of what one needs to know in order to understanding quantum computing theory and algorithms. As such, our treatment will gloss over some details and mathematical background.

We progress by covering some basic linear algebra before introducing the prevailing notation and formalism used in the field. It is important to note that the formalism of quantum mechanics is built on that of linear (and, more fundamentally, Lie) algebra(s). After the mathematics introduction, we will then discuss the six postulates of quantum mechanics in order to gain a more thorough understanding of quantum mechanics before moving on to topics more specific to quantum computing.
2.1 Linear Algebra Review

Before we dive into basic quantum mechanics, let’s review some important concepts and
definitions from linear algebra which will also help us develop a common language with
which to proceed.

First stop: vectors. Vectors are simply matrices with one of the dimensions set to one.
We thus have two types of vectors: column vectors and row vectors. For a column vector \( v \)
in \( \mathbb{R}^n \), we have:

\[
v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}
\]

where \( v_i \in \mathbb{R} \). A row vector \( w \) is then:

\[
w = \begin{pmatrix} w_1 & w_2 & \cdots & w_n \end{pmatrix}
\]

with \( w_i \in \mathbb{R} \).

Quantum mechanical states exist in complex spaces. So, using the above examples, one
would actually have vectors in \( \mathbb{C}^n \) such that \( v_i, w_i \in \mathbb{C} \). Specifically, for quantum computing,
our quantum bits, or qubits, are two-state systems, so one operates in the smaller \( \mathbb{C}^2 \).

Next, we look at transposes and conjugates. Transposing simply makes each
row in a matrix a column and each column a row. In 2 dimensions, we have the transpose
of a matrix \( A \) where

\[
A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}
\]

equal to

\[
A^T = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}
\]

If we then conjugate the matrix, we take the complex conjugate of each value in the
matrix or vector. Namely, we’d now have:

\[
A^\dagger = (A^T)^* = \begin{pmatrix} a_{11}^* & a_{12}^* \\ a_{21}^* & a_{22}^* \end{pmatrix}
\]
where we have $A^*$ equal to the complex conjugation of each entry in $A$ and thus $A^\dagger$ defined as the \textbf{conjugate transpose} or \textbf{Hermitian adjoint} of the matrix $A$. When $A$ acts on a vector $v$, the conjugate transpose reverses the order of operations, i.e. $(Av)^\dagger = v^\dagger A^\dagger$, due to the transpose identity for multiplication.

Lastly, we consider \textbf{eigenvalues}. For a matrix $B \in \mathbb{C}^n$, we define eigenvectors $v_i$ and corresponding eigenvalues $\lambda_i$ such that

$$B v_i = \lambda_i v_i.$$ 

While we refer to dedicated texts on linear algebra to discuss how eigenvectors and eigenvalues are calculated, we note that eigen-parameters are significant for quantum mechanics and thus quantum computing since they represent the results of a measurement operation. More details are discussed in Sections 2.3.2 and 2.4.3.

\subsection*{2.2 Dirac Notation}

It is now useful to introduce a notation formalism used in quantum mechanics and, especially, in quantum computing: Dirac “bra-ket” notation. While it may at first look odd, it is in reality a simple translation of the “wordier” vector notations used in linear algebra.

Namely, we introduce two definitions: the “bra” and the “ket”. Together, when we take an inner product (Section 2.3.1), they form a “bra-ket” or bracket.\footnote{Physicists are really quite banal when coming to naming anything. So much so that we are often mistaken to be clever.}

The ket, written as $|\psi\rangle$, where $\psi$ is an arbitrary variable used to label the ket, represents a column vector of arbitrary length. Again, in quantum computing, since we only concern ourselves with individual systems of two states, this becomes a 2-by-1 column vector. The bra, $\langle \psi |$ then represents the conjugate transpose of the corresponding bra. So, for our purposes, the bra is a 1-by-2 row vector. More concretely, for a ket $|\psi\rangle$ such that

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

the bra $\langle \psi | = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$.

For a qubit, we’ll define the ground and excited states with $|0\rangle$ and $|1\rangle$, respectively, as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

which are the real basis vectors of $\mathbb{C}^2$. The full quantum state of one qubit will then be a linear, complex superposition of these two basis vectors which are, by definition,
normalized (magnitude one) and orthogonal (inner product zero). An arbitrary qubit state $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ for $\alpha, \beta \in \mathbb{C}$. The state has corresponding bra $\langle \phi | = \alpha^* \langle 0 | + \beta^* \langle 1 |$. We also impose the restriction $|\alpha|^2 + |\beta|^2 = 1$ to normalize the state for reasons to be discussed in Section 2.4.3.

2.3 Linear Algebra in QM

2.3.1 Inner Product

When applying linear algebra to quantum mechanics there are a few concepts to operations and concepts to highlight. First is that of the inner product, which is a generalization of the dot product. For vectors like kets an bras, it is in fact just the dot product. But, it is useful to take a closer look using Dirac notation.

Dirac notation actually makes the inner product quite straightforward. Let’s look at a state $|\psi\rangle$ with complex entries. To take the inner product of $|\psi\rangle$ with itself in order to find the magnitude of $|\psi\rangle$, we simply multiply $|\psi\rangle$ with its conjugate transpose, which is exactly $\langle \psi |$. So, the inner product of $|\psi\rangle$ with itself is $\langle \psi | \psi \rangle$. For a normalized state, namely for a state where we impose the condition that the square magnitudes of its coefficients on basis states sum to one: $\sum_{i=1}^{n} |\alpha_i|^2 = 1$, the inner product will also be one. To see this, we decompose the inner product of $|\psi\rangle$ with itself.

Taking $|\psi\rangle$ to be in $\mathbb{C}^n$, we can represent $|\psi\rangle$ as a complex superposition of the basis vectors of $\mathbb{C}^n$:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |e_i\rangle$$

for $\alpha \in \mathbb{C}$. Now taking the inner product against itself, we find

$$\langle \psi | \psi \rangle = \sum_{i,j=1}^{n} \alpha_j^* \alpha_i \langle e_j | e_i \rangle$$

$$= \sum_{i,j=1}^{n} \alpha_j^* \alpha_i \delta_{i,j}$$

$$= \sum_{i=1}^{n} \alpha_i^* \alpha_i$$

$$= \sum_{i=1}^{n} |\alpha_i|^2 = 1$$

What about the inner product of two different states, say, $|\psi\rangle$ and $|\phi\rangle$? Well, since the inner product is again defined such that we take the complex transpose of one of the states,
we have, for the inner product of $|\psi\rangle$ and $|\phi\rangle$, $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle$. Defining $|\phi\rangle = \sum_{i=1}^{n} \beta_i |e_i\rangle$, we’d have $\langle\phi|\psi\rangle = \sum_{i=1}^{n} \beta_i^* \alpha_i$. For normalized states, this value ranges from 0 to 1 (Can you show it?) and represents the "overlap" between the two states.

The inner product is a very important concept in quantum mechanics and quantum computing, so it is worth getting comfortable with it using Dirac notation.

### 2.3.2 Operators

Next, we consider quantum operators. Simply put, operators act on state vectors and are represented by matrices in the corresponding n-dimensional complex space. Some are defined in infinite dimensional space and must be truncated for finite dimensions. These operators become the classical analog of "gates" in a quantum algorithm.

Quantum operators are represented as a variable (often capital) with a hat, eg. $\hat{H}$, $\hat{x}$, or $\hat{a}$, and, in technical terms, are defined as mapping one vector space $V$ to another $W$. For a quantum operator $\hat{A}$, $\hat{A} : V \rightarrow W$. They have (but are not limited to) the following properties:

1. **linearity**
   - For quantum operator $\hat{A}$ in $V \in \mathbb{C}^n$, $\hat{A} \sum_{i=1}^{n} |e_i\rangle = \sum_{i=1}^{n} \hat{A} |e_i\rangle$.

2. **composites**
   - For quantum operators $\hat{A}$, $\hat{B}$ in $V \in \mathbb{C}^n$, $(\hat{A}\hat{B}) |\psi\rangle = \hat{A}(\hat{B} |\psi\rangle)$

3. **commutation**
   - "Order matters"
   - For quantum operators $\hat{A}$, $\hat{B}$ in $V \in \mathbb{C}^n$, $\hat{A}\hat{B} |\psi\rangle \neq \hat{B}\hat{A} |\psi\rangle$
   - In fact, we have the idea of the commutator: The commutator of $\hat{A}$ and $\hat{B}$ is $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ and their anti-commutator is $\{\hat{A}, \hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$.
   - We say that two operators commute if their commutator is zero.

We have special names for operators with distinct properties. Namely, we call an operator with the property $\hat{A}^\dagger = \hat{A}$ **hermitian** and an operator with the property $\hat{A}^\dagger \hat{A} = \hat{A}\hat{A}^\dagger = I \equiv \hat{A}^{-1}$ **unitary**. Unitary operations are “reversible” since action on a state with $\hat{A}^\dagger$ will undo the action of $\hat{A}$. Both hermitian and unitary operators are significant for quantum mechanics. We will discuss this in more detail in Section 2.4.

Some important operators in quantum computing are
identity: \( I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)

the Pauli matrices:

\[
\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\]

and the Hadamard: \( \hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \).

We will discuss all of these operators and their function in more detail in future lectures.

2.3.3 Tensor Product

The tensor product is an important tool for thinking of multiple quantum systems. A single qubit, which, again, is a two-state system, will exist in a complex vector space, called a Hilbert space \( \mathcal{H}_A \). If we introduce another qubit into our quantum computer, it will exist in its own Hilbert space \( \mathcal{H}_B \). How then, do we talk about these two qubit together?

Well, with a tensor product. Our full quantum computer system is now the tensor product of the two Hilbert spaces, namely \( \mathcal{H}_A \otimes \mathcal{H}_B \). The state of each qubit will exist only in its relevant Hilbert space and an operator in \( \mathcal{H}_A \) will only act on a state in \( \mathcal{H}_A \) and vice versa. If qubit A is in state \( |\psi\rangle \) and qubit B is in state \( |\phi\rangle \), then our two-qubit computer is in state \( |\psi\rangle_A \otimes |\phi\rangle_B \). Of course, this is generalizable to infinite numbers of qubits, or tensored Hilbert spaces.

The tensor product carries a few properties:

1. For \( c \in \mathbb{C} \), \( c (|\psi\rangle_A \otimes |\phi\rangle_B) = c |\psi\rangle_A \otimes |\phi\rangle_B = |\psi\rangle_A \otimes c |\phi\rangle_B \)

2. Distribution:

\[
(|\psi_1\rangle_A + |\psi_2\rangle_A) \otimes |\phi\rangle_B = |\psi_1\rangle_A \otimes |\phi\rangle_B + |\psi_2\rangle_A \otimes |\phi\rangle_B
\]

3. Operators act in their own spaces:

\( \hat{A}_A \otimes \hat{B}_B (|\psi\rangle_A \otimes |\phi\rangle_B) = \hat{A}_A |\psi\rangle_A \otimes \hat{B}_B |\phi\rangle_B \)

We also make a notation simplification:

\[
|\psi\rangle_A \otimes |\phi\rangle_B = |\psi, \phi\rangle = |\psi \phi\rangle
\]

The tensor product acts as following on vectors and matrices:

\[
\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \gamma \\ \alpha \delta \\ \beta \gamma \\ \beta \delta \end{pmatrix}
\]
For an $n \times m$ matrix $A$ and $p \times q$ matrix $B$:

$$A \otimes B = \begin{pmatrix}
A_{11}B & A_{12}B & \ldots & A_{1n}B \\
A_{21}B & A_{22}B & \ldots & A_{2n}B \\
\vdots & \vdots & \ddots & \vdots \\
A_{n1}B & A_{n2}B & \ldots & A_{nn}B
\end{pmatrix}$$

We call two-qubit states that can be written as the tensor product of two states product states and those that cannot entangled states. For example, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is a product state while $|\Psi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ is not.

### 2.4 Postulates of QM

To gain a more technical and intuitive understanding of quantum mechanics, we discuss the postulates of the theory. There are six postulates which dictate the basis of quantum mechanical theory. We model our discussion around MIT Professor Jaffe’s notes from 8.05 as taught in 1996 (basic quantum mechanics has not really changed since then). This section will provide many of the important consequences involving quantum operators and measurement that are significant for quantum computing.

#### 2.4.1 First Postulate

A quantum state is represented by a ket, some $|\psi\rangle$ in the state space, called a wavefunction. It completely specifies the quantum state.

The space of states is a vector space which means that the superposition of two states is again a state of the system. This allows us to define arbitrary states $|\psi\rangle = \sum_i a_i |e_i\rangle$ for basis vectors $|e_i\rangle$ of the n-dimensional state space. This describes phenomena like the double-slit diffraction of electrons.

As a Hilbert space, the space of states has with it a defined inner product. Namely,

$$\langle |\psi\rangle , |\phi\rangle \rangle \equiv \langle \psi|\phi \rangle = \int dx \psi^*(x)\phi(x)$$

We first define the inner product as an operation acting on two states in the ket space. Then the second step introduces the “bra space” of the same dimension as the ket space, and defines the inner product as an operation involving one element of the each space. Finally, we reduce to the familiar continuous inner product which represents the overlap of $|\psi\rangle$ and $|\phi\rangle$. This notation allows us to see clearly that

$$\langle \psi|\phi \rangle^* = \langle \phi|\psi \rangle .$$
2.4.2 Second Postulate

Classical observables are introduced into quantum mechanics using operators. Specifically, every observable (measurable property) of a physical system is described by an operator that acts state kets.

Classical observables (such as position $x$ or momentum $p$) are made “quantum" by transforming them into quantum operators. One simply adds the operator hat ($\hat{\cdot}$) on top of the observable’s variable.

Notation-wise, an operator acts on a state from the left, ie. $\hat{A}|\psi\rangle$. In general, an operator acting on a state will change the state. For every operator, there are, however, states which are not changed by the action of the operator, giving, for example,

$$\hat{A}|\psi_i\rangle = a_i|\psi_i\rangle$$

(3)

These states are eigenstates to the operator and the value $a_i$ is the eigenvalue which represents the observable’s value. An operator acting on a state which is not one of its eigenstates, will produce a probabilistic outcome based on the states representation in the basis of eigenstates for the operator. In this case, the operator will also change the quantum state of the system.

2.4.3 Third Postulate

The result of a measurement of an observable with an operator $\hat{A}$ will only ever be an eigenvalue of $\hat{A}$.

This postulates leads to the “quantum" or “quantized" nature of quantum mechanics. Some operators, like the position $\hat{x}$ or momentum $\hat{p}$ operators, have a set of continuous eigenvalues, so this proposition is not far removed from what we are used to from classical mechanics. However, for operators with discrete eigenvalues such as the Hamiltonian (ie. energy) operator for particle in a bound well, this proposition creates an unintuitive result.

We note an important requirement here. First, measured values, in other words, the eigenvalues, must be real since these are real, classically measured observables. This means that operators corresponding to an observable must be Hermitian (remember Section 2.3.2). Hermitian operators also have eigenstates which form a complete basis which means that any state in the space can be decomposed into a linear superposition of eigenstates of the operator. These operators can be re-written as $\hat{A} = \sum_i \lambda_i |a_i\rangle \langle a_i|$ for eigenvalues $\lambda_i$ and corresponding eigenvectors $|a_i\rangle$. 

10
2.4.4 Fourth Postulate

When a measurement of an observable with operator $\hat{A}$ is made on a generic state $|\psi\rangle$, the probability of obtaining a certain eigenvalue $a_i$ is given by the square of the inner product of $|\psi\rangle$ with the corresponding eigenstate $|a_i\rangle$.

Professor Jaffe gives a very good treatment of this postulate, so we abbreviate them here.

We assume that the states are normalized which is in general possible. States are usually normalized to unity,

$$\langle \psi | \psi \rangle = 1$$
$$\langle a_j | a_k \rangle = \delta_{jk} \quad (4)$$

The complex number, $\langle a_i | \psi \rangle$ is known as the “probability amplitude”, to measure $a_i$ as the value for the observable $\hat{A}$ in the state $|\psi\rangle$.

The postulate suggests the following algebraic exercise. First, any state can be expanded as a superposition of $\hat{A}$-eigenstates (see Postulate 3),

$$|\psi\rangle = \sum_n c_n |a_n\rangle \quad (5)$$

Next use the orthonormality of the $\hat{A}$-eigenstates to find an expression for the expansion coefficients $c_n$,

$$\langle a_j | \psi \rangle = \sum_n c_n \langle a_j | a_n \rangle = c_j \quad (6)$$

So,

$$|\psi\rangle = \sum_n \langle a_n | \psi \rangle |a_n\rangle \quad (8)$$

where we have the complex number $\langle a_n | \psi \rangle$ and the state $|a_n\rangle$. The component of $|\psi\rangle$ along the direction of the nth eigenstate of $\hat{A}$ is given by $\langle a_n | \psi \rangle$. The measurement operation yields the result $a_n$ with a probability proportional to the square of this component, $|\langle a_n | \psi \rangle|^2$.

The probability of obtaining some result at all is unity. For states normalized to unity,

$$|\langle \psi | \psi \rangle|^2 = \left| \sum_m \sum_n c_m^* c_n \langle a_m | a_n \rangle \right|^2 \quad (9)$$
Using $|\langle \psi | \psi \rangle|^2 = 1$ and $\langle a_m | a_n \rangle = \delta_{mn}$, we get

$$\sum_n |c_n|^2 = 1.$$  \hspace{1cm} (10)

According to the usual rules of probability, we can compute the “expectation value” of the observable $A$. If the probability to observe $a_n$ is $|c_n|^2$, then the expected value (denoted $\langle A \rangle$) is

$$\langle A \rangle = a_n |c_n|^2$$  \hspace{1cm} (11)

as long as each eigenstate has a unique eigenvalue (the operator $\hat{A}$ has no degenerate eigenvalues).

### 2.4.5 Fifth Postulate

*Immediately after the measurement of an observable $A$ with a value $a_n$, the state of the system is the normalized eigenstate $|a_n\rangle$.*

This postulate gives way to the idea of the “collapse of the wavepacket”. While measuring a state $|\psi\rangle$ for the observable $A$ gives the value $a_n$ with probability $|\langle a_n | \psi \rangle|$, results for remeasuring immediately after the first measurement are not statistically distributed. Namely, after measurement, the state $|\psi\rangle$ is found in the renormalized state $|a_n\rangle$ since the outcome is always $a_n$.

Wavefunction collapse is one of the more unintuitive concepts in quantum mechanics, but is supported by experimental results with repeated measurements.

### 2.4.6 Sixth Postulate

*Quantum states generally change (evolve) with time. This time evolution preserves the normalization of the state. The time evolution of the state of a quantum system is described by $|\psi(t)\rangle = \hat{U}(t,t_0)|\psi(t_0)\rangle$, for some unitary operator $\hat{U}$.*

A quantum state must evolve by a unitary operator since the norm of the state must be preserved. While individual probabilities of observing certain eigenvalues of an operator may change, the total sum ($\sum_n |c_n|^2$ from before) remains the same. The probability for measuring some value of any operator remains unity.
As such, for a state evolving with time $|\psi(t)\rangle$, we maintain $|\langle\psi(t)|\psi(t)\rangle|^2 = 1$ for all $t$. So,

$$|\langle\psi(t)|\psi(t)\rangle|^2 = 1$$

$$= |\langle\psi(t_0)| \hat{U}^\dagger(t, t_0) \hat{U}(t, t_0) |\psi(t_0)\rangle|^2$$

$$= |\langle\psi(t_0)|\psi(t_0)\rangle|^2 = 1,$$

which is consistent with our earlier requirement for a unitary operator. This also means that time evolution is a reversible process. We reverse some time evolution given by $\hat{U}(t, t_0)$ we simply act with $\hat{U}(t_0, t) = \hat{U}^\dagger(t, t_0)$.

This postulate actually leads to the Schrödinger equation which requires that a state $|\psi\rangle$ evolves under

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

for a Hermitian operator $\mathcal{H}$ which is a system-dependent operator called the Hamiltonian.

### 2.5 Uncertainty Principle

The postulates of quantum mechanics highlight the probabilistic nature of the theory. This in turn gives rise to some interesting (and sometime unintuitive or even concerning) phenomena. One of these is the uncertainty principle which states that there is a limit to the precision with which one is able to determine the values of conjugate observables (such as position and momentum and energy and time).

Stepping back to classical probability theory, we can define an expectation value $\langle A \rangle$, variance $(\Delta A)^2$, and standard deviation $(\Delta A)$ such that for possible values $a_i$ each with probability $p_i$,

$$\langle A \rangle = \sum_i a_i p_i,$$

$$(\Delta A)^2 = \langle (A - \langle A \rangle)^2 \rangle = \langle A^2 \rangle - \langle A \rangle^2,$$

and

$$\Delta A = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}.$$
use $p_i = |\langle \psi | \phi_i \rangle|^2$ to find $\Delta A \Delta B$ in terms of $[A, B]$. The standard deviation $\Delta A$ measures the uncertainty in our knowledge of the value of the observable $A$, so we will be placing a limit on our this uncertainty.

First, in quantum mechanics, the expectation value of an observable simplifies to

$$\langle A \rangle = \sum_i a_i p_i$$
$$= \sum_i a_i \langle \psi | \phi_i \rangle \langle \phi_i | \psi \rangle$$
$$= \langle \psi | \left( \sum_i a_i | \phi_i \rangle \langle \phi_i | \right) | \psi \rangle$$
$$= \langle \psi | A | \psi \rangle. \tag{19}$$

To derive the uncertainty principle, let

$$\langle \psi | A \rangle = re^{i\phi}$$

where $re^{i\phi}$ represents some arbitrary complex number. Using $\langle \psi | AB | \psi \rangle = \langle \psi | BA | \psi \rangle$ for Hermitian operators $\hat{A}$ and $\hat{B}$, one finds

$$\langle \psi | AB - BA | \psi \rangle = re^{i\phi} - re^{-i\phi} = 2ir \sin \phi, \tag{22}$$
$$\langle \psi | AB + BA | \psi \rangle = re^{i\phi} + re^{-i\phi} = 2r \cos \phi, \tag{23}$$

and

$$|\langle \psi | AB + BA | \psi \rangle|^2 + |\langle \psi | AB - BA | \psi \rangle|^2 = 4r^2. \tag{24}$$

Thus follows

$$|\langle \psi | AB - BA | \psi \rangle|^2 \leq 4 |\langle \psi | AB | \psi \rangle|^2 \tag{25}$$

since both arguments on the left side of Eq. 24 are necessarily greater than or equal to zero. One further reduces using the inner product inequality from linear algebra to find

$$\frac{|\langle \psi | [A, B] | \psi \rangle|^2}{4} \leq \langle \psi | A^2 | \psi \rangle \langle \psi | B^2 | \psi \rangle. \tag{26}$$

Now, define $A = C - \langle C \rangle$ and $B = D - \langle D \rangle$ where $[A, B] = [C, D]$, $\langle \psi | A^2 | \psi \rangle = (\Delta C)^2$, and $\langle \psi | B^2 | \psi \rangle = (\Delta D)^2$. So,

$$\left| \frac{\langle \psi | [C, D] | \psi \rangle}{2} \right|^2 \leq (\Delta C)^2 (\Delta D)^2, \tag{27}$$
which brings us to the Heisenberg Uncertainty principle:

\[
\frac{\langle \psi | [C,D] | \psi \rangle}{2} \leq \Delta C \Delta D. \tag{28}
\]

This statement gains significance when we considering the position and momentum conjugate variables. Since \([\hat{x}, \hat{p}] = i\hbar\), \(\Delta \hat{x} \Delta \hat{p} \geq \frac{\hbar}{2}\), so one can only measure together the position and momentum variables of a system to a minimum of \(\frac{\hbar}{2}\). Increasing knowledge about the position of a system necessarily decreases the knowledge an observer can have about the momentum of a system (and vice versa). This is true for all non-commuting observables.

### 2.6 Local Hidden Variables

Einstein was rather uncomfortable with the idea that quantum mechanics was a fundamentally probabilistic theory\(^2\). He say quantum mechanics as akin to thermodynamics which describes macroscopic effects using derivations from microscopic or “hidden” variables. We illustrate this idea with an example using a system of three (two-state) quantum spins (like an atom or a qubit, for example). This system has a total Hilbert space

\[
\mathcal{H} = \mathcal{H}_{\text{spin}}^\otimes 3 = \mathcal{H}_{\text{spin}}^A \otimes \mathcal{H}_{\text{spin}}^B \otimes \mathcal{H}_{\text{spin}}^C. \tag{29}
\]

For a given state \(|\psi\rangle\), one cannot predict the outcome of measuring each spin along a single axis. However, one could assume that each spin has a secret (secret to the observer) setting: either \(\uparrow = +1\) or \(\downarrow = -1\) for each of \(x, y,\) and \(z\) for each spin. We label these \(S_x^1\) for an \(\hat{x}\) measurement on the first qubit, and so on. As such, the system has its own truth table, so to speak, which determines the outcome of any measurement on the system (say, \(\hat{x}_1 \hat{y}_2 \hat{y}_3\) or \(\hat{z}_1 \hat{x}_2 \hat{y}_3\)).

In 1993, physicists Greenberger, Horne, and Zeilinger attempted to show the invalidity of local hidden variables. They wrote down a state, known as the GHZ state:

\[
|\Psi\rangle_{\text{GHZ}} = \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle) \tag{30}
\]

for a system of three spins. We will measure the following operators on the GHZ state: \(\hat{x}_1 \hat{x}_2 \hat{x}_3, \hat{x}_1 \hat{y}_2 \hat{y}_3, \hat{y}_1 \hat{x}_2 \hat{y}_3, \hat{y}_1 \hat{y}_2 \hat{x}_3\).

\(^2\)as shown by his famous statement “God does not play dice.”
The expectation value of the first observable $x_1x_2x_3$ on the GHZ state is

$$\langle \hat{x}_1 \hat{x}_2 \hat{x}_3 \rangle_{GHZ} = \frac{1}{\sqrt{2}} \langle \hat{x}_1 \sigma_x \sigma_x \sigma_x | \hat{x}_2 \sigma_x \sigma_x \sigma_x | \hat{x}_3 \sigma_x \sigma_x \sigma_x | \Psi \rangle_{GHZ}$$

$$= \frac{1}{\sqrt{2}} \langle \Psi |_{GHZ} 1 \sigma_x (|000\rangle - |111\rangle)$$

$$= \frac{1}{\sqrt{2}} \langle \Psi |_{GHZ} (|111\rangle - |000\rangle)$$

$$= -\frac{1}{\sqrt{2}} \langle \Psi |_{GHZ} (|000\rangle - |111\rangle)$$

$$= -\langle \Psi |_{GHZ}$$

$$= -1.$$ \hfill (31)

For $x_1y_2y_3$, the expectation value is

$$\langle \hat{x}_1 \hat{y}_2 \hat{y}_3 \rangle_{GHZ} = \frac{1}{\sqrt{2}} \langle \hat{x}_1 \sigma_y \sigma_y \sigma_y | \hat{y}_2 \sigma_y \sigma_y \sigma_y | \hat{y}_3 \sigma_y \sigma_y \sigma_y | \Psi \rangle_{GHZ}$$

$$= \frac{1}{\sqrt{2}} \langle \Psi |_{GHZ} (|111\rangle_A (i |1\rangle_B (i |1\rangle_C) - |0\rangle_A (-i |0\rangle_B) (-i |0\rangle_C))$$

$$= -\frac{1}{\sqrt{2}} \langle \Psi |_{GHZ} (-|111\rangle + |000\rangle)$$

$$= \langle \Psi |_{GHZ}$$

$$= 1.$$ \hfill (32)

as is the expectation values for $y_1x_2y_3$ and $y_1y_2x_3$.

We have, then

$$\langle \hat{x}_1 \hat{x}_2 \hat{x}_3 \rangle \langle \hat{x}_1 \hat{y}_2 \hat{y}_3 \rangle \langle \hat{y}_1 \hat{x}_2 \hat{x}_3 \rangle \langle \hat{y}_1 \hat{y}_2 \hat{x}_3 \rangle = (-1)(+1)(+1)(+1)$$

$$= -1.$$ \hfill (33)

However, if we calculate this same value using the hidden variables approach, we find

$$\langle S_x^1 S_x^2 S_x^3 \rangle \langle S_y^1 S_y^2 S_y^3 \rangle \langle S_x^1 S_x^2 S_x^3 \rangle \langle S_y^1 S_y^2 S_y^3 \rangle = \langle S_x^1 \rangle^2 \langle S_y^1 \rangle^2 \langle S_x^2 \rangle^2 \langle S_y^2 \rangle^2 \langle S_x^3 \rangle^2 \langle S_y^3 \rangle^2$$

$$= (+1)^2$$

$$= +1.$$ \hfill (34)

which is clearly a contradiction. So, if quantum mechanics is correct, as research and experiment suggest, our world really is probabilistic after all\textsuperscript{3}.

\textsuperscript{3}Sorry, Mr. Einstein.
2.7 The Bloch Sphere

The Bloch sphere is a useful tool for visualizing qubit states (or any quantum state in $\mathcal{H}^2$. A pure quantum state is represented by a vector on the surface of a unit sphere. The state $|0\rangle$ exists at the top of the sphere (the north pole) and the state $|1\rangle$ exists at the bottom (the south pole). Using spherical coordinates, arbitrary qubit states are defined on the sphere with $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle$ with polar angle $\theta$ and azimuthal angle $\phi$. Any state can be written $|\psi\rangle = e^{i\gamma} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right)$ where we factor out the phase associated with the $|0\rangle$ basis state. However, in quantum mechanics, the arbitrary phase $e^{i\gamma}$ has no observable effects on the state. So, any qubit state is described by a point on the unit sphere.

Using this formula, we can define the states which match the positive and negative x, y, and z-axes as

$$
+z = |0\rangle \\
-z = |1\rangle \\
+x = +\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
-x = -\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
+y = +i\rangle = \frac{1}{\sqrt{2}} (|0\rangle + i |1\rangle) \\
-y = -i\rangle = \frac{1}{\sqrt{2}} (|0\rangle - i |1\rangle)
$$

which one can prove to oneself using appropriate values for $\theta$ and $\phi$.

Let’s consider the action of the Pauli matrices on states on the Bloch sphere. We will find that they, when exponentiated, generate rotations. Specifically, a rotation along some axis $\hat{n}$ is represented by

$$
R_n(\theta) = e^{-i\frac{\theta}{2} \hat{n} \cdot \vec{\sigma}}
$$

where $\vec{\sigma}$ is the “vector” of Pauli matrices. In the second line, we use the fact that $\sigma_i^2 = 1$ for the Paulis. In the following, we show that the above truly is a rotation on the Bloch sphere.

To do so, it is useful to consider the density operator formed by the outer product of
the qubit state:

\[ \rho = |\psi\rangle \langle \psi| = |\psi\rangle \otimes (\psi) \]

\[= \left( \begin{array}{cc}
\cos^2 \frac{\theta}{2} & e^{-i\phi} \cos \frac{\theta}{2} \sin \frac{\theta}{2} \\
e^{i\phi} \cos \frac{\theta}{2} \sin \frac{\theta}{2} & \sin^2 \frac{\theta}{2}
\end{array} \right) \]

\[= \frac{1}{2} \left( \begin{array}{cc}
1 + \cos \theta & \cos \phi \sin \theta - i \sin \phi \sin \theta \\
\cos \phi \sin \theta + i \sin \phi \sin \theta & 1 - \cos \theta
\end{array} \right) \]

\[= \frac{1}{2} \left( I + X \cos \phi \sin \theta + Y \sin \phi \sin \theta + Z \cos \theta \right) \]

\[= \frac{1}{2} \left( I + \vec{r}_{\rho} \cdot \vec{\sigma} \right) \]

where we have \( I, X, Y, Z \) as the identity and Pauli matrices and \( \vec{r}_{\rho} = (r_x, r_y, r_z) = (\cos \phi \sin \theta, \sin \phi \sin \theta, \cos \theta) \) as a unit vector in spherical coordinates.

The action of an operator on a quantum state must obey unitary evolution, preserving the norm of the state. The action of a unitary operator on a state can we used to find the action on the density operator \( \rho \). Since a unitary operator acting on a state \( |\psi\rangle \) is given by \( |\psi\rangle \rightarrow \hat{U} |\psi\rangle \), the action of the operator on \( \rho \) is

\[ \rho = |\psi\rangle \langle \psi| \rightarrow \hat{U} |\psi\rangle \langle \psi| \hat{U}^\dagger. \]

Our rotation matrix is unitary since the Pauli matrices are Hermitian. Let’s observe the action of a z-axis rotation on our density matrix. For a rotation around the z-axis, \( R_z(\theta) = \cos^2 \frac{\theta}{2} I - i \sin^2 \frac{\theta}{2} \sigma_z \). Since \( \rho \) is a sum of the Pauli matrices, we can evaluate \( R_z(\theta) \) on each individually:

\[ \rho' = R_z(\theta) \rho R_z(\theta)^\dagger \]

\[= \frac{1}{2} \left( I + r_x R_z(\theta) X R_z(\theta)^\dagger + r_y R_z(\theta) Y R_z(\theta)^\dagger + r_z R_z(\theta) Z R_z(\theta)^\dagger \right). \]

For the first term, the we use the unitary property of the rotation matrix.

Expanding the \( X \) term, we have

\[ R_z(\theta) X R_z(\theta)^\dagger = \left( \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} \sigma_z \right) X \left( \cos \frac{\theta}{2} I + i \sin \frac{\theta}{2} \sigma_z \right) \]

\[= \cos^2 \frac{\theta}{2} X + i \sin \frac{\theta}{2} \cos \frac{\theta}{2} \sigma_z X Z - i \sin \frac{\theta}{2} \cos \frac{\theta}{2} \sigma_z X Z \]

\[= \cos^2 \frac{\theta}{2} X + \sin \frac{\theta}{2} \cos \frac{\theta}{2} Y + \sin \frac{\theta}{2} \cos \frac{\theta}{2} Y - \sin^2 \frac{\theta}{2} X \]

\[= \left( \cos^2 \frac{\theta}{2} - \sin^2 \frac{\theta}{2} \right) X + 2 \sin \frac{\theta}{2} \cos \frac{\theta}{2} Y \]

\[= \cos \theta X + \sin \theta Y. \]
Similarly, we can show

\[ R_z(\theta)YR_z(\theta)^\dagger = \cos \theta Y - \sin \theta X \] (50)

\[ R_z(\theta)ZR_z(\theta)^\dagger = Z. \] (51)

Now, rewriting \( \rho' \),

\[
\rho' = \frac{1}{2} \left( I + r_x R_z(\theta)X R_z(\theta)^\dagger + r_y R_z(\theta)Y R_z(\theta)^\dagger + r_z R_z(\theta)ZR_z(\theta)^\dagger \right)
\]

\[
= \frac{1}{2} \left( I + r_x \cos \theta X + \sin \theta Y + r_y \cos \theta Y - \sin \theta X + r_z Z \right)
\]

\[
= \frac{1}{2} \left( I + (r_x \cos \theta - r_y \sin \theta)X + (r_x \sin \theta + r_y \cos \theta)Y + r_z Z \right) \quad (52)
\]

\[
= \frac{1}{2} \left( I + r'_x X + r'_y Y + r'_z Z \right) \quad (53)
\]

where we have the transformed positions

\[
r'_x = r_x \cos \theta - r_y \sin \theta
\]

\[
r'_y = r_x \sin \theta + r_y \cos \theta
\]

\[
r'_z = r_z \quad (54)
\]

which match exactly what we expect from a rotation around the z-axis. We can then construct the \( R_z(\theta) \) rotation matrix

\[
\begin{pmatrix}
\cos \theta & -\sin \theta & 0 \\
\sin \theta & \cos \theta & 0 \\
0 & 0 & 1
\end{pmatrix}.
\] (55)

We can do something similar to construct the matrix for a rotation around an arbitrary axis by making composite rotations with \( R_x \), \( R_y \), and \( R_z \).

### 2.7.1 Density Matrix

The density matrix is a powerful construct that allows us to, for example, compare quantum states with classical statistics and consider the effect of measurements. We define the density matrix \( \rho \):

\[
\rho = |\psi\rangle \langle \psi|
\] (56)

as in Section 2.7.

\[\text{Give it shot!}\]
As an example, we can use the density matrix to determine the difference between a coin flip and an equal quantum superposition.

We term processes that take the off-diagonal elements to zero “decoherence”, which is an important negative effect which is, for many architectures, the main obstacle toward scalable quantum processors.

3 Quantum Circuits

With the above background, we can now take a look at quantum analogues of classical computing gates. In classical computing, bits can be 0 or 1 and \( n \) input bits are mapped to \( m \) output bits. We also have traditional logical operations, or gates, such as AND, OR, NOT, NAND, and Fanout (copy) (see Table 1).

The set of AND, OR, NOT is a universal set of gates. Namely, all other gates can be created from combinations of elements in the universal set. The NAND gate is also universal (with ancila bits) as is the Toffoli gate, which we will discuss later.

We define a reversible gate as a gate where given an output you can figure out the inputs. The Toffoli gate is reversible while the NAND gate is not. Reversibility relates to Landauer’s principle which states that

\[
\text{For every bit of information erased, you dissipate energy greater than } k_b T \ln 2 \approx 10^{-20} J
\]

Since irreversible gates by definition involve the erasure of information. In quantum systems, since our kets evolve by unitary operations which are reversible, we require all quantum gates to be reversible.

3.1 Single Qubit Gates

The common single qubit gates are the Pauli matrices

Pauli \( x \), \( \sigma_x \) acts as a NOT gate on our computational basis. \( \sigma_z \), the PHASE gate, adds a phase to \(|1\rangle\). Lastly, \( \sigma_y \) adds a global phase (adds the same phase to both basis states) as well as performs a NOT operation. As such, \( \sigma_y \) is a combination of \( \sigma_x \) and \( \sigma_z \). In fact, the

\[
\begin{array}{c|cc|c|cc|c|cc}
 & a & b & & a & b & & a & b \\
\hline
\text{AND:} & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\text{OR:} & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
\text{NAND:} & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\end{array}
\]

Table 1: Basic classical gates
Pauli matrices are related by permutation:

$$\sigma_i \sigma_j = \delta_{ij} \mathbb{I} + \epsilon_{ijk} \sigma_k$$  \hspace{1cm} (57)

which means that we can get all three Pauli gates from just two of them. In Eq. 57, we use the Levi-Civita symbol $\epsilon_{ijk}$.

The Hadamard gate,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$  \hspace{1cm} (58)

maps

$$|0\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle).$$

These new states are again orthogonal. The Hadamard gate actually represents a rotation around the line on the x-z plane that is at a 45° angle.

### 3.2 Two Qubit Gates

To actually make a useful quantum processor though, we need to have gates for multiple qubits on hand. The most general simple two qubit gate is a controlled unitary which applies a unitary operator on the second qubit based on the state of the first, “control”, qubit. The gate applies the unitary to qubit 2 if the control qubit is in the state $|1\rangle$ and applies the identity otherwise. The 4x4 matrix which represents the action of the two qubit gate in the tensored two qubit space is

$$CU = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}.$$  \hspace{1cm} (59)

An example of a controlled unitary operator is the CNOT gate which has the unitary equal to $\sigma_x$:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$  \hspace{1cm} (60)
The action of CNOT on the state with control bit $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ and target qubit $|\phi\rangle = a |0\rangle + b |1\rangle$ produces entanglement since each part of the control bit’s superposition states acts on the target qubit separately.

3.3 No-Cloning Theorem

In quantum systems, we do not have access to a Fanout, or copy, gate. Namely, any state $|\psi\rangle$ cannot be copied onto another quantum system. Let’s begin our proof by supposing we have two quantum systems A and B with which we can build a tensored Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Now assume we have a unitary operator whose action is to copy the normalized state of system A into the state of system B irrespective of the current state of B. In other words, we define a $U$ in $\mathcal{H}$ such that

$$U |\psi\rangle |e\rangle = e^{i\alpha_{\psi,e}} |\psi\rangle |\psi\rangle$$

where we have introduced an arbitrary global phase which has no action on the quantum system but which depends on the initial states $|\psi\rangle$ and $|e\rangle$. Recall that the quantum mechanical state defines a normalized vector in a Hilbert space only up to a phase factor.

We choose two arbitrary initial states of system A: $|\psi\rangle$ and $|\phi\rangle$. Now, we proceed such that

$$\langle\psi|\phi\rangle \langle e|e\rangle = \langle\psi| \langle e| U^\dagger U |\phi\rangle |e\rangle$$
$$= e^{i(\alpha_{\psi,e} - \alpha_{\psi,e})} \langle\psi| \langle\psi| |\phi\rangle |\phi\rangle$$
$$= e^{i(\alpha_{\psi,e} - \alpha_{\psi,e})} |\langle\psi|\phi\rangle|^2$$

which gives us, assuming normalized state $|e\rangle$,

$$|\langle\psi|\phi\rangle|^2 = |\langle\psi|\phi\rangle|^2.$$  

This means that our unitary only for the same or orthogonal states, which contradicts our initial presumption that our unitary works for arbitrary states. So, we no that no such operator exists, proving the no-cloning theorem.

3.4 Deutsch-Josza Algorithm

The Deutsch-Josza algorithm is a simple demonstration of quantum speed-up. It allows us to determine whether a function is constant or variable. We refer to the description in the book *Introduction to Quantum Computing* by Phillip Kaye and Raymond Laflamme (posted on course page).
3.5 Superdense Coding

Let’s say Alice (A) and Bob (B) share an entangled pair:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$  (64)

We can created this entangled state by taking starting their qubits in the \(|0\rangle\) state, applying a Hadamard \(H\) on Alice’s qubit, and finally applying a CNOT with Alice’s qubit has the control.

Now, we ask: how does Alice transmit certain sets of information? Well, we must encode our possible bits: In short, Alice performs certain operations on her qubit to encode a two-bit value before sending her qubit to Bob. Bob then makes a “Bell measurement”. A “Bell measurement” simply unentangles an entangled state. Namely, he applies a CNOT with Alice’s qubit as the control and then applies a Hadamard on Alice’s qubit before measuring. Working this out, we will find that Bob will simply measure Alice’s original two-bit states.

<table>
<thead>
<tr>
<th>message</th>
<th>transformation</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>(I_A \otimes I_B)</td>
<td>(</td>
</tr>
<tr>
<td>00</td>
<td>(X_A \otimes I_B)</td>
<td>(</td>
</tr>
<tr>
<td>10</td>
<td>(Z_A \otimes I_B)</td>
<td>(</td>
</tr>
<tr>
<td>11</td>
<td>(X_A, Z_A \otimes I_B)</td>
<td>(</td>
</tr>
</tbody>
</table>

3.6 Quantum Teleportation

While this subject is rather over-hyped, it is indeed true that quantum mechanics can lead to a certain kind of state teleportation. First, let’s again begin with our friends Alice and Bob. Say they share the entangled state from Eq. 64, \(|\beta_{00}\rangle\). Now, Alice wants to teleport a
separate state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. The full system state is then:

$$|\psi\rangle \otimes |\beta_{00}\rangle = (\alpha |0\rangle + \beta |1\rangle) \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$= \frac{1}{2\sqrt{2}}(|00\rangle + |11\rangle)_A \otimes (\alpha |0\rangle + \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|01\rangle + |10\rangle)_A \otimes (\alpha |0\rangle + \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|00\rangle - |11\rangle)_A \otimes (\alpha |0\rangle - \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|01\rangle - |10\rangle)_A \otimes (\alpha |0\rangle - \beta |1\rangle)_B.$$  \hspace{1cm} (65)

Now, Alice applies a CNOT with her state $|\psi\rangle$ as the control and her qubit of the entangled pair as the target and then performs a Hadamard on the state $|\psi\rangle$. This is just the Bell measurement from Section 3.5. This means that Alice’s qubit is now encoded into a two-bit value which can then be used to perform operations on Bob’s half of the entangled pair. After the CNOT, we find:

$$U_{CNOT} |\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{2\sqrt{2}}(|00\rangle + |10\rangle)_A \otimes (\alpha |0\rangle + \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|01\rangle + |11\rangle)_A \otimes (\alpha |0\rangle + \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|00\rangle - |11\rangle)_A \otimes (\alpha |0\rangle - \beta |1\rangle)_B$$

$$+ \frac{1}{2\sqrt{2}}(|01\rangle - |10\rangle)_A \otimes (\alpha |0\rangle - \beta |1\rangle)_B.$$  \hspace{1cm} (66)

Now performing the Hadamard and measuring Alice’s two qubits (her $|\psi\rangle$ and entangled qubit), we know which state Bob holds based on the measurement of Alice’s qubits. Namely, she measures 00, 01, 10, 11 based on the Bell measurement we discussed above. This measurement then collapses Bob’s state to $\alpha |0\rangle + \beta |1\rangle$, $\alpha |1\rangle + \beta |0\rangle$, $\alpha |0\rangle - \beta |1\rangle$, or $\alpha |1\rangle - \beta |0\rangle$, respectively. As such, we can use Alice’s measurement to perform transformations on Bob’s qubit such that Bob ends with the original state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. Specifically, we would apply an X operation if Alice’s first bit is 1 and a Z operation if Alice’s second bit is 1.
3.7 Universality

A universal computer can solve any problem. The universal set of gates includes the Clifford gates: CNOT, H, S plus the T gate where

\[
S = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}
\]

and

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