Lecture Notes

edX Quantum Cryptography: Week 0

Stephanie Wehner and Nelly Ng

Welcome to the lecture notes! Here you will find details as well as additional material for edX' "Quantum Cryptography". Week 0 is a - hopefully! - gentle introduction to quantum information. We will teach you all that you need to know to work with qubits and measurements mathematically. If you are curious how such qubits can be realized physically, or simply want more details than we provide here, we recommend [1] and [2].

0.1 Mathematical notation

Let us start by recalling commonly used definitions. For a complex number $c = a + ib \in \mathbb{C}$ with $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$, we use $c^* = a - ib$ to denote its *complex conjugate*. We will also need mathematical notation that is used throughout quantum information. First, we will write vectors in a special way known as the "bra-ket" notation. While it may look a little cumbersome at first sight, it turns out to provide a convenient way of dealing with the many operations we will perform with such vectors. Let's start with two examples. We write $|v\rangle \in \mathbb{C}^2$ to denote a vector in a 2-dimensional vector space. For example,

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

The "bra" of this vector is the conjugate transpose, which for our example looks like

$$\langle v| = \left((|0\rangle)^*\right)^T = \begin{pmatrix} 1^* \\ 0^* \end{pmatrix}^T = (1\ 0) . \tag{2}$$

The general definition of the "bra-ket" notation is as follows:

Definition 0.1.1 — Ket and Bra notation. A *ket*, denoted $|\cdot\rangle$, represents a d-dimensional column vector in the complex vector space $\mathbb{C}^d$. A *bra*, denoted $\langle\cdot|$, is a d-dimensional row vector equal to the complex conjugate of the corresponding ket, namely

$$\langle\cdot| = (|\cdot\rangle^*)^T, \tag{3}$$

where * denotes the entry-wise conjugate, and T denotes the transpose.

Since we work with complex numbers, we also introduce the *absolute value* of such numbers.

Definition 0.1.2 — Absolute value of a complex number. Consider a complex number $z \in \mathbb{C}$ expressed as $z = x + iy$ where $x, y \in \mathbb{R}$ are real numbers representing the real and imaginary parts of z respectively. The *absolute value*, or otherwise known as *modulus* of z is given by

$$|z| = \sqrt{z^* z} = \sqrt{x^2 + y^2}. \tag{4}$$

For example, for $z = 1 + i2$ its absolute value is given by $|z| = \sqrt{1^2 + 2^2} = \sqrt{5}$. Very frequently, we will need to compute the inner product of two vectors in the "bra-ket" notation. This inner product is defined as follows:

Definition 0.1.3 — Inner Product. Given two d-dimensional vectors

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \qquad \text{and} \qquad |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}, \tag{5}$$

their *inner product* is given by $\langle v_1|v_2\rangle := \langle v_1|\,|v_2\rangle = \sum_{i=1}^{d} a_i^* b_i$.

Note that the inner product of two vectors $|v_1\rangle, |v_2\rangle \in \mathbb{C}^d$ is in general a complex number. Later on, we shall see that the modulus squared of the inner product $|\langle v_1|v_2\rangle|^2$ is of much significance. As an example, let us consider the inner product of the vector $|v\rangle$ given in (2) and

$$|w\rangle = \begin{pmatrix} 2 \\ 3 \end{pmatrix} . \tag{6}$$

We have

$$\langle v|w\rangle = (1\ 0)\begin{pmatrix} 2 \\ 3 \end{pmatrix} = 1\cdot 2 + 0\cdot 3 = 2 . \tag{7}$$

Exercise 0.1.1 Show that $|\langle v_1|v_2\rangle|^2 = \langle v_1|v_2\rangle\langle v_2|v_1\rangle$. Hint: first, prove the relation $(\langle v_1|v_2\rangle)^* = \langle v_2|v_1\rangle$. ■

Quite frequently, we will care about the 2-norm, or more simply length, of a vector.

Definition 0.1.4 — Length of a ket vector. Consider a ket vector

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} . \tag{8}$$

The length of $|v\rangle$ is given by

$$\| |v\rangle \|_2 = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{d} a_i^* a_i} = \sqrt{\sum_{i=1}^{d} |a_i|^2} . \tag{9}$$

If $\| |v\rangle \|_2 = 1$ we say that $|v\rangle$ has norm 1, or simply, $|v\rangle$ is *normalized*.

■ **Example 0.1.1** Consider a ket $|v\rangle = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} \in \mathbb{C}^2$. The corresponding bra is given by $\langle v| = \frac{1}{2}\begin{pmatrix} 1-i & 1+i \end{pmatrix}$, and the length of $|v\rangle$ is

$$\sqrt{\langle v|v\rangle} = \sqrt{\frac{1}{4}\cdot 2\cdot (1+i)(1-i)} = \sqrt{\frac{1}{2}(1+i-i-i^2)} = \sqrt{\frac{1}{2}\cdot 2} = 1. \tag{10}$$

■

We are assuming that your are familiar with the notion of an orthonormal basis from linear algebra. We will often write such a basis as $\{|b\rangle\}_b$. The condition of being orthonormal can be expressed succinctly as $\langle b|\hat{b}\rangle = \delta_{b\hat{b}}$ [1] for all $b, \hat{b}$.

0.2 What are qubits?

We are all intuitively familiar with the notion of bits in classical computing. How do quantum bits differ from classical bits? To see this let us start by writing classical bits somewhat differently. Instead of writing them as '0' and '1', let us first associate them with two vectors

$$0 \to |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } 1 \to |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} . \tag{11}$$

[1] $\delta_{ab} = 0$ if $a \neq b$, and $\delta_{ab} = 1$ for $a = b$.

Classical bits have many properties we take for granted, for example, we can copy them arbitrarily often. As we will see shortly, the same is not true in the quantum regime! Thinking of a physical implementation of bits, $|0\rangle$ and $|1\rangle$ could label the ground and excited state of an atom respectively. A bit can then be encoded by preparing the atom in the ground state (for $|0\rangle$) or the excited state (for $|1\rangle$). Many possible physical implementations of bits exist.

0.2.1 A single qubit

When thinking about vectors, it is indeed natural to ask whether we could have any vector $\alpha|0\rangle + \beta|1\rangle$. This is precisely the mathematical description of quantum bits. Instead of being just "0" and "1", quantum bits can be in a *superposition* between "0" and "1". Since "quantum bit" is somewhat long, researchers simply use the term "qubit" to refer to a quantum bit. Thinking of bits as vectors, a qubit can be described by a vector $|v\rangle \in \mathbb{C}^2$. The vector space $\mathbb{C}^2$ is also known as the *state space* of the qubit. An example of a qubit state is

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ . \tag{12}$$

Does any vector $|v\rangle \in \mathbb{C}^2$ form a valid qubit state? It turns out that in order to be a valid qubit, $|v\rangle$ must be normalized, just as the vectors $|0\rangle$ and $|1\rangle$ corresponding to classical bits were indeed normalized (check this for yourself!). For the moment, let us just take this as a rule, leading to the following definition.

Definition 0.2.1 — Qubit. A (pure) state of a *qubit* can be represented as a 2-dimensional ket vector $|\psi\rangle \in \mathbb{C}^2$,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \qquad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1. \tag{13}$$

The condition on α and β means that $|\psi\rangle$ is normalized. These complex numbers α and β are also called *amplitudes* of $|\psi\rangle$.

Throughout these lectures we will be mostly focusing on encoding information in qubits. However in general, quantum information can also be encoded in higher dimensional quantum systems. Therefore, one can similarly define a *qudit* as below:

Definition 0.2.2 — Qudit. A *qudit*, or a d-dimensional quantum system can be represented as a d-dimensional ket vector $|\psi\rangle \in \mathbb{C}^d$,

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \ , \qquad \text{where } \forall i, \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1. \tag{14}$$

The condition on the coefficients α_i means that $|\psi\rangle$ is a vector of length of 1.

■ **Example 0.2.1** An example of a qubit is given by the vector $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The length of $|-\rangle$ is

$$\sqrt{\langle -|-\rangle} = \sqrt{\frac{1}{2}\begin{pmatrix}1 & -1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix}} = \sqrt{\frac{1}{2}\cdot 2} = 1, \tag{15}$$

so $|-\rangle$ is normalized. ■

Exercise 0.2.1 Verify that for all values of θ, $|\Psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ is a valid qubit state. ■

In our definition of qubits, we started from a way to write classical bits as vectors $|0\rangle$ and $|1\rangle$. Note that these two vectors are orthonormal, which in the quantum notation can be expressed as $\langle 1|0\rangle = 0$ and $\langle 1|1\rangle = \langle 0|0\rangle = 1$. These two vectors thus form a basis for $\mathbb{C}^2$, in that any vector $|v\rangle \in \mathbb{C}^2$ can be written as $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ for some coefficients $\alpha, \beta \in \mathbb{C}$. This basis corresponding to "classical" bits is used so often that it carries a special name:

Definition 0.2.3 — Standard basis. Consider the 2-dimensional complex vector space $\mathbb{C}^2$. The *standard basis*, or sometimes known as the *computational basis*, $\mathscr{S} = \{|0\rangle, |1\rangle\}$ is an orthonormal basis for this vector space, where the basis vectors are

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{16}$$

Of course, there might be many other bases for $\mathbb{C}^2$. Another favorite basis which we will use rather frequently is the Hadamard basis defined as follows:

Definition 0.2.4 — Hadamard basis. The *Hadamard basis* is an orthonormal basis $\mathscr{H} = \{|+\rangle, |-\rangle\}$ consisting of the two basis elements

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and } |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{17}$$

Let us verify that this is indeed an orthonormal basis using the "bra-ket" notation. As we have seen in Example 0.2.1, $|-\rangle$ is normalized. Similarly,

$$\langle +|+\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\cdot 2 = 1, \qquad \Longrightarrow, \sqrt{\langle +|+\rangle} = 1 \tag{18}$$

so $|+\rangle$ is also normalized. Furthermore, the inner product

$$\langle +|-\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0, \tag{19}$$

so $|+\rangle$ and $|-\rangle$ are orthogonal to each other.

Exercise 0.2.2 Express $|1\rangle$ in the Hadamard basis. That is, find coefficients α and β such that $|1\rangle = \alpha|+\rangle + \beta|-\rangle$. ■

0.2.2 Multiple qubits

Classically, if we have two bits, we write them as '00', '01' and so forth. But how can we write two qubits? One strategy is to again associate each of the two classical bits $x_1, x_2 \in \{0,1\}^2$ with a vector. Labelling the first qubit A and the second one B, we could perform the mapping from strings to orthonormal vectors as

$$0_A 0_B \to |00\rangle_{AB} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad 0_A 1_B \to |01\rangle_{AB} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$1_A 0_B \to |10\rangle_{AB} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad 1_A 1_B \to |11\rangle_{AB} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Note that the resulting vectors are in $\mathbb{C}^d$ with dimension $d = 2^2 = 4$, where the dimension corresponds to the number of possible strings. It turns out that one can write a two-qubit state $|\psi\rangle_{AB} \in \mathbb{C}^4$ as a superposition of these vectors, where we again demand that $|\psi_{AB}\rangle$ is normalized. As an example, let us consider a state $|\psi_{AB}\rangle$ that is an equal superposition of all the above standard basis vectors:

$$|\psi\rangle_{AB} = \frac{1}{2}|00\rangle_{AB} + \frac{1}{2}|01\rangle_{AB} + \frac{1}{2}|10\rangle_{AB} + \frac{1}{2}|11\rangle_{AB} \tag{20}$$

$$= \frac{1}{2}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{21}$$

$$= \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}. \tag{22}$$

The sum of amplitudes $\frac{1}{2}$ squared is $4 \cdot \frac{1}{2^2} = 1$, therefore $|\psi\rangle$ is a valid two qubit quantum state. As you might have guessed, we now proceed analogously when considering n qubits. To address multiple qubits, we first look at the vector representation for multiple classical bits. For binary strings of length n, consider the vector space $\mathbb{C}^{2^n}$, where each coordinate is labelled by a string $x = x_1, \ldots, x_n$. There are a total of $d = 2^n$ such strings, so we can label each string x with a different integer $i \in [1, d]$. We can then express the string x as a vector $|x\rangle$ that is 0 everywhere, except at the position labelled by i. A quantum state of n qubits can then be written as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \ , \tag{23}$$

with $\alpha_x \in \mathbb{C}$ and $\sum_x |\alpha_x|^2 = 1$. The numbers α_x are again called *amplitudes*. We emphasize that the dimension of the vector space $\mathbb{C}^{2^n}$ increases exponentially with the number n of bits. The space $\mathbb{C}^d$ with $d = 2^n$ is thereby called the *state space* of n qubits. This means that we need an exponential number of parameters α_x to keep track of only n qubits, in sharp contrast to the n parameters $x_1, \ldots, x_n$ to describe n classical bits.

You might wonder whether this was the only way to write down qubits. After all, we had simply chosen some mapping from strings of length n to vectors in $\mathbb{C}^d$. Could we have chosen any other mapping from strings to vectors? It turns out that the answer to this is yes - as long as each string gets mapped to a vector that is orthonormal to the others. The mapping above, however, is very convenient and generally adopted within the realm of quantum computing. Analogous to the case of a single qubit, the basis given by the set of vectors $\{|x\rangle \mid x \in \{0,1\}^n\}$ is called the *standard/computational basis*.

Definition 0.2.5 — Standard basis for n qubits. Consider the state space of n qubits $\mathbb{C}^d$, where $d = 2^n$. For each distinct string $x \in \{0,1\}^n$, associate x with a distinct integer $i \in \{1, 2, \cdots d\}$. The standard basis for $\mathbb{C}^d$ is an orthonormal basis given by $\mathscr{S}_n = \{|x\rangle\}_{x \in \{0,1\}^n}$,

where $|x\rangle$ are d-dimensional vectors

$$|x\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \longrightarrow i\text{-th position.} \tag{24}$$

Let us summarize our discussion in the following definition of an n qubit quantum state.

Definition 0.2.6 An n-qubit state $|\psi\rangle \in \mathbb{C}^d$ with $d = 2^n$ can be written as a superposition of standard basis elements

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \qquad \text{where } \forall x, \alpha_x \in \mathbb{C} \text{ and } \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1. \tag{25}$$

Let us now consider two examples of two qubit states. The first is so famous it carries a special name and we will see it very frequently in the course of these notes.

■ **Example 0.2.2** Consider two qubits A and B, in the two qubit state known as the *EPR pair* [2], one can label the joint state as AB

$$|\text{EPR}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{26}$$

which is an equal superposition between the vectors $|00\rangle_{AB}$ and $|11\rangle$. The length of this vector is given by the (square root of) inner product

$$\langle \text{EPR}|\text{EPR}\rangle_{AB} = \frac{1}{\sqrt{2}}(\langle 00|_{AB} + \langle 11|_{AB}) \cdot \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{27}$$

$$= \frac{1}{2}(\underbrace{\langle 00|00\rangle_{AB}}_{1} + \underbrace{\langle 00|11\rangle_{AB}}_{0} + \underbrace{\langle 11|00\rangle_{AB}}_{0} + \underbrace{\langle 11|11\rangle_{AB}}_{1}) \tag{28}$$

$$= \frac{1}{2}\cdot 2 = 1, \qquad \Longrightarrow \qquad \sqrt{\langle EPR|EPR\rangle} = 1. \tag{29}$$

■

■ **Example 0.2.3** Consider the two qubit state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |11\rangle_{AB}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}. \tag{30}$$

For this state, the second qubit always corresponds to bit 1. We will later see that this is significantly different state compared to $|\text{EPR}\rangle_{AB}$ (hint: it is not entangled!). ■

0.3 Tensor Product: how to combine qubits

Let's imagine that we have two qubits, A and B. We know that we can describe the state of A as $|\psi\rangle_A$ and the one of B as $|\phi\rangle_B$. How can we write down the combined state $|\psi\rangle_{AB}$ of A *and* B

[2] The acronym EPR stands for Einstein, Podolsky and Rosen. Later we shall show that this state is entangled.

together? The rule for computing the joint state is given by the so-called tensor product (sometimes also called Kronecker product). For two qubits

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}, \tag{31}$$

$$|\phi\rangle_B = \alpha_B |0\rangle_B + \beta_B |1\rangle_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix}, \tag{32}$$

the joint state $|\psi\rangle_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ can be expressed as the tensor product of individual vectors $|\psi\rangle_A$ and $|\phi\rangle_B$

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi\rangle_B = \begin{pmatrix} \alpha_A |\psi\rangle_B \\ \beta_A |\psi\rangle_B \end{pmatrix} = \begin{pmatrix} \alpha_A \alpha_B \\ \alpha_A \beta_B \\ \beta_A \alpha_B \\ \beta_A \beta_B \end{pmatrix}. \tag{33}$$

As you may have guessed, we can of course also combine the state of two quantum systems A and B if they are larger than just one qubit. The general definition of the tensor product of two vectors is given by

Definition 0.3.1 Given two vectors $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$ respectively, the tensor product is given by

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 |\psi_2\rangle \\ \vdots \\ \alpha_d |\psi_2\rangle \end{pmatrix}, \tag{34}$$

and $|\psi_1\rangle \otimes |\psi_2\rangle$ lies in the state space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$.

The following simplified (or rather, lazy) notations are commonly used in quantum information:

$$\text{Omitting the tensor product symbol:} \quad |\psi\rangle_A \otimes |\psi\rangle_B = |\psi\rangle_A |\psi\rangle_B. \tag{35}$$

$$\text{Writing classical bits as a string:} \quad |0\rangle_A \otimes |0\rangle_B = |0\rangle_A |0\rangle_B = |00\rangle_{AB}. \tag{36}$$

$$\text{Combining several identical states:} \quad |\psi\rangle_1 \otimes |\psi\rangle_2 \cdots \otimes |\psi\rangle_n = |\psi\rangle^{\otimes n}. \tag{37}$$

Proposition 0.3.1 The tensor product satisfies several useful properties:

1. Distributive: $|\psi_1\rangle \otimes (|\psi_2\rangle + |\psi_3\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi_3\rangle$.
   Similarly, $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\psi_3\rangle = |\psi_1\rangle \otimes |\psi_3\rangle + |\psi_2\rangle \otimes |\psi_3\rangle$.
2. Associative: $|\psi_1\rangle \otimes (|\psi_2\rangle \otimes |\psi_3\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) \otimes |\psi_3\rangle$.
3. NOT commutative: In general, $|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle$ unless of course $|\psi_1\rangle = |\psi_2\rangle$.

These relations hold not only for kets, but also for bras.

To understand the definition of the tensor product, let us have a look at a few examples. The first relates to the definition of the standard basis for multiple qubits. Indeed, you may have been wondering, if we could have proceeded in a somewhat less ad hoc manner than starting from classical strings $x \in \{0,1\}^n$ and assigning to them vectors $|x\rangle$ in a space of dimension $d = 2^n$. Indeed, you may have started to wonder why n qubits resulted in a state space of a dimension that is exponential in n in the first place. The reason for this, is that the law of quantum mechanics tells us that the state space of two quantum systems is indeed combined by the tensor product.

■ **Example 0.3.1** Let's recover the standard basis of two qubits, from the standard basis of the individual qubits using the tensor product rule. Recall that the standard basis for two qubits AB is

given by

$$|00\rangle_{AB} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix},\ |01\rangle_{AB} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},\ |10\rangle_{AB} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix},\ |11\rangle_{AB} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

This basis can be constructed, by taking the tensor product of standard basis elements for individual qubits: $|0\rangle_A \otimes |0\rangle_B, |0\rangle_A \otimes |1\rangle_B, |1\rangle_A \otimes |0\rangle_B, |1\rangle_A \otimes |1\rangle_B$. For example, consider

$$|1\rangle_A \otimes |0\rangle_B = \begin{pmatrix}0\\1\end{pmatrix} \otimes |0\rangle_B = \begin{pmatrix}0\,|0\rangle_B\\1\,|0\rangle_B\end{pmatrix} = \begin{pmatrix}0\cdot 1\\0\cdot 0\\1\cdot 1\\1\cdot 0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle_{AB}. \tag{38}$$

■

We have already seen a few other examples of two qubit states. Let's see whether we can recover them from two individual qubit states using the tensor product.

■ **Example 0.3.2** Consider the states $|+\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)$ and $|1\rangle_B$. The joint state $|\psi\rangle_{AB}$ is given by

$$|\psi\rangle_{AB} = |+\rangle_A \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot|1\rangle_B\\1\cdot|1\rangle_B\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}. \tag{39}$$

One can also express the joint state in the standard basis by:

$$\begin{aligned}|\psi\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |1\rangle_B && (40)\\ &= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |1\rangle_B) && (41)\\ &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |11\rangle_{AB}). && (42)\end{aligned}$$

This is the state we have seen in Example 0.2.3. ■

■ **Example 0.3.3** Consider the states $|+\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)$ and $|+\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B)$. The joint state $|\psi\rangle_{AB}$ is

$$\begin{aligned}|\psi\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) && (43)\\ &= \frac{1}{2}(|00\rangle_{AB} + |01\rangle_{AB} + |10\rangle_{AB} + |11\rangle_{AB}) && (44)\\ &= \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}. && (45)\end{aligned}$$

This is the state we have seen in (20), which is an equal superposition of all standard basis vectors for the two qubits. ■

The following is an example of a state that can actually not be expressed as the tensor product of two qubit states. Such states are rather special, and play an important role later in our course. Nevertheless, let's have a look at it to see how we might also express a two qubit state in different bases.

■ **Example 0.3.4** Consider the state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B). \tag{46}$$

Let us express this state in terms of the standard basis, by expanding the terms

$$|+\rangle_A|+\rangle_B = \frac{1}{2}(|0\rangle_A + |1\rangle_A)(|0\rangle_B + |1\rangle_B) = \frac{1}{2}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB}) \tag{47}$$

$$|-\rangle_A|-\rangle_B = \frac{1}{2}(|0\rangle_A - |1\rangle_A)(|0\rangle_B - |1\rangle_B) = \frac{1}{2}(|00\rangle_{AB} - |10\rangle_{AB} - |01\rangle_{AB} + |11\rangle_{AB}). \tag{48}$$

Substituting this into Eq. (46) gives

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B) \tag{49}$$

$$= \frac{1}{2\sqrt{2}}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB} + |00\rangle_{AB} - |10\rangle_{AB} - |01\rangle_{AB} + |11\rangle_{AB}) \tag{50}$$

$$= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = |\text{EPR}\rangle_{AB} \tag{51}$$

where $|\text{EPR}\rangle_{AB}$ is the state we have seen previously in Example 0.2.2. We see that the coefficients of $|\text{EPR}\rangle_{AB}$ are the same whether we write it in the Hadamard basis or the standard basis. ■

0.4 Simple measurements

Let us consider what happens if we measure a qubit. Classically, you can think of the measurement of a bit as simply a readout: we have a system that encodes the state '0' and '1' and we make a measurement to find out which one it is.

0.4.1 Measurement in the standard basis

Let's first consider a single qubit. Quantum measurements can result in probabilistic outcomes, highlighting that quantum information and classical information really are fundamentally different. For example, if the state $|\psi\rangle \in \mathbb{C}^2$ is a superposition between $|0\rangle$ and $|1\rangle$, then upon measuring $|\psi\rangle$, we obtain different measurement outcomes corresponding to some probability distribution. How are such probabilities generated? The probability of different outcomes, for instance for outcome '0', can be computed by, roughly speaking, "looking at how much '0' is actually in our qubit vector". This is quantified by the inner product between $|\psi\rangle$ and $|0\rangle$. More concretely, consider a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are complex numbers. Upon measuring the qubit, one obtains the outcome "0" with probability p_0 and "1" with probability p_1. These probabilities can be determined by computing the inner products

$$p_0 = |\langle\psi|0\rangle|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right|^2 = |\alpha|^2, \tag{52}$$

$$p_1 = |\langle\psi|1\rangle|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right|^2 = |\beta|^2. \tag{53}$$

We now see a good reason for the condition $|\alpha|^2+|\beta|^2=1$: it means that $p_0+p_1=1$, that is, the probabilities of observing '0' and '1' add up to one. In quantum computer science, it is customary to label the outcomes '0' for "$|0\rangle$" and '1' for "$|1\rangle$" [3], while in physics people often use $+1$ for "$|0\rangle$" and -1 for "$|1\rangle$".

Application: Randomness from a deterministic process

Can we do anything interesting with what we have learned so far? It turns out the answer is yes: by preparing just single qubits and measuring in the standard basis, we can in principle achieve a task that it is impossible classically. Namely, we can produce true random numbers. Consider the following process illustrated in Figure 1: first, prepare a qubit in the state $|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. Next, measure this state in the standard basis. The probability of obtaining each outcome can then

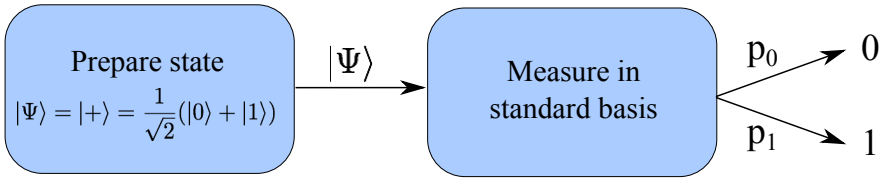

Figure 1: Generation of genuine randomness from the preparation of a qubit in superposition.

be calculated by evaluating the inner products:

$$p_0=|\langle+|0\rangle|^2=\left|\frac{1}{\sqrt{2}}(\langle 0|+\langle 1|)|0\rangle\right|^2=\left|\frac{1}{\sqrt{2}}(\underbrace{\langle 0|0\rangle}_{1}+\underbrace{\langle 1|0\rangle}_{0})\right|^2=\frac{1}{(\sqrt{2})^2}=\frac{1}{2}, \tag{54}$$

$$p_1=|\langle+|1\rangle|^2=\left|\frac{1}{\sqrt{2}}(\langle 0|+\langle 1|)|1\rangle\right|^2=\left|\frac{1}{\sqrt{2}}(\underbrace{\langle 0|1\rangle}_{0}+\underbrace{\langle 1|1\rangle}_{1})\right|^2=\frac{1}{(\sqrt{2})^2}=\frac{1}{2}. \tag{55}$$

This simple example already tells us something about the power of quantum information: We could build a machine that deterministically prepares the qubit $|+\rangle$, followed by a measurement in the standard basis. Since $p_0=p_1=1/2$, this machine allows us to produce a perfect random number - even though no randomness has been used inside our machine! In contrast, one can prove that no classical deterministic machine can produce random numbers from scratch.

We saw how to measure a single qubit in the standard basis. The rule for computing probabilities of measurement outcomes generalizes in a direct way to measuring n-qubit states. Indeed, consider an n-qubit quantum state

$$|\Psi\rangle=\sum_{x\in\{0,1\}^n}\alpha_x|x\rangle\ . \tag{56}$$

What happens when $|\Psi\rangle$ is measured in the standard basis $\{|x\rangle\}_x$? It turns out that the probability of outcome x is given by $p_x=|\langle x|\Psi\rangle|^2=|\alpha_x|^2$, explaining again the need for normalization of the vector $|\Psi\rangle$.

0.4.2 Measuring a qubit in other bases

Can we measure our qubit in any other basis? The answer to this is yes! Indeed this is another feature that distinguishes quantum from classical, where the only basis around is the standard basis. To find out how to analyze such a more general setting, let us first take a step back and consider how we found the probabilities above. When measuring in the standard basis, the probabilities are

[3] And more generally, x for outcomes "$|x\rangle$"

given by the squared amplitudes when writing out the state in terms of the standard basis. When measuring a qubit in a different orthonormal basis, given by vectors $\mathscr{G} = \{|v\rangle, |v^{\perp}\rangle\}$, it is intuitive that we would have to express the qubit in the new basis. That is, we need to find amplitudes $\hat{\alpha}$ and $\hat{\beta}$ such that

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \hat{\alpha}|v\rangle + \hat{\beta}|v^{\perp}\rangle \ . \tag{57}$$

■ **Example 0.4.1** As an example, let consider again the qubit $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$. Instead of measuring it in the standard basis, let us now measure in the basis $\mathscr{H} = \{|+\rangle, |-\rangle\}$ given by the two orthonormal vectors $|+\rangle$ and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$. Clearly, we can write the qubit as $1 \cdot |+\rangle + 0 \cdot |-\rangle$. Thus the probability of obtaining measurement outcome "$|+\rangle$" is 1. We thus see that the probabilities of measurement outcomes depends dramatically on the basis in which we measure. ■

■ **Example 0.4.2** Consider measuring an arbitrary qubit $\alpha|0\rangle + \beta|1\rangle$ in the basis $\{|+\rangle, |-\rangle\}$. To find out how to express the qubit in this other basis, it is convenient to determine how the basis elements $|0\rangle$ and $|1\rangle$ look like in this basis. We find that

$$|0\rangle = \frac{1}{2}[(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)] = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \ , \tag{58}$$

$$|1\rangle = \frac{1}{2}[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)] = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \ . \tag{59}$$

We thus have

$$\alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}[\alpha(|+\rangle + |-\rangle) + \beta(|+\rangle - |-\rangle)] = \tag{60}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \ . \tag{61}$$

This means that we obtain outcome "$|+\rangle$" with probability $|\alpha+\beta|^2/2$ and outcome "$|-\rangle$" with probability $|\alpha-\beta|^2/2$. ■

Exercise 0.4.1 Consider the state $|\Psi\rangle = |0\rangle$. What are the probabilities p_0, p_1 for measuring $|\Psi\rangle$ in the standard basis? What are the probabilities p_+, p_- for measuring $|\Psi\rangle$ in the Hadamard basis? ■

Quite often we do not care about the entire probability distribution, but just the probability of one specific outcome. Is there a more efficient way to find this probability than to rewrite the entire state $|\psi\rangle$ in another basis? To investigate this, let us consider a single qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ . \tag{62}$$

Remember that the elements of the standard basis are orthonormal. This means that

$$(|0\rangle)^{\dagger}|0\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \ , \tag{63}$$

$$(|0\rangle)^{\dagger}|1\rangle = \begin{pmatrix} 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \ . \tag{64}$$

Because the vectors are orthonormal, we could thus have found the desired probabilities by simply computing the inner product between two vectors, as claimed above. Specifically, when given the

qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we obtain outcomes "$|0\rangle$" and "$|1\rangle$" with probabilities

$$p_0 = |\langle 0|\psi\rangle|^2 = \left|(1\ 0)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\alpha|^2 \tag{65}$$

$$p_1 = |\langle 1|\psi\rangle|^2 = \left|(0\ 1)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\beta|^2 \tag{66}$$

$$\tag{67}$$

■ **Example 0.4.3** Suppose we measure $|0\rangle$ in the Hadamard basis $\mathscr{H}$ (see above). The probabilities of observing outcomes "$|+\rangle$" and "$|-\rangle$" are given by

$$p_+ = |\langle +|0\rangle|^2 = \left|(1/\sqrt{2}\ 1/\sqrt{2})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,, \tag{68}$$

$$p_- = |\langle -|0\rangle|^2 = \left|(1/\sqrt{2}\ -1/\sqrt{2})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,. \tag{69}$$

■

For multiple qubits, the rule for finding probabilities is analogous.

Definition 0.4.1 Suppose that we measure a quantum state $|\psi\rangle$ in the orthonormal basis $\{|b_j\rangle\}_{j=1}^d$. The probability of observing outcome "b_j" can be found by computing

$$p_j = |\langle b_j|\psi\rangle|^2\,. \tag{70}$$

The post-measurement state when obtaining outcome "b_j" is given by $|b_j\rangle$.

Let us now consider some examples to gain intuition on measuring quantum systems in different bases. First, let us have a look at a single qubit example.

■ **Example 0.4.4** Consider the qubit $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, and measure the qubit in the $\{|+\rangle, |-\rangle\}$ basis. The probabilities of obtaining "+" and "–" can be evaluated as follows:

$$p_+ = |\langle\Psi|+\rangle|^2 = \left|\frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle + |1\rangle)\right|^2 \tag{71}$$

$$= \frac{1}{4}\left|\langle 0|0\rangle + \langle 0|1\rangle - i\langle 1|0\rangle - i\langle 1|1\rangle\right|^2 \tag{72}$$

$$= \frac{1}{4}|1-i|^2 \tag{73}$$

$$= \frac{1}{4}(1-i)(1+i) = \frac{1}{2}, \tag{74}$$

$$p_- = |\langle\Psi|-\rangle|^2 = \left|\frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle - |1\rangle)\right|^2 \tag{75}$$

$$= \frac{1}{4}\left|\langle 0|0\rangle - \langle 0|1\rangle - i\langle 1|0\rangle + i\langle 1|1\rangle\right|^2 \tag{76}$$

$$= \frac{1}{4}|1+i|^2 \tag{77}$$

$$= \frac{1}{4}(1+i)(1-i) = \frac{1}{2}, \tag{78}$$

This example shows that when the states involved have complex-valued amplitudes, one has to take extra caution when evaluating the inner product: namely when taking the bra $\langle\Psi|$, one should

remember to alter the +/- sign whenever a complex number is involved (since the bra $\langle\Psi|$ is the conjugate transpose of the ket $|\Psi\rangle$). ■

While we will generally talk about n-qubits, we can of course also consider a quantum system comprised of three levels $|0\rangle$, $|1\rangle$, and $|2\rangle$, i.e. a qutrit. The rule for obtaining the probabilities of measurement outcomes remains unchanged.

■ **Example 0.4.5** Consider a *qutrit*, which is a 3-dimensional quantum system represented by the vector

$$|v\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\end{pmatrix}, \tag{79}$$

and measure in the basis $\mathscr{B} = \{|b_1\rangle, |b_2\rangle, |b_3\rangle\}$ where

$$|b_1\rangle = \begin{pmatrix}1\\0\\0\end{pmatrix}, \qquad |b_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\end{pmatrix}, \qquad |b_3\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\end{pmatrix}. \tag{80}$$

The probabilities of obtaining each outcome can be calculated as follows:

$$p_{b_1} = |\langle b_1|v\rangle|^2 = \frac{1}{2}, \tag{81}$$

$$p_{b_2} = |\langle b_2|v\rangle|^2 = \langle b_2|v\rangle\langle v|b_2\rangle = \frac{1}{2\sqrt{2}}(1+1)\cdot\frac{1}{2\sqrt{2}}(1+1) = \frac{1}{2}, \tag{82}$$

$$p_{b_3} = |\langle b_3|v\rangle|^2 = \langle b_3|v\rangle\langle v|b_3\rangle = \frac{1}{2\sqrt{2}}(1-1)\cdot\frac{1}{2\sqrt{2}}(1-1) = 0. \tag{83}$$

■

Expectation values

Physicists (but also computer scientists!) like to compute expectation values of measurement outcomes, as they provide an indication of the average behavior, if one was to perform a measurement many times (however we shall see later, that the measurement will perturb the state!). Let us suppose that we measure a qubit $|\Psi\rangle$ in the standard basis $\{|0\rangle, |1\rangle\}$. We will also adopt the physics convention of labelling these outcomes ± 1. This means that we associate the outcome "$|0\rangle$" with outcome $+1$, and outcome "$|1\rangle$" with outcome -1. The expectation value the outcome obtained when measuring $|\Psi\rangle$ is then

$$E = 1\cdot|\langle 0|\psi\rangle|^2 - 1\cdot|\langle 1|\psi\rangle|^2. \tag{84}$$

Note that since $|\langle 0|\psi\rangle|^2 = \langle\psi|0\rangle\langle 0|\psi\rangle$, we have

$$E = \langle\psi|\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)|\psi\rangle = \langle\psi|Z|\psi\rangle \tag{85}$$

where $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. As we shall see later, Z is called the Pauli-Z matrix.

0.4.3 Measuring multiple systems

We saw how to measure some quantum state $|\psi\rangle$. Let us now consider what happens if we measure the state of multiple qubits, where we think of measuring each qubit in a separate basis. To understand this, it is useful to realize that a basis for the joint state space $\mathbb{C}_A^{d_A}\otimes\mathbb{C}_B^{d_B}$ can be obtained from bases for the individual state spaces $\mathbb{C}_A^{d_A}$ and $\mathbb{C}_B^{d_B}$. Specifically, if $\{|b_j^A\rangle\}_j$ is a basis for $\mathbb{C}_A^{d_A}$ and $\{|b_j^B\rangle\}_j$ is a basis for the state space $\mathbb{C}_B^{d_B}$, then the set of vectors $\{\{|b_j^A\rangle\otimes|b_k^B\rangle\}_{j=1}^{d_A}\}_{k=1}^{d_B}$ gives a basis for $\mathbb{C}_A^{d_A}\otimes\mathbb{C}_B^{d_B}$.

■ **Example 0.4.6** Consider the basis $\{|0\rangle_A, |1\rangle_A\}$ for qubit A, and the basis $\{|+\rangle_B, |-\rangle_B\}$ for qubit B. A basis for the joint state AB is then given by $\{|0\rangle_A|+\rangle_B, |0\rangle_A|-\rangle_B, |1\rangle_A|+\rangle_B, |1\rangle_A|-\rangle_B\}$. ■

Let us now think how we might construct some measurement for two quantum states from measurements of the individual ones. Suppose we measure particle A in the basis $\{|b_j^A\rangle\}_j$ and particle B in the basis $\{|b_k^B\rangle\}_k$ when the joint state of both particles is given by $|\psi\rangle_{AB}$. What is the probability that we obtain outcome " $|b_j^A\rangle$ " on A, and outcome " $|b_k^B\rangle$ " on B? To find such joint probabilities, we first write down the joint basis of quantum states A and B as above: $\{\{|b_j^A\rangle|b_k^B\rangle\}_j\}_k$. We can then apply the usual rule to compute the probability as

$$p_{jk} = |\langle b_j^A|\langle b_k^B||\psi\rangle_{AB}|^2 \,. \tag{86}$$

■ **Example 0.4.7** Consider two qubits in an EPR pair

$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{87}$$

and measure them both in the standard basis. The probabilities of obtaining outcomes 00, 01, 10, and 11 are given by

$$p_{00} = p_{11} = \frac{1}{2}, \tag{88}$$

$$p_{01} = p_{10} = 0. \tag{89}$$

■

0.5 Transformations on qubits

Just like on classical bits, we can perform operations on qubits. Since we can write quantum states as vectors, we are looking for a linear operator U that maps vectors to vectors

$$|\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle \tag{90}$$

for some matrix U. If $|\psi_{\text{in}}\rangle \in \mathbb{C}^d$, then U is a $d \times d$ matrix with complex entries. Recall that for any quantum state we have $\langle\psi|\psi\rangle = 1$. And we have also seen that this is quite important, because it tells us that the sum of the probabilities, if we measure the state, should also be 1. This means that the operation U should preserve the inner product [4], i.e.,

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}|U^\dagger U|\psi_{\text{in}}\rangle = 1 \,. \tag{91}$$

Similarly, the same should be true for the operation $U^\dagger$

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}|UU^\dagger|\psi_{\text{in}}\rangle = 1 \,. \tag{92}$$

We see that in order to preserve probabilities the operation U should preserve the length of any vector. This is the case precisely if $U^\dagger U = UU^\dagger = \mathbb{I}$, where $\mathbb{I}$ is the identity matrix. Such a matrix $\mathbb{I}$ will continually appear throughout these notes, and we define it below.

Definition 0.5.1 — Identity. The identity $\mathbb{I}$ is a diagonal, square matrix where each diagonal element is equal to 1, i.e.

$$\mathbb{I} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}. \tag{93}$$

[4] Remember that $(U|\psi\rangle)^\dagger = \langle\psi|U^\dagger$.

For any dimension d, we denote the $d \times d$ identity matrix as $\mathbb{I}_d$.

R The identity matrix is a unitary operation that preserves all quantum states, i.e. for any quantum state $|\psi\rangle$, $\mathbb{I}|\psi\rangle = |\psi\rangle$.

We will typically not specify the dimension of the identity matrix explicitly if it can be inferred from context. The only allowed operations in the quantum regime are unitary operations.

Definition 0.5.2 — Unitary operation. An operation U is unitary if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.

To gain some intuition about unitary operations, let us have a look at some useful examples.

■ **Example 0.5.1** Consider the matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{94}$$

You can convince yourself that $H^\dagger = H$ and thus

$$H^\dagger H = HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I}\,. \tag{95}$$

That is, H is unitary. We have that

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle\ . \tag{96}$$

Similarly, you can convince yourself that $H|1\rangle = |-\rangle$. We thus see that H transforms the computational basis $\{|0\rangle, |1\rangle\}$ into the Hadamard basis $\{|+\rangle, |-\rangle\}$. Indeed, H is called the *Hadamard transform*. ■

Note that $\mathbb{I}$ is itself also a unitary operation, called the *identity operation*. It just means that the state is not transformed at all. Let us now consider a somewhat more complicated operation.

■ **Example 0.5.2** For any $\theta \in \mathbb{R}$, consider the matrix

$$R(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}. \tag{97}$$

The adjoint of this matrix is given by

$$R^\dagger(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{98}$$

and therefore

$$R(\theta)R^\dagger(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{99}$$

$$= \begin{pmatrix} \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} & 0 \\ 0 & \sin^2\frac{\theta}{2} + \cos^2\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{100}$$

One can check that $R^\dagger(\theta)R(\theta) = \mathbb{I}$ as well, therefore $R(\theta)$ is unitary.

$$R(\theta)|0\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2} \end{pmatrix}. \tag{101}$$

$$R(\theta)|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin\frac{\theta}{2} \\ \cos\frac{\theta}{2} \end{pmatrix}. \tag{102}$$

If we take $\theta = \frac{\pi}{2}$, then $\cos\frac{\theta}{2} = \sin\frac{\theta}{2} = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}$ and therefore

$$R\left(\frac{\pi}{2}\right)|0\rangle = |+\rangle \qquad \text{and} \qquad R\left(\frac{\pi}{2}\right)|1\rangle = -|-\rangle\,. \tag{103}$$

■

0.5.1 Pauli matrices as unitary operations

In this section we look at the Pauli matrices, commonly denoted as X, Y, Z. These are quite famous in physics, but also have rather interesting interpretations as bit and phase flip operations as we will see below. The Pauli matrices are unitary 2×2 matrices, with the following form

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{104}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{105}$$

$$Y = iXZ. \tag{106}$$

The Pauli-X matrix acts on the standard basis vectors by interchanging them:

$$X|0\rangle = |1\rangle\ , \tag{107}$$

$$X|1\rangle = |0\rangle\ . \tag{108}$$

In analogy to classical computation X is also referred to as NOT, since it changes 0 to 1 and vice versa. This is also known as a *bit flip* operation. On the other hand, the Pauli-Z matrix acts on the standard basis by introducing a *phase flip*

$$Z|0\rangle = |0\rangle\ , \tag{109}$$

$$Z|1\rangle = -|1\rangle\ . \tag{110}$$

The Pauli-Z matrix has the effect of interchanging the vectors $|+\rangle$ and $|-\rangle$. To be precise, we have

$$Z|+\rangle = Z(|0\rangle + |1\rangle)/\sqrt{2} = (Z|0\rangle + Z|1\rangle)/\sqrt{2} = (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle\,. \tag{111}$$

Similarly, $Z|-\rangle = |+\rangle$. We thus see that Z acts like a bit flip upon the Hadamard basis, while it acts like a phase flip in the standard basis. Applying both a bit and a phase flip gives $Y = iXZ$. The i makes Y Hermitian, that is, $Y^\dagger = Y$. This matrix, when acted upon the standard basis vectors, introduces a bit flip and a phase flip:

$$Y|0\rangle = iXZ|0\rangle = iX|0\rangle = i|1\rangle\,. \tag{112}$$

$$Y|1\rangle = -iXZ|0\rangle = -iX|1\rangle = -i|0\rangle\,. \tag{113}$$

Exercise 0.5.1 Verify that the Pauli matrices X, Z and Y are indeed unitary. ■

0.6 No cloning!

In this section we show that arbitrary qubits, unlike classical bits, cannot be copied. Here, we provide a slightly different proof than shown in the lecture. If we did have a copying unitary C it

should give us $C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ for *any* input qubit $|\psi\rangle$. By contradiction, let us suppose such a unitary existed. In particular, such a unitary gives us

$$C(|\psi_1\rangle \otimes |0\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle \tag{114}$$
$$C(|\psi_2\rangle \otimes |0\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle \tag{115}$$

Since C is a unitary, we have $C^\dagger C = \mathbb{I}$ and hence

$$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle\langle 0|0\rangle \tag{116}$$
$$= (\langle\psi_1| \otimes \langle 0|)C^\dagger C(|\psi_2\rangle \otimes |0\rangle) \tag{117}$$
$$= (\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) = (\langle\psi_1|\psi_2\rangle)^2. \tag{118}$$

Clearly whenever $0 < |\langle\psi_1|\psi_2\rangle| < 1$, the above cannot hold and hence such a copying unitary C cannot exist. Note that $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = |+\rangle$, for example, have precisely this property.

The fact that we cannot clone, that is, copy arbitrary quantum states shows that quantum information really is very different from classical information. It also allows us to gain further understanding: note that this also means that we cannot determine α and β from a single copy of a qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Otherwise, we could copy the qubit by making a machine that prepares a qubit in the superposition $\alpha|0\rangle + \beta|1\rangle$.

While this has some nice features - for example, an inbuilt copy protection mechanism - it also means that qubits are very precious. When trying to send a qubit for example, we cannot simply try again when we failed such as with classical bits. If you could not hear me in the videos clearly, you could rewind, turn up the volume and try again. If I were talking qubits to you, there would be no way to do that!

0.7 Bloch sphere

For single qubits, there is a very convenient visual representation in terms of the so-called Bloch sphere. It should be noted that such a nice representation only exists for single qubits. To make this work, express the qubit as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{119}$$

where γ, θ and ϕ are real numbers. The global phase $e^{i\gamma}$ is neglected, since it has no observable effects on the probability of measurement outcomes. To see this, consider the states

$$|\psi_1\rangle = e^{i\gamma_1}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{120}$$
$$|\psi_2\rangle = e^{i\gamma_2}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{121}$$

for some real numbers γ_1, γ_2. Note that $|\psi_1\rangle = e^{i(\gamma_1-\gamma_2)}|\psi_2\rangle$. We thus have that for any measurement with respect to a basis $\{|b\rangle\}_b$, the probability of obtaining any outcome b is equal for both states, since

$$|\langle\psi_1|b\rangle|^2 = \langle b|\psi_1\rangle\langle\psi_1|b\rangle = e^{i(\gamma_1-\gamma_2)}e^{-i(\gamma_1-\gamma_2)}\langle b|\psi_2\rangle\langle\psi_2|b\rangle = |\langle\psi_2|b\rangle|^2. \tag{122}$$

Also, note that this parametrization preserves the normalization condition since $|\alpha|^2 + |\beta|^2 = \cos^2(\theta/2) + \sin^2(\theta/2) = 1$. In terms of the numbers (θ, ϕ) we can thus think of the qubit as a point on a 3 dimensional sphere as in Figure 2. It should be emphasized that this sphere does not follow the same coordinates as we have used for the vectors $|v\rangle \in \mathbb{C}^2$, but rather we need to translate to this new coordinate system.

Definition 0.7.1 The parametrization (θ, ϕ) of

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \tag{123}$$

is called the *Bloch sphere representation* (Figure 2) and a qubit can be described by a *Bloch vector* $\vec{r} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.

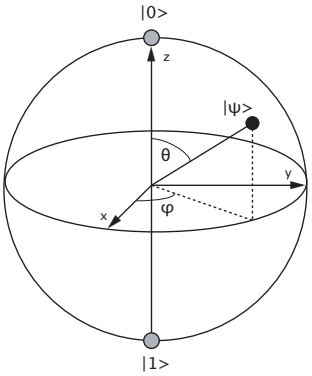

Figure 2: Bloch Sphere

Consider a qubit in the representation of Eq. (119) where $\gamma = \phi = 0$. Then the Bloch sphere representation of such a qubit lies on the xz-plane. The usefulness of this representation becomes immediately apparent when we consider the effects of the Hadamard transform on a qubit. Note that $(|0\rangle + |1\rangle)/\sqrt{2}$ can be found in Figure 2 at the intersection of the positive x-axis and the sphere. It is then easy to see that we can describe the effect of H on $(|0\rangle + |1\rangle)/\sqrt{2}$ as a rotation around the y-axis towards $|1\rangle$, followed by a reflection in the xy-plane. In fact, the Bloch sphere representation allows one to view all single qubit operations as rotations on this sphere. While we will make little use of this in this class, it is interesting to see how single qubit unitaries U can be expressed as rotations on the Bloch sphere. A rotation matrix $R_s(\theta)$ is a unitary operation that rotates a qubit Bloch vector around the axes $s \in \{x, y, z\}$ by an angle θ. Such matrices have the following form:

$$R_x(\theta) = e^{-i\theta X/2},\ R_y(\theta) = e^{-i\theta Y/2} \text{ and } R_z(\theta) = e^{-i\theta Z/2}, \tag{124}$$

where X, Y, Z are the Pauli matrices. Especially important for this text will be the rotation around the z axis. We can express it in more detail as

$$R_z(\theta) = e^{-i\theta Z/2} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = e^{-i\theta/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Any arbitrary single qubit operation U can be expressed in terms of these rotations as

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta)$$

for some real numbers α, β, γ and δ.

Lastly, it is worth noting that such a clean and simple representation only holds for the case of single qubits: for higher dimensional systems, it is not possible to represent a qudit in terms of a d-dimensional sphere!

Important identities for calculations

Given two vectors $|v_1\rangle = \begin{pmatrix} a_1 & \cdots & a_d \end{pmatrix}^T$ and $|v_2\rangle = \begin{pmatrix} b_1 & \cdots & b_d \end{pmatrix}^T$,

1. **(Inner product)** $\langle v_1|v_2\rangle := \langle v_1|\,|v_2\rangle = \sum_{i=1}^{d} a_i^* b_i$.
2. **(Tensor Product)**

$$|v_1\rangle \otimes |v_2\rangle := \begin{pmatrix} a_1b_1 & a_1b_2 & \cdots & a_1b_d & a_2b_1 & \cdots & a_2b_d & \cdots & a_db_d \end{pmatrix}^T.$$

Commonly used orthonormal bases for qubits

Standard basis for 1 qubit: $\mathscr{S} = \{|0\rangle, |1\rangle\}$ where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
Standard basis for n qubits: $\mathscr{S}_n = \{|x\rangle\}_{x\in\{0,1\}^n}$ where for any string $x = x_1x_2\cdots x_n$, $|x\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$.
Hadamard basis for 1 qubit: $\mathscr{H} = \{|+\rangle, |-\rangle\}$ where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Since these are orthonormal bases, the following holds:

$$\langle 0|1\rangle = \langle 1|0\rangle = 0, \qquad \langle 0|0\rangle = \langle 1|1\rangle = 1, \tag{125}$$
$$\langle +|-\rangle = \langle -|+\rangle = 0, \qquad \langle +|+\rangle = \langle -|-\rangle = 1, \tag{126}$$
$$\langle x|x'\rangle = \delta_{xx'}, \text{ where } x, x' \in \{0,1\}^n \text{ and } \delta_{xx'} \text{ is the Kronecker-delta function.} \tag{127}$$

Common representations of a qubit

Standard representation: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$.
Bloch sphere representation: $|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right)$, where $\gamma, \theta, \phi \in \mathbb{R}$.

Properties of the tensor product

For any $|v_1\rangle, |v_2\rangle$ and $|v_3\rangle$,

1. Distributive: $|v_1\rangle \otimes (|v_2\rangle + |v_3\rangle) = |v_1\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |v_3\rangle$
   Also, $|v_1\rangle \otimes (|v_2\rangle + |v_3\rangle) = |v_1\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |v_3\rangle$.
2. Associative: $|v_1\rangle \otimes (|v_2\rangle \otimes |v_3\rangle) = (|v_1\rangle \otimes |v_2\rangle) \otimes |v_3\rangle$.

Similarly, these relations hold for any $\langle v_1|, \langle v_2|$ and $\langle v_3|$.

Probability of measurement outcomes

Consider measuring a quantum state $|\Psi\rangle$ in an orthonormal basis $\mathscr{B} = \{|b_i\rangle\}_{i=1}^d$. The probability of measuring a particular outcome "b_i" is $p_i = |\langle\Psi|b_i\rangle|^2$. After the measurement, if a certain outcome "b_i" is observed, then the state $|\Psi\rangle$ has collapsed to $|b_i\rangle$.

Pauli matrices

The Pauli matrices are 2×2 matrices,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = iXZ, \tag{128}$$

and the following relations hold:

$$X|0\rangle = |1\rangle, \; X|1\rangle = |0\rangle \qquad X|+\rangle = |+\rangle, \; X|-\rangle = -|-\rangle \tag{129}$$
$$Z|0\rangle = |0\rangle, \; Z|1\rangle = -|1\rangle \qquad Z|+\rangle = |-\rangle, \; Z|-\rangle = |+\rangle \tag{130}$$
$$Y|0\rangle = i|1\rangle, \; Y|1\rangle = -i|0\rangle \qquad Y|+\rangle = -i|-\rangle, \; Y|-\rangle = i|+\rangle \tag{131}$$

Bibliography

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000 (cited on page 2).

[2] B. Schumacher and M. Westmoreland. *Quantum Processes Systems, and Information*. Cambridge University Press, 2010 (cited on page 2).