Chapter 6
Entanglement

In this chapter, we will find out how we can apply quantum mechanics to more than one system. In doing so, we encounter what is truly strange in quantum mechanics, namely *entanglement*. We also explore some of the more shocking applications of quantum mechanics, including teleportation and quantum computing.

6.1 The State of Two Electrons

We have looked at thought experiments with a single photon in a Mach–Zehnder interferometer, a single electron in a Stern–Gerlach apparatus, and the interaction of a two-level atom with an optical pulse. We found that their states are all described by a two-dimensional complex vector, and the observables and evolution operators are described by 2×2 matrices. But what if we have *two* photons, or two electrons, or two atoms? Or three?

Let's consider two electrons, and assume that they are spatially well-separated so we can label "electron 1" and "electron 2" without any ambiguity. It is easy to write the state of electron 1 as

$$|\psi\rangle_1 = a|\uparrow\rangle_1 + b|\downarrow\rangle_1 \quad \text{with} \quad |a|^2 + |b|^2 = 1\,, \tag{6.1}$$

where we add a subscript "1" to emphasise that we refer to electron 1. Similarly, we can write down the state of electron 2:

Electronic supplementary material The online version of this chapter (https://doi.org/10.1007/978-3-319-92207-2_6) contains supplementary material, which is available to authorized users.

P. Kok, *A First Introduction to Quantum Physics*,
Undergraduate Lecture Notes in Physics,
https://doi.org/10.1007/978-3-319-92207-2_6

$$|\phi\rangle_2 = c|\uparrow\rangle_2 + d|\downarrow\rangle_2 \quad \text{with} \quad |c|^2 + |d|^2 = 1\,. \tag{6.2}$$

The question is: what is the state of the composite system consisting of these two electrons?

We can construct the states of the composite system from the states of the individual systems. Remember that the symbols and writing inside the ket are nothing more than convenient labels, indicating the measurement outcomes. We therefore have four possible measurement outcomes if we measure the spin of each electron in the z-direction:

$$\begin{aligned}
&|\text{electron 1} = \uparrow,\ \text{electron 2} = \uparrow\rangle\,,\\
&|\text{electron 1} = \uparrow,\ \text{electron 2} = \downarrow\rangle\,,\\
&|\text{electron 1} = \downarrow,\ \text{electron 2} = \uparrow\rangle\,,\\
&|\text{electron 1} = \downarrow,\ \text{electron 2} = \downarrow\rangle\,.
\end{aligned} \tag{6.3}$$

This is hardly convenient, so instead we may write

$$|\uparrow_1, \uparrow_2\rangle\,, \quad |\uparrow_1, \downarrow_2\rangle\,, \quad |\downarrow_1, \uparrow_2\rangle\,, \quad |\downarrow_1, \downarrow_2\rangle\,. \tag{6.4}$$

By convention, the ordering of the $\uparrow$ and $\downarrow$ arrow is fixed, and do we really need the comma? Clearly, we can reduce this further to

$$|\uparrow\uparrow\rangle\,, \quad |\uparrow\downarrow\rangle\,, \quad |\downarrow\uparrow\rangle \quad \text{and} \quad |\downarrow\downarrow\rangle\,. \tag{6.5}$$

These are four quantum states that make perfect sense in the light of measuring S_z on each electron separately. And because this is quantum mechanics, we can take superpositions of these states, such as

$$|\psi\rangle = \frac{1}{2}|\uparrow\uparrow\rangle + \frac{1}{2}|\uparrow\downarrow\rangle + \frac{1}{2}|\downarrow\uparrow\rangle + \frac{1}{2}|\downarrow\downarrow\rangle\,. \tag{6.6}$$

Next, suppose that the electrons are in the states given in Eqs. (6.1) and (6.2). How do we write this in terms of the states of Eq. (6.5)? We can look first at the probabilities of the measurement outcomes of S_z on the two electrons. Since the electrons are completely independent, the probabilities multiply:

$$\begin{aligned}
\Pr(\uparrow\uparrow) &= \Pr(\uparrow_1) \times \Pr(\uparrow_2) = |a|^2|c|^2\\
\Pr(\uparrow\downarrow) &= \Pr(\uparrow_1) \times \Pr(\downarrow_2) = |a|^2|d|^2\\
\Pr(\downarrow\uparrow) &= \Pr(\downarrow_1) \times \Pr(\uparrow_2) = |b|^2|c|^2\\
\Pr(\downarrow\downarrow) &= \Pr(\downarrow_1) \times \Pr(\downarrow_2) = |b|^2|d|^2
\end{aligned} \tag{6.7}$$

It is easy to verify that the probabilities sum to one:

$$\Pr(\uparrow\uparrow) + \Pr(\uparrow\downarrow) + \Pr(\downarrow\uparrow) + \Pr(\downarrow\downarrow) = 1\,. \tag{6.8}$$

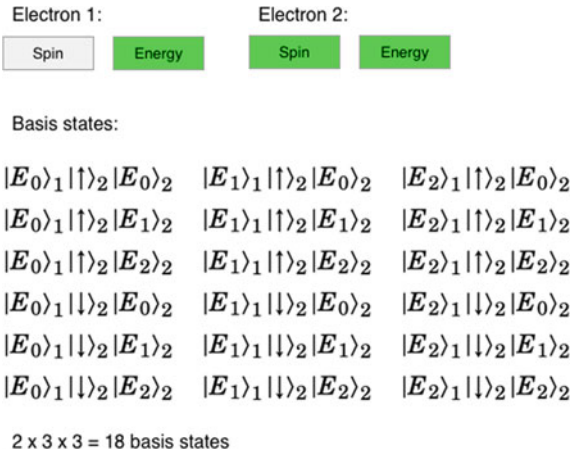

Fig. 6.1 Constructing states for composite systems. The interactive figure is available online (see supplementary material 1)

The two-electron spin state that is consistent with these probabilities is

$$|\psi\rangle = ac|\uparrow\uparrow\rangle + ad|\uparrow\downarrow\rangle + bc|\downarrow\uparrow\rangle + bd|\downarrow\downarrow\rangle\,. \tag{6.9}$$

But this is nothing more than the product of the two spin states:

$$\begin{aligned} |\psi\rangle_1|\phi\rangle_2 &= (a|\uparrow\rangle_1 + b|\downarrow\rangle_1)(c|\uparrow\rangle_2 + d|\downarrow\rangle_2) \\ &\equiv ac|\uparrow\uparrow\rangle + ad|\uparrow\downarrow\rangle + bc|\downarrow\uparrow\rangle + bd|\downarrow\downarrow\rangle\,. \end{aligned} \tag{6.10}$$

So we can combine the states of two quantum system into a composite quantum system by multiplying out the states in the manner above, and keep the order of the symbols in the ket! You can now show that the state in Eq. (6.6) is the same as two electrons that are each in the state

$$|\psi\rangle = |\phi\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle\,. \tag{6.11}$$

As a convention, in this book we will use lower case Greek letters for simple quantum systems, and upper case Greek letters for composite quantum systems. In Fig. 6.1 we encounter other examples of composite systems.

6.2 Entanglement

The four states in Eq. (6.5) form a basis for all quantum states of two electron spins. In other words, we can take any superposition of these four states, and obtain another valid quantum state, as long as the normalisation condition is satisfied. However, this can lead to strange situations. For example, consider the state

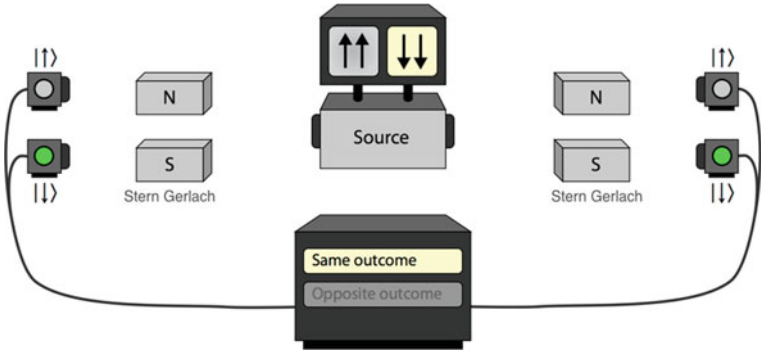

Fig. 6.2 Creating classical correlations. The interactive figure is available online (see supplementary material 2)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle\,. \tag{6.12}$$

Try as you might, you will not be able to find values of a, b, c, and d in Eq. (6.10) such that you obtain the state in Eq. (6.12). This means that there are no single electron states of the form of Eqs. (6.1) and (6.2) that give the same behaviour as the two electrons in the state $|\Phi^+\rangle$. In other words, the two electrons in the state $|\Phi^+\rangle$ are entangled, because we cannot write down the state of each electron individually.

In general, two quantum systems are entangled if you cannot write the total state as a product of states for the separate systems. The total state is called an *entangled state*. By contrast, if the total state can be written as the product of two states for the individual quantum systems, the total state is called separable.

What is the physical difference between entangled and separable states? Let's construct a thought experiment that can shed some light on this. Consider a source that emits electrons in opposite directions, one to Alice, and the other to Bob. They both measure the spin of the electron they receive in the z-direction. If the state of the electrons is given by $|\Phi^+\rangle$, it is not hard to see that they both find $\uparrow$ and $\downarrow$ measurement outcomes 50% of the time. But crucially, when Alice measures $\uparrow$ so does Bob, and vice versa when Alice measures $\downarrow$, Bob gets $\downarrow$ as well.

So maybe this is what entanglement means. Does it just say that the source creates the state $|\uparrow\uparrow\rangle$ half the time, and $|\downarrow\downarrow\rangle$ the other half, making the choice, for example, via a coin toss (see Fig. 6.2)? If that were true, suppose that in one particular run of the experiment the source sent $|\uparrow\uparrow\rangle$, but now Alice and Bob measure the spin in the x-direction instead. We know that we can write the states $|\uparrow\rangle$ and $|\downarrow\rangle$ in terms of the eigenstates $|+\rangle$ and $|-\rangle$ of the S_x observable:

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\,, \tag{6.13}$$

and

$$|\downarrow\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\,. \tag{6.14}$$

The state $|\uparrow\uparrow\rangle$ translates into

$$|\uparrow\uparrow\rangle = \frac{1}{2}|{+}{+}\rangle + \frac{1}{2}|{+}{-}\rangle + \frac{1}{2}|{-}{+}\rangle + \frac{1}{2}|{-}{-}\rangle\,, \tag{6.15}$$

which means that Alice and Bob obtain all measurement outcomes "++", "+−", "−+", and "−−", all with probability 1/4. In other words, there is no correlation between the measurement outcomes of Alice and Bob, because Alice's outcome tells her nothing about Bob's measurement outcome and vice versa. The same measurement outcomes are obtained when the source creates two electrons with spin $|\downarrow\downarrow\rangle$, since

$$|\downarrow\downarrow\rangle = \frac{1}{2}|{+}{+}\rangle - \frac{1}{2}|{+}{-}\rangle - \frac{1}{2}|{-}{+}\rangle + \frac{1}{2}|{-}{-}\rangle\,, \tag{6.16}$$

The minus signs in the amplitudes have no effect on the probabilities, since the probabilities are the square of the amplitudes. These measurement statistics are the result of a source that creates two electrons in the state $|\uparrow\uparrow\rangle$ or $|\downarrow\downarrow\rangle$, each with probability 1/2.

However, when the source truly creates the entangled state $|\Phi^+\rangle$, the measurement statistics will be different. Specifically, the minus signs in Eq. (6.16) will become important. When we translate the entangled state $|\Phi^+\rangle$ into the eigenvectors for the spin observables in the x-direction, we obtain

$$\begin{aligned}|\Phi^+\rangle &= \frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle \\ &= \frac{1}{2\sqrt{2}}\left(|{+}{+}\rangle + |{+}{-}\rangle + |{-}{+}\rangle + |{-}{-}\rangle\right) + \frac{1}{2\sqrt{2}}\left(|{+}{+}\rangle - |{+}{-}\rangle - |{-}{+}\rangle + |{-}{-}\rangle\right) \\ &= \frac{1}{\sqrt{2}}|{+}{+}\rangle + \frac{1}{\sqrt{2}}|{-}{-}\rangle\,.\end{aligned} \tag{6.17}$$

You see that the minus signs are responsible for the cancellation of the terms $|{+}{-}\rangle$ and $|{-}{+}\rangle$. As a result, there is a perfect correlation between the measurement outcomes of Alice and Bob when they measure the spin in the x-direction. Somehow, the correlations in the entangled state $|\Phi^+\rangle$ are stronger than the correlations we get when we choose $|\uparrow\uparrow\rangle$ or $|\downarrow\downarrow\rangle$ on the basis of a coin toss (see Fig. 6.3), because they manifest themselves in both the $\{\uparrow, \downarrow\}$ and $\{+, -\}$ directions.

Entanglement is a phenomenon that exists only in quantum mechanics, so we can say that quantum mechanics allows for stronger correlations between systems than classical physics. These stronger correlations have some very interesting consequences. One is quantum teleportation, in which the quantum state of a system

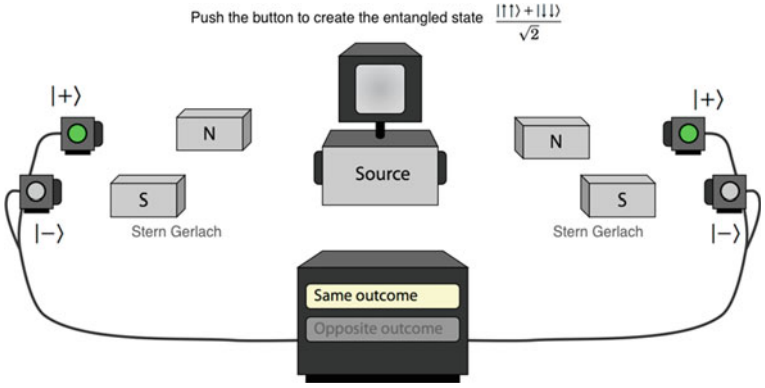

Fig. 6.3 Creating quantum correlations. The interactive figure is available online (see supplementary material 3)

can be transported over arbitrary distances without the need for a quantum system to carry it along. The other consequence is that we can build more powerful computers using entanglement. We consider these applications in the next two sections.

6.3 Quantum Teleportation

Probably the most extraordinary use of the quantum correlations present in entanglement is *quantum teleportation* (Bennett et al. 1993). It is the process of transferring the quantum state from one particle, held by Alice, to another particle, held by Bob. In cartoon form, it would look something like Fig. 6.4 (don't worry about what is going on inside the machine at this point). Furthermore, this transfer must succeed without either Alice or Bob gaining any information about the quantum state—say the electron spin. To make things extra hard, the three spins must not change places, so Alice cannot take spin 1 and bring it to Bob. Finally, Alice and Bob may be arbitrarily far apart, for example with Alice here on Earth and Bob somewhere in the Andromeda galaxy two million light years away. Surely, this is impossible…

Your first inclination might be to measure the spin of Alice's electron, and send the measurement result to Bob, who prepares the spin of his electron according to the measurement outcome. However, this will not work well. Alice needs to choose a direction to measure the spin of her electron. Once she has chosen a direction, she cannot measure any of the other two directions and expect to get a meaningful answer about the original spin direction (see Sect. 3.4). To see this, assume that the state of the electron is

$$|\psi\rangle = \cos\theta|\uparrow\rangle + i\,\sin\theta|\downarrow\rangle\,. \tag{6.18}$$

A measurement of the spin in the z-direction will give outcome $\uparrow$ with probability $p_\uparrow = \cos^2\theta$ and outcome $\downarrow$ with probability $p_\downarrow = \sin^2\theta$. After the measurement, the

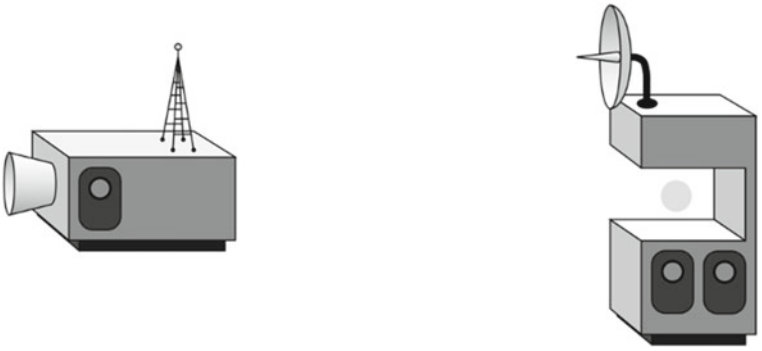

Fig. 6.4 Cartoon of a teleportation machine. The interactive figure is available online (see supplementary material 4)

electron will be in the spin state $|\uparrow\rangle$ or $|\downarrow\rangle$, respectively. Measuring the spin next in the x- or y-direction will give one of two outcomes, but always with probability of $1/2$. This does not give us any more information about θ. Only the first measurement gives information about θ, but since the outcome is one bit of information (up or down), it can never contain enough to fully capture the value of θ. So a measure-and-send approach will not work.

However, we can achieve our goal of sending the state using quantum teleportation. Before we give a detailed description of this remarkable phenomenon we will need to construct a few more entangled states. The state space of two electrons is spanned by four orthogonal basis states, as given in Eq. (6.5). Alternatively, we can create a basis out of four entangled states:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle\,, \quad \text{and} \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}|\uparrow\downarrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\uparrow\rangle\,, \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle\,, \quad \text{and} \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}|\uparrow\downarrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\uparrow\rangle\,. \end{aligned} \tag{6.19}$$

This is called the Bell basis, after John Steward Bell, and the states $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ are called the Bell states. They are maximally entangled states, in the sense that they describe the strongest possible correlations between two electron spins. We can also use these states as eigenvectors of an observable called the Bell operator. When we measure the Bell operator (called a Bell measurement), the outcomes tell us which of the Bell states the electrons are in. This is a joint measurement of the two spins, and does not reveal anything about the individual spins.[1]

[1] This is not as strange as it sounds: when you look at macroscopic object, say a pencil, you do not see the individual atoms in the pencil, but rather the collective state of the atoms that make up the pencil.

We are now ready to describe the process of quantum teleportation: Alice holds an electron, labelled 1, in the spin state

$$|\psi\rangle_1 = a|\uparrow\rangle_1 + b|\downarrow\rangle_1 . \tag{6.20}$$

In addition, Alice and Bob each hold one of a pair of entangled electrons, labelled 2 and 3, in the state

$$|\Phi^+\rangle_{23} = \frac{1}{\sqrt{2}}|\uparrow_2, \uparrow_3\rangle + \frac{1}{\sqrt{2}}|\downarrow_2, \downarrow_3\rangle . \tag{6.21}$$

Let's say that Alice holds electron 2 and Bob holds electron 3. Next, we combine the state of the three electrons and expand it as

$$\begin{aligned} |\Upsilon\rangle = |\psi\rangle_1|\Phi^+\rangle_{23} &= (a|\uparrow\rangle_1 + b|\downarrow\rangle_1)\left(\frac{1}{\sqrt{2}}|\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(a|\uparrow\uparrow\uparrow\rangle + a|\uparrow\downarrow\downarrow\rangle + b|\downarrow\uparrow\uparrow\rangle + b|\downarrow\downarrow\downarrow\rangle\right), \end{aligned} \tag{6.22}$$

where we dropped the electron labels and pulled a common factor $1/\sqrt{2}$ out in front in the last line. This is the state of the system of three electrons (keep the order inside the kets the same!).

Alice now performs a Bell measurement on her two spins (1 and 2), which gives a measurement outcome that allows us to tell which one of the Bell states $|\Phi^\pm\rangle$ or $|\Psi^\pm\rangle$ the electrons are in. We write the spin states of the two electrons held by Alice $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, and $|\downarrow\downarrow\rangle$ in the Bell basis:

$$\begin{aligned} |\uparrow\uparrow\rangle_{12} &= \frac{|\Phi^+\rangle_{12} + |\Phi^-\rangle_{12}}{\sqrt{2}} \quad \text{and} \quad |\uparrow\downarrow\rangle_{12} = \frac{|\Psi^+\rangle_{12} + |\Psi^-\rangle_{12}}{\sqrt{2}} , \\ |\downarrow\downarrow\rangle_{12} &= \frac{|\Phi^+\rangle_{12} - |\Phi^-\rangle_{12}}{\sqrt{2}} \quad \text{and} \quad |\downarrow\uparrow\rangle_{12} = \frac{|\Psi^+\rangle_{12} - |\Psi^-\rangle_{12}}{\sqrt{2}} . \end{aligned} \tag{6.23}$$

This is the "reverse" relation compared to Eq. (6.19). You should verify that these equations hold. We can use these substitutions for electrons 1 and 2 to write the state $|\Upsilon\rangle$ before the measurement as

$$\begin{aligned} |\Upsilon\rangle = \frac{1}{2}\big[&|\Phi^+\rangle_{12}(a|\uparrow\rangle_3 + b|\downarrow\rangle_3) + |\Phi^-\rangle_{12}(a|\uparrow\rangle_3 - b|\downarrow\rangle_3) \\ &+|\Psi^+\rangle_{12}(b|\uparrow\rangle_3 + a|\downarrow\rangle_3) + |\Psi^-\rangle_{12}(b|\uparrow\rangle_3 - a|\downarrow\rangle_3)\big] . \end{aligned} \tag{6.24}$$

Alice finds one of four possible outcomes in her Bell measurement, and for each outcome we can read off the state of Bob's electron:

$$\begin{aligned}
\Phi^+ &: \quad |\psi\rangle_3 = a|\uparrow\rangle + b|\downarrow\rangle\,, \\
\Phi^- &: \quad |\psi\rangle_3 = a|\uparrow\rangle - b|\downarrow\rangle\,, \\
\Psi^+ &: \quad |\psi\rangle_3 = a|\downarrow\rangle + b|\uparrow\rangle\,, \\
\Psi^- &: \quad |\psi\rangle_3 = a|\downarrow\rangle - b|\uparrow\rangle\,.
\end{aligned} \tag{6.25}$$

From these outcomes, it is clear that the state held by Bob is different for the different measurement outcomes of Alice's Bell measurement. Let this sink in for a moment: After setting up the entangled state between Alice and Bob, who may be literally light years apart, Bob has done absolutely nothing to his spin, yet its state is different depending on Alice's measurement outcome! This should shock you: the information contained in a and b somehow made it from Alice to Bob without any communication, only a local measurement by Alice! Is there some violation of causality? No! It is a direct consequence of the stronger-than-classical correlations present in entangled states.

In order to turn the state of Bob's spin into the original state that entered Alice's device, Bob needs to apply a correction to his electron spin. Since he does not know the outcome of Alice's measurement, he must wait for a signal from Alice that tells him which correction to apply. This will take two classical bits, because there are four measurement outcomes. The correction operators that Bob needs to apply are:

$$\Phi^+ : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \Phi^- : \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \Psi^+ : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \Psi^- : \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{6.26}$$

Only after this correction does Bob have his electron in the original state

$$|\psi\rangle_3 = a|\uparrow\rangle_3 + b|\downarrow\rangle_3\,. \tag{6.27}$$

Notice how the label "1" in Eq. (6.20) has turned into a "3" in Eq. (6.27). The fact that Bob has to wait for Alice's measurement outcome means that causality is not violated. The process of teleportation is shown in Fig. 6.5.

To appreciate how remarkable this protocol really is, let's recall some of its most distinctive properties. First, no matter is transported, only the state of the system. In this sense teleportation is completely different from the transporter in Star Trek, to which it is often compared. In Star Trek, it seems that matter appears out of nowhere in the form of the away team at the surface of a planet. This cannot happen in physics, because matter is energy, and it would violate energy conservation. Second, neither Alice nor Bob learns anything about the input state $|\psi\rangle$. And finally, quantum teleportation cannot be used to signal faster than light. So there is no problem with quantum mechanics and Einstein's theory of relativity coexisting as far as teleportation is concerned. Still, quantum mechanics allows us to transfer a potentially large amount of information (contained in a and b) at the cost of sending only two bits of information.

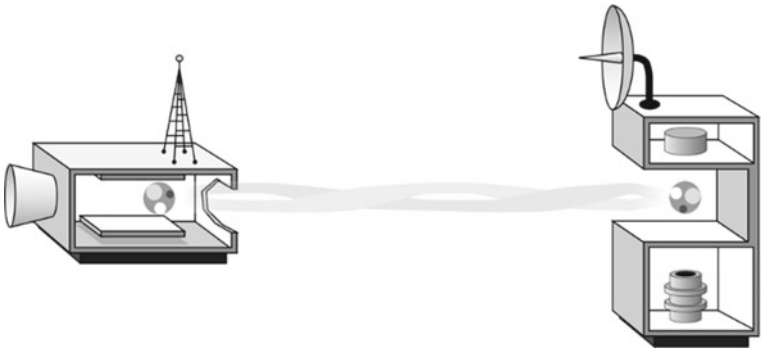

Fig. 6.5 Inside the teleportation machine. The interactive figure is available online (see supplementary material 5)

Richard Feynman famously said (Feynman 1963), that the double slit experiment captures everything that is mysterious about quantum mechanics: it contains the *only* mystery. However, this is not quite true, because it does not contain entanglement. Instead, quantum teleportation is the process that contains the true mystery about quantum mechanics.

6.4 *Mathematical Intermezzo*: Qubits and Computation

Ordinary (or "classical") computers operate using bits, which are units of information that are labelled $\mathsf{0}$ or $\mathsf{1}$. These bits of information are always carried by physical systems whose states are correspondingly labelled $\mathsf{0}$ and $\mathsf{1}$. For example, in a memory chip, the information carrier is a capacitor that either holds charge or not (bit value $\mathsf{0}$ or $\mathsf{1}$, respectively). The extension to quantum mechanics is immediate: instead of a classical physical system with states that can be either $\mathsf{0}$ or $\mathsf{1}$, we use quantum systems, whose states can be any superposition of $\mathsf{0}$ or $\mathsf{1}$. In our notation we write

$$|\psi\rangle = a|\mathsf{0}\rangle + b|\mathsf{1}\rangle\,. \tag{6.28}$$

We call this a quantum bit, or *qubit*. The actual physical system can be an electron spin with $|\mathsf{0}\rangle = |\uparrow\rangle$ and $|\mathsf{1}\rangle = |\downarrow\rangle$, a two-level atom with $|\mathsf{0}\rangle = |g\rangle$ and $|\mathsf{1}\rangle = |e\rangle$, a photon in two possible paths with $|\mathsf{0}\rangle = |\text{path 1}\rangle$ and $|\mathsf{1}\rangle = |\text{path 2}\rangle$, or any other system that has a two dimensional state space in quantum mechanics. Here, we will use generic qubits for the description of a quantum computation. Translating the abstract computation into a physical implementation is then a task for scientists and engineers who know how to manipulate photons, electrons, atoms, etc.

The idea behind computation is that an input bit string evolves according to some computational rules based on logical operators like AND, OR and NOT into an output bit string. For example

$$\mathsf{AND}(1,1) = 1 \quad \text{and} \quad \mathsf{AND}(1,0) = 0 \quad \text{etc.}, \tag{6.29}$$

or

$$\mathsf{NOT}(0) = 1 \quad \text{and} \quad \mathsf{NOT}(1) = 0\,. \tag{6.30}$$

These computational rules can encode any problem you want to solve. If you find these rule a little tricky, you may think of 0 and 1 as FALSE and TRUE. The expression $\mathsf{AND}(1,1) = 1$ then means that AND returns TRUE if both propositions in its argument are true. So the proposition "the Sun shines and I am happy" is true if "the Sun shines" is true and "I am happy" is true.

One more thing we need to learn is how to add bits. There is no value 2 in a bit, just 0 and 1. Nevertheless, we often want to add two bits. How do we do this? The answer is to add "modulo 2", where 2 turns into 0. The standard addition "+" is replaced by a "$\oplus$" to indicate that we used addition modulo 2. For example, we have

$$\begin{aligned} 0 \oplus 0 &= 0 \\ 0 \oplus 1 &= 1 \\ 1 \oplus 0 &= 1 \\ 1 \oplus 1 &= 0\,. \end{aligned} \tag{6.31}$$

Adding a bit value of 1 to another bit is effectively the same as "flipping" the bit value from 0 to 1 and from 1 to 0 (incidentally, this is the NOT operator). You are already very familiar with addition modulo 12 because you use it implicitly when you read the time: four hours after 11 am is three pm. Doing the calculation explicitly, we add 4 to 11 modulo 12:

$$11 \oplus 4 = 15 \bmod 12 = 3. \tag{6.32}$$

Addition modulo two works along the same lines, but simpler because the numbers are smaller.

Equation (6.31) describes the "exclusive or" operator XOR between two bits. It differs from the OR operator in that it is 0 when both bits are 1:

$$\begin{aligned} \mathsf{XOR}(0,0) &= 0 \\ \mathsf{XOR}(0,1) &= 1 \\ \mathsf{XOR}(1,0) &= 1 \\ \mathsf{XOR}(1,1) &= 0\,. \end{aligned} \tag{6.33}$$

We can also interpret the XOR as a controlled NOT, where the outcome of the XOR is a bit flip of the first bit if the second bit has value 1 (or vice versa; the XOR is symmetric in the input). You can now see how this operation is important

in computations, because it does something to one bit depending on the value of another bit.

6.5 Quantum Computers

Quantum mechanics has many applications in everyday life. For example, quantum mechanics is indispensable for the understanding of the semiconductor devices we use in all modern computers. But an even more profound use for quantum mechanics is quantum computing.

To show the basic idea behind quantum computing, we choose a very simple calculation: Suppose that we have a function f, which takes as input a single bit and produces another single bit as output. There are exactly four such functions:

f_1	f_2	f_3	f_4
$f(0) = 0$	$f(0) = 1$	$f(0) = 0$	$f(0) = 1$
$f(1) = 0$	$f(1) = 0$	$f(1) = 1$	$f(1) = 1$

These functions can be divided into two classes called "constant": $f(0) = f(1)$, and "balanced": $f(0) \neq f(1)$. The functions f_1 and f_4 above are constant, while the functions f_2 and f_3 are balanced. To check whether a function is balanced or constant, you normally have to evaluate the function twice: once with input 0, and once with input 1. We compare the outcomes, which then tells us whether f is constant or balanced. There is no way to do this by evaluating f fewer than two times, either on paper or with a classical computer. However, on a quantum computer we can tell whether f is constant or balanced by evaluating f only once.[2]

In the remainder of this section, we will show how a quantum computer can tell the difference between constant and balanced functions with only a single application of the function f. The algorithm was invented by David Deutsch (1989), and uses only two qubits that are initially prepared in the state $|01\rangle \equiv |0\rangle_1|1\rangle_2$. First, we apply a so-called Hadamard gate to each qubit. This is just a unitary operator that changes the state of a qubit according to

$$|0\rangle \underset{H}{\rightarrow} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,, \tag{6.34}$$

and

$$|1\rangle \underset{H}{\rightarrow} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\,. \tag{6.35}$$

We can write this unitary operator in matrix form as

[2] Perhaps this is not a very interesting calculation, but it serves as a simple example that demonstrates the power of quantum mechanics for computing.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{6.36}$$

where H stands for "Hadamard" here, and not "Hamiltonian" as earlier. Those are two different operators, and you should not confuse them!

Notice how the Hadamard is mathematically identical to the beam splitter transformation in Chap. 2. If we label the Hadamard gate with subscripts according to the qubits they operate on, we can write the evolved state as

$$H_1 H_2 |0\rangle|1\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)\,. \tag{6.37}$$

Next, we apply the unitary operator U_f that implements the function f. We do not know how to write this as a unitary operator, because we do not know which of the four functions f_1, f_2, f_3, or f_4 we are implementing. We therefore need to be clever about it.

The function f affects the quantum state of the two qubits in a very specific way. Since we want to use unitary operators in the quantum computer, the computation must be reversible (remember that unitary transformations U always have an inverse U^{-1}, and can therefore always be reversed; that's what the inverse does). For a computation, we can make everything reversible by always keeping track of the input. This unitary operator U_f can be implemented for our function f in the following way:

$$\begin{aligned}
|0\rangle|0\rangle &\underset{U_f}{\to} |0\rangle|0 \oplus f(0)\rangle\,, \\
|0\rangle|1\rangle &\underset{U_f}{\to} |0\rangle|1 \oplus f(0)\rangle\,, \\
|1\rangle|0\rangle &\underset{U_f}{\to} |1\rangle|0 \oplus f(1)\rangle\,, \\
|1\rangle|1\rangle &\underset{U_f}{\to} |1\rangle|1 \oplus f(1)\rangle\,.
\end{aligned} \tag{6.38}$$

We can write this more compactly as

$$|x\rangle|y\rangle \underset{U_f}{\to} |x\rangle|y \oplus f(x)\rangle\,, \tag{6.39}$$

where x and y can take the values 0 and 1.

We want to know what the function does to the input state in Eq. (6.37). To this end, we calculate the effect of f on $|0\rangle(|0\rangle - |1\rangle)$ and $|1\rangle(|0\rangle - |1\rangle)$ separately:

$$\begin{aligned}
|0\rangle(|0\rangle - |1\rangle) &\underset{U_f}{\to} |0\rangle(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle)\,, \\
|1\rangle(|0\rangle - |1\rangle) &\underset{U_f}{\to} |1\rangle(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)\,.
\end{aligned} \tag{6.40}$$

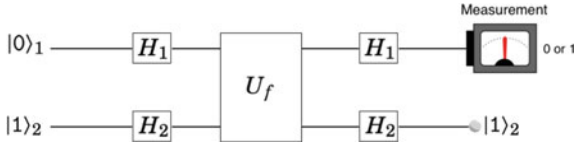

Fig. 6.6 Deutsch' algorithm in circuit form, with the Hadamard operators H_1 and H_2, and the single function call U_f. The interactive figure is available online (see supplementary material 6)

You may have noticed that we ignored the normalisation factor of 1/2. Since it is an overall factor, it does not affect the calculation, but strictly speaking we should carry it along if we want to calculate probabilities.

Since the outcome of $f(0)$ and $f(1)$ is a single bit, we can infer that

$$|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle = |0\rangle - |1\rangle \quad \text{if} \quad f(0) = 0\,, \tag{6.41}$$

or

$$|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle = -|0\rangle + |1\rangle \quad \text{if} \quad f(0) = 1\,. \tag{6.42}$$

We can write this compactly as

$$|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle = (-1)^{f(0)}(|0\rangle - |1\rangle)\,, \tag{6.43}$$

where we use the trick that $(-1)^0 = 1$ and $(-1)^1 = -1$. Similarly, we find

$$|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle)\,. \tag{6.44}$$

The state of the two qubits after applying the function f is therefore

$$\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle)\,. \tag{6.45}$$

Now if f is constant such that $f(0) = f(1)$, then up to an overall minus sign the first qubit will be in the state $|0\rangle + |1\rangle$. However, when f is balanced, $f(0) \neq f(1)$, and the state of qubit 1 becomes $|0\rangle - |1\rangle$. We can distinguish between these two states by applying another Hadamard to qubit 1, and measure whether the qubit is 0 or 1. If we find outcome 0 the function f is constant, and if we find 1, f is balanced. The steps of this calculation are shown in Fig. 6.6.

On a classical computer, we would have had to call the function twice, namely $f(0)$ and $f(1)$. However, on a quantum computer we call the function f only once, since we apply the unitary operator that gives us Eq. (6.39) only once.[3] So a quantum computer can solve problems with fewer calls to the function f. This becomes even

[3] You may wonder how we can implement U_f if we do not know f, but the point is that U_f is provided by some third party, or it is determined by some intermediate step in our computation.

462 347 950 278 203 702 501 505 522 342 002 665 331 946 475 632 708 577 739 234 697 784 021 818 140 522 674
835 309 196 163 416 854 110 243 970 766 758 695 342 543 748 648 643 466 538 624 332 779 501 208 848 831 412
318 949 546 425 213 770 986 123 218 920 991 417 525 715 823 853 168 208 512 390 153 750 241 932 708 388 543
649 473 207 897 291 446 477 938 324 479 425 026 680 675 167 906 376 383 548 080 575 988 477 319 816 177 170
358 052 679 605 289 152 840 388 527 832 392 549 520 085 586 988 144 677 185 063 589 682 077 908 927 194 968
763 102 990 652 140 972 984 570 273 963 646 719 303 069 803 321 415 538 148 010 197 650 803 018 640 916 340
428 037 541 756 215 330 967 921 857 099 324 273 470 336 668 080 317 517 568 273 246 212 729 299 786 812 996
213 318 540 193 686 768 966 638 631 505 039 426 144 382 013 243 722 075 433 193 895 396 449 242 863 781 661
096 403 032 797 729 777 324 675 445 757 988 990 806 682 128 301 589 585 625 404 539 963 918 751 562 488 316
111 490 163 920 025 739 750 105 478 587 062 824 899 939 271 968 625 907 066 047 409 531 160 274 348 277 690
853 293 007 679 329 437 716 093 563 352 405 390 449 899 076 707 567 686 170 341 951 292 961 575 030 591 035
333 999 264 176 628 337 315 636 656 819 482 742 865 413 569 115 316 362 362 401 423 280 762 602 231 291 513
376 192 875 958 826 079 719 634 210 515 509 860 269 580 141 236 897 260 749 302 046 804 291 326 072 691 383
195 105 775 859 878 885 583 576 316 437 777 908 228 631 422 056 478 570 072 248 642 389 058 509 749 217 542
788 270 157 240 969 341 176 521 789 292 658 854 983 608 895 967 517 794 787 229 737 736 185 878 610 604 212
043 224 870 701 623 802 895 692 921 626 807 844 754 717 906 096 442 740 910 050 085 003 208 490 366 787 832
833 335 027 976 891 526 325 015 110 460 686 668 129 298 036 464 820 365 795 364 103 090 269 234 748 691 878
198 067 631 338 259 483 628 021 755 866 850 255 572 257 399 480 210 126 207 963 418 287 191 960 225 073 176
633 358 736 514 966 189 809 007 670 162 221 782 446 030 434 293 473 899 297 435 667 577 068 035 299 729 602
469 965 034 027 838 521 415 316 911 707 684 133 014 532 291 078 523 932 317 542 374 087 783 700 097 253 286
939 692 162 168 693 152 984 085 524 987 570 311 180 948 487 723 809 119 845 926 787 034 490 707 796 581 502
652 623 320 085 614 236 244 299 400 766 034 707 707 077 105 801 761 644 635 453 492 713 489 213 703 078 573
429 984 587 446 050 033 491 373 441 286 637 193 614 498 559 884 404 831 734 434 281 178 221 079 758 411 718
699 748 468 558 432 470 770 923 665 450 590 347 550 865 903 585 971 264 602 410 477 343 544 742 795 151 885
042 906 506 792 358 507 463 513 616 901 678 633 445 665 084 188 293 014 818 159 530 550 450 937 995 770 887
434 483 782 244 417 402 082 458 744 360 441 525 135 048 661 574 229 568 612 552 416 708 798 433 854 440 479
768 038 171 031 275 803 281 320 122 294 494 105 273 874 996 713 004 022 943 403 466 208 235 634 992 811 388
509 205 864 981 865 479 475 169 535 594 505 259 968 813 633 461 801 209 333 273 576 877 409 417 053 028 248
160 933 256 981 232 603 196 644 488 378 713 095 686 003 330 281 066 637 529 748 828 854 562 463 533 251 975
597 244 602 805 216 576 531 592 880 514 908 242 781 228 492 548 966 185 276 811 559 143 174 042 071 693 087
533 599 980 942 966 766 655 514 107 580 873 666 897 349 236 260 518 529 627 255 826 135 487 502 375 985 361
557 640 727 326 592 237 444 567 065 986 491 795 093 987 861 760 160 478 946 889 049 309 960 672 287 948 802
843 869 271 432 179 649 542 074 301 142 966 065 865 124 285 813 925 751 642 775 151 535 301 351 711 281 783
966 131 752 651 258 578 862 783 654 078 120 763 223 873 887 425 689 391 641 004 461 906 279 865 123 906 777
474 802 714 192 159 536 914 283 222 778 277 242 913 626 528 919 962 107 196 121 778 906 493 272 908 787 557
730 741 548 731 111 669 178 534 878 981 050 918 328 182 376 506 738 709 363 344 257 065 718 159 737 540 003
824 475 424 354 788 090 714 440 814 365 487 289 845 327 317 685 016 166 748 932 852 274 604 894 708 794 101

Fig. 6.7 A 2997 digit number that may be used in a cryptographic protocol

more dramatic if we have a constant or balanced function with N input bits. This generalisation by Deutsch and Richard Jozsa (1992) of the Deutsch algorithm, called the Deutsch–Jozsa algorithm, still allows you to find out whether the function is constant or balanced with a *single* call to the function f, but on a classical computer you need at least $N/2 + 1$ calls to the function f (we take the worst case scenario). The quantum computer gives an enormous advantage when N is large, because it requires dramatically fewer steps in the computation (only one call to f).

You may wondering why this is interesting. The Deutsch–Jozsa algorithm is merely a toy problem, with little practical value. However, in 1994 Peter Shor (1997) showed that a quantum computer can factorise large integers in fewer steps than a classical computer. He designed an algorithm for factoring an integer N that requires on the order of $(\log N)^3$ computational steps in a quantum computer to give the right result. By contrast, the best known classical algorithm to date requires on the order of N steps. So a quantum computer is exponentially faster than a classical computer in factoring integers. As an example, a classical computer can factor the number 15 in roughly 15 steps, while a quantum computer can factor it in $(\log_2 15)^3 = 60$ steps. This is not an improvement at all! But consider factoring a very large number of 2997 digits, say as shown in Fig. 6.7. The number of steps on a quantum computer is about 9×10^7. If the quantum computer has the same clock speed as a typical laptop, say 2 GHz, this calculation takes about 14 s. On the other hand, factoring the 2997 digit number on a classical computer with a clock speed of 2 GHz will take over 30 billion years, which is more than twice the age of the universe!

Shor's algorithm is important because the difficulty of factoring lies at the heart of modern cryptography. If we can build a quantum computer, we can crack pretty much all cryptographic codes that are used today. No wonder governments around the world are interested in building a quantum computer! Other applications of quantum computers include the design of new molecules, drugs, and other materials with predefined properties. Currently, we cannot calculate the properties of large atom configurations on classical computers because of their quantum mechanical character. However, these types of calculations would be easy for a quantum computer, since all it does is encode the rules of interaction of quantum systems, just like classical computers encode the rules that govern the behaviour of classical systems.

It is very difficult to build a large enough quantum computer to perform these tasks, and currently many people around the world are trying to figure out how to make it work. One of the main problems is the fragility of the qubits, which we study in the next chapter.

Exercises

1. Consider two electrons with spin 1/2. Indicate whether the following states are separable or entangled:

   (a) $|\Psi\rangle = (|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle + \sqrt{2}|\downarrow\downarrow\rangle)/2$
   (b) $|\Psi\rangle = \frac{1}{2}|\uparrow\uparrow\rangle + \frac{1}{2}|\uparrow\downarrow\rangle + \frac{1}{2}|\downarrow\uparrow\rangle - \frac{1}{2}|\downarrow\downarrow\rangle$
   (c) $|\Psi\rangle = \frac{1}{\sqrt{15}}|\uparrow\uparrow\rangle + \frac{2}{\sqrt{15}}|\uparrow\downarrow\rangle + \frac{\sqrt{2}}{\sqrt{15}}|\downarrow\uparrow\rangle + \frac{2\sqrt{2}}{\sqrt{15}}|\downarrow\downarrow\rangle$.

   If the state is separable, give the states of the individual systems.
2. Suppose we have a quantum state $|\psi\rangle = a|0\rangle + b|1\rangle$ with unknown a and b, and a unitary copier machine U that operates as follows:

$$U|0, \text{blank}\rangle = |0, 0\rangle \qquad \text{and} \qquad U|1, \text{blank}\rangle = |1, 1\rangle\,, \tag{6.46}$$

   where $|\text{blank}\rangle$ is some blank qubit state onto which U copies the value of the first qubit. Can this machine copy the state $|\psi\rangle$ perfectly?
3. Calculate the eigenvalues and the eigenstates of the bit flip operator X, and show that the eigenstates form an orthonormal basis. Calculate the expectation value of X for $|\psi\rangle = 1/\sqrt{3}|0\rangle + i\sqrt{2/3}|1\rangle$.
4. Consider a qubit in an arbitrary pure state $|\psi\rangle_1 = a|0\rangle_1 + b|1\rangle_1$, and a second qubit in the state $|+\rangle_2 = (|0\rangle_2 + |1\rangle_2)/\sqrt{2}$.

   (a) Calculate the two-qubit state after applying a CZ gate, defined by

$$\begin{aligned} |00\rangle &\to |00\rangle\,, \qquad |10\rangle \to |10\rangle\,, \\ |01\rangle &\to |01\rangle\,, \qquad |11\rangle \to -|11\rangle\,. \end{aligned}$$

(b) Apply a Hadamard gate to the first qubit and then perform a measurement in the $\{0, 1\}$ basis. What is are the resulting states for qubit 2? This is sometimes called "local teleportation".
(c) The Hadamard followed by a measurement of $0, 1$ is the same as a measurement of $+, -$. Show that a measurement in the equatorial plane of the Bloch sphere induces a rotation around the axis defined by $\{0, 1\}$ on the second qubit.
(d) Show that by daisy-chaining three local teleportation events we can induce any single qubit gate on the input qubit $|\psi\rangle$.

5. Show that the following states form an orthonormal basis for two qubits:

$$
\begin{aligned}
|\phi_1\rangle &= \frac{1}{\sqrt{2}}|0, 1\rangle + \frac{1}{\sqrt{2}}|1, 0\rangle\,, \\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}|0, -\rangle + \frac{1}{\sqrt{2}}|1, +\rangle\,, \\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}|+, 1\rangle + \frac{1}{\sqrt{2}}|-, 0\rangle\,, \\
|\phi_4\rangle &= \frac{1}{\sqrt{2}}|+, -\rangle + \frac{1}{\sqrt{2}}|-, +\rangle\,.
\end{aligned}
$$

6. Show that we can get any Bell state in Eq. (6.19) from any other using only a *local* unitary operation on one of the qubits.
7. Consider the two-qubit state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. The evolution $U = \exp(i\omega t|1\rangle\langle 1|)$ is applied to both qubits. Show that the time it takes for $|\Phi^+\rangle$ to evolve back to itself is twice as short as when U is applied to only one qubit.
8. Construct a matrix that relates the Bell basis in Eq. (6.19) to the spin basis in Eq. (6.23), and show that this matrix is unitary.

References

C.H. Bennett et al., Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. **70**, 1895 (1993)
D. Deutsch, R. Jozsa, Rapid solutions of problems by quantum computation. Proc. Roy. Soc. A; London **439**, 553 (1992)
D. Deutsch, Quantum computational networks. Proc. Roy. Soc. A; London **425**, 73 (1989)
R. Feynman, *Lectures on Physics*, vol. I (Addison–Wesley, USA, 1963), pp. 37–42
P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**, 1484–1509 (1997)