Quantum Information Lecture 1

Lecturer: Aaron Szasz
TA: Jacob Barnett*

Perimeter Institute for Theoretical Physics,
31 Caroline Street North, Waterloo, Ontario N2J 2Y5, Canada

June 20, 2023

Contents

1 Outline

Course objective: Introduce the fundamentals of quantum information. In particular, we will define and demystify entanglement and its usage. Furthermore, we will end up using mixed states.

Lesson plans:

- **Day 1**: Review systems with either one or two spin-$\frac{1}{2}$ particles (a.k.a. qubit).
- **Day 2**: Introduce entanglement.
- **Day 3**: Mixed quantum states.
- **Day 4**: Applications, e.g. quantum teleportation.

Warning: Your TA is rather mathematically inclined and will sprinkle in digressions throughout these notes. Don't panic!

2 Qubits

All 1-qubit systems are equivalent. This statement will be clarified after some math.

*jbarnett@perimeterinstitute.ca

2.1 States as Kets

The kinematics, or space of quantum states, is given by the vector space $\mathbb{C}^2$. We will denote the canonical basis of $\mathbb{C}^2$ using the "ket" notation of $|0\rangle$ and $|1\rangle$. Using the "matrix" notation of traditional linear algebra,

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1}$$

An arbitrary vector in $\mathbb{C}^2$ is, thus,

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

An **inner product** is a map, $\langle \cdot | \cdot \rangle$, that takes vectors and outputs a complex number. Inner products satisfy some special properties which I list below. For qubits, we will use a specific inner product defined as follows: given two vectors $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\phi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$ in $\mathbb{C}^2$, their inner product is

$$\langle \phi|\psi\rangle := \gamma^*\alpha + \delta^*\beta. \tag{3}$$

Quantum states are *normalized* vectors, which means $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is a quantum state if and only if $|\alpha|^2 + |\beta|^2 = 1$. When α, β are real numbers, we can thus interpret the space of states as a circle. A most general state is represented with the Bloch sphere, which we might talk about later. The Bloch sphere a physicist's interpretation of the homeomorphism from the complex projective line to the sphere.

A more general inner product is any map satisfying the following criteria:

- *Conjugate Symmetry*:

$$\langle \psi|\phi\rangle = \langle \phi|\psi\rangle^*\,. \qquad\qquad \forall\, \psi, \phi \in \mathcal{H}. \tag{4}$$

- *Linearity*:

$$\langle \psi_0|\alpha\phi_0 + \beta\phi_1\rangle = \alpha\,\langle \psi_0|\phi_0\rangle + \beta\,\langle \psi_0|\phi_1\rangle \qquad\qquad \forall \alpha, \beta \in \mathbb{C},\; \psi_0, \phi_0, \phi_1 \in \mathcal{H}. \tag{5}$$

- *Positive-Definiteness*:

$$\langle \psi|\psi\rangle > 0 \qquad\qquad \forall \psi \in \mathcal{H} \setminus \{0\}. \tag{6}$$

A **Hilbert space** is a vector space with an inner product space where you define limits in some sense. The precise definition won't be given here. In finite-dimensions, every inner product space is a Hilbert space. The typical setting for quantum information is a finite-dimensional Hilbert space.

A **orthonormal basis** of a Hilbert space is a linearly independent set of vectors, $|v_i\rangle$, whose orthogonal complement is the zero vector, and which satisfy

$$\langle v_i|v_j\rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise}\,. \end{cases} \tag{7}$$

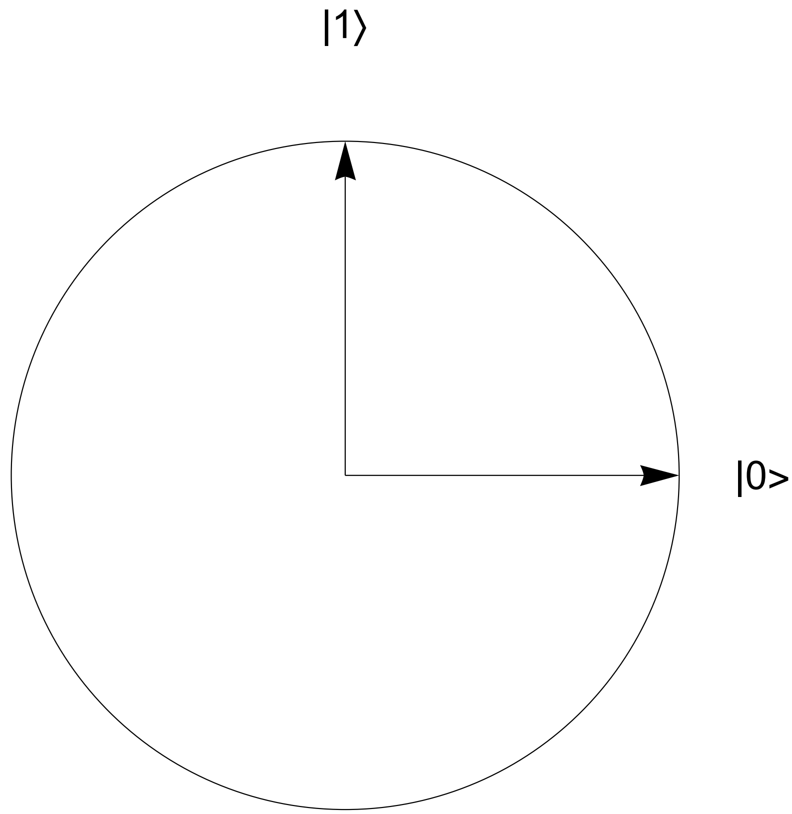

Figure 1: Some examples of qubit states.

The important thing about orthonormal bases is that an arbitrary vector[1], $|\psi\rangle \in \mathcal{H}$, can be written using a **Parseval identity**,

$$|\psi\rangle = \sum_i c_i |v_i\rangle \,, \tag{8}$$

where $c_i \in \mathcal{H}$.

For example, one orthonormal basis is the set $\{|0\rangle, |1\rangle\}$. Another is $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$.

2.2 Operators

The simplest functions on $\mathbb{C}^2$ are the **linear maps**. Linear maps that act on Hilbert spaces are called **linear operators**. A linear map on a Hilbert space, $O : \mathcal{H} \to \mathcal{H}$, satisfies

$$O(a|\psi\rangle + b|\phi\rangle) = aO(|\psi\rangle) + bO(|\phi\rangle) \qquad \forall a, b \in \mathbb{C} \text{ and } |\psi\rangle, |\phi\rangle \in \mathcal{H}. \tag{9}$$

Often, we use the shorthand $O|\psi\rangle$ for $O(|\psi\rangle)$.

Suppose we want to calculate the action of a linear map on an arbitrary qubit state, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Note

$$O|\psi\rangle = \alpha O|0\rangle + \beta O|1\rangle \,. \tag{10}$$

[1]Technicality: I think you need the Hilbert space to be separable for this to work, although I could be wrong. All finite-dimensional Hilbert spaces are separable.

Furthermore, since $O\left|i\right\rangle \in \mathbb{C}^2$ for all $i \in \{1, 2\}$, we must have

$$O\left|0\right\rangle = O_{00}\left|0\right\rangle + O_{10}\left|1\right\rangle \tag{11}$$

$$O\left|1\right\rangle = O_{10}\left|0\right\rangle + O_{11}\left|1\right\rangle \tag{12}$$

for four complex numbers, $O_{ij} \in \mathbb{C}$. Thus, the result of $O\left|\psi\right\rangle$ is completely determined by the numbers O_{ij},

$$O(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) = \alpha(O_{00}\left|0\right\rangle + O_{10}\left|1\right\rangle) + \beta(O_{10}\left|0\right\rangle + O_{11}\left|1\right\rangle). \tag{13}$$

The **braket** notation, introduced by Dirac[2], gives a nifty representation of the operator O in terms of the coefficients O_{ij}. Define the **dual vectors**, or **bras**, to be linear maps from a Hilbert space into $\mathbb{C}$. These maps are typically called **linear functionals**. Every state in $\mathcal{H}$ defines a corresponding dual vector, $\left\langle\psi\right| : \mathcal{H} \to \mathbb{C}$, through the inner product,

$$\left\langle\psi\right|(\left|\phi\right\rangle) := \left\langle\psi|\phi\right\rangle. \tag{14}$$

As a special case, the map $\gamma\left\langle 0\right| + \delta\left\langle 1\right|$ maps $\left|0\right\rangle \to \gamma$ and $\left|1\right\rangle \to \delta$. The Riesz representation theorem tells us that every dual vector can be written in the above form. In particular, dual vectors can be written with the column vector notation,

$$\gamma\left\langle 0\right| + \delta\left\langle 1\right| =: (\gamma, \delta). \tag{15}$$

With dual vectors, we can come up with a nice representation for linear operators[3], which Aaron is calling the **state representation**. For every qubit operator,

$$O = \sum_{ij} O_{ij}\left|i\right\rangle\left\langle j\right|, \tag{16}$$

where $i \in \{0, 1\}$.

We can put the numbers O_{ij} into a square grid of numbers called a **matrix**. Aaron likes to refer to the matrix associated to O as O_M. In particular,

$$O_M := \begin{pmatrix} O_{00} & O_{01} \\ O_{10} & O_{11} \end{pmatrix}. \tag{17}$$

Example: A very important operator is the **identity operator**, defined by[4]

$$\mathbb{1}\left|\psi\right\rangle := \left|\psi\right\rangle \qquad\qquad \forall \left|\psi\right\rangle \in \mathcal{H}. \tag{18}$$

Using dual vectors in finite-dimensional $\mathcal{H}$, we arrive at a **resolution of the identity**. In particular, for qubits,

$$\mathbb{1} = \left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|. \tag{19}$$

Here's some more examples, the three new entries in the table are called **Pauli matrices**:

[2] See link:Dirac 1939.

[3] in finite-dimensional spaces.

[4] I like the notation $\mathbb{1}$ for the identity operator. Aaron is using Id. Some authors like to call it I.

Name	State Rep.	Matrix Rep.
$\mathbb{1}$	$\lvert 0\rangle\langle 0\rvert + \lvert 1\rangle\langle 1\rvert$	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$
σ_z	$\lvert 0\rangle\langle 0\rvert - \lvert 1\rangle\langle 1\rvert$	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$
σ_x	$\lvert 0\rangle\langle 1\rvert + \lvert 1\rangle\langle 0\rvert$	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
σ_y	$\mathfrak{i}\lvert 0\rangle\langle 0\rvert - \mathfrak{i}\lvert 1\rangle\langle 1\rvert$	$\begin{pmatrix}0 & -\mathfrak{i}\\ \mathfrak{i} & 0\end{pmatrix}$

2.3 Unitaries

Operators that correspond to state update (such as time evolution), typically referred to as U, must do two things: it must map normalized states into normalized states and it must map a pair of orthogonal states into a pair of orthogonal states. The necessary and sufficient condition for this is that $U : \mathcal{H} \to \mathcal{H}$ is an *isometry*, which means

$$U^\dagger U = \mathbb{1}, \tag{20}$$

where $U^\dagger$ is the **adjoint** of U. I won't define the adjoint for a general operator, but I will say that if $U : \mathbb{C}^2 \to \mathbb{C}^2$ is a qubit operator, then $U^\dagger$ is given by complex conjugate transposition. In particular, we have

$$U = \sum_{ij} U_{ij} \lvert i\rangle \langle j\rvert \;\Rightarrow\; U^\dagger = \sum_{ij} U^*_{ji} \lvert i\rangle \langle j\rvert\,. \tag{21}$$

Typically, we also assume that U is **unitary**. In finite-dimensional Hilbert spaces, all isometries are unitaries. In the infinite-dimensional setting, a unitary is a surjective isometry. In either case, unitaries are operators, U, which satisfy

$$UU^\dagger = U^\dagger U = \mathbb{1}. \tag{22}$$

The set of all unitaries on $\mathbb{C}^n$ is called $U(n)$.

Example: Suppose we have a qubit unitary that maps "real" states, where a real state is of the form $a\lvert 0\rangle + b\lvert 1\rangle$ for $a, b \in \mathbb{R}$, into real states. This map is said to be an element of the orthogonal group, $O(2)$. Every $O(2)$ element is either a **rotation** or a **reflection**[5]. As a further special case, the operator σ_z from the table above is a reflection across the "x"-axis, which is the linear space spanned by $\lvert 0\rangle$.

Suppose we apply a unitary, U, to a state, $\lvert\psi\rangle = \alpha\lvert 0\rangle + \beta\lvert 1\rangle$, arriving at a new state. One way to interpret this process is that the new state is given by different coefficients in the original basis,

$$U(\alpha\lvert 0\rangle + \beta\lvert 1\rangle) = \alpha'\lvert 0\rangle + \beta'\lvert 1\rangle \tag{23}$$

for some $\alpha', \beta' \in \mathbb{C}$ which depend on U. Another way to interpret this is that the basis we express $\lvert\psi\rangle$ in has changed: Now we have

$$U(\alpha\lvert 0\rangle + \beta\lvert 1\rangle) = \alpha\lvert 0\rangle' + \beta\lvert 1\rangle'\,, \tag{24}$$

[5] An amusing geometric fact is that every rotation is a product of two reflections.

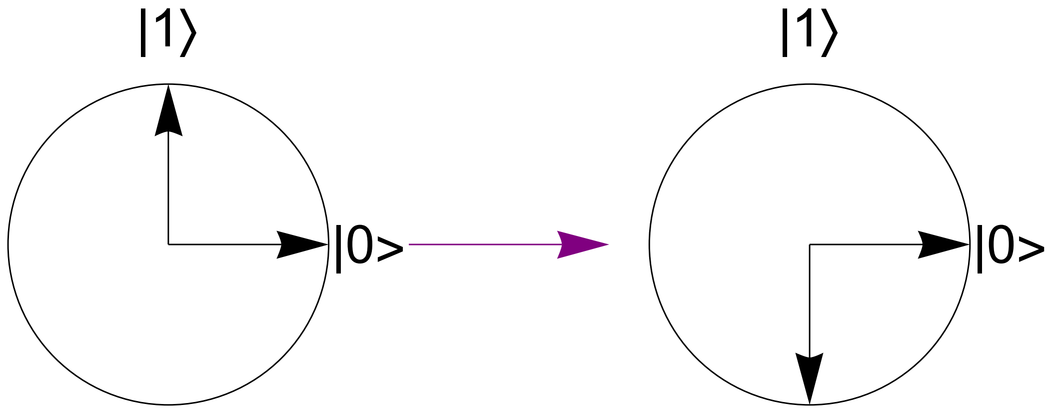

Figure 2: Here's a picture of what σ_z does to the "real" qubit states from the previous figure.

where

$$|i'\rangle := U\,|i\rangle \qquad\qquad i \in \{0,1\}. \tag{25}$$

In other words, any unitary change of state can be re-interpreted as a change of basis.

If we go back to our geometric picture of the "real" states, if state update of $|\psi\rangle$ corresponds to a rotation by the angle θ clockwise, then state update can equivalently be viewed by rotating the basis elements counter-clockwise by θ (this can be proven by explicitly writing down U, as you will do in exercise 5 for lecture 1).

A theorem from mathematics is that all Hilbert spaces of the same dimension are isomorphic, which means there's a unitary map between them. Something perhaps stronger is that given two states in the same Hilbert space, there always exists a unitary map which carries one of these states into the other. The way you prove this in general is by reducing the problem to the problem for qubits: Consider the Hilbert space as a direct sum of the space spanned by the two states you cared about and the orthogonal complement, which can be interpreted as a space of other junk states. Define your unitary to be the direct sum of the unitary in the two-dimensional space and the identity in the junk space. I'm not going to solve the two-dimensional problem here. In particular, this means that **all 1-qubit systems are equivalent**. I feel like a conjectured equivalence of multi-qubit systems doesn't follow from this logic, since multi-qubit systems are defined with a tensor product, and a given Hilbert space admits many tensor product structures. Furthermore, the unitary map between two states can mess up the tensor product structure by being an entangled map.

2.4 Measurement

Suppose $|\psi\rangle$ lives in the Hilbert space $\mathcal{H}$. Every orthonormal basis defines a **measurement**. The act of measuring the state $|\psi\rangle$ in the orthonormal basis $|v_i\rangle$ will product the state $|v_i\rangle$ with probability $|\langle v_i|\psi\rangle|^2$ (this is the so-called Born rule).

Example:

Measuring the state $|0\rangle$ in the orthonormal basis $\{|0\rangle, |1\rangle\}$ yields the state $|0\rangle$ with 100 percent probability. Measuring the same state $|0\rangle$ in the orthonormal basis $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$ yields the state $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ with probability $1/2$, and the state $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ with probability $1/2$.

To understand measurement, I'd recommend studying the **Stern-Gerlach experiment**.