Contents

Chapter 0

Background material

In this introductory chapter we give a gentle introduction to quantum information. We will introduce all that you need to know to work with quantum bits — qubits — and measurements at a mathematical level. To learn more about how qubits can be realized physically, or simply want more background than we provide here, we recommend [**nielsen&chuang:qc**] and [**schumacher:book**]. We assume that you are familiar with basic notions in linear algebra such as finite-dimensional vector spaces, vectors and matrices.

0.1 Mathematical notation

Let us start by recalling common notation that we will use throughout. Let $\mathbb{C}$ be the field of complex numbers, and $i = \sqrt{-1} \in \mathbb{C}$. For a complex number $c = a + ib \in \mathbb{C}$ with $a, b \in \mathbb{R}$ we write $c^* = a - ib$ for its *complex conjugate*. Complex numbers are equipped with an *absolute value* (sometimes also called *modulus*), defined as follows.

Definition 0.1.1 (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 *of z is given by*

$$|z| := \sqrt{z^* z} = \sqrt{x^2 + y^2}. \tag{1}$$

For example, for $z = 1 + i2$ its absolute value is given by $|z| = \sqrt{1^2 + 2^2} = \sqrt{5}$.

A vector space V over $\mathbb{C}$ is a set of vectors $v \in V$ with complex coefficients, such that V contains 0 and is stable under vector addition and multiplication by scalars (in this case, complex numbers). In quantum information vectors are written in a special way known as the “bra-ket” notation. While it may look a little cumbersome at first, 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 $V = \mathbb{C}^2$. For example,

$$|v\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} . \tag{2}$$

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

$$\langle v| := ((|v\rangle)^*)^T = \begin{pmatrix} 1^* \\ 0^* \end{pmatrix}^T = (1\ 0) . \tag{3}$$

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

Definition 0.1.2 (bra-ket notation)**.** *A* ket*, denoted $|\cdot\rangle$, represents a d-dimensional column vector in the complex vector space $\mathbb{C}^d$. (The dimension d is usually left implicit in the notation.) A* bra*, denoted $\langle\cdot|$, is a d-dimensional row vector equal to the complex conjugate of the corresponding ket, namely*

$$\langle\cdot| = (|\cdot\rangle^*)^T, \tag{4}$$

where * denotes the entry-wise conjugate, and T denotes the transpose. We also use the "dagger" notation for the conjugate-transpose: for any vector $|u\rangle \in \mathbb{C}^d$,

$$|u\rangle^\dagger \ = \ (|u\rangle^*)^T \ .$$

This notation extends to matrices: $A^\dagger = (A^*)^T$.

We will frequently need to compute the inner product of two vectors in the "bra-ket" notation. The 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 $| \langle v_1|v_2\rangle |^2$ has a physical significance. As an example, let us consider the inner product of the vector $|v\rangle$ given in (2) and

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

We have

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

Exercise 0.1.1. *Show that for any two vectors $|v_1\rangle$ and $|v_2\rangle$,*

$$| \langle v_1|v_2\rangle |^2 = \langle v_1|v_2\rangle \langle v_2|v_1\rangle\ \ .$$

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

It is convenient to have a measure of "length" of a vector. For this we use the Euclidean norm.

Definition 0.1.4 (Norm of a ket vector)**.** *Consider a ket vector*

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

The length*, or* norm*, 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 that $|v\rangle$ 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 norm 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 assume that your are familiar with the notion of an orthonormal basis from linear algebra. We often write such a basis as $\{|b\rangle\}_b$, which is shorthand for $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$ where d is the dimension of the vector space in which the kets live. The condition of being orthonormal can be expressed succinctly as $\langle b|b'\rangle = \delta_{bb'}$ for all $b, b' \in \{0, \dots, d-1\}$.[1]

0.2 What are qubits?

We are all familiar with the notion of a "bit" in classical computing: a bit is a value $b \in \{0, 1\}$, that has some physical representation (e.g. current/no current) that we don't generally care about and represents some information that is stored and manipulated by an algorithmic procedure. 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', we can first associate a 2-dimensional vector to each of them, as

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

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.

A quantum bit is a more general object than a bit: instead of the only two options being $|0\rangle$ and $|1\rangle$, a quantum bit is defined by any normalized linear combination of them, i.e. any vector of the form $\alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. We often say that the quantum bit is in a "superposition" of $|0\rangle$ and $|1\rangle$, with "amplitudes" α and β. Examples of qubits are

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) , \quad \text{and} \quad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) . \tag{12}$$

Since "quantum bit" is somewhat long, researchers simply use the term "qubit" to refer to a quantum bit. Thus a qubit is a normalized vector $|v\rangle \in \mathbb{C}^2$, and the vector space $\mathbb{C}^2$ is also known as the *state space* of the qubit.

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

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

Whenever the condition on α and β is satisfied we say that $|\psi\rangle$ is normalized*. The complex numbers α and β are called* amplitudes *of $|\psi\rangle$.*

[1] Here δ_{ab} is the *Kronecker symbol*, defined as $\delta_{ab} = 0$ if $a \neq b$ and $\delta_{ab} = 1$ for $a = b$.

You probably noticed the use of the word “pure” in the definition. This is because there is a more general notion of qubit, called a “mixed” state, that we introduce later in this chapter.

Throughout the book we mostly focus on encoding information in qubits. In general, quantum information can also be encoded in higher dimensional systems. Indeed one can similarly define a qu*d*it as follows.

Definition 0.2.2 (Qudit)**.** *A pure state of a* qudit *can be represented as a d-dimensional ket vector $|\psi\rangle \in \mathbb{C}^d$,*

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

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

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 $\mathbb{C}^2$, so 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)**.** *The* standard basis*, also known as the* computational basis*, of $\mathbb{C}^2$ is the orthonormal basis $\mathcal{S} = \{|0\rangle, |1\rangle\}$ where*

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \textit{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} . \tag{15}$$

There are many other bases for $\mathbb{C}^2$. Another favorite basis which we will use frequently is the Hadamard basis.

Definition 0.2.4 (Hadamard basis)**.** *The* Hadamard basis *of $\mathbb{C}^2$ is the orthonormal basis $\mathcal{H} = \{|+\rangle, |-\rangle\}$ where*

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} . \tag{16}$$

Let us verify that this is indeed an orthonormal basis using the “bra-ket” notation:

$$\langle +|+\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \cdot 2 = 1, \qquad \Longrightarrow \qquad \sqrt{\langle +|+\rangle} = 1 \ , \tag{17}$$

so $|+\rangle$ is also normalized. A similar calculation gives that $|-\rangle$ is normalized as well. In fact, you can verify that normalization follows from the more general Exercise 0.2.1, by observing that $|+\rangle = |\psi_{\pi/4}\rangle$ and $|-\rangle = |\psi_{3\pi/4}\rangle$. Furthermore, the inner product

$$\langle +|-\rangle = \frac{1}{2}\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}1\\-1\end{pmatrix} = 0, \tag{18}$$

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

Exercise 0.2.2. *Decompose the state $|1\rangle$ in the Hadamard basis. In other words, find coefficients α and β such that $|1\rangle = \alpha\,|+\rangle + \beta\,|-\rangle$.* ■

0.3 Multiple qubits

Classically we can write the state of two bits as '00', '01', and so forth. How do we write the state of two qubits? Proceeding as we did earlier, we can associate a vector to each of the four possible configurations of the two classical bits $x_1, x_2 \in \{0,1\}^2$. This gives us a mapping from 2-bit strings to 4-dimensional vectors as

$$00 \to |00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad 01 \to |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$10 \to |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \qquad 11 \to |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

More generally, a pure state of two qubits can always be expressed as a normalized vector $|\psi\rangle \in \mathbb{C}^4$. Since the four vectors above form an orthonormal basis of $\mathbb{C}^4$, any such $|\psi\rangle$ has a decomposition as a linear combination of the four basis vectors:

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

In quantum-speak we say that $|\psi\rangle$ is a "superposition" of the four basis vectors, with "amplitudes" α_{00}, α_{01}, α_{10} and α_{11}.

As a concrete example, let us consider a state $|\psi\rangle$ that is an equal superposition of all four standard basis vectors for the space of 2 qubits:

$$|\psi\rangle_{AB} = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \tag{19}$$

$$= \frac{1}{2}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \tag{20}$$

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

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.

We can proceed analogously to define a pure state of n qubits, for $n = 1, 2, 3, \ldots$. To see how such a state can be represented we first look at the vector representation for multiple classical bits. There are a total of $d = 2^n$ strings of n bits. Each such string x can be associated to a basis vector $|x\rangle \in \mathbb{C}^d$, where x is 0 everywhere, except at the coordinate indexed by the integer $i \in \{0, \ldots, d-1\}$ of which x is the binary representation (specifically, $i = x_1 + 2x_2 + \cdots + 2^{n-1}x_n$). A general pure state of n qubits can then be expressed as

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \ , \tag{22}$$

with $\alpha_x \in \mathbb{C}$ and $\sum_x |\alpha_x|^2 = 1$. The numbers α_x are again called *amplitudes*. It is worth noticing 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 called the *state space* of n qubits. Analogously 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* (or *computational*) basis.

Definition 0.3.1 (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 with x the integer $i \in \{0, 1, 2, \ldots d\}$ of which it is the binary representation. The standard basis for $\mathbb{C}^d$ is the orthonormal basis $\{|x\rangle\}_{x\in\{0,1\}^n}$, where for $x \in \{0,1\}^n$, $|x\rangle$ is the d-dimensional vector*

$$|x\rangle = \begin{pmatrix}0\\ \vdots \\ 1 \\ \vdots \\ 0\end{pmatrix} \longrightarrow i\text{-th position.} \tag{23}$$

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

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\,, \qquad \text{where } \forall x, \alpha_x \in \mathbb{C} \text{ and } \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1. \tag{24}$$

We look at two examples of two qubit states. The first is so famous it carries a special name, and we will see it very frequently throughout the book.

Example 0.3.1. *The* 2*-qubit state known as the* EPR pair *is defined as:*[2]

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}\,, \tag{25}$$

which is an equal superposition between the vectors $|00\rangle_{AB}$ *and* $|11\rangle$. ■

It is a useful exercise to verify that the state $|\mathrm{EPR}\rangle$ is normalized. For this we compute the inner product

$$\langle \mathrm{EPR}|\mathrm{EPR}\rangle_{AB} = \frac{1}{\sqrt{2}}(\langle 00|_{AB} + \langle 11|_{AB}) \cdot \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{26}$$

$$= \frac{1}{2}(\underbrace{\langle 00|00\rangle_{AB}}_{1} + \underbrace{\langle 00|11\rangle_{AB}}_{0} + \underbrace{\langle 11|00\rangle_{AB}}_{0} + \underbrace{\langle 11|11\rangle_{AB}}_{1}) \tag{27}$$

$$= \frac{1}{2} \cdot 2 = 1, \qquad \Longrightarrow \qquad \sqrt{\langle EPR|EPR\rangle} = 1. \tag{28}$$

Example 0.3.2. *Consider the two qubit state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}\,. \tag{29}$$

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

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

0.4 Combining qubits using the tensor product

So far we have learned how to represent the state of 1 qubit, of 2 qubits, and more generally of any number n of qubits. In each case the quantum state is a normalized vector that can be expressed as a linear combination of basis vectors associated with the n-bit strings.

Now imagine given two qubits, A and B, each of which is represented by a vector, $|\psi\rangle_A \in \mathbb{C}^2$ and $|\phi\rangle_B \in \mathbb{C}^2$ respectively. We will often refer to A and B as "systems", or "registers"; these words are used interchangeably to specify an abstract quantum system that can be of one or more qubits. AB itself is a system, that consists of two subsystems, A and B. The state of system A is $|\psi\rangle_A$, and the state of system B is $|\psi\rangle_B$. How do we represent the state of system AB?

The rule that allows us to move from the individual representation of two quantum states to a single joint representation for both of them is called the *tensor product* (sometimes also called the Kronecker product). For the example of two single-qubit states we know that it is always possible to express

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}, \tag{30}$$

$$|\phi\rangle_B = \alpha_B |0\rangle_B + \beta_B |1\rangle_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix} \quad . \tag{31}$$

Note how we indexed the state of each qubit using the letter A or B respectively. You will soon see that this is a convenient way of keeping track of what part of a given quantum state is associated with different qubits that constitute it. The joint state $|\psi\rangle_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ of both qubits is then obtained as the tensor product of the individual vectors $|\psi\rangle_A$ and $|\phi\rangle_B$, which by definition evaluates to

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi\rangle_B = \begin{pmatrix} \alpha_A |\psi\rangle_B \\ \beta_A |\psi\rangle_B \end{pmatrix} = \begin{pmatrix} \alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B \end{pmatrix}. \tag{32}$$

More generally, for quantum systems A and B that are larger than just one qubit, the definition of the tensor product is as follows.

Definition 0.4.1. *For arbitrary integer $d_1, d_2 \geq 1$ and vectors $|\psi_1\rangle \in \mathbb{C}^{d_1}$ and $|\psi_2\rangle \in \mathbb{C}^{d_2}$, their tensor product is the vector $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ given by*

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 |\psi_2\rangle \\ \vdots \\ \alpha_d |\psi_2\rangle \end{pmatrix} . \tag{33}$$

The following simplified (also known as “lazy”) notations are commonly used:

$$\text{Omitting the tensor product symbol:} \quad |\psi\rangle_A \otimes |\psi\rangle_B = |\psi\rangle_A |\psi\rangle_B \,. \tag{34}$$

$$\text{Writing classical bits as a string:} \quad |0\rangle_A \otimes |0\rangle_B = |0\rangle_A |0\rangle_B = |00\rangle_{AB} \,. \tag{35}$$

$$\text{Combining several identical states:} \quad |\psi\rangle_1 \otimes |\psi\rangle_2 \cdots \otimes |\psi\rangle_n = |\psi\rangle^{\otimes n} \,. \tag{36}$$

Proposition 0.4.1. *The tensor product satisfies the following properties.*

1. *Distributivity:* $|\psi_1\rangle \otimes (|\psi_2\rangle + |\psi_3\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle + |\psi_1\rangle \otimes |\psi_3\rangle$.
   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. *Associativity:* $|\psi_1\rangle \otimes (|\psi_2\rangle \otimes |\psi_3\rangle) = (|\psi_1\rangle \otimes |\psi_2\rangle) \otimes |\psi_3\rangle$.

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

Be careful that the tensor product is NOT commutative: in general, $|\psi_1\rangle \otimes |\psi_2\rangle \neq |\psi_2\rangle \otimes |\psi_1\rangle$, unless of course $|\psi_1\rangle = |\psi_2\rangle$. Convince yourself of this fact by computing the representation as 4-dimensional vectors, using the rule (32), of $|0\rangle \otimes |1\rangle$ and $|1\rangle \otimes |0\rangle$.

To understand the definition of the tensor product, let us have a look at a few examples. The first shows how the tensor product can be applied to construct a basis for the space of n qubits from a basis for the space of a single qubit.

Example 0.4.1. *Recall that the standard basis for two qubits A and B is given by*

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

This basis can be obtained by taking the tensor product of standard basis elements for the 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*

$$|1\rangle_A \otimes |0\rangle_B = \begin{pmatrix}0\\1\end{pmatrix} \otimes |0\rangle_B = \begin{pmatrix}0\,|0\rangle_B\\1\,|0\rangle_B\end{pmatrix} = \begin{pmatrix}0\cdot 1\\0\cdot 0\\1\cdot 1\\1\cdot 0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} = |10\rangle_{AB} \,. \tag{37}$$

■

We have seen a few examples of two qubit states. Let’s see whether we can recover them from individual qubit states by taking the tensor product.

Example 0.4.2. *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*

$$|\psi\rangle_{AB} = |+\rangle_A \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}_A \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot|1\rangle_B\\1\cdot|1\rangle_B\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}. \tag{38}$$

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

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes |1\rangle_B \tag{39}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |1\rangle_B) \tag{40}$$

$$= \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |11\rangle_{AB}). \tag{41}$$

This is the state from Example 0.3.2. ∎

Example 0.4.3. *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*

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A) \otimes \frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) \tag{42}$$

$$= \frac{1}{2}(|00\rangle_{AB} + |01\rangle_{AB} + |10\rangle_{AB} + |11\rangle_{AB}) \tag{43}$$

$$= \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}. \tag{44}$$

This is the state we have seen in (19)*, which is an equal superposition of all standard basis states for the two qubits.* ∎

The following is an example of a state that can *not* be expressed directly as the tensor product of two single-qubit states. Such states have special properties, and they play an important role throughout the book. Nevertheless, let's take a close look and see how any two-qubit state can be expressed from the state of individual qubits using not only the tensor product operation, but also linear combinations.

Example 0.4.4. *Consider the state of two qubits*

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B). \tag{45}$$

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

$$|+\rangle_A |+\rangle_B = \frac{1}{2}(|0\rangle_A + |1\rangle_A)(|0\rangle_B + |1\rangle_B) = \frac{1}{2}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB}) \tag{46}$$

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

Substituting this into Eq. (45) *gives*

$$\begin{aligned} |\Psi\rangle_{AB} &= \frac{1}{\sqrt{2}}(|+\rangle_A |+\rangle_B + |-\rangle_A |-\rangle_B) & (48) \\ &= \frac{1}{2\sqrt{2}}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB} + |00\rangle_{AB} - |10\rangle_{AB} - |01\rangle_{AB} + |11\rangle_{AB}) & (49) \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = |\mathrm{EPR}\rangle_{AB} & (50) \end{aligned}$$

where $|\mathrm{EPR}\rangle_{AB}$ *is the state we have seen previously in Example 0.3.1. We see that the coefficients of* $|\mathrm{EPR}\rangle_{AB}$ *are the same whether we write it in the Hadamard basis or the standard basis. As we will see later , this state* cannot *be written as* $|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$, *for any choice of single-qubit states* $|\psi\rangle_A$ *and* $|\phi\rangle_B$. *Nevertheless, it can still decomposed as a linear combination of multiple such states, in more than one way, such as* (45) *and* (50). ■

0.5 Simple measurements

As you may have observed, the quantum state as we have defined it so far is a very abstract object: a normalized vector in a complex vector space. In real life, objects don't look like vectors. Instead, they tend to have physical properties, such as location, momentum, color, etc. Given a quantum state represented as a vector, what kind of physical properties can be associated to it, and what is the rule for deriving the value of each property from the quantum state?

In quantum mechanics this is a difficult question, but we will give you simple rules that can be used to answer it. First consider the case of a classical bit: as described, this is simply a value that is either '0' or '1'. Given the state of a bit, we can "read" it, and this will result in the "outcome" 0 or 1, directly reflecting the state of the bit. For qubits, the situtation is more complicated (which is what makes them interesting!), as the quantum state can be "read" in multiple different ways.

0.5.1 Measurement in the standard basis

Let's first consider measurements on a single qubit. Remember that a state of a qubit is represented by a normalized vector $|\psi\rangle \in \mathbb{C}^2$, that can always be expressed as a superposition of the basis vectors $|0\rangle$ and $|1\rangle$, with amplitudes $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$.

A good way to think about a quantum measurement is as a question that can be asked about such a state. The measurement rule then provides a way to answer the question. For example, by analogy with the classical setting we could ask the question: "Is $|\psi\rangle$ in state $|0\rangle$ or in state $|1\rangle$?". Given that "obviously", $|\psi\rangle$ is neither of these: it is a *superposition* of the two basis states, how do we answer such a question?

Yet the measurement rule gives a way to answer the question. Quantum measurements are special in two significant ways: first, in general they result in probabilistic outcomes; second, they perturb the quantum state on which they are performed.

In the case of our example, the probability of each possible outcome, for example the outcome '0', can be computed by, roughly speaking, "looking at how much '$|0\rangle$' is present in the state of the qubit". The way this is quantified is by taking the squared inner product between $|\psi\rangle$ and $|0\rangle$. Concretely, if $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, then the measurement associated with the question "Is $|\psi\rangle$ in state $|0\rangle$ or in state $|1\rangle$?" returns the outcome "$|0\rangle$" with probability p_0, and "$|1\rangle$" with probability p_1, where

$$\begin{aligned} p_0 &= |\,\langle\psi|0\rangle\,|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right|^2 = |\alpha|^2, \\ p_1 &= |\,\langle\psi|1\rangle\,|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right|^2 = |\beta|^2. \end{aligned} \tag{51}$$

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 '$|0\rangle$' and '$|1\rangle$' add up to one. In quantum computing 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 '$|1\rangle$'. In the book we will mostly use the first convention, though we may sometimes use the second; which will always be clear in context.

As the title of the section hints, it is possible to make other kinds of measurements on a qubit, corresponding to other questions that can be asked about it. Before we discuss what kind of questions can be asked, and how to determine

[3] And more generally, x for outcome '$|x\rangle$', for a bit string x.

their answer from the state of the qubit, we give a first cryptographic application of quantum information: the generation of genuine randomness.

Application: randomness from a deterministic process. Can we do anything interesting with what we have learned so far? It turns out that the answer is yes: by preparing just single qubits and measuring them in the standard basis we can achieve a task that 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 be calculated by evaluating the inner products, using the recipe given in (51):

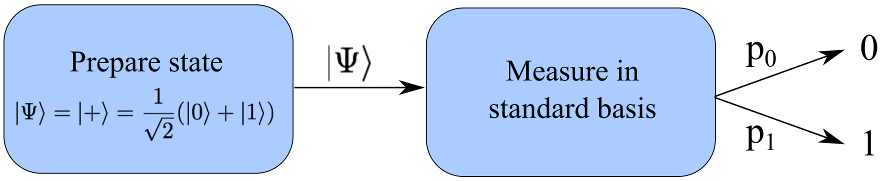
Prepare state
$|\Psi\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
$|\Psi\rangle$
Measure in standard basis
p_0
0
p_1
1

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

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

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

This simple example tells us something about the power of quantum information: it is in principle possible to build a machine that deterministically prepares the qubit $|+\rangle$ and subsequently measures it in the standard basis. Since $p_0 = p_1 = 1/2$, this machine obtains an outcome that is perfectly uniformly distributed between '0' and '1'.[4] Even though the machine is perfectly deterministic (it always does exactly the same thing), each time the process is executed the outcome is unpredictable. This intrinsic randomness is a consequence of the rules of quantum mechanics as we have presented them, and is an integral part of the power of quantum information

[4] This is possible not only in principle, but also in practice, and machines based precisely on this description are manufactured, sold and used on a daily basis by anyone from banks (for cryptography) to casinos (you can guess what for).

for cryptography: as we will see throughout the book, uncertainty, or ignorance, is the key to security.

We have described the measurement rule for the case of a single qubit, measured in the standard basis. The rule generalizes directly to a measurement of an n-qubit state in the standard basis. Indeed, consider an arbitrary n-qubit quantum state expressed as a superposition in the standard basis

$$|\Psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \ . \tag{52}$$

When $|\Psi\rangle$ is measured in the standard basis $\{|x\rangle\}_x$, the probability of obtaining the outcome x is naturally given by $p_x = |\langle x|\,\Psi\rangle|^2 = |\alpha_x|^2$. Once again, the normalization condition on the vector $|\Psi\rangle$ shows that these probabilities sum to 1, as expected.

0.5.2 Measuring a qubit in an arbitrary basis

What other kinds of observations, or measurements, are allowed in quantum mechanics? As it turns out, any orthonormal basis for the state space of one (or multiple) qubits leads to a valid measurement. Indeed, abstractly speaking there is nothing special about the standard basis: it is “a” basis of the state space $\mathbb{C}^d$, but many other bases exist.

To find out how to analyze this more general setting, let us first take a step back and consider how we found the probabilities in the case of measurements in the standard basis. To obtain them, we first expressed an arbitrary quantum state as a superposition over elements of the standard basis, and then took the square of the amplitudes to obtain the outcome probabilities.

When measuring a qubit in a different orthonormal basis, given by vectors $\{|v_0\rangle, |v_1\rangle\}$, we proceed in a similar way: first, expand the quatnum state as a superposition over vectors from the new basis, i.e. find amplitudes $\hat{\alpha}$ and $\hat{\beta}$ such that

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \hat{\alpha}\,|v_0\rangle + \hat{\beta}\,|v_1\rangle \ . \tag{53}$$

Due to the assumption that $\{|v_0\rangle, |v_1\rangle\}$ is a basis, the complex numbers $\hat{\alpha}$ and $\hat{\beta}$ are uniquely defined. In fact, since the basis is orthonormal you can verify that

$$\hat{\alpha} = \langle v_0|\,\psi\rangle \quad \text{and} \quad \hat{\beta} = \langle v_1|\,\psi\rangle \ .$$

Second, take the modulus squared of the associated amplitudes to obtain the probability of each outcome: here, the outcome is ‘$|v_0\rangle$’ with probability $|\hat{\alpha}|^2$ and ‘$|v_1\rangle$’ with probability $|\hat{\beta}|^2$.

Example 0.5.1. *As an example, 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 $\{|+\rangle, |-\rangle\}$ 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 in this case the probability of obtaining measurement outcome '$|+\rangle$' is 1, and the probability of outcome '$|-\rangle$' is 0. The probabilities of measurement outcomes depend dramatically on the basis in which we measure: for this measurement, there is no randomness in the outcomes!* ■

Example 0.5.2. *Consider measuring an arbitrary qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ 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 that basis. We find that*

$$|0\rangle = \frac{1}{2}\left[(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)\right] = \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right) , \tag{54}$$

$$|1\rangle = \frac{1}{2}\left[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)\right] = \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right) . \tag{55}$$

Replacing in the definition of $|\psi\rangle$, we get

$$\alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}\left[\alpha(|+\rangle + |-\rangle) + \beta(|+\rangle - |-\rangle)\right] = \tag{56}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle . \tag{57}$$

This means that upon measuring the qubit $|\psi\rangle$ in the basis $\{|+\rangle, |-\rangle\}$ the outcome '$|+\rangle$' is obtained with probability $|\alpha+\beta|^2/2$ and the outcome "$|-\rangle$" is obtained with probability $|\alpha-\beta|^2/2$. In particular, you can check that this calculation recovers the one performed in the previous example as a special case. ■

Exercise 0.5.1. *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

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle . \tag{58}$$

Remember that the elements of the standard basis are orthonormal. As a result, we could have found the desired probabilities by simply computing the inner product between two vectors, as described above. Specifically, when given the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we obtain outcomes '$|0\rangle$' and '$|1\rangle$' with probabilities

$$p_0 = |\langle 0|\psi\rangle|^2 = \left|(1\ 0)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\alpha|^2 \tag{59}$$

$$p_1 = |\langle 1|\psi\rangle|^2 = \left|(0\ 1)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\beta|^2 \tag{60}$$

Example 0.5.3. *Suppose we measure $|0\rangle$ in the Hadamard basis. The probabilities of observing outcomes "$|+\rangle$" and "$|-\rangle$" are given by*

$$p_+ = |\langle +|0\rangle|^2 = \left|(1/\sqrt{2}\ 1/\sqrt{2})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,, \tag{61}$$

$$p_- = |\langle -|0\rangle|^2 = \left|(1/\sqrt{2}\ -1/\sqrt{2})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,. \tag{62}$$

■

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

Definition 0.5.1. *Suppose that $|\psi\rangle \in \mathbb{C}^d$ is a pure quantum state in dimension d. Suppose that $|\psi\rangle$ is measured in the orthonormal basis $\{|b_j\rangle\}_{j=1}^d$ of $\mathbb{C}^d$. Then the probability of obtaining the outcome "$|b_j\rangle$" is*

$$p_j = |\langle b_j|\psi\rangle|^2\,. \tag{63}$$

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

Example 0.5.4. *Consider the single-qubit state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$. Measure the qubit in the basis $\{|+\rangle, |-\rangle\}$. The probabilities of obtaining outcomes '$+$' and*

'$-$' can be evaluated as follows:

$$\begin{aligned}
p_+ = |\langle\Psi|+\rangle|^2 &= \left|\frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle + |1\rangle)\right|^2 && (64)\\
&= \frac{1}{4}\Big|\langle 0|0\rangle + \langle 0|1\rangle - i\langle 1|0\rangle - i\langle 1|1\rangle\Big|^2 && (65)\\
&= \frac{1}{4}|1-i|^2 && (66)\\
&= \frac{1}{4}(1-i)(1+i) = \frac{1}{2}, && (67)\\
p_- = |\langle\Psi|-\rangle|^2 &= \left|\frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle - |1\rangle)\right|^2 && (68)\\
&= \frac{1}{4}\Big|\langle 0|0\rangle - \langle 0|1\rangle - i\langle 1|0\rangle + i\langle 1|1\rangle\Big|^2 && (69)\\
&= \frac{1}{4}|1+i|^2 && (70)\\
&= \frac{1}{4}(1+i)(1-i) = \frac{1}{2}. && (71)
\end{aligned}$$

This example shows that when the states involved have complex-valued amplitudes, one has to take additional care when evaluating the inner product: namely when taking the bra $\langle\Psi|$, one should remember that the bra $\langle\Psi|$ is the conjugate transpose of the ket $|\Psi\rangle$, and thus one has to alter the ± sign whenever a complex number is involved. ■

While we will generally talk about n-qubit states, it is also legitimate to consider quantum states in d dimensions, where d is not necessarily a power of 2.

Example 0.5.5. *Consider a* qutrit $|\psi\rangle \in \mathbb{C}^3$*, which is a* 3*-dimensional quantum system, represented by the vector*

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\end{pmatrix}. \qquad (72)$$

Suppose that $|\psi\rangle$ is measured in the basis $\{|b_1\rangle, |b_2\rangle, |b_3\rangle\}$, where

$$|b_1\rangle = \begin{pmatrix}1\\0\\0\end{pmatrix}, \qquad |b_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\end{pmatrix}, \qquad |b_3\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\end{pmatrix}. \qquad (73)$$

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

$$p_{b_1} = |\langle b_1|\psi\rangle|^2 = \frac{1}{2}, \tag{74}$$

$$p_{b_2} = |\langle b_2|\psi\rangle|^2 = \langle b_2|v\rangle \langle v|b_2\rangle = \frac{1}{2\sqrt{2}}(1+1)\cdot\frac{1}{2\sqrt{2}}(1+1) = \frac{1}{2}, \tag{75}$$

$$p_{b_3} = |\langle b_3|\psi\rangle|^2 = \langle b_3|v\rangle \langle v|b_3\rangle = \frac{1}{2\sqrt{2}}(1-1)\cdot\frac{1}{2\sqrt{2}}(1-1) = 0. \tag{76}$$

■

Expectation values. Physicists (but also computer scientists!) like to compute *expectation values* of measurement outcomes, as they provide an indication of average behavior, if one was to perform a measurement many times. To see what this means, suppose that we measure a qubit $|\psi\rangle$ in the standard basis $\{|0\rangle, |1\rangle\}$. For this discussion we adopt the physics convention of labeling the two possible outcomes as $+1$ and -1 respectively: '$+1$' for '$|0\rangle$', and '-1' for $|1\rangle$. Then the expectation value of the outcome obtained when measuring $|\Psi\rangle$ is by definition

$$E = 1\cdot|\langle 0|\psi\rangle|^2 - 1\cdot|\langle 1|\psi\rangle|^2 \,. \tag{77}$$

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

$$E = \langle\psi|\left(|0\rangle\langle 0| - |1\rangle\langle 1|\right)|\psi\rangle = \langle\psi|\, Z\, |\psi\rangle \tag{78}$$

where

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

is a 2×2 matrix. We will encounter Z very frequently in the future; it is called the "Pauli-Z observable".

0.5.3 Measuring multiple qubits

Since we can always consider a state of n qubits as a single quantum state of dimension $d = 2^n$, the rule for describing measurements of arbitrary-dimensional states given in the previous section can be applied to the case of an n-qubit state. Nevertheless, it is often more convenient not to forget the qubit structure of the state. Let us then see explicitly what happens when such a state is measured. Let's do it in general: consider a 2-qudit state in the space $|\psi\rangle_{AB} \in \mathbb{C}^{d_A}_A \otimes \mathbb{C}^{d_B}_B$, for arbitrary dimension $d_A, d_B \geq 1$. First remember how a basis for this space can be obtained from bases for the individual state spaces $\mathbb{C}^{d_A}_A$ and $\mathbb{C}^{d_B}_B$: if $\{|b^A_j\rangle\}_j$ is a basis for $\mathbb{C}^{d_A}_A$ and $\{|b^B_j\rangle\}_j$ is a basis for the state space $\mathbb{C}^{d_B}_B$, then the set of vectors $\{\{|b^A_j\rangle \otimes |b^B_k\rangle\}_{j=1}^{d_A}\}_{k=1}^{d_B}$ gives a basis for $\mathbb{C}^{d_A}_A \otimes \mathbb{C}^{d_B}_B$.

Example 0.5.6. *Consider the basis* $\{|0\rangle_A, |1\rangle_A\}$ *for qudit A, and the basis* $\{|+\rangle_B, |-\rangle_B\}$ *for qudit B. A basis for the joint state AB is then given by* $\{|0\rangle_A |+\rangle_B, |0\rangle_A |-\rangle_B, |1\rangle_A |+\rangle_B, |1\rangle_A |-\rangle_B\}$. ■

Suppose now that we would like to measure qudit A in the basis $\{|b_j^A\rangle\}_j$, and qudit B in the basis $\{|b_k^B\rangle\}_k$. What is the probability that we obtain outcome '$|b_j^A\rangle$ ' for A, and outcome '$|b_k^B\rangle$' for B? To find out, we first write down a basis for the joint state space of qudits A and B: $\{\{|b_j^A\rangle|b_k^B\rangle\}_j\}_k$. We then apply the usual measurement rule to compute the probability

$$p_{jk} = |\langle b_j^A|\langle b_k^B|\,|\psi\rangle_{AB}|^2 \,. \tag{79}$$

Example 0.5.7. *Consider two qubits in an EPR pair*

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \,. \tag{80}$$

Suppose each qubit is measured in the standard basis. Then the probabilities of obtaining outcomes 00*,* 01*,* 10*, and* 11 *are given by*

$$p_{00} = p_{11} = \frac{1}{2} \,, \quad p_{01} = p_{10} = 0 \,. \tag{81}$$

■

0.5.4 Post-measurement states

In general, when a state $|\psi\rangle \in \mathbb{C}^d$ is measured in a basis $\{|b_i\rangle\}$ of $\mathbb{C}^d$, once the measurement outcome "b_i'' is obtained, the state $|\psi\rangle$ automatically "collapses" to the basis state that is consistent with the outcome: it becomes the state $|b_i\rangle$. We will discuss the formalism associated with post-measurement states in more detail in the next chapter, when we consider generalized measurements.

0.6 Transformations on qubits

Just like it is possible to manipulate classical bits, such as by flipping a bit or adding two bits, it is possible to perform operations on qubits. However, the laws of quantum mechanics do not allow every possible operation: some operations are physically impossible. First consider operations that transform the state of a some qubits to a different state of the same qubits. More generally, we are interested in those operations that transform normalized states in $\mathbb{C}^d$ to normalized states in the same space.

A first condition on any such transformation for it to be a valid quantum operations is that it should be *linear*: any quantum map U that performs a transformation

$$U : |\psi_{\text{in}}\rangle \mapsto |\psi_{\text{out}}\rangle = U(|\psi_{\text{in}}\rangle) \tag{82}$$

must satisfy

$$U(\alpha |\psi_1\rangle + \beta |\psi_2\rangle) = \alpha U(|\psi_1\rangle) + \beta U(|\psi_2\rangle) \ .$$

This allows us to immediately claim that any quantum operation that acts on d-dimensional qudits can be represented by some $d \times d$ matrix U with complex coefficients, as indeed every linear map on $\mathbb{C}^d$ has a matrix representation. Linearity is not the only constraint however, there is an additional one. Recall that for any quantum state we have $\langle\psi|\psi\rangle = 1$. As we have seen, this condition is quite important because it tells us that the sum of the probabilities, if we measure the state, should be 1. This means that the operation U should preserve the inner product, [5] i.e. for all possible states $|\psi_{\text{in}}\rangle$,

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}| U^\dagger U |\psi_{\text{in}}\rangle = 1 \ , \tag{83}$$

where recall that the "dagger" notation $U^\dagger$ designates the conjugate-transpose: $U^\dagger = (U^*)^T$. Similarly, the same should be true for the operation $U^\dagger$

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}| UU^\dagger |\psi_{\text{in}}\rangle = 1 \ . \tag{84}$$

We see that in order to preserve probabilities the operation U should preserve the length of any vector. This condition is equivalent to the condition that $U^\dagger U = UU^\dagger = \mathbb{I}$, where $\mathbb{I}$ is the identity matrix.

Definition 0.6.1 (Identity)**.** *The identity matrix is a diagonal, square matrix with all diagonal entries equal to* 1*:*

$$\mathbb{I} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} . \tag{85}$$

For any dimension d, we denote the $d \times d$ identity matrix as $\mathbb{I}_d$. We sometimes leave the dimension implicit and simply write $\mathbb{I}$.

Remark 0.6.1. *The identity matrix leaves all quantum states invariant, i.e. for any quantum state $|\psi\rangle$, $\mathbb{I}|\psi\rangle = |\psi\rangle$.*

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

Definition 0.6.2 (Unitary operation)**.** *An operation U is unitary if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.*

The allowed operations on quantum states are precisely the unitary operations.To gain some intuition on them, let us have a look at some examples.

Example 0.6.1. *Consider the matrix*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{86}$$

You can verify that $H^\dagger = H$ and thus

$$H^\dagger H = HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I} \, . \tag{87}$$

That is, H is unitary. We have that

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \left|+\right\rangle \, . \tag{88}$$

Similarly, you can verify that $H\left|1\right\rangle = \left|-\right\rangle$. We thus see that H transforms the computational basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ into the Hadamard basis $\{\left|+\right\rangle, \left|-\right\rangle\}$. The transformation 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 0.6.2. *For any $\theta \in \mathbb{R}$, consider the matrix*

$$R(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} . \tag{89}$$

The adjoint of this matrix is given by

$$R^\dagger(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} , \tag{90}$$

and therefore

$$\begin{aligned} R(\theta)R^\dagger(\theta) &= \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \cdot \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} & 0 \\ 0 & \sin^2\frac{\theta}{2} + \cos^2\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \end{aligned}$$

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

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

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

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

$$R\left(\frac{\pi}{2}\right)\left|0\right\rangle = \left|+\right\rangle \qquad \text{and} \qquad R\left(\frac{\pi}{2}\right)\left|1\right\rangle = -\left|-\right\rangle. \tag{91}$$

■

Since we will be working with unitaries a lot, it is useful to have multiple ways of recognizing them. Definition 0.6.2 provides one such way. Here is another.

Lemma 1. *Let U be a linear map on $\mathbb{C}^d$ represented by a $d \times d$ matrix. Then U is unitary if and only if the columns of U form an orthonormal basis of $\mathbb{C}^d$. Equivalently, U is unitary if and only if it sends the canonical basis $\{\left|e_1\right\rangle, \dots, \left|e_d\right\rangle\}$ to $\{\left|u_1\right\rangle = U\left|e_1\right\rangle, \dots, \left|u_d\right\rangle = U\left|e_d\right\rangle\}$ such that $\{\left|u_1\right\rangle, \dots, \left|u_d\right\rangle\}$ is also an orthonormal basis of $\mathbb{C}^d$.*

More generally, U is unitary if and only if it transforms any orthonormal basis of $\mathbb{C}^d$ into an orthonormal basis.

Proof. The condition that the columns $\left|u_1\right\rangle, \dots, \left|u_d\right\rangle$ of U are orthonormal is equivalent to the condition $U^*U = \mathbb{I}$. The latter condition is equivalent to $\|U\left|v\right\rangle\| = \|\left|v\right\rangle\|$ for any vector $\left|v\right\rangle$. By taking the conjugate, this is equivalent to $\|U^*\left|v\right\rangle\| = \|\left|v\right\rangle\|$ for any vector $\left|v\right\rangle$, hence $UU^* = \mathbb{I}$ as well.

For the "more generally" part, note that if $U^*U = \mathbb{I}$ then U transforms any orthonormal basis in an orthonormal basis. Conversely, if U transforms any orthonormal basis in an orthonormal basis then it transforms the standard basis in an orthonormal basis, so using the first part U is unitary. □

Remark 0.6.2. *A useful consequence is that if one fixes k orthonormal vectors $\left|v_1\right\rangle, \dots, \left|v_k\right\rangle$ in $\mathbb{C}^d$, for $1 \leq k \leq d$, then there always exists a quantum operation (i.e. a unitary map) that sends $\left|e_i\right\rangle$ to $\left|v_i\right\rangle$ for all $i \in \{1, \dots, k\}$. (In fact, as soon as $k < d$ there are many such operations!) To see this, simply complete $\left|v_1\right\rangle, \dots, \left|v_k\right\rangle$ into an orthonormal basis $\{\left|v_1\right\rangle, \dots, \left|v_k\right\rangle, \dots, \left|v_d\right\rangle\}$ of $\mathbb{C}^d$ and define U to be the matrix whose columns are given by $\left|v_1\right\rangle, \dots, \left|v_d\right\rangle$. By Lemma 1 U is a unitary map, and it sends $\left|e_i\right\rangle$ to $\left|v_i\right\rangle$, as desired.*

0.6.1 Pauli matrices as unitary operations

The Pauli matrices, commonly denoted X, Y, Z, play quite a prominent role in physics. As we will see below they also have an interesting interpretation as operations in quantum computing. The Pauli matrices are unitary 2×2 matrices defined as

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{92}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{93}$$

$$Y = iXZ. \tag{94}$$

Exercise 0.6.1. *Verify that the Pauli matrices X, Z and Y are unitary.* ■

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

$$X|0\rangle = |1\rangle\ , \tag{95}$$

$$X|1\rangle = |0\rangle\ . \tag{96}$$

In analogy to classical computation X is often 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*

$$Z|0\rangle = |0\rangle\ , \tag{97}$$

$$Z|1\rangle = -|1\rangle\ . \tag{98}$$

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

$$Z|+\rangle = Z(|0\rangle + |1\rangle)/\sqrt{2} = (Z|0\rangle + Z|1\rangle)/\sqrt{2} = (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle\,. \tag{99}$$

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:

$$Y|0\rangle = iXZ|0\rangle = iX|0\rangle = i|1\rangle\,. \tag{100}$$

$$Y|1\rangle = -iXZ|0\rangle = -iX|1\rangle = -i|0\rangle\,. \tag{101}$$

0.7 No cloning!

In this section we show that arbitrary qubits, unlike classical bits, cannot be copied. We will see throughout the book that this fundamental limitation of quantum mechanics plays an essential role in quantum cryptography.

To see why, suppose that there existed a copying unitary C. Such a unitary would have the property that

$$C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \ , \tag{102}$$

for *any* input qubit $|\psi\rangle$. Then for any $|\psi_1\rangle$ and $|\psi_2\rangle$,

$$C(|\psi_1\rangle \otimes |0\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle \tag{103}$$
$$C(|\psi_2\rangle \otimes |0\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle \tag{104}$$

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

$$\begin{aligned}
\langle\psi_1|\psi_2\rangle &= \langle\psi_1|\psi_2\rangle\langle 0|0\rangle &(105)\\
&= (\langle\psi_1| \otimes \langle 0|)(|\psi_2\rangle \otimes |0\rangle) &(106)\\
&= (\langle\psi_1| \otimes \langle 0|)C^\dagger C(|\psi_2\rangle \otimes |0\rangle) &(107)\\
&= (\langle\psi_1| \otimes \langle\psi_1|)(|\psi_2\rangle \otimes |\psi_2\rangle) = (\langle\psi_1|\psi_2\rangle)^2. &(108)
\end{aligned}$$

Clearly whenever $0 < |\langle\psi_1|\psi_2\rangle| < 1$ the above cannot hold and hence such a copying unitary C does not exist. Note that $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = |+\rangle$, for example, have precisely this property. Hence there does not even exist a unitary that satisfies (102) just for these two states.

An interesting consequence of the no-cloning principle, that distinguishes quantum information from classical information, is that in general given an unknown qubit state $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ it is not possible to determine the amplitudes α and β exactly. Indeed, if this were possible, then one would be able to clone $|\psi\rangle$ by first determining the amplitudes and then building a machine that repeatedly prepares a qubit in the state $\alpha\,|0\rangle + \beta\,|1\rangle$. As a result, qubits are very precious: when trying to send a qubit through a communication channel it is not possible to simply “try again” in case the communication fails.

0.8 The Bloch sphere

Single-qubit states can be represented in a very convenient visual way in terms of the so-called Bloch sphere. To see how this works, write an arbitrary qubit state as

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right), \tag{109}$$

where γ, θ and ϕ are real numbers that can always be taken in $[0, 2\pi)$. As a first step we observe that the global phase $e^{i\gamma}$ can be neglected, as it has no effect at all on the outcome distribution of any measurement that could be performed on the state. To see this, consider the states

$$|\psi_1\rangle = e^{i\gamma_1}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{110}$$

$$|\psi_2\rangle = e^{i\gamma_2}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{111}$$

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

$$|\langle\psi_1|b\rangle|^2 = \langle b|\psi_1\rangle\langle\psi_1|b\rangle = e^{i(\gamma_1-\gamma_2)}e^{-i(\gamma_1-\gamma_2)}\langle b|\psi_2\rangle\langle\psi_2|b\rangle = |\langle\psi_2|b\rangle|^2. \tag{112}$$

Also, note that this parametrization preserves the normalization condition since $|\alpha|^2 + |\beta|^2 = \cos^2(\theta/2) + \sin^2(\theta/2) = 1$. Thus the state can be characterized using the real numbers (θ, ϕ) only, which allows us to 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 0.8.1. *The parametrization* (θ, ϕ) *of*

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \tag{113}$$

is called the Bloch sphere representation *(Figure 2). Any single-qubit state* (113) *can be represented by a* Bloch vector $\vec{r} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.

Consider a qubit in the representation of Eq. (109) 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. For the sake of building intuition about quantum operations, it is useful 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

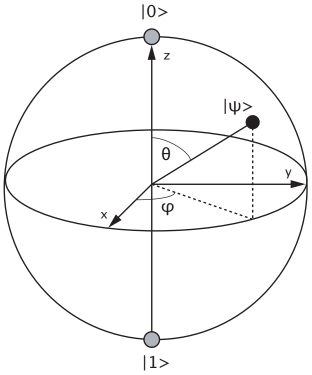

Figure 2: Bloch Sphere

Bloch vector around the axes $s \in \{x, y, z\}$ by an angle θ. Such matrices have the following form:

$$R_x(\theta) = e^{-i\theta X/2},\ R_y(\theta) = e^{-i\theta Y/2} \text{ and } R_z(\theta) = e^{-i\theta Z/2}, \tag{114}$$

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.

0.9 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)**

$$|v_1\rangle \otimes |v_2\rangle := \begin{pmatrix} a_1 b_1 & a_1 b_2 & \cdots & a_1 b_d & a_2 b_1 & \cdots & a_2 b_d & \cdots & a_d b_d \end{pmatrix}^T.$$

Commonly used orthonormal bases for qubits

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

$$\langle 0|1\rangle = \langle 1|0\rangle = 0, \qquad \langle 0|0\rangle = \langle 1|1\rangle = 1, \tag{115}$$

$$\langle +|-\rangle = \langle -|+\rangle = 0, \qquad \langle +|+\rangle = \langle -|-\rangle = 1, \tag{116}$$

$$\left\langle x|x'\right\rangle = \delta_{xx'}, \text{ where } x, x' \in \{0,1\}^n \text{ and } \delta_{xx'} \text{ is the Kronecker-delta function.} \tag{117}$$

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 $\mathcal{B} = \{|b_i\rangle\}_{i=1}^d$. 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,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = iXZ, \tag{118}$$

and the following relations hold:

$$X|0\rangle = |1\rangle\,,\; X|1\rangle = |0\rangle \qquad X|+\rangle = |+\rangle\,,\; X|-\rangle = -|-\rangle \tag{119}$$

$$Z|0\rangle = |0\rangle\,,\; Z|1\rangle = -|1\rangle \qquad Z|+\rangle = |-\rangle\,,\; Z|-\rangle = |+\rangle \tag{120}$$

$$Y|0\rangle = i|1\rangle\,,\; Y|1\rangle = -i|0\rangle \qquad Y|+\rangle = -i|-\rangle\,,\; Y|-\rangle = i|+\rangle \tag{121}$$