Quantum Information
Lecture Notes

Quantum Information and Computation Group,
Institute for Integrated Circuits,
Johannes Kepler University Linz, Austria

Summer Term 2024

Johannes Kofler

Cite as:
Johannes Kofler, *Quantum Information Lecture Notes*, Johannes Kepler Universtiy Linz, 2024.

The cover page picture was generated with the Microsoft Designer Image Creator.

Contents

1. Introduction

1.1 What is Information?

We all have an intuitive understanding of the term *information*. It refers to the abstract concept that data is being obtained/received, memorized/stored, and transmitted/communicated. Information is *physical* in the sense that it is carried by physical objects or systems such as hard disks or electromagnetic waves, and that it is interpreted or used by physical entities such as computers or humans. Information is quantifiable in the sense that these physical objects can carry different amounts of information.

Information theory is the scientific field that studies storage, quantification, and communication of information. It dates back to the 1920s, and then in particular to Claude Shannon's seminal work "A Mathematical Theory of Commuication" from 1948, where (negative) *entropy* was established as a measure of uncertainty reduction by a message. We will of course discuss this important concept later in this lecture.

The invention of the transistor in 1947 is typically considered as the starting point of our *information age*. The corresponding rise of telecommunication, personal computers, and the internet has had an enormous socio-economic impact on our world and has completely transformed the way we live – how we communicate, learn and teach, work, and spend our free time.

1.2 What is Quantum Information?

Since *information is physical*, it needs to be carried by physical systems. In our everyday macroscopic world, nature is governed by the laws of *classical physics*, in particular classical mechanics and electromagnetism. The microscopic world of atoms and photons (the "particles" of light), however, is governed by physical laws which are radically different, namely by the laws of *quantum mechanics*.

Quantum mechanics is a theory of the beginning of the 20th century. Its mathematical formulation took place in the 1920s and early 1930s due to, among others, Werner Heisenberg and Erwin Schrödinger. The strange and counter-intuitive characteristics of quantum mechanics gave rise to fiercely contested debates within the community of physicists. While some problems regarding the interpretation (i.e. the understanding of the "meaning")

of certain quantum mechanical concepts still remain open until today, quantum physics has proven to be an extremely accurate and successful description of our natural world, and it has paved the way for many technological breakthroughs. This so-called *first quantum revolution* led to the atomic bomb, the transistor, the laser, magnetic resonance imaging, and many other developments.

Currently, we are entering the *second quantum revolution*, also known as the *quantum information age*. Here, quantum information – i.e. information carried by quantum systems such as atoms or photons – is harnessed to solve tasks which are impossible classically. Quantum computation and quantum cryptography are two such modern quantum information technologies. While the majority of funding may still be dominated by governmental funding, private investments have seen a stellar increase in the last decade (Figure 1.1).

This course provides and introduction to the field of Quantum Information – from its basic concepts and mathematical foundations to specific schemes and protocols.

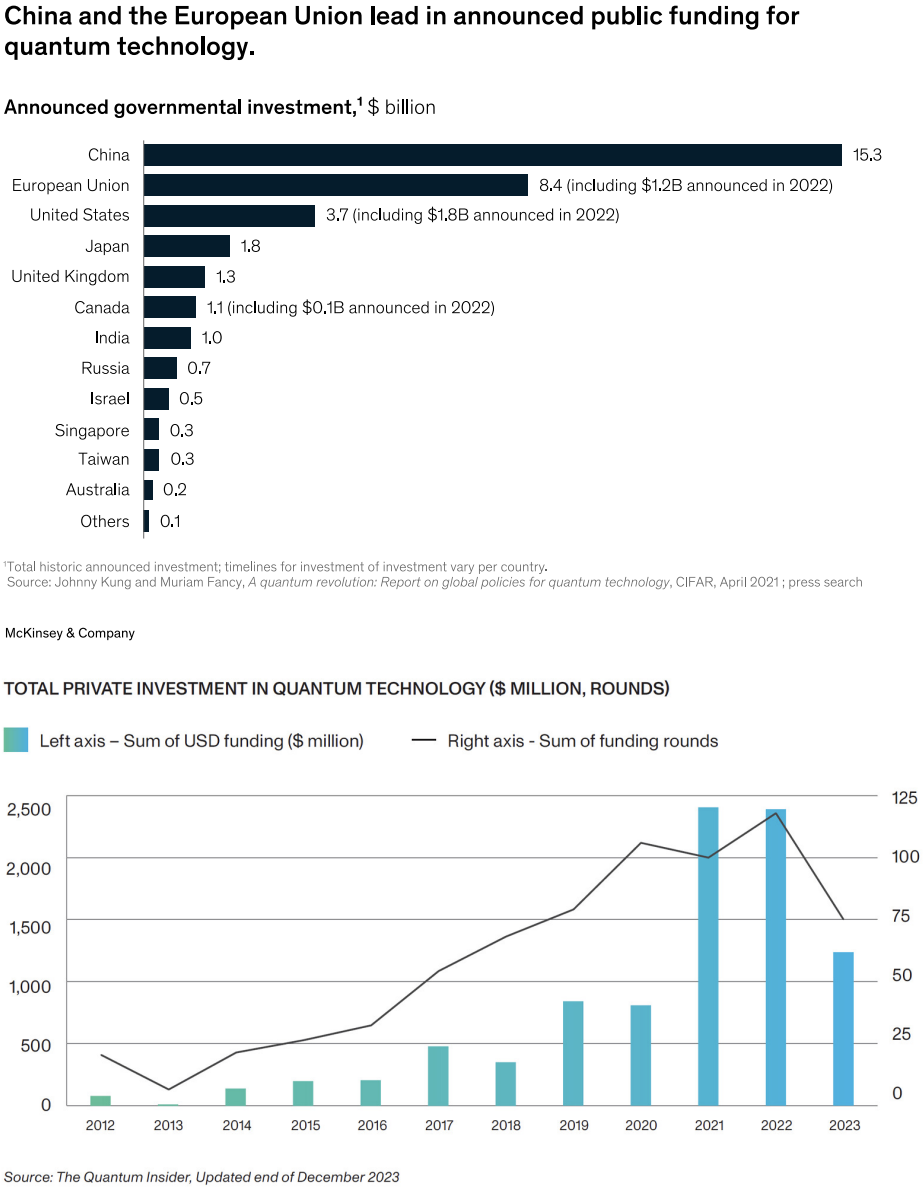

Figure 1.1: Top: Total historic announced public funding for quantum technologies as of May 2023. Bottom: Private investment history from 2012 to 2023 for quantum technologies.

2. Basic Concepts

2.1 Quantum States

2.1.1 From Bits to Qubits

The fundamental concept in classical information theory is the *bit*, which can take on only two possible values. As the allowed bit values (or bit states) b, we typically use 0 and 1:

$$b \in \{0, 1\}. \tag{2.1}$$

While all bits are eventually represented by physical systems, we can describe them as mathematical objects, i.e. integer numbers or Boolean (or logical or truth) values "false" and "true". A classical bit is a *discrete* mathematical object.

Similarly, the most important building block in quantum information is the *quantum bit*, or *qubit* for short. The qubit states $|0\rangle$ and $|1\rangle$ are two such specific states. They are called the *computational basis states*. The symbol $|.\rangle$ belongs to the Dirac notation and is called a *ket* (the last letters of the word "bracket").

The most important difference between classical bits and qubits is that the latter are not discrete but *continuous*. A qubit can be in *superposition* state of the two basis states $|0\rangle$ and $|1\rangle$. A superposition state $|\psi\rangle$ is a linear combination of the states $|0\rangle$ and $|1\rangle$. The most general form reads:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle. \tag{2.2}$$

Here, α and β are in general *complex* numbers with the normalization constraint

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.3}$$

These computational basis states $|0\rangle$ and $|1\rangle$ – and hence all states $|\psi\rangle$ which they span – are two-dimensional vectors. And since the coefficients α and β are complex numbers, $|\psi\rangle$ is a vector in a two-dimensional complex vector space. (Later, we will use scalar products of vectors, so this vector space is a Hilbert space.) This all may sound a bit complicated at first. We will see in a moment why complex numbers are important and why the kets are indeed vectors.

When a qubit in the state (2.2) is measured in the computational basis, then one obtains the result 0 with probability $|\alpha|^2$, and the result 1 with probability $|\beta|^2$. The total probability must be 1, which explains the normalization condition (2.3).

2.1.2 The Bloch Sphere

To get a better (geometrical) understanding of our qubit state, let us rewrite (2.2) in terms of two real parameters $\theta \in [0,\pi]$ and $\varphi \in [0,2\pi)$:

$$\alpha = \cos\tfrac{\theta}{2}, \tag{2.4}$$
$$\beta = e^{i\varphi}\sin\tfrac{\theta}{2}. \tag{2.5}$$

With the parametrization (2.4)-(2.5), our quantum state (2.2) reads:

$$|\psi(\theta,\varphi)\rangle = \cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle. \tag{2.6}$$

This obeys the normalization constraint (2.3) from above as $|\cos(\frac{\theta}{2})|^2 + |e^{i\varphi}\sin(\frac{\theta}{2})|^2 = 1$. But wait a second. At the start, we had two complex numbers α and β, each of which has a real and an imaginary part. Hence, we effectively had 4 real numbers: $\mathrm{Re}(\alpha)$, $\mathrm{Im}(\alpha)$, $\mathrm{Re}(\beta)$, and $\mathrm{Im}(\beta)$. And now we are down to two real values θ and φ. Did we lose generality now?

No, we did not. The normalization constraint (2.3) reduces our free parameters from 4 to 3. The cosine and sine prefactors, parametrized by only one angle θ, allow all valid "weightings" of the computational basis states, i.e. they can reach all values of $|\alpha^2|$ and $|\beta^2|$ under the normalization condition. Moreover, we do have a complex phase factor with the phase φ in front of the ket $|1\rangle$. But why no complex phase factor for the $|0\rangle$ state? If we had a state of the form $|\psi(\theta,\varphi)\rangle = e^{i\varphi_0}\cos\frac{\theta}{2}|0\rangle + e^{i\varphi_1}\sin\frac{\theta}{2}|1\rangle$, i.e. with two phase factors, we can rewrite this as: $|\psi(\theta,\varphi)\rangle = e^{i\varphi_0}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$ with $\varphi = \varphi_1 - \varphi_0$. The global phase φ_0 has is not observable effect until it becomes a relative phase (e.g. in an interference experiment) with respect to another qubit.

One can depict all possible qubit states as being on the surface of the so-called Bloch sphere (see Figure 2.1). Any point on this surface is parametrized by a polar angle θ and an azimuthal angle φ. The condition (2.3) ensures that all qubit states are normalized to length 1.

Let us look at some especially important states on the Bloch sphere, namely the basis states along the z, x, and y axis directions:

$$|\psi(0,0)\rangle = \quad |0\rangle \quad =: |z+\rangle, \tag{2.7}$$
$$|\psi(\pi,0)\rangle = \quad |1\rangle \quad =: |z-\rangle, \tag{2.8}$$
$$|\psi(\tfrac{\pi}{2},0)\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) =: |x+\rangle =: |+\rangle, \tag{2.9}$$
$$|\psi(\tfrac{\pi}{2},\pi)\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |x-\rangle =: |-\rangle, \tag{2.10}$$
$$|\psi(\tfrac{\pi}{2},\tfrac{\pi}{2})\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) =: |y+\rangle =: |R\rangle, \tag{2.11}$$
$$|\psi(\tfrac{\pi}{2},\tfrac{3\pi}{2})\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) =: |y-\rangle =: |L\rangle, \tag{2.12}$$

Our computational basis states $|0\rangle$ and $|1\rangle$ are on the north and south pole, respectively, i.e. in the $+z$ and $-z$ direction, respectively. With $\theta = \frac{\pi}{2}$, we are positioned on the equator. Then, with $\varphi = 0$ and $\varphi = \pi$, we point into the $+x$ and $-x$ direction, respectively. These

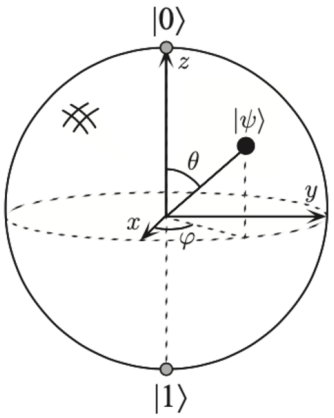

Figure 2.1: Graphical illustration of the Bloch sphere. The state of a single quantum bit lives on the surface of a sphere with radius 1. Any point on the Bloch sphere is parametrized by a polar angle θ and an azimuthal angle φ. Image taken from Ref. [19].

states are typically abbreviated with $|+\rangle$ and $|-\rangle$. Similarly, with $\varphi = \frac{\pi}{2}$ and $\varphi = \frac{3\pi}{2}$, we point into the $+y$ and $-y$ direction, respectively. These states are usually abbreviated with $|R\rangle$ and $|L\rangle$, where – in case you wondered – the notation refers to right and left circular polarised light. The 6 states listed above are the basis states of the z, x, and y basis respectively.

Exercise 2.1 Show that the computational (z) basis states $|0\rangle$ and $|1\rangle$ are equal-weight superpositions of the x-basis states $|+\rangle$ and $|-\rangle$. ∎

Solution:

$$\frac{|+\rangle+|-\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = |0\rangle, \tag{2.13}$$

$$\frac{|+\rangle-|-\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}} - \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = |1\rangle. \tag{2.14}$$

Whether a quantum state is a superposition state or not, depends on the *choice* of basis. What is a basis state in one basis, is a superposition state in another basis.

Exercise 2.2 Show that the computational (z) basis states $|0\rangle$ and $|1\rangle$ are equal-weight superpositions of the y-basis states $|R\rangle$ and $|L\rangle$. ∎

Solution: Very similar to the previous exercise.

Exercise 2.3 Write the state $|R\rangle$ in the x-basis. ∎

Solution: $|R\rangle = \frac{1+i}{2}|+\rangle + \frac{1-i}{2}|-\rangle$.

Exercise 2.4 Write down, approximately, the state $|\psi\rangle$ shown in Figure 2.1 in the z-basis. ∎

Solution: Try to estimate θ and φ and then use Eq. (2.6).

2.1.3 Information Amount in a Qubit

There are *infinitely* many points on the surface of the Bloch sphere. So, while there are only two possible states (0 and 1) for a classical bit, there are infinitely many possible states for a qubit. Can we therefore store an infinite amount of information into a single qubit? We certainly could fit the whole Wikipedia into the (bit representation of the) real numbers θ and φ.

Unfortunately, a single qubit cannot represent that amount of information directly. Any measurement of our qubit will only give one of two possible results. However, as we will see throughout this course, there is indeed some "hidden" information in these continuous variables θ and φ which is of central importance for the advantages of quantum information processing compared to its classical counterpart.

2.1.4 Physical Realizations of Qubits

There are many physical realizations of qubits. One very prominent example are photons, the quanta of light. For a single photon, its polarization state is a qubit. The computational basis states $|0\rangle$ and $|1\rangle$ are the *horizontal* and *vertical* polarization states $|H\rangle$ and $|V\rangle$. A general polarisation state is an arbitrary superposition of horizontal and vertical polarization and can thus be written as

$$|\psi_{\text{photon}}\rangle = \alpha\,|H\rangle + \beta\,|V\rangle. \tag{2.15}$$

The $|+\rangle/|-\rangle$ basis corresponds to diagonally polarised light in the $+45\,^\circ$-plane. This is why this basis (the x-basis) is also called the *diagonal basis*. A measurement in the diagonal basis is implemented by putting a polarizer oriented at $+45\,^\circ$. The $|R\rangle/|L\rangle$ basis corresponds to (right and left) circular polarization states.

Another example is the spin of an electron. The basis states are spin up $|\uparrow\rangle$ along the z-axis and spin down $|\downarrow\rangle$ along the z-axis. In general, the electron spin can be in an arbitrary superposition state:

$$|\psi_{\text{electron}}\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle. \tag{2.16}$$

If the electron is, e.g., prepared with spin along $+x$ direction, its state is $|+\rangle = |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$.

Another example is the electronic state of an atom. For simplicity, let us imagine the hydrogen atom which has only one electron. And let us only consider the ground state $|g\rangle$ and the first excited electronic state $|e\rangle$, while ignoring all higher excitations. You may think of an experiment, where, e.g., a laser can stimulate transitions between the ground and excited state but no transition to any higher energy states. Then the electronic energy state of this atom is a two-level quantum system, i.e. a qubit. In general, it can be in an arbitrary superposition of the ground and the first excited state:

$$|\psi_{\text{atom}}\rangle = \alpha\,|g\rangle + \beta\,|e\rangle. \tag{2.17}$$

There are many more physical realizations of qubits such as trapped ions, quantum dots, nuclear spins, superconducting qubits, etc.

While enormous efforts have been made in the last decades to push the quantum nature of matter to the macroscopic regime, we have not (yet?) reached the realm of biological systems. In 1935, the Austrian physicist Erwin Schrödinger put forward a famous thought

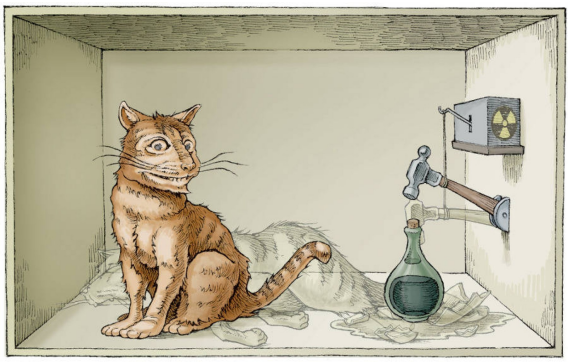

Figure 2.2: Illustration of Schrödinger's famous thought experiment. Picture taken from Ref. [14].

experiment, where a cat is positioned in a sealed chamber. A radioactive atom may or not decay – these two possibilities exist in a quantum superposition. If a decay happens, a Geiger counter will detect it and release a hammer which destroys a flask with poison, killing the cat. After a suitable time, within which there is a 50 % chance that a decay happened and a 50 % chance that no decay took place, the cat will be in an equal-weight superposition of "dead" and "alive":

$$|\psi_{\text{cat}}\rangle = \frac{1}{\sqrt{2}}\left(|\text{dead}\rangle + |\text{alive}\rangle\right). \tag{2.18}$$

Whether it is possible to create such states, is an open scientific question. Quantum mechanics in principle allows it. But the more massive the objects become, the stronger the tension with the general theory of relativity.

2.2 Quantum Measurements

2.2.1 The Born Rule

A fundamental postulate for measurements in quantum mechanics is the *Born rule*. It says that the probability of finding a system in a certain state it given by the squared modulus of the (complex) amplitude of the system in that state. Let us look at a simple example by revisiting the qubit state (2.2):

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle. \tag{2.19}$$

We ask ourselves: What is the probability that, given a measurement in the computational basis, we get the result 0?

We first have to build the scalar product between state $|0\rangle$ (i.e. the outcome state in question) and the input state (2.19) itself. Mathematically, this is done by multiplying the covector of the ket $|0\rangle$, i.e. the *bra* $\langle 0|$ with the vector $|\psi\rangle$. The *bra-ket* is the scalar product:

$$\begin{aligned}\langle 0|\psi\rangle &= \langle 0|\left(\alpha\,|0\rangle + \beta\,|1\rangle\right)\\ &= \alpha\,\langle 0|0\rangle + \beta\,\langle 0|1\rangle.\end{aligned} \tag{2.20}$$

For the last equation, we have used linearity of the scalar product.

Now, it is time to introduce the vector notation for our computational basis states. After all, qubits states live in a two-dimensional (i.e. there exist two computational basis states) vector space. By convention, we use the first dimension of the vector space for $|0\rangle$ and the second dimension for $|1\rangle$:

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.21}$$

The corresponding covectors are

$$\langle 0| \equiv (1 \;\; 0), \quad \langle 1| \equiv (0 \;\; 1). \tag{2.22}$$

This helps us to see the orthonormality of the basis states:

$$\langle 0|0\rangle = (1 \;\; 0) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \cdot 1 + 0 \cdot 0 = 1, \tag{2.23}$$

$$\langle 0|1\rangle = (1 \;\; 0) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1 \cdot 0 + 0 \cdot 1 = 0, \tag{2.24}$$

$$\langle 1|0\rangle = (0 \;\; 1) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0 \cdot 1 + 1 \cdot 0 = 0, \tag{2.25}$$

$$\langle 1|1\rangle = (0 \;\; 1) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \cdot 0 + 1 \cdot 1 = 1. \tag{2.26}$$

This means: The scalar product of any basis vector with itself is 1. And the scalar product between two different basis vectors is 0.

We can continue the scalar product from above and find

$$\langle 0|\psi\rangle = \alpha \langle 0|0\rangle + \beta \langle 0|1\rangle = \alpha. \tag{2.27}$$

This (complex) value is the *probability amplitude*. The probability itself is given by the modulus squared (Born rule) of this amplitude. Hence, the answer to our question from above – what is the chance to obtain outcome 0 in the state $|\psi\rangle$ – is given by

$$P(0|\psi) = |\langle 0|\psi\rangle|^2 = |\alpha|^2. \tag{2.28}$$

Similarly, the probability for outcome 1 reads

$$P(1|\psi) = |\langle 1|\psi\rangle|^2 = |\beta|^2. \tag{2.29}$$

Exercise 2.5 Compute the probability for outcome 0 for a measurement in the computational basis for all 6 basis states (2.8)-(2.12). ∎

Solution:

$$\begin{aligned}
P(0|0) &= |\langle 0|0\rangle|^2 = |1|^2 = 1, \\
P(0|1) &= |\langle 0|1\rangle|^2 = |0|^2 = 0, \\
P(0|+) &= |\langle 0|+\rangle|^2 = |\langle 0|\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}|^2 = \tfrac{1}{2}, \\
P(0|-) &= |\langle 0|-\rangle|^2 = |\langle 0|\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}(\langle 0|0\rangle - \langle 0|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}|^2 = \tfrac{1}{2},
\end{aligned} \tag{2.30}$$

$$P(0|R) = |\langle 0|R\rangle|^2 = |\langle 0|\tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}(\langle 0|0\rangle + i\langle 0|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}|^2 = \tfrac{1}{2},$$
$$P(0|L) = |\langle 0|L\rangle|^2 = |\langle 0|\tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}(\langle 0|0\rangle - i\langle 0|1\rangle)|^2 = |\tfrac{1}{\sqrt{2}}|^2 = \tfrac{1}{2}.$$

The probabilty for outcome 1 is always the complement: $P(1|.) = 1 - P(0|.)$, as the two outcome probabilities need to sum to 1. While the state $|0\rangle$ is identical to itself (i.e. the scalar product is 1, see first equation above) and while it is orthogonal to the state $|1\rangle$ (i.e. the scalar product is 0, see second equation above), it has a *partial overlap* of size $1/\sqrt{2}$ with the other 4 basis states. The probability to measure outcome 0 in these 4 basis states is $\frac{1}{2}$.

It is important to note that states are orthogonal (i.e. have scalar product 0) if they are at *opposite* points on the Bloch sphere, and not rotated by 90 degrees. In other words, while the x, y, and z directions on the Bloch sphere are orthogonal in our three-dimensional space, they do *not* correspond to orthogonal quantum states in the vector space. The three most prominent cases of orthogonal state pairs are the basis states themselves:

$$\langle 0|1\rangle = 0, \tag{2.31}$$
$$\begin{aligned}\langle +|-\rangle &= \left[\tfrac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\right]\left[\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \\ &= \tfrac{1}{2}\left(\langle 0|0\rangle + \langle 1|0\rangle + \langle 0|1\rangle - \langle 1|1\rangle\right) = \tfrac{1}{2}(1+0+0-1) = 0,\end{aligned} \tag{2.32}$$
$$\begin{aligned}\langle R|L\rangle &= \left[\tfrac{1}{\sqrt{2}}(\langle 0| - i\langle 1|)\right]\left[\tfrac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\right] \\ &= \tfrac{1}{2}\left(\langle 0|0\rangle - i\langle 1|0\rangle - i\langle 0|1\rangle + i^2\langle 1|1\rangle\right) = \tfrac{1}{2}(1+0+0-1) = 0.\end{aligned} \tag{2.33}$$

Here, we had to be careful with the bra $\langle R|$ as we need to complex conjugate all amplitudes. More formally, the bra is the conjugate transpose (also called: Hermitian transpose) of the corresponding ket. For an arbitrary state (2.19), we can write:

$$\langle \psi| = |\psi\rangle^\dagger = (\alpha|0\rangle + \beta|1\rangle)^\dagger = \bar{\alpha}\langle 0| + \bar{\beta}\langle 1|, \tag{2.34}$$

where $\bar{\alpha}$ and $\bar{\beta}$ are the complex conjugates of α and β, respectively. The Hermitian transpose symbol is called "dagger". Applying the Hermitian transpose again, brings back the original state:

$$(|\psi\rangle^\dagger)^\dagger = \langle\psi|^\dagger = |\psi\rangle. \tag{2.35}$$

Exercise 2.6 Compute the Hermitian transpose of the state $|R\rangle$ in both the Dirac and the vector notation. ■

Solution:

$$|R\rangle^\dagger = \left[\tfrac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)\right]^\dagger = \tfrac{1}{\sqrt{2}}(\langle 0| - i\langle 1|), \tag{2.36}$$
$$|R\rangle^\dagger = \left[\tfrac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix} + i\begin{pmatrix}0\\1\end{pmatrix}\right)\right]^\dagger = \left[\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}\right]^\dagger = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & -i\end{pmatrix}. \tag{2.37}$$

2.2.2 Post-Measurement States

A fundamental property of quantum mechanics is that, in general, a measurement changes – often we say: *collapses* – the state. This is distinctly different from the classical case, where you can measure a classical bit as often as you like without any change.

Let us once again use our general qubit state (2.19) and let us measure it in the computational basis $|0\rangle/|1\rangle$. Then, we can symbolically write:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \begin{array}{l} \xrightarrow[|0\rangle/|1\rangle]{P=|\alpha|^2} |0\rangle \\ \xrightarrow[|0\rangle/|1\rangle]{P=|\beta|^2} |1\rangle \end{array} \tag{2.38}$$

Below each arrow, we write the measurement basis. Above the arrow, we write the outcome probability. With probability $|\alpha|^2$, we will obtain result 0. If that outcome occurs, the quantum system becomes *projected* into state $|0\rangle$ and all further measurements in the computational basis will give result 0 with probability 1. If, however, outcome 1 occurs in the first measurement, which happens with probability $|\beta|^2$, then the quantum system will be projected into the state $|1\rangle$.

This "active" role of measurements is very important. And it also already forecasts a fundamental experimental challenge when working with quantum bits. They are fragile in the sense that any unwanted measurement can alter the qubit state. One needs to shield and protect them from their environment.

From (2.38), we can see that we can alter the state by measurements. This implies that we can – merely by measurements – bring a qubit into its orthogonal state. Let's start with a qubit in state $|0\rangle$. Any measurement in the computational basis has probability 0 to obtain outcome 1 (i.e. end up in state $|1\rangle$). We can write $P(1|0) = 0$ also like this:

$$|0\rangle \xrightarrow[|0\rangle/|1\rangle]{P=0} |1\rangle. \tag{2.39}$$

But what if we first measure in the $|+\rangle/|-\rangle$ basis? In such a $|+\rangle/|-\rangle$ measurement, starting from state $|0\rangle$, the probability to obtain state $|+\rangle$ or $|-\rangle$, is given by

$$P(+|0) = |\langle +|0\rangle|^2 = \tfrac{1}{2}, \tag{2.40}$$

$$P(-|0) = |\langle -|0\rangle|^2 = \tfrac{1}{2}. \tag{2.41}$$

Compare this to Exercise 2.5, where we computed "the other way round", but the probability is the same: $P(+|0) = P(0|+)$. And once we are in one of these states, if we then measure again in the $|0\rangle/|1\rangle$ computational basis, how large is the probability that we obtain result 1? We can calculate

$$P(1|+) = |\langle 1|+\rangle|^2 = \tfrac{1}{2}, \tag{2.42}$$

$$P(1|-) = |\langle 1|-\rangle|^2 = \tfrac{1}{2}. \tag{2.43}$$

We can summarize this as follows:

$$|0\rangle \begin{array}{lll} \xrightarrow[|+\rangle/|-\rangle]{P=1/2} & |+\rangle & \xrightarrow[|0\rangle/|1\rangle]{P=1/2} |1\rangle \\ \xrightarrow[|+\rangle/|-\rangle]{P=1/2} & |-\rangle & \xrightarrow[|0\rangle/|1\rangle]{P=1/2} |1\rangle \end{array} \tag{2.44}$$

Hence, with this "intermediate measurment" procedure, there is a 50 % chance that we will obtain result 1:

$$|0\rangle \xrightarrow[\text{interm. meas.}]{P=1/2} |1\rangle. \tag{2.45}$$

Compare this to (2.39).

Exercise 2.7 Quantum state dragging: Starting in state $|0\rangle$, let us make a measurement in the $|u_1\rangle/|v_1\rangle$ basis with basis states $|u_1\rangle = \cos\frac{\varepsilon}{2}|0\rangle + \sin\frac{\varepsilon}{2}|1\rangle$, $|v_1\rangle = -\sin\frac{\varepsilon}{2}|0\rangle + \cos\frac{\varepsilon}{2}|1\rangle$. Show that this is indeed a basis by calculating $\langle u_1|v_1\rangle$. Here, ε is a number much smaller than 1. Compute the probability P_ε to find the starting state $|0\rangle$ in the state $|u_1\rangle$. If we indeed find $|u_1\rangle$ (and not $|v_1\rangle$), let us call that a "success". Then we define a new basis, rotated by another angle ε, i.e. $|u_2\rangle = \cos\frac{2\varepsilon}{2}|0\rangle + \sin\frac{2\varepsilon}{2}|1\rangle$, $|v_2\rangle = -\sin\frac{2\varepsilon}{2}|0\rangle + \cos\frac{2\varepsilon}{2}|1\rangle$. Show that the transition ("success") probability from $|u_1\rangle$ to $|u_2\rangle$ is the same as it was in the first step from $|0\rangle$ to $|u_1\rangle$. (You can use the trigonometric identity: $\cos\varepsilon\cos\frac{\varepsilon}{2} + \sin\varepsilon\sin\frac{\varepsilon}{2} = \cos\frac{\varepsilon}{2}$.) This process can now be continued again and again. Show that after $N = \frac{\pi}{\varepsilon}$ such steps, we will reach $|u_N\rangle = |1\rangle$. The probability that we succeed at *every* step is the product of all individual success probabilities: $P_{\text{total}} = P_\varepsilon^N$. Compute P_{total} in the limit of very small ε. ∎

Solution: Blackboard or homework. The result is remarkable, namely $\lim_{N\to\infty} P_{\text{total}} = 1$. In the limit of many measurements with very small rotations, we can "drag" the state from $|0\rangle$ to its orthogonal state $|1\rangle$ with certainty.

2.3 Quantum State Transformations

2.3.1 Unitary Operations

In the previous section, we discussed quantum state changes via measurements. This type of (non-linear) state change only works probabilistically. There is also a "deterministic" way to (linearly) transform a quantum state $|\psi\rangle$ into another state $|\psi'\rangle$. This is done via a unitary operation U:

$$|\psi'\rangle = U|\psi\rangle. \tag{2.46}$$

Unitary operators are exactly those operators whose Hermitian transpose is equal to the inverse:

$$U^\dagger = U^{-1}. \tag{2.47}$$

This implies that U preserves the inner product: Let us take two quantum states $|\psi\rangle$ and $|\phi\rangle$ and apply U to both states, i.e. $|\psi'\rangle = U|\psi\rangle$ and $|\phi'\rangle = U|\phi\rangle$. Then the inner product of the transformed states reads:

$$\langle\psi'|\phi'\rangle = \langle\psi|U^\dagger U|\phi\rangle = \langle\psi|\phi\rangle. \tag{2.48}$$

Here, we used $\langle\psi'| = |\psi'\rangle^\dagger = (U|\psi\rangle)^\dagger = \langle\psi|U^\dagger$ and $U^\dagger U = U^{-1}U = \mathbb{1}$, where $\mathbb{1}$ is the identity operator.

Equation (2.48) is very important. Take $|\phi\rangle = |\psi\rangle$. Then we can see that $\langle\psi'|\psi'\rangle = \langle\psi|\psi\rangle$. Since $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is a normalized state with $|\alpha|^2 + |\beta|^2 = 1$ (i.e. $\langle\psi|\psi\rangle = 1$), also $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ must be normalized with $|\alpha'|^2 + |\beta'|^2 = 1$ (i.e. $\langle\psi'|\psi'\rangle = 1$). Unitary transformations preserve state normalization, and they are, in general, the only operations which have this property.

We remark that in quantum mechanics $U = \exp(-iHt/\hbar)$ is the time-evolution operator, with H the Hamiltonian (i.e. energy operator the system), t the time, and $\hbar$ the reduced Planck constant. All unitary transformations are *continuous* processes that need a certain time to be implemented.

2.3.2 Quantum Gates

From the quantum information perspective, in particular from the perspective of computer science, we may think of unitary transformations as *quantum gates*.

Classically, there is only one non-trivial gate for a single bit, namely the NOT gate. It takes a bit as input value and outputs its negation, i.e. $0 \to 1$ and $1 \to 0$. Analytically, given a bit $b \in \{0,1\}$:

$$\mathrm{NOT}(b) = 1 - b. \tag{2.49}$$

How does a quantum analogue of the NOT gate look like? The *quantum NOT gate* is called the Pauli X gate and, in matrix notation, it has the form

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.50}$$

Taking an arbitrary input state

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{2.51}$$

the X gate acts as follows:

$$X\,|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta\,|0\rangle + \alpha\,|1\rangle. \tag{2.52}$$

So it indeed switches the amplitudes in front of the basis states. In particular, $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. The X gate is therefore often called the *bit-flip gate*. (There is also a Pauli Y and a Pauli Z gate. We will come across them later.)

Exercise 2.8 Compute the action of the X gate on the states $|+\rangle$ and $|-\rangle$. ∎

Solution:

$$X\,|+\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle, \tag{2.53}$$

$$X\,|-\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = -|-\rangle. \tag{2.54}$$

In words: The states (vectors) $|+\rangle$ and $|-\rangle$ are eigenstates (eigenvectors) of the operator (matrix) X. The eigenvalues are $+1$ and -1, respectively.

Another important single-qubit operation is the *Hadamard gate*:

$$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.55}$$

When acting on computational basis states, it creates the diagonal basis states:

$$H\,|0\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle, \tag{2.56}$$

$$H\,|1\rangle = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle. \tag{2.57}$$

Exercise 2.9 Apply the Hadamard gate onto the state $|+\rangle$. ∎

Solution: $H|+\rangle = |0\rangle$. In fact, $H^2 = \mathbb{1}$.

All unitary transformations on single qubits can be decomposed into 3 subsequent rotations (about suitable angles around the z-y-z axes) of the state vector moving it along the surface of the Bloch sphere and a global phase factor $e^{i\alpha}$:

$$U(\alpha,\beta,E,\delta) = e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos\frac{E}{2} & -\sin\frac{E}{2} \\ \sin\frac{E}{2} & \cos\frac{E}{2} \end{pmatrix}\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}. \quad (2.58)$$

Exercise 2.10 Show that the Hadamard gate is realized by the unitary (2.58) using $\alpha = \frac{\pi}{2}$, $\beta = 0$, $E = \frac{\pi}{2}$, and $\delta = \pi$. ∎

Solution: Blackboard or homework.

We note again: All gates must be physically implemented (via a Hamiltonian) and are therefore continuous (in time) transformations, not "jumps" from an input state to an output state.

2.3.3 The Measurement Problem

Unitary transformations U have the following properties:

- Deterministic: The final state $U|\psi\rangle$ is reached with certainty.
- Invertible: We can undo a unitary transformation U by applying the transformation $U^\dagger$. Since $U^\dagger U = \mathbb{1}$, we get $U^\dagger U|\psi\rangle = \mathbb{1}|\psi\rangle = |\psi\rangle$.
- Continuous: Every unitary transformation (in physics) is the result of a continuous dynamical process through time.

Note the fundamental difference to quantum measurements, which are:

- Probabilistic: Quantum mechanics only specifies outcome probabilities. Measurement results are in general random.
- Irreversible: The post-measurement state contains less information than the state before measurement. In general, you can't go back. Measurements cannot be undone.
- Discontinuous: The collapse of the state vector is (mathematically) treated as a discontinuous and instantaneous process.

These two processes – unitary evolution on one side and measurement on the other – are *fundamentally incompatible*. They are mathematically contradictory. This is at the heart of the so-called *measurement problem* of quantum mechanics: Under which circumstances should we use the continuous (Schrödinger) time evolution and unitary transformations, and when are we supposed to apply the discontinuous effect of measurement? If all physical processes are governed by the Schrödinger equation and if all measurements are eventually physical processes, why are they incompatible?

Don't worry if you can't answer these questions. No one can! They are debated since almost 100 years without a generally satisfying solution.

The measurement problem is closely linked to the problem of the different interpretations of quantum mechanics. There are radically different views about the "meaning" of the quantum state and about the nature of reality, such as the Copenhagen interpretation, the many-worlds interpretation, and Bohmian mechanics.

2.3.4 Notation Summary

Let us briefly summarize the most important mathematical concepts of this chapter:

Notation	Description
$\|\psi\rangle$	State vector (or ket).
$\langle\psi\|$	Covector (or bra) of the vector $\|\psi\rangle$.
$\bar{z} = a - ib$	Complex conjugate of complex number $z = a + ib$.
$\langle\phi\|\psi\rangle$	Scalar product between the states $\|\phi\rangle$ and $\|\psi\rangle$.
A^T	Transpose of the matrix A, rows and columns are exchanged.
$\bar{A}$	Conjugate matrix of A, all entries are complex conjugated.
$A^\dagger$	Hermitian transpose (or conjugate transpose) of the matrix A, $A^\dagger = \bar{A}^T$.
U	Unitary matrix, $U^\dagger = U^{-1}$.

3. Single-Qubit Quantum Experiments

3.1 The Double-Slit Experiment

In the 17th century, Isaac Newton put forward the hypothesis that light consists of particles. Later, the wave nature of light was shown, in particular by Thomas Young's 1801 famous double-slit interference experiment. In this experiment, it was demonstrated that the pattern observed after a double slit is *not* simply the sum of two one-slit patterns. In particular, in the two-slit pattern shows *interference fringes*, i.e. there are minima (where no light hits the screen) at locations where light would be detected behind an individual slit.

In 1905, Albert Einstein suggested that light consists of "energy packets" or quanta to explain the photoelectric effect. This – yet again – particle nature, together with the wave-like behaviour in interference experiments, has established the so called *wave-particle duality*. Light consists of quanta in the sense that on a detection screen individual detection events ("clicks") occur. Also, light is a wave in the sense that it the emerging pattern shows interference fringes (see Figures 3.1 and 3.2).

The wave picture and the particle picture are both mental constructs that help in an intuitive understanding of the observed phenomena. But ultimately, photons are neither particles nor waves but are described by quantum mechanics. The photonic wavefunction (i.e. an infinitely-dimensional state vector that assigns a complex number to each point in our real 3-dimensional space) obeys the Schrödinger equation. It propagates through both slits *simultaneously* and can then interfere with itself. This gives rise to an interference pattern. While the (complex-valued) wavefunction is not a real wave but rather a mathematical object, its modulus squared amplitude at every point in space corresponds to probability to detect a photon.

What if we put an apparatus in one of the two slits, say the left one. The apparatus is built such that it contains a detector and photon source. If the apparatus detects a photon, it emits a new photon in the same direction the old would have travelled. Surely, this will not change anything, right? Well, it does! The measurement destroys the superposition character of the photon's state at the screen

$$\psi_{\text{photon}} = \frac{1}{\sqrt{2}} \left(|\text{left}\rangle + |\text{right}\rangle \right) \tag{3.1}$$

and collapses it into either $|\text{left}\rangle$ (when the apparatus detected and re-emitted a photon)

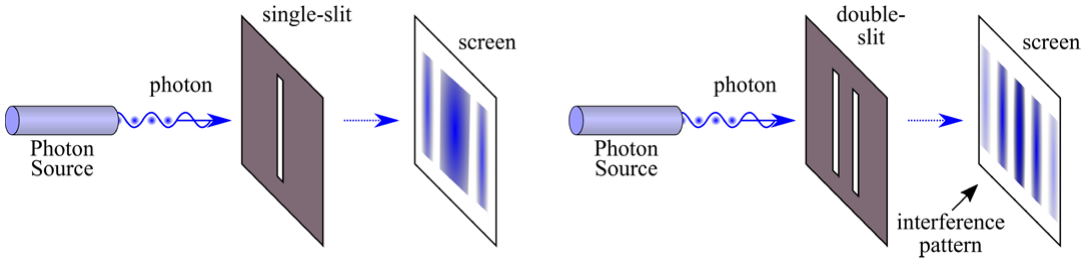

Figure 3.1: Left: If photons are sent through a single slit and then detected at a screen, an interference pattern with a main maximum and side maxima of smaller intensity will emerge. Right: The double slit experiment. Picture adapted from Ref. [18].

Figure 3.2: Experimental results of a single-slit (left) and double-slit (right) experiment. Picture taken from Wikipedia, then color inverted.

or $|\text{right}\rangle$ (when the apparatus did not detect a photon). The resulting pattern on the screen over many repetitions will be the "boring" sum of two one-particle pattern without interference fringes.

In fact, any (partial or full) *information leakage* about the photon's path will (partially or fully) destroy the interference pattern. It need not be via measurements. It could also be via interaction with the environment. This process is called *decoherence*. And it is the main reason why it is so hard to experimentally realize superpositions of macroscopic objects. The tiniest interaction with surrounding atoms or photons decoheres a Schrödinger cat within (a tiny fraction of) the blink of en eye.

3.2 The Elitzur-Vaidman Bomb

Is it possible to ascertain the existence of an object in a given region of space without interacting with it? That would be particularly useful for, e.g., "detecting" – without destruction – a bomb which would detonate already under the tiniest form of interaction, say with a single photon. Classically, this task is impossible to accomplish. In 1993, Elitzur and Vaidman put forward a quantum solution to the problem. The heart of it is a Mach-Zehnder interferometer (see Figure 3.3).

We have a source which emits a single photon in the path 0, i.e. we can write its quantum state as $|0\rangle$, with 0 denoting the path. The photon hits a 50-50 beam splitter (BS_1) which makes a unitary transformation that creates an equal-weight superposition of the photon traveling in path 1 and 2, where every reflection produces a phase factor i:

$$|0\rangle \xrightarrow{\text{BS}_1} \frac{|1\rangle+i|2\rangle}{\sqrt{2}}. \tag{3.2}$$

In each path, there is a mirror. Each mirror (reflection) produces a phase factor i:

$$\frac{|1\rangle+i|2\rangle}{\sqrt{2}} \xrightarrow{\text{mirrors}} \frac{i|3\rangle-|4\rangle}{\sqrt{2}}. \tag{3.3}$$

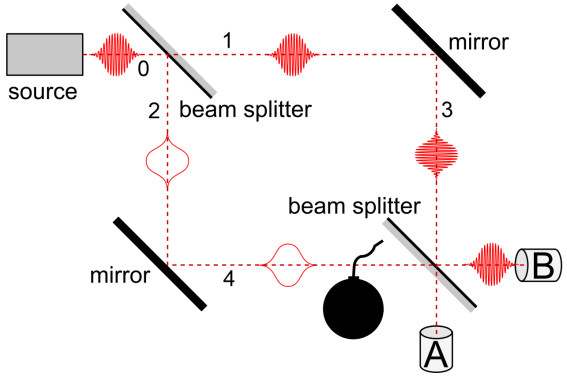

Figure 3.3: A Mach-Zehnder interferometer, potentially with a bomb in one of its arms. Image taken from Wikipedia and adapted (added path numbers).

Assuming that there is no bomb in path 4, the photon states will "meet" again on the second beam splitter BS_2. It acts in the same way as BS_1, i.e. it creates a superposition of the outgoing paths and puts a phase factor i on the reflected one. This will transform our quantum state as follows:

$$\frac{i|3\rangle - |4\rangle}{\sqrt{2}} \xrightarrow{\mathrm{BS}_2} \frac{1}{\sqrt{2}}\left[i\frac{|\mathrm{A}\rangle + i|\mathrm{B}\rangle}{\sqrt{2}} - \frac{|\mathrm{B}\rangle + i|\mathrm{A}\rangle}{\sqrt{2}}\right] = -|\mathrm{B}\rangle. \tag{3.4}$$

The final phase factor -1 is not important. All photons will travel to the detector in path B. We say that there is a completely constructive interference in path B, and a completely destructive interference in path A.

But what if there is an extremely sensitive bomb in path 4 which explodes upon impact of a single photon? The bomb acts as measurement device. With probability $1/2$, the bomb will detect the photon and explode, as the amplitude for the state $|4\rangle$ in the right hand side in (3.3) is $1/\sqrt{2}$. With probability $1/2$, the bomb does not explode. Since the bomb is a perfect measurement device, its non-explosion collapses the state into state $|3\rangle$. Then, BS_2 creates an equal-weight superposition of paths A and B. Hence, overall we have:

- Probability $\frac{1}{2}$: The bomb explodes. We now know that is existed. Well, bad luck.
- Probability $\frac{1}{4}$: Photon detection in detector B. This is the same result as in the case above, when there is no bomb. Thus, we cannot deduce whether or not there is a bomb in path 4.
- Probability $\frac{1}{4}$: Photon detection in path A. This outcome is only possible, if there is a bomb in path 4. Hence, we have determined the existence of the bomb without destroying it.

Elitzur and Vaidman then extended this scheme to build a bomb tester that can distinguish between live bombs and duds. We will not elaborate this further here. In any case, the above analysis shows how *information* about an object can be obtained in a quantum setup, which is impossible to achieve in classical physics.

4. Multi-Qubit States

4.1 Product States

Until this point, we only discussed one-qubit states. Now, we would like to go to an arbitrary number of qubits.

Let's start with two qubits, denoted by A and B, in the arbitrary states

$$|\psi\rangle_A = \alpha\,|0\rangle_A + \beta\,|1\rangle_A = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{4.1}$$

$$|\phi\rangle_B = \gamma|0\rangle_B + \delta\,|1\rangle_B = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}. \tag{4.2}$$

The *product state* of these two-qubits is the four-dimensional *tensor product*

$$\begin{aligned} |\Psi\rangle_{AB} &= |\psi\rangle_A \otimes |\phi\rangle_B = (\alpha\,|0\rangle_A + \beta\,|1\rangle_A) \otimes (E\,|0\rangle_B + \delta\,|1\rangle_B) \\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{pmatrix} \\ &= \alpha\gamma|0\rangle_A \otimes |0\rangle_B + \alpha\delta\,|0\rangle_A \otimes |1\rangle_B + \beta\gamma|1\rangle_A \otimes |0\rangle_B + \beta\delta\,|1\rangle_A \otimes |1\rangle_B. \end{aligned} \tag{4.3}$$

We have used "full" notation here. Typically, one writes the final state concisely as

$$|\Psi\rangle = \alpha\gamma|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma|10\rangle + \beta\delta\,|11\rangle. \tag{4.4}$$

For the sake of completeness, let us write down the four computational basis states of the four-dimensional two-qubit space:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{4.5}$$

These 4 states form an orthonormal basis.

If both qubits are measured in the computational basis, then the probabilities for the results 00, 01, 10, and 11 are given by $|\alpha\gamma|^2$, $|\alpha\delta|^2$, $|\beta\gamma|^2$, $|\beta\delta|^2$, respectively. These are simple products, e.g., the probability to measure both qubits in state 0 is the probability to measure the first qubit in state 0 (which is $|\alpha|^2$) times the probability to measure the second qubit in state 0 (which is $|\gamma|^2$): $P(00) = |\alpha|^2|\gamma|^2 = |\alpha\gamma|^2$.

Exercise 4.1 Show that state (4.3) is normalized. ∎

Proof: Using the fact that the single qubit states are normalized, we can compute

$$\begin{aligned} |\alpha\gamma|^2 + |\alpha\delta|^2 + |\beta\gamma|^2 + |\beta\delta|^2 &= |\alpha|^2|\gamma|^2 + |\alpha|^2|\delta|^2 + |\beta|^2|\gamma|^2 + |\beta|^2|\delta|^2 \\ &= |\alpha|^2(|\gamma|^2 + |\delta|^2) + |\beta|^2(|\gamma|^2 + |\delta|^2) \\ &= |\alpha|^2 + |\beta|^2 = 1. \end{aligned} \tag{4.6}$$

Analogously to the case of two qubits, the product state of three qubits A, B, and C, which are in states $|\psi\rangle_A$, $|\phi\rangle_B$, and $|\chi\rangle_C$, respectively, is the 8-dimensional tensor product of three one-qubit states:

$$|\Psi\rangle_{ABC} = |\psi\rangle_A \otimes |\phi\rangle_B \otimes |\chi\rangle_C. \tag{4.7}$$

Unfortunately, there is no Bloch sphere representation anymore for quantum states with more than one qubit.

4.2 Entanglement

The state (4.3) is not the most general two-qubit state. We have chosen the two quantum bits being "separated" in the sense that each qubit had its own state. Then, their joint state is simply the product state. This exactly what we are used to from our classical world. To describe the state of two systems, you simply describe both systems individually.

However, the most general two-qubit state has the form

$$|\Psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{4.8}$$

where $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. So what is the difference to (4.4)? Well, in (4.8) the parameters a, b, c, and d are (except for the normalization) "free". But in the state (4.4), there are very special relations. Hence, (4.4) is a special instance of (4.8), using $a = \alpha\gamma$, $b = \alpha\delta$, $c = \beta\gamma$, and $d = \beta\delta$

Consider this state:

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}. \tag{4.9}$$

It obviously obeys the normalization condition. However, the system of equations

$$\alpha\gamma = a = \tfrac{1}{\sqrt{2}}, \quad \alpha\delta = b = 0, \tag{4.10}$$

$$\beta\gamma = c = 0, \qquad \beta\delta = d = \tfrac{1}{\sqrt{2}}, \tag{4.11}$$

does not have a solution. To see this, multiply the first and the last equation. That gives: $\alpha\gamma\beta\delta = \frac{1}{2}$. Then, multiply the second and the third: $\alpha\delta\beta\gamma = 0$. That is a contradiction. Thus, the state (4.9) cannot be written as a tensor product of two *individual* quantum states. We call such a state *entangled*.

More formally, a state is entangled if and only if it *cannot* be written in the form of a product state (4.3). For two qubits A and B:

$$|\Psi\rangle_{\text{ent}} \neq |\psi\rangle_A \otimes |\phi\rangle_B. \tag{4.12}$$

Entanglement is the phenomenon when two or more quantum systems are correlated in such a (non-classical) way that even a perfect and complete description of all individual systems does not fully specify their joint state. And vice versa, knowing everything about their joint state, does not imply maximal knowledge about the individual constituents. When two or more systems are in an entangled state, they – in some sense – cannot be thought of as individual systems anymore, even if they are separated in space. This is, in fact, what Erwin Schrödinger called the "essence of quantum physics". There is no classical analogon for entanglement, i.e. there is no way how in our everyday world around us classical objects would have such a characteristic.

As we will see later, entangled states can give rise to correlations (of measurement results) whose "strength" cannot be achieved by any classical process. Moreover, entanglement is a necessary resource for many quantum information technologies such as quantum computing and entanglement-based quantum cryptography.

A very important set of entangled states are the so-called Bell states, one of which we have seen already above. Let us introduce all four of them now:

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) = \tfrac{|00\rangle+|11\rangle}{\sqrt{2}}, \tag{4.13}$$

$$|\Phi^-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) = \tfrac{|00\rangle-|11\rangle}{\sqrt{2}}, \tag{4.14}$$

$$|\Psi^+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) = \tfrac{|01\rangle+|10\rangle}{\sqrt{2}}, \tag{4.15}$$

$$|\Psi^-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) = \tfrac{|01\rangle-|10\rangle}{\sqrt{2}}. \tag{4.16}$$

There are many experimental ways to realize Bell states. One is spontaneous parametric down conversion (see Figure 4.1), which creates a Bell state in the polarisation of two photons, such as the so called singlet state

$$|\Psi^-\rangle = \tfrac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle). \tag{4.17}$$

Measuring the two photons in the computational H/V basis will always lead to anti-correlated outcomes: either the first photon is horizontally polarised and the second is vertically polarised, or the first photon is vertically polarized and the second one is horizontally polarised.

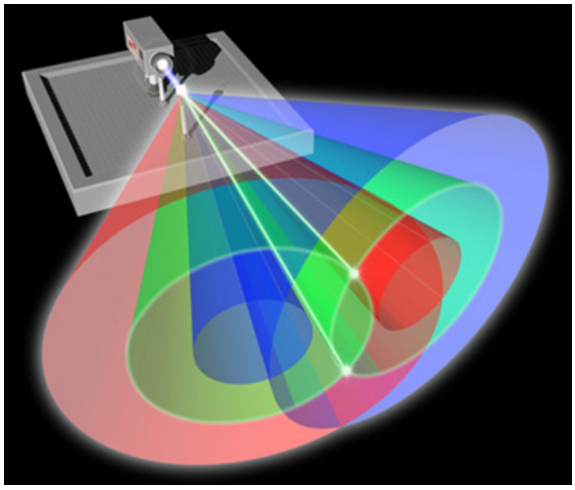

Figure 4.1: Spontaneous parametric down conversion. A laser shines light on a non-linear crystal. Individual photons can decay into a pair of two photons which exit along cones of different opening angles and colors (photon frequencies). All photons on the left cones are horizontally polarised. All photons on the right cones are vertically polarized. If a pair of photons has the same color (green) and is selected along the cone intersection (drawn in white), they become *indistinguishable*. This leads to a polarisation entangled Bell state of the form (4.17). Picture taken from Ref. [9].

A prominent entangled state of three qubits is the so-called Greenberger-Horne-Zeilinger (GHZ) state, which lives in an $(2^3 = 8)$-dimensional complex vector space:

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \tag{4.18}$$

Exercise 4.2 Show that the 4 Bell states (4.13)-(4.16) form an orthonormal basis of 2-qubit states. ∎

Solution: Blackboard or homework.

4.3 Post-Measurement States

Assume we are given the general two-qubit state

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle) + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{4.19}$$

Let us perform a measurement in the computational basis. The (complex-valued) probability amplitude for an outcome is the scalar product of the bra-vector of the outcome state with the state $|\Psi\rangle$. For the four possible outcomes 00, 01, 10, and 11, we get

$$\langle 00|\Psi\rangle = \langle 00|\left(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle\right) = \alpha_{00}, \tag{4.20}$$
$$\langle 01|\Psi\rangle = \langle 01|\left(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle\right) = \alpha_{01}, \tag{4.21}$$
$$\langle 10|\Psi\rangle = \langle 10|\left(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle\right) = \alpha_{10}, \tag{4.22}$$
$$\langle 11|\Psi\rangle = \langle 11|\left(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle\right) = \alpha_{11}. \tag{4.23}$$

Here, we have used the orthonormality conditions: $\langle ij|i'j'\rangle = 1$ only if $i = i'$ and $j = j'$. Otherwise, it is 0. Have a look at (4.5) again.

We can also choose to measure only one qubit. Say, we measure only the second qubit B and are interested in the probability amplitude to observe result 1:

$$\begin{aligned}\langle 1|_B|\Psi\rangle &= \langle 1|_B\left[\alpha_{00}\,|0\rangle_A|0\rangle_B + \alpha_{01}\,|0\rangle_A|0\rangle_B + \alpha_{10}\,|0\rangle_A|1\rangle_B + \alpha_{11}\,|1\rangle_A|1\rangle_B\right] \\ &= \alpha_{01}\,|0\rangle_A + \alpha_{11}\,|1\rangle_A. \end{aligned} \tag{4.24}$$

The result is now not a scalar, but a state vector for qubit A. The probability to indeed observe this outcome 1 for qubit B is $|\alpha_{01}|^2 + |\alpha_{11}|^2$ which is in general smaller than 1. We have to divide (4.24) by the square root of this probability to get the correctly normalized post-measurement state of qubit A:

$$|\psi\rangle_A = \frac{\alpha_{01}|0\rangle_A + \alpha_{11}|1\rangle_A}{\sqrt{|\alpha_{01}|^2 + |\alpha_{11}|^2}}. \tag{4.25}$$

Exercise 4.3 Given the GHZ state $(|000\rangle_{ABC} + |111\rangle_{ABC})/\sqrt{2}$, perform a measurement on the third qubit, i.e. C, in the diagonal basis. What are the two possible post-measurement states (depending on C's outcomes $+$ and $-$, respectively) of the first two qubits A and B? ■

Solution: Blackboard or homework.

4.4 Multi-Qubit Gates

Two-qubit gates are unitary 4×4 matrices. A prominent example is the controlled NOT gate, called CNOT (see Figure 4.2):

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{4.26}$$

If the first qubit (the control) is in state $|0\rangle$, it leaves the second qubit (the target) unchanged. If the control is in state $|1\rangle$, a NOT operation on the target is performed. The first qubit remains unchanged in any case. In the computational basis with $a, b \in 0, 1$ and with $\oplus$ denoting the XOR operation, we can write:

$$|a,b\rangle \xrightarrow{\text{CNOT}} |a, a \oplus b\rangle, \tag{4.27}$$

$$\text{CNOT}\,[a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle] = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle. \tag{4.28}$$

Let us compute one case explicitly, namely for the initial state $|11\rangle$:

$$\text{CNOT}\,|11\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle. \tag{4.29}$$

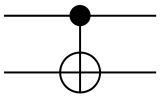

Figure 4.2: Each horizontal line represents a qubit. The CNOT gate consists of a control (black dot) and and a target (the cross).

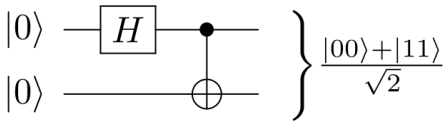

Figure 4.3: An entangling circuit: A Hadamard followed by a CNOT.

While classical computer circuits are composed of wires and logic gates, *quantum circuits* are composed of wires and quantum gates. We are now in the position to create a simple but powerful quantum circuit, i.e. a sequence of quantum gates (unitary transformations) acting on a known initialization (see Figure 4.3).

Let us initialize our input qubits as $|00\rangle = |0\rangle_A|0\rangle_B$. First, we apply the Hadamard gate H on the first qubit. Since no action is performed on the second qubit, we apply the 2×2 identity matrix $\mathbb{1}_2 = \mathrm{diag}(1,1)$ on it. The total operation is the tensor product:

$$\begin{aligned}(H\otimes\mathbb{1}_2)|00\rangle_{AB} &= H|0\rangle_A\otimes\mathbb{1}_2|0\rangle_B = |+\rangle|0\rangle_{AB}\\ &= \tfrac{1}{\sqrt{2}}(|0\rangle_A+|1\rangle_A)|0\rangle_B = \tfrac{1}{\sqrt{2}}(|00\rangle_{AB}+|10\rangle_{AB}).\end{aligned} \tag{4.30}$$

This is still a product state. Next, we apply the CNOT gate (and omit qubit labels):

$$\mathrm{CNOT}\,\tfrac{1}{\sqrt{2}}(|00\rangle+|10\rangle) = \tfrac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{4.31}$$

You hopefully immediately recognize the $|\Phi^+\rangle$ Bell state. Our circuit created entanglement out of an initially non-entangled product state.

There are, of course, also gates that act on more than 2 qubits. However, it is always possible to decompose any given N-qubit gate into a sequence of 2-qubit gates.

Designing quantum circuits for useful applications is the field of *quantum computation*. The most famous quantum algorithm is Shor's algorithm that allows to find prime factors of integers exponentially faster than the best known classical algorithm, which makes it an existential threat to RSA cryptography. We refer to the winter semester lecture "Quantum Computing".

5. Quantum Information Protocols

5.1 No-Cloning

Typically, it is a rather trivial feature of classical bits that they can be copied. We can simply read out the bit and obtain its value, and then create a second bit with the same value as the first. In quantum mechanics, the situation is much trickier.

We are given a qubit in an unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i.e. we do not know the amplitudes α and β, and we would like to create another qubit in the same state. If we measure our unknown qubit, we will collapse it into the basis of our choice. That will tell us, in general, very little about α and β. E.g. if we measure in the computational basis and get result 1, then we know that β cannot be 0 and that *probably, but not certainly* $|\beta| > |\alpha|$. But we don't know much more than that. And since we had only this one qubit and since this is now in the collapsed state, we are out of luck. Any future measurement will act on the collapsed state. There is no more information to be gained from the original state. Game over.

If we had (infinitely) many copies of our unknown qubit, then we could indeed measure repeatedly and along multiple bases and find the unknown amplitudes. But in the task at hand, we are given only one copy the state. Hence, the measurement approach does not work.

Alternatively, let us try to construct a unitary transformation which acts as a copy machine. We are seeking a unitary evolution U which, given any unknown input state $|\psi\rangle$ and some "standard blank state" $|s\rangle$, can copy the unknown state onto the blank state (see Figure 5.1):

$$|\psi\rangle|s\rangle \xrightarrow{U} U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle. \tag{5.1}$$

That transformation should work for arbitrary input states. Let us denote by $|\phi\rangle$ another state to be copied. And let us put qubit labels A (the unknown qubit) and B (the initally blank qubit)

$$U(|\psi\rangle_A|s\rangle_B) = |\psi\rangle_A|\psi\rangle_B, \tag{5.2}$$
$$U(|\phi\rangle_A|s\rangle_B) = |\phi\rangle_A|\phi\rangle_B. \tag{5.3}$$

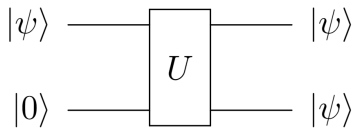

Figure 5.1: A unitary transformation U which can clone or copy any arbitrary input state $|\psi\rangle$ onto a standard blank input state $|s\rangle$, e.g. the $|0\rangle$ state. Does such a transformation exit?

Now we take the scalar products of the left hand sides and the right hand sides: We multiply the conjugate transpose of the left hand side of the first equation with the left hand side of the second equation. And we multiply the conjugate transpose of the right hand side of the first equation with the right hand side of the second equation

$$\langle\psi|_A\langle s|_B U^\dagger U\,|\phi\rangle_A|s\rangle_B = \langle\psi|_A\langle\psi|_B|\phi\rangle_A|\phi\rangle_B. \tag{5.4}$$

Since U is unitary (i.e. $U^\dagger U = \mathbb{1}$) and since the blank state is properly normalized (i.e. $\langle s|s\rangle = 1$) we obtain

$$\langle\psi|_A|\phi\rangle_A = \langle\psi|_A|\phi\rangle_A\,\langle\psi|_B|\phi\rangle_B. \tag{5.5}$$

These are all numbers, and we can write more concisely:

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2. \tag{5.6}$$

But this last equation holds only in very special cases, namely when $|\psi\rangle$ and $|\phi\rangle$ are the same (then $1 = 1$) or when they are orthogonal (then $0 = 0$). For all other unknown input states with $\langle\psi|\phi\rangle \notin \{0,1\}$, we have reached a *contradiction*.

The only way to resolve this contradiction is to conclude that the universal quantum cloning machine U from Equation (5.1) does not exist. This is the *no-cloning theorem* due to Wootters and Zurek [15]: It is impossible to perfectly copy an unknown quantum state using using a unitary transformation.

5.2 Superdense Coding

In communication protocols, two or more parties transmit information to each other via some physical process. In the following, let us consider only two parties named Alice and Bob.

A natural question that we can ask ourselves is: How much information – measured in terms of classical bits – can Alice communicate to Bob by sending N qubits? The answer is: At most N bits.

Assume that Bob knows nothing about the incoming qubits, i.e. in particular Alice has not told him in which basis he should measure them. For example, Alice may have chosen the $|+\rangle/|-\rangle$ basis to encode information. She prepares a $|+\rangle$ state to encode bit 0 and state $|-\rangle$ to encode 1. If Bob measures the incoming N qubits in the $|+\rangle/|-\rangle$ basis, he will completely retrieve the information Alice has sent him. If, however, he measures, for instance, in the computational basis, he will have complete randomness for his outcomes. His outcome sequence of N bits will contain no information about Alice's message whatsoever.

Superdense coding (also simply called dense coding) is a *quantum communication protocol* in which transmitting N qubits allows to communicate *more than* N bits of information – given the two parties share entangled states. It was proposed by Bennett and Wiesner in 1970 and later published in 1992 [3]. Let us go through the protocol:

Step 1: Entanglement sharing. The Bell state

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \tag{5.7}$$

is created by a third party named Charlie and *shared* between Alice and Bob, i.e. qubit A is sent to Alice's laboratory and qubit B is sent to Bob's laboratory. (Alternatively, Alice could create the Bell state, send one qubit to Bob, and keep one qubit for herself.)

Step 2: Encoding. Alice would like to send a 2-bit string $a_1a_2 \in \{00,01,10,11\}$ to Bob. If she wants to send 00, then she leaves her qubit untouched, i.e. she applies the identity operation $\mathbb{1}_A$. The joint quantum state will not change:

$$00: \quad |\Phi^+\rangle \xrightarrow{\mathbb{1}_A} |\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right). \tag{5.8}$$

We have not explicitly written (and also subsequently will not write) Bob's action above the arrow, which is always an identity operation $\mathbb{1}_B$ on his qubit, as he waits passively in his lab and does nothing in the encoding step.

In case Alice wants to transmit the string 01, she applies the Pauli X (or quantum NOT) gate $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ onto her qubit, which will cause a bit flip. The total quantum state will transform into yet another Bell state, namely $|\Psi^+\rangle$:

$$01: \quad |\Phi^+\rangle \xrightarrow{X_A} |\Psi^+\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right). \tag{5.9}$$

If Alice wants to send the string 10, then she applies the Pauli Z (or phase flip) gate $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. This will put a -1 factor in front of Alice's $|1\rangle$ state and transform the 2-qubit quantum state into a different Bell state, namely $|\Phi^-\rangle$:

$$10: \quad |\Phi^+\rangle \xrightarrow{Z_A} |\Phi^-\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right). \tag{5.10}$$

If she wants to transmit 11, she first applies X and then Z. This will first create a bit flip and then put a factor -1 on her $|1\rangle$ state. This can also be written as $ZX = iY = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, where Y is the Pauli Y gate. This transformation will lead to the last Bell state $|\Psi^-\rangle$:

$$11: \quad |\Phi^+\rangle \xrightarrow{Z_A X_A} |\Psi^-\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right). \tag{5.11}$$

In summary, Alice can encode one of the 4 possible 2-bit strings $a_1a_2 \in \{00,01,10,11\}$ by choosing one out of 4 different transformations $Z_A^{a_1}X_A^{a_2}$ which each creates one of the 4 possible Bell states.

Step 3: Transmission. This step is conceptually simple – Alice sends her qubit to Bob. Experimentally, this requires a quantum channel. A photon, e.g., may be sent in a glass fiber or through free space via telescopes. Other physical qubit realizations require their own techniques.

Step 4: Decoding. The last step in the dense coding protocol is for Bob, who is now in possession of both qubits, to perform a measurement in the Bell basis. Since the Bell states form an orthonormal basis, he can distinguish the 4 possible states with certainty. How can he do this?

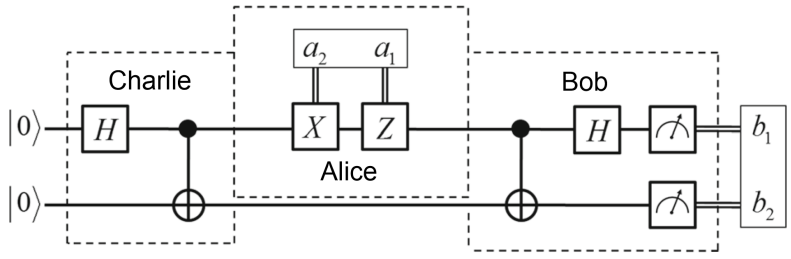

Figure 5.2: Dense coding: Charlie prepares a $|\Phi^+\rangle$ Bell state for Alice and Bob. Alice encodes a 2-bit message a_1a_2 into her qubit by applying $Z_A^{a_1}X_A^{a_2}$. After Bob receives Alice's qubit, he can decode the message with a sequence of a CNOT and a Hadamard gate and measurement in the computational basis. This allows Alice to transmit 2 bits by only sending 1 qubit. Picture adapted from Ref. [16].

Bob first applies a CNOT operation with A as control and B as target. Let's do this for all four possible states:

$$\text{CNOT}\,|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B + |1\rangle_A|0\rangle_B), \tag{5.12}$$

$$\text{CNOT}\,|\Psi^+\rangle = \tfrac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B + |1\rangle_A|1\rangle_B), \tag{5.13}$$

$$\text{CNOT}\,|\Phi^-\rangle = \tfrac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B - |1\rangle_A|0\rangle_B), \tag{5.14}$$

$$\text{CNOT}\,|\Psi^-\rangle = \tfrac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B - |1\rangle_A|1\rangle_B). \tag{5.15}$$

Then, Bob applies the operation $H_A \otimes \mathbb{1}_B$, i.e. the Hadamard transformation on qubit A and the identity on qubit B. Recall that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$, see (2.56) and (2.57). Again, let's do this for all four options from above:

$$\begin{aligned}(H_A \otimes \mathbb{1}_B)\,\tfrac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B + |1\rangle_A|0\rangle_B) &= \tfrac{1}{\sqrt{2}}\,(|+\rangle_A|0\rangle_B + |-\rangle_A|0\rangle_B) \\ &= \tfrac{1}{2}\,[(|0\rangle_A + |1\rangle_A)|0\rangle_B + (|0\rangle_A - |1\rangle_A)|0\rangle_B] = |0\rangle_A|0\rangle_B, \end{aligned} \tag{5.16}$$

$$\begin{aligned}(H_A \otimes \mathbb{1}_B)\,\tfrac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B + |1\rangle_A|1\rangle_B) &= \tfrac{1}{\sqrt{2}}\,(|+\rangle_A|1\rangle_B + |-\rangle_A|1\rangle_B) \\ &= \tfrac{1}{2}\,[(|0\rangle_A + |1\rangle_A)|1\rangle_B + (|0\rangle_A - |1\rangle_A)|1\rangle_B] = |0\rangle_A|1\rangle_B, \end{aligned} \tag{5.17}$$

$$\begin{aligned}(H_A \otimes \mathbb{1}_B)\,\tfrac{1}{\sqrt{2}}\,(|0\rangle_A|0\rangle_B - |1\rangle_A|0\rangle_B) &= \tfrac{1}{\sqrt{2}}\,(|+\rangle_A|0\rangle_B - |-\rangle_A|0\rangle_B) \\ &= \tfrac{1}{2}\,[(|0\rangle_A + |1\rangle_A)|0\rangle_B - (|0\rangle_A - |1\rangle_A)|0\rangle_B] = |1\rangle_A|0\rangle_B, \end{aligned} \tag{5.18}$$

$$\begin{aligned}(H_A \otimes \mathbb{1}_B)\,\tfrac{1}{\sqrt{2}}\,(|0\rangle_A|1\rangle_B - |1\rangle_A|1\rangle_B) &= \tfrac{1}{\sqrt{2}}\,(|+\rangle_A|1\rangle_B - |-\rangle_A|1\rangle_B) \\ &= \tfrac{1}{2}\,[(|0\rangle_A + |1\rangle_A)|1\rangle_B - (|0\rangle_A - |1\rangle_A)|1\rangle_B] = |1\rangle_A|1\rangle_B. \end{aligned} \tag{5.19}$$

After these operations, Bob can measure both qubits in the computational basis. As outcomes, Bob will exactly obtain the 2-bit string that Alice has encoded earlier: $b_1b_2 = a_1a_2$. The dense coding scheme is depicted in Figure 5.2. Note that Alice's and Bob's laboratories can be arbitrarily widely separated in space.

In summary, superdense coding teaches us one of Bennett's laws of information. Let's denote the resource of a shared entangled state as 1 ebit (short for "entanglement bit"). Note that 1 ebit involves 2 qubits. This 1 ebit together with 1 bit of (classical) communication allows to communicate 2 bits of information:

$$1\text{ ebit} + 1\text{ bit} \geq 2\text{ bits}. \tag{5.20}$$

Here, where $\geq$ means "can do the job of".

Superdense coding is a secure form of communication. A potential eavesdropper, typically named Eve, who may intercept the qubit which Alice sends to Bob would be unable to decode the message. Without access to Bob's B qubit, the intercepted qubit A does not contain any information at all and will give random results (in all measurement bases). In a later chapter about mixed states, we will learn the technique to prove this statement.

5.3 Quantum Teleportation

Teleportation is usually a term we know from Science Fiction. Many of you may think about "beaming" in Star Trek. (Legend has it that the transporter in Star Trek was only invented because the landing scenes of shuttles would have been too expensive.) In teleportation, some material object, e.g. a human, disappears in one place and appears almost instantaneously at a remote location.

Quantum teleportation is a scheme where Alice is provided with an unknown quantum bit which should be "reconstructed" at Bob's remote location. No physical object – in particular not the qubit itself – but only (classical) information is transmitted. Quantum teleportation was proposed in 1993 [2] and experimentally realized for the first time in 1997 [4].

Assume for a moment that Alice would somehow know the quantum state that needs to be teleported to Bob. (Either she prepared the state herself. Or she was provided with (infinitely) many copies which allowed her to precisely determine the amplitudes, which are complex numbers in a continuous space.) Then she would have to transmit an (infinitely) large amount of classical information to Bob such that he can prepare the qubit state. Remarkably, quantum teleportation works

(i) with only one copy at Alice's side of the unknown quantum state to be teleported,
(ii) without Alice ever knowing the amplitudes of this state, and
(iii) with transmission of only 2 bits of classical information from Alice to Bob.

The prerequisite for this "magic" is that Alice and Bob initially share a Bell state (also called an EPR pair). Figure 5.3 schematically illustrates the setup.

Let's go through the protocol step by step: First, just like in dense coding, Alice and Bob share an entangled Bell state. Any of the four Bell states will work, so let us take – without loss of generality, the $|\Phi^+\rangle$ state:

$$|\Phi^+\rangle_{AB} = \tfrac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{5.21}$$

Qubit A is in Alice's laboratory, and qubit B is in Bob's. Alice is now provided with another qubit C in an arbitrary (and unknown) state to be teleported:

$$|\psi\rangle_C = \alpha\,|0\rangle_C + \beta\,|1\rangle_C. \tag{5.22}$$

The total 3-qubit state reads:

$$|\psi\rangle_C|\Phi+\rangle_{AB} = (\alpha\,|0\rangle_C + \beta\,|1\rangle_C)\,\tfrac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{5.23}$$

The crucial step of the protocol is that Alice now measures her two qubits A and C in the Bell basis. Such a measurement effectively projects her two qubits – which had nothing to do with each other unitl now – into an entangled sate.

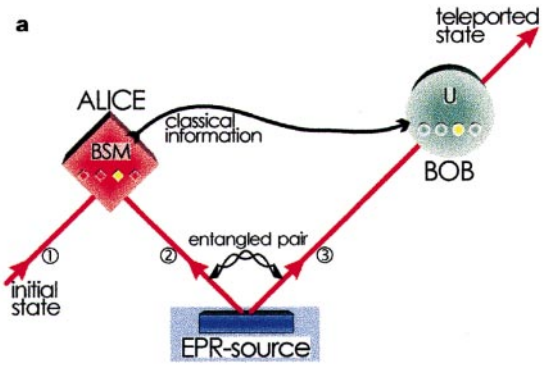

Figure 5.3: Quantum teleportation scheme. An Einstein-Podolsky-Rosen (EPR) source creates a Bell pair which is shared between Alice and Bob. An arbitrary initial state is sent to Alice. In a Bell state measurement (BSM), she measures that input state jointly with her entangled qubit. The measurement result – corresponding to one of the four possible Bell states, i.e. 2 bits of information – is transmitted to Bob, who uses this classical information to perform a simple transformation on his qubit which restores the initial state. Picture taken from the article of the first experimental demonstration [4].

We need to rewrite our state (5.23) such that Alice's two-qubit computational basis states $|00\rangle_{AC}$, $|01\rangle_{AC}$, $|10\rangle_{AC}$, and $|11\rangle_{AC}$ are expressed in the Bell basis. This can be done with the help of the following superpositions of Bell states:

$$\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{CA}+|\Phi^-\rangle_{CA}\right)=\frac{1}{2}\left(|00\rangle_{CA}+|11\rangle_{CA}+|00\rangle_{CA}-|11\rangle_{CA}\right)=|00\rangle_{CA}, \quad (5.24)$$

$$\frac{1}{\sqrt{2}}\left(|\Psi^+\rangle_{CA}+|\Psi^-\rangle_{CA}\right)=\frac{1}{2}\left(|01\rangle_{CA}+|10\rangle_{CA}+|01\rangle_{CA}-|10\rangle_{CA}\right)=|01\rangle_{CA}, \quad (5.25)$$

$$\frac{1}{\sqrt{2}}\left(|\Psi^+\rangle_{CA}-|\Psi^-\rangle_{CA}\right)=\frac{1}{2}\left(|01\rangle_{CA}+|10\rangle_{CA}-|01\rangle_{CA}+|10\rangle_{CA}\right)=|10\rangle_{CA}, \quad (5.26)$$

$$\frac{1}{\sqrt{2}}\left(|\Phi^+\rangle_{CA}-|\Phi^-\rangle_{CA}\right)=\frac{1}{2}\left(|00\rangle_{CA}+|11\rangle_{CA}-|00\rangle_{CA}+|11\rangle_{CA}\right)=|11\rangle_{CA}. \quad (5.27)$$

The state (5.23) has four terms. We rewrite them one by one:

$$\frac{1}{\sqrt{2}}\alpha\,|00\rangle_{CA}|0\rangle_B=\frac{1}{2}\alpha\left(|\Phi^+\rangle_{CA}+|\Phi^-\rangle_{CA}\right)|0\rangle_B, \quad (5.28)$$

$$\frac{1}{\sqrt{2}}\alpha\,|01\rangle_{CA}|1\rangle_B=\frac{1}{2}\alpha\left(|\Psi^+\rangle_{CA}+|\Psi^-\rangle_{CA}\right)|1\rangle_B, \quad (5.29)$$

$$\frac{1}{\sqrt{2}}\beta\,|10\rangle_{CA}|0\rangle_B=\frac{1}{2}\beta\left(|\Psi^+\rangle_{CA}-|\Psi^-\rangle_{CA}\right)|0\rangle_B, \quad (5.30)$$

$$\frac{1}{\sqrt{2}}\beta\,|11\rangle_{CA}|1\rangle_B=\frac{1}{2}\beta\left(|\Phi^+\rangle_{CA}-|\Phi^-\rangle_{CA}\right)|1\rangle_B. \quad (5.31)$$

We add up all four terms and simplify:

$$\begin{aligned}|\psi\rangle_C|\Phi+\rangle_{AB}=&\frac{1}{2}\big[|\Phi^+\rangle_{CA}\left(\alpha|0\rangle_B+\beta|1\rangle_B\right)+|\Phi^-\rangle_{CA}\left(\alpha|0\rangle_B-\beta|1\rangle_B\right)\\&+|\Psi^+\rangle_{CA}\left(\alpha|1\rangle_B+\beta|0\rangle_B\right)+|\Psi^-\rangle_{CA}\left(\alpha|1\rangle_B-\beta|0\rangle_B\right)\big]. \quad (5.32)\end{aligned}$$

This is the *same* state as (5.23), just written in the Bell basis of qubits A and C. And, remarkably, we can already see that Bob's qubit is in a state that is either equal to or closely resembles the unknown input state.

We have already established in our analysis of superdense coding that a measurement in the Bell basis can be performed perfectly. Alice needs to apply a CNOT and a Hadamard

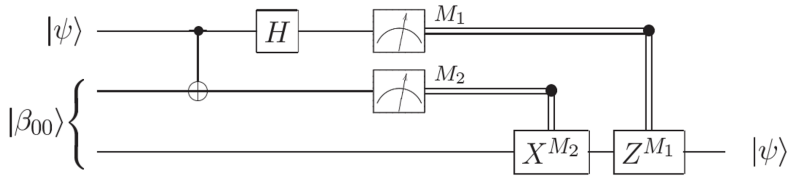

Figure 5.4: Circuit representation of quantum teleportation. The top wire corresponds to the input state $|\psi\rangle$ of qubit C which is sent to Alice. The center wire (A) and bottom wire (B) represent the shared Bell state $|\beta_{00}\rangle = |\Phi^+\rangle_{AB}$. Alice performs a Bell state measurement on qubits C and A via a CNOT and Hadamard. The two classical output bits M_1 and M_2 are communicated to Bob who can perform a unitary transformation $Z^{M_1}X^{M_2}$ on his qubit B to perfectly recreate the input state $|\psi\rangle$. Picture adapted from Ref. [19].

and then measure in the computational basis. Her outcome bits are called $M_1 \in \{0,1\}$ and $M_2 \in \{0,1\}$. All four outcomes $M_1M_2 \in \{00,01,10,11\}$ have the same probability $\frac{1}{4}$. Once Alice has performed the Bell state measurement, she transmits the outcome as a string of two *classical* bits M_1M_2 to Bob:

$$|\Phi^+\rangle_{CA} \to M_1M_2 = 00 \tag{5.33}$$
$$|\Psi^+\rangle_{CA} \to M_1M_2 = 01 \tag{5.34}$$
$$|\Phi^-\rangle_{CA} \to M_1M_2 = 10 \tag{5.35}$$
$$|\Psi^-\rangle_{CA} \to M_1M_2 = 11 \tag{5.36}$$

What should Bob do now? Well, since he also knows the state decomposition (5.32), he can act accordingly:

- If Bob receives the bit string $M_1M_2 = 00$, he knows that Alice has found $|\Phi^+\rangle_{AC}$. Therefore, he does not need to do anything (i.e. he applies the identity operation). His qubit B is already exactly in the state $\alpha|0\rangle_B + \beta|1\rangle_B$ in which qubit C was.
- If Bob receives the bit string $M_1M_2 = 01$, he knows that Alice has measured $|\Psi^+\rangle_{AC}$ and that his qubit is in state $\alpha|1\rangle_B + \beta|0\rangle_B$. All he needs to do is apply the (bit flip) X gate. This will transform his qubit to the desired teleported state.
- If Bob receives $M_1M_2 = 10$ (Alice measured $|\Phi^-\rangle$), his qubit is in state $\alpha|0\rangle_B - \beta|1\rangle_B$. He needs apply the (phase flip) Z gate.
- If Bob receives $M_1M_2 = 11$ (Alice measured $|\Psi^-\rangle$), his qubit is in state $\alpha|1\rangle_B - \beta|0\rangle_B$. He needs to first apply X and then Z.

In summary, by applying $Z^{M_1}X^{M_2}$, Bob can restore the unknown input state of qubit C "in" his qubit B on his side. The circuit representation of quantum teleportation is shown in Figure 5.4. In the circuit, where time runs from left to right, X^{M_2} is applied before Z^{M_1}. This corresponds to the transformation $Z^{M_1}X^{M_2}$, which acts from the left onto a state, i.e. X^{M_2} is applied first.

Some interesting questions emerge:

1. Does quantum teleportation violate the physical principle that nothing – neither an object nor information – can propagate faster than the (vacuum) speed of light? This principle is a cornerstone of relativity theory and thus of all physics. The answer is no. Qubit C is physically not transmitted at all, only its state is teleported. And for the teleportation to succeed, Alice needs to classically communicate information to Bob, e.g.,

Figure 5.5: Quantum teleportation over 143 km from Tenerife (left: the optical ground station) to La Palma, 2400 meters above sea level. Picture taken from Ref. [10].

via electromagnetic waves or a telephone line. This communication is bounded by the speed of light. Without this classical information, teleportation does not provide Bob with any information at all about qubit C.

2. Does quantum teleportation violate the the no-cloning theorem? The answer is again no. After teleportation, qubit B is in the correct teleported quantum state. Qubit C, however, is not anymore in its original state but in the post-measurement state corresponding to Alice's measurement outcome.

3. What can we learn from teleportation? We can deduce another one of Bennett's laws of information, namely that 1 ebit together with 2 bits of classical information is as powerful as directly communicating a qubit:

$$1 \text{ ebit} + 2 \text{ bits} \geq 1 \text{ qubit}. \tag{5.37}$$

Using photons, quantum teleportation can be achieved over very long distances. In glass fibers, dozens or hundreds of kilometers are feasible. In free space, the Earth based record is 143 km (using telescope ground stations, see Figure 5.5) [12], and with satellites thousands of kilometers have been reached.

5.4 Entanglement Swapping and Quantum Repeaters

Entanglement swapping was put forward in 1993 [17] and is closely related to quantum teleportation. The schematic setup is shown in Figure 5.6. It works as follows: There are two EPR sources. The first source produces a Bell pair of qubits labelled 1 and 2. The second source produces a Bell pair of qubits 3 and 4. Qubits 2 and 3 are then subjected to a Bell state measurement (BSM), which "projects" qubits 1 and 4 into a Bell pair although these two qubits have never interacted in any way whatsoever. Which particular Bell state qubits 1 and 4 end up in, depends on the initially produced Bell pair and the result of the Bell state measurement.

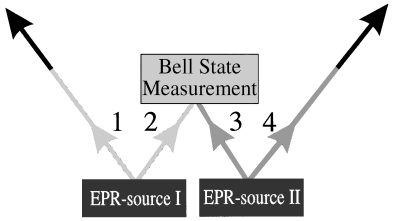

Figure 5.6: In entanglement swapping, two entangled Bell pairs are created by two EPR sources. Qubit 2 from the first pair and qubit 3 from the second pair are then subjected to a Bell state measurement. This projects qubits 1 and 4 into a Bell state. Picture taken from Ref. [17].

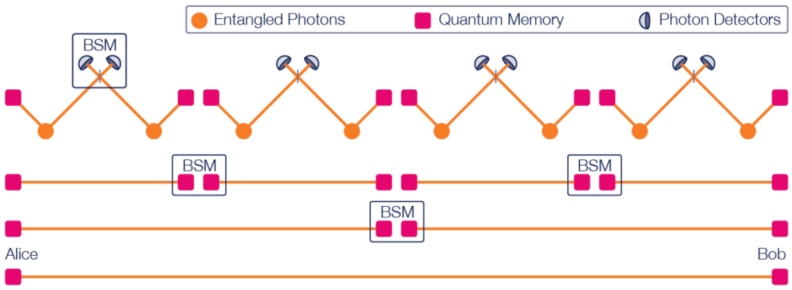

Figure 5.7: A quantum repeater allows to create entanglement between two distant locations using multiple pair sources and entanglement swapping sites. Picture from Ref. [13].

Exercise 5.1 Start with the initial 4-particle state of two Bell (singlet) pairs $|\Psi\rangle_{1234} = |\Psi^-\rangle_{12}|\Psi^-\rangle_{34}$. Project qubits 3 and 4 onto the singlet state by applying the bra $\langle\Psi^-|_{23}$ from the left. Compute the resulting state of qubits 1 and 4. ∎

Solution: Blackboard or homework.

Entanglement swapping is at the heart of the quantum repeater which itself is likely an essential tool for building large scale quantum networks. Assume that Alice and Bob would like to share entangled Bell pairs but are too far apart from each other such that this is technologically not possible, e.g. due to transmission loss in glass fibers. Figure 5.7 shows the solution: In a quantum repeater scheme, many Bell pairs are created simultaneously at different spatially distant locations. Entanglement swapping (and quantum memories) are then used to create an entangled pair between Alice and Bob.

6. Bell's Inequality

6.1 The EPR Argument

Already in the early years of quantum mechanics, some of its founding fathers – in particular Albert Einstein and Erwin Schrödinger – were very unsatisfied with its probabilistic nature. Einstein famously wrote in 1926 in a letter to Max Born: "Jedenfalls bin ich überzeugt, daß der [Alte] nicht würfelt." ("I, at any rate, am convinced that [He] does not throw dice.") And, also in 1926, Schrödinger wrote: "Wenn es doch bei dieser verdammten Quantenspringerei bleiben soll, so bedaure ich, mich mit der Quantentheorie überhaupt beschäftigt zu haben." ("If all this damned quantum jumping were really here to stay, I should be sorry I ever got involved with quantum theory.")

In 1935, Albert Einstein, Boris Podolsky, and Nathan Rosen (EPR) put forward a thought experiment in which two position-momentum entangled particles at distant locations – say one qubit is with Alice and the other one with Bob in a different laboratory – show quantum correlations in mutually exclusive properties [7]. Position and momentum can be thought as analogs to the computational and the diagonal basis. These are so-called *non-commuting* properties, i.e. you cannot measure them simultaneously, and a measurement of one property will change the outcome statistics of the other property.

We will discuss the EPR argument in a variant due to David Bohm, i.e. we will not use position and momentum (as in the original paper) but qubits, as we have developed the necessary formalism already: Assume that Alice and Bob share an entangled singlet state. The singlet state has the remarkable property that Alice's and Bob's results are anti-correlated not only in the computational basis, but also in the x (and y, for that matter) basis:

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} = -\frac{|+-\rangle - |-+\rangle}{\sqrt{2}}. \tag{6.1}$$

If Alice chose to measure her particle in the computational $|0\rangle/|1\rangle$ basis and observed result $A_z \in \{0,1\}$, she would know with certainty that a computational basis measurement on Bob's particle would yield the opposite outcome, i.e. $B_z = 1$ if $A_z = 0$, and $B_z = 0$ if $A_z = 1$. If, however, Alice chose to measure her particle in the diagonal $|+\rangle/|-\rangle$ basis and observed result $A_x \in \{+,-\}$, she would know with certainty that a measurement of Bob's

particle in the diagonal basis would lead to the opposite result, i.e. $B_x = -$ if $A_x = +$, and $B_x = +$ if $A_x = -$.

Which property to measure on her particle, is Alice's free choice. And since Bob's laboratory is at a distant location, the "reality" of his particle must not depend on what Alice does in her lab. So, actually, both the computational basis state and the diagonal basis state of Bob's particle must "exist" independent of and prior to Alice's measurement. In other words: Both outcomes of Bob – the one in the computational (B_z) and the one in the diagonal basis (B_x) – must simultaneously be *elements of reality* as they can be predicted with certainty. This contradicts quantum mechanics which cannot give such a "complete" description of Bob's particle. In quantum mechanics, there exists no qubit state which can simultaneously define with certainty the outcome of a computational-basis measurement and the outcome of a diagonal-basis measurement. Therefore, EPR deduced that quantum mechanics is *incomplete*. In the final sentence of the paper, they expressed their believe that a complete description should be possible.

Niels Bohr – as the leading proponent of the Copenhagen interpretation – rejected EPR's viewpoint by stressing that one is not allowed to draw conclusions about (Bob's) reality based on unperformed measurements (by Alice). However, the search for *hidden variables* had started. These hidden variables would allow a complete description of physical reality "underneath" the quantum state.

Exercise 6.1 Prove the second equality sign in (6.1). ∎

Solution: Blackboard or homework.

6.2 Local Realism

It was an open question for many decades after the EPR paper, how to find a hidden variable description – i.e. a completion – of quantum mechanics. Einstein himself was certain that it should exist. In 1964, however, John Bell demonstrated that the world view of local realism is, in fact, incompatible with the predictions of quantum mechanics [1].

Local realism is the classical worldview in which the following two assumptions hold:

- *Realism*: All properties of objects exist prior to and independent of measurement. This means that there are hidden variables which, in principle, allow a complete description of physical reality.
- *Locality:* No physical influence can travel faster than the vacuum speed of light. This is the cornerstone of the special theory of relativity and one of the most fundamental principles in all of physics.

There is a third assumption called *Freedom of Choice* (or Measurement Independence) which postulates that measurement settings can be chosen statistically independently from the hidden variables.

Bell's theorem proves the incompatibility of local hidden variable theories and quantum mechanics. It implies that either local realism or quantum mechanics must be wrong. Moreover, an experiment can now decide between the two theories in the sense that it can rule out one of them. (No experiment can, of course, prove the other surviving theory. In fact, no scientific theory can ever be proven as that would require infinitely many experiments in infinitely many different circumstances. Experiments can only falsify a theory, on the one hand, or give more credibility to it, on the other. Natural science differs radically from mathematics in that sense, as in the latter statements can really be proven.)

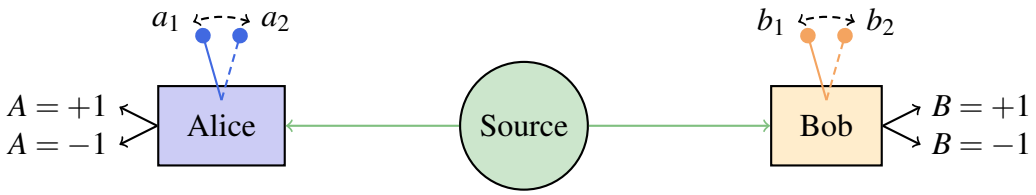

Figure 6.1: In a CHSH setup, a source emits pairs of entangled particles. For each arriving particle, Alice and Bob can each choose between two measurement settings. And each party observes one of two possible outcomes for every measured particle.

6.3 The CHSH Inequality

We will go through this groundbreaking result of Bell not via his original paper but using a simpler derivation due to Clauser, Horne, Shimony, and Holt (CHSH) [6]. Let us consider Figure 6.1.

A source in the middle of the setup sequentially emits pairs of particles. Let's denote the pairs by $i = 1,...,n$, i.e. there are n runs of the experiment. From each pair, one particle is sent to Alice, and the other is sent to Bob. In each run i, each particle carries a hidden variable (vector) $\lambda^{(i)}$ which should be thought of as a complete "instruction list" how it should behave upon future measurements. It is not in any way restrictive that Alice's and Bob's particle of pair i carry the same $\lambda^{(i)}$. Rather the opposite. You can think that $\lambda^{(i)} = (\lambda_A^{(i)}, \lambda_B^{(i)})$, i.e. that Alice's particle not only carries all instructions for itself but also all instructions for Bob's particle.

For each arriving particle i, Alice can choose her measurement setting $a^{(i)}$ between two options (angles) a_1 and a_2. Similarly for Bob, who chooses his setting $b^{(i)}$ between b_1 and b_2. E.g. for run $i = 3$, Alice may choose setting $a^{(3)} = a_1$ and Bob may choose setting $b^{(3)} = b_2$.

Each particle is then measured in the corresponding basis, and the results are denoted as $A^{(i)}$ and $B^{(i)}$, respectively. The outcomes are dichotomic, i.e. only the two values $+1$ and -1 are possible. E.g. in run 5, Alice may choose setting a_2 and Bob may choose b_1. Her outcome is $+1$ and his is -1. Then we would write this as $A_2^{(5)} = +1$ and $B_1^{(5)} = -1$, i.e. the subscripts denote the setting choices.

The assumption of realism implies that in every run, the hidden variable determines Alice's outcomes for both setting choices. Although only one choice can actually be implemented, both measurement results "exist". Similar for Bob. We still need to explicitly allow that the measurement results not only depend on the hidden variable and the local setting choice, but also on the setting choice of the other party. That means, in realism we have:

$$A^{(i)} = A(\lambda^{(i)}, a^{(i)}, b^{(i)}), \tag{6.2}$$

$$B^{(i)} = B(\lambda^{(i)}, b^{(i)}, a^{(i)}). \tag{6.3}$$

The assumption of locality implies that – given Alice's and Bob's choices and measurements are space-like separated in the sense of special relativity such that not even light can travel fast enough to communicate information – Alice's result does not depend on Bob's setting choice and vice versa. Hence, we obtain

$$A^{(i)} = A(\lambda^{(i)}, a^{(i)}), \tag{6.4}$$

$$B^{(i)} = B(\lambda^{(i)}, b^{(i)}). \tag{6.5}$$

Thus, local realism implies the existence of all four outcome values and the fact that they depend only on the hidden variable and the local setting choice (let us suppress the index i for better readability):

$$A_1 = A(\lambda, a_1), \tag{6.6}$$
$$A_2 = A(\lambda, a_2), \tag{6.7}$$
$$B_1 = B(\lambda, b_1), \tag{6.8}$$
$$B_2 = B(\lambda, b_2). \tag{6.9}$$

Now, let us consider the following algebraic combination:

$$A_1\,(B_1 + B_2) + A_2\,(B_1 - B_2) = \pm 2. \tag{6.10}$$

It holds in every run i. Proof: If $B_1 = B_2$, the second bracket vanishes. The first bracket is either $1+1=2$ or $-1-1=-2$. This gets multiplied by A_1 which is $+1$ or -1. In any case, the result is $+2$ or -2. If, on the other hand, $B_1 \neq B_2$, the first bracket vanishes. Then the second bracket is either $+2$ or -2. Multiplication with A_2, which is $+1$ or -1, leads again to result $+2$ or -2.

We reintroduce proper notation with indices and rewrite the above expression:

$$A_1^{(i)} B_1^{(i)} + A_1^{(i)} B_2^{(i)} + A_2^{(i)} B_1^{(i)} - A_2^{(i)} B_2^{(i)} = \pm 2. \tag{6.11}$$

Now, let us calculate the expectation value over all runs i:

$$\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle = \frac{1}{n} \sum_{i=1}^{n} [A_1^{(i)} B_1^{(i)} + A_1^{(i)} B_2^{(i)} + A_2^{(i)} B_1^{(i)} - A_2^{(i)} B_2^{(i)}].$$

Clearly, the average over lots of $+2$'s and -2's cannot exceed $+2$. Similarly, it cannot fall below -2. Thus, we can write:

$$S \equiv |\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle| \leq 2. \tag{6.12}$$

This is the famous CHSH inequality, which holds for all local hidden variable theories.

If Alice and Bob perform n runs and randomly choose their settings in each run, then in roughly $n/4$ cases they have chosen settings a_1, b_1. The outcomes A_1, B_1 – which they communicate to each other – of all those runs allows them to calculate the expectation value $\langle A_1 B_1 \rangle$. Similarly, the other three expectation values are obtained. No local realistic theory – this includes classical mechanics, electrodynamics, optics, etc. – can violate the CHSH inequality (6.12). The correlations cannot violate the local realistic bound (i.e. the right hand side) of 2.

So what about quantum mechanics? How can it violate the CHSH inequality (6.12) and yield $S > 2$? Let us assume that in every run the source emits the Bell singlet state

$$|\Psi^-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) = \tfrac{|01\rangle_{AB} - |10\rangle_{AB}}{\sqrt{2}}, \tag{6.13}$$

where A and B denote the parties Alice and Bob, respectively (and not outcome values). Alice's measurement a_1 corresponds to a measurement in the $|a_1\rangle / |a_1\rangle^\perp$ basis:

$$|a_1\rangle = \cos\tfrac{\alpha_1}{2}\,|0\rangle + \sin\tfrac{\alpha_1}{2}\,|1\rangle, \quad |a_1\rangle^\perp = -\sin\tfrac{\alpha_1}{2}\,|0\rangle + \cos\tfrac{\alpha_1}{2}\,|1\rangle, \tag{6.14}$$

where $\langle a_1|a_1\rangle^{\perp} = 0$. If $|a_1\rangle$ is obtained, the outcome is called $A_1 = +1$, and if $|a_1\rangle^{\perp}$ is obtained, the outcome is called $A_1 = -1$. Similarly, the basis states of Alice's second measurement setting a_2 and Bob's basis states for his measurement settings b_1, b_2 read:

$$|a_2\rangle = \cos\tfrac{\alpha_2}{2}\,|0\rangle + \sin\tfrac{\alpha_2}{2}\,|1\rangle, \quad |a_2\rangle^{\perp} = -\sin\tfrac{\alpha_2}{2}\,|0\rangle + \cos\tfrac{\alpha_2}{2}\,|1\rangle, \tag{6.15}$$

$$|b_1\rangle = \cos\tfrac{\beta_1}{2}\,|0\rangle + \sin\tfrac{\beta_1}{2}\,|1\rangle, \quad |b_1\rangle^{\perp} = -\sin\tfrac{\beta_1}{2}\,|0\rangle + \cos\tfrac{\beta_1}{2}\,|1\rangle, \tag{6.16}$$

$$|b_2\rangle = \cos\tfrac{\beta_2}{2}\,|0\rangle + \sin\tfrac{\beta_2}{2}\,|1\rangle, \quad |b_2\rangle^{\perp} = -\sin\tfrac{\beta_2}{2}\,|0\rangle + \cos\tfrac{\beta_2}{2}\,|1\rangle. \tag{6.17}$$

The expectation (or correlation) value $\langle A_j B_k\rangle$, with $j,k \in \{1,2\}$, is given as follows:

$$\begin{aligned}
\langle A_j B_k\rangle &= p(A_j = +1, B_k = +1) + p(A_j = -1, B_k = -1) \\
&\quad - p(A_j = +1, B_k = -1) - p(A_j = -1, B_k = +1) \\
&= p(A_j = B_k) - p(A_j \neq B_k) \\
&= p(A_j = B_k) - [1 - p(A_j = B_k)] \\
&= 2\,p(A_j = B_k) - 1 \\
&= 2\,[p(A_j = +1, B_k = +1) + p(A_j = -1, B_k = -1)] - 1.
\end{aligned} \tag{6.18}$$

So, we are left to compute $p_{jk}(+1,+1) \equiv p(A_j = +1, B_k = +1)$, i.e. the probability that, with setting choices a_j, b_k, both parties obtain the result $+1$, and $p_{jk}(-1,-1) \equiv p(A_j = -1, B_k = -1)$, i.e. the probability that both parties obtain the result -1. Let's start with the first one:

$$\begin{aligned}
p_{jk}(+1,+1) &= |\langle a_j|\langle b_k|\Psi^-\rangle|^2 \\
&= \Big|\big(\cos\tfrac{\alpha_j}{2}\,\langle 0|_A + \sin\tfrac{\alpha_j}{2}\,\langle 1|_A\big)\big(\cos\tfrac{\beta_k}{2}\,\langle 0|_B + \sin\tfrac{\beta_k}{2}\,\langle 1|_B\big)\,\tfrac{|01\rangle_{AB} - |10\rangle_{AB}}{\sqrt{2}}\Big|^2 \\
&= \tfrac{1}{2}\Big|\cos\tfrac{\alpha_j}{2}\sin\tfrac{\beta_k}{2} - \sin\tfrac{\alpha_j}{2}\cos\tfrac{\beta_k}{2}\Big|^2 \\
&= \tfrac{1}{2}\sin^2\tfrac{\alpha_j - \beta_k}{2}.
\end{aligned} \tag{6.19}$$

Similarly, we can calculate the second probability:

$$\begin{aligned}
p_{jk}(-1,-1) &= |\langle a_j|^{\perp}\langle b_k|^{\perp}\Psi^-\rangle|^2 \\
&= \Big|\big(-\sin\tfrac{\alpha_j}{2}\,\langle 0|_A + \cos\tfrac{\alpha_j}{2}\,\langle 1|_A\big)\big(-\sin\tfrac{\beta_k}{2}\,\langle 0|_B + \cos\tfrac{\beta_k}{2}\,\langle 1|_B\big)\,\tfrac{|01\rangle_{AB} - |10\rangle_{AB}}{\sqrt{2}}\Big|^2 \\
&= \tfrac{1}{2}\Big|-\sin\tfrac{\alpha_j}{2}\cos\tfrac{\beta_k}{2} + \cos\tfrac{\alpha_j}{2}\sin\tfrac{\beta_k}{2}\Big|^2 \\
&= \tfrac{1}{2}\sin^2\tfrac{\alpha_j - \beta_k}{2}.
\end{aligned} \tag{6.20}$$

This is actually the same result as for $p_{jk}(+1,+1)$ due to the symmetry of the state. Hence, for the expectation value (6.18), we can write

$$\begin{aligned}
\langle A_j B_k\rangle &= 2\sin^2\tfrac{\alpha_j - \beta_k}{2} - 1 \\
&= -\cos(\alpha_j - \beta_k).
\end{aligned} \tag{6.21}$$

We can obtain an optimal – in the sense of leading to the largest possible value for S – result, if we choose, for example, the following measurement settings (see Figure 6.2):

$$\alpha_1 = 0, \quad \alpha_2 = \tfrac{\pi}{2}, \quad \beta_1 = \tfrac{\pi}{4}, \quad \beta_2 = -\tfrac{\pi}{4}. \tag{6.22}$$

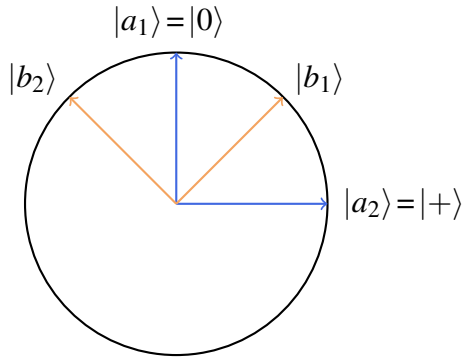

Figure 6.2: For the Bell singlet state, one example for a set of optimal settings for Alice's (blue) and Bob's (orange) measurements is $\alpha_1 = 0, \alpha_2 = \frac{\pi}{2}, \beta_1 = \frac{\pi}{4}, \beta_2 = -\frac{\pi}{4}$.

They lead to the correlation values

$$\langle A_1 B_1 \rangle = \langle A_1 B_2 \rangle = \langle A_2 B_1 \rangle = -\tfrac{1}{\sqrt{2}}, \tag{6.23}$$

$$\langle A_2 B_2 \rangle = +\tfrac{1}{\sqrt{2}}. \tag{6.24}$$

Hence, the quantum mechanical Bell value becomes

$$\begin{aligned} S_{\mathrm{QM}} &= |\langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle| \\ &= |-\tfrac{1}{\sqrt{2}} - \tfrac{1}{\sqrt{2}} - \tfrac{1}{\sqrt{2}} - \tfrac{1}{\sqrt{2}}| \\ &= 2\sqrt{2} \approx 2.828. \end{aligned} \tag{6.25}$$

This is larger than the local realistic bound of 2 in the CHSH inequality (6.12). The predictions of quantum mechanics violate Bell's inequality.

Bell experiments have been performed since 1972 with ever increasing levels of sophistication and certainty, closing potential loopholes that would still allow an explanation of the observed Bell violation in terms of local hidden variables. The conclusion of all these experiment is that Bell's inequality can be violated using quantum mechanically entangled states. The predictions of quantum mechanics agree with the experimental results. This means that quantum mechanics prevailed and that local realism is an untenable view of the world. (Bell's inequality, however, does not say anything about non-local hidden variable theories such as Bohmian mechanics.)

The 2022 Nobel Prize in Physics was awarded to Alain Aspect, John Clauser and Anton Zeilinger for seminal Bell experiments. In 2015, three "loophole-free" experiments were performed; the one of the Zeilinger group was set up in the Vienna Hofburg and allowed only a less than 10^{-30} probability for an explanation of the observed correlations in terms of local hidden variables [11].

Exercise 6.2 Show numerically (using some computer software tool) that no set of angles $\alpha_1, \alpha_2, \beta_1, \beta_2$ can lead to a larger S-value than $2\sqrt{2}$. ■

Solution: Homework.

The "quantum bound" of $2\sqrt{2}$ is called Tsirelson bound. We remark that there are theories – so called PR boxes – which are no-signalling (i.e. not violating the locality

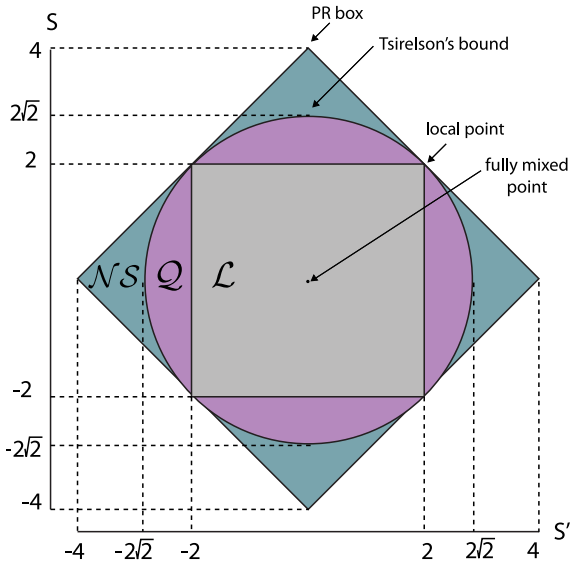

Figure 6.3: A two-dimensional section of the no-signalling polytope $\mathscr{NS}$. The vertical axis represents the CHSH value S, while the horizontal axis represents the value of a symmetry of the CHSH expression S' where settings have been relabeled. Local hidden variable correlations are in the polytope $\mathscr{L}$ and satisfy $S < 2$. PR boxes can achieve a CHSH value of $S = 4$. Quantum mechanical correlations form a smooth region $\mathscr{Q}$, not a polytope, and can reach the Tsirelson bound of $S = 2\sqrt{2}$. Picture from Ref. [5].

assumption) but distinct from quantum mechanics that would allow to reach the algebraic bound of $S = 4$. However, they seem to not be realised in nature. Figure 6.3 illustrates the achievable S-values for different theories.

6.4 The CHSH Game

One can rephrase the CHSH setup into a game, involving two cooperating but separated parities, Alice and Bob, and a referee called Charlie. Here are the rules of the game:

- Charlie chooses two random bits $a \in \{0,1\}$ and $b \in \{0,1\}$.
- He sends a to Alice and b to Bob.
- Alice responds to Charlie with bit $A \in \{0,1\}$, and Bob responds with $B \in \{0,1\}$.
- For $a = b = 1$, Alice and Bob win if their answers were different, i.e. $A \neq B$. In the other three cases $\{a = b = 0\}, \{a = 0, b = 1\}, \{a = 1, b = 0\}$, they win if their outputs are the same, i.e. $A = B$. In summary, they win if $A \oplus B = a \wedge b$, and lose otherwise.

The four combinations of Charlie's bits all occur with $\frac{1}{4}$ probability. Hence, Alice's and Bob's success probability for winning the CHSH game is

$$p_{\text{succ}} = \tfrac{1}{4}\big[p(A=B|a=0,b=0) + p(A=B|a=0,b=1) + p(A=B|a=1,b=0) + p(A\neq B|a=1,b=1)\big]. \tag{6.26}$$

In full analogy to the previous section but taking the Bell state, one can show that with classical strategies – i.e. within local realism – the success probability of Alice and Bob is bounded by $p_{\text{succ}}^{(\text{LR})} \leq \frac{3}{4}$. However, quantum mechanically and using the Bell

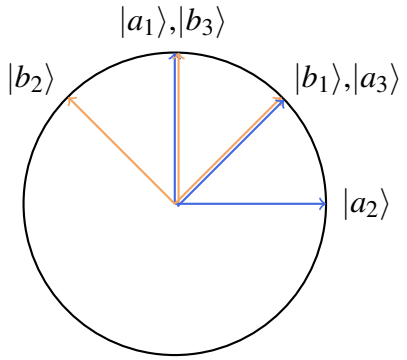

Figure 6.4: In the E91 protocol, Alice (blue) and Bob (orange) each choose between 3 settings. They again use the CHSH angles $\alpha_1, \alpha_2, \beta_1, \beta_2$, see Figure (6.2). In addition, Alice uses $\alpha_3 = \beta_1$ and Bob uses $\beta_3 = \alpha_1$.

state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, the two parties can reach a success probability of $p_{\text{succ}}^{(\text{QM})} = \cos^2 \frac{\pi}{8} = \frac{1}{4}(2+\sqrt{2}) \approx 0.854$.

6.5 Entanglement-Based Quantum Key Distribution

In 1991, Artur Ekert devised a protocol (nowadays called "E91") where entangled states are employed to create a private and secure key between two distant parties [8]. This key can then be used in one-time-pad cryptography, which is the only information-theoretically secure cryptographic scheme, i.e. it remains safe even if an adversary has infinite computing power.

The E91 protocol works as follows: Alice and Bob, who are in distant laboratories, share singlet states which are emitted from some source at another location. For each particle they obtain, they randomly pick a setting. The setting choices are illustrated in Figure 6.4. Again, the CHSH angles $\alpha_1, \alpha_2, \beta_1, \beta_2$ from Figure (6.2) are used. In addition, Alice has the option $\alpha_3 = \beta_1$ and Bob may choose $\beta_3 = \alpha_1$.

Hence, in total there are 9 possible setting combinations. If n pairs are created, each setting combination appears roughly $n/9$ times. After all n pairs are measured, Alice and Bob communicate (openly and classically) their setting choices to each other, but not their outcomes. Let us analyze the different combinations:

- (α_1, β_3) and (α_3, β_1): In these two combinations, Alice and Bob chose the same measurement direction. Due to the anti-symmetric nature of the singlet state, their results are opposite: $A = -B$. If Alice converts her "$+1$" outcomes to bits with value 1 and her "-1" outcomes to bits with value 0, and if Bob does the opposite ("$+1$"$\to 0$, "-1"$\to 1$), then they will obtain the same bit string of 0's and 1's. This is their secret key.
- (α_1, β_1), (α_1, β_2), (α_2, β_1), and (α_2, β_2): These four setting combinations are relevant for the CHSH inequality. Alice and Bob need to communicate also their outcomes to each other in order that they can compute the S-value.
- (α_3, β_2), (α_2, β_3) and (α_3, β_3): The results of these combinations are discarded. They are neither relevant for the CHSH inequality nor for the key.

Quantum key distribution uses quantum mechanics to distribute a key to two distant parties.

Entanglement guarantees perfect anti-correlation of their results when they measure in the same basis. And the violation of a Bell inequality ensures that no eavesdropper has intercepted their qubits and tampered with them. If the Bell value S is (close to) $2\sqrt{2}$, they know that an eavesdropper – a "man in the middle" or even someone who controls the pair source – can have (almost) no information about their key. If the S-value is below 2, Alice and Bob are fully insecure and must not use their key.

While a full security proof is far beyond the scope of this lecture, let us consider three possible attack scenarios: (1) An eavesdropper intercepts some of the qubits, measures them to obtain knowledge about the key, and then re-emits them to Alice or Bob. Such an attack would destroy the entanglement in these pairs and lead to a degradation of the Bell value which would be detected by Alice and Bob. (2) If the eavesdropper could copy qubits without measuring them, the scheme would indeed be insecure. But such copying is forbidden due to the no-cloning theorem. (3) And finally, *monogamy of entanglement* prevents Eve from creating a three-partite entangled state which would allow her to learn the key and simultaneously allow Alice and Bob to violate the CHSH inequality. The GHZ state is a three-partite entangled state, but it will not violate the CHSH inequality – the entanglement in the GHZ state is between all three parties, not between only two.

In summary, entanglement-based quantum key distribution is a method whose security is guaranteed by the laws of nature, and not by the mere complexity of some mathematical task.

7. Mixed States

7.1 Density Matrices

Until now, we have represented quantum states as vectors. An alternative approach – which is mathematically equivalent and yet often more practical – is to use a *density matrix* (or density operator). The formalism of density matrices will later also allow us to describe quantum systems which are statistical mixtures.

Given the most general one-qubit state vector $|\psi\rangle = \binom{\alpha}{\beta}$, the corresponding density matrix ρ is defined as the outer product

$$\rho \equiv |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\bar{\alpha} \;\; \bar{\beta}) = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}. \tag{7.1}$$

Let's write down the density matrices of our z, x, and y basis states:

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1 \;\; 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{7.2}$$

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0 \;\; 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{7.3}$$

$$|+\rangle\langle +| = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \end{pmatrix} (1 \;\; 1) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \tag{7.4}$$

$$|-\rangle\langle -| = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \end{pmatrix} (1 \;\; -1) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \tag{7.5}$$

$$|R\rangle\langle R| = \frac{1}{2}\begin{pmatrix} 1 \\ i \end{pmatrix} (1 \;\; -i) = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \tag{7.6}$$

$$|L\rangle\langle L| = \frac{1}{2}\begin{pmatrix} 1 \\ -i \end{pmatrix} (1 \;\; i) = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}. \tag{7.7}$$

The same logic applies for states of multiple qubits. For a general two-qubit state $|\psi\rangle =$

$(\alpha,\beta,E,\delta)^T$, the density matrix reads:

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \alpha \\ \beta \\ E \\ \delta \end{pmatrix} (\bar{\alpha} \;\; \bar{\beta} \;\; \bar{E} \;\; \bar{\delta}) = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} & \alpha\bar{E} & \alpha\bar{\delta} \\ \bar{\alpha}\beta & |\beta|^2 & \beta\bar{E} & \beta\bar{\delta} \\ \bar{\alpha}E & \bar{\beta}E & |E|^2 & E\bar{\delta} \\ \bar{\alpha}\delta & \bar{\beta}\delta & \bar{E}\delta & |\delta|^2 \end{pmatrix}. \tag{7.8}$$

Let's consider two concrete examples, namely the product state $|00\rangle$ and the Bell singlet state:

$$|00\rangle\langle 00| = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} (1 \;\; 0 \;\; 0 \;\; 0) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{7.9}$$

$$|\Psi^-\rangle\langle\Psi^-| = \frac{1}{2} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} (0 \;\; 1 \;\; -1 \;\; 0) = \frac{1}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{7.10}$$

Density matrices have the following 4 properties:

- Hermitian: $\rho^\dagger = \rho$
- Normalized: $\mathrm{Tr}(\rho) = 1$
- Positive-semidefinite: $\rho \geq 0$

Applying a unitary transformation U to a state $\rho = |\psi\rangle\langle\psi|$, leads to a transformed state ρ' in the following way:

$$\rho' = U\rho U^\dagger = U|\psi\rangle\langle\psi|U^\dagger. \tag{7.11}$$

7.2 Pure and Mixed States

We are now in the position to introduce a more general class of quantum states. Until now, we have only considered so-called *pure states*, where we know (for certain) the quantum state the system is in. But how do we treat a situation where we have a *statistical ensemble* of states?

Consider the situation where a source emits N possible quantum states $|\psi_i\rangle$, with $i = 1,\ldots,N$, where each has probability p_i to be emitted, with $\sum_{i=1}^N p_i = 1$. In the state vector formalism, we cannot represent this ensemble. (The state $|\psi\rangle = \sqrt{p_1}|\psi_1\rangle + \sqrt{p_2}|\psi_2\rangle + \ldots + \sqrt{p_N}|\psi_N\rangle$ does *not* represent the above described ensemble, as it is still pure state where all possible states are superposed.) The density matrix formalism, however, allows us to *mix* the individual states $\rho_i = |\psi_i\rangle\langle\psi_i|$ into an ensemble. The so-called *mixed state* has the form

$$\rho = \sum_{i=1}^N p_i \rho_i = \sum_{i=1}^N p_i |\psi_i\rangle\langle\psi_i|. \tag{7.12}$$

Mixed states are weighted (convex) sums of at least two pure states. Pure states are states, where only one probability $p_i = 1$, and all others are 0.

Pure states $\rho = |\psi\rangle\langle\psi|$ have the property

$$\rho^2 = \rho\,\rho = |\psi\rangle\langle\psi||\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \rho. \tag{7.13}$$

	Pure states	Mixed states
State vector	$\|\psi\rangle$	-
Density matrix	$\rho = \|\psi\rangle\langle\psi\|$	$\rho = \sum_{i=1}^{N} p_i \|\psi_i\rangle\langle\psi_i\|$
Trace	$\mathrm{Tr}[\rho] = 1$	$\mathrm{Tr}[\rho] = 1$
Square	$\rho^2 = \rho$	$\rho^2 \neq \rho$
Purity	$\mathrm{Tr}[\rho^2] = 1$	$\frac{1}{N} \leq \mathrm{Tr}[\rho^2] < 1$

Table 7.1: Pure versus mixed states.

For mixed states, on the other hand, we have

$$\rho^2 = \sum_{i=1}^{N}\sum_{j=1}^{N} p_i p_j |\psi_i\rangle\langle\psi_i|\psi_j\rangle\langle\psi_j| = \sum_{i=1}^{N} p_i^2 |\psi_i\rangle\langle\psi_i| \neq \rho. \tag{7.14}$$

Here, we have assumed that all $|\psi_i\rangle$ and $|\psi_j\rangle$ are orthonormal, i.e. their scalar product is 0, except for the case $i = j$ when it is 1.

All quantum states (pure or mixed) have trace equal to 1:

$$\mathrm{Tr}[\rho] = \sum_k \langle k|\rho|k\rangle = \sum_k \sum_{i=1}^{N} p_i \langle k|\psi_i\rangle\langle\psi_i|k\rangle = \sum_k \sum_{i=1}^{N} p_i |\langle k|\psi_i\rangle|^2 = \sum_{i=1}^{N} p_i = 1. \tag{7.15}$$

Here, we have used that the trace can be computed by summing over a complete set of basis states $|k\rangle$ (for n qubits, there are 2^n basis states). $|\langle k|\psi_i\rangle|^2$ are the probabilities to obtain result k, and all these probabilities must sum up to 1: $\sum_k |\langle k|\psi_i\rangle|^2 = 1$. Finally, the sum over all probabilities p_i sums up to 1 as well.

Hence, using (7.13), we have for pure states:

$$\mathrm{Tr}[\rho^2] = \mathrm{Tr}[\rho] = 1. \tag{7.16}$$

For mixed states (where at least two of the p_i are larger than 0), we use (7.14) and obtain

$$\mathrm{Tr}[\rho^2] = \sum_k \sum_{i=1}^{N} p_i^2 \langle k|\psi_i\rangle\langle\psi_i|k\rangle = \sum_k \sum_{i=1}^{N} p_i^2 |\langle k|\psi_i\rangle|^2 = \sum_{i=1}^{N} p_i^2 < 1. \tag{7.17}$$

In fact, $\mathrm{Tr}[\rho^2]$ is a measure of how pure a quantum state is and is therefore called the *state purity*. Pure states have the largest possible purity equal to 1 (when only one p_i is 1, and all others are 0). Mixed states have purity smaller than 1. The minimum purity is attained for the completely mixed state when all p_i are the same and equal to $\frac{1}{N}$ with N the state dimensionality. (For n qubits, we have $N = 2^n$.) Then $\mathrm{Tr}[\rho^2] = \sum_{i=1}^{N} (\frac{1}{N})^2 = \frac{1}{N}$.

Table 7.1 summarizes some important information regarding pure and mixed states.

Exercise 7.1 Compute the mixed state ρ_z for an ensemble where state $|0\rangle$ is produced with probability 1/2, and state $|1\rangle$ is produced with probability 1/2. Then compute the mixed state ρ_x for an ensemble where state $|+\rangle$ is produced with probability 1/2, and state $|-\rangle$ is produced with probability 1/2. Calculate the state purities. ■

Solution:

$$\rho_z = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \tfrac{1}{2}\begin{pmatrix}1&0\\0&0\end{pmatrix} + \tfrac{1}{2}\begin{pmatrix}0&0\\0&1\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \tfrac{1}{2}\mathbb{1}, \tag{7.18}$$

$$\rho_x = \tfrac{1}{2}|+\rangle\langle +| + \tfrac{1}{2}|-\rangle\langle -| = \tfrac{1}{4}\begin{pmatrix}1&1\\1&1\end{pmatrix} + \tfrac{1}{4}\begin{pmatrix}1&-1\\-1&1\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \tfrac{1}{2}\mathbb{1}, \tag{7.19}$$

$$\mathrm{Tr}[\rho_z^2] = \mathrm{Tr}[\rho_x^2] = \mathrm{Tr}[(\tfrac{1}{2}\mathbb{1})^2] = \tfrac{1}{4}\mathrm{Tr}[\mathbb{1}] = \tfrac{1}{2}. \tag{7.20}$$

This exercise shows us an important property of density matrices. Two different ensembles can lead to the same mixed state. In the example above, both ensembles are in fact completely mixed and lead to (half) the identity matrix. The attained state purity is the minimum possible, namely 1 divided by the state dimensionality.

Exercise 7.2 Let us revist Eq. (5.32) in the teleportation protocol. If Bob does not get the information of Alice's Bell state measurement via a classical communication channel, he is in fact left with a statistical mixture of the four states $\alpha|0\rangle+\beta|1\rangle$, $\alpha|0\rangle-\beta|1\rangle$, $\alpha|1\rangle+\beta|0\rangle$, and $\alpha|1\rangle-\beta|0\rangle$, each with probability 1/4. Show that Bob's density matrix is completely mixed (which reflects that, in teleportation, no information is communicated faster than the speed of light). ∎

Solution:

$$\begin{aligned}\rho &= \frac{1}{4}\left[\begin{pmatrix}\alpha\\\beta\end{pmatrix}(\bar\alpha\ \ \bar\beta) + \begin{pmatrix}\alpha\\-\beta\end{pmatrix}(\bar\alpha\ \ -\bar\beta) + \begin{pmatrix}\beta\\\alpha\end{pmatrix}(\bar\beta\ \ \bar\alpha) + \begin{pmatrix}-\beta\\\alpha\end{pmatrix}(-\bar\beta\ \ \bar\alpha)\right]\\ &= \frac{1}{4}\left[\begin{pmatrix}|\alpha|^2 & \alpha\bar\beta\\ \bar\alpha\beta & |\beta|^2\end{pmatrix} + \begin{pmatrix}|\alpha|^2 & -\alpha\bar\beta\\ -\bar\alpha\beta & |\beta|^2\end{pmatrix} + \begin{pmatrix}|\beta|^2 & \bar\alpha\beta\\ \alpha\bar\beta & |\alpha|^2\end{pmatrix} + \begin{pmatrix}|\beta|^2 & -\bar\alpha\beta\\ -\alpha\bar\beta & |\alpha|^2\end{pmatrix}\right]\\ &= \frac{1}{4}\begin{pmatrix}2|\alpha|^2+2|\beta|^2 & 0\\ 0 & 2|\alpha|^2+2|\beta|^2\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix} = \frac{1}{2}\mathbb{1}.\end{aligned} \tag{7.21}$$

Exercise 7.3 Compute the equal-weight mixture of the four Bell states. ∎

Solution: Blackboard or homework. The result is the fully mixed two-qubit state $\rho = \frac{1}{4}\mathrm{diag}(1,1,1,1) = \frac{1}{4}\mathbb{1}_4$.

7.3 The Bloch Sphere

As we know already, pure single-qubit states lie on the surface of the Bloch sphere. For mixed single-qubit states, there is an equally nice geometric representation, namely that they live in the interior of the Bloch sphere (technically, the Bloch ball). Mathematically, any qubit density matrix ρ can be expanded into the identity and the vector of Pauli matrices, called the Pauli vector $\vec{S} = (X,Y,Z)^T$:

$$\begin{aligned}\rho &= \frac{1}{2}\left[\mathbb{1} + \vec{a}\cdot\vec{S}\right] = \frac{1}{2}\left[\mathbb{1} + a_x X + a_y Y + a_z Z\right]\\ &= \frac{1}{2}\left[\begin{pmatrix}1&0\\0&1\end{pmatrix} + a_x\begin{pmatrix}0&1\\1&0\end{pmatrix} + a_y\begin{pmatrix}0&-i\\i&0\end{pmatrix} + a_z\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right]\\ &= \frac{1}{2}\begin{pmatrix}1+a_z & a_x - i a_y\\ a_x + i a_y & 1-a_z\end{pmatrix}.\end{aligned} \tag{7.22}$$

Here, $\vec{a} = (a_x, a_y, a_z)^T$ is the so-called Bloch vector, which indicates the point within (or on) the sphere that corresponds to the mixed state ρ. Pure states have radius $|\vec{a}| = 1$ (surface of the sphere), while mixed states have $|\vec{a}| < 1$ (interior of the sphere). The center of the Bloch sphere at $\vec{a} = (0,0,0)^T$ corresponds to the fully mixed state.

Exercise 7.4 Compute the three states for the Bloch vectors $\vec{a}_0 = (0,0,0)^T$, $\vec{a}_1 = (1,0,0)^T$, $\vec{a}_2 = (0,1,0)^T$, and $\vec{a}_3 = (0,0,1)^T$. ■

Solution:

$$\rho_0 = \frac{1}{2}\left[\mathbb{1} + \vec{a}_0 \cdot \vec{S}\right] = \frac{1}{2}\mathbb{1}, \tag{7.23}$$

$$\begin{aligned}\rho_1 &= \frac{1}{2}\left[\mathbb{1} + \vec{a}_1 \cdot \vec{S}\right] = \frac{1}{2}[\mathbb{1} + X] \\ &= \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = |+\rangle\langle +|,\end{aligned} \tag{7.24}$$

$$\begin{aligned}\rho_2 &= \frac{1}{2}\left[\mathbb{1} + \vec{a}_2 \cdot \vec{S}\right] = \frac{1}{2}[\mathbb{1} + Y] \\ &= \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}\right] = \frac{1}{2}\begin{pmatrix}1 & -i\\ i & 1\end{pmatrix} = |R\rangle\langle R|,\end{aligned} \tag{7.25}$$

$$\begin{aligned}\rho_3 &= \frac{1}{2}\left[\mathbb{1} + \vec{a}_3 \cdot \vec{S}\right] = \frac{1}{2}[\mathbb{1} + Z] \\ &= \frac{1}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} = |0\rangle\langle 0|.\end{aligned} \tag{7.26}$$

Exercise 7.5 Compute the state purity of a mixed qubit state with Bloch vector $\vec{a}$. ■

Solution: We first note (1) that the Pauli matrices are traceless, (2) that squares of Pauli matrices are the identity, and (3) that two different Pauli matrices anti-commute and that their product is proportional to the other third Pauli matrix:

$$\mathrm{Tr}[X] = \mathrm{Tr}[Y] = \mathrm{Tr}[Z] = 0, \tag{7.27}$$

$$X^2 = Y^2 = Z^2 = \mathbb{1}, \tag{7.28}$$

$$XY = -YX = iZ, \tag{7.29}$$

$$YZ = -ZY = iX, \tag{7.30}$$

$$ZX = -XZ = iY. \tag{7.31}$$

Let us then also compute:

$$\begin{aligned}(\vec{a}\vec{S})^2 &= (a_x X + a_y Y + a_z Z)^2 \\ &= [a_x^2 X^2 + a_y^2 Y^2 + a_z^2 Z^2 + a_x a_y (XY + YX) + a_y a_z (YZ + ZY) + a_z a_x (ZX + XZ)] \\ &= |\vec{a}|^2 \mathbb{1}.\end{aligned} \tag{7.32}$$

Then, we can calculate the purity as follows:

$$\begin{aligned}\mathrm{Tr}[\rho^2] &= \mathrm{Tr}[\tfrac{1}{2}(\mathbb{1} + \vec{a}\vec{S})^2] = \tfrac{1}{4}\mathrm{Tr}[(\mathbb{1} + \vec{a}\vec{S})(\mathbb{1} + \vec{a}\vec{S})] \\ &= \tfrac{1}{4}\mathrm{Tr}[\mathbb{1} + 2\vec{a}\vec{S} + (\vec{a}\vec{S})^2] = \tfrac{1}{4}\mathrm{Tr}[\mathbb{1} + |\vec{a}|^2\mathbb{1}] = \tfrac{1}{4}(1 + |\vec{a}|^2)\mathrm{Tr}[\mathbb{1}]\end{aligned}$$

$$= \tfrac{1}{2}(1+|\vec{a}|^2). \tag{7.33}$$

In the second line, we used the tracelessness of Pauli operators, $\mathrm{Tr}[\vec{a}\,\vec{S}] = 0$. Pure states have $|\vec{a}| = 1$ and purity 1. Mixed states have purity smaller than 1. The fully mixed state with $|\vec{a}| = 0$ has purity $\frac{1}{2}$.

7.4 Measurements

Let us now discuss measurements. We remind ourselves: In the case of a given pure state $|\psi\rangle$, the probability p to find some state $|\phi\rangle$ is given by

$$p_\phi = |\langle\phi|\psi\rangle|^2 = \langle\psi|\phi\rangle\langle\phi|\psi\rangle. \tag{7.34}$$

Let us denote by $P_\phi = |\phi\rangle\langle\phi|$ the *observable* corresponding to state $|\phi\rangle$, i.e. the projection operator (matrix) onto state $|\phi\rangle$. Then, we can rewrite the equation above as

$$p_\phi = \langle\psi|P_\phi|\psi\rangle. \tag{7.35}$$

E.g., projecting onto $P_\phi = |0\rangle\langle 0|$ would be a measurement (in the computational basis), asking for the probability of observing the $|0\rangle$ state. Projectors are idempotent, i.e. $P^2 = P$.

We can make this a little bit more general and define a measurement operator A as sum over projectors

$$A = \sum_i a_i P_i, \tag{7.36}$$

where the a_i are the corresponding measurement outcomes. In general, A is not a projector anymore, i.e. $A^2 \neq A$. The *expectation value* of the observable A is still computed in the same way as in (7.35):

$$\langle A\rangle = \langle\psi|A|\psi\rangle. \tag{7.37}$$

For instance, $A = |0\rangle\langle 0| - |1\rangle\langle 1|$ would be a measurement in the computational basis where the state $|0\rangle$ corresponds to outcome $+1$ and the state $|1\rangle$ corresponds to outcome -1. For every state, the expectation value would be value between -1 and $+1$.

For a mixed state $\rho = \sum_{i=1}^N p_i\,|\psi_i\rangle\langle\psi_i|$, the expectation value is computed as follows:

$$\begin{aligned}\langle A\rangle &= \sum_{i=1}^N p_i\,\langle\psi_i|A|\psi_i\rangle = \sum_{i=1}^N p_i\,\mathrm{Tr}[\langle\psi_i|A|\psi_i\rangle] \\ &= \mathrm{Tr}\Big[\sum_{i=1}^N p_i\,|\psi_i\rangle\langle\psi_i|A\Big] = \mathrm{Tr}[\rho A].\end{aligned} \tag{7.38}$$

Here we have used that (1) a trace of a number is that number, (2) the trace is linear, and (3) the trace is cyclic.

If – when measuring observable A in state ρ – the measurement outcome a_i was found, the post-measurement density matrix has the form

$$\rho_i' = \frac{P_i\,\rho\,P_i}{\mathrm{Tr}[\rho\,P_i]} = \frac{P_i\,\rho\,P_i}{\mathrm{Tr}[P_i\,\rho\,P_i]}. \tag{7.39}$$

The denominators are the same since the trace is cyclic and projection operators are idempotent.

Exercise 7.6 Compute the expectation value of $A = |0\rangle\langle 0| - |1\rangle\langle 1|$ in the state $\rho = \frac{1}{4}|0\rangle\langle 0| + \frac{3}{4}|1\rangle\langle 1|$. Assume that outcome -1 is obtained. Calculate the post-measurement state using Eq. (7.39). ∎

Solution:

$$\langle A\rangle = \mathrm{Tr}[\rho A] = \mathrm{Tr}\left[\begin{pmatrix}\frac{1}{4} & 0\\ 0 & \frac{3}{4}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right] = \mathrm{Tr}\left[\begin{pmatrix}\frac{1}{4} & 0\\ 0 & -\frac{3}{4}\end{pmatrix}\right] = -\tfrac{1}{2}. \tag{7.40}$$

With probability $\frac{1}{4}$ outcome $+1$ is obtained, and with probability $\frac{3}{4}$ outcome -1 is obtained. Hence, the expectation value is $\frac{1}{4}(+1) + \frac{3}{4}(-1) = -\frac{1}{2}$. Given the outcome -1, the post-measurement state is

$$\begin{aligned}\rho_i' &= \frac{P_i\rho P_i}{\mathrm{Tr}[P_i\rho P_i]} = \frac{1}{\mathrm{Tr}[P_i\rho P_i]}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}\frac{1}{4} & 0\\ 0 & \frac{3}{4}\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\\ &= \frac{1}{\mathrm{Tr}[P_i\rho P_i]}\begin{pmatrix}0 & 0\\ 0 & \frac{3}{4}\end{pmatrix}\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = \frac{1}{\mathrm{Tr}[P_i\rho P_i]}\begin{pmatrix}0 & 0\\ 0 & \frac{3}{4}\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix} = |1\rangle\langle 1|,\end{aligned} \tag{7.41}$$

as it should be, by definition, given the measurement result.

7.5 Entanglement of Mixed States

In the case of pure states, we distinguished between product states and entangled states. The situation is very similar in the case of mixed states.

Consider the bipartite case of two systems A and B. We call their joint state ρ_{AB} *separable* if and only if it can be written as a mixture of product states:

$$\rho_{AB}^{\mathrm{sep}} = \sum_{i=1}^{N} p_i \rho_A^{(i)} \otimes \rho_B^{(i)}. \tag{7.42}$$

This state is produced by a source which emits an ensemble of product states, i.e. with probability p_i it emits the product state $\rho_A^{(i)} \otimes \rho_B^{(i)}$.

A state is entangled if and only if it is not separable, i.e. if only if it cannot be written in the above form:

$$\rho_{AB}^{\mathrm{ent}} \neq \sum_{i=1}^{N} p_i \rho_A^{(i)} \otimes \rho_B^{(i)}. \tag{7.43}$$

It is highly non-trivial, in general, to decide for a given density matrix whether it is entangled or not. In fact, this is believed to be an NP-hard problem.

Exercise 7.7 Is the two-qubit state

$$\rho_{AB} = \begin{pmatrix}\frac{1}{4} & \frac{1}{4} & 0 & 0\\ \frac{1}{4} & \frac{1}{2} & 0 & -\frac{1}{4}\\ 0 & 0 & 0 & 0\\ 0 & -\frac{1}{4} & 0 & \frac{1}{4}\end{pmatrix} \tag{7.44}$$

entangled? ∎

Solution: No, it is separable: $\rho_{AB} = \frac{1}{2}|0\rangle_A\langle 0| \otimes |+\rangle_B\langle +| + \frac{1}{2}|-\rangle_A\langle -| \otimes |1\rangle_B\langle 1|$. Note: There is no easy way to find this solution. This exercise was reverse-engineered.

7.6 Reduced States

Assume we are given a state ρ_{AB} of two quantum systems A and B. What is the state ρ_A of system A alone, i.e. when ignoring system B? The answer to this question is obtained by performing the *partial trace* over system B:

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB}. \tag{7.45}$$

The trace is obtained by summing over B's basis states. In the case of qubits, we have

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \sum_{b=0,1} \langle b|\rho_{AB}|b\rangle. \tag{7.46}$$

Here, the notation is a bit lazy. In full notation, we would have to write: $\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \sum_{b=0,1} (1_a \otimes \langle b|_B)\, \rho_{AB}\, (1_A \otimes |b\rangle_B)$.

If the initial state ρ_{AB} is separable, we get

$$\begin{aligned}\rho_A = \mathrm{Tr}_B\, \rho_{AB} &= \sum_{i=1}^{N} \sum_{b=0,1} p_i\, (1_A \otimes \langle b|_B)\, (\rho_A^i \otimes \rho_B^i)\, (1_A \otimes |b\rangle_B) \\ &= \sum_{i=1}^{N} \sum_{b=0,1} p_i\, (1\, \rho_A^i\, 1) \otimes \langle b|_B \rho_B^i |b\rangle_B = \sum_{i=1}^{N} p_i\, \rho_A^i\, \mathrm{Tr}[\rho_B^i].\end{aligned}$$

If the initial state is entangled, the partial trace can only be calculated via (7.46).

The reduced density matrix $\rho_A = \mathrm{Tr}_B\, \rho_{AB}$ allows Alice to compute all her measurement results (probabilities). Similarly, Bob's state is $\rho_B = \mathrm{Tr}_A\, \rho_{AB}$. Given three parties A, B, C, the reduced state of A and B is $\rho_{AB} = \mathrm{Tr}_C\, \rho_{ABC}$. The reduced state of only A is then $\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \mathrm{Tr}_B \mathrm{Tr}_C\, \rho_{ABC}$.

Exercise 7.8 You are given the following states:

$$(1)\ \ \rho_{AB} = \tfrac{3}{4}|01\rangle\langle 01| + \tfrac{1}{4}|10\rangle\langle 10|, \tag{7.47}$$

$$(2)\ \ \rho_{AB} = |\Psi^-\rangle\langle\Psi^-|, \tag{7.48}$$

$$(3)\ \ \rho_{ABC} = |\mathrm{GHZ}\rangle\langle \mathrm{GHZ}|. \tag{7.49}$$

For (1) and (2), compute the reduced state of system A. For (3), compute the reduced state of systems AB. ■

Solution:

$$\begin{aligned}(1)\ \ \rho_A = \mathrm{Tr}_B\, \rho_{AB} &= \sum_{b=0,1} \langle b|_B \left(\tfrac{3}{4}|01\rangle_{AB}\langle 01| + \tfrac{1}{4}|10\rangle_{AB}\langle 10|\right)|b\rangle_B \\ &= \tfrac{3}{4}|0\rangle_A\langle 0| + \tfrac{1}{4}|1\rangle_A\langle 1|, \qquad (7.50) \\ (2)\ \ \rho_A = \mathrm{Tr}_B\, \rho_{AB} &= \sum_{b=0,1} \langle b|_B \tfrac{1}{2}(|01\rangle_{AB} - |10\rangle_{AB})(\langle 01|_{AB} - \langle 10|_{AB})\, |b\rangle_B \\ &= \tfrac{1}{2} \sum_{b=0,1} \langle b|_B \left(|01\rangle_{AB}\langle 01| - |10\rangle_{AB}\langle 01| - |01\rangle_{AB}\langle 10| + |10\rangle_{AB}\langle 10|\right)|b\rangle_B\end{aligned}$$

$$= \tfrac{1}{2}\left(|0\rangle_A\langle 0| + |1\rangle_A\langle 1|\right) = \tfrac{1}{2}\,\mathbb{1}_A, \tag{7.51}$$

$$(3)\quad \rho_{AB} = \mathrm{Tr}_C\,\rho_{ABC} = \sum_{c=0,1} \langle c|_C \tfrac{1}{2}(|000\rangle_{ABC} + |111\rangle_{ABC})(\langle 000|_{ABC} + \langle 111|_{ABC})\,|c\rangle_C$$

$$= \tfrac{1}{2}\left(|00\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\right). \tag{7.52}$$

The last two examples are noteworthy: (2) If Alice and Bob share a Bell state, then the reduced state of Alice's qubit is just the fully mixed state. Her local qubit has no individual properties, i.e. her local measurement results are completely random in all bases. (3) If Alice, Bob, and Charlie share a GHZ state, and if Charlie's qubit is ignored or inaccessible, then Alice and Bob have to describe their reduced two-qubit state with the reduced density matrix. All of Alice's and Bob's measurement results can be computed from it. This is a 50:50 mixture of both qubits being 0 or both qubits being 1. That is a separable state, i.e. there is no entanglement anymore. (This is the reason why an eavesdropper cannot use a GHZ state to crack the E91 protocol. The reduced density matrix of Alice and Bob won't allow to violate the CHSH inequality.)

7.7 Decoherence

We are now equipped with the mathematical tools to develop a rudimentary and simplified picture of quantum decoherence. It is the main reason why we do not see quantum effects around us in the everyday macroscopic classical world. Decoherence offers a *partial* partial solution to the measurement problem in the sense that it shows how constant unitary interaction of a quantum system with its environment can have similar effects as what measurements are doing.

Let us consider the case of a generalized GHZ state of n qubits, where n can be thought of being macroscopically large ($n \sim 10^{23}$):

$$|\mathrm{GHZ}\rangle_S = \tfrac{1}{\sqrt{2}}\left(|00\ldots0\rangle_S + |11\ldots1\rangle_S\right), \tag{7.53}$$

where S stands for "System". This is a Schrödinger cat-like state. Now let us assume that our cat interacts with one single photon in initial state $|0\rangle_E$ from its environment (E) in a CNOT like manner, where some qubit it the cat (the one which is hit by the photon) is the control and the photon is the target. The resulting joint cat-photon state reads:

$$\begin{aligned}|\Psi\rangle_{SE} &= \mathrm{CNOT}\,|\mathrm{GHZ}\rangle_S|0\rangle_E \\ &= \mathrm{CNOT}\,\tfrac{1}{\sqrt{2}}\left(|00\ldots0\rangle_S + |11\ldots1\rangle_S\right)|0\rangle_E \\ &= \tfrac{1}{\sqrt{2}}\left(|00\ldots0\rangle_S|0\rangle_E + |11\ldots1\rangle_S|1\rangle_E\right).\end{aligned} \tag{7.54}$$

This is still a very precious pure and entangled quantum state. Let us introduce the shortcuts

$$|00\ldots0\rangle_S = |\mathrm{d}\rangle_S, \tag{7.55}$$

$$|11\ldots1\rangle_S = |\mathrm{a}\rangle_S, \tag{7.56}$$

where "d" ("a") stands for "dead" ("alive"). The density matrix of both the cat and the photon reads:

$$\begin{aligned}\rho_{SE} &= |\Psi\rangle_{SE}\langle\Psi| \\ &= \tfrac{1}{2}\left(|\mathrm{d}\rangle_S|0\rangle_E + |\mathrm{a}\rangle_S|1\rangle_E\right)\left(\langle\mathrm{d}|_S\langle 0|_E + \langle\mathrm{a}|_S\langle 1|_E\right)\end{aligned}$$

$$= \tfrac{1}{2}\big(|\mathrm{d}\rangle_S\langle\mathrm{d}|\otimes|0\rangle_E\langle 0| + |\mathrm{a}\rangle_S\langle\mathrm{d}|\otimes|1\rangle_E\langle 0| + |\mathrm{d}\rangle_S\langle\mathrm{a}|\otimes|0\rangle_E\langle 1| + |\mathrm{a}\rangle_S\langle\mathrm{a}|\otimes|1\rangle_E\langle 1|\big). \tag{7.57}$$

Now let us – very reasonably – assume that the photon escapes with the speed of light and that we will never be able again to extract information out of it. This implies that the correct description of our cat, ρ_S, will be the reduced density matrix:

$$\begin{aligned}\rho_S &= \mathrm{Tr}_E[\rho_{SE}] \\ &= \sum_{b=0,1} \langle b|_E \Psi\rangle_{SE}\langle\Psi|b\rangle_E \\ &= \tfrac{1}{2}\big(|\mathrm{d}\rangle_S\langle\mathrm{d}| + |\mathrm{a}\rangle_S\langle\mathrm{a}|\big).\end{aligned} \tag{7.58}$$

Only the diagonal terms survive and we end up with a "boring" classical 50:50 mixture of the cat being dead and alive without any entanglement or interesting (quantum) features. This is what one single photon can do to a Schrödinger cat in the fraction of a second.

Note that, given the state (7.54), one could – in theory – restore the Schrödinger cat by "finding" the photon and projecting it onto the diagonal basis state $(|0\rangle_E + |1\rangle_E)/\sqrt{2}$. But don't forget: The environment of our every-day world consists not only of one photon but of a myriad of them. So, in practise, there is no way to save the Schrödinger cat unless you create a a completely controlled laboratory situation, totally isolating it from its environment by putting it in a box near absolute zero temperature in an almost perfect vacuum.

8. Entropy and Information

8.1 Shannon Entropy

The concept of entropy plays a fundamental role in both classical and quantum information theory. It is a measure of the uncertainty in the description of a physical system. Vice versa, it quantifies the information we gain, on average, when we learn the state of the system.

Let us consider a discrete random variable X. The values x of the random variable could be "heads" and "tails" for a coin, or "0" and "1" for a bit, or the numbers 1 to 6 for a die. However, these labels are not important. What does matter are the probabilities $p_1, p_2, \ldots, p_N$, where $\sum_{i=1}^{N} p_i = 1$, for these, in general, N possible events to happen. The *Shannon entropy* is a function only of these probabilities:

$$H(X) \equiv H(p_1, p_2, \ldots, p_N) \equiv H(p) \equiv -\sum_{i=1}^{N} p_i \log p_i. \tag{8.1}$$

Here, $p = (p_1, p_2, \ldots, p_N)$ denotes the probability distribution of the N possible events. The choice of basis for the logarithm depends on the field of application. In physics, one typically uses the natural logarithm. In computer science, base 2 ist commonly used and gives the unit of bits. For the case of $p_i = 0$, we note that $\lim_{p_i \to 0} p_i \log p_i = 0$.

Assume you have a source which produces a string $X_1, X_2, X_3, \ldots$ of independent and identically distributed random variables. What are the minimal physical resources to store the information produced by the source? *Shannon's noiseless coding theorem* states that one requires $H(X)$ bits per symbol.

So, loosely speaking and in summary: The Shannon entropy of a distribution measures "prior uncertainty of state" = "information gain upon measurement" = "minimal storage requirement".

The Shannon entropy has the following properties:

- Non-negative: $H(p_1, p_2, \ldots, p_N) \geq 0$. Equality holds if and only if all $p_i = 0$ except for one which equals 1, corresponding to a distribution with perfect certainty.
- Upper-bounded: $H(p_1, p_2, \ldots, p_N) \leq \log N$. Equality is attained for the uniform distribution $p_i = \frac{1}{N}$ for all i.

- Concave: Given two distributions $p = (p_1, p_2, \ldots, p_N)$ and $q = (q_1, q_2, \ldots, q_N)$ and a mixing parameter $\alpha \in [0,1]$, the Shannon entropy of the mixture is larger than or equal to the mixture of entropies: $H(\alpha p + (1-\alpha)q) \geq \alpha H(p) + (1-\alpha)H(q)$.

Exercise 8.1 A source produces a string of symbols, where the four possible symbols are A, B, C, and D. The probabilities are: $p_A = \frac{1}{2}$, $p_B = \frac{1}{4}$, and $p_C = p_D = \frac{1}{8}$. What is the optimal compression method into bits? ∎

Solution: Straightforwardly, we could encode A $\to$ 00, B $\to$ 01, $C \to$ 10, and D $\to$ 11. This requires 2 bits per symbol and is a good first attempt. We could then try to compress better and use shorter bit strings for the more frequent symbols, for instance: A $\to$ 0, B $\to$ 1, $C \to$ 00, and D $\to$ 01. However, this is not a valid solution due to lack of uniqueness, as e.g. the bit string "0000" could stem from the symbol string "AAAA" or from "CC". A clever and unique encoding looks like this:

$$\text{A} \to 0, \quad \text{B} \to 10, \quad C \to 110, \quad \text{D} \to 111. \tag{8.2}$$

On average, this requires $\frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 + \frac{1}{8}\cdot 3 + \frac{1}{8}\cdot 3 = \frac{7}{4}$ bits per symbol. This is indeed optimal as it matches the Shannon entropy of the source, $H(X) = -\frac{1}{2}\log\frac{1}{2} - \frac{1}{4}\log\frac{1}{4} - \frac{1}{8}\log\frac{1}{8} - \frac{1}{8}\log\frac{1}{8} = \frac{7}{4}$.

8.2 Von Neumann Entropy

The *von Neumann entropy* S is a measure for the mixedness of a quantum state, similar to the purity. For a quantum state ρ it is defined as

$$S(\rho) \equiv \text{Tr}[\rho \log \rho]. \tag{8.3}$$

The logarithm of a matrix is usually computed via diagonalization. Given the density matrix in its eigenbasis, $\rho = \sum_{i=1}^{N} \lambda_i |v_i\rangle\langle v_i|$ with λ_i the eigenvectors and $|v_i\rangle$ the eigenvectors, the von Neumann entropy can be written as

$$S(\rho) = -\sum_{i=1}^{N} \lambda_i \log \lambda_i. \tag{8.4}$$

The von Neumann entropy has the following properties:

- Non-negative: $S(\rho) \geq 0$. Equality holds if ρ is a rank-1 projector, i.e. all eigenvalues are 0 except for one which equals 1, corresponding to pure states.
- Upper-bounded: $S(\rho) \leq \log N$. Equality is attained for the fully mixed state $\rho = \frac{1}{N}\mathbb{1}$.
- Concave: The von Neumann entropy of a mixture of quantum states (with mixing probabilities p_i) is larger than or equal to the mixture of entropies, $S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i)$.

Exercise 8.2 Compute the von Neumann entropy of the fully mixed state of $n = 3$ qubits. ∎

Solution: The Hilbert space dimension is $N = 2^3 = 8$. The fully mixed state of three qubits is thus $\rho = \frac{1}{8}\mathbb{1}_8 = \sum_{i=1}^{8} \frac{1}{8}|v_i\rangle\langle v_i|$, where the $|v_i\rangle$ are the 8 computational basis states. The von Neumann entropy hence is

$$S(\tfrac{1}{8}\mathbb{1}_8) = -\sum_{i=1}^{8} \lambda_i \log \lambda_i = -8 \cdot \tfrac{1}{8} \cdot \log \tfrac{1}{8} = \log 8 = 3, \tag{8.5}$$

where we have used the logarithm with base 2 in the final step. This is the maximum attainable entropy for 3 qubits.

Exercise 8.3 Compute the von Neumann entropy of the pure state $|\psi\rangle$. ∎

Solution: The density matrix $|\psi\rangle\langle\psi|$ is a rank-1 projector with only one non-zero eigenvalue, and that eigenvalue is 1. Hence, the von Neumann entropy is

$$S(|\psi\rangle\langle\psi|) = -1\log 1 = 0. \tag{8.6}$$

8.3 Conditional Entropy

The conditional entropy quantifies the amount of information needed, on average, to describe the outcome of a random variable Y under the condition that the outcome of another (correlated) random variable X is known. It is defined as

$$H(Y|X) \equiv -\sum_x \sum_y p(x,y)\log\frac{p(x,y)}{p(x)}, \tag{8.7}$$

where x and y are the possible outcomes of the random variables X and Y, respectively.

The conditional entropy has the following properties:

- Non-negativity: $H(Y|X) \geq 0$.
- Minimum: $H(Y|X) = 0$ if and only if Y is completely determined by X. Then knowing X completely specifies Y and no more information is needed to decribe Y.
- Maximum: $H(Y|X) = H(Y)$ if and only if Y and X are independent random variables. Then knowing X does not give any information about Y, such that describing Y requires the full entropy of Y.
- Chain rule: $H(X,Y) = H(Y|X) + H(X)$. One needs $H(X,Y)$ bits to describe the joint state of both random variables. If we first learn X, we gain $H(X)$ bits of information. Then we need only $H(Y|X)$ bits to learn the full state. Similarly, $H(X,Y) = H(X|Y) + H(Y)$.

Figure 8.1 shows the relationship between the individual entropies $H(X)$ and $H(Y)$, the conditional entropies $H(X|Y)$ and $H(Y|X)$, the joint entropy $H(X,Y)$, and the mutual information $I(X;Y) = H(X) + H(Y) - H(X,Y)$. The latter is the Kullback-Leibler divergence (which is also called relative entropy) between the joint distribution and the product of individuals: $I(X;Y) = D_{\mathrm{KL}}(P_{(X,Y)}||P_X P_Y)$. The mutual information is the price to pay for encoding (X,Y) as a pair of independent random variables when in fact they are dependent.

Exercise 8.4 Consider two *correlated* random variables $X \in \{0,1\}$ and $Y \in \{0,1\}$, representing two coin tosses. The joint distribution reads:

$X \setminus Y$	0	1
0	0.45	0.00
1	0.05	0.50

Compute the conditional entropy $H(Y|X)$. ∎

Solution: The joint entropy is $H(X,Y) = -\sum_x \sum_y p(x,y)\log p(x,y)$, i.e. $-0.45\log 0.45 - 0.05\log 0.05 - 0.50\log 0.50 \approx 1.23$. The probabilities for X are $p(x=0) = 0.45$ and $p(x=1) = 0.55$. Hence, the entropy for X is $H(X) = -0.45\log 0.45 - 0.55\log 0.55 \approx 0.99$. Therefore, the conditional entropy of Y given X is $H(Y|X) = H(X,Y) - H(X) \approx 0.24$.

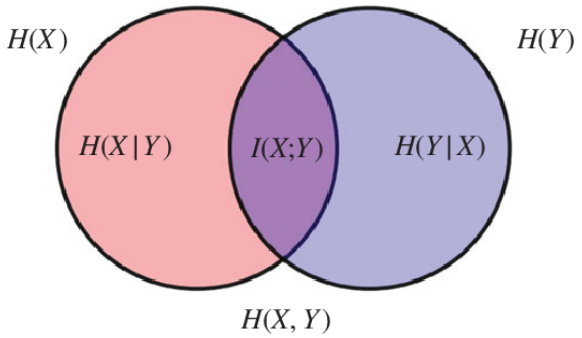

Figure 8.1: Venn diagram displaying information measures associated with correlated variables X and Y. The left circle (red and violet area) is the individual entropy $H(X)$. The right circle (blue and violet area) is the individual entropy $H(Y)$. The total area (red and violet and blue) is the joint entropy $H(X,Y)$. The (red) area contained in the left but not the right circle is the conditional entropy $H(X|Y)$. Similarly, the (blue) area contained in the right but not the left circle is the is the conditional entropy $H(Y|X)$. The violet intersection is the mutual information $I(X;Y)$. Picture adapted from Wikipedia.

Intuition: X and Y are quite correlated and likely to show the same outcome. If you learn the value of X, you only need to learn, on average, 0.24 additional bits to also know Y.

8.4 Conditional Quantum Entropy

The conditional quantum entropy is the quantum generalization of the classical conditional entropy. Given a bipartite quantum state ρ_{AB}, the entropy of the joint system is the von Neumann entropy $S(AB) = S(\rho_{AB})$. The entropies of the subsystems are $S(A) = S(\rho_A) = S(\mathrm{Tr}_B \rho_{AB})$ and $S(B) = S(\rho_B) = S(\mathrm{Tr}_A \rho_{AB})$. The quantum conditional entropy is defined as

$$S(A|B) \equiv S(AB) - S(B) = S(\rho_{AB}) - S(\rho_B). \tag{8.8}$$

Remarkably, the quantum conditional entropy can be negative, unlike the classical conditional entropy, which is always non-negative. The negative conditional entropy measures the additional number of bits above the classical limit which can be transmitted in a superdense coding protocol. If the quantum conditional entropy is positive, it implies that state cannot reach the classical limit.

Exercise 8.5 Compute the conditional quantum entropy of the Bell state $|\Psi^-\rangle$. ∎

Solution: The Bell state is pure, so its von Neumann entropy is $S(\rho_{AB}) = 0$. The reduced state of Bob's qubit is the fully mixed state, so its entropy is the logarithm of the dimension of Bob's Hilbert space, i.e. $S(\rho_B) = \log 2 = 1$. Therefore, the conditional quantum entropy is $S(A|B) = S(\rho_{AB}) - S(\rho_B) = -1$. This implies, correctly, that in superdense coding 1 bit more than the classical limit (which is 1 transmitted bit), i.e. 2 bits in total can be communicated using the Bell state as a resource.

9. Quantum Sensing

Strongly linked to quantum information science is the field of quantum sensing. Applications of quantum sensing are quantum metrology – the study of making high-resolution measurements of physical parameters using quantum theory – and quantum imaging – the study of imaging objects with a resolution that is beyond what is possible in classical optics.

9.1 Standard Quantum Limit and Heisenberg Limit

Classical physics and classical electromagnetism cannot overcome the so-called *standard quantum limit* (SQL), often called *shot-noise limit* (SNL). It poses a fundamental bound on the precision of measurements when only "classical" states, i.e. separable quantum states are used.

Consider a Mach-Zehnder interferometer which has a phase shift ϕ in one of its arms. Classical interferometry uses (classical) laser light. If the light beam has, on average, n photons, the SQL bounds the achievable resolution in estimating the phase ϕ. Concretely, the SQL bounds the minimal variance of the parameter estimator:

$$(\Delta\phi)^2_{\mathrm{SQL}} \geq \frac{1}{n}. \tag{9.1}$$

Using entangled states of light with n photons, this limit can be broken, and a much better precision further down to the so-called *Heisenberg limit* (HL) can be achieved:

$$(\Delta\phi)^2_{\mathrm{HL}} \geq \frac{1}{n^2}. \tag{9.2}$$

Such quantum enhancement with (non-classical) "squeezed" light is, e.g., used in the LIGO gravitational wave observatory.

9.2 The Fundamental Task of Quantum Metrology

In the following, we will discuss this fundamental task of quantum metrology in more detail, namely estimating the unknown phase ϕ of a unitary operator

$$U(\phi) = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}. \tag{9.3}$$

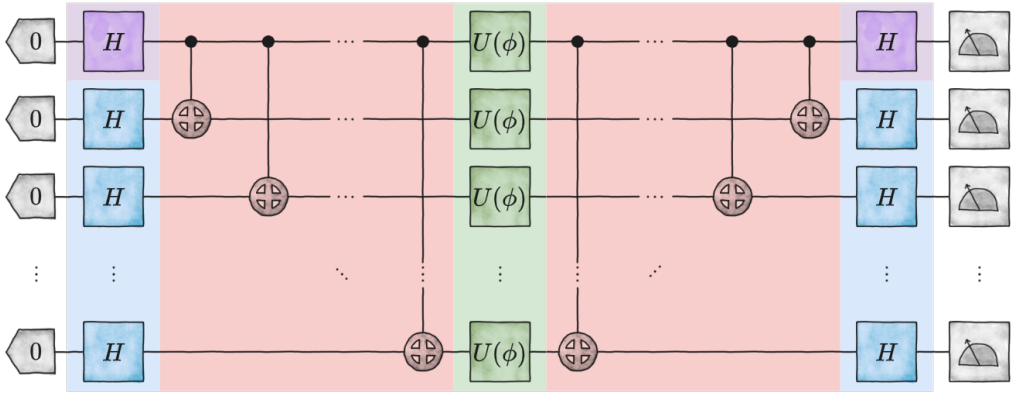

Figure 9.1: Quantum phase estimation. Read from left to right. We initialize n qubits in the computational basis product state $|00\ldots0\rangle$. (1) In the protocol without entanglement, everything except the red part is implemented. All qubits are subject to a Hadamard gate H, the unitary phase gate $U(\phi)$, again a Hadamard H, and a final measurement in the computational basis. (2) In the protocol with entanglement, everything except the blue part is implemented. The violet and red parts uses a single Hadamard as well as a sequence of CNOTs to create a GHZ state and, after the phase gates, undoes it before measurement. Circuit designed using the "Quantum Circuit Library", `https://github.com/wilkensJ/drawio-library`.

Figure 9.1 illustrates our setup. Let us first calculate the separable case without entanglement, where everything except the red part is applied. In the input state, all n qubits are initialized in state $|0\rangle$. Every qubit is subjected to a Hadamard gate. After the layer of phase gates, again every qubit is subjected to a Hadamard gate and a measurement in the computational basis. To read out phase information, we compute the probability to measure a "0" outcome in all n detectors:

$$\begin{aligned} p_{\text{sep}}(00\ldots0) &= |\langle 00\ldots0|H^{\otimes n}U(\phi)^{\otimes n}H^{\otimes n}|00\ldots0\rangle|^2 \\ &= |\langle ++\ldots+|U(\phi)^{\otimes n}|++\ldots+\rangle|^2 \\ &= |\langle +|U(\phi)|+\rangle^n|^2 \\ &= |[\tfrac{1}{2}(e^{i\phi}+e^{-i\phi})]^n|^2 \\ &= \cos^{2n}(\phi). \end{aligned} \tag{9.4}$$

To come from the third to the fourth line, we can use the vector notation: $\langle +|U(\phi)|+\rangle = \frac{1}{2}(1\ 1)\begin{pmatrix}\exp(i\phi) & 0\\ 0 & \exp(-i\phi)\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{2}(e^{i\phi}+e^{-i\phi})$.

Now let us compute the scenario where entanglement is used. The violet and red part creates a GHZ state. After the phase gates, the reverse sequence of gates with a measurement in the computational basis corresponds to a measurement of the GHZ state. To read out phase information, we again compute the probability to measure a "0" outcome in all n detectors:

$$\begin{aligned} p_{\text{ent}}(00\ldots0) &= |\langle \text{GHZ}|U(\phi)^{\otimes n}|\text{GHZ}\rangle|^2 \\ &= |\tfrac{1}{2}[\langle 00\ldots0|U(\phi)^{\otimes n}|00\ldots0\rangle + \langle 11\ldots1|U(\phi)^{\otimes n}|00\ldots0\rangle \end{aligned}$$

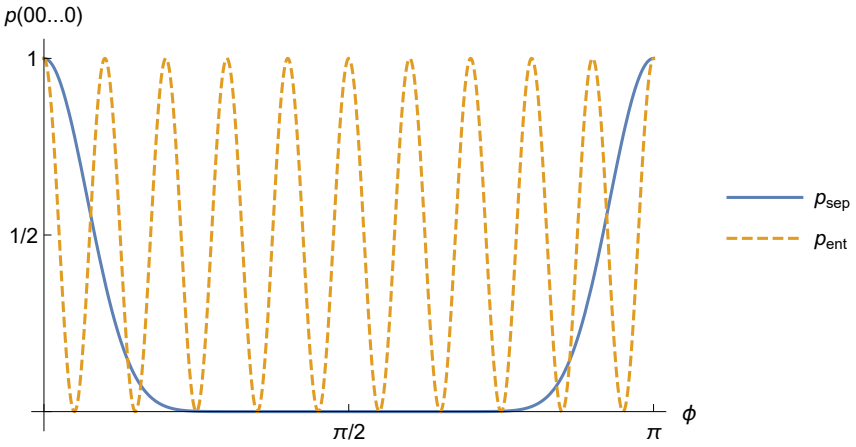

Figure 9.2: Comparison of the final output probability between the separable (p_{sep}) and the entangled (p_{ent}) scenario for the case of $n = 10$ qubits. In the entangled case, the probability oscillates n times faster and therefore, for small parameter ϕ, deviates from the value $p_{\text{sep}}(00\ldots0) = 1$ much faster than the separable one. This allows for a better estimation of the parameter.

$$
\begin{aligned}
&\quad + \langle 00\ldots0|U(\phi)^{\otimes n}|11\ldots1\rangle + \langle 11\ldots1|U(\phi)^{\otimes n}|11\ldots1\rangle]|^2 \\
&= |\tfrac{1}{2}[\langle 0|U(\phi)|0\rangle^n + 0 + 0 + \langle 1|U(\phi)|1\rangle^n]|^2 \\
&= |\tfrac{1}{2}[(e^{i\phi})^n + (e^{-i\phi})^n]|^2 \\
&= \cos^2(n\phi). \qquad (9.5)
\end{aligned}
$$

Figure 9.2 compares the probability for the separable and the entangled case.

In parameter estimation theory, the Cramér-Rao bound states that the variance of any unbiased estimator is at least the inverse Fisher information I_F. The latter is given by the negative (expected value of the) second derivative of the logarithm of the probability distribution. In our cases, to first order in ϕ (and without proof):

$$I_F(p_{\text{sep}}) = -\frac{\partial^2}{\partial\phi^2}\log p_{\text{sep}} = 2n, \qquad (9.6)$$

$$I_F(p_{\text{ent}}) = -\frac{\partial^2}{\partial\phi^2}\log p_{\text{ent}} = 2n^2. \qquad (9.7)$$

This gives us – except for a factor of 2, in complete analogy to the interferometer example from above – the standard quantum limit for the separable case and the Heisenberg limit for the entangled case:

$$(\Delta\phi)^2_{\text{sep}} \geq \frac{1}{I_F(p_{\text{sep}})} = \frac{1}{2n}, \qquad (9.8)$$

$$(\Delta\phi)^2_{\text{ent}} \geq \frac{1}{I_F(p_{\text{ent}})} = \frac{1}{2n^2}. \qquad (9.9)$$

For large n, one has $(\Delta\phi)^2_{\text{ent}} \ll (\Delta\phi)^2_{\text{sep}}$. Therefore, harnessing entanglement allows to estimate the unknown parameter ϕ to much better precision than with a classical device using only separable states. This is the core of quantum metrology.

Bibliography

Articles

[1] J.S. Bell. "On the Einstein Podolsky Rosen Paradox". In: *Physics Physique Fizika* 1 (1964), page 195. DOI: doi:10.1103/PhysicsPhysiqueFizika.1.195 (cited on page 42).

[2] C. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. Wootters. "Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels". In: *Physical Review Letters* 70 (1993), page 1895. DOI: doi:10.1103/PhysRevLett.70.1895 (cited on page 35).

[3] C. Bennett and S. Wiesner. "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". In: *Physical Review Letters* 69 (1992), page 2881. DOI: doi:10.1103/PhysRevLett.69.2881 (cited on page 33).

[4] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. "Experimental quantum teleportation". In: *Nature* 390 (1997), page 575. DOI: doi:10.1038/37539 (cited on pages 35, 36).

[5] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. "Bell nonlocality". In: *Reviews of Modern Physics* 86 (2014), page 419. DOI: https://doi.org/10.1103/RevModPhys.86.419 (cited on page 47).

[6] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. "Proposed experiment to test local hidden-variable theories". In: *Physical Review Letters* 23 (1969), page 880. DOI: doi:10.1103/PhysRevLett.23.880 (cited on page 43).

[7] A. Einstein, R. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47 (1935), page 777. DOI: https://doi.org/10.1103/PhysRev.47.777 (cited on page 41).

[8] A.K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical Review Letters* 67 (1991), page 661. DOI: https://doi.org/10.1103/PhysRevLett.67.661 (cited on page 48).

[9] "ESA explores the quantum world". In: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/ESA_explores_the_quantum_world (2004) (cited on page 28).

[10] "ESA observatory breaks world quantum teleportation record". In: https://www.esa.int/Enabling_Support/Space_Engineering_Technology/ESA_observatory_breaks_world_quantum_teleportation_record (2012) (cited on page 38).

[11] M. Giustina, M.A.M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M.W. Mitchell, J. Beyer, T. Gerrits, A.E. Lita, L.K. Shalm, S.W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". In: *Physical Review Letters* 115 (2015), page 250401. DOI: https://doi.org/10.1103/PhysRevLett.115.250401 (cited on page 46).

[12] X.S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger. "Quantum teleportation over 143 kilometres using active feed-forward". In: *Nature* 489 (2012), page 269. DOI: doi:10.1038/nature11472 (cited on page 38).

[13] "Quantum Repeaters". In: https://qt.eu/quantum-principles/communication/quantum-repeaters (2018) (cited on page 39).

[14] R. Scharf. "Schrödingers Katze erhellt das Quantenreich". In: *Frankfurter Allgemeine Zeitung* https://www.faz.net/aktuell/wissen/physik-mehr/die-seltsame-welt-der-atome-schroedingers-katze-erhellt-das-quantenreich-12529251.html (2013) (cited on page 13).

[15] W. Wootters and W. Zurek. "A Single Quantum Cannot be Cloned". In: *Nature* 299 (1982), page 802. DOI: doi:10.1038/299802a0 (cited on page 32).

[16] A. Zhukov, E. Kiktenko, A. Elistratov, W. Pogosov, and Y. Lozovik. "Quantum communication protocols as a benchmark for programmable quantum computers". In: *Quantum Information Processing* 18 (2019), page 31. DOI: doi:10.1007/s11128-018-2144-y (cited on page 34).

[17] M. Żukowski, A. Zeilinger, M.A. Horne, and A. K. Ekert. ""Event-Ready-Detectors" Bell Experiment via Entanglement Swapping". In: *Physical Review Letters* 71 (1993), page 4287. DOI: https://doi.org/10.1103/PhysRevLett.71.4287 (cited on pages 38, 39).

Books

[18] A. Aaronson. *Introduction to Quantum Information Science, Lecture Notes*. 2018 (cited on page 22).

[19] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. 10th Edition. Cambridge University Press, 2010 (cited on pages 11, 37).