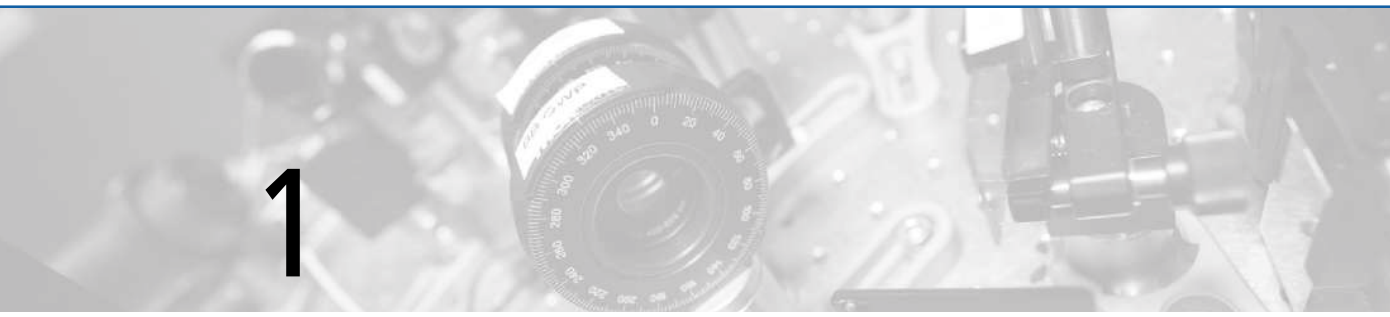

1 Background Material

In this chapter, we give a gentle introduction to quantum information. We will introduce the basics of working with quantum bits – qubits – and examine how to write down simple measurements at the mathematical level. At the end, we will apply our newfound knowledge to see how we can use quantum information to design a deterministic machine that produces true randomness – a feat that is impossible classically. Such a machine is called a quantum random number generator. Quantum random number generators are one of the first commercially available applications of quantum information to cryptography, and it is exciting that we can describe their underlying principle in our first chapter! We conclude with a brief overview of the state of the art of quantum communication technologies needed to realize quantum crytographic protocols in the real world.

For this chapter, and throughout the book, we assume that you already know how to perform calculations involving complex numbers, and that you are familiar with basic notions from linear algebra such as finite-dimensional vector spaces, vectors, and matrices. For suggestions on how to pick up the necessary background, as well as additional resources to learn about how qubits can be realized physically, see the chapter notes at the end of the chapter.

1.1 Mathematical Notation

Let us start by recalling common notation that we use throughout this book. We will use $\mathbb{C}$ to denote the field of complex numbers, and write $i = \sqrt{-1} \in \mathbb{C}$ for the imaginary unit. Remember that any complex number c can be written as $c = a + ib \in \mathbb{C}$ for some real numbers $a, b \in \mathbb{R}$. In this context, we call a the *real part* of c, and b the *imaginary part* of c respectively. The *complex conjugate* of a complex number $c \in \mathbb{C}$ can be written as $c^* = a - ib$. For a complex number, we can define its *absolute value* (sometimes also called *modulus*) as follows.

Definition 1.1.1 (Absolute value of a complex number). *Consider a complex number $c \in \mathbb{C}$ expressed as $c = a + ib$, where $a, b \in \mathbb{R}$. The* absolute value *of c is given by*

$$|c| := \sqrt{c^* c} = \sqrt{a^2 + b^2}. \tag{1.1}$$

For example, the absolute value of $c = 1 + i2$ is $|c| = \sqrt{1^2 + 2^2} = \sqrt{5}$.

Remember that a vector space V over $\mathbb{C}$ is a collection of vectors with complex coefficients, such that V contains the all 0 vector and is stable under vector addition and multiplication by scalars (in this case, the complex numbers). In quantum information vectors are written in a special way known as the "bra-ket" or "Dirac" notation. While it may look a little cumbersome at first, it turns out to provide a convenient way of dealing with the many operations that we will perform with such vectors. To explain the Dirac notation, let us 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,

$$|v\rangle = \begin{pmatrix} 1+i \\ 0 \end{pmatrix} . \tag{1.2}$$

The vector $|v\rangle$ is called a "ket" vector. The "bra" of this vector is its conjugate transpose, which looks like

$$\langle v| := ((|v\rangle)^*)^T = \begin{pmatrix} (1+i)^* \\ 0^* \end{pmatrix}^T = (1-i \quad 0) . \tag{1.3}$$

Here and throughout the book we use the notation ":=" to indicate a definition. The general definition of the "bra-ket" notation is as follows.

Definition 1.1.2 (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*

$$\langle\cdot| = (|\cdot\rangle^*)^T, \tag{1.4}$$

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

We will frequently use the "dagger" notation for the conjugate-transpose: for any vector $|u\rangle \in \mathbb{C}^d$,

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

This notation extends to matrices in the natural way, $A^\dagger := (A^*)^T$.

In quantum information we very often need to compute the inner product of two vectors. The "bra-ket" notation makes this operation very convenient.

Definition 1.1.3 (Inner product). *Given two d-dimensional vectors*

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \qquad \text{and} \qquad |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix} , \tag{1.5}$$

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

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 will see that the modulus squared of the inner product $|\langle v_1|v_2\rangle|^2$

has a physical significance when it comes to measuring qubits. As an example, let us consider the inner product of the vector $|v\rangle$ given in (1.2) and

$$|w\rangle = \begin{pmatrix} 2i \\ 3 \end{pmatrix} . \tag{1.6}$$

We have

$$\langle v|w\rangle = (1-i \quad 0)\begin{pmatrix} 2i \\ 3 \end{pmatrix} = (1-i)\cdot 2i + 0\cdot 3 = 2i - 2i^2 = 2+2i\,. \tag{1.7}$$

Exercise 1.1.1 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 notion of the "length" of a vector. For this we use the *Euclidean norm*.

Definition 1.1.4 (Norm of a ket vector). *Consider a ket vector*

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} . \tag{1.8}$$

The length*, or* norm*, of* $|v\rangle$ *is given by*

$$\| |v\rangle \|_2 := \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{d} a_i^* a_i} = \sqrt{\sum_{i=1}^{d} |a_i|^2}\ . \tag{1.9}$$

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

Example 1.1.1 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

$$\sqrt{\langle v|v\rangle} = \sqrt{\frac{1}{4}\cdot 2\cdot (1+i)(1-i)} = \sqrt{\frac{1}{2}(1+i-i-i^2)} = \sqrt{\frac{1}{2}\cdot 2} = 1. \tag{1.10}$$

■

You should be familiar with the notion of an orthonormal basis for a vector space V from linear algebra. We often write such a basis as $\mathcal{B} = \{|b\rangle\}_b$, which is shorthand for $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$, where d is the dimension of the vector space V in which the kets live, and is often implicit.[1] The condition of being orthonormal can be expressed

1 By convention, in quantum information bases are usually indexed starting at 0, rather than 1. So the standard orthonormal basis of $\mathbb{C}^2$ will be written $\{|0\rangle, |1\rangle\}$.

succinctly as $\langle b|b'\rangle = \delta_{bb'}$ for all $b, b' \in \{0, \ldots, d-1\}$, where δ_{ab} is the *Kronecker symbol*, defined as $\delta_{ab} = 0$ if $a \neq b$ and $\delta_{ab} = 1$ for $a = b$. That is, the different vectors of the basis are orthogonal, and are each normalized to have length 1. Recall that if $\mathcal{B}$ is the basis for a vector space V, then any vector $|v\rangle \in V$ can be expressed as $|v\rangle = \sum_b c_b |b\rangle$, for some coefficients $c_0, \ldots, c_{d-1} \in \mathbb{C}$.

1.2 What Are Quantum Bits?

We are all familiar with the notion of a "bit" in classical computing: mathematically, a bit is a value $b \in \{0,1\}$ that represents some information that is stored and manipulated by an algorithmic procedure. Physically, classical bits can be realized in hardware in many different ways, as long as the two physical states corresponding to "0" and "1" can be distinguished sufficiently clearly. For example, when transmitting data over a fiber-optic cable, the presence of a light pulse can be used to represent a "1" and its absence a "0". Typically, computing and communication systems need more than a single bit to operate, and one talks about a *string of bits* $b = (b_1, \ldots, b_n) \in \{0,1\}^n$.

How do quantum bits differ from classical bits? To define a quantum bit, let us start by writing classical bits somewhat differently. Instead of writing them as "0" and "1", we associate a 2-dimensional vector to each of them as

$$0 \to |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad 1 \to |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.11}$$

The main difference between quantum bits and classical bits is that while a physical classical bit can be in only one of the two states $|0\rangle$ or $|1\rangle$, a qubit can be in any state 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. As we will see later, such amplitudes are directly related to the probabilities of obtaining certain outcomes when measuring the qubit, and the demand that $|\alpha|^2 + |\beta|^2 = 1$ is needed to ensure that these probabilities add up to 1. Since "quantum bit" is somewhat long, researchers use the term "qubit" to refer to a quantum bit. To recap, 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.

Physically, qubits can be realized in many different ways. In the context of quantum communication, $|0\rangle$ and $|1\rangle$ can be realized, for example, by the presence and absence of a photon, in direct analogy to the example from classical communication given above. Amazingly, it is also possible to create a *superposition* between the presence and absence of a photon, and thus realize a qubit.

Definition 1.2.1 (Qubit). *A* pure state of a qubit *can be represented by a 2-dimensional ket vector* $|\psi\rangle \in \mathbb{C}^2$*,*

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \quad \text{where} \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1. \tag{1.12}$$

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 $|\psi\rangle$.*

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, which we introduce in the next chapter.

Example 1.2.1 Some examples of qubits that we will frequently encounter in quantum cryptography are

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ , \quad \text{and} \quad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \ . \tag{1.13}$$

■

QUIZ 1.2.1 *Is $|\psi\rangle = \frac{1}{4}|0\rangle + \frac{1}{8}|1\rangle$ a valid quantum state?*

(a) *Yes*
(b) *No*

QUIZ 1.2.2 *Is $|\psi\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ a valid quantum state?*

(a) *Yes*
(b) *No*

Exercise 1.2.1 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.

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 define a qu*d*it as follows.

Definition 1.2.2 (Qudit). *A pure state of a* qudit *can be represented as a d-dimensional ket vector $|\psi\rangle \in \mathbb{C}^d$,*

$$|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle \ , \quad \text{where} \quad \forall i, \ \alpha_i \in \mathbb{C} \text{ and } \sum_{i=0}^{d-1} |\alpha_i|^2 = 1. \tag{1.14}$$

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 1.2.3 (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*

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{and} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.15}$$

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

Definition 1.2.4 (Hadamard basis). *The* Hadamard basis *of* $\mathbb{C}^2$ *is the orthonormal basis* $\mathcal{H} = \{|+\rangle, |-\rangle\}$ *where*

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{1.16}$$

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

$$\langle +|+\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}\cdot 2 = 1, \quad \Longrightarrow \quad \sqrt{\langle +|+\rangle} = 1, \tag{1.17}$$

so $|+\rangle$ is normalized. A similar calculation gives that $|-\rangle$ is normalized as well. You may wish to verify that this normalization already follows from the more general Exercise 1.2.1, by observing that $|+\rangle = |\psi_{\pi/4}\rangle$ and $|-\rangle = |\psi_{3\pi/4}\rangle$ as defined there. Furthermore, the inner product

$$\langle +|-\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = 0, \tag{1.18}$$

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

Exercise 1.2.2 Decompose the state $|1\rangle$ in the Hadamard basis. In other words, find coefficients α and β such that $|1\rangle = \alpha|+\rangle + \beta|-\rangle$. Verify that $|\alpha|^2 + |\beta|^2 = 1$. This reflects the fact that the formula for the length of a vector given in Definition 1.1.4 does not depend on the choice of the orthonormal basis.

1.3 Multiple Qubits

Classically we can write the state of two bits as a string "00", "01", and so forth. What is the state of two qubits? Proceeding as we did earlier, we can first associate a vector to each of the four possible strings of two classical bits $x_1, x_2 \in \{0,1\}^2$. This gives us a mapping from two-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 two qubits:

$$\begin{aligned}|\psi\rangle_{AB} &= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \\ &= \frac{1}{2}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}. \end{aligned} \tag{1.19}$$

The sum of four 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 is 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

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \ , \tag{1.20}$$

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 1.3.1 (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*

$$|x\rangle = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \longrightarrow i\text{-th position.} \tag{1.21}$$

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

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \qquad \text{where } \forall x, \alpha_x \in \mathbb{C} \text{ and } \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1. \tag{1.22}$$

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 1.3.1 The two-qubit state known as the *EPR pair* is defined as:[2]

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right) = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \tag{1.23}$$

which is an equal superposition between the vectors $|00\rangle$ 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

$$\begin{aligned} \langle \mathrm{EPR}|\mathrm{EPR}\rangle &= \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|) \cdot \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{2}(\underbrace{\langle 00|00\rangle}_{1} + \underbrace{\langle 00|11\rangle}_{0} + \underbrace{\langle 11|00\rangle}_{0} + \underbrace{\langle 11|11\rangle}_{1}) \\ &= \frac{1}{2}\cdot 2 = 1, \qquad \Longrightarrow \qquad \sqrt{\langle \mathrm{EPR}|\mathrm{EPR}\rangle} = 1. \end{aligned} \tag{1.24}$$

Example 1.3.2 Consider the two-qubit state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}. \tag{1.25}$$

2 The abbreviation EPR stands for Einstein, Podolsky, and Rosen. Later we will show that this state is "entangled."

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

QUIZ 1.3.1 *Let* $|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$. *Is this a valid two-qubit state?*

(a) *Yes*
(b) *No*

1.4 Combining Qubits Using the Tensor Product

So far we have learned how to represent the state of one qubit, of two qubits, and more generally of any number n of qubits as a $d = 2^n$-dimensional vector. This normalized vector can be expressed as a linear combination of basis vectors associated with the n-bit strings.

Let us now imagine that we have two qubits, A and B, and that we can write the state of qubit A as $|\psi\rangle_A \in \mathbb{C}^2$ and the state of qubit B as $|\phi\rangle_B \in \mathbb{C}^2$ respectively. How can we find the vector that represents the state of both qubit A and qubit B at the same time? When talking about multiple qubits, we will often refer to A and B as "systems," or "registers"; these words are used interchangeably to designate abstract quantum systems A and B, which could represent physical quantum states situated in different physical locations. Later on, A and B might consist of more than one qubit, and correspond to quantum systems held by different participants such as Alice (A) and Bob (B). We will use AB to denote the joint quantum system, consisting of the qubit(s) of A and the qubit(s) of B. In general, we will use subscripts (here A and B) to denote this, e.g. vector $|\psi\rangle_A$ denotes the state of system A, and $|\phi\rangle_B$ the state of B. Note that from a mathematical standpoint there is no difference between $|0\rangle_A$ and $|0\rangle_B$: both are given by the same vector $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

Let us introduce a new piece of mathematics that allows us to write down the vector for the system AB using our knowledge of the vectors for A and B. The rule that will allow us to do this is known as 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

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}, \tag{1.26}$$

$$|\phi\rangle_B = \alpha_B |0\rangle_B + \beta_B |1\rangle_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix}. \tag{1.27}$$

The joint state $|\psi\rangle_{AB} \in \mathbb{C}^2 \otimes \mathbb{C}^2$ of both qubits is obtained as the tensor product of the individual vectors $|\psi\rangle_A$ and $|\phi\rangle_B$, which by definition evaluates to

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi\rangle_B = \begin{pmatrix} \alpha_A |\psi\rangle_B \\ \beta_A |\psi\rangle_B \end{pmatrix} = \begin{pmatrix} \alpha_A \alpha_B \\ \alpha_A \beta_B \\ \beta_A \alpha_B \\ \beta_A \beta_B \end{pmatrix}. \tag{1.28}$$

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 1.4.1. *For 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*

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 |\psi_2\rangle \\ \vdots \\ \alpha_d |\psi_2\rangle \end{pmatrix}. \tag{1.29}$$

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

$$\text{Omitting the tensor product symbol:} \quad |\psi\rangle_A \otimes |\psi\rangle_B = |\psi\rangle_A |\psi\rangle_B. \tag{1.30}$$

$$\text{Writing classical bits as a string:} \quad |0\rangle_A \otimes |0\rangle_B = |0\rangle_A |0\rangle_B = |00\rangle_{AB}. \tag{1.31}$$

$$\text{Combining several identical states:} \quad |\psi\rangle_1 \otimes |\psi\rangle_2 \cdots \otimes |\psi\rangle_n = |\psi\rangle^{\otimes n}. \tag{1.32}$$

The tensor product satisfies a few important properties, which we will use frequently throughout the book.

Proposition 1.4.1 *Properties of the tensor product:*

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 $|\psi_1\rangle = |\psi_2\rangle$. You may convince yourself of this fact by computing the representation as 4-dimensional vectors, using the rule (1.28), of $|0\rangle \otimes |1\rangle$ and $|1\rangle \otimes |0\rangle$.

To practice with 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.