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 new found 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

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

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 shall 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 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

[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 $\{|0\rangle, |1\rangle\}$.

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 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 $|\alpha|^2 + |\beta|^2 = 1$ denotes a valid state of a qubit. 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 in 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, that we introduce in the next chapter.

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

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

■

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*

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

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, by observing that $|+\rangle = |\psi_{\pi/4}\rangle$ and $|-\rangle = |\psi_{3\pi/4}\rangle$ 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 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:

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

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 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

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

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

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

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

$$\begin{aligned} \langle \mathrm{EPR}|\mathrm{EPR}\rangle &= \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|) \cdot \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) && (1.24)\\ &= \frac{1}{2}(\underbrace{\langle 00|00\rangle}_{1} + \underbrace{\langle 00|11\rangle}_{0} + \underbrace{\langle 11|00\rangle}_{0} + \underbrace{\langle 11|11\rangle}_{1}) && (1.25)\\ &= \frac{1}{2}\cdot 2 = 1, \qquad \Longrightarrow \qquad \sqrt{\langle EPR|EPR\rangle} = 1. && (1.26) \end{aligned}$$

Example 1.3.2 *Consider the* 2*-qubit state*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}\,. \tag{1.27}$$

For this state, the second qubit always corresponds to the 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".

Quiz 1.3.1 *Let* $|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$. *Is this a valid 2-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 1 qubit, of 2 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 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 qubits A and 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 the 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. Not 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

$$|\psi\rangle_A = \alpha_A |0\rangle_A + \beta_A |1\rangle_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix}, \tag{1.28}$$

$$|\phi\rangle_B = \alpha_B |0\rangle_B + \beta_B |1\rangle_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix} \quad . \tag{1.29}$$

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

$$|\psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \otimes |\psi\rangle_B = \begin{pmatrix} \alpha_A |\psi\rangle_B \\ \beta_A |\psi\rangle_B \end{pmatrix} = \begin{pmatrix} \alpha_A\alpha_B \\ \alpha_A\beta_B \\ \beta_A\alpha_B \\ \beta_A\beta_B \end{pmatrix}. \tag{1.30}$$

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*

$$|\psi_1\rangle \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix} \otimes |\psi_2\rangle = \begin{pmatrix} \alpha_1 |\psi_2\rangle \\ \vdots \\ \alpha_d |\psi_2\rangle \end{pmatrix} . \tag{1.31}$$

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

$$\text{Omitting the tensor product symbol:} \quad |\psi\rangle_A \otimes |\psi\rangle_B = |\psi\rangle_A |\psi\rangle_B . \tag{1.32}$$

$$\text{Writing classical bits as a string:} \quad |0\rangle_A \otimes |0\rangle_B = |0\rangle_A |0\rangle_B = |00\rangle_{AB} . \tag{1.33}$$

$$\text{Combining several identical states:} \quad |\psi\rangle_1 \otimes |\psi\rangle_2 \cdots \otimes |\psi\rangle_n = |\psi\rangle^{\otimes n} . \tag{1.34}$$

The tensor product satisfies a few important properties, which we will use frequently all 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 (1.30), 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.

Example 1.4.1 *Recall that the standard basis for two qubits A and B is given by*

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

This basis can be 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

$$|1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes |0\rangle_B = \begin{pmatrix} 0 |0\rangle_B \\ 1 |0\rangle_B \end{pmatrix} = \begin{pmatrix} 0 \cdot 1 \\ 0 \cdot 0 \\ 1 \cdot 1 \\ 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle_{AB} . \tag{1.35}$$

■

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

Example 1.4.2 *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*

$$|\psi\rangle_{AB} = |+\rangle_A \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}_A \otimes |1\rangle_B = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot|1\rangle_B\\1\cdot|1\rangle_B\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\0\\1\end{pmatrix}. \quad (1.36)$$

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

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

This is the state from Example 1.3.2. ■

Example 1.4.3 *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*

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

This is the state we have seen in (1.19)*, which is an equal superposition of all standard basis states for the two qubits.* ■

Quiz 1.4.1 $|\psi\rangle \otimes |\phi\rangle = |\phi\rangle \otimes |\psi\rangle$ *for all* $|\psi\rangle$ *and* $|\phi\rangle$. *True or false?*

a) True
b) False

Quiz 1.4.2 *Consider a two-qubit state* $|\psi\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$. *How do you write this state in a vector form in the standard basis? In other words, compute* $|\psi\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$.

a) $|\psi\rangle = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_2\beta_2 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \end{pmatrix}$

b) $|\psi\rangle = \begin{pmatrix} \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ 0 \\ 0 \end{pmatrix}$

c) $|\psi\rangle = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix}$

Quiz 1.4.3 *Consider the following state $|\psi\rangle$ of two qubits: $|\psi\rangle = |-\rangle \otimes |-\rangle$, where $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Written in the standard basis, this state can be expressed as $|\psi\rangle = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)$. True or false?*

a) True

b) False

Looking at these examples, one may wonder whether *any* state $|\psi\rangle_{AB}$ of two qubits may be expressed as the tensor product of two states $|\psi\rangle_A$ and $|\psi\rangle_B$. It is turns out that this is *not* the case! Later, we will see that such states have special properties (in Chapter 4 we will learn they are *entangled*), and without them much of quantum cryptography would not be possible. Let's see an example of such a state, for which it is impossible to find any such $|\psi\rangle_A$ and $|\psi\rangle_B$. To avoid any confusion, our example also illustrates that the state $|\psi\rangle_{AB}$ can of course still be expressed as a linear combination of the standard basis for 2 qubits.

Example 1.4.4 *Consider the state of two qubits*

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B\big)\,. \tag{1.37}$$

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

$$\begin{aligned} |+\rangle_A|+\rangle_B &= \frac{1}{2}(|0\rangle_A + |1\rangle_A)(|0\rangle_B + |1\rangle_B) \\ &= \frac{1}{2}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB})\,, \\ |-\rangle_A|-\rangle_B &= \frac{1}{2}(|0\rangle_A - |1\rangle_A)(|0\rangle_B - |1\rangle_B) \\ &= \frac{1}{2}(|00\rangle_{AB} - |10\rangle_{AB} - |01\rangle_{AB} + |11\rangle_{AB})\,. \end{aligned}$$

Substituting this into Eq. (1.37) *gives*

$$\begin{aligned}|\psi\rangle_{AB} &= \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B) \\ &= \frac{1}{2\sqrt{2}}(|00\rangle_{AB} + |10\rangle_{AB} + |01\rangle_{AB} + |11\rangle_{AB} + |00\rangle_{AB} - |10\rangle_{AB} - |01\rangle_{AB} + |11\rangle_{AB}) \\ &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) = |\mathrm{EPR}\rangle_{AB} \end{aligned} \tag{1.38}$$

where $|\mathrm{EPR}\rangle_{AB}$ *is the state we have seen previously in Example 1.3.1. 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 you will show in Exercise* **??***, 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* (1.37) *and* (1.38). ■

1.5 Simple measurements

Let us now examine how we can mathematically describe the simplest possible measurements on our qubit(s). Thinking back to the example encoding of classical bits "0" and "1" by the absence and presence of a light pulse, a way to physically measure them immediately presents itself: we could simply "look" whether light is present or not. When we see light, we record a "1" and when we see no light, we write down a "0".

How about measuring a qubit? In our example of using the absence of a photon to represent a $|0\rangle$ and the presence a $|1\rangle$ an idea for a measurement immediately presents itself: we could install a detector capable of measuring a single photon and record a "0" when no photon is detected and a "1" otherwise.

1.5.1 Measurement in the standard basis

It turns out that this idea of a measuring mathematically is known as measuring the qubit in the standard (or computational) basis. Remember that a state of a qubit can be 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 in the example above we are asking the question: "Is $|\psi\rangle$ in state $|0\rangle$ (no photon) or in state $|1\rangle$ (photon)?". Given that $|\psi\rangle$ is in general neither of these — it is in a *superposition* of the two basis states — how do we answer such a question? The measurement rule gives a way to do this. 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.

For 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

$$p_0 = |\,\langle\psi|0\rangle\,|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right|^2 = |\alpha|^2,$$
$$p_1 = |\,\langle\psi|1\rangle\,|^2 = \left|\begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right|^2 = |\beta|^2. \tag{1.39}$$

We now see a good reason for the condition $|\alpha|^2 + |\beta|^2 = 1$: it means that $p_0 + p_1 = 1$, the probabilities of observing '$|0\rangle$' and '$|1\rangle$', add up to 1.

Quiz 1.5.1 *The state $|1\rangle$ is measured in the standard basis. What is the probability of obtaining the outcome 0?*

a) 0
b) $\frac{1}{2}$
c) $\frac{3}{4}$
d) $\frac{\sqrt{3}}{2}$

What happens after the measurement? Measuring our qubit in the standard basis destroys the superposition. Thinking back to our physical example, once we detected a photon, we are in the state $|1\rangle$. If we did not detect a photon, $|0\rangle$. There is no way for us to re-create the superposition, and we we will say the state has *collapsed*.

In quantum information we 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 when convenient; which will always be clear in context.

1.5.2 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 build a deterministic machine — i.e. a machine that uses no randomness itself — that nevertheless produces true random numbers.

Consider the following process illustrated in Figure 1.1: 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

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

of obtaining each outcome can be calculated by evaluating the inner products, using the recipe given in (1.39):

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

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

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'.

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 for cryptography: as we will see throughout the book, uncertainty, or ignorance, is the key to security. Moreover, machines exploiting such ideas have already been built, see e.g. Figure 1.2.

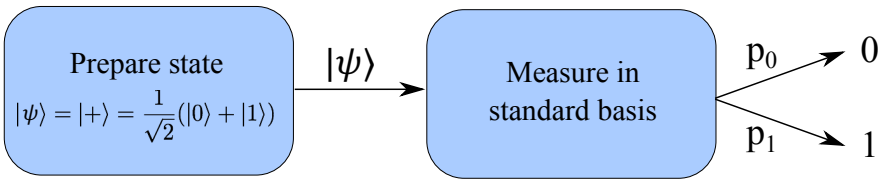

Fig. 1.1 Generation of true randomness from the deterministic preparation of a qubit in superposition.

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

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \ . \tag{1.40}$$

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.

1.5.3 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 can

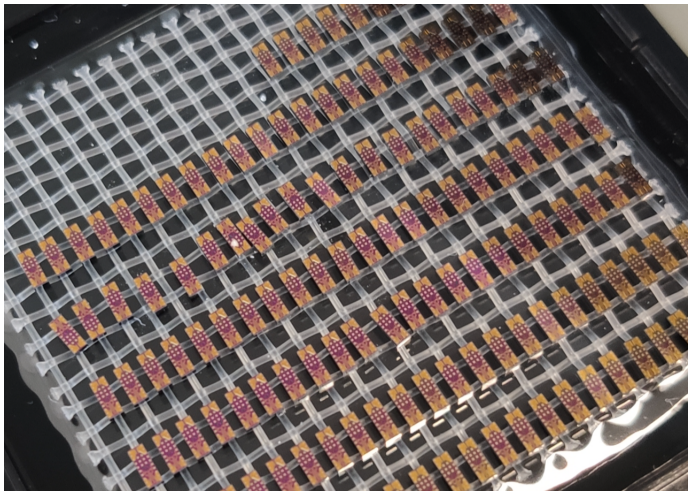

Fig. 1.2 Chip generating quantum random numbers (QuSide)

Box 1.1 **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 $E = 1 \cdot |\langle 0|\psi\rangle|^2 - 1 \cdot |\langle 1|\psi\rangle|^2$. Since $|\langle 0|\psi\rangle|^2 = \langle\psi|0\rangle\langle 0|\psi\rangle$, we have $E = \langle\psi| \left(|0\rangle\langle 0| - |1\rangle\langle 1|\right) |\psi\rangle = \langle\psi| Z |\psi\rangle$, 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 frequently in the future; it is called the "Pauli Z observable".

be used to define 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, we expand the quantum state as a superposition over

vectors from the new basis, i.e. find amplitudes $\hat{\alpha}$ and $\hat{\beta}$ such that

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \hat{\alpha}\,|v_0\rangle + \hat{\beta}\,|v_1\rangle\ . \tag{1.41}$$

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 and can be found by simple linear algebra. Second, take the modulus squared of the associated amplitudes $\hat{\alpha}$ and $\hat{\beta}$ 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 1.5.1 *Consider the qubit $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Instead of measuring it in the standard basis, let us now measure in the basis $\{|+\rangle, |-\rangle\}$ given by the two orthonormal vectors of the Hadamard basis, $|+\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. 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 $|1|^2 = 1$, 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 1.5.2 *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*

$$|0\rangle = \frac{1}{2}\big((|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)\big) = \frac{1}{\sqrt{2}}\,(|+\rangle + |-\rangle)\ , \tag{1.42}$$

$$|1\rangle = \frac{1}{2}\big((|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)\big) = \frac{1}{\sqrt{2}}\,(|+\rangle - |-\rangle)\ . \tag{1.43}$$

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

$$\alpha\,|0\rangle + \beta\,|1\rangle = \frac{1}{\sqrt{2}}\big(\alpha(|+\rangle + |-\rangle) + \beta(|+\rangle - |-\rangle)\big) \tag{1.44}$$

$$= \frac{\alpha+\beta}{\sqrt{2}}\,|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}\,|-\rangle\ . \tag{1.45}$$

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. ∎

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

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\ . \tag{1.46}$$

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

$$p_0 = |\langle 0|\psi\rangle|^2 = \left|(1\ 0)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\alpha|^2 \tag{1.47}$$

$$p_1 = |\langle 1|\psi\rangle|^2 = \left|(0\ 1)\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\right|^2 = |\beta|^2 \tag{1.48}$$

Example 1.5.3 *Suppose we measure $|0\rangle$ in the Hadamard basis. The probabilities of observing outcomes "$|+\rangle$" and "$|-\rangle$" are given by*

$$p_+ = |\langle +|0\rangle|^2 = \left|(\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,, \tag{1.49}$$

$$p_- = |\langle -|0\rangle|^2 = \left|(\frac{1}{\sqrt{2}}\ \frac{-1}{\sqrt{2}})\begin{pmatrix}1\\ 0\end{pmatrix}\right|^2 = \frac{1}{2}\,. \tag{1.50}$$

■

For qudits, the rule for finding probabilities is analogous.

Definition 1.5.1 *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*

$$p_j = |\langle b_j|\psi\rangle|^2\,. \tag{1.51}$$

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 1.5.4 *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:

$$\begin{aligned}
p_+ = |\langle +|\psi\rangle|^2 &= \left|\frac{1}{2}(\langle 0| + \langle 1|)(|0\rangle + i|1\rangle)\right|^2 \\
&= \frac{1}{4}\left|\langle 0|0\rangle + \langle 1|0\rangle + i\langle 1|0\rangle + i\langle 1|1\rangle\right|^2 \\
&= \frac{1}{4}|1+i|^2 \\
&= \frac{1}{4}(1-i)(1+i) = \frac{1}{2}, \\
p_- = |\langle -|\psi\rangle|^2 &= \left|\frac{1}{2}(\langle 0| - \langle 1|)(|0\rangle + i|1\rangle)\right|^2 \\
&= \frac{1}{4}\left|\langle 0|0\rangle - \langle 1|0\rangle + i\langle 0|1\rangle - i\langle 1|1\rangle\right|^2 \\
&= \frac{1}{4}|1-i|^2 \\
&= \frac{1}{4}(1+i)(1-i) = \frac{1}{2}.
\end{aligned}$$

■

Quiz 1.5.2 *The state* $|1\rangle$ *is measured in the basis* $\{|0'\rangle, |1'\rangle\}$*, where* $|0'\rangle = \frac{1}{2}\left(|0\rangle + \sqrt{3}|1\rangle\right)$ *and* $|1'\rangle = \frac{1}{2}\left(\sqrt{3}|0\rangle - |1\rangle\right)$*. What is the probability of obtaining the outcome* $0'$*?*

a) 0
b) $\frac{1}{2}$
c) $\frac{3}{4}$
d) $\frac{\sqrt{3}}{2}$

While we will generally talk about states of qubits, we may occasionally consider quantum states in d dimensions, where d is not necessarily a power of 2.

Example 1.5.5 *Consider a* qutrit $|\psi\rangle \in \mathbb{C}^3$*, which is a* 3*-dimensional quantum system, represented by the vector*

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\1\\0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0\\0\\1\end{pmatrix}. \tag{1.52}$$

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

$$|b_1\rangle = \begin{pmatrix}1\\0\\0\end{pmatrix}, \qquad |b_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\end{pmatrix}, \qquad |b_3\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\end{pmatrix}. \tag{1.53}$$

Box 1.2 **Distinguishing quantum states**

Suppose we are given a quantum state $|\psi\rangle \in \mathbb{C}^d$. We do not know $|\psi\rangle$ exactly, but we do know that $|\psi\rangle$ is one of two possible quantum states, $|\psi_0\rangle$ or $|\psi_1\rangle$. How is it possible to find out which of the two states $|\psi_0\rangle$ and $|\psi_1\rangle$ we have? If $|\psi_0\rangle$ and $|\psi_1\rangle$ are *orthogonal* then there is always an orthonormal basis $\{|b_0\rangle, |b_2\rangle, \ldots, |b_{d-1}\rangle\}$ such that $|b_0\rangle = |\psi_0\rangle$ and $|b_1\rangle = |\psi_1\rangle$. A measurement of $|\psi\rangle$ in this basis will yield the outcome b_0 if and only if $|\psi\rangle = |\psi_0\rangle$ and the outcome b_1 if and only if $|\psi\rangle = |\psi_1\rangle$, hence the two states can be perfectly distinguished. If, however, $|\psi_0\rangle$ and $|\psi_1\rangle$ are not orthogonal then it is impossible to distinguish them with certainty using a quantum measurement. We return to this question in Chapter 5.

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

$$p_{b_1} = |\langle b_1|\psi\rangle|^2 = \frac{1}{2}, \tag{1.54}$$

$$p_{b_2} = |\langle b_2|\psi\rangle|^2 = \langle b_2|v\rangle \langle v|b_2\rangle = \frac{1}{2\sqrt{2}}(1+1)\cdot\frac{1}{2\sqrt{2}}(1+1) = \frac{1}{2}, \tag{1.55}$$

$$p_{b_3} = |\langle b_3|\psi\rangle|^2 = \langle b_3|v\rangle \langle v|b_3\rangle = \frac{1}{2\sqrt{2}}(1-1)\cdot\frac{1}{2\sqrt{2}}(1-1) = 0. \tag{1.56}$$

■

1.5.4 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 see explicitly what happens when such a state is measured. Let us do it in general: consider a 2-qudit state in the space $|\psi\rangle_{AB} \in \mathbb{C}_A^{d_A} \otimes \mathbb{C}_B^{d_B}$, 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 $\mathbb{C}_A^{d_A}$ and $\mathbb{C}_B^{d_B}$: 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 $\{\{|b_j^A\rangle \otimes |b_k^B\rangle\}_{j=0}^{d_A}\}_{k=0}^{d_B}$ gives a basis for $\mathbb{C}_A^{d_A} \otimes \mathbb{C}_B^{d_B}$.

Example 1.5.6 *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 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

$$p_{jk} = |\langle b_j^A|\langle b_k^B|\,|\psi\rangle_{AB}\,|^2\,. \tag{1.57}$$

Example 1.5.7 *Consider two qubits in an EPR pair*

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\,. \tag{1.58}$$

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

$$p_{00} = p_{11} = \frac{1}{2}\,, \quad p_{01} = p_{10} = 0\,. \tag{1.59}$$

■

1.5.5 Post-measurement states

In general, when a state $|\psi\rangle \in \mathbb{C}^d$ is measured in a basis $\{|b_i\rangle\}_i$ 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.

1.6 Unitary transformations and gates

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.

1.6.1 Unitary transformations

First consider operations that transform the state of some qubits to a different state of the same qubits. Mathematically, we are interested in operations that transform normalized states in $\mathbb{C}^d$ to normalized states in the same space. According to the laws of quantum mechanics, a necessary condition on any such transformation for it to be a valid quantum operation is that it should be *linear*: any quantum map U that performs a transformation

$$U : |\psi_{\mathrm{in}}\rangle \mapsto |\psi_{\mathrm{out}}\rangle = U(|\psi_{\mathrm{in}}\rangle) \tag{1.60}$$

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 deduce that any quantum operation that acts on d-dimensional qudits can be represented by some $d \times d$ matrix U with complex coefficients. This is because any linear map on $\mathbb{C}^d$ has a matrix representation. Furthermore, since we want the operation to map quantum states to quantum states, it should preserve lengths: for all possible states $|\psi_{\text{in}}\rangle$,

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}| U^\dagger U |\psi_{\text{in}}\rangle = 1 \,, \tag{1.61}$$

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

$$\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle = \langle\psi_{\text{in}}| UU^\dagger |\psi_{\text{in}}\rangle = 1 \,. \tag{1.62}$$

This shows that the condition that the operation U preserves the length of any vector is equivalent to the condition that $U^\dagger U = UU^\dagger = \mathbb{I}$, where $\mathbb{I}$ is the identity matrix.

Definition 1.6.1 (Identity) *The identity matrix is a diagonal, square matrix with all diagonal entries equal to* 1*:*

$$\mathbb{I} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} . \tag{1.63}$$

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

Definition 1.6.2 (Unitary operation) *An operation U is unitary if and only if $U^\dagger U = UU^\dagger = \mathbb{I}$.*

The allowed operations on quantum states $|\psi\rangle$ are precisely the unitary operations. Note that $\mathbb{I}$ is itself a unitary operation, called the *identity operation*. This just means that the state is not transformed at all.Note that since $U^\dagger U = \mathbb{I}$, any operation U is reversible: if $|\psi\rangle$ has been transformed to $U|\psi\rangle$ we can undo U by applying $U^\dagger$, which is also unitary, to obtain $U^\dagger U|\psi\rangle = \mathbb{I}|\psi\rangle = |\psi\rangle$. To gain some intuition on them, let us have a look at some examples.

Example 1.6.1 *Consider the matrix*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{1.64}$$

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

$$H^\dagger H = HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{I} \,. \tag{1.65}$$

That is, H is unitary. We have that

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle \ . \tag{1.66}$$

Similarly, you can verify that $H|1\rangle = |-\rangle$. We thus see that H transforms the computational basis $\{|0\rangle, |1\rangle\}$ into the Hadamard basis $\{|+\rangle, |-\rangle\}$. The transformation H is called the Hadamard transform*, or* Hadamard gate*.* ∎

Let us now consider a somewhat more complicated operation.

Example 1.6.2 *For any $\theta \in \mathbb{R}$, consider the matrix*

$$R(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}. \tag{1.67}$$

The conjugate-transpose of this matrix is given by

$$R^\dagger(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{1.68}$$

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. Moreover,

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

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

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

$$R\left(\frac{\pi}{2}\right)|0\rangle = |+\rangle \qquad \text{and} \qquad R\left(\frac{\pi}{2}\right)|1\rangle = -|-\rangle\,. \tag{1.69}$$

∎

Quiz 1.6.1 *What is the action of the Hadamard transformation on $|+\rangle$?*

a) $H|+\rangle = |0\rangle$
b) $H|+\rangle = |1\rangle$
c) $H|+\rangle = |-\rangle$

Since we will be working with unitaries a lot, it is useful to have multiple ways of recognizing them. Definition 1.6.2 provides one such way. Here is another.

Lemma 1.6.2 *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 $\{|e_0\rangle, \ldots, |e_{d-1}\rangle\}$ to $\{|u_0\rangle = U|e_0\rangle, \ldots, |u_{d-1}\rangle = U|e_{d-1}\rangle\}$ such that $\{|u_0\rangle, \ldots, |u_{d-1}\rangle\}$ 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 $|u_0\rangle, \ldots, |u_{d-1}\rangle$ of U are orthonormal is equivalent to the condition $U^\dagger U = \mathbb{I}$. The latter condition is equivalent to

$$\| U|v\rangle \|^2 = \langle v| U^\dagger U |v\rangle = \langle v|v\rangle = \| |v\rangle \|^2$$

for any vector $|v\rangle$. By taking the conjugate, this is equivalent to $\|U^\dagger |v\rangle\| = \| |v\rangle \|$ for any vector $|v\rangle$, hence $UU^\dagger = \mathbb{I}$ 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 1.6.3 *A useful consequence is that if one fixes k orthonormal vectors $|v_0\rangle, \ldots, |v_k\rangle$ in $\mathbb{C}^d$, for $0 \leq k \leq d-1$, then there always exists a unitary U that sends $|e_i\rangle$ to $|v_i\rangle = U|e_i\rangle$ for all $i \in \{0, \ldots, k\}$. (In fact, as soon as $k < d-1$ there are many such operations!) To see this, simply complete $|v_0\rangle, \ldots, |v_k\rangle$ to an orthonormal basis $\{|v_0\rangle, \ldots, |v_k\rangle, \ldots, |v_{d-1}\rangle\}$ of $\mathbb{C}^d$ and define U to be the matrix whose columns are given by $|v_0\rangle, \ldots, |v_{d-1}\rangle$. By Lemma 1.6.2, U is a unitary map, and it sends $|e_i\rangle$ to $|v_i\rangle = U|e_i\rangle$, as desired.*

Quiz 1.6.2 *Is $U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ a valid unitary transformation?*

a) Yes
b) No

Quiz 1.6.3 *Consider a unitary transformation $U = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Which operation corresponds to $U^\dagger$?*

a) $U^\dagger = \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$
b) $U^\dagger = \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix}$
c) $U^\dagger = \begin{pmatrix} i & 0 \\ 0 & -1 \end{pmatrix}$
d) $U^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}$

Quiz 1.6.4 *Consider a unitary operation U that has the following action: $U|0\rangle|0\rangle = |0\rangle|0\rangle$ and $U|1\rangle|0\rangle = |1\rangle|1\rangle$. What is the action of U on $|-\rangle|0\rangle$?*

a) $U|-\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle)$
b) $U|-\rangle|0\rangle = |-\rangle|-\rangle$

1.6.2 Pauli matrices as unitary operations

The Pauli matrices are unitary 2×2 matrices defined as

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

(The i is there to make Y Hermitian, that is, $Y^\dagger = Y$.) These matrices play a prominent role in physics, because they model simple observables (see Box 1.1) that can be performed on a single qubit. As we will see below they also have an interesting interpretation as operations or *gates* in quantum computing.

Exercise 1.6.1 Verify that the Pauli matrices X, Z and Y are unitary.

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

$$X|0\rangle = |1\rangle\ ,$$
$$X|1\rangle = |0\rangle\ .$$

In analogy to classical computation X is often referred to as the NOT gate, 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*

$$Z|0\rangle = |0\rangle\ ,$$
$$Z|1\rangle = -|1\rangle\ .$$

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

$$Z|+\rangle = Z\big(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\big) = \frac{1}{\sqrt{2}}(Z|0\rangle + Z|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,. \quad (1.70)$$

Similarly, $Z|-\rangle = |+\rangle$. We thus see that Z acts like a bit flip on the Hadamard basis, while it acts like a phase flip in the standard basis. Applying both a bit and a phase flip gives $Y = iXZ$. This matrix, when acting on the standard basis vectors, introduces a bit flip and a phase flip:

$$Y|0\rangle = iXZ|0\rangle = iX|0\rangle = i|1\rangle\,. \quad (1.71)$$
$$Y|1\rangle = -iXZ|0\rangle = -iX|1\rangle = -i|0\rangle\,. \quad (1.72)$$

1.6.3 No cloning!

We now use our understanding of unitaries U to 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 we cannot copy arbitrary qubits $|\psi\rangle$, suppose that there existed a copying unitary C. Such a unitary would have the property that

$$C(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \ , \tag{1.73}$$

for *any* input qubit $|\psi\rangle$. That is, it would produce a copy of $|\psi\rangle$. Then for any $|\psi_1\rangle$ and $|\psi_2\rangle$,

$$\begin{aligned} C(|\psi_1\rangle \otimes |0\rangle) &= |\psi_1\rangle \otimes |\psi_1\rangle \\ C(|\psi_2\rangle \otimes |0\rangle) &= |\psi_2\rangle \otimes |\psi_2\rangle \end{aligned}$$

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

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

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 (1.73) just for these two states. Note that if we have only classical bits $|0\rangle$ and $|1\rangle$, then these can be copied. Indeed, $0^2 = 0$ and so for this restricted case there is no contradiction in (**??**).

An interesting consequence of the no-cloning principle, that distinguishes quantum information from classical information, is that in general given an unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ it is not possible to determine the amplitudes α and β exactly. Indeed, if it were possible to measure α and β, then one would be able to clone $|\psi\rangle$ by first determining the amplitudes α and β 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. For example, when trying to send a qubit $|\psi\rangle$ through a communication channel it is generally not possible to simply "try again" in case the communication fails.

1.7 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

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{1.74}$$

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

$$|\psi_1\rangle = e^{i\gamma_1}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{1.75}$$

$$|\psi_2\rangle = e^{i\gamma_2}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{1.76}$$

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 an outcome b is equal for both states, since

$$|\langle\psi_1|b\rangle|^2 = \langle b|\psi_1\rangle\langle\psi_1|b\rangle = e^{i(\gamma_1-\gamma_2)}e^{-i(\gamma_1-\gamma_2)}\langle b|\psi_2\rangle\langle\psi_2|b\rangle = |\langle\psi_2|b\rangle|^2. \tag{1.77}$$

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. This allows us to think of the qubit as a point on a 3-dimensional sphere, as in Figure 1.3. It should be emphasized that this sphere does not follow the same coordinates as we have used for the vectors $|v\rangle \in \mathbb{C}^2$; we need to translate to the new coordinate system.

Definition 1.7.1 *The parametrization* (θ, ϕ) *of*

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) \tag{1.78}$$

is called the Bloch sphere representation *(Figure 1.3). Any single-qubit state* (1.78) *can be represented by a* Bloch vector $\vec{r} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.

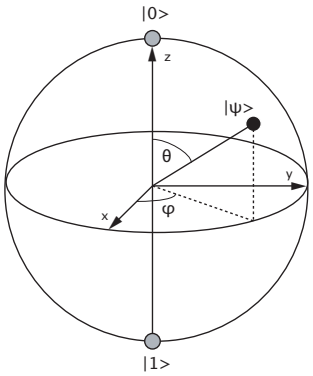

Fig. 1.3 The Bloch Sphere. The qubit $|\psi\rangle$ is represented by its Bloch vector $\vec{r} = (\cos\phi\sin\theta, \sin\phi\sin\theta, \cos\theta)$.

Consider a qubit in the representation of Eq. (1.74) 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 gate on a qubit. Note that $(|0\rangle + |1\rangle)/\sqrt{2}$ can be found in Figure 1.3 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 this can be done. 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:

$$R_x(\theta) = e^{-i\theta X/2},\ R_y(\theta) = e^{-i\theta Y/2} \text{ and } R_z(\theta) = e^{-i\theta Z/2}, \tag{1.79}$$

where X, Y, Z are the Pauli matrices introduced in the previous section. Especially important is the rotation around the z axis. We can express it in more detail as

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

It can be shown that 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.

Remark 1.7.1 *It would be natural to think that more generally for n-qubit states $|\psi\rangle = \sum_x \alpha_x |x\rangle$ the coefficients α_x can be re-parametrized using $2^{n+1} - 1$ real parameters and plotted on some form of higher-dimensional analogue of the Bloch sphere. Unfortunately this is not the case, and the Bloch sphere representation is only used for a single qubit, where it forms a useful visualization tool.*

Quiz 1.7.1 *Which of the following states lies on the x-axis of the Bloch sphere?*

a) $|\psi_1\rangle = |0\rangle$
b) $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
c) $|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$

Quiz 1.7.2 *Which of the following states lies on the equator, i.e. the xy plane, of the Bloch sphere for all values of θ in the indicated range?*

a) $|\psi_1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\frac{\pi}{2}} \sin\left(\frac{\theta}{2}\right)|1\rangle,\ \theta \in [0, \pi]$
b) $|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right),\ \theta \in [0, 2\pi]$
c) $|\psi_3\rangle = e^{i\theta}|1\rangle,\ \theta \in [0, 2\pi]$

1.8 Implementing quantum cryptography

The goal of this book is to teach you the theory needed to become a a quantum cryptographer, who is capable of analyzing – and maybe even designing your own! – quantum cryptographic protocols. As such, we will adopt a mathematical approach throughout the remainder of this book, and not consider how quantum cryptographic protocols can be implemented in the real world. That is, we will simply assume that qubits can be manipulated, exchanged and measured by the protocol participants. If you are nevertheless interested in understanding physical implementations, we provide a very brief introduction to such implementations in this section. Indeed, you may wish to know how far quantum cryptography actually is from a practical reality? Or, if you want to embark on designing your own protocols, which protocols may be easier to realize in practice?

1.8.1 Ingredients

As you might imagine, there is no easy answer to such questions: it depends! To get ourselves closer to answering them, it is useful to examine what is actually needed to implement a quantum cryptographic protocol in the real world. First, we need a device that a user can use to manipulate quantum information locally in order to play their part in a quantum cryptographic protocol. That is, we need a device that can perform quantum measurements, or even more general quantum operations. In full analogy to the classical world, you can think of this device as the quantum laptop that a user might use in order to execute their part of a protocol. In the context of quantum communication, such a device is generally called an end node. In the quantum domain, very simple end nodes capable of preparing and measuring one quantum bit at a time can already be used to realize quantum cryptographic functionality that is impossible to replicate classically. Indeed, we will see one example in Chapter 8! Such end nodes may be realized using relatively simple photonic quantum devices that do not require a quantum memory.

At first glance, it may be surprising that one can do things that are impossible classically with an end node that can only deal with a single qubit at a time. After all, in quantum computing one needs a quantum computer capable of manipulating more quantum bits than can be simulated on a classical supercomputer in order to gain a quantum advantage. Intuitively, the reason why such simple end nodes suffice to gain a quantum advantage in quantum cryptography is the fact that already one qubit suffices to observe some of the properties of quantum mechanics that are essential for cryptography, such as the no-cloning principle and uncertainty relations. What's more, two quantum bits – one for each end node – can share a property called quantum entanglement that we will learn about in Chapter 4. Since it is impossible to simulate all the properties of quantum entanglement using any amount of classical communication, we can unlock many of the benefits of quantum cryptography using two simple end nodes that share an entangled pair of qubits. Of course, using more sophisticated end nodes one may hope to realize more complex quantum cryptographic functionality. We will see some examples of this later in Chapters 10 and 13.

End nodes themselves are of course not enough: they need a way to talk to each other! The second ingredient that we need is a means to transmit quantum states from one end node to the other, or to create quantum entanglement between quantum devices. That is, we need a a way to communicate quantum information between end nodes. This is analogous to the classical communication channel between laptops or phones that is needed in order to execute classical cryptographic protocols. Quantum communication can be performed over physical media that are able to carry light, such as commercial telecom fibers, or through the air such as freespace connections from a quantum satellite to a ground station.

The third ingredient needed to make quantum cryptographic technologies broadly usable is a bit more subtle to express and relates to the cost and reliability of quantum communication technologies. Such cost could be lowered, for example, by an ability to share parts of such technologies between many users. Classically, it is often cost effective for many users to share a network such as the internet, which introduces an extra layer of complexity. This motivates the creation of quantum communication networks that can be shared by many users.

When assessing how difficult it is to realize a quantum cryptographic protocol in practice, it is important to examine all ingredients. First, we thus want to examine the requirements of the end nodes that are needed in order to realize a protocol. That is, we want to answer questions such as how many qubits the protocol participants need to manipulate at once? Does a protocol only require quantum measurements? Or, do we need to store qubits for some time in a quantum memory? Second, we need to be able to allow for quantum communication between the end nodes. This leads to a number of questions, including how far the protocol participants should be from each other. Whether a quantum cyptographic protocol is of interest in practice often depends on the allowed distance between the protocol participants. For example, secret communication using quantum cryptography is generally a lot more interesting if our protagonists Alice and Bob are at least in two separate buildings!

Due to the various different ingredients necessary to realize quantum cryptography in practice, progress in quantum communication technologies is often thought about along three axes (Figure 1.4). Each of these axes corresponds to one of the three ingredients above. Progress may be made independently along one of the axes: (1) accessibility, measures how available the technology is to users in terms of practical measures such as cost, reliability, and ease of use. When designing your own quantum cryptographic protocols to be put into industrial use, this criteria is evidently important to answer the question whether the benefits of using the protocol (presently) justify the costs for the users. The second criteria, (2) distance, measures the distance over which end-to-end quantum communication or entanglement generation can be performed. This is important for understanding how far protocol participants can be away from each other, and whether a quantum cryptographic protocol leads to an interesting use case for achievable distances. Finally, (3) functionality measures the capabilities of the end nodes, matched by the quantum communication channel connecting them. We already mentioned some of such capabilities above: for example, our protocol might ask to perform quantum measurements, or require storing information in a quantum memory, or maybe even ask for quantum operations on many qubits at once.

Trying to understand progress along such axes is evidently in general quite a complicated

endeavor, requiring us to consider many aspects, and indeed many parameters describing the properties of quantum hardware. Delving into the details of quantum hardware implementations certainly deserves a book on its own, and we thus focus here on one simplifying classification. This classification does however allow us get some initial insights into which types of protocols may be more easy to realize in practice. Specifically, functionality has been characterized by stages of development of a quantum network [WEH18]. Each subsequent stage is more difficult to build from the perspective of quantum hardware, but offers a higher level of functionality to the end user. Examples of existing quantum protocols may be classified into such stages of functionalities (Figure 1.5), which we briefly sketch here for completeness. To create a baseline, the stages of functionality of a quantum network include a trusted repeater stage. At this stage, no end-to-end quantum communication or cryptographic security is possible. Instead, the communication channel is chopped up into segments connected via a trusted repeater, often also called trusted node. Quantum cryptography may be used to secure communication on each segment, but interception at each trusted node on the segment is possible (in Chapter 8 we will figure out how to do this as an exercise!). The first true quantum network stage is the prepare-and-measure stage, where each end node may send a one qubit state to any other end node in such a way that the state is either measured, or the transmission is declared lost. In the entanglement network stage, end nodes are able to produce quantum entanglement between them, while the end nodes themselves remain simple devices capable of measuring only one qubit bit at a time. In the quantum network stage, end nodes are for the first time able to store and manipulate a small number of quantum bits, unlocking more advanced protocols. Higher stages demand significant advances in end nodes, achieving essentially noise free computation on at least a few quantum bits (Few qubit fault tolerant stage), and finally connecting end nodes that are large scale quantum computers (Quantum Computing stage). You can find examples of some protocols we will discuss later in this book in Figure 1.5. We would like to emphasize that is it unknown whether there does not exist a better analysis, or an altogether different protocol in order to solve the same tasks in a lower stages of functionality. We hope that by the end of this book, you are well on your way to both designing and analyzing your own quantum protocols to tackle this question!

1.8.2 State of the Art

So now that we gathered some background knowledge on quantum communication technologies, let us return to the pressing question: where are we at in putting quantum cryptography into practice? Can we already realize all the protocols presented in this book?

Let us examine such questions along the three axes above. At short distances, and limited functionality, quantum communication is already a commercial reality using relatively easy to use and reliable devices. Devices that realize quantum key distribution (QKD) for secure communication (see Chapter 8) over short distances are commercially available from many vendors around the globe (see e.g. [Quab, Quac, BV, Quaa]). Short presently refers to around 100km in deployed telecom fiber, where longer distances of several hundred kms have been realized in research labs (see e.g. [Lab]). These connections are generally point-to-point, and require a dedicated fiber connection between users. At present, many systems

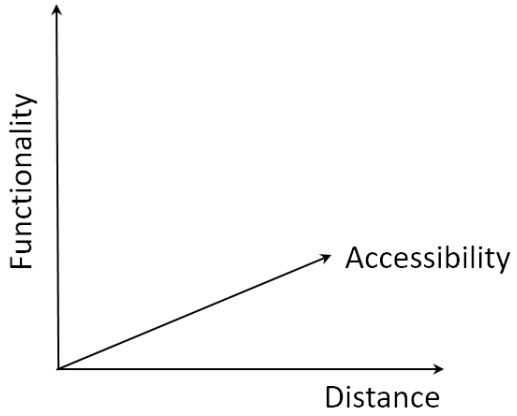

Fig. 1.4 Three axes along which one may measure progress in quantum communication technologies.

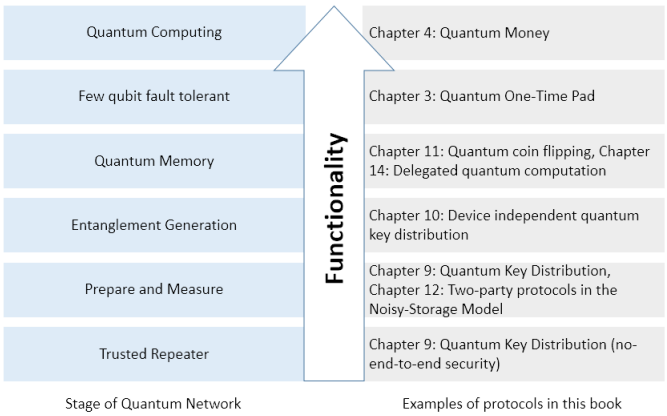

Fig. 1.5 Stages of Quantum Network Development. Each stage is more difficult to build, but allows access to a larger set of possible application protocols. Examples from this book can be found for all stages. We emphasize that it is generally unknown whether an advanced analysis, or an advanced protocol, would allow the realization of the same task in a lower stage. Indeed, it is quite possible some of the protocols mentioned in this book could be realized in a lower stage, provided one would extend their analysis to the case of noisy quantum devices. Quantum money could in principle also be of interest without a quantum communication network, but requires a long-lasting quantum memory to unlock its full potential.

require a dedicated dark fiber, that is, a fiber that is not used for any other communication at the same time. However, some systems can already share a fiber with conventional classical fiber communication. Recent years have seen implementations of a variant of QKD called MDI-QKD (see e.g. Figure 1.6) that we will explore in the Julia sheet accompany-

Fig. 1.6 Commercial MDI-QKD system by QBird. Several users are connected via one central hub. [Photo QBird B.V.]

ing Chapter 8. Here many users are connected to a central hub that can be used to perform QKD between any two users in a metropolitan area connected to it. In principle, one might imagine to later connect such hubs via long-distance backbones to realize a large quantum network connecting together many metropolitan networks.

How about longer distances? Long-distance quantum communication is a highly active area of research. You may be wondering why long distance quantum communication is actually difficult. After all, we have become quite advanced in terms of classical communication over world-wide distances. Qubits are generally transmitted using light, for example as photons over an optical fiber. It turns out, however, that the transmission of photons over fiber is highly lossy (in fact, exponential in the length of the fiber!). Fiber connections alone thus cannot help us transmit qubits over large distances. In the classical domain, one uses signal amplifiers along fibers in order to mitigate the loss of light in the fiber. Unfortunately – or maybe fortunately for cryptography! – we cannot use such amplifiers in the quantum domain, since they effectively create a copy of some of the quantum information we are trying to send. Moreover, as we saw above, it is impossible to make a copy of an arbitrary quantum bit. The fact that we cannot copy arbitrary qubits thus makes it quite challenging to send quantum information over long distances. However, it is also the very same feature of quantum communication that makes it so suitable for solving cryptographic tasks.

Broadly speaking, two complementary approaches exist in developing long-distance quantum communication in the future. While outside the scope of this book, we provide a number of references that allow you to start reading about such developments. One approach is to use (telecom) fibers in the ground. This necessitates the development of a quantum repeater that allows us to overcome the exponential loss in fiber. Such a quantum repeater would be inserted at specific intervals into the ground. Such a fiber based approach

would allow the connection of potentially many users via the existing telecom grid. Several possible repeater designs are envisioned and we refer to [MLK+16, SSdRG11] for some surveys introducing these fascinating ideas. At present, no quantum repeaters exist that can bridge significant distances, and only proof of principle experiments have been performed (see e.g. [LRGR+21, LTMR21, BRM+20]). Important for us here in this book is the fact that a quantum repeater would enable end-to-end quantum communication, and hence all the protocols in this book can in principle be realized with end-to-end security once such a device has been built. Right now, several networks exist that chain together short QKD links using a trusted node (see above). A trusted node, however, does not enable end-to-end quantum communication, and also no end-to-end security.

Another approach to bridging long-distances is to use quantum satellites. Proof of principle demonstrations have been performed, including generating quantum entanglement over more than 1200kms [YCL+17] (post-selected on successful detection events). Quantum satellites thus promise to bridge very long distances. Yet, they typically require large scale telescopes on the ground, which may make them less suitable for connecting very many users on the ground. Depending on the orbit of the satellite, quantum communication may also only be possible for a small part of the day. Quite conceivably, the two approaches may go hand-in-hand in the future: quantum satellites might be used to create very long-distance backbones for quantum communication, while fiber based communication may be used for medium scale distances to achieve high connectivity on the ground.

How about achieving higher stages of functionality? When considering protocols that ask for more than preparing and measuring single qubits, or producing entanglement between end nodes, we need to move to a higher stage of functionality in order to put them into practice. We again provide a very brief overview including some references to help you get started. Achieving higher stages not only requires an advancement of the quantum communication network connecting users, but crucially also the end nodes that the users use to run applications. Starting with the quantum memory stage, the end nodes are expected to have a quantum memory, and the ability to execute general quantum operations on the qubits. This enables them to execute protocols that require the protocol participants to store qubits for some period of time. From this stage onwards, end nodes are thus no longer simple photonic devices as presently used in QKD systems, but processing nodes. I.e., small quantum computers capable of manipulating qubits, not necessarily in a fault-tolerant manner as desired for general quantum computation. Small means that the processing nodes have only a small number of qubits, possibly not more than one or two. Crucial for the use of such processing nodes as end nodes is that they must posses an optical interface capable of connecting to a quantum network, and storage times that are long enough to allow for (classical) communication to be exchanged between the users while still retaining sufficient information inside the quantum memory. As with quantum repeaters, the development of such processing nodes is an active area of research and we refer to [WEH18] for an overview. As of now, the ability to link multiple processing nodes has been demonstrated by creating a three node quantum network [PHB+21] depicted in Figure 1.7.

As you can see, quantum communication is on the one hand already a commercial reality. On the other hand, much of it is still at the forefront of cutting edge quantum research.

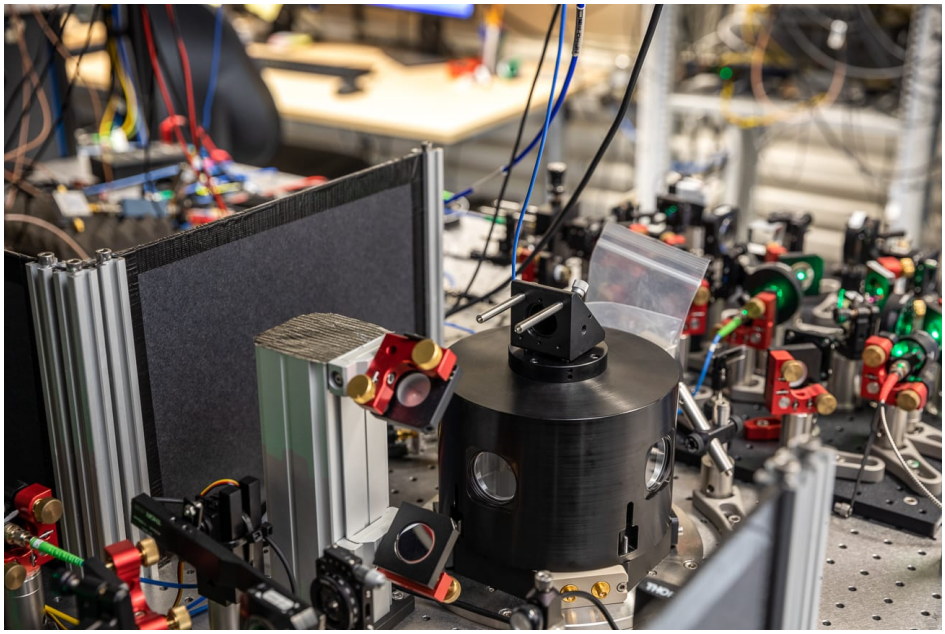

Fig. 1.7 Alice, one of the three nodes of the Delft processing node quantum network. Inside the black aluminum cylinder, the diamond sample is cooled to $-270°C$, to reduce the noise from the environment and enable the quantum control. [Hanson Lab, Photo Marieke de Lorijn for QuTech]

There is much to do, both in understanding existing quantum protocols, but also in exploring completely new quantum application protocols. We hope that this book will prepare you for contributing to this existing field of research.

1.9 Chapter notes

For for more extensive background than we provide here, we recommend the standard textbook on quantum information by Nielsen and Chuang [NC00]. Another classic, which also makes the connection with physical implementations, is [SW10]. For a far more extensive introduction to linear algebra, without reference to quantum information, we can recommend the book by Strand [SSSS93]. If you want to learn much more about quantum mechanics (far more than needed for this book), a standard textbook is by Griffiths [GS18]. For a more light-hearted introduction, focusing on the intuition, we recommend the small book by Susskind [SF14].

1.10 Cheat Sheet

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: $\mathcal{S} = \{|0\rangle, |1\rangle\}$ 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 hold:

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

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 $p_i = |\langle b_i|\psi\rangle|^2$. After the measurement, if a certain outcome "b_i" is observed, then the state $|\psi\rangle$ collapses to $|b_i\rangle$.

Pauli matrices

The Pauli matrices are 2×2 matrices,

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

and the following relations hold:

$$X|0\rangle = |1\rangle\,,\ X|1\rangle = |0\rangle \qquad X|+\rangle = |+\rangle\,,\ X|-\rangle = -|-\rangle$$
$$Z|0\rangle = |0\rangle\,,\ Z|1\rangle = -|1\rangle \qquad Z|+\rangle = |-\rangle\,,\ Z|-\rangle = |+\rangle$$
$$Y|0\rangle = i|1\rangle\,,\ Y|1\rangle = -i|0\rangle \qquad Y|+\rangle = -i|-\rangle\,,\ Y|-\rangle = i|+\rangle$$

1.11 Quiz solutions

Quiz 1.2.1 b)
Quiz 1.2.2 a)
Quiz 1.3.1 b)
Quiz 1.4.1 b)
Quiz 1.4.2 c)
Quiz 1.4.3 b)
Quiz 1.5.1 a)
Quiz 1.5.2 c)
Quiz 1.6.1 a)
Quiz 1.6.2 b)
Quiz 1.6.3 d)
Quiz 1.6.4 a)
Quiz 1.7.1 b)
Quiz 1.7.2 b)