# Lectures on Quantum Information

William G. Faris
University of Arizona

August 15, 2002

## Contents

# 1 Introduction

These lectures are an elementary introduction to entangled states and to quantum information. They begin with a brief account of quantum mechanics, focusing on quantum events and their probabilities. The first topic is a review of the theory of square complex matrices. Then quantum events are realized mathematically as orthogonal projection matrices.

The first example is the system consisting of a single spin 1/2 particle. This system is formulated in terms of 2 by 2 matrices. Each non-trivial event corresponds to whether the spin of the particle is in a certain direction.

Next there is a brief introduction to the logic of quantum events. The main difference between quantum mechanics and probability is that in quantum mechanics there are events that are not compatible.

The next example is the main subject of the lectures. This is the system of two spin 1/2 particles. This example is formulated in terms of 4 by 4 matrices. For each of the two particles there is an event associated with each given direction. Two events associated with two different particles are compatible. It turns out that there is a state of the system where these events are very far from independent.

The lectures conclude with a discussion of the significance of this example for our understanding of nature. The dependence between the spins of the two particles presents the simplest and most striking example of an entangled quantum state. Such examples point to a holistic nature of quantum mechanics that has startling consequences. This is made precise in Bell's theorem, which says that the dependence has no explanation in terms of conventional probability. There is also some mention of quantum cryptography as a development in the relatively new field of quantum information.

# 2 Matrices

## 2.1 Algebra of square matrices

An $n$ by $n$ complex matrix is a square array $A$ of complex numbers with $n$ rows and $n$ columns. The entry in the $i$th row and $j$th column is denoted $A_{ij}$. Matrices admit several algebraic operations.

Addition and subtraction. The *sum* or *difference* of two $n$ by $n$ matrices $A$, $B$ is denoted $A \pm B$ and is defined by

$$(A \pm B)_{ij} = A_{ij} \pm B_{ij}. \tag{1}$$

Multiplication. The *product* of two $n$ by $n$ matrices $A$, $B$ is denoted $AB$ and is defined by

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik} B_{kj}. \tag{2}$$

For each $n$ there is an $n$ by $n$ *zero matrix* $O$ that has all entries zero. There is another $n$ by $n$ *identity* matrix $I$ that has the diagonal entries $I_{ii} = 1$, but all off-diagonal entries $I_{ij} = 0$ for $i \neq j$.

The algebra of matrices includes such addition identities as $A + B = B + A$, $A + 0 = A$, $A - A = 0$. Two matrices are said to *commute* if $AB = BA$. Typical matrices do not commute. However there are useful multiplication identities such as $A(B \pm C) = AB \pm AC$, $(B \pm C)A = BA \pm CA$, $A0 = 0$, $0A = 0$, $AI = A$, $IA = A$.

A *diagonal* $n$ by $n$ matrix is a matrix with zeros everywhere except on the main diagonal. Thus a diagonal matrix is specified by a list of $n$ complex numbers. Thus one can think of a complex matrix as a generalization of the concept of a list of complex numbers.

## 2.2 The adjoint of a matrix

The *adjoint* of an $n$ by $n$ matrix $A$ is the matrix $A^*$ defined by

$$(A^*)_{ij} = \overline{A_{ji}}. \tag{3}$$

That is, one reflects the matrix over the diagonal and takes the complex conjugate of each entry.

The adjoint satisfies algebraic properties like $A^{**} = A$, $(A \pm B)^* = A^* \pm B^*$ and $(AB)^* = B^*A^*$. It can be thought of as a generalization of the concept of complex conjugation.

A matrix $A$ is said to be *self-adjoint* if $A = A^*$. The diagonal entries of a self-adjoint matrix are real. Thus a self-adjoint matrix is a generalization of the concept of a list of $n$ real numbers.

A matrix $A^*A$ is automatically self-adjoint. It is the analog of the absolute value squared of a complex number. The diagonal entries of such a matrix are real and positive.

## 2.3 The trace of a matrix

The *trace* of an $n$ by $n$ matrix $A$ is the complex number defined by

$$\mathrm{tr}(A) = \sum_{i=1}^{n} A_{ii}. \tag{4}$$

Thus the trace is the sum of the diagonal entries.

The trace satisfies algebraic properties that include $\mathrm{tr}(A \pm B) = \mathrm{tr}(A) \pm \mathrm{tr}(B)$, $\mathrm{tr}(AB) = \mathrm{tr}(BA)$, and $\mathrm{tr}(A^*) = \overline{\mathrm{tr}(A)}$. The trace of a self-adjoint matrix is a real number. Furthermore, it is easy to see that $\mathrm{tr}(A^*A) \geq 0$.

## 2.4 Projection matrices

A matrix $P$ is said to be a *projection* if $P^2 = P$. The trace of a projection is a natural number $0, 1, 2, \ldots, n$. This number is called the *rank* or *dimension* of the projection.

A matrix $E$ is said to be an *orthogonal projection* if $E = E^*$ and $E^2 = E$, that is, if $E$ is a self-adjoint projection. An orthogonal projection that is diagonal has just the numbers one and zero on the diagonal. An orthogonal projection is a generalization of the concept of a list of $n$ numbers, each of which is either one or zero. In general, one can think of an orthogonal projection as assuming the value one with a certain multiplicity, which is the rank $r = \mathrm{tr}(E)$ of the orthogonal projection. Corresponding, it can assume the value zero with multiplicity $n - r$.

### 2.5 Problems

1. Which of the following are correct trace identities? (a) $\mathrm{tr}(AB) = \mathrm{tr}(A)\mathrm{tr}(B)$. (b) $\mathrm{tr}(AA^*) \geq 0$. (c) $\mathrm{tr}(ABC) = \mathrm{tr}(CAB)$. (d) $\mathrm{tr}(ABC) = \mathrm{tr}(CBA)$.

2. Define the Hilbert-Schmidt norm $\|A\|_2$ of a matrix to be given by $\|A\|_2^2 = \mathrm{tr}(A^*A)$. Prove that $|\mathrm{tr}(A^*B)| \leq \|A\|_2\|B\|_2$.

3. If $E$ is an orthogonal projection, then when is $I - E$ an orthogonal projection? If $E$ and $F$ are orthogonal projections, then when is $EF$ an orthogonal projection?

4. If $E$ and $F$ are orthogonal projections, express $\mathrm{tr}(EF)$ as the square of the Hilbert-Schmidt norm of a certain matrix.

5. Find all 2 by 2 complex matrices $C$ such that $C^* = C$ and $C^2 = I$. Such a matrix is called a *complex reflection* if also $\mathrm{tr}(C) = 0$. Find all complex reflections. Show that the set of all complex reflections form a sphere.

6. Find all 2 by 2 complex matrices $E$ that satisfy the equations $E^* = E$ and $E^2 = E$ for an orthogonal projection. Show that the orthogonal projections with $\mathrm{tr}(E) = 1$ form a sphere. Hint: Let $E = \frac{1}{2}(I + C)$.

## 3 Quantum mechanics

### 3.1 Quantum events and quantum states

Quantum mechanics for an $n$ level system is formulated in terms of $n$ by $n$ matrices. A *quantum event* is an orthogonal projection $E$. That is, it is an $n$ by $n$ matrix with $E = E^*$ and $E^2 = E$.

A *quantum state* is an orthogonal projection $R$ with $\mathrm{tr}(R) = 1$.

### 3.2 Quantum probability

**Theorem 1** *If the probability of a quantum event $E$ in the quantum state $R$ is defined by*

$$\mathbf{P}_R[E] = \mathrm{tr}(ER), \tag{5}$$

*then $0 \leq \mathbf{P}_R[E] \leq 1$.*

Proof: Observe that $\mathbf{P}_R(E) = \mathrm{tr}(ER) = \mathrm{tr}(ER^2) = \mathrm{tr}(RER)$. Furthermore, $RER = (RE)(ER) = (ER)^*(ER)$. It follows that $0 \leq \mathbf{P}_R(E)$. Thus the probability of an arbitrary event is positive. The orthogonal projection $I - E$ plays the role of the complementary event. Since $\mathrm{tr}(ER) + \mathrm{tr}((I - E)R) = \mathrm{tr}(R) = 1$, it follows that $\mathbf{P}_R(E) + \mathbf{P}_R(I - E) = 1$. Thus the probability of the event and its complement sum to one. From this we see that $0 \leq \mathbf{P}_R(E) \leq 1$.

### 3.3 Problems

1. A quantum state is an orthogonal projection of rank one. Define the distance $d(R, S)$ between two quantum states to be given in terms of the Hilbert-Schmidt norm by $d(R, S) = (1/\sqrt{2})\|R - S\|_2$. What is the maximum distance between two quantum states?

2. Say that $R$ and $S$ are quantum states with $RS = 0$. Let $G = R + S$, so that $G$ is an orthogonal projection with rank 2. Let $C$ be a self-adjoint matrix satisfying $CG = GC = C$ and $C^2 = G$ and $\mathrm{tr}(C) = 0$. Let $E = (1/2)(G + C)$. Show that $E$ is also a quantum state and that $E$ satisfies $EG = GE = E$. Such a state is called a *superposition* of $R$ and $S$. The superpositions of $R$ and $S$ form a sphere, with $R$ at the north pole (corresponding to $C = R - S$) and with $S$ at the south pole (corresponding to $C = S - R$). The latitude circles are parametrized by $p = \mathrm{tr}(RER)$ and $q = \mathrm{tr}(SES)$ with $p+q = 1$. We may write $E = GEG = RER + SES + RES + SER$, or $E = pR + qS + RES + SER$. The last two terms are called the *interference terms*.

# 4 One quantum bit

## 4.1 One spin 1/2 particle

In classical computation one *bit* is the information contained in a choice of 0 or 1. In quantum computation one *qubit* is the information contained in a choice of a quantum state in a two-level system. Sometimes this system is referred to as a single spin 1/2 particle.

Let $(x, y, z)$ be a triple of real numbers with $x^2 + y^2 + z^2 = 1$. For each such unit vector there is a orthogonal projection

$$E(x, y, z) = \frac{1}{2}\begin{bmatrix} 1 + z & x - iy \\ x + iy & 1 - z \end{bmatrix}. \tag{6}$$

**Proposition 1** *The matrix $E(x, y, z)$ satisfies the equations $E = E^*$ and $E^2 = E$ for a projection matrix. Furthermore, it has rank one.*

Thus for every unit vector $(x, y, z)$ there is a corresponding quantum state for the single spin 1/2 particle given by $E(x, y, z)$.

The quantum events are also given in this way. The only non-trivial quantum events are given by the projections $E(x', y', z')$. Thus for every unit vector $(x', y', z')$ there is a corresponding quantum event given by $E(x', y', z')$. Of course there are also the trivial quantum events 0 and $I$.

For each direction $(x', y', z')$ there is a spin variable that can either be along this direction or opposite to this direction. The interpretation of the quantum event $E(x', y', z')$ is that the spin variable is along this direction. Sometimes one thinks of the spin variable for a given direction as having the value $1/2$ when the spin is along the direction and the value $-1/2$ when the spin is opposite to the direction.

**Proposition 2** *The quantum events associated with unit vectors in opposite directions satisfy*

$$E(-x', -y', -z') + E(x', y', z') = I \tag{7}$$

*and so are the negations of each other. All pairs of quantum events for this system determined by unit vectors that are not in the same or opposite directions are incompatible.*

**Theorem 2** *Consider a system consisting of a single spin 1/2 particle. If the state is determined by the unit vector $(x, y, z)$, then the probability that the spin is in the direction of the unit vector $(x', y', z')$ is*

$$\mathbf{P}_{(x,y,z)}[E(x', y', z')] = \frac{1}{2}(1 + xx' + yy' + zz') = \frac{1}{2}(1 + \cos(\theta)) = \cos^2(\theta/2). \tag{8}$$

Proof. Multiply the matrices. Take the trace of the result.

Remark. The presence of the $\theta/2$ in the last formula is the reason for the terminology spin 1/2.

### 4.2 Problems

1. Recall the definition of distance between quantum states in a previous problem. What is the distance between the two quantum states $E(x, y, z)$ and $E(x', y', z')$?

## 5 Quantum logic

### 5.1 Compatible quantum events

Quantum events $E, F$ are said to be *compatible* if they commute, that is, if $EF = FE$. In that case $EF$ is also a quantum event.

### 5.2 Negation, conjunction, disjunction

The *negation* or *complement* of a quantum event is the quantum event

$$\neg E = I - E. \tag{9}$$

The *conjunction* of two compatible quantum events $E, F$ is defined to be

$$E \wedge F = EF. \tag{10}$$

The conjunction is not defined for events that are not compatible.

The peculiarity of quantum mechanics (compared to probability theory) is that conjunction is defined only for events that are compatible.

The *disjunction* of two compatible quantum events $E, F$ is defined to be

$$E \vee F = \neg(\neg E \wedge \neg F). \tag{11}$$

The disjunction is not defined for events that are not compatible.

Note: The disjunction of two compatible events may be written in matrix algebra rather than in logic. It is then

$$E \vee F = I - (I - E)(I - F) = E + F - EF. \tag{12}$$

The probability of the complement of a quantum event is

$$\mathbf{P}_R[\neg E] = 1 - \mathbf{P}_R[E]. \tag{13}$$

The probability of the disjunction of two compatible quantum events is

$$\mathbf{P}_R[E \vee F] = \mathbf{P}_R[E] + \mathbf{P}_R[F] - \mathbf{P}_R[E \wedge F]. \tag{14}$$

Two compatible quantum events are said to be *exclusive* if $E \wedge F = 0$. For exclusive events we have the law $\mathbf{P}_R[E \vee F] = \mathbf{P}_R[E] + \mathbf{P}_R[F]$.

Two compatible quantum events are said to be *independent* if $\mathbf{P}_R[E \wedge F] = \mathbf{P}_R[E]\mathbf{P}_R[F]$. Sometimes the size of the *correlation* $4(\mathbf{P}(E \wedge F] - \mathbf{P}[E]\mathbf{P}[F])$ is taken as a measure of the lack of independence. This correlation is always between $-1$ and $1$.

## 5.3 Problems

1. Prove the following *uncertainty principle*:

$$P_S[E] + P_S[F] \leq 1 + 2\sqrt{\mathrm{tr}(EF)}. \tag{15}$$

   Hint: Expand $(E+F-1)^2$. This principle implies that certain events that are not compatible are nevertheless almost exclusive, in a certain sense. The most famous example is when $E$ is the event that a particle has its position in a certain small interval and $F$ is the event that the particle has its momentum in a certain small interval. Then $\mathrm{tr}(EF)$ is a physical constant times the product of the lengths of the two intervals, divided by $2\pi$. If the product of the lengths is sufficiently small, then, for every state, it is impossible that the position probability and the momentum probability both be near one.

2. Some authors have proposed to define the conjunction of two events $E, F$ that are not compatible. For instance, it may be shown that $(EFE)^n$ converges to a matrix $G$ as $n \to \infty$. Show that $G$ is an orthogonal projection.

# 6 Two quantum bits

## 6.1 Two spin 1/2 particles

Now we look at a 4-level system consisting of two spin 1/2 particles. One belongs to Alice and one belongs to Bob. There are now two sets of spin matrices. For Alice we have the Kronecker product of the matrices $E(x,y,z)$ and $I$, that is, $E^A(x,y,z)$ given by

$$\frac{1}{2}\begin{bmatrix} 1+z\begin{bmatrix}1&0\\0&1\end{bmatrix} & x-iy\begin{bmatrix}1&0\\0&1\end{bmatrix} \\ x+iy\begin{bmatrix}1&0\\0&1\end{bmatrix} & 1-z\begin{bmatrix}1&0\\0&1\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+z & 0 & x-iy & 0 \\ 0 & 1+z & 0 & x-iy \\ x+iy & 0 & 1-z & 0 \\ 0 & x+iy & 0 & 1-z \end{bmatrix}. \tag{16}$$

This is just two copies of the projection matrix. The first copy belongs with the first and third rows and columns, while the second copy belongs with the second and fourth rows and columns. For Bob we have the Kronecker product of $I$ and $E(x,y,z)$, that is $E^B(x,y,z)$ given by

$$\frac{1}{2}\begin{bmatrix} 1\begin{bmatrix}1+z & x-iy\\x+iy&1-z\end{bmatrix} & 0\begin{bmatrix}1+z & x-iy\\x+iy&1-z\end{bmatrix} \\ 0\begin{bmatrix}1+z & x-iy\\x+iy&1-z\end{bmatrix} & 1\begin{bmatrix}1+z & x-iy\\x+iy&1-z\end{bmatrix}\end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1+z & x-iy & 0 & 0 \\ x+iy & 1-z & 0 & 0 \\ 0 & 0 & 1+z & x-iy \\ 0 & 0 & x+iy & 1-z \end{bmatrix}. \tag{17}$$

This is again two copies of the projection matrix. The first copy belongs with the first and second rows and columns, while the second copy belongs with the third and fourth rows and columns. Each of these matrices has rank two.

**Proposition 3** *The orthogonal projection operators $E^A(x,y,z)$ and $E^B(x',y',z')$ commute with each other.*

The orthogonal projection $E^A(x,y,z)E^B(x',y',z')$ has rank one and thus defines a state. This is a state in which the A spin and the $B$ spin are independent. The $A$ spin in the $(x,y,z)$ direction is 1/2 and the $B$ spin in the $(x',y',z')$ direction is also 1/2.

In this system there are other interesting orthogonal projections that define quantum events and quantum states. The orthogonal projection

$$E_0 = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{18}$$

corresponds to the event of total spin 0, while the complementary orthogonal projection

$$E_1 = \frac{1}{2}\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix} \tag{19}$$

corresponds to the event of total spin 1. These projections have rank one and three respectively. The projection matrix $R_0 = E_0$ may thus be regarded also as a quantum state and is called the *singlet state.*

The singlet state has the property that for an arbitrary direction the probability that both particles have spin in this direction is zero. On the other hand, the probability that one or the other of the particles has spin in this direction is one.

**Theorem 3** *The singlet state $R_0$ is the unique state such that for each direction the conjunction $E^A(x, y, z)E^B(x, y, z)$ has probability zero.*

**Theorem 4** *Consider a system of two spin 1/2 particles in the singlet state. The probability that the spin of particle A is in the $(x, y, z)$ direction is*

$$\mathbf{P}_0[E^A(x, y, z)] = \mathrm{tr}(E^A(x, y, z)R_0) = \frac{1}{2}. \tag{20}$$

*Similarly, the probability that the spin of particle B is in the $(x', y', z')$ direction is*

$$\mathbf{P}_0[E^B(x', y', z')] = \mathrm{tr}(E^B(x', y', z')R_0) = \frac{1}{2}. \tag{21}$$

**Theorem 5** *Consider a system of two spin 1/2 particles in the singlet state. The probability that the spin of particle A is in the $(x, y, z)$ direction and the spin of particle B is in the $(x', y', z')$ direction is*

$$\begin{aligned} \mathbf{P}_0[E^A(x, y, z)E^B(x', y', z')] &= \mathrm{tr}(E^A(x, y, z)E^B(x', y', z')R_0) \\ = \frac{1}{4}(1 - xx' - yy' - zz') &= \frac{1}{4}(1 - \cos(\theta)) = \frac{1}{2}\sin^2(\theta/2). \end{aligned} \tag{22}$$

A state in which the event $E_1$ has probability one is called a *triplet state.* An example of a triplet state is a state $E^A(x, y, z)E^B(x, y, z)$ in which the spins are aligned in a fixed direction $(x, y, z)$. Each individual spin in this direction has the alue 1/2, so the total spin in this direction is 1.

## 6.2 Problems

1. Let $0 \leq p \leq 1$ and $0 \leq q \leq 1$ and $p + q = 1$. Let $\chi$ be arbitrary. Show that the state

$$R = \begin{bmatrix} p & 0 & 0 & \sqrt{pq}e^{i\chi} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \sqrt{pq}e^{-i\chi} & 0 & 0 & q \end{bmatrix}. \tag{23}$$

   is a triplet state. (This is a superposition of the triplet state where both spins are up and the triplet state where both spins are down.)

2. Find the probabilities of $E(x, y, z)$ and $E(x', y', z')$ and of $E(x, y, z)E(x', y', z')$ in the superposition triplet state $R$.

3. Look at $E^A(0, 0, 1)$ and $E^B(0, 0, 1)$ in the superposition triplet state $R$. When are these independent? That is, when is the probability of the conjunction equal to the product of the probabilities?

# 7 Entangled states

## 7.1 Quantum mechanics as a physical theory

The quantum theory has several astonishing characteristics:

- It explains all of physics and chemistry on the molecular, atomic, and subatomic scales.
- It involves linear algebra and nothing else.
- It gives a holistic description of nature in which an arbitrary collection of particles can display correlated behavior.
- Its interpretation is confused and controversial. The most common interpretation says (roughly) that nothing is real unless it is measured.

The holistic nature of quantum theory was first brought out in a famous paper of Einstein, Rosen, and Podolsky. They proposed a thought experiment that illustrated this feature. Later David Bohm proposed a variant of this experiment involving spin that could actually be performed. Subsequently, John Bell gave a profound analysis of this spin experiment.

## 7.2 The spin experiment

A spin $1/2$ particle is a quantum system with a particularly simple structure. For each direction in space, there is a *spin variable* that can have two possible values, say $+1/2$ and $-1/2$. For each such direction, one can set up an experimental apparatus that measures this variable. The values obtained are random and are predicted by quantum theory. If one takes the opposite direction in space, then spin $-1/2$ and $+1/2$ in that opposite direction are regarded as the same as spin $+1/2$ and $-1/2$ in the original direction.

The Bohm experiment involves two experimenters, Alice and Bob. They are in distant locations. One of the experimenters prepares a system consisting of two spin $1/2$ particles prepared in the *singlet state*. This is a special quantum mechanical state in which the particles have a certain correlated behavior. Then one of the particles is sent to the other experimenter. So Alice has a particle, Bob has a particle, Alice and Bob are far apart, and each is ready to do an experiment.

The singlet state has the following properties. For each particle and for each direction in space, the probability of the spin variable for that direction having the value $+1/2$ is $1/2$, and the probability of the spin variable for that direction having the value $-1/2$ is also $1/2$. However the values for the two particles are correlated in a special way. Say that the angle between the axis chosen for the Alice particle and the Bob particle is $\theta$. Then the probability that Alice and Bob get the same answer (both $+1/2$ or both $-1/2$) is $\sin^2(\theta/2)$. It follows that the probability that Alice and Bob get different answers is $\cos^2(\theta/2)$.

More specifically, the probability that Alice and Bob get particular values when the angle between their measurement directions is $\theta$ is given by the following table:

$$\begin{aligned}
P[+1/2,+1/2] &= (1/2)\sin^2(\theta/2) \\
P[+1/2,-1/2] &= (1/2)\cos^2(\theta/2) \\
P[-1/2,+1/2] &= (1/2)\cos^2(\theta/2) \\
P[-1/2,-1/2] &= (1/2)\sin^2(\theta/2). \qquad (24)
\end{aligned}$$

Notice that if Alice and Bob happen to choose the same direction, so $\theta = 0$, then they always get opposite answers. If they choose opposite directions, so $\theta = \pi$, then they also always get the same answer. So it is reasonable to say that for any common choice of axis the spins are in opposite directions. The total spin is zero.

If, on the other hand, Alice and Bob choose directions that are at right angles, so that $\theta = \pi/2$, then the chance that they get the same answer is $1/2$.

It will specially important for us to have the answer when the angle is $2\pi/3$. In this case the probability that they get the same answer is $3/4$, and the probability that they get different answers is $1/4$. This is again saying that spins tend to be in opposite directions, but in a probabilistic sense.

In probability, we may say that two events $U$ and $V$ are probabilistically equivalent if $\mathbf{P}[U] = \mathbf{P}[V] = \mathbf{P}[U \wedge V]$. If $U$ and $V$ are probabilistically equivalent, then for every event $W$ we have $\mathbf{P}[U \wedge W] = \mathbf{P}[V \wedge W]$.

Pick three directions in space in a plane that are at angle $2\pi/3$ with each other. Let $E^A$, $F^A$, and $G^A$ be the events that the spin of the Alice particle is $+1/2$ in the first, second, or third of these directions. Let $E^B$, $F^B$,and $G^B$ be the events that the spin of the Bob particle is $+1/2$ in the same directions. Then for the first direction $\mathbf{P}[\neg E^A] = \frac{1}{2}$, $\mathbf{P}[E^B] = \frac{1}{2}$, and $\mathbf{P}[\neg E^A \wedge E^B] = \frac{1}{2}$. Thus $\neg E^A$ and $E^B$ are probabilistically equivalent. Similarly, for the second direction, $\neg F^A$ and $F^B$ are probabilistically equvalent. And finally, for the third direction $\neg G^A$ and $G^B$ are probabilistically equivalent.

In summary, these equations imply that whenever the two directions for the two particles are the same, the event that the $A$ particle has spin $-1/2$ is probabilistically equivalent to the event that the $B$ particle has spin $+1/2$.

**Theorem 6** *Consider the system of two spin 1/2 particles in the singlet state. Suppose that there were a probability assignment obeying the usual probability laws that agrees with the probability predictions of quantum mechanics for this system. Then we would have the inequality*

$$\mathbf{P}[E^A \wedge F^B] + \mathbf{P}[F^A \wedge G^B] + \mathbf{P}[G^A \wedge E^B] \leq 1. \qquad (25)$$

The hypothesis of the theorem implies in particular that events involving two different directions for one particle can be combined in accordance with the laws of a fixed probability assignment. Of course quantum mechanics regards these events as incompatible, but the probability assignment is supposed to be an extension of quantum mechanics. This theorem is called Bell's first theorem, and the inequalities are Bell's inequalities.

Here is the proof of Bell's first theorem. Suppose that probabilities associated with the same particle were meaningful. Since $E^B$ is equivalent to $\neg E^A$, $F^B$ is equivalent to $\neg F^A$, and $G^B$ is equivalent to $\neg G^A$, we would have the equations

$$\begin{aligned} \mathbf{P}[E^A \wedge F^B] &= \mathbf{P}[E^A \wedge \neg F^A] \\ \mathbf{P}[F^A \wedge G^B] &= \mathbf{P}[F^A \wedge \neg G^A] \\ \mathbf{P}[G^A \wedge E^B] &= \mathbf{P}[G^A \wedge \neg E^A]. \end{aligned} \tag{26}$$

However from elementary probability

$$\mathbf{P}[E^A \wedge \neg F^A] + \mathbf{P}[F^A \wedge \neg G^A] + \mathbf{P}[G^A \wedge \neg E^A] \leq 1. \tag{27}$$

**Corollary 1** *There is no probability assignment obeying the usual probability laws that agrees with the probability predictions of quantum mechanics for this system.*

Proof: According to quantum mechanics,

$$\begin{aligned} \mathbf{P}[E^A \wedge F^B] &= \frac{3}{8} \\ \mathbf{P}[F^A \wedge G^B] &= \frac{3}{8} \\ \mathbf{P}[G^A \wedge E^B] &= \frac{3}{8}. \end{aligned} \tag{28}$$

This contradicts Bell's inequalities. Thus for quantum mechanics there are no joint probabilities for spin in different directions for the same particle.

Since Bell's inequalities contradict the prediction of quantum mechanics, it follows that quantum mechanics must violate the hypothesis of the theorem. Events involving measurements in two different directions for the same particle cannot be combined in accordance with the laws of a fixed probability assignment. Making one measurement interferes in an essential way with the possibility of making the other measurement. There is much more to be said about the implications of this theorem. An excellent source is the appendix to the book *The Infamous Boundary*, by David Wick.

## 7.3 Quantum cryptography

It is tempting to put quantum entanglement to practical use. There are several ways to proceed. Here is one example. Say that Alice and Bob are located far apart. They can communicate openly. However they desire to generate a key to encode secret information. This key must have the property that a third party Eve cannot obtain it without being detected.

Here is a first attempt. Alice and Bob order pairs of spin 1/2 particles in the singlet state from a supplier. They decide on a certain direction $a$ in space in which to perform spin measurements. With probability $1/2$, Alice measures a spin $+1/2$ in this direction, Bob measures a spin $-1/2$ in this direction. With probability $1/2$, Alice measures a spin $-1/2$ in this direction, Bob measures a spin $+1/2$ in this direction. Thus for each pair of particles Alice and Bob get opposite results. It is as if they each could look at the flip of a single coin. They record the results, and this gives each of them the key to the code in which they will communicate.

This first attempt is not as secure as might be desired, since Eve might also somehow manage to make spin measurements in the $a$ direction.

The second attempt is more subtle. Alice and Bob each randomly choose to use one of two perpendicular directions $a$ and $b$ for their spin measurements. When Alice and Bob both happen to choose $a$, then they get opposite results as before. When they both happen to choose $b$, the same thing happens. When they choose different directions, then their results are completely independent of each other, as if they flipped two coins. After all this experimentation takes place, Alice and Bob communicate openly and tell what directions they chose. They then use the cases when they happened to choose the same direction to establish their key.

Now Eve cannot detect the code without being detected. Say, for instance, that Eve made measurements in the $a$ direction. These would perhaps not be detected when Alice and Bob themselves made measurements in the $a$ direction. However when Alice and Bob both make measurements in the $b$ direction, they will notice that they no longer get results that are exact opposites. They can establish this by open communication about the results of a certain fraction of their experiments. The measurements Eve made in the $a$ direction have betrayed themselves. This is because a measurement in the $a$ direction in the entangled state precludes measurements by Alice and Bob in the $b$ direction in that state. That is, this measurements by Alice or Bob in the $b$ direction no longer give the results predicted by the entangled state, and this is something they would eventually notice. Of course all this requires a detailed analysis to prove. Such a proof is provided by quantum information theory.

## 7.4 Problems

1. Prove that if $U$ and $V$ are probabilistically equivalent, then $\mathbf{P}[U \wedge W] = \mathbf{P}[V \wedge W]$.

2. Prove the probability inequality $\mathbf{P}[E \wedge \neg F] + \mathbf{P}[F \wedge \neg G] + \mathbf{P}[G \wedge \neg E] \leq 1$.

3. In probability two events are said to be *independent* if the probability that they both occur is the product of the individual probabilities. Consider the system of two spin $1/2$ particles in the singlet state. For which relative orientations $\theta$ are the events that the A particle has spin $+1/2$ and that the B particle has spin $+1/2$ independent?

4. For each direction in space, there is a triplet state of the two spin $1/2$ particle system in which both particles are aligned in this direction. Let

$\theta_a$ be the angle between the measured spin component of the A particle and the direction for the triplet state. Let $\theta_b$ be the angle between the measured spin component of the B particle and the direction for the triplet state. Then the probability that the A measurement and the B measurement both give $+1/2$ is $\cos^2(\theta_a/2)\cos^2(\theta_b/2)$. Use this to work out the probabilities for all four outcomes. Show that these probabilities sum to one. For which parameter values are the events for the A and B particle independent? Suppose the direction of this triplet state is known. Does the result of a measurement on the $A$ particle give any additional useful information about the result of a measurement on the B particle?