Chapter 13

Quantum Information

In Chapter 10 of these notes the multi-state model for quantum systems was presented. This model was then applied to systems intended for energy conversion in Chapter 11 and Chapter 12. Now it is applied to systems intended for information processing.

The science and technology of quantum information is relatively new. The concept of the quantum bit (named the qubit) was first presented, in the form needed here, in 1995. There are still many unanswered questions about quantum information (for example the quantum version of the channel capacity theorem is not known precisely). As a result, the field is in a state of flux. There are gaps in our knowledge.

13.1 Quantum Information Storage

We have used the bit as the mathematical model of the simplest classical system that can store information. Similarly, we need a model for the simplest quantum system that can store information. It is called the "qubit." At its simplest, a qubit can be thought of as a small physical object with two states, which can be placed in one of those states and which can subsequently be accessed by a measurement instrument that will reveal that state. However, quantum mechanics both restricts the types of interactions that can be used to move information to or from the system, and permits additional modes of information storage and processing that have no classical counterparts.

An example of a qubit is the magnetic dipole which was used in Chapters 9, 11, and 12 of these notes. Other examples of potential technological importance are quantum dots (three-dimensional wells for trapping electrons) and photons (particles of light with various polarizations).

Qubits are difficult to deal with physically. That's why quantum computers are not yet available. While it may not be hard to create qubits, it is often hard to measure them, and usually very hard to keep them from interacting with the rest of the universe and thereby changing their state unpredictably.

Suppose our system is a single magnetic dipole. The dipole can be either "up" or "down," and these states have different energies. The fact that the system consists of only a single dipole makes the system fragile.

The reason that classical bits are not as fragile is that they use more physical material. For example, a semiconductor memory may represent a bit by the presence or absence of a thousand electrons. If one is missing, the rest are still present and a measurement can still work. In other words, there is massive redundancy in the mechanism that stores the data. Redundancy is effective in correcting errors. For a similar reason, it is possible to read a classical bit without changing its state, and it is possible for one bit to control the input of two or more gates (in other words, the bit can be copied).

However, there are at least three reasons why we may want to store bits without such massive redundancy. First, it would be more efficient. More bits could be stored or processed in a structure of the same size or cost. The semiconductor industry is making rapid progress in this direction, and before 2015 it should be possible to make memory cells and gates that use so few atoms that statistical fluctuations in the number of data-storing particles will be a problem. Second, sensitive information stored without redundancy could not be copied without altering it, so it would be possible to protect the information securely, or at least know if its security had been compromised. And third, the properties of quantum mechanics could permit modes of computing and communications that cannot be done classically.

A model for reading and writing the quantum bit is needed. Our model for writing (sometimes called "preparing" the bit) is that a "probe" with known state (either "up" or "down") is brought into contact with the single dipole of the system. The system and the probe then exchange their states. The system ends up with the probe's previous value, and the probe ends up with the system's previous value. If the previous system state was known, then the state of the probe after writing is known and the probe can be used again. If not, then the probe cannot be reused because of uncertainty about its state. Thus writing to a system that has unknown data increases the uncertainty about the environment. The general principle here is that discarding unknown data increases entropy.

The model for reading the quantum bit is not as simple. We assume that the measuring instrument interacts with the bit in some way to determine its state. This interaction forces the system into one of its stationary states, and the state of the instrument changes in a way determined by which state the system ends up in. If the system was already in one of the stationary states, then that one is the one selected. If, more generally, the system wave function is a linear combination of stationary states, then one of those states is selected, with probability given by the square of the magnitude of the expansion coefficient.

We now present three models of quantum bits, with increasingly complicated behavior.

13.2 Model 1: Tiny Classical Bits

The simplest model of a quantum bit is one which we will consider only briefly. It is not general enough to accommodate the most interesting properties of quantum information.

This model is like the magnetic dipole model, where only two states (up and down) are possible. Every measurement restores the system to one of its two values, so small errors do not accumulate. Since measurements can be made without changing the system, it is possible to copy a bit. This model of the quantum bit behaves essentially like a classical bit except that its size may be very small and it may be able to be measured rapidly.

This model has proven useful for energy conversion systems. It was used in Chapter 12 of these notes.

13.3 Model 2: Superposition of States (the Qubit)

The second model makes use of the fact that the states in quantum mechanics can be expressed in terms of wave functions which obey the Schrödinger equation. Since the Schrödinger equation is linear, any linear combination of wave functions that obey it also obeys it. Thus, if we associate the logical value 0 with the wave function ψ_0 and the logical value 1 with the wave function ψ_1 then any linear combination of the form

$$\psi = \alpha\psi_0 + \beta\psi_1 \tag{13.1}$$

where α and β are complex constants with $|\alpha|^2 + |\beta|^2 = 1$, is a valid wave function for the system. Then the probability that a measurement returns the value 0 is $|\alpha|^2$ and the probability that a measurement returns the value 1 is $|\beta|^2$. When a measurement is made, the values of α and β change so that one of them is 1 and the other is 0, consistent with what the measurement returns.

It might seem that a qubit defined in this way could carry a lot of information because both α and β can take on many possible values. However, the fact that a measurement will return only 0 or 1 along with the

fact that these coefficients are destroyed by a measurement, means that only one bit of information can be read from a single qubit, no matter how much care was exerted in originally specifying α and β precisely.

13.4 Model 3: Multiple Qubits with Entanglement

Consider a quantum mechanical system with four states, rather than two. Let us suppose that it is possible to make two different measurements on the system, each of which returns either 0 or 1. It is natural to denote the stationary states with two subscripts, one corresponding to the first measurement and the other to the second. Thus the general wave function is of the form

$$\psi = \alpha_{00}\psi_{00} + \alpha_{01}\psi_{01} + \alpha_{10}\psi_{10} + \alpha_{11}\psi_{11} \tag{13.2}$$

where the complex coefficients obey the normalization condition

$$1 = \mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2 + \mid \alpha_{10} \mid^2 + \mid \alpha_{11} \mid^2 \tag{13.3}$$

You may think of this model as two qubits, one corresponding to each of the two measurements. These qubits are not independent, but rather are **entangled** in some way. Then it is natural to ask what happens if one of them is measured. A measurement of, for example, the first qubit will return 0 with probability $\mid \alpha_{00} \mid^2 + \mid \alpha_{01} \mid^2$ and if it does the wave function collapses to only those stationary states that are consistent with this measured value,

$$\psi = \frac{\alpha_{00}\psi_{00} + \alpha_{01}\psi_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \tag{13.4}$$

(note that the resulting wave function was "re-normalized" by dividing by $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$).

There is no need for this system to be physically located in one place. In fact, one of the most interesting examples involves two qubits which are entangled in this way but where the first measurement is done in one location and the second in another. A simple case is one in which there are only two of the four possible stationary states initially, so $\alpha_{01} = 0$ and $\alpha_{10} = 0$. This system has the remarkable property that as a result of one measurement the wave function is collapsed to one of the two possible stationary states and the result of this collapse can be detected by the other measurement, possibly at a remote location.

It is possible to define several interesting logic gates which act on multiple qubits. These have the property that they are reversible; this is a general property of quantum-mechanical systems.

Among the interesting applications of multiple qubits are

- Computing some algorithms (including factoring integers) faster than classical computers
- Teleportation (of the information needed to reconstruct a quantum state)
- Cryptographic systems
- Backwards information transfer (not possible classically)
- Superdense coding (two classical bits in one qubit if another qubit was sent earlier)

These applications are described in several books and papers, including these three:

- T. P. Spiller, "Quantum Information Processing: Cryptography, Computation, and Teleportation," Proc. IEEE, vol. 84, no. 12, pp. 1719–1746; December, 1996. Although this article is now several years old, it is still an excellent introduction.
- Michael A. Nielsen and Isaac L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge, UK; 2000

- Hoi-Kwong Lo, Sandu Popescu, and Tim Spiller, "Introduction to Quantum Computation and Information," World Scientific, Singapore; 1998. The book is based on a lecture series held at Hewlett-Packard Laboratories, Bristol, UK, November 1996–April, 1997

13.5 Detail: Qubit and Applications

Sections 13.5 to 13.11 are based on notes written by Luis Pérez-Breva May 4, 2005.

The previous sections have introduced the basic features of quantum information in terms of the wave function. We first introduced the wave function in the context of physical systems in Chapter 10. The wave function is a controversial object, that has given rise to different schools of thought about the physical interpretation of quantum mechanics. Nevertheless, it is extremely useful to derive probabilities for the location of a particle at a given time, and it allowed us to introduce the multi-state model in Chapter 10 as a direct consequence of the linearity of Schrödinger equation.

In the first chapters of these notes, we introduced the bit as a binary (two-state) quantity to study classical information science. In quantum information science we are also interested in two-state systems. However, unlike the classical bit, the quantum mechanical bit may also be in a state of superposition. For example we could be interested in superpositions of the first two energy levels of the infinite potential well. The type of mathematics required for addressing the dynamics of two-state systems, possibly including superpositions, is linear algebra (that we reviewed in Chapter 2 in the context of the discrete cosine transformation.)

To emphasize that we are interested in the dynamics of two-state systems, and not in the dynamics of each state, it is best to abstract the wave function and introduce a new notation, the bracket notation. In the following sections, as we introduce the bracket notation, we appreciate the first important differences with the classical domain: the no-cloning theorem and entanglement. Then we give an overview of the applications of quantum mechanics to communication (teleportation and cryptography), algorithms (Grover fast search, Deutsch-Josza) and information science (error correcting codes).

13.6 Bracket Notation for Qubits

The bracket notation was introduced by P. Dirac for quantum mechanics. In the context of these notes, bracket notation will give us a new way to represent old friends like column and row vectors, dot products, matrices, and linear transformations. Nevertheless, bracket notation is more general than that; it can be used to fully describe wave functions with continuous variables such as position or momentum.[1]

13.6.1 Kets, Bras, Brackets, and Operators

Kets, bras, brackets and operators are the building bricks of bracket notation, which is the most commonly used notation for quantum mechanical systems. They can be thought of as column vectors, row vectors, dot products and matrices respectively.

$|\, Ket\rangle$

A ket is just a column vector composed of complex numbers. It is represented as:

$$|\, k\rangle = \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \overrightarrow{k}\,. \tag{13.5}$$

The symbol k inside the ket $|\, k\rangle$ is the label by which we identify this vector. The two kets $|\, 0\rangle$ and $|\, 1\rangle$ are used to represent the two logical states of qubits, and have a standard vector representation

$$|\, 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\, 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{13.6}$$

[1] Readers interested in an extremely detailed (and advanced) exposition of bracket notation may find the first chapters of the following book useful: *"Quantum Mechanics volume I" by Cohen-Tannoudji, Bernard Diu and Frank Laloe, Wiley-Interscience (1996).*

Recall from Equation 13.1 that the superposition of two quantum states ψ_0 andψ_1 is

$$\psi = \alpha\psi_0 + \beta\psi_1 \tag{13.7}$$

where α and β are complex numbers. In bracket notation, this superposition of $\mid 0\rangle$ and $\mid 1\rangle$ can be written as

$$\begin{aligned} \mid \psi\rangle &= \alpha \mid 0\rangle + \beta \mid 1\rangle && (13.8)\\ &= \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} && (13.9)\\ &= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} && (13.10) \end{aligned}$$

$\langle Bra \mid$

Bras are the Hermitian conjugates of kets. That is, for a given ket, the corresponding bra is a row vector (the transpose of a ket), where the elements have been complex conjugated. For example, the qubit from 13.10 has a corresponding bra $\langle\psi \mid$ that results from taking the Hermitian conjugate of equation 13.10

$$\begin{aligned} (\mid \psi\rangle)^\dagger &= (\alpha \mid 0\rangle + \beta \mid 1\rangle)^\dagger && (13.11)\\ &= \alpha^* (\mid 0\rangle)^\dagger + \beta^* (\mid 1\rangle)^\dagger && (13.12)\\ &= \alpha^* \begin{pmatrix} 1 \\ 0 \end{pmatrix}^\dagger + \beta^* \begin{pmatrix} 0 \\ 1 \end{pmatrix}^\dagger && (13.13)\\ &= \alpha^* \begin{pmatrix} 1 & 0 \end{pmatrix} + \beta^* \begin{pmatrix} 0 & 1 \end{pmatrix} && (13.14)\\ &= \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} && (13.15) \end{aligned}$$

The symbol † is used to represent the operation of hermitian conjugation of a vector or a matrix.[2] The star (*) is the conventional notation for the conjugate of a complex number: $(a + i\,b)^* = a - i\,b$ if a and b are real numbers.

$\langle Bra \mid Ket\rangle$

The dot product is the product of a bra (row vector) $\langle q \mid$, by a ket (column vector) $\mid k\rangle$, it is called bracket and denoted $\langle q \mid k\rangle$, and is just what you would expect from linear algebra

$$\langle q \mid k\rangle = \begin{pmatrix} q_1^* & q_2^* \end{pmatrix} \times \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} = \sum_j q_j^* k_j. \tag{13.16}$$

Note that the result of $\langle q \mid k\rangle$ is a complex number.

Brackets allow us to introduce a very important property of kets. Kets are always assumed to be normalized, which means that the dot product of a ket by itself is equal to 1. This implies that at least one of the elements in the column vector of the ket must be nonzero. For example, the dot product of an arbitrary qubit ($\mid \psi\rangle$) by itself, $\langle\psi \mid \psi\rangle = 1$, so

$$\begin{aligned} \langle\psi \mid \psi\rangle &= (\alpha^*\langle 0 \mid + \beta^*\langle 1 \mid) \cdot (\alpha \mid 0\rangle + \beta \mid 1\rangle)\\ &= \alpha^*\alpha\langle 0 \mid 0\rangle + \beta^*\alpha\langle 1 \mid 0\rangle\alpha^*\beta\langle 0 \mid 1\rangle + \beta^*\beta\langle 1 \mid 1\rangle\\ &= \alpha^*\alpha + \beta^*\beta\\ &= |\alpha|^2 + |\beta|^2 = 1 \end{aligned} \tag{13.17}$$

[2] This operation is known by several different names, including "complex transpose" and "adjoint."

This is precisely the result we postulated when we introduced the qubit as a superposition of wave functions. In Chapter 10, we saw that the product of a wavefunction by its complex conjugate is a probability distribution and must integrate to one. This requirement is completely analogous to requiring that a ket be normalized.[3]

The dot product can be used to compute the probability of a qubit of being in either one of the possible states $\mid 0\rangle$ and $\mid 1\rangle$. For example, if we wish to compute the probability that the outcome of a measurement on the qubit $\mid \psi\rangle$ is state $\mid 0\rangle$, we just take the dot product of $\mid 0\rangle$ and $\mid \psi\rangle$ and square the result

$$\begin{aligned}\Pr\left(\mid 0\rangle\right) &= \left|\langle 0 \mid \psi\rangle\right|^2 \\ &= \left|\alpha\langle 0 \mid 0\rangle + \beta\langle 0 \mid 1\rangle\right|^2 \\ &= \left|\alpha_1 + \beta_0\right|^2 \\ &= \left|\alpha\right|^2 \end{aligned} \tag{13.18}$$

$\widehat{Operators}$

Operators are objects that transform one ket $\mid k\rangle$ into another ket $\mid q\rangle$. Operators are represented with hats: $\widehat{O}$. It follows from our definition of ket that an operator is just a matrix,

$$\begin{aligned}\widehat{O} \mid k\rangle &= \begin{pmatrix} o_{11} & o_{12} \\ o_{21} & o_{22} \end{pmatrix} \times \begin{pmatrix} k_1 \\ k_2 \end{pmatrix} \\ &= \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} \\ &= \mid q\rangle \end{aligned} \tag{13.19}$$

Operators act on bras in a similar manner

$$\langle k \mid \widehat{O}^\dagger = \langle q \mid \tag{13.20}$$

Equations 13.19 and 13.20 and the requirement that kets be normalized allow us to derive an important property of operators. Multiplying both equations we obtain

$$\langle k \mid \widehat{O}^\dagger \widehat{O} \mid k\rangle = \langle q \mid q\rangle \tag{13.21}$$

$$\langle k \mid \widehat{O}^\dagger \widehat{O} \mid k\rangle = 1, \tag{13.22}$$

the second line follows from assuming that $\widehat{O}$ preserves the normalization of the ket, and since $\langle k \mid k\rangle = 1$, it implies that $\widehat{O}^\dagger \widehat{O} = \mathbb{I}$. Operators that have this property are said to be unitary, and their inverse is equal to their adjoint. All quantum mechanical operators must be unitary, or else, the normalization of the probability distribution would not be preserved by the transformations of the ket. Note that this is the exact same reasoning we employed to require that time evolution be unitary back in Chapter 10. From the physical standpoint unitarity means that doing and then undoing the operation defined by $\widehat{O}$ should leave us with the same we had in origin (Note the similarity with the definition of reversibility).

There is an easy way to construct an operator if we know the input and output kets. We can use the exterior product, that is, the product of a column vector by a row vector (the dot product is often also called inner or interior product, hence the name of exterior product). We can construct the operator $\widehat{O}$ using the exterior product of a ket by a bra

$$\widehat{O} \mid k\rangle = (\mid q\rangle\langle k \mid) \mid k\rangle = \mid q\rangle\langle k \mid k\rangle = \mid q\rangle \tag{13.23}$$

[3] It may not be immediately obvious that $\int \Psi^* \Psi dx$ is a dot product. To see that it is, discretize the integral $\int \Psi^* \Psi dx \rightarrow \sum_i \Psi_i^* \Psi_i$ and compare to the definition of dot product. You may argue that in doing so we have transformed a function Ψ into a vector with elements Ψ_i; but we defined a ket as a vector to relate it to linear algebra. If the ket were to represent a function, then the appropriate definition of the dot product would be $\langle \Phi \mid \Psi\rangle = \int \Phi^* \Psi dx$.

note that this would not be possible if the kets were not normalized to 1; another way to put it is that the normalization of the ket inforces the fact that operators built in this way are unitary.

For example, to transform a qubit in the state $\mid 0\rangle$ into the qubit in the state $\mid \psi\rangle$ defined above, we construct the operator

$$\widehat{O}_2 = \alpha \mid 0\rangle\langle 0 \mid + \beta \mid 1\rangle\langle 0 \mid \tag{13.24}$$

we can verify that this operator produces the expected result

$$\begin{aligned} \widehat{O}_2 \mid 0\rangle &= \alpha \mid 0\rangle\langle 0 \mid 0\rangle + \beta \mid 1\rangle\langle 0 \mid 0\rangle \\ &= \alpha \mid 0\rangle 1 + \beta \mid 1\rangle 1 \\ &= \alpha \mid 0\rangle + \beta \mid 1\rangle \\ &= \mid \psi\rangle \end{aligned} \tag{13.25}$$

we have just performed our first quantum computation!

In quantum mechanics books it is custommary to drop the hat from the operators ($\widehat{O} \to O$) to "simplify notation." Often at an introductory level (and an advanced level as well), this simplification causes confusion between operators and scalars; in these notes we will try to avoid doing so.

13.6.2 Tensor Product—Composite Systems

The notation we have introduced so far deals with single qubit systems. It is nonetheless desirable to have a notation that allows us to describe composite systems, that is systems of multiple qubits. A similar situation arises in set theory when we have two sets A and B and we want to consider them as a whole. In set theory to form the ensemble set we use the cartesian product $A \times B$ to represent the ensemble of the two sets. The analogue in linear algebra is called tensor product and is represented by the symbol $\otimes$. It applies equally to vectors and matrices (i.e. kets and operators).

From a practical standpoint, the tensor product concatenates physical systems. For example, a two particle system would be represented as $\mid \textit{particle } 1\rangle \otimes \mid \textit{particle } 2\rangle$, and the charge and the spin of a particle would be represented also by the tensor product $\mid \textit{charge}\rangle \otimes \mid \textit{spin}\rangle$. If we have two qubits $\mid \psi\rangle$ and $\mid \phi\rangle$, the system composed by these two qubits is represented by $\mid \psi\rangle \otimes \mid \phi\rangle$.

Athough they share a similar goal, cartesian and tensor product differ in the way elements of the ensemble are built out of the parts. Cartesian product produces tuples. So if A and B are two sets of numbers, an element of their cartesian product $A \times B$ is a pair of numbers (a, b) such that a belongs to A and b belongs to B. It is a simple concatenation.

The elements of a tensor product are obtained from the constituent parts in a slightly different way. For example, consider two *2×2 matrices*

$$\mathbb{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \mathbb{B} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{13.26}$$

the tensor product yields a *4×4 matrix*

$$\mathbb{A} \otimes \mathbb{B} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix} \tag{13.27}$$

Although it may not be obvious at first sight, this way of constructing the tensor product is consistent with the way we do matrix multiplication. As an operation, it has a very interesting feature, it outputs 4×4 matrices out of 2×2 matrices, but not all 4×4 matrices can be generated in this way (for the mathematically inclined reader, the tensor product operation is not surjective, or "onto"), it is this feature of the tensor

product that will motivate the discussion about entanglement, probably the most peculiar feature of quantum mechanics.

You should take some time to get used to the tensor product, and ensure you do not get confused with all the different products we have introduced in in the last two sections.

1. the dot product ($\langle k \mid q \rangle$) yields a complex number;
2. the exterior product ($\mid k \rangle\langle q \mid$) yields a square matrix of the same dimension that the Ket;
3. The tensor product ($\mid k \rangle \otimes \mid q \rangle$) is used to examine composite systems. It yields a vector (or matrix) of a dimension equal to the sum of the dimensions of the two kets (or matrices) in the product.

Tensor Product in bracket notation

As we mentioned earlier, the tensor product of two qubits $\mid q_1 \rangle$ and $\mid q_2 \rangle$ is represented as $\mid q_1 \rangle \otimes \mid q_1 \rangle$. Sometimes notation is abridged and the following four representations of the tensor product are made equivalent

$$\mid q_1 \rangle \otimes \mid q_2 \rangle \equiv \mid q_1 \rangle \mid q_2 \rangle \equiv \mid q_1, q_2 \rangle \equiv \mid q_1 q_2 \rangle \tag{13.28}$$

For n qubits, it is frequent to abbreviate notation giving to each qubit $\mid q \rangle$ an index:

$$\mid q_1 \rangle \otimes \mid q_2 \rangle \otimes \ldots \otimes \mid q_n \rangle = \bigotimes_{j=1}^{n} \mid q_j \rangle \tag{13.29}$$

The dual of a tensor product of kets is the tensor product of the corresponding bras. This implies that in the abridged notations, the complex conjugate operation turns kets into bras, *but the labels retain their order*

$$\begin{aligned} (\mid q_1 q_2 \rangle)^\dagger &= (\mid q_1 \rangle \otimes \mid q_2 \rangle)^\dagger \\ &= \langle q_1 \mid \otimes \langle q_2 \mid) \\ &= \langle q_1 q_2 \mid). \end{aligned} \tag{13.30}$$

As a consequence, the result of the dot product of two composite systems is the multiplication of the individual dot products taken in order

$$\begin{aligned} \langle q_1 q_2 \mid w_1 w_2 \rangle &= (\langle q_1 \mid \otimes \langle q_2 \mid)(\mid w_1 \rangle \otimes \mid w_2 \rangle) \\ &= \langle q_1 \mid w_1 \rangle \otimes \langle q_2 \mid w_1 \rangle \end{aligned} \tag{13.31}$$

confusion often arises in the second term, where in the absence of the parenthesis it is easy to get confused by $\langle q_2 \mid\mid w_1 \rangle$ and interpret it as a $\langle \mid \rangle$ (note the two vertical separators in the correct form), and then try to to take the dot products inside out, instead of taking them in parallel as it should be done.

13.6.3 Entangled qubits

We have previously introduced the notion of entanglement in terms of wave functions of a system that allows two measurements to be made. Here we see that it follows from the propeerties of the tensor product as a means to concatenate systems. Consider two qubits $\mid \psi \rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ and $\mid \varphi \rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, according to the definition of the tensor product,

$$\mid \psi \rangle \otimes \mid \varphi \rangle = \begin{pmatrix} \alpha a \\ \alpha b \\ \beta a \\ \beta b \end{pmatrix} \tag{13.32}$$

If we operate in the ensemble system (i.e. ignoring that it is composed by two subsystems), it is not unthinkable to reach a state described by the following ket

$$| \psi_{12}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \tag{13.33}$$

It turns out that the composite system $| \psi_{12}\rangle$ **cannot be expressed as a tensor product of two independent qubits**. That is, operating directly on the ensemble, it is possible to reach states that cannot be described by two isolated systems.

To see why it is so, try to equal equations 13.32 and 13.33: the first element of the ket requires $\alpha a = 0$; this implies that either α or a must be zero. However if $\alpha = 0$ the second element cannot be 1, and similarly, if $a = 0$ the third element would have to be zero instead of one. So there is no combination of α, β, a, and b that allows us to write the system described in equation 13.33 as a tensor product like the one described in equation 13.32. We conclude that

$$| \psi_{12}\rangle \neq | \psi\rangle \otimes | \varphi\rangle. \tag{13.34}$$

We have already encountered similar situations in the context of "mixing" in chapter 11. There, we noted that intensive variables could no longer be well defined in terms of the subsystems, furtermore, if the process of mixing two subsystems was not reversible, the entropy in the final system was bigger than the sum of the entropies, and it no longer made sense to try to express the composite system in terms of its original constituents. The two situations are different but there is certainly room for analogy.

Whenever this situation arises at the quantum level, we say that the two qubits (or any two systems) are entangled. This word is a translation from the German word "Verschränkung", that is often also translated as "interleaved", Schrödinger coined this word to describe the situation in which:

"Maximal knowledge of a total system does not necessarily include total knowledge of all of its parts, not even when these are fully separated from each other and at the moment are not influencing each other at all.".[4]

The most salient difference with what we saw in the mixing process arises from the fact that, as Schrödinger points out in the paragraph above, this "interleaving" of the parts remains even after separating them, and the measurement of one of the parts will condition the result on the other. This is what Einstein called "spooky action at a distance".

We can illustrate the effect of entanglement on measurements rewriting equation 13.33 by means of a superposition of two tensor products

$$| \psi_{12}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \tag{13.35}$$

$$= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right] \tag{13.36}$$

$$= \frac{1}{\sqrt{2}} [| 0\rangle_1 | 1\rangle_2 + | 1\rangle_1 | 0\rangle_2]$$

$$= \frac{1}{\sqrt{2}} [| 0_1 1_2\rangle + | 1_1 0_2\rangle] , \tag{13.37}$$

[4] Extract from "Die gegenwartige Situation in der Quantenmechanik," Erwin Schrödinger, Naturwissenschaftern. 23 : pp. 807-812; 823-823, 844-849. (1935). English translation: John D. Trimmer, Proceedings of the American Philosophical Society, 124, 323-38 (1980).

where we have added subindices to distinguish between the two qubits. This is also a good example to start appreciating the power of bracket notation to simplfy expressions.

If we measure the first qubit, we will obtain either $\mid 0\rangle_1$ or $\mid 1\rangle_1$. To compute the probability that the outcome is $\mid 0\rangle_1$, we take the dot product of the entangled state with $\mid 0_1, ?_2\rangle = \mid 0\rangle_1$

$$\langle 0_1, ?_2 \mid \psi_{12}\rangle = \langle 0_1, ?_2 \mid \cdot \frac{1}{\sqrt{2}} [\mid 0\rangle_1 \mid 1\rangle_2 + \mid 1\rangle_1 \mid 0\rangle_2] \tag{13.38}$$

$$= \frac{1}{\sqrt{2}} (\langle 0 \mid 0\rangle_1 \langle ? \mid 1\rangle_2 + \langle 0 \mid 1\rangle_1 \langle ? \mid 0\rangle_2) \tag{13.39}$$

$$= \frac{1}{\sqrt{2}} \langle ? \mid 1\rangle_2 \tag{13.40}$$

This results says that the outcome will be $\mid 0\rangle_1$ with a probability of 1/2, if and only if the second system collapses at the same time to the state $\mid 1\rangle_2$ (note that otherwise if the question mark represented a 0, the probability would be equal to zero). So the measurement on the first system conditions the value on the second system even if the systems are far apart.

To appreciate the spookyness of entanglement, it may be worth thinking of it in a more mundane setting. Imagine you have such a great connection with a colleague that every time he yawns you systematically yawn as well. Your common friends will pay no attention to it as it is a normal thing to happen, we know that when somebody yawns people in the surroundings tend to yawn. You would certainly scare them though if your colleague went to Europe and you remained in the US, and every once in a while you were driven to have a yawn, precisely when your friend had one. In fact, to be scared your friends would need the input from a referee at each side of the ocean to record the events and match time tags. The question would arise as to whether you and your colleague can use your the yawn-connection for the purpose of inmediate communication, since there appears to be a need for a referee. This cartoon example is certainly not quantum mechanical, however it illustrates what is it about entanglement that has fascinated and scared at the same time some of the greatest minds of our time. And at the same time, it introduces one caveat of quantum communication: the need for a classical exchange to verify that communication has existed (the referees). You will have a chance to appreciate this in a real quantum mechanical setting when we discuss teleportation.

13.7 No Cloning Theorem

One of the most natural operations in classical information is to copy bits, it happens all the time in our computers. Quantum logic diverges from classical logic already at this level. *Qubits cannot be copied*, or as it is usually stated: qubits cannot be cloned.

There are several intuitive arguments that can help us understand why it is so. Remember that in Chapter 10 we emphasized that the act of measuring changes the system being measured; if the system is in a superposition, the result of the measurement will be one of the states of the superposition. And the superposition is destroyed. Intuitively, if measuring is at all required to do the cloning, then it will be impossible to have two clones, since we cannot learn anything about the initial superposition. Furthermore, the superposition itself is destroyed by the act of measuring. This implies that a viable cloning device cannot use measurement.

Assume we have such a device and it operates without requiring measurement. One of the foundations of quantum mechanics is the uncertainty principle introduced by Heisenberg. The principle says that certain physical variables cannot be measured at the same time to an arbitrary precision. The example is position and momentum; if the position of a particle is measured with a given precision Δx, the precision with which its momentum is measured is limited: $\Delta p > \hbar/2\Delta x$. With the presumed cloning machine at hand it should be possible to clone the particle and measure momentum to arbitrary precision in one clone and position to arbitrary precision in the other, possibly violating Heisenberg's principle.

These arguments by themselves do not prove the impossibility of cloning, but suggest that the matter is by no means trivial.

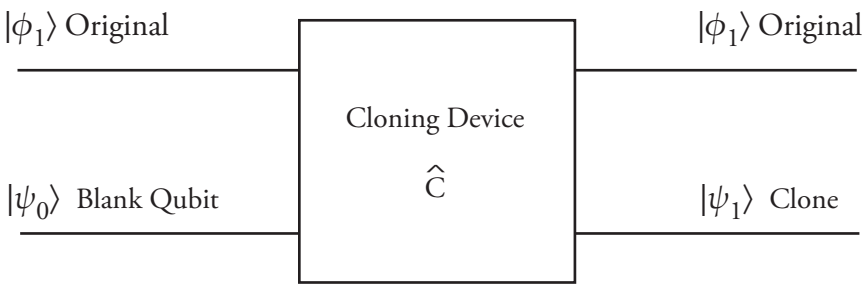

Figure 13.1: Suggested cloning device

To show that cloning is not possible, let us assume that it were possible to clone, and that we could set up a "machine" like the one in Figure 13.1. The cloning device takes the information of one qubit $|\ \phi_1\rangle$ and copies it into another "blank" qubit, the result is a qubit $|\ \psi_1\rangle$ identical to $|\ \phi_1\rangle$, and the original $|\ \phi_1\rangle$ is unmodified. According to what we saw in our overview of bracket notation, such a machine is an operator (we will call it $\widehat{C}$) because it transforms two qubits into two other qubits; and as an operator, $\widehat{C}$ must be unitary. Thus we define $\widehat{C}$

$$|\ Original\rangle \otimes |\ Blank\rangle \quad \xrightarrow{\widehat{C}} \quad |\ Original\rangle \otimes |\ clone\rangle \tag{13.41}$$

We are now ready to clone two arbitrary qubits $|\ \phi_1\rangle$ and $|\ \phi_2\rangle$ separately.

$$\widehat{C}\ |\ \phi_1\rangle\ |\ blank\rangle = |\ \phi_1\rangle\ |\ \psi_1\rangle \tag{13.42}$$

$$\widehat{C}\ |\ \phi_2\rangle\ |\ blank\rangle = |\ \phi_2\rangle\ |\ \psi_2\rangle \tag{13.43}$$

$$\tag{13.44}$$

where it is understood that $|\ \phi_1\rangle = |\ \psi_1\rangle$ and $|\ \phi_2\rangle = |\ \psi_2\rangle$, and we have given them different names to distinguish original from copy.

Since the cloning machine is unitary, it preserves the dot products, so we can compare the dot product before and after cloning

$$\langle \phi_2 \mid \langle blank \mid\mid \phi_1\rangle \mid blank\rangle = \langle \phi_2 \mid \langle \psi_2 \mid\mid \phi_1\rangle \mid \psi_1\rangle \tag{13.45}$$

Recall the rules for taking the dot product of tensor products, each element in the tensor product of kets is multiplied by the bra in the same position in the tensor product of bras, therefore

$$\langle \phi_2 \mid \phi_1\rangle\langle blank \mid blank\rangle = \langle \phi_2 \mid \phi_1\rangle\langle \psi_2 \mid \psi_1\rangle \tag{13.46}$$

The requirements that kets be normalized imposes that $\langle blank \mid blank\rangle = 1$. The above equation can only be true in two cases:

- $\langle \phi_2 \mid \phi_1\rangle = 0$, which means that $|\ \phi_1\rangle$ and $|\ \phi_2\rangle$ are orthogonal. This means that we can clone states chosen at random from a set of orthogonal states. And is equivalent to say that we can clone $|\ 0\rangle$ and $|\ 1\rangle$, which we already knew since we do that classically all the time.
- $\langle \psi_2 \mid \psi_1\rangle = 1$, which means that $\psi_2 = \psi_1$, that is, that clones obtained in each operation are identical. If the two originals were different, as we had assumed, what this result says is that the clone is independent from the original, which is quite a bizarre property for a clone!.

This proof shows that perfect cloning of qubits cannot be achieved. We can certainly store the result of a measurement (this is another way of phrasing the first case), but we cannot clone the superpositions.

13.8 Representation of Qubits

The no-cloning theorem prepares us to expect changes in quantum logic with respect to its classical analog. To fully appreciate the differences, we have to work out a representation of the qubit that unlike the classical bit, allows us to picture superpositions. We will introduce two such representations, a pictorial one that represents the qubit bit as a point in the surface of a sphere, and an operational one that presents the qubit as a line in a circuit much like the logic circuits we explored in Chapter 1.

13.8.1 Qubits in the Bloch sphere

Consider a qubit in an arbitrary superposition

$$| \psi\rangle = \alpha \mid 0\rangle + \beta \mid 1\rangle. \tag{13.47}$$

If α and β were real, equation 13.17 would define a circle of radius one, and we would picture the qubit as a point in the boundary of the circle. However, α and β are complex numbers, so we will have to work a little bit harder to derive a similar intuition.

Every complex number can be represented by a phase and a magnitude, so we can rewrite α and β as:

$$\alpha = Ae^{ia} \qquad \beta = Be^{ib} \tag{13.48}$$

from the normalization of the kets (Equation 13.17), we can derive that

$$\begin{aligned} 1 &= |\alpha|^2 + |\beta|^2 \\ &= A^2 + B^2, \end{aligned} \tag{13.49}$$

and this now is the equation of a circle centered at the origin, so both A and B can be rewritten in terms of an angle[5] $\theta/2$.

$$A = \cos\frac{\theta}{2} \qquad B = \sin\frac{\theta}{2}. \tag{13.50}$$

let us introduce this result in the equation 13.47 of the original superposition:

$$| \psi\rangle = \cos\frac{\theta}{2}e^{ia} \mid 0\rangle + sin\frac{\theta}{2}e^{ib} \mid 1\rangle. \tag{13.51}$$

we can still do one more thing, take e^{ia} out as a common factor

$$\begin{aligned} | \psi\rangle &= e^{ia}\left(\cos\frac{\theta}{2} \mid 0\rangle + sin\frac{\theta}{2}e^{i(b-a)} \mid 1\rangle\right) \\ &= e^{ia}\left(\cos\frac{\theta}{2} \mid 0\rangle + sin\frac{\theta}{2}e^{i\varphi} \mid 1\rangle\right) \end{aligned} \tag{13.52}$$

where we have renamed $\varphi = b - a$. If we ignore the global phase factor(e^{ia}), the two angles θ and φ define a point in a unit sphere. This sphere is called the Bloch Sphere, and is shown in Figure 13.2.

Each point in its surface represents one possible superposition of the states $\mid 0\rangle$ and $\mid 1\rangle$. For example, consider the qubit in the state $\mid \eta\rangle = \frac{1}{\sqrt{2}}(\mid 0\rangle + \mid 1\rangle)$, we can compare this state with equation 13.52, and conclude that then $\theta/2 = \pi/4$, $\varphi = 0$, so that the qubit $\mid \eta\rangle$ is represented by a vector parallel to the x-axis of the Bloch Sphere.

[5]The choice of the angle as $\theta/2$ instead of θ is a technical detail for us, it is adequate for using the spin of an electron as a qubit, if instead, we used the polarization of the photon, then the adequate choice would be θ. This is related to fermions and bosons of which you may have heard, but whose nature is irrelevant to us here.

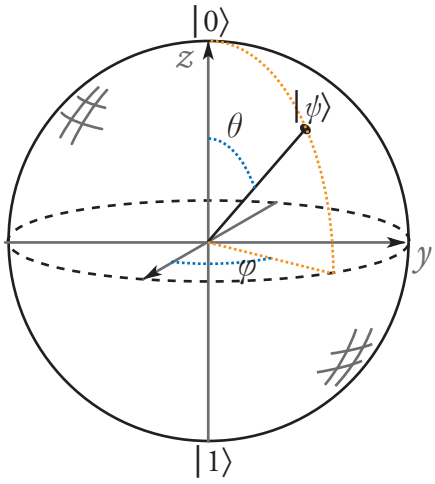

Figure 13.2: Geometrical representation of a Qubit: Bloch Sphere

When we introduced operators we said that they transformed the superposition state of qubits while preserving their normalization. In the context of the Bloch Sphere, this means that operators move dots around the unit sphere, i.e., define trajectories.

Back to equation 13.52, we still need to consider what happens to the global phase factor e^{ia} that we had ignored. This factor would seem to imply that the dot in the Bloch sphere can rotate over itself by an angle a. However, as we are ultimately interested in the probability of each state (because it is the state and not the superpositions what we measure), we should see what happens to this factor as we take the square of the dot products. For example let us examine the probability that measuring the qubit from equation 13.52 yields $\mid 1\rangle$ as an answer

$$\begin{aligned}
|\langle 1 \mid \psi\rangle|^2 &= \left|\langle 1 \mid \cdot e^{ia}\left(\cos\frac{\theta}{2} \mid 0\rangle + sin\frac{\theta}{2}e^{i\varphi} \mid 1\rangle\right)\right|^2 \\
&= \left|e^{ia}\right|^2 \times \left|\cos\frac{\theta}{2}\langle 1 \mid 0\rangle + sin\frac{\theta}{2}e^{i\varphi}\langle 1 \mid 1\rangle\right|^2 \\
&= 1 \times \left|0 + sin\frac{\theta}{2}e^{i\varphi} \times 1\right|^2 \\
&= \left|sin\frac{\theta}{2}e^{i\varphi}\right|^2 .
\end{aligned} \tag{13.53}$$

We see that the global phase factor squares to one, and so plays no role in the calculation of the probability. It is often argued that global phase factors disappear when computing probabilities, and so, are not measurable.

13.8.2 Qubits and symmetries

The Bloch sphere depicts each operation on a qubit as a trajectory on the sphere. However, any trajectory on the sphere can be represented by means of a sequence of rotations about the three axis. So, one way to address the definition of the operations on the qubit is to study rotations about the axis of the bloch sphere. This is intimately connected with the study of symmetries. Thomas Bohr was the first to suggest to use symmetries to interpret quantum mechanics.

We say that an object has a certain symmetry if after applying the corresponding symmetry operation (for example a rotation) the object appears to not have changed; then we say the object is invariant to that symmetry operation. In general, symmetry operations are rotations, reflections and inversions; and invariant

means that start and end position of the object are indistinguishable. For example, Figure 13.3 shows a

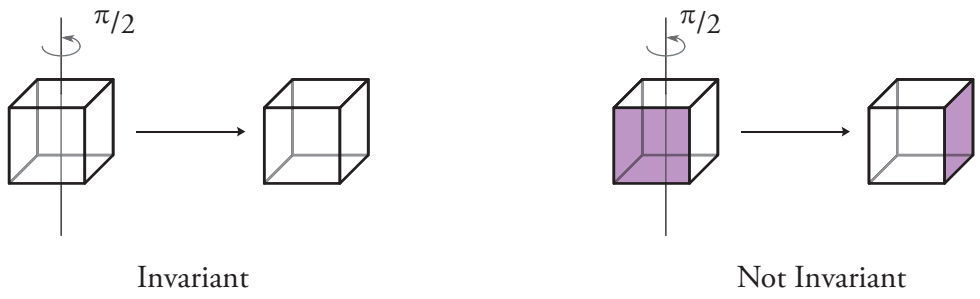

Figure 13.3: Concept of invariance. Symmetry operation: rotation of $\pi/2$ about the vertical axis.

cube, invariant to a rotation of $\pi/2$ about an axis in the center of any of its faces. To distinguish start and end position, you would have to paint one face of the cube, as in the picture to the right of Figure 13.3. Then the cube is no longer invariant to a rotation of $\pi/2$. We would then say that the group of symmetries of the cube to the left of Figure 13.3, contains, among others, the group of rotations of $\pi/2$ about the axis drawn in the figure.

The way physicists use symmetries is to characterize objects by studying the operations that best describe how to transform the object and what are its invariances. Then the representation of the qubit in the Bloch sphere is particularly useful, since it tells us to focus on the group of spatial rotations. In the remainder of this section we will reconcile both views, our perspective of operators as matrices, and the symmetries of the Bloch sphere.

We have already seen that operators on qubits are 2×2 unitary matrices, the additional technical requirement we have to impose to have the group of spatial rotations is that the determinant of the matrices is +1 (as opposed to -1). This group has a name, it is called SU(2)[6]. We can build all of the matrices of SU(2) combining the following four matrices:

$$\mathbb{I} \stackrel{def}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x \stackrel{def}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y \stackrel{def}{=} \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z \stackrel{def}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{13.54}$$

these matrices are known as the Pauli matrices in honor of Wolfgang Pauli. Note that technically they do not belong to SU(2), to be mathematically rigorous we need to multiply each of them by i, the imaginary number (to verify that this is so, compute their determinant with and without multiplying by i).

Action of Pauli matrices on an arbitrary qubit

The best way to capture the intuition behind Pauli matrices, is to apply each of them to a qubit in an arbitrary superposition state

$$|\,\psi\rangle = \alpha\,|\,0\rangle + \beta\,|\,1\rangle = \cos\frac{\theta}{2}\,|\,0\rangle + \sin\frac{\theta}{2}e^{i\varphi}\,|\,1\rangle \tag{13.55}$$

[6]Groups are conventionally named with letters like O,U, SU, SO, etc. Each of this letters has a meaning. SU(2) stands for the special (S) group of unitary (U) matrices of dimension 2. Special means that the determinant of the matrices is +1, and unitary has here the same meaning it had in the discussion of the operators.

and interpret the result

$$\begin{aligned}\sigma_x \mid 0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \quad \rightarrow \text{ Rotation of } \pi \text{ about x axis} \end{aligned} \tag{13.56}$$

$$\begin{aligned}\sigma_y \mid 0\rangle &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= i \begin{pmatrix} -\beta \\ \alpha \end{pmatrix} \quad \rightarrow \text{ Rotation of } \pi \text{ about y axis} \end{aligned} \tag{13.57}$$

$$\begin{aligned}\sigma_z \mid 0\rangle &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \quad \rightarrow \text{ Rotation of } \pi \text{ about z axis} \end{aligned} \tag{13.58}$$

Figure 13.4 illustrates the operation of σ_y on a qubit in an arbitrary superposition on the Bloch sphere.

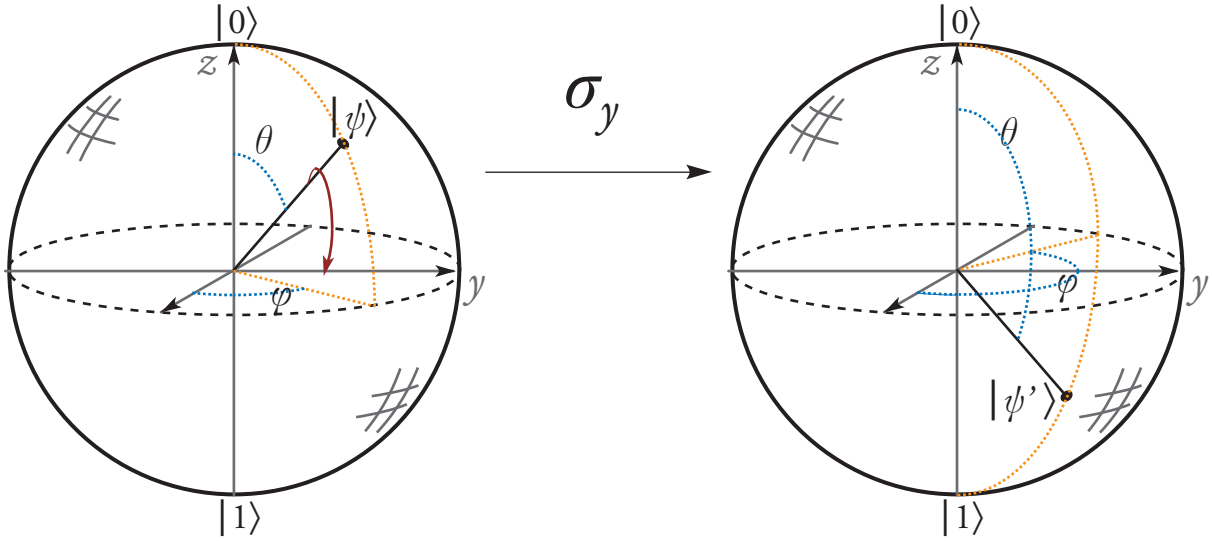

Figure 13.4: Operation of σ_y, on the Bloch sphere

Hence Pauli matrices are rotations of π about each of the axes of the bloch sphere (this motivates the names we gave them). However, to fully explore the surface of the Bloch sphere we need to be able to define arbitrary rotations (not just multiples of π). To do so we use the neat trick of exponentiating Pauli Matrices. Recall Euler's formula relating the exponential function to sine and cosine,

$$e^{ix} = \cos x + i \sin x. \tag{13.59}$$

Euler's formula applies when x is a real number. But we are interested in obtaining a similar result for Pauli matrices. We can prove the equivalent to Euler's formula for Pauli matrices by replacing x by $\frac{\theta}{2}\sigma_x$, and

expanding the exponential as a Taylor series (note that $\sigma_x\sigma_x = \mathbb{I}$)

$$e^{i\sigma_x\theta/2} = 1 + i\frac{\theta}{2}\sigma_x - \frac{1}{2}\left(\frac{\theta}{2}\right)^2\mathbb{I} - i\frac{1}{3}\left(\frac{\theta}{2}\right)^3\sigma_x + \frac{1}{4}\left(\frac{\theta}{2}\right)^4\mathbb{I} + \cdots \tag{13.60}$$

$$= \left(1 - \frac{1}{2}\left(\frac{\theta}{2}\right)^2 + \frac{1}{4}\left(\frac{\theta}{2}\right)^4 + \cdots\right)\mathbb{I} + i\left(0 + \left(\frac{\theta}{2}\right) - \frac{1}{3}\left(\frac{\theta}{2}\right)^3 + \cdots\right)\sigma_x \tag{13.61}$$

$$= \cos\frac{\theta}{2}\mathbb{I} + i\sin\frac{\theta}{2}\,\sigma_x. \tag{13.62}$$

This result shows us how to do arbitrary rotations of an angle θ about the x axis, the resulting operator is often called $R_x(\theta) = e^{i\sigma_x\theta/2}$. The cases of R_y and R_z are completely analogous.

Summing up, we have shown how to represent any qubit as a point in the Bloch sphere and we have learnt how to navigate the bloch sphere doing arbitrary rotations about any of the three axis. It follows that we have obtained an expression for the group of operations of symmetry that allow us to write the form of any operator acting on a single qubit.

13.8.3 Quantum Gates

In the first chapter of these notes, we explored all the possible functions of one and two input arguments and then singled out the most useful boolean functions *NOT*, *AND*, *NAND*, *NOR*, *OR*, *XOR*. Then, we associated it to a pictogram that we called gate, and reviewed the mechanisms to build logic circuits to do computations.

In the previous section we did the same thing for qubits, we characterized all the operators that may transform the value of a single qubit: we defined Pauli's matrices and explained how to do arbitrary rotations. By analogy with the classical case, Pauli matrices and arbitrary rotations are the gates of a quantum circuit. In more advanced treatises on quantum computing you would want to prove a variety of results about the quantum gates, such as the minimum set of gates necessary to do any quantum computation and various results on the generalization from 1 to n qubits. Here we will limit ourselves to summarizing the main details of the quantum algebra, its symbolic representation, and its properties.

Elementary Quantum Gates

The 5 elementary quantum gates are listed in Table 13.1. Their symbolic representation is much simpler

Pauli X	$X =$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv \sigma_x$	It is equivalent to doing a NOT or bit flip
Pauli Y	$Y =$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \equiv \sigma_y$	
Pauli Z	$Z =$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \equiv \sigma_z$	Changes the internal phase
Hadamard	$H =$	$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
Phase	$S =$	$\begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$	

Table 13.1: Elementary quantum gates.

than that of their classical counterparts, it is shown in Figure 13.5.

Table 13.2 enumerates some of the properties of the elementary quantum gates from Table 13.1. These properties are the quantum counterpart to the properties of classical bit functions that we enumerated in

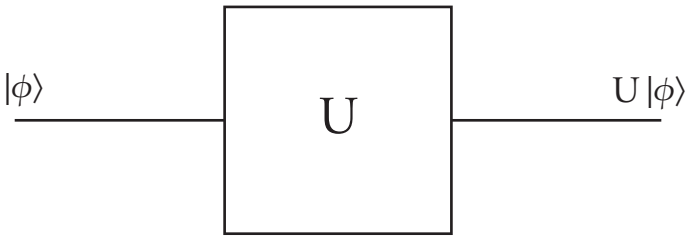

Figure 13.5: Generic quantum gate. Where U is the name given to the generic unitary matrix that this gate represents.

Chapter 1. These and other more advanced rules, help simplify quantum circuits much as deMorgan's law helps in simplifying classical circuits.

$H = \frac{1}{\sqrt{2}}(X + Z)$	$HXH = Z$
$XYX = -Y$	$HYH = -Y$
$XZX = -Z$	$HZH = X$
$XR_y(\theta)X = R_y(-\theta)$	$XR_z(\theta)X = R_y(-\theta)$

Table 13.2: Some of the main properties of single qubit gates.

Two-qubit gates. Controlled Gates

The first thing to note about multiple qubit gates is that the operators are unitary and square, and so unlike classical gates, quantum gates will always have the same number of inputs and outputs. Another way to say it is that all quantum gates are naturally reversible, as it should be expected from the fact that operators are unitary.

The most important two qubit gates are the controlled gates. In a controlled gate the first input qubit is a control qubit, with the same meaning than the classical control bit. If it is in the $|\ 1\rangle$ state, it will trigger the gate that acts on the second qubit, otherwise, it will not trigger it and the second qubit will remain unaltered. A generic example is shown in Figure 13.6, the gate in that example would be named C-U. There

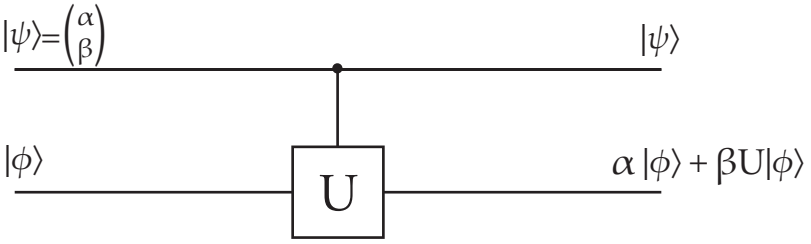

Figure 13.6: Generic quantum controlled gate (C-U). Where U is the name given to the generic unitary matrix that this gate represents.

are two controlled gates that are very relevant to the algorithms we will describe later on, the C-X also known as C-NOT and the C-Z also known as C-Phase. The popularity of the CNOT gate has awarded it a symbol of its own, shown in Figure 13.7.

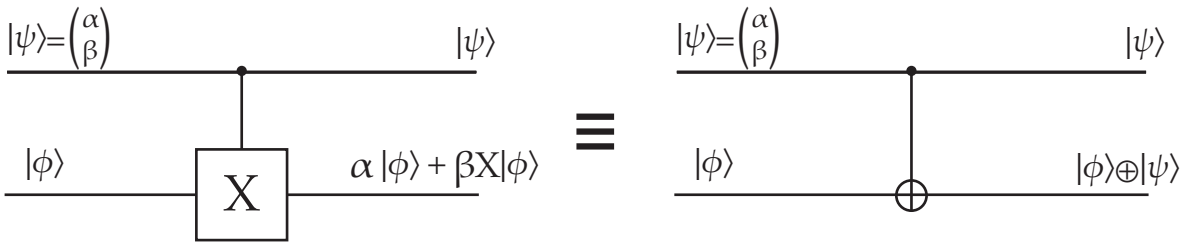

Figure 13.7: CNOT gate.

Finally, it is worth reviewing the matrix representation of the C-Z gate

$$C-Z=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&|1&0|\\0&0&|0&-1|\end{pmatrix} \tag{13.63}$$

where we have emphasized that the bottom right square is the Z matrix.

13.9 Quantum Communication

Two of the most tantalizing applications of quantum mechanics applied to information theory come from the field of communications. The first is the possibility that a quantum computer could break classical cryptographic codes in virtually no time. The second is the idea that quantum bits can be teleported.

In this section we will review the principles behind both teleportation and quantum cryptography (the solution to the problem of code breaking). As we are about to see, entanglement is key in both applications. The two most famous characters in communications: Alice and Bob, will play the main role in teleportation. For quantum cryptography, Eve will play a supporting role.

13.9.1 Teleportation - Alice and Bob's story

Alice and Bob, entangled a pair of qubits $\mid \phi_{AB}\rangle$ when they first met, as is the tradition in the 21st century, people no longer shake hands.

$$\mid \phi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0_A\rangle\otimes \mid 0_B\rangle + \mid 1_A\rangle\otimes \mid 1_B\rangle\right) \tag{13.64}$$

They shared a good time, but after school, life took each of them through separate paths. However, they each kept their piece of the entangled pair (it is unlawful not to do so in the 21st century). Now, the pair looks like

$$\mid \phi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(\mid 0_A\rangle \overset{\text{far}}{\otimes} \mid 0_B\rangle + \mid 1_A\rangle \overset{\text{far}}{\otimes} \mid 1_B\rangle\right) \tag{13.65}$$

Alice has now decided to come forward and confess to Bob her love for him. However, she is afraid of rejection and she has heard that qubits can be "teleported instantly", so she decides that the best course of action is to send him a love letter in a qubit $\mid \psi_L\rangle = \alpha \mid 0_L\rangle + \beta \mid 1_L\rangle$ (it could not have been otherwise, love is in the ket).

To do so, Alice carefully puts the qubit of the pair she once entangled with Bob in a composite system with her love-ket-letter $\mid \psi_L\rangle$. The complete three-qubit system can be represented using tensor products

$$\mid \phi_A\psi_L\phi_B\rangle = \frac{1}{\sqrt{2}}\left(\mid 0_A\rangle\otimes(\alpha \mid 0_L\rangle + \beta \mid 1_L\rangle) \overset{\text{far}}{\otimes} \mid 0_B\rangle + \mid 1_A\rangle\otimes(\alpha \mid 0_L\rangle + \beta \mid 1_L\rangle) \overset{\text{far}}{\otimes} \mid 1_B\rangle\right) \tag{13.66}$$

Note that the order in the cross product is not relevant. It only matters when multiplying two composite systems, there we must ensure that each subsystem appears in the same position in each of the kets we multiply.

Alice has now a two-qubit system, and Bob, far away as he is, has one qubit which is entangled with one of the two qubits Alice has. Next, she takes the Bell-Analyzer-1001 (see Figure 13.8), a gift from Bob that she has cherished all this time, and uses it on her two qubits. The Bell analyzer does the following , starting

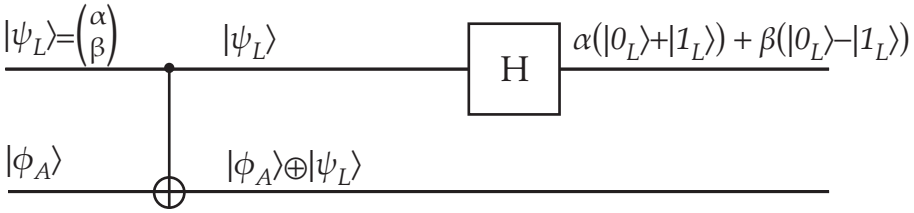

Figure 13.8: Bell analyzer.

from the initial state

$$|\,\phi_A\psi_L\phi_B\rangle = \frac{1}{\sqrt{2}}\left[|\,0_A\rangle\otimes(\alpha\,|\,0_L\rangle+\beta\,|\,1_L\rangle)\overset{\text{far}}{\otimes}|\,0_B\rangle+|\,1_A\rangle\otimes(\alpha\,|\,0_L\rangle+\beta\,|\,1_L\rangle)\overset{\text{far}}{\otimes}|\,1_B\rangle\right]$$

The CNOT gate has the effect of coupling the love-ket-letter with Alice's qubit, and indirectly, since Alice's qubit is entangled with Bob's, with Bob's as well. If ψ_L where equal to $|\,0\rangle$, Alice's other qubit would go unmodified (this is the first line in the equation below). If on the contrary it were $|\,1\rangle$, it would be added modulo 2 to Alice's otherqubit, or, in other words, Alice's other qubit would be flipped (this is what happens in the second line below). Since ψ_L is itself a superposition, what it ends up happening is that a fraction of the qubit remains unmodified with amplitude α and the other fraction is flipped, with amplitude β. So in practice what the CNOT does is transfer the superposition to Alice's Qubit

$$\begin{aligned}&=\frac{1}{\sqrt{2}}\alpha\left(|\,0_A\rangle\overset{\text{far}}{\otimes}|\,0_B\rangle+|\,1_A\rangle\overset{\text{far}}{\otimes}|\,1_B\rangle\right)\otimes|\,0_L\rangle\\ &+\frac{1}{\sqrt{2}}\beta\left(|\,1_A\rangle\overset{\text{far}}{\otimes}|\,0_B\rangle+|\,0_A\rangle\overset{\text{far}}{\otimes}|\,1_B\rangle\right)\otimes|\,1_L\rangle\end{aligned}$$

At this point Alice's and Bob's qubit have both the information of the superposition that was originally in the love-ket-letter. The Hadamard gate produces a new superposition out of the love-ket-letter as follows

$$\begin{aligned}&=\frac{1}{\sqrt{2}}\alpha\left(|\,0_A\rangle\overset{\text{far}}{\otimes}|\,0_B\rangle+|\,1_A\rangle\overset{\text{far}}{\otimes}|\,1_B\rangle\right)\otimes\frac{1}{\sqrt{2}}(|\,0_L\rangle+|\,1_L\rangle)\\ &+\frac{1}{\sqrt{2}}\beta\left(|\,1_A\rangle\overset{\text{far}}{\otimes}|\,0_B\rangle+|\,0_A\rangle\overset{\text{far}}{\otimes}|\,1_B\rangle\right)\otimes\frac{1}{\sqrt{2}}(|\,0_L\rangle-|\,1_L\rangle)\end{aligned}$$

At this point the information about the superposition in the original ket-love-letter is no longer in Alice's hands. However, to appreciate that it is so, we need to make some manipulations and reordering of the cross products. The Expression above can be separated in two sides, what Alice has and what Bob has, and then it breaks down into four terms that have a clearer interpretation

$$\begin{aligned}
&= \frac{1}{2} \mid 0_A\rangle \otimes \mid 0_L\rangle \overset{\text{far}}{\otimes} (\alpha \mid 0_B\rangle + \beta \mid 1_B\rangle) \\
&+ \frac{1}{2} \mid 0_A\rangle \otimes \mid 1_L\rangle \overset{\text{far}}{\otimes} (\alpha \mid 0_B\rangle - \beta \mid 1_B\rangle) \\
&+ \frac{1}{2} \mid 1_A\rangle \otimes \mid 0_L\rangle \overset{\text{far}}{\otimes} (\alpha \mid 1_B\rangle + \beta \mid 0_B\rangle) \\
&+ \frac{1}{2} \mid 1_A\rangle \otimes \mid 1_L\rangle \overset{\text{far}}{\otimes} (\alpha \mid 1_B\rangle - \beta \mid 0_B\rangle)
\end{aligned} \tag{13.67}$$

The manipulation we did leaves no doubt, all the information about the original superposition is in Bob's side. However the information reached bob as a superposition of the right love-ket-letter and all the possible errors produced by phase change (sign) and bit flips!.

Alice realizes now that there is no way for her to avoid talking with Bob about her love-ket-leter. Bob has the information, but to recover the exact superposition from the love-ket-letter he needs to know how to unscramble it, and only Alice can tell him. The next steps are the key to faultless teleportation

- Alice measures her two qubits, she will obtain either of $\mid 0_A 0_L\rangle, \mid 0_A 1_L\rangle, \mid 1_A 0_L\rangle$, or $\mid 1_A 1_L\rangle$ with equal probability.
- Upon Alice's measurement, Bob's qubit takes the value of one of the four possible superpositions. And so, the result of her measurement can help Bob unscramble his bit
- If she measured $\mid 0_A 0_L\rangle$, she will tell Bob not to do anything to his qubit. If she measured $\mid 0_A 1_L\rangle$, Bob will have to correct for the phase (that can be done with a Z gate). If she measured $\mid 1_A 0_L\rangle$, the states in the message have been flipped, and to unflip them Bob will have to use a bit-flip (a.k.a not, a.k.a X) gate. Finally if she measured $\mid 1_A 1_L\rangle$, Bob will have to correct both for the phase and the bit flip.

In total, Alice tells Bob to follow one of 4 possibilities, so she needs to communicate to him 2 classical bits, and then Bob will be able to read the love-ket-letter.

Now Bob better be ready to understand the love letter, because Alice no longer has it! Notice how quantum teleportation transfers the information about the superposition instantly, but Alice needs to measure her system and tell to Bob the result for him to unscramble his bit. In a sense, after teleportation, Bob is doing error correction based on the syndrome measured by Alice; the first bit of Alice informs about bit-flip errors and the second about phase errors. When we get to talk about quantum error correction, we will see that these are the two types of errors that appear in quantum communication.

It is important to appreciate that Alice can only communicate the syndrome to Bob classically, hence, instantaneous teleportation is impossible, Bob will not be able to read the love letter in less time than "far"/"speed of light". Remember the example of the yawn-connection?, there too observers had to exchange data to ensure that communication had occurred.

Quantum teleportation has served us as a verification of the no-cloning theorem, (Alice no longer has a copy of the love letter, much like it happens with "snail" mail), and has helped us introduce the notion of error and error correction. We have also seen that instantaneous communication is not possible, because classical communication is needed to correct for the errors.

13.9.2 Quantum Cryptography

This section is still under construction. Sorry.

13.10 Quantum Algorithms

This section is still under construction. Sorry.

13.10.1 Deutsch Josza

This section is still under construction. Sorry.

13.10.2 Grover

This section is still under construction. Sorry.

13.11 Quantum Information Science

This section is still under construction. Sorry.

Quantum Error Correcting Codes

This section is still under construction. Sorry.

6.050J / 2.110J Information and Entropy
Spring 2008