4

Quantum correlations

One might expect that going from a single qubit to two qubits would not lead to much of anything new. However, we shall see that the two-qubit structure is extraordinarily rich, because it introduces quantum correlations between the two qubits, correlations which cannot be reproduced using classical probabilistic arguments. Going then from two qubits to n qubits does not lead to anything fundamentally new. As we shall see in Chapter 5, these configurations of quantum systems, called entangled states, are what lead to the special features of quantum computing, due to the exponential growth of the number of states.

4.1 Two-qubit states

The mathematical construction of a two-qubit state rests on the idea of the tensor product, an idea which we shall introduce by means of an elementary example. Let $\mathcal{H}_A$ be a two-dimensional vector space of functions $f_A(x)$ with, for example, the basis vectors $\{\cos x, \sin x\}$:

$$f_A(x) = \lambda_A \cos x + \mu_A \sin x,$$

and let $\mathcal{H}_B$ be another two-dimensional vector space of functions $f_B(y)$ with the basis vectors $\{\cos y, \sin y\}$:

$$f_B(x) = \lambda_B \cos y + \mu_B \sin y.$$

We can construct a function of two variables called the "tensor product of f_A and f_B":

$$\begin{aligned} f_A(x) f_B(y) = {} & \lambda_A \lambda_B \cos x \cos y + \lambda_A \mu_B \cos x \sin y \\ & + \mu_A \lambda_B \sin x \cos y + \mu_A \mu_B \sin x \sin y. \end{aligned}$$

A possible basis of the tensor product space is

$$\{\cos x \cos y, \cos x \sin y, \sin x \cos y, \sin x \sin y\}.$$

https://doi.org/10.1017/CBO9780511755361.006

Any function in this space can be decomposed on this basis:

$$g(x, y) = \alpha \cos x \cos y + \beta \cos x \sin y + \gamma \sin x \cos y + \delta \sin x \sin y,$$

but this function will not in general take the form of the tensor product $f_A(x) f_B(y)$. A necessary (and sufficient) condition for it to take that form is $\alpha\delta = \beta\gamma$.

Let us follow this procedure to construct a two-qubit state mathematically. The first qubit A lives in a Hilbert space $\mathcal{H}_A$ which has orthonormal basis $\{|0_A\rangle, |1_A\rangle\}$, and the second qubit B lives in a Hilbert space $\mathcal{H}_B$ which has orthonormal basis $\{|0_B\rangle, |1_B\rangle\}$. It is natural to represent a physical state in which the first qubit is in the state $|0_A\rangle$ and the second is in the state $|0_B\rangle$ by a vector written as $|X_{00}\rangle = |0_A \otimes 0_B\rangle$. Taking into account all the other possible values of the qubits, we will *a priori* have four possibilities:

$$|X_{00}\rangle = |0_A \otimes 0_B\rangle, \quad |X_{01}\rangle = |0_A \otimes 1_B\rangle, \quad |X_{10}\rangle = |1_A \otimes 0_B\rangle, \quad |X_{11}\rangle = |1_A \otimes 1_B\rangle. \tag{4.1}$$

The notation $\otimes$ stands for the tensor product. It is not difficult to construct a state in which the qubit A is in the normalized state

$$|\varphi_A\rangle = \lambda_A |0_A\rangle + \mu_A |1_A\rangle, \qquad |\lambda_A|^2 + |\mu_A|^2 = 1,$$

and the qubit B is in the normalized state

$$|\varphi_B\rangle = \lambda_B |0_B\rangle + \mu_B |1_B\rangle, \qquad |\lambda_B|^2 + |\mu_B|^2 = 1.$$

We shall denote this state as $|\varphi_A \otimes \varphi_B\rangle$:

$$\begin{aligned} |\varphi_A \otimes \varphi_B\rangle &= \lambda_A\lambda_B |0_A \otimes 0_B\rangle + \lambda_A\mu_B |0_A \otimes 1_B\rangle \\ &\quad + \mu_A\lambda_B |1_A \otimes 0_B\rangle + \mu_A\mu_B |1_A \otimes 1_B\rangle \\ &= \lambda_A\lambda_B |X_{00}\rangle + \lambda_A\mu_B |X_{01}\rangle + \mu_A\lambda_B |X_{10}\rangle + \mu_A\mu_B |X_{11}\rangle. \end{aligned} \tag{4.2}$$

The correspondence with the preceding functional space is obvious. We have constructed the space $\mathcal{H}_A \otimes \mathcal{H}_B$ as the *tensor product* of the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. We note that the vector $|\varphi_A \otimes \varphi_B\rangle$ is also normalized. [1] Physicists are rather lax in their notation, and following in this tradition the reader will sometimes here find $|\varphi_A \otimes \varphi_B\rangle$, or $|\varphi_A\rangle \otimes |\varphi_B\rangle$, or even $|\varphi_A \varphi_B\rangle$, with the symbol for the tensor product omitted.

The crucial point is that the most general state of $\mathcal{H}_A \otimes \mathcal{H}_B$ is not of the form of a tensor product $|\varphi_A \otimes \varphi_B\rangle$; states of the form $|\varphi_A \otimes \varphi_B\rangle$ make up only a small subset (not even a subspace!) of the vectors of $\mathcal{H}_A \otimes \mathcal{H}_B$. The most general state has the form

$$\begin{aligned} |\Psi\rangle &= \alpha_{00} |0_A \otimes 0_B\rangle + \alpha_{01} |0_A \otimes 1_B\rangle + \alpha_{10} |1_A \otimes 0_B\rangle + \alpha_{11} |1_A \otimes 1_B\rangle \\ &= \alpha_{00} |X_{00}\rangle + \alpha_{01} |X_{01}\rangle + \alpha_{10} |X_{10}\rangle + \alpha_{11} |X_{11}\rangle, \end{aligned} \tag{4.3}$$

[1] More rigorously, it should be checked that the product $|\varphi_A \otimes \varphi_B\rangle$ is independent of the choice of bases in $\mathcal{H}_A$ and $\mathcal{H}_B$. This can be proved immediately; see Exercise 4.6.1.

and for $|\Psi\rangle$ to be of the form $|\varphi_A \otimes \varphi_B\rangle$ a necessary (and sufficient) condition is that

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10},$$

which *a priori* has no reason to be valid. Let us give a very simple example of a state $|\Phi\rangle$ which is *not* of the form $|\varphi_A \otimes \varphi_B\rangle$:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|0_A \otimes 1_B\rangle + |1_A \otimes 0_B\rangle\right). \tag{4.4}$$

Here

$$\alpha_{00} = \alpha_{11} = 0, \qquad \alpha_{01} = \alpha_{10} = \frac{1}{\sqrt{2}},$$

and $\alpha_{00}\alpha_{11} \neq \alpha_{01}\alpha_{10}$. We also define the tensor product $M_A \otimes M_B$ of two operators M_A and M_B as

$$[M_A \otimes M_B]_{i_A p_B; j_A q_B} = [M_A]_{i_A j_A}[M_B]_{p_B q_B}.$$

As an example, let us give the tensor product of two 2×2 matrices:

$$M_A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad M_B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

The matrix $M_A \otimes M_B$ is a 4×4 matrix, with the lines and columns ordered as 00, 01, 10, 11:

$$M_A \otimes M_B = \begin{pmatrix} aM_B & bM_B \\ cM_B & dM_B \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}.$$

A two-qubit state which does not have the form $|\varphi_A \otimes \varphi_B\rangle$ is called an *entangled state*. The *fundamental* property of such a state is the following: if $|\Psi\rangle$ is an entangled state, then the qubit A cannot be in a definite quantum state $|\varphi_A\rangle$. Let us first show this for a special case, that of the state $|\Phi\rangle$ (4.4). Let M be a physical property of the qubit A. In the space $\mathcal{H}_A \otimes \mathcal{H}_B$ this physical property is represented by $M \otimes I_B$. We calculate its expectation value $\langle\Phi|M\Phi\rangle$ as

$$\begin{aligned} \langle M\rangle_\Phi = \langle\Phi|M\Phi\rangle &= \frac{1}{2}\left[\langle 0_A \otimes 1_B| + \langle 1_A \otimes 0_B|\right]\left[|(M0_A) \otimes 1_B\rangle + |(M1_A) \otimes 0_B\rangle\right] \\ &= \frac{1}{2}\left(\langle 0_A|M0_A\rangle + \langle 1_A|M1_A\rangle\right), \end{aligned} \tag{4.5}$$

where we have used

$$\langle 0_B|0_B\rangle = \langle 1_B|1_B\rangle = 1, \qquad \langle 0_B|1_B\rangle = \langle 1_B|0_B\rangle = 0.$$

Let us prove that there is no state

$$|\varphi_A\rangle = \lambda|0_A\rangle + \mu|1_A\rangle$$

such that

$$\langle\Phi|M\Phi\rangle = \langle\varphi_A|M\varphi_A\rangle.$$

Computing the expectation value of M, we obtain

$$\langle\varphi_A|M\varphi_A\rangle = |\lambda|^2\langle 0_A|M0_A\rangle + (\lambda^*\mu\langle 0_A|M1_A\rangle + \lambda\mu^*\langle 1_A|M0_A\rangle) + |\mu|^2\langle 1_A|M1_A\rangle.$$

A necessary condition for reproducing (4.5) would be $|\lambda| = |\mu| = 1/\sqrt{2}$, but then the terms involving $\lambda^*\mu$ would not vanish (unless $\langle 0_A|M1_A\rangle$ vanishes accidentally), in contradiction with (4.5). The result (4.5) has a simple physical interpretation: the state of the qubit A is an *incoherent* mixture of 50% of the state $|0_A\rangle$ and 50% of the state $|1_A\rangle$, and not a linear superposition. In summary, it is not possible in general to describe *part* of a quantum system by a state vector.

An example of an incoherent superposition is natural or unpolarized light. It is an incoherent mixture of 50% light polarized along Ox and 50% light polarized along Oy, whereas light polarized at 45° is a *coherent* superposition of 50% light polarized along Ox and 50% light polarized along Oy:

$$|\theta = \pi/4\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + |y\rangle\right).$$

Right-handed circularly polarized light is also a coherent superposition:

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + \mathrm{i}|y\rangle\right).$$

We see the importance of phases: for example, the states $|\theta = \pi/4\rangle$ and $|R\rangle$ both correspond to 50% probability of observing a photon polarized along Ox or along Oy, but these two states are completely different: one is a linear polarization and the other is a circular polarization.

Box 4.1: Example of a physical realization of an entangled state

Obtaining an entangled state starting from a tensor product is not completely straightforward. It is necessary to introduce an interaction between the two qubits. Let us take as an example two spins 1/2. A possible interaction[2] between these two spins is

$$\hat{H} = \frac{\hbar\omega}{2}\vec{\sigma}_A \cdot \vec{\sigma}_B.$$

[2] Such an interaction might originate in the interaction between the two magnetic moments associated with the spins, but in general it will more likely be associated with an exchange interaction originating in the Pauli exclusion principle.

https://doi.org/10.1017/CBO9780511755361.006

We use the result of Exercise 4.6.4

$$\frac{1}{2}(I+\vec{\sigma}_A\cdot\vec{\sigma}_B)|ij\rangle = |ji\rangle$$

to show that

$$(\vec{\sigma}_A\cdot\vec{\sigma}_B)\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle) = (\vec{\sigma}_A\cdot\vec{\sigma}_B)|\Phi_+\rangle = |\Phi_+\rangle,$$

$$(\vec{\sigma}_A\cdot\vec{\sigma}_B)\frac{1}{\sqrt{2}}(|10\rangle-|01\rangle) = (\vec{\sigma}_A\cdot\vec{\sigma}_B)|\Phi_-\rangle = -3|\Phi_-\rangle.$$

The vectors $|\Phi_+\rangle$ and $|\Phi_-\rangle$ are eigenvectors of $\vec{\sigma}_A\cdot\vec{\sigma}_B$ with the eigenvalues[3] $+1$ and -3, respectively. Let us start at time $t=0$ from a nonentangled state, for example, $|\Phi(t=0)\rangle = |10\rangle$. To obtain its time evolution it is sufficient to decompose this state on $|\Phi_+\rangle$ and $|\Phi_-\rangle$:

$$|\Phi(t=0)\rangle = \frac{1}{\sqrt{2}}(|\Phi_+\rangle+|\Phi_-\rangle).$$

We can immediately write down the time evolution:

$$\begin{aligned}
\mathrm{e}^{-\mathrm{i}\hat{H}t/\hbar}|\Phi(0)\rangle &= \frac{1}{\sqrt{2}}\left(\mathrm{e}^{-\mathrm{i}\omega t/2}|\Phi_+\rangle+\mathrm{e}^{3\mathrm{i}\omega t/2}|\Phi_+\rangle\right)\\
&= \frac{1}{\sqrt{2}}\,\mathrm{e}^{\mathrm{i}\omega t/2}\left(\mathrm{e}^{-\mathrm{i}\omega t}|\Phi_+\rangle+\mathrm{e}^{\mathrm{i}\omega t}|\Phi_+\rangle\right)\\
&= \mathrm{e}^{\mathrm{i}\omega t/2}(\cos\omega t|10\rangle-\mathrm{i}\sin\omega t|01\rangle).
\end{aligned}$$

One can now choose $\omega t=\pi/4$ to obtain the entangled state $|\Psi\rangle$:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle-\mathrm{i}|01\rangle).$$

The difficulty is that $\hat{H}$ is in general an interaction *internal* to the system, which, in contrast to the external interactions used to manipulate the individual qubits, cannot easily be turned on and off in order to adjust t. If the interaction is a short-range one, it is possible to move the two qubits closer together and farther apart in order to control the time over which they interact. The construction of entangled states in the case of NMR using series of radiofrequency pulses will be discussed in Section 6.1. In the case of trapped ions, a two-ion state is entangled by allowing it to pass through the intermediary of an ion vibrational mode (Section 6.2). It is also possible to obtain an entangled state of two objects by using a third auxiliary object, for example, two atoms can be entangled by making them interact with a photon of a resonant cavity.

[3] Physicists will recognize these as corresponding to the triplet ($|\Phi_+\rangle$) and singlet ($|\Phi_-\rangle$) states.

4.2 The state operator (or density operator)

Now let us generalize these results to a quantum system formed of any two subsystems, where we use $|i_A\rangle(|i_B\rangle)$ to refer to an orthonormal basis of the subsystem $A(B)$. To simplify the notation, it will be convenient to make the substitutions $i_A \to i$ and $i_B \to \mu$. The most general state then is

$$|\Phi\rangle = \sum_{i,\mu} \alpha_{i\mu} |i \otimes \mu\rangle. \tag{4.6}$$

Let M be a physical property of the subsystem A:

$$|M\Phi\rangle = \sum_{i,\mu} \alpha_{i\mu} |Mi \otimes \mu\rangle.$$

We calculate the expectation value of M as

$$\begin{aligned} \langle \Phi | M\Phi \rangle &= \sum_{j,\nu} \sum_{i,\mu} \alpha^*_{j\nu} \alpha_{i\mu} \langle j \otimes \nu | Mi \otimes \mu \rangle \\ &= \sum_{i,j} \sum_{\mu} \alpha^*_{j\mu} \alpha_{i\mu} \langle j | Mi \rangle = \sum_{i,j} \rho_{ij} \langle j | Mi \rangle = \sum_{i,j} \rho_{ij} M_{ji} = \mathrm{Tr}(\rho M), \end{aligned} \tag{4.7}$$

where $\mathrm{Tr}A$ stands for the *trace* $\sum_i A_{ii}$ of an operator A, that is, the sum of its diagonal elements. It is straightforward to prove that $\mathrm{Tr}AB = \mathrm{Tr}BA$, from which one deduces that the trace is basis independent. In obtaining (4.7) we have used

$$\langle j \otimes \nu | Mi \otimes \mu \rangle = \delta_{\nu\mu} \langle j | Mi \rangle,$$

because in $\mathcal{H}_A \otimes \mathcal{H}_B$, M is actually $M \otimes I_B$. The equation (4.7) defines an object which will play a crucial role, the *state operator* (or density operator)[4] ρ of the subsystem A:

$$\boxed{\rho_{ij} = \textstyle\sum_\mu \alpha_{i\mu} \alpha^*_{j\mu}} \tag{4.8}$$

The state operator of the subsystem A is called the *reduced state operator* and is denoted ρ_A. The subsystem A is not in general described by a state vector, but by a state operator which allows us to compute the expectation values of physical properties. This state operator is Hermitian ($\rho = \rho^\dagger$), positive[5] ($\rho \geq 0$ as is easily proved from (4.8)), and it has unit trace $\mathrm{Tr}\rho = 1$:

$$\mathrm{Tr}\rho = \sum_i \rho_{ii} = \sum_i \sum_\mu |\alpha_{i\mu}|^2 = ||\Phi||^2 = 1.$$

[4] The standard terminology is "density operator." However, this historical term is completely unjustified: to what density does it refer? We prefer the term "state operator," which is the generalization to mixtures of the term "state vector" for pure states.

[5] A positive (or nonnegative) operator A is one for which $\langle \varphi | A\varphi \rangle$ is real and $\langle \varphi | A\varphi \rangle \geq 0 \ \forall |\varphi\rangle$ (it is strictly positive if $\langle \varphi | A\varphi \rangle > 0$). It is necessarily Hermitian in a complex space. A necessary and sufficient condition for a Hermitian operator to be positive is that its eigenvalues be nonnegative.

Physical states such as those studied in Chapter 2 are called *pure states*: they are described by a state vector. It is easy to check that the state operator of a pure state obeys $\rho^2 = \rho$ and vice versa: any state operator satisfying $\rho^2 = \rho$ describes a pure state (Exercise 4.6.2). However, the most general description of a quantum system must be given in terms of a state operator.

Since ρ is Hermitian, it can be diagonalized and written in an orthonormal basis $|i\rangle$ as

$$\rho = \sum_i \mathsf{p}_i |i\rangle\langle i|. \tag{4.9}$$

Since ρ is positive $\mathsf{p}_i \geq 0$, and the condition $\mathrm{Tr}\rho = 1$ gives $\sum_i \mathsf{p}_i = 1$, so that the p_i can be interpreted as probabilities. It can be said that ρ represents a *statistical mixture* (or simply a *mixture*) of states $|i\rangle$, each state $|i\rangle$ having a probability p_i; in the preparation stage, each state $|i\rangle$ is prepared with a probability p_i, without any phase coherence between the different states $|i\rangle$.

It is easy to generalize (4.8) when a quantum system (AB) is described by a state operator ρ_{AB} with matrix elements[6] $\rho^{AB}_{i\mu;j\nu}$, and not by a state vector. Let M be a physical property of the system A, which is therefore represented in the space $\mathcal{H}_A \otimes \mathcal{H}_B$ by the Hermitian operator $M \otimes I_B$. We wish to find an operator ρ_A such that the expectation value of M is given by

$$\langle M \rangle = \mathrm{Tr}(\rho_A M). \tag{4.10}$$

Using the same argument as above, we calculate the expectation value of $M \otimes I_B$:

$$\begin{aligned} \langle M \otimes I_B \rangle &= \mathrm{Tr}_{AB}\left(\rho_{AB}[M \otimes I_B]\right) \\ &= \sum_{ij\mu\nu} \rho^{AB}_{i\mu;j\nu} M_{ji} \delta_{\nu\mu} = \sum_{i,j} M_{ji} \sum_{\mu} \rho^{AB}_{i\mu;j\mu}. \end{aligned} \tag{4.11}$$

The expression generalizing (4.8) then shows that ρ_A has the form

$$\boxed{\rho^A_{ij} = \textstyle\sum_\mu \rho^{AB}_{i\mu;j\mu}, \qquad \rho_A = \mathrm{Tr}_B \rho_{AB}} \tag{4.12}$$

because the expectation value of M is given by (4.10) with the choice (4.12) for ρ_A. It can be shown that (4.12) is the unique solution giving the correct expectation value of M. The operation which takes us from ρ_{AB} to ρ_A is called the *partial trace* of ρ_{AB} with respect to B.

The importance of the concept of state operator is confirmed by the *Gleason theorem*, which we shall state without proof and which basically says that the most general description of a quantum system is given by a state operator.

[6] To make the notation more readable, AB is written as a superscript to make room for the subscripts labeling the matrix elements.

The Gleason theorem Let a set of projectors $\mathcal{P}_i$ act on a Hilbert space of states $\mathcal{H}$ and let there be a test associated with each $\mathcal{P}_i$ where the probability $\mathsf{p}(\mathcal{P}_i)$ of passing the test satisfies

$$0 \leq \mathsf{p}(\mathcal{P}_i) \leq 1, \qquad \mathsf{p}(I) = 1,$$

as well as

$$\mathsf{p}(\mathcal{P}_i \cup \mathcal{P}_j) = \mathsf{p}(\mathcal{P}_i) + \mathsf{p}(\mathcal{P}_j) \text{ if } \mathcal{P}_i \cap \mathcal{P}_j = \emptyset \,(\text{or } \mathcal{P}_i \mathcal{P}_j = \delta_{ij} \mathcal{P}_i).$$

This property should hold for any set of mutually orthogonal $\mathcal{P}_i$ such that $\sum_i \mathcal{P}_i = I$. Then if the dimension of $\mathcal{H} \geq 3$, there exists a positive Hermitian operator ρ of unit trace such that

$$\mathsf{p}(\mathcal{P}_i) = \mathrm{Tr}(\rho \mathcal{P}_i).$$

In other words, if we wish to associate a probability $\mathsf{p}(\mathcal{P}_i)$ with an ensemble of tests $\mathcal{P}_i$ which has "reasonable" properties, then this probability will be given by a trace involving a state operator.

If $|\Phi\rangle$ is a tensor product of the form $|\varphi_A \otimes \varphi_B\rangle$ and if to $|\Phi\rangle$ we apply a unitary transformation which is a tensor product of transformations acting on A and B, $U_A \otimes U_B$, this corresponds simply to a change of orthonormal basis in the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and an entangled state cannot be made. To make an entangled state, *it is necessary to make the two qubits interact*. In contrast to the superposition of two states which is a basis dependent concept, entanglement is a basis independent concept. The Schmidt purification theorem, whose proof is left to Exercise 4.6.5, allows us to give more precise statements.

The Schmidt purification theorem Any state $|\Phi\rangle$ of $\mathcal{H}_A \otimes \mathcal{H}_B$ can be written as

$$|\Phi\rangle = \sum_i \sqrt{\mathsf{p}_i}\, |i_A \otimes i_B\rangle \tag{4.13}$$

with

$$\langle i_A | j_A \rangle = \langle i_B | j_B \rangle = \delta_{ij}.$$

The states $|i_A\rangle$ and $|i_B\rangle$ clearly depend on $|\Phi\rangle$. This expression immediately gives the reduced state operators ρ_A and ρ_B. To show this, let us begin with the full state operator ρ_{AB}:

$$\rho_{AB} = |\Phi\rangle\langle\Phi| = \sum_{i,j} |i_A \otimes i_B\rangle\langle j_A \otimes j_B|.$$

Let $|i\rangle$ be an orthonormal basis of $\mathcal{H}$. It is easy to calculate the traces using the following result:

$$\mathrm{Tr}|\varphi\rangle\langle\psi| = \sum_i \langle i|\varphi\rangle\langle\psi|i\rangle = \sum_i \langle\psi|i\rangle\langle i|\varphi\rangle = \langle\psi|\varphi\rangle, \tag{4.14}$$

because $\sum_i |i\rangle\langle i| = I$ and so the state operators ρ_A and ρ_B are given by

$$\rho_A = \sum_i \mathsf{p}_i |i_A\rangle\langle i_A|, \qquad \rho_B = \sum_i \mathsf{p}_i |i_B\rangle\langle i_B| \tag{4.15}$$

with the *same* p_i. The number of nonzero p_i is the *Schmidt number*. If we apply to the state $|\Phi\rangle$ a unitary transformation which is the tensor product of transformations acting on A and B, $U_A \otimes U_B$, we cannot change the Schmidt number by manipulating the qubits A and B *separately*. We recover the above result for a tensor product by noting that the Schmidt number of a tensor product is 1. If $\mathcal{H}_A$ and $\mathcal{H}_B$ have dimension N, a state of the form

$$|\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \mathrm{e}^{\mathrm{i}\alpha(i)} |i_A \otimes i_B\rangle, \tag{4.16}$$

where $\exp[\mathrm{i}\alpha(i)]$ is a phase factor, is termed a *maximally entangled state*, or a *Bell state*. For example, $|\Phi\rangle$ in (4.4) is a Bell state. The reduced state matrices corresponding to (4.16) are multiples of the identity: $\rho_A = \rho_B = I/N$. This is a characteristic property of maximally entangled states.

4.3 The quantum no-cloning theorem

The indispensable condition for the quantum cryptography method of Section 2.5 to be perfectly secure is that the spy Eve not be able to reproduce (clone) the state of the particle sent by Alice to Bob while leaving Bob's measurement result unchanged, so that interception of the message is undetectable. The impossibility of Eve doing this is guaranteed by the quantum no-cloning theorem. To demonstrate this theorem, we suppose that we wish to duplicate an *unknown* quantum state $|\chi_1\rangle$. Of course, if $|\chi_1\rangle$ were known, there would be no problem because the preparation procedure would be known. The system on which we wish to print the copy is denoted $|\varphi\rangle$ and is the equivalent of a blank page. For example, if we wish to clone a spin 1/2 state $|\chi_1\rangle$, then $|\varphi\rangle$ will also be a state of spin 1/2. The evolution of the state vector in the cloning process must be of the form

$$|\chi_1 \otimes \varphi\rangle \to |\chi_1 \otimes \chi_1\rangle. \tag{4.17}$$

This evolution is governed by a unitary operator U whose exact form is unimportant:

$$|U(\chi_1 \otimes \varphi)\rangle = |\chi_1 \otimes \chi_1\rangle. \tag{4.18}$$

This operator U must be universal (because the photocopying operation cannot depend on the state to be copied) and therefore independent of $|\chi_1\rangle$, which is unknown by hypothesis. If we wish to clone a second original $|\chi_2\rangle$ we must have

$$|U(\chi_2 \otimes \varphi)\rangle = |\chi_2 \otimes \chi_2\rangle.$$

Let us now evaluate the scalar product

$$X = \langle \chi_1 \otimes \varphi | U^\dagger U (\chi_2 \otimes \varphi) \rangle$$

in two different ways:

$$\begin{array}{ll} (1) & X = \langle \chi_1 \otimes \varphi | \chi_2 \otimes \varphi \rangle = \langle \chi_1 | \chi_2 \rangle, \\ (2) & X = \langle \chi_1 \otimes \chi_1 | \chi_2 \otimes \chi_2 \rangle = (\langle \chi_1 | \chi_2 \rangle)^2. \end{array} \tag{4.19}$$

The result is that either $|\chi_1\rangle \equiv |\chi_2\rangle$ or $\langle \chi_1 | \chi_2 \rangle = 0$. It is possible to clone a state $|\chi_1\rangle$ or an orthogonal state, but not a linear superposition of the two. This proof of the no-cloning theorem explains why it is not possible in quantum cryptography to restrict oneself to a basis of orthogonal polarization states $\{|x\rangle, |y\rangle\}$ for photons. It is the use of linear superpositions of the polarization states $|x\rangle$ and $|y\rangle$ which allows the presence of a spy to be detected. The no-cloning theorem makes it impossible for Eve to clone the photon sent by Alice to Bob when its polarization is unknown to Bob; if Eve could perform this cloning, she would then be able to produce a large number of such photons and measure the polarization without problem, see Exercise 2.6.1.

4.4 Decoherence

Let us consider two qubits A and B in the entangled state

$$|\Psi\rangle = \lambda |0_A 0_B\rangle + \mu |1_A 1_B\rangle$$

and compute the state matrix of qubit A using (4.14):

$$\rho_A = \mathrm{Tr}_B |\Psi\rangle\langle\Psi| = |\lambda|^2 |0_A\rangle\langle 0_A| + |\mu|^2 |1_A\rangle\langle 1_A| = \begin{pmatrix} |\lambda|^2 & 0 \\ 0 & |\mu|^2 \end{pmatrix}. \tag{4.20}$$

All the information on the phases of the complex numbers λ and μ seems to have disappeared, and we are left in the $\{|0_A\rangle, |1_A\rangle\}$ basis with a diagonal state matrix. It is easy to generalize the preceding argument and derive the following theorem: *if a pair of states of the system of interest becomes correlated with mutually orthogonal states of another system, then all the phase coherence between the orthogonal states of the first system is lost*. This loss of phase coherence is called *decoherence*. Since the information on the phases is contained in the nondiagonal matrix elements of ρ, these matrix elements are often called *coherences*. However, this theorem should be interpreted with care. First of all, although ρ_A is diagonal in the $\{|0_A\rangle, |1_A\rangle\}$ basis, this will not be the case in general in another basis except if $\rho_A = I/2$. For example, in the $\{|+_A\rangle, |-_A\rangle\}$ basis

$$|\pm_A\rangle = \frac{1}{\sqrt{2}} (|0_A\rangle \pm |1_A\rangle)$$

https://doi.org/10.1017/CBO9780511755361.006

ρ_A (4.20) takes the form

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & |\lambda|^2 - |\mu|^2 \\ |\lambda|^2 - |\mu|^2 & 1 \end{pmatrix}. \tag{4.21}$$

The second remark is that the information on the phases is not really lost: it is only *locally* lost, that is, it is lost if we restrict ourselves to measurements of physical properties of qubit A. Joint physical properties of qubits A and B will depend in general on the phases of λ and μ. In the case of a quantum computer, a large number of qubits become entangled and the state matrix of any individual qubit is almost diagonal. However, if the qubits are perfectly isolated, the global state vector retains the phase information, and indeed this must be so if we want the quantum computation to be meaningful. The third remark is that coherence may be recovered dynamically, even if it seems to have been temporarily lost. To explain this point, let us assume that the states $|0_B\rangle$ and $|1_B\rangle$ are not exactly orthogonal, but that $\langle 0_B|1_B\rangle = \varepsilon$, $|\varepsilon| \ll 1$, and that the two-qubit Hamiltonian has the form

$$\hat{H} = \frac{\hbar}{2} K \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \frac{\hbar}{2} KX. \tag{4.22}$$

It is easily checked (for example, by relabeling the rows and columns of the matrix X in the order 00, 11, 01, 11) that the evolution operator is

$$\exp(-\mathrm{i}\hat{H}t/\hbar) = I_A \otimes I_B \cos\frac{Kt}{2} - \mathrm{i}X \sin\frac{Kt}{2}. \tag{4.23}$$

If we start at time $t = 0$ from the state $|\Psi_0\rangle = |0_A 0_B\rangle$, the state vector at time $t = \pi/2K$ will be

$$\Psi\left(t = \frac{\pi}{2K}\right) = \frac{1}{\sqrt{2}}\left(|0_A 0_B\rangle - \mathrm{i}|1_A 1_B\rangle\right),$$

and the corresponding state matrix of qubit A becomes

$$\rho_A = \frac{1}{2}\begin{pmatrix} 1 & \mathrm{i}\varepsilon \\ -\mathrm{i}\varepsilon & 1 \end{pmatrix}. \tag{4.24}$$

It appears that the state matrix exhibits almost perfect decoherence. However, if we wait until time $t = \pi/K$ the state vector becomes $-\mathrm{i}|1_A 1_B\rangle$. It is possible to work out a more precise model where the states $|0_B\rangle$ and $|1_B\rangle$ represent almost nonoverlapping, and consequently almost orthogonal, wave packets. It can then be shown that $K \propto \varepsilon$, so that the oscillations predicted by (4.23) have a very long period, and the qubit A may appear to have lost coherence for a long time.

https://doi.org/10.1017/CBO9780511755361.006

As long as we have complete control over all the quantum variables, we have only "adiabatic" or "false" decoherence: at some instant of time, the measurement of local physical properties may not depend on the phases, but the phases are still there and they reappear in the measurement of more complex physical properties and/or from dynamical evolution. We shall face "true" decoherence if we lose control over some of the quantum variables. For example, suppose that in a Young's slit experiment performed with complex molecules, such as fullerenes in a thermally excited state, a photon is emitted when the molecule passes through one of the slits and escapes to infinity. If the wavelength of this photon is shorter than the distance between the two slits,[7] the state of the photon will be almost orthogonal to that of a photon emitted by the molecule going through the other slit. The path of the molecule will become correlated with orthogonal degrees of freedom of the environment, so that we get information on which path is taken and the interference is destroyed. In this case it is clear that we have lost control over the photon degrees of freedom, and information has leaked into the environment in an uncontrollable fashion. This is an example of true decoherence: the system becomes entangled with orthogonal states of the environment, but we do not have access to these states. It can also be said that "the environment measures the system," since the emitted photon measures the path of the molecule. In general, the environment is a very complicated quantum system, and quantum coherences are distributed over such a large number of degrees of freedom that they become unobservable.

It follows from the preceding discussion that if we want to retain control over the operation of a quantum computer, it is essential that the computer be immune to decoherence: the qubits must not be coupled to the *quantum* degrees of freedom of their environment. In other words, an ideal quantum computer must be completely isolated. In many models the characteristic time which controls the decay of coherence, called the *decoherence time*, is inversely proportional to some positive power of the size of the system, often the square of this size. Thus, we expect decoherence to be more and more important as the number of qubits increases. The following example will illustrate this property. Suppose that the interaction of a qubit with the environment during a time interval Δt has the following effect on a single qubit:

$$|0\rangle \to |0\rangle, \qquad |1\rangle \to -|1\rangle$$

with a probability $\mathsf{p} = \Gamma \Delta t \ll 1$. The decoherence time is $\tau_{\mathrm{D}} = 1/\Gamma$. We have not explicitly written out the states of the environment, the only important point being

[7] This will happen if the temperature of the molecule is sufficiently high, so that it can be found in a highly excited state.

that the states $|0\rangle$ and $|1\rangle$ do not become entangled with states of the environment. If the qubit is in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$

then the interaction will transform it into

$$|\psi'\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \sigma_z|4\rangle \tag{4.25}$$

with probability p, and the initial phase relation between the two components of $|\psi\rangle$ will be lost, introducing errors in the computation. The process (4.25) is conventionally called *phase flip*. Now, consider the n-qubit state

$$|\Psi_n\rangle = \frac{1}{\sqrt{2}}(|00\cdots0\rangle + |11\cdots1\rangle). \tag{4.26}$$

The phase relation between the two components of $|\Psi\rangle$ will be lost as soon as *one* of the qubits flips sign. It is reasonable to assume that each of the qubits interacts with the environment independently of the others. Then in the time interval Δt the state $|\Psi\rangle$ will be transformed into

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\cdots0\rangle - |11\cdots1\rangle\right)$$

with probability $\mathsf{p}_n = n\Gamma\Delta t$. In other words, the decoherence time for the system of n qubits will be shorter by a factor of n compared to the decoherence time for a single qubit: $\tau_{\mathrm{D}}(n) = \tau_{\mathrm{D}}/n$.

To conclude this section, let us describe a simple model for the coupling of a qubit to its environment which leads to phase decoherence. This model is conventionally called the *phase damping channel*. In this model the state of the qubit does not change, but the environment, which is initially in the state $|0_E\rangle$, is sent with probability p into the state $|1_E\rangle(|2_E\rangle)$ if the qubit is in the state $|0_A\rangle(|1_A\rangle)$:

$$\begin{aligned}
|0_A0_E\rangle &\to \sqrt{1-\mathsf{p}}|0_A0_E\rangle + \sqrt{\mathsf{p}}|0_A1_E\rangle = |0_A\rangle \otimes \left(\sqrt{1-\mathsf{p}}\,|0_E\rangle + \sqrt{\mathsf{p}}\,|1_E\rangle\right), \\
|1_A0_E\rangle &\to \sqrt{1-\mathsf{p}}\,|1_A0_E\rangle + \sqrt{\mathsf{p}}\,|1_A2_E\rangle = |1_A\rangle \otimes \left(\sqrt{1-\mathsf{p}}\,|0_E\rangle + \sqrt{\mathsf{p}}\,|2_E\rangle\right).
\end{aligned} \tag{4.27}$$

One can imagine, for example, that the qubit elastically scatters a photon of the cosmic microwave background, and that the final state of the photon depends on the state of the qubit. We note that the states $|0_A\rangle$ and $|1_A\rangle$ do not become entangled with the environment, while any linear combination of these

two states would become entangled. States which do not become entangled with their environment are termed *pointer states*. The most general initial state is

$$|\Phi\rangle = (\lambda|0_A\rangle + \mu|1_A\rangle) \otimes |0_E\rangle \ , \tag{4.28}$$

so that the initial state matrix of the qubit is

$$\rho_A = \begin{pmatrix} |\lambda|^2 & \lambda\mu^* \\ \lambda^*\mu & |\mu|^2 \end{pmatrix} = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix}. \tag{4.29}$$

The process (4.27) can be represented in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_E$ by a unitary operator U, which is only partially known, [8] and

$$U|\Phi\rangle = \lambda\sqrt{1-\mathsf{p}}\,|0_A 0_E\rangle + \lambda\sqrt{\mathsf{p}}\,|0_A 1_E\rangle + \mu\sqrt{1-\mathsf{p}}\,|1_A 0_E\rangle + \mu\sqrt{\mathsf{p}}\,|1_A 2_E\rangle. \tag{4.30}$$

Using (4.14), it is now straightforward to find the transformed state matrix ρ'_A of the qubit: [9]

$$\begin{aligned} \rho'_A = \mathrm{Tr}_E\left[U|\Phi\rangle\langle\Phi|U^\dagger\right] &= |\lambda|^2|0_A\rangle\langle 0_A| \\ &+ |\mu|^2|1_A\rangle\langle 1_A| + (\lambda\mu^*(1-\mathsf{p})|0_A\rangle\langle 1_A| + \mathrm{H.c.}) \end{aligned} \tag{4.31}$$

or

$$\rho'_A = \begin{pmatrix} \rho_{00} & (1-\mathsf{p})\rho_{01} \\ (1-\mathsf{p})\rho_{10} & \rho_{11} \end{pmatrix}. \tag{4.32}$$

After n iterations of (4.30) we find

$$\rho'^{(n)}_A = \begin{pmatrix} \rho_{00} & (1-\mathsf{p})^n\rho_{01} \\ (1-\mathsf{p})^n\rho_{10} & \rho_{11} \end{pmatrix} \xrightarrow[n\to\infty]{} \begin{pmatrix} \rho_{00} & \rho_{01}\mathrm{e}^{-\Gamma t} \\ \rho_{10}\mathrm{e}^{-\Gamma t} & \rho_{11} \end{pmatrix}. \tag{4.33}$$

Indeed, if we assume that p is proportional to Δt, $\mathsf{p} = \Gamma\Delta t$, and we observe the qubit during a time interval t, $n = t/\Delta t$, then

$$\rho_{01}(t) = \rho_{01}(1-\Gamma\Delta t)^{t/\Delta t} \xrightarrow[\Delta t\to 0]{} \rho_{01}\mathrm{e}^{-\Gamma t}. \tag{4.34}$$

The initial state decays into an incoherent mixture of the states $|0_A\rangle$ and $|1_A\rangle$ with a decoherence time of $\tau_D = 1/\Gamma$. For $t \to \infty$, the state matrix becomes diagonal

$$\rho(t) \xrightarrow[t\to\infty]{} \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix}.$$

[8] U is a 6×6 matrix and only four of its matrix elements are given in (4.27), but the missing entries can be filled in while preserving the unitarity.

[9] For example, $\mathrm{Tr}_E\left(|0_A 1_E\rangle\langle 1_A 1_E|\right) = |0_A\rangle\langle 1_A|$.

It is essential to observe that no unitary evolution in $\mathcal{H}_A$ can lead from the initial state matrix ρ_A (4.29) to the final diagonal from. Indeed, a unitary transformation transforms a pure state into a pure state, and there is no unitary operator such that

$$U\rho_A U^\dagger = \begin{pmatrix} |\lambda|^2 & 0 \\ 0 & |\mu|^2 \end{pmatrix}.$$

The unitary evolution takes place in the $\mathcal{H}_A \otimes \mathcal{H}_B$ Hilbert space.

4.5 The Bell inequalities

One proof [10] of the nonclassical nature of the correlations of an entangled state is given by the Bell inequalities, which we shall explain using an example. Let us suppose that we have constructed pairs of photons A and B traveling in opposite directions whose linear polarizations along Ox or Oy are entangled (Fig. 4.1):

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left(|x_A x_B\rangle + |y_A y_B\rangle\right). \tag{4.35}$$

Alice and Bob are able to measure the polarizations of the photons issued from a single pair, because the photon pairs are separated by a time interval sufficient for them not to overlap. Alice measures the polarization of photon A and Bob the polarization of photon B, then they check to see whether the polarizations are correlated: if Alice and Bob orient *both* of their analyzers either along the axis Ox or along Oy, they can check that the two photons either pass through both

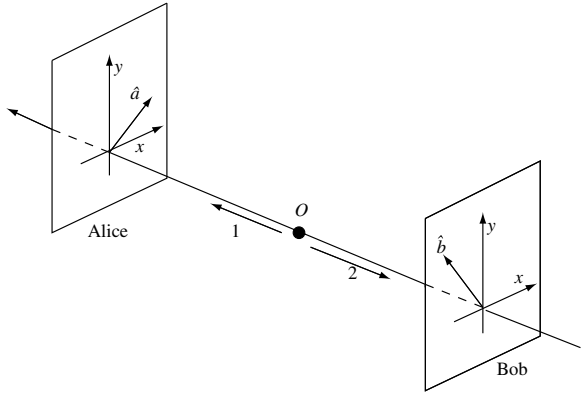

Figure 4.1 Configuration of an EPR type of experiment.

[10] This section is a digression from the main topic and may be omitted from a first reading.

their analyzers or are stopped by both of them. Mathematically, this results from the probability amplitudes

$$\langle x_A x_B|\Phi\rangle = \frac{1}{\sqrt{2}}, \qquad \langle x_A y_B|\Phi\rangle = 0, \qquad \langle y_A x_B|\Phi\rangle = 0, \qquad \langle y_A y_B|\Phi\rangle = \frac{1}{\sqrt{2}}.$$

To write this result in a convenient form, it is useful to describe the correlation of the polarizations as follows (A_x and B_x are just the operator $M = \mathcal{P}_x - \mathcal{P}_y$ introduced in Section 2.4):

$$A_x = +1 \text{ if polarization } A \parallel Ox, \qquad B_x = +1 \text{ if polarization } B \parallel Ox,$$
$$A_x = -1 \text{ if polarization } A \parallel Oy, \qquad B_x = -1 \text{ if polarization } B \parallel Oy.$$

Under these conditions, Alice and Bob observe, for example, the following series of results:

$$\text{Alice}: \quad A_x = +--+-+++--,$$
$$\text{Bob}: \quad B_x = +--+-+++--,$$

which gives the expectation value of the product $A_x B_x$:

$$\langle A_x B_x\rangle = 1. \tag{4.36}$$

Upon reflection, this result is not very surprising. It is a variation of the game of the two customs inspectors.[11] Two travelers A and B, each carrying a suitcase, depart in opposite directions from the origin and eventually are checked by two customs inspectors Alice and Bob. One of the suitcases contains a red ball and the other a green ball, but the travelers have picked up their closed suitcases at random and do not know what color the ball inside is. If Alice checks the suitcase of traveler A, she has a 50% chance of finding a green ball. But if in fact she finds a green ball, clearly Bob will find a red ball with 100% probability! Correlations between the two suitcases were introduced at the time of departure, and these correlations reappear as a correlation between the results of Alice and Bob.

However, as first noted by Einstein, Podolsky, and Rosen (EPR) in a celebrated paper[12] (which used a different example, ours being due to Bohm), the situation becomes much less commonplace if Alice and Bob decide to perform another series of measurements using the orientations $\hat{\theta}$ and $\hat{\theta}_\perp$ instead of Ox and Oy. In fact, $|\Phi\rangle$ is invariant under rotation about Oz, because (2.19) can be used to show immediately (Exercise 4.6.8) that $|\Phi\rangle$ can also be written as

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|\theta_A \theta_B\rangle + |\theta_{\perp A}\theta_{\perp B}\rangle\right). \tag{4.37}$$

[11] Invented just for this occasion!

[12] Einstein *et al.* (1935). The term "EPR paradox" is sometimes used, but in fact there is nothing paradoxical in the EPR analysis.

If A_x is replaced by A_θ, then

$$A_\theta = +1 \text{ if polarization } A \parallel \hat{\theta}, \qquad B_\theta = +1 \text{ if polarization } B \parallel \hat{\theta},$$
$$A_\theta = -1 \text{ if polarization } A \parallel \hat{\theta}_\perp, \qquad B_\theta = -1 \text{ if polarization } B \parallel \hat{\theta}_\perp.$$

Then as in (4.16) we will have

$$\langle A_\theta B_\theta \rangle = 1. \tag{4.38}$$

Knowing the polarization of photon A along $\hat{\theta}$, we can predict with certainty the polarization of photon B along $\hat{\theta}$ (or $\hat{\theta}_\perp$) for any choice of θ. One gets the impression that Alice and Bob can communicate instantaneously, even if they are separated by several light years, and thus that relativity is violated. Of course, this is only an illusion, because in order to be able to compare their results and check (4.38), Alice and Bob must be able to exchange messages via a classical path and therefore at a speed less than that of light. Moreover, it is straightforward to reproduce these correlations using a classical model (Fig. 4.2), in which the correlations are fixed in advance.

However, this will no longer be possible if Alice and Bob decide to use different axes $\hat{a}$ and $\hat{b}$. We use the following generalization of the case of parallel axes (see the example in Fig. 4.2): polarization $\parallel \hat{a} : A(\hat{a}) = +1, \ldots,$ polarization

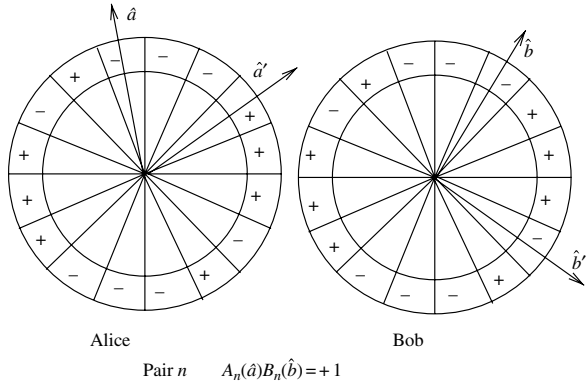

Figure 4.2 A classical model for EPR correlations. The suitcases of travelers A and B are now circles divided into small angular sectors defining the orientations $\hat{a}, \ldots, \hat{b}'$ in the plane xOy, which are labeled $+$ for polarization in the given direction or $-$ for polarization in the orthogonal direction. The two circles are identical and two diametrically opposite points are identified and both labeled $+$ or $-$. The figure corresponds to $A_{\hat{a}} = -1$, $A_{\hat{a}'} = +1$, $B_{\hat{b}} = -1$, and $B_{\hat{b}'} = -1$.

$\perp \hat{b} : B(\hat{b}) = -1$. Then we construct the expectation value $E(\hat{a}, \hat{b})$ measured in N experiments with $N \to \infty$:

$$E(\hat{a}, \hat{b}) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} A_n(\hat{a}) B_n(\hat{b}). \tag{4.39}$$

Let us now construct the combination X_n with the orientations ($\hat{a}$ or $\hat{a}'$) for a and ($\hat{b}$ or $\hat{b}'$) for b, $A_n = A_n(\hat{a})$, $B'_n = B_n(\hat{b}'), \ldots$, where n numbers the pairs, and Alice and Bob are able to identify unambiguously the photons belonging to the same pair:

$$X_n = A_n B_n + A_n B'_n + A'_n B'_n - A'_n B_n = A_n(B_n + B'_n) + A'_n(B'_n - B_n). \tag{4.40}$$

Here $X_n = \pm 2$, which leads to the following *Bell inequality*:

$$|\langle X \rangle| = \left| \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} X_n \right| \leq 2. \tag{4.41}$$

The quantity X_n is "counterfactual" because it cannot be measured for a single pair: there are four possible choices for the orientation of the measurement axes, but only one choice for a particular pair. The EPR point of view is that *each photon carries all the information on its intrinsic polarization* and that the four combinations $A_n B_n \cdots A'_n B'_n$ exist for any pair n, even if only one can be measured in a given experiment. However, this does not necessarily mean that the EPR viewpoint is incorrect, because, as Feynman has stated, "It is not true that we can pursue science completely by using only those concepts which are directly subject to experiment." Proof that the EPR viewpoint is incorrect will come from experiment.

What does quantum physics actually say? It is easy to calculate $E(\hat{a}, \hat{b})$. Owing to the rotational invariance, it is always possible to choose $\hat{a}$ parallel to Ox. We write $|\Phi\rangle$ as

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left[|x_A\rangle \left(\cos\theta |\theta_B\rangle - \sin\theta |\theta_{\perp B}\rangle\right) + |y_A\rangle \left(\sin\theta |\theta_B\rangle + \cos\theta |\theta_{\perp B}\rangle\right) \right],$$

writing out $|x_B\rangle$ and $|y_B\rangle$ as functions of $|\theta_B\rangle$ and $|\theta_{\perp B}\rangle$ (see (2.19)). We can then immediately calculate the scalar products:

$$\langle x_A \theta_B | \Phi \rangle = \frac{1}{\sqrt{2}} \cos\theta, \qquad \langle x_A \theta_{\perp B} | \Phi \rangle = -\frac{1}{\sqrt{2}} \sin\theta,$$

$$\langle y_A \theta_B | \Phi \rangle = \frac{1}{\sqrt{2}} \sin\theta, \qquad \langle y_A \theta_{\perp B} | \Phi \rangle = \frac{1}{\sqrt{2}} \cos\theta,$$

and so

$$E(\hat{x}, \hat{\theta}) = \frac{1}{2} \left[2\cos^2\theta - 2\sin^2\theta \right] = \cos(2\theta), \tag{4.42}$$

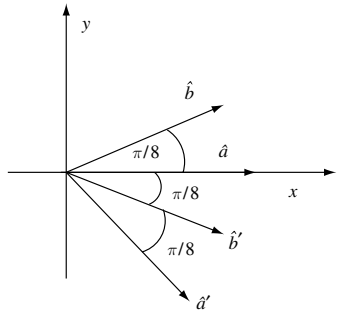

Figure 4.3 An optimal angular configuration.

or, in a form which is manifestly rotationally invariant,

$$E(\hat{a}, \hat{b}) = \cos(2\hat{a} \cdot \hat{b}).$$

With the angles chosen as in Fig. 4.3 we find

$$|\langle X \rangle| = 2\sqrt{2} \simeq 2.82. \tag{4.43}$$

There is no classical correlation which can reproduce the quantum correlations: *the quantum correlations are too strong to be explained classically*. Even if the qubits A and B are several light years apart, they cannot be considered as separate entities and there is no local probabilistic classical algorithm which is capable of reproducing their correlations. The qubits A and B form a unique entity; they are nonseparable, or entangled.

Let us also note that the no-cloning theorem forbids propagation of information at superluminal velocities. Alice can choose to use either the basis $\{|x\rangle, |y\rangle\}$ or the basis $\{|+\pi/4\rangle, |-\pi/4\rangle\}$ to measure the polarization of her photon. If Bob could clone his own photon, he would be able to measure its polarization and instantly deduce the basis chosen by Alice for her corresponding photon, even if she were located several light years away from him.

4.6 Exercises

4.6.1 Basis independence of the tensor product

Let us suppose that we have constructed the tensor product of two spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ starting from the bases $\{|m_A\rangle\}$ and $\{|n_B\rangle\}$:

$$|\varphi_A \otimes \chi_B\rangle = \sum_{m,n} c_m d_n |m_A \otimes n_B\rangle.$$

Let $|i_A\rangle$ and $|j_B\rangle$ be two other orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$ deduced from the bases $|m_A\rangle$ and $|n_B\rangle$ by the unitary transformations $R\,(R^{-1} = R^{\dagger})$ and $S\,(S^{-1} = S^{\dagger})$, respectively:

$$|i_A\rangle = \sum_m R_{im}\,|m_A\rangle, \qquad |j_B\rangle = \sum_n S_{jn}\,|n_B\rangle.$$

Calculate the tensor product $|i \otimes j\rangle$. To construct the tensor product, we now decompose $|\varphi\rangle$ and $|\chi\rangle$ in the respective bases $|i\rangle$ and $|j\rangle$:

$$|\varphi\rangle = \sum_{i=1}^{N} \hat{c}_i |i_A\rangle, \qquad |\chi\rangle = \sum_{j=1}^{M} \hat{d}_j |j_B\rangle.$$

Show that

$$\sum_{i,j} \hat{c}_i \hat{d}_j |i_A \otimes j_B\rangle = |\varphi \otimes \chi\rangle.$$

4.6.2 Properties of the state operator

1. Starting from (4.9),

$$\rho = \sum_i \mathsf{p}_i |i\rangle\langle i|, \qquad \sum_i \mathsf{p}_i = 1,$$

show that the most general state operator ρ must possess the following properties.

1. It must be Hermitian: $\rho = \rho^{\dagger}$.
2. It must have unit trace: $\mathrm{Tr}\rho = 1$.
3. It must be positive: $\langle\varphi|\rho|\varphi\rangle \geq 0\ \forall|\varphi\rangle$.

Show that the expectation value of a physical property M is

$$\langle M\rangle = \mathrm{Tr}(\rho M).$$

2. Show also that if $\rho^2 = \rho$, then all the p_i are zero except one, which is equal to unity, and prove that the condition $\rho^2 = \rho$ is the necessary and sufficient condition for a state to be pure. Also show that $\mathrm{Tr}\rho^2 = 1$ is a necessary and sufficient condition for the state operator to describe a pure state.

4.6.3 The state operator for a qubit and the Bloch vector

1. We wish to find the most general form of ρ for a qubit; ρ will be represented by a 2×2 state matrix. Show that the most general Hermitian matrix of unit trace in $\mathcal{H}$ has the form

$$\rho = \begin{pmatrix} a & c \\ c^* & 1-a \end{pmatrix},$$

https://doi.org/10.1017/CBO9780511755361.006

where a is a real number and c is a complex number. Show that the positivity of the eigenvalues of ρ introduces a supplementary constraint on the matrix elements:

$$0 \leq a(1-a) - |c|^2 \leq \frac{1}{4}.$$

Show that the necessary and sufficient condition for the quantum state described by ρ to be represented by a vector of $\mathcal{H}$ is $a(1-a) = |c|^2$. Calculate a and c for the matrix ρ describing the normalized state vector $|\psi\rangle = \lambda|0\rangle + \mu|1\rangle$ with $|\lambda|^2 + |\mu|^2 = 1$, and show that in this case $a(1-a) = |c|^2$.

2. Show that ρ can be written as a function of a vector $\vec{b}$ called the *Bloch vector*:

$$\rho = \frac{1}{2}\begin{pmatrix} 1+b_z & b_x - \mathrm{i}b_y \\ b_x + \mathrm{i}b_y & 1-b_z \end{pmatrix} = \frac{1}{2}\left(I + \vec{b}\cdot\vec{\sigma}\right),$$

provided that $|\vec{b}|^2 \leq 1$. Show that a quantum state represented by a vector of $\mathcal{H}$ corresponds to the case $|\vec{b}|^2 = 1$. To interpret the vector $\vec{b}$ physically, we calculate the expectation value of $\vec{\sigma}$:

$$\langle \sigma_i \rangle = \mathrm{Tr}\,(\rho\,\sigma_i).$$

Show that $\vec{b}$ is the expectation value of $\vec{\sigma}$.

3. When the spin is placed in a constant magnetic field $\vec{B}$, the Hamiltonian is given by

$$H = -\frac{1}{2}\gamma\,\vec{\sigma}\cdot\vec{B},$$

where γ is a constant. Assuming that $\vec{B}$ is parallel to the axis Oz, $\vec{B} = (0, 0, B)$, write down the evolution equation for ρ and show that the vector $\vec{b}$ rotates (precesses) about $\vec{B}$ with an angular frequency to be determined.

4.6.4 The SWAP operator

1. Show that the operator

$$\frac{1}{2}\left(I + \vec{\sigma}_A\cdot\vec{\sigma}_B\right)$$

permutes the values of the two bits A and B:

$$\frac{1}{2}\left(I + \vec{\sigma}_A\cdot\vec{\sigma}_B\right)|i_A j_B\rangle = |j_A i_B\rangle.$$

The notation $\vec{\sigma}_A\cdot\vec{\sigma}_B$ stands for both the scalar product and the tensor product.

2. The operator $\frac{1}{2}\left(I+\vec{\sigma}_A\cdot\vec{\sigma}_B\right)$ is called the *SWAP operator*. Its matrix representation in the basis $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$ is

$$U_{\text{SWAP}}=\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}.$$

Check that its square root $U_{\text{SWAP}}^{1/2}$ is given by

$$U_{\text{SWAP}}^{1/2}=\frac{1}{1+\mathrm{i}}\begin{pmatrix}1+\mathrm{i}&0&0&0\\0&1&\mathrm{i}&0\\0&\mathrm{i}&1&0\\0&0&0&1+\mathrm{i}\end{pmatrix},$$

and that the so-called cZ gate can be constructed from

$$\text{cZ}=\mathrm{e}^{\mathrm{i}\pi\sigma_z^A/4}\,\mathrm{e}^{-\mathrm{i}\pi\sigma_z^B/4}\,U_{\text{SWAP}}^{1/2}\,\mathrm{e}^{\mathrm{i}\pi\sigma_z^A/2}\,U_{\text{SWAP}}^{1/2}=\begin{pmatrix}I&0\\0&\sigma_z\end{pmatrix}.$$

4.6.5 The Schmidt purification theorem

Let $|\varphi_{AB}\rangle\in\mathcal{H}_A\otimes\mathcal{H}_B$ be a pure state of the system AB, and let $\{|m_A\rangle\}$ and $\{|\mu_B\rangle\}$ be two orthonormal bases of $\mathcal{H}_A$ and $\mathcal{H}_B$. The most general decomposition of $|\varphi_{AB}\rangle$ on the basis $\{|m_A\otimes\mu_B\rangle\}$ of $\mathcal{H}_A\otimes\mathcal{H}_B$ is written as

$$|\varphi_{AB}\rangle=\sum_{m,\mu}c_{m\mu}|m_A\otimes\mu_B\rangle.$$

We define the vectors $|\tilde{m}_B\rangle\in\mathcal{H}_B$ as

$$|\tilde{m}_B\rangle=\sum_{\mu}c_{m\mu}|\mu_B\rangle$$

and rewrite the above decomposition as

$$|\varphi_{AB}\rangle=\sum_{m}|m_A\otimes\tilde{m}_B\rangle.$$

The vectors $\{|\tilde{m}_B\rangle\}$ do not *a priori* form an orthonormal basis of $\mathcal{H}_B$. We choose as the basis of $\mathcal{H}_A$ a set of vectors $\{|m_A\rangle\}$ which diagonalizes ρ_A:

$$\rho_A=\text{Tr}_B|\varphi_{AB}\rangle\langle\varphi_{AB}|=\sum_m\mathfrak{p}_m|m_A\rangle\langle m_A|.$$

https://doi.org/10.1017/CBO9780511755361.006

Comparing this expression for ρ_A with

$$\rho_A = \sum_{m,n} \langle \tilde{n}_B | \tilde{m}_B \rangle |m_A\rangle\langle n_A|,$$

prove that

$$\langle \tilde{n}_B | \tilde{m}_B \rangle = \mathsf{p}_m \delta_{mn}$$

and the vectors $|\tilde{n}_B\rangle$ are orthogonal after all. How can an orthonormal basis $|n_B\rangle$ be constructed? How should the terms such that $\mathsf{p}_n = 0$ be treated? Show that in this basis

$$|\varphi_{AB}\rangle = \sum_n \mathsf{p}_n^{1/2} |n_A \otimes n_B\rangle.$$

4.6.6 A model for phase damping

Let us consider the NMR case where a spin 1/2 is submitted to a fluctuating magnetic field $\vec{B}_0(t)$. The state $|1\rangle$ can assumed to be stable (spontaneous emission is negligible), but the resonance frequency $\omega_0 = \gamma B_0/\hbar$ is time dependent. The state vector of the spin system at time t is

$$|\Psi(t)\rangle = \lambda(t)|0\rangle + \mu(t)|1\rangle,$$

with $\lambda(t)$ and $\mu(t)$ given by

$$\mathrm{i}\dot{\lambda}(t) = -\frac{1}{2}\omega_0(t)\lambda(t), \qquad \mathrm{i}\dot{\mu}(t) = \frac{1}{2}\omega_0(t)\mu(t), \qquad \lambda(0) = \lambda_0, \mu(0) = \mu_0.$$

The solution is

$$\lambda(t) = \lambda_0 \exp\left(\frac{\mathrm{i}}{2}\int_0^t \omega_0(t')\,\mathrm{d}t'\right), \qquad \mu(t) = \mu_0 \exp\left(-\frac{\mathrm{i}}{2}\int_0^t \omega_0(t')\,\mathrm{d}t'\right).$$

Assume that $\omega_0(t)$ is a Gaussian stationary random function with connected autocorrelation function

$$C(t') = \langle \omega_0(t+t')\omega_0(t)\rangle - \langle\omega_0\rangle^2,$$

where $\langle \bullet \rangle$ is an ensemble average over all realizations of the random function. Also assume that

$$C(t') \simeq C \exp\left(-\frac{|t'|}{\tau}\right).$$

Show that the populations ρ_{00} and ρ_{11} are time independent, but that the time evolution of the coherences is given by

$$\rho_{01}(t) = \rho_{01}(t=0)\mathrm{e}^{\mathrm{i}\langle\omega_0\rangle t}\,\mathrm{e}^{-C\tau t}, \qquad t \gg \tau.$$

https://doi.org/10.1017/CBO9780511755361.006

4.6.7 Amplitude damping channel

In the so-called *amplitude damping channel*, we have instead of (4.27) the following evolution

$$U|0_A \otimes 0_E\rangle = |0_A \otimes 0_E\rangle,$$
$$U|1_A \otimes 0_E\rangle = \sqrt{1-\mathsf{p}}\,|1_A \otimes 0_E\rangle + \sqrt{\mathsf{p}}\,|0_A \otimes 1_E\rangle.$$

This is a model for describing the spontaneous decay of an atom in an excited state $|1_A\rangle$ into its ground state $|0_A\rangle$, while $|0_E\rangle$ is a state with zero photons and $|1_E\rangle$ a state with one photon. The probability of decay during a time interval Δt is p.

1. Starting from the state

$$|\Phi\rangle = (\lambda|0_A\rangle + \mu|1_A\rangle) \otimes |0_E\rangle,$$

compute the final state matrix ρ'_A. Show that the time evolution may be written in the form

$$\rho_A(t=0) \to \rho(t) = \begin{pmatrix} 1-\mathrm{e}^{-\Gamma t}\,\rho_{11} & \mathrm{e}^{-\Gamma t/2}\,\rho_{01} \\ \mathrm{e}^{-\Gamma t/2}\,\rho_{10} & \mathrm{e}^{-\Gamma t}\,\rho_{11} \end{pmatrix}.$$

Deduce from this that, in this model, the transverse relaxation time T_2 is twice the longitudinal relaxation time T_1, $T_2 = 2T_1$ (see Section 3.4).
2. Suppose that at time Δt one observes the environment in the zero photon state $|0_E\rangle$. What is then the state of the atom? Show that the failure to detect a photon has changed the state of the atom.

4.6.8 Invariance of the state (4.35) under rotation

Using

$$|\theta\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle,$$
$$|\theta_\perp\rangle = -\sin\theta|x\rangle + \cos\theta|y\rangle,$$

show that

$$|\Phi\rangle = \frac{1}{\sqrt{2}}\left(|x_A x_B\rangle + |y_A y_B\rangle\right) = \frac{1}{\sqrt{2}}\left(|\theta_A \theta_B\rangle + |\theta_{A\perp}\theta_{B\perp}\rangle\right).$$

4.7 Further reading

A popularized approach to entangled states can be found in Hey and Walters (2003), Chapter 8. The state operator is studied in Nielsen and Chuang (2000), Chapter 2, Preskill (1999), Chapter 3, and Le Bellac (2006), Chapter 6. Very clear

accounts of decoherence are found in Leggett (2002), Zurek (1991) and in Paz and Zurek (2002). Aspect (1999) reviews the experimental tests of Bell inequalities. Advanced theoretical discussions are found in Mermin (1993) and in Peres (1993), Chapters 6 and 7. A proof of the Gleason theorem and a demonstration of Schmidt decomposition are given by Peres (1993), Chapters 5 and 7. Interference using complex molecules is discussed by Arndt *et al.* (2005).

https://doi.org/10.1017/CBO9780511755361.006