Lecture Notes for Ph219/CS219: Quantum Information and Computation Chapter 2

John Preskill
California Institute of Technology

Updated July 2015

Contents

2
Foundations I: States and Ensembles

2.1 Axioms of quantum mechanics

In this chapter and the next we develop the theory of *open* quantum systems. We say a system is open if it is imperfectly isolated, and therefore exchanges energy and information with its unobserved environment. The motivation for studying open systems is that all realistic systems are open. Physicists and engineers may try hard to isolate quantum systems, but they never completely succeed.

Though our main interest is in open systems we will begin by recalling the theory of closed quantum systems, which *are* perfectly isolated. To understand the behavior of an open system S, we will regard S combined with its environment E as a closed system (the whole "universe"), then ask how S behaves when we are able to observe S but not E.

Quantum theory is a mathematical model of the physical world. For the case of closed systems we can characterize the model by stating five axioms; these specify how to represent states, observables, measurements, and dynamics, and also how to combine two systems to obtain a composite system.

Axiom 1. States. A state is a complete description of a physical system. In quantum mechanics, a state is a *ray* in a *Hilbert space*.

What is a Hilbert space?

a) It is a *vector space* over the complex numbers $\mathbb{C}$. Vectors will be denoted $|\psi\rangle$ (Dirac's ket notation).

b) It has an *inner product* $\langle\psi|\varphi\rangle$ that maps an ordered pair of vectors to $\mathbb{C}$, and that has the properties:

i) Positivity: $\langle\psi|\psi\rangle > 0$ for $|\psi\rangle \neq 0$.

ii) Linearity: $\langle\varphi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\varphi|\psi_1\rangle + b\langle\varphi|\psi_2\rangle$.

iii) Skew symmetry: $\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^*$.

(The * denotes complex conjugation.)

c) It is *complete* in the norm $||\psi|| = \langle\psi|\psi\rangle^{1/2}$.

(Completeness is an important proviso in infinite-dimensional function spaces, since it ensures the convergence of certain eigenfunction expansions. But mostly we will be content to work with finite-dimensional inner-product spaces.)

What is a ray? It is an equivalence class of vectors that differ by multiplication by a nonzero complex scalar. For any nonzero ray, we can by convention choose a representative of the class, denoted $|\psi\rangle$, that has unit norm:

$$\langle\psi|\psi\rangle = 1. \tag{2.1}$$

Thus states correspond to normalized vectors, and the overall phase of the vector has no physical significance: $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$ describe the same state, where $|e^{i\alpha}| = 1$.

Since every ray corresponds to a possible state, given two states $|\varphi\rangle, |\psi\rangle$, another state can be constructed as the linear *superposition* of the two, $a|\varphi\rangle + b|\psi\rangle$. The *relative* phase in this superposition *is* physically significant; we identify $a|\varphi\rangle + b|\varphi\rangle$ with $e^{i\alpha}(a|\varphi\rangle + b|\psi\rangle)$ but *not* with $a|\varphi\rangle + e^{i\alpha}b|\psi\rangle$.

We use the notation $\langle\psi|$ (Dirac's bra notation) for a linear function (a *dual vector*) that takes vectors to complex numbers, defined by $|\varphi\rangle \to \langle\psi|\varphi\rangle$.

Axiom 2. Observables. An observable is a property of a physical system that in principle can be measured. In quantum mechanics, an observable is a *self-adjoint operator*.

An operator is a linear map taking vectors to vectors,

$$\boldsymbol{A} : |\psi\rangle \mapsto \boldsymbol{A}|\psi\rangle, \quad \boldsymbol{A}\,(a|\psi\rangle + b|\varphi\rangle) = a\boldsymbol{A}|\psi\rangle + b\boldsymbol{A}|\varphi\rangle. \tag{2.2}$$

(We will often denote operators by boldface letters.) The adjoint $\boldsymbol{A}^\dagger$ of the operator $\boldsymbol{A}$ is defined by

$$\langle\varphi|\boldsymbol{A}\psi\rangle = \langle\boldsymbol{A}^\dagger\varphi|\psi\rangle, \tag{2.3}$$

for all vectors $|\varphi\rangle, |\psi\rangle$ (where here $\boldsymbol{A}|\psi\rangle$ has been denoted as $|\boldsymbol{A}\psi\rangle$). $\boldsymbol{A}$ is self-adjoint if $\boldsymbol{A} = \boldsymbol{A}^\dagger$, or in other words, if $\langle\varphi|\boldsymbol{A}|\psi\rangle = \langle\psi|\boldsymbol{A}|\varphi\rangle^*$ for all vectors $|\varphi\rangle$ and $|\psi\rangle$. If $\boldsymbol{A}$ and $\boldsymbol{B}$ are self adjoint, then so is $\boldsymbol{A}+\boldsymbol{B}$ (because $(\boldsymbol{A}+\boldsymbol{B})^\dagger = \boldsymbol{A}^\dagger + \boldsymbol{B}^\dagger$), but $(\boldsymbol{AB})^\dagger = \boldsymbol{B}^\dagger\boldsymbol{A}^\dagger$, so that $\boldsymbol{AB}$ is self adjoint

only if $\boldsymbol{A}$ and $\boldsymbol{B}$ commute. Note that $\boldsymbol{AB} + \boldsymbol{BA}$ and $i(\boldsymbol{AB} - \boldsymbol{BA})$ are always self-adjoint if $\boldsymbol{A}$ and $\boldsymbol{B}$ are.

A self-adjoint operator in a Hilbert space $\mathcal{H}$ has a spectral representation – its eigenstates form a complete orthonormal basis in $\mathcal{H}$. We can express a self-adjoint operator $\boldsymbol{A}$ as

$$\boldsymbol{A} = \sum_n a_n \boldsymbol{E}_n. \tag{2.4}$$

Here each a_n is an eigenvalue of $\boldsymbol{A}$, and $\boldsymbol{E}_n$ is the corresponding orthogonal projection onto the space of eigenvectors with eigenvalue a_n. The $\boldsymbol{E}_n$'s satisfy

$$\begin{aligned} \boldsymbol{E}_n \boldsymbol{E}_m &= \delta_{n,m} \boldsymbol{E}_n. \\ \boldsymbol{E}_n^\dagger &= \boldsymbol{E}_n. \end{aligned} \tag{2.5}$$

The orthogonal projector onto the one-dimensional space spanned by the vector $|\psi\rangle$ may be expressed as $|\psi\rangle\langle\psi|$, where $\langle\psi|$ is the bra that annihilates vectors orthogonal to $|\psi\rangle$. Therefore, an alternative notation for the spectral representation of $\boldsymbol{A}$ is

$$\boldsymbol{A} = \sum_n |n\rangle a_n \langle n|, \tag{2.6}$$

where $\{|n\rangle\}$ is the orthonormal basis of eigenstates of $\boldsymbol{A}$, with $\boldsymbol{A}|n\rangle = a_n|n\rangle$.

(For unbounded operators in an infinite-dimensional space, the definition of self-adjoint and the statement of the spectral theorem are more subtle, but this need not concern us.)

Axiom 3. Measurement. A measurement is a process in which information about the state of a physical system is acquired by an observer. In quantum mechanics, the measurement of an observable $\boldsymbol{A}$ prepares an eigenstate of $\boldsymbol{A}$, and the observer learns the value of the corresponding eigenvalue. If the quantum state just prior to the measurement is $|\psi\rangle$, then the outcome a_n is obtained with *a priori probability*

$$\mathrm{Prob}(a_n) = \|\boldsymbol{E}_n|\psi\rangle\|^2 = \langle\psi|\boldsymbol{E}_n|\psi\rangle \ ; \tag{2.7}$$

if the outcome a_n is attained, then the (normalized) quantum state just after the measurement is

$$\frac{\boldsymbol{E}_n|\psi\rangle}{\|\boldsymbol{E}_n|\psi\rangle\|}. \tag{2.8}$$

If the measurement is immediately repeated, then according to this rule the same outcome is obtained again, with probability one. If many identically prepared systems are measured, each described by the state $|\psi\rangle$, then the *expectation value* of the outcomes is

$$\langle a\rangle \equiv \sum_n a_n \mathrm{Prob}(a_n) = \sum_n a_n \langle\psi|\boldsymbol{E}_n|\psi\rangle = \langle\psi|\boldsymbol{A}|\psi\rangle. \tag{2.9}$$

Axiom 4. Dynamics. Dynamics describes how a state evolves over time. In quantum mechanics, the time evolution of a closed system is described by a *unitary operator*.

In the *Schrödinger picture* of dynamics, if the initial state at time t is $|\psi(t\rangle$, then the final state $|\psi(t')\rangle$ at time t' can be expressed as

$$|\psi(t')\rangle = U(t',t)|\psi(t)\rangle|\psi(t)\rangle, \tag{2.10}$$

where $U(t',t)$ is the unitary time evolution operator. Infinitesimal time evolution is governed by the *Schrödinger equation*

$$\frac{d}{dt}|\psi(t)\rangle = -i\boldsymbol{H}(t)|\psi(t)\rangle, \tag{2.11}$$

where $\boldsymbol{H}(t)$ is a self-adjoint operator, called the *Hamiltonian* of the system. (The Hamiltonian has the dimensions of energy; we have chosen units in which Planck's constant $\hbar = h/2\pi = 1$, so that energy has the dimensions of inverse time.) To first order in the infinitesimal quantity dt, the Schrödinger equation can be expressed as

$$|\psi(t+dt)\rangle = (\boldsymbol{I} - i\boldsymbol{H}(t)dt)|\psi(t)\rangle. \tag{2.12}$$

Thus the operator $\boldsymbol{U}(t+dt,t) \equiv \boldsymbol{I} - i\boldsymbol{H}(t)dt$ is unitary; because $\boldsymbol{H}$ is self-adjoint it satisfies $\boldsymbol{U}^\dagger\boldsymbol{U} = 1$ to linear order in dt. Since a product of unitary operators is unitary, time evolution governed by the Schrödinger equation over a finite interval is also unitary. In the case where $\boldsymbol{H}$ is time independent we may write $\boldsymbol{U}(t',t) = e^{-i(t'-t)\boldsymbol{H}}$.

Our final axiom relates the description of a composite quantum system AB to the description of its component parts A and B.

Axiom 5. Composite Systems. If the Hilbert space of system A is $\mathcal{H}_A$ and the Hilbert space of system B is $\mathcal{H}_B$, then the Hilbert space of the composite systems AB is the *tensor product* $\mathcal{H}_A \otimes \mathcal{H}_B$. If system A is prepared in the state $|\psi\rangle_A$ and system B is prepared in the state $|\varphi\rangle_B$, then the composite system's state is the product $|\psi\rangle_A \otimes |\varphi\rangle_B$.

What is a tensor product of Hilbert spaces? If $\{|i\rangle_A\}$ denotes an orthonormal basis for $\mathcal{H}_A$ and $\{|\mu\rangle_B\}$ a basis for $\mathcal{H}_B$, then the states $|i,\mu\rangle_{AB} \equiv |i\rangle_A \otimes |\mu\rangle_B$ are a basis for $\mathcal{H}_A \otimes \mathcal{H}_B$, where the inner product on $\mathcal{H}_A \otimes \mathcal{H}_B$ is defined by

$$ {}_{AB}\langle i,\mu|j,\nu\rangle_{AB} = \delta_{ij}\delta_{\mu\nu}. \tag{2.13}$$

The tensor product operator $\boldsymbol{M}_A \otimes \boldsymbol{N}_B$ is the operator that applies $\boldsymbol{M}_A$ to system A and $\boldsymbol{N}_B$ to system B. Its action on the orthonormal basis $|i,\mu\rangle_{AB}$ is

$$\boldsymbol{M}_A \otimes \boldsymbol{N}_B |i,\mu\rangle_{AB} = \boldsymbol{M}_A|i\rangle_A \otimes \boldsymbol{N}_B|\mu\rangle_B = \sum_{j,\nu} |j,\nu\rangle_{AB} \, (M_A)_{ji} \, (N_B)_{\nu\mu} \, . \tag{2.14}$$

An operator that acts trivially on system B can be denoted $\boldsymbol{M}_A \otimes \boldsymbol{I}_B$, where $\boldsymbol{I}_B$ is the identity on $\mathcal{H}_B$, and an operator that acts trivially on system A can be denoted $\boldsymbol{I}_A \otimes \boldsymbol{N}_B$.

These five axioms provide a complete mathematical formulation of quantum mechanics. We immediately notice some curious features. One oddity is that the Schrödinger equation is linear, while we are accustomed to nonlinear dynamical equations in classical physics. This property seems to beg for an explanation. But far more curious is a mysterious dualism; there are two quite distinct ways for a quantum state to change. On the one hand there is unitary evolution, which is deterministic. If we specify the initial state $|\psi(0)\rangle$, the theory predicts the state $|\psi(t)\rangle$ at a later time.

But on the other hand there is measurement, which is probabilistic. The theory does not make definite predictions about the measurement outcomes; it only assigns probabilities to the various alternatives. This is troubling, because it is unclear why the measurement process should be governed by different physical laws than other processes.

The fundamental distinction between evolution and measurement, and in particular the intrinsic randomness of the measurement process, is sometimes called the *measurement problem* of quantum theory. Seeking a more pleasing axiomatic formulation of quantum theory is a worthy task which may eventually succeed. But these five axioms correctly account for all that we currently know about quantum physics, and provide the foundation for all that follows in this book.

2.2 The Qubit

The indivisible unit of classical information is the *bit*, which takes one of the two possible values $\{0, 1\}$. The corresponding unit of quantum information is called the "quantum bit" or *qubit*. It describes a state in the simplest possible quantum system.

The smallest nontrivial Hilbert space is two-dimensional. We may denote an orthonormal basis for a two-dimensional vector space as $\{|0\rangle, |1\rangle\}$. Then the most general normalized state can be expressed as

$$a|0\rangle + b|1\rangle, \tag{2.15}$$

where a, b are complex numbers that satisfy $|a|^2 + |b|^2 = 1$, and the overall phase is physically irrelevant. A *qubit* is a quantum system described by a two-dimensional Hilbert space, whose state can take any value of the form eq.(2.15).

We can perform a measurement that projects the qubit onto the basis $\{|0\rangle, |1\rangle\}$. Then we will obtain the outcome $|0\rangle$ with probability $|a|^2$, and the outcome $|1\rangle$ with probability $|b|^2$. Furthermore, except in the cases $a = 0$ and $b = 0$, the measurement irrevocably disturbs the state. If the value of the qubit is initially unknown, then there is no way to determine a and b with that single measurement, or any other conceivable measurement. However, *after* the measurement, the qubit has been prepared in a *known* state – either $|0\rangle$ or $|1\rangle$ – that differs (in general) from its previous state.

In this respect, a qubit differs from a classical bit; we can measure a classical bit without disturbing it, and we can decipher all of the information that it encodes. But suppose we have a classical bit that really does have a definite value (either 0 or 1), but where that value is initially unknown to us. Based on the information available to us we can only say that there is a *probability* p_0 that the bit has the value 0, and a probability p_1 that the bit has the value 1, where $p_0 + p_1 = 1$. When we measure the bit, we acquire additional information; afterwards we know the value with 100% confidence.

An important question is: what is the essential difference between a qubit and a *probabilistic* classical bit? In fact they are *not* the same, for several reasons that we will explore. To summarize the difference in brief: there is only one way to look at a bit, but there is more than one way to look at a qubit.

2.2.1 Spin-$\frac{1}{2}$

First of all, the coefficients a and b in eq.(2.15) encode more than just the probabilities of the outcomes of a measurement in the $\{|0\rangle, |1\rangle\}$ basis. In particular, the *relative phase* of a and b also has physical significance.

The properties of a qubit are easier to grasp if we appeal to a geometrical interpretation of its state. For a physicist, it is natural to interpret eq.(2.15) as the spin state of an object with spin-$\frac{1}{2}$ (like an electron). Then $|0\rangle$ and $|1\rangle$ are the spin up ($|\uparrow\rangle$) and spin down ($|\downarrow\rangle$) states along

a particular axis such as the z-axis. The two real numbers characterizing the qubit (the complex numbers a and b, modulo the normalization and overall phase) describe the *orientation* of the spin in three-dimensional space (the polar angle θ and the azimuthal angle φ).

We will not go deeply here into the theory of symmetry in quantum mechanics, but we will briefly recall some elements of the theory that will prove useful to us. A *symmetry* is a transformation that acts on a state of a system, yet leaves all observable properties of the system unchanged. In quantum mechanics, observations are measurements of self-adjoint operators. If $\boldsymbol{A}$ is measured in the state $|\psi\rangle$, then the outcome $|a\rangle$ (an eigenvector of $\boldsymbol{A}$) occurs with probability $|\langle a|\psi\rangle|^2$. A symmetry should leave these probabilities unchanged, when we "rotate" both the system *and* the apparatus.

A symmetry, then, is a mapping of vectors in Hilbert space

$$|\psi\rangle \mapsto |\psi'\rangle, \tag{2.16}$$

that preserves the absolute values of inner products

$$|\langle\varphi|\psi\rangle| = |\langle\varphi'|\psi'\rangle|, \tag{2.17}$$

for all $|\varphi\rangle$ and $|\psi\rangle$. According to a famous theorem due to Wigner, a mapping with this property can always be chosen (by adopting suitable phase conventions) to be either unitary or antiunitary. The antiunitary alternative, while important for discrete symmetries, can be excluded for continuous symmetries. Then the symmetry acts as

$$|\psi\rangle \mapsto |\psi'\rangle = \boldsymbol{U}|\psi\rangle, \tag{2.18}$$

where $\boldsymbol{U}$ is unitary (and in particular, *linear*).

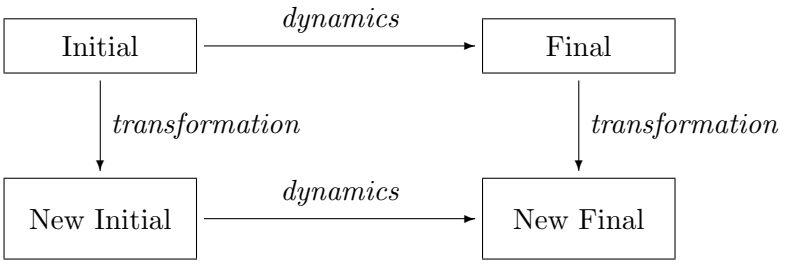
Symmetries form a *group*: a symmetry transformation can be inverted, and the product of two symmetries is a symmetry. For each symmetry operation R acting on our physical system, there is a corresponding unitary transformation $\boldsymbol{U}(R)$. Multiplication of these unitary operators must respect the group multiplication law of the symmetries – applying $R_1 \circ R_2$ should be equivalent to first applying R_2 and subsequently R_1. Thus we demand

$$\boldsymbol{U}(R_1)\boldsymbol{U}(R_2) = \text{ Phase}(R_1, R_2) \cdot \boldsymbol{U}(R_1 \circ R_2) \tag{2.19}$$

A phase depending on R_1 and R_2 is permitted in eq.(2.19) because quantum states are *rays*; we need only demand that $\boldsymbol{U}(R_1 \circ R_2)$ act the same way as $\boldsymbol{U}(R_1)\boldsymbol{U}(R_2)$ on rays, not on vectors. We say that $\boldsymbol{U}(R)$ provides a unitary representation, up to a phase, of the symmetry group.

So far, our concept of symmetry has no connection with dynamics. Usually, we demand of a symmetry that it respect the dynamical evolution of the system. This means that it should not matter whether we

first transform the system and then evolve it, or first evolve it and then transform it. In other words, the diagram



is commutative, and therefore the time evolution operator $e^{it\boldsymbol{H}}$ commutes with the symmetry transformation $\boldsymbol{U}(R)$:

$$\boldsymbol{U}(R)e^{-it\boldsymbol{H}} = e^{-it\boldsymbol{H}}\boldsymbol{U}(R) \ ; \tag{2.20}$$

expanding to linear order in t we obtain

$$\boldsymbol{U}(R)\boldsymbol{H} = \boldsymbol{H}\boldsymbol{U}(R). \tag{2.21}$$

For a continuous symmetry, we can choose R infinitesimally close to the identity, $R = I + \epsilon T$, and then $\boldsymbol{U}$ is close to $\boldsymbol{I}$:

$$\boldsymbol{U} = \boldsymbol{I} - i\varepsilon\boldsymbol{Q} + O(\varepsilon^2), \tag{2.22}$$

where $\boldsymbol{Q}$ is an operator determined by T. From the unitarity of $\boldsymbol{U}$ (to order ε) it follows that $\boldsymbol{Q}$ is an observable, $\boldsymbol{Q} = \boldsymbol{Q}^\dagger$. Expanding eq.(2.21) to linear order in ε we find

$$[\boldsymbol{Q}, \boldsymbol{H}] = 0 \ ; \tag{2.23}$$

the observable $\boldsymbol{Q}$ commutes with the Hamiltonian.

Eq.(2.23) is a *conservation law*. It says, for example, that if we prepare an eigenstate of $\boldsymbol{Q}$, then time evolution governed by the Schrödinger equation will preserve the eigenstate. Thus we see that symmetries imply conservation laws. Conversely, given a conserved quantity $\boldsymbol{Q}$ satisfying eq.(2.23) we can construct the corresponding symmetry transformations. Finite transformations can be built as a product of many infinitesimal ones:

$$R = (1 + \frac{\theta}{N}T)^N \Rightarrow \boldsymbol{U}(R) = (\boldsymbol{I} + i\frac{\theta}{N}\boldsymbol{Q})^N \rightarrow e^{i\theta\boldsymbol{Q}}, \tag{2.24}$$

taking the limit $N \rightarrow \infty$. Once we have decided how infinitesimal symmetry transformations are represented by unitary operators, then it is also

determined how finite transformations are represented, for these can be built as a product of infinitesimal transformations. We say that $\boldsymbol{Q}$ is the *generator* of the symmetry.

Let us briefly recall how this general theory applies to spatial rotations and angular momentum. An infinitesimal rotation by $d\theta$ (in the counterclockwise sense) about the axis specified by the unit vector $\hat{n} = (n_1, n_2, n_3)$ can be expressed as

$$R(\hat{n}, d\theta) = I - id\theta\hat{n} \cdot \vec{J}, \tag{2.25}$$

where (J_1, J_2, J_3) are the components of the angular momentum. A finite rotation is expressed as

$$R(\hat{n}, \theta) = \exp(-i\theta\hat{n} \cdot \vec{J}). \tag{2.26}$$

Rotations about distinct axes don't commute. From elementary properties of rotations, we find the commutation relations

$$[J_k, J_\ell] = i\varepsilon_{k\ell m} J_m, \tag{2.27}$$

where $\varepsilon_{k\ell m}$ is the totally antisymmetric tensor with $\varepsilon_{123} = 1$, and repeated indices are summed. To implement rotations on a quantum system, we find self-adjoint operators $\boldsymbol{J}_1, \boldsymbol{J}_2, \boldsymbol{J}_3$ in Hilbert space that satisfy these relations.

The "defining" representation of the rotation group is three dimensional, but the simplest nontrivial irreducible representation is two dimensional, given by

$$\boldsymbol{J}_k = \frac{1}{2}\boldsymbol{\sigma}_k, \tag{2.28}$$

where

$$\boldsymbol{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.29}$$

are the Pauli matrices. This is the unique two-dimensional irreducible representation, up to a unitary change of basis. Since the eigenvalues of $\boldsymbol{J}_k$ are $\pm\frac{1}{2}$, we call this the spin-$\frac{1}{2}$ representation. (By identifying $\boldsymbol{J}$ as the angular-momentum, we have implicitly chosen units with $\hbar = 1$.)

The Pauli matrices also have the properties of being mutually anticommuting and squaring to the identity,

$$\boldsymbol{\sigma}_k\boldsymbol{\sigma}_\ell + \boldsymbol{\sigma}_\ell\boldsymbol{\sigma}_k = 2\delta_{k\ell}\boldsymbol{I}\ ; \tag{2.30}$$

therefore $(\hat{n} \cdot \vec{\boldsymbol{\sigma}})^2 = n_k n_\ell \boldsymbol{\sigma}_k\boldsymbol{\sigma}_\ell = n_k n_k \boldsymbol{I} = \boldsymbol{I}$ (where repeated indices are summed). By expanding the exponential series, we see that finite rotations are represented as

$$\boldsymbol{U}(\hat{n}, \theta) = e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\boldsymbol{\sigma}}} = \boldsymbol{I}\cos\frac{\theta}{2} - i\hat{n} \cdot \vec{\boldsymbol{\sigma}}\sin\frac{\theta}{2}. \tag{2.31}$$

The most general 2×2 unitary matrix with determinant 1 can be expressed in this form. Thus, we are entitled to think of a qubit as a spin-$\frac{1}{2}$ object, and an arbitrary unitary transformation acting on the qubit's state (aside from a possible physically irrelevant rotation of the overall phase) is a *rotation* of the spin.

A peculiar property of the representation $\boldsymbol{U}(\hat{n},\theta)$ is that it is *double-valued*. In particular a rotation by 2π about any axis is represented non-trivially:

$$\boldsymbol{U}(\hat{n},\theta=2\pi)=-\boldsymbol{I}. \tag{2.32}$$

Our representation of the rotation group is really a representation "up to a sign"

$$\boldsymbol{U}(R_1)\boldsymbol{U}(R_2)=\pm\boldsymbol{U}(R_1\circ R_2). \tag{2.33}$$

But as already noted, this is acceptable, because the group multiplication is respected on *rays*, though not on vectors. These double-valued representations of the rotation group are called *spinor* representations. (The existence of spinors follows from a topological property of the group — that it is not simply connected.)

While it is true that a rotation by 2π has no detectable effect on a spin-$\frac{1}{2}$ object, it would be wrong to conclude that the spinor property has no observable consequences. Suppose I have a machine that acts on a pair of spins. If the first spin is up, it does nothing, but if the first spin is down, it rotates the second spin by 2π. Now let the machine act when the first spin is in a *superposition* of up and down. Then

$$\frac{1}{\sqrt{2}}\left(|\uparrow\rangle_1+|\downarrow\rangle_1\right)|\uparrow\rangle_2\mapsto\frac{1}{\sqrt{2}}\left(|\uparrow\rangle_1-|\downarrow\rangle_1\right)|\uparrow\rangle_2\ . \tag{2.34}$$

While there is no detectable effect on the second spin, the state of the first has flipped to an orthogonal state, which is very much observable.

In a rotated frame of reference, a rotation $R(\hat{n},\theta)$ becomes a rotation through the same angle but about a rotated axis. It follows that the three components of angular momentum transform under rotations as a vector:

$$\boldsymbol{U}(R)\boldsymbol{J}_k\boldsymbol{U}(R)^\dagger=R_{k\ell}\boldsymbol{J}_\ell. \tag{2.35}$$

Thus, if a state $|m\rangle$ is an eigenstate of $\boldsymbol{J}_3$

$$\boldsymbol{J}_3|m\rangle=m|m\rangle, \tag{2.36}$$

then $\boldsymbol{U}(R)|m\rangle$ is an eigenstate of $R\boldsymbol{J}_3$ with the same eigenvalue:

$$\begin{aligned} R\boldsymbol{J}_3\left(\boldsymbol{U}(R)|m\rangle\right) &= \boldsymbol{U}(R)\boldsymbol{J}_3\mathbf{U}(R)^\dagger\boldsymbol{U}(R)|m\rangle \\ &= \boldsymbol{U}(R)\boldsymbol{J}_3|m\rangle=m\left(\boldsymbol{U}(R)|m\rangle\right). \end{aligned} \tag{2.37}$$

Therefore, we can construct eigenstates of angular momentum along the axis $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ by applying a counterclockwise rotation through θ, about the axis $\hat{n}' = (-\sin\varphi, \cos\varphi, 0)$, to a $\boldsymbol{J}_3$ eigenstate. For our spin-$\frac{1}{2}$ representation, this rotation is

$$\begin{aligned} \exp\left(-i\frac{\theta}{2}\hat{n}'\cdot\vec{\boldsymbol{\sigma}}\right) &= \exp\left[\frac{\theta}{2}\begin{pmatrix} 0 & -e^{-i\varphi} \\ e^{i\varphi} & 0 \end{pmatrix}\right] \\ &= \begin{pmatrix} \cos\frac{\theta}{2} & -e^{-i\varphi}\sin\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \end{aligned} \tag{2.38}$$

and applying it to $\binom{1}{0}$, the $\boldsymbol{J}_3$ eigenstate with eigenvalue 1, we obtain

$$|\psi(\theta,\varphi)\rangle = \begin{pmatrix} e^{-i\varphi/2}\cos\frac{\theta}{2} \\ e^{i\varphi/2}\sin\frac{\theta}{2} \end{pmatrix}, \tag{2.39}$$

(up to an overall phase). We can check directly that this is an eigenstate of

$$\hat{n}\cdot\vec{\boldsymbol{\sigma}} = \begin{pmatrix} \cos\theta & e^{-i\varphi}\sin\theta \\ e^{i\varphi}\sin\theta & -\cos\theta \end{pmatrix}, \tag{2.40}$$

with eigenvalue one. We now see that eq.(2.15) with $a = e^{-i\varphi/2}\cos\frac{\theta}{2}$, $b = e^{i\varphi/2}\sin\frac{\theta}{2}$, can be interpreted as a spin pointing in the (θ,φ) direction.

We noted that we cannot determine a and b with a single measurement. Furthermore, even with many identical copies of the state, we cannot completely determine the state by measuring each copy only along the z-axis. This would enable us to estimate $|a|$ and $|b|$, but we would learn nothing about the relative phase of a and b. Equivalently, we would find the component of the spin along the z-axis

$$\langle\psi(\theta,\varphi)|\sigma_3|\psi(\theta,\varphi)\rangle = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta, \tag{2.41}$$

but we would not learn about the component in the x-y plane. The problem of determining $|\psi\rangle$ by measuring the spin is equivalent to determining the unit vector $\hat{n}$ by measuring its components along various axes. Altogether, measurements along three different axes are required. *E.g.*, from $\langle\sigma_3\rangle$ and $\langle\sigma_1\rangle$ we can determine n_3 and n_1, but the sign of n_2 remains undetermined. Measuring $\langle\sigma_2\rangle$ would remove this remaining ambiguity.

If we are permitted to rotate the spin, then only measurements along the z-axis will suffice. That is, measuring a spin along the $\hat{n}$ axis is equivalent to first applying a rotation that rotates the $\hat{n}$ axis to the axis $\hat{z}$, and then measuring along $\hat{z}$.

In the special case $\theta = \frac{\pi}{2}$ and $\varphi = 0$ (the $\hat{x}$-axis) our spin state is

$$|\uparrow_x\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle + |\downarrow_z\rangle\right) \tag{2.42}$$

("spin-up along the x-axis"). The orthogonal state ("spin down along the x-axis") is

$$|\downarrow_x\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle - |\downarrow_z\rangle\right). \tag{2.43}$$

For either of these states, if we measure the spin along the z-axis, we will obtain $|\uparrow_z\rangle$ with probability $\frac{1}{2}$ and $|\downarrow_z\rangle$ with probability $\frac{1}{2}$.

Now consider the combination

$$\frac{1}{\sqrt{2}}\left(|\uparrow_x\rangle + |\downarrow_x\rangle\right). \tag{2.44}$$

This state has the property that, if we measure the spin along the x-axis, we obtain $|\uparrow_x\rangle$ or $|\downarrow_x\rangle$, each with probability $\frac{1}{2}$. Now we may ask, what if we measure the state in eq.(2.44) along the z-axis?

If these were probabilistic classical bits, the answer would be obvious. The state in eq.(2.44) is in one of two states, and for *each* of the two, the probability is $\frac{1}{2}$ for pointing up or down along the z-axis. So of course we should find up with probability $\frac{1}{2}$ when we measure the state $\frac{1}{\sqrt{2}}\left(|\uparrow_x\rangle + |\downarrow_x\rangle\right)$ along the z-axis.

But not so for qubits! By adding eq.(2.42) and eq.(2.43), we see that the state in eq.(2.44) is really $|\uparrow_z\rangle$ in disguise. When we measure along the z-axis, we always find $|\uparrow_z\rangle$, never $|\downarrow_z\rangle$.

We see that for qubits, as opposed to probabilistic classical bits, probabilities can add in unexpected ways. This is, in its simplest guise, the phenomenon called "quantum interference," an important feature of quantum information.

To summarize the geometrical interpretation of a qubit: we may think of a qubit as a spin-$\frac{1}{2}$ object, and its quantum state is characterized by a unit vector $\hat{n}$ in three dimensions, the spin's direction. A unitary transformation rotates the spin, and a measurement of an observable has two possible outcomes: the spin is either up or down along a specified axis.

It should be emphasized that, while this *formal* equivalence with a spin-$\frac{1}{2}$ object applies to any two-level quantum system, not every two-level system transforms as a spinor under spatial rotations!

2.2.2 Photon polarizations

Another important two-state system is provided by a *photon*, which can have two independent polarizations. These photon polarization states also transform under rotations, but photons differ from our spin-$\frac{1}{2}$ objects in two important ways: (1) Photons are massless. (2) Photons have spin-1 (they are not spinors).

We will not present here a detailed discussion of the unitary representations of the Poincare group. Suffice it to say that the *spin* of a particle classifies how it transforms under the *little group*, the subgroup of the Lorentz group that preserves the particle's momentum. For a massive particle, we may always boost to the particle's rest frame, and then the little group is the rotation group.

For massless particles, there is no rest frame. The finite-dimensional unitary representations of the little group turn out to be representations of the rotation group in *two* dimensions, the rotations about the axis determined by the momentum. For a photon, this corresponds to a familiar property of classical light — the waves are polarized transverse to the direction of propagation.

Under a rotation about the axis of propagation, the two linear polarization states ($|x\rangle$ and $|y\rangle$ for horizontal and vertical polarization) transform as

$$\begin{aligned} |x\rangle &\rightarrow \cos\theta|x\rangle + \sin\theta|y\rangle \\ |y\rangle &\rightarrow -\sin\theta|x\rangle + \cos\theta|y\rangle. \end{aligned} \tag{2.45}$$

This two-dimensional representation is actually reducible. The matrix

$$\begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{2.46}$$

has the eigenstates

$$|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \qquad |L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} i \\ 1 \end{pmatrix}, \tag{2.47}$$

with eigenvalues $e^{i\theta}$ and $e^{-i\theta}$, the states of right and left circular polarization. That is, these are the eigenstates of the rotation generator

$$\boldsymbol{J} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \boldsymbol{\sigma}_2, \tag{2.48}$$

with eigenvalues ± 1. Because the eigenvalues are ± 1 (*not* $\pm\frac{1}{2}$) we say that the photon has spin-1.

In this context, the quantum interference phenomenon can be described as follows. The polarization states

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}\left(|x\rangle + |y\rangle\right), \\ |-\rangle &= \frac{1}{\sqrt{2}}\left(-|x\rangle + |y\rangle\right), \end{aligned} \tag{2.49}$$

are mutually orthogonal and can be obtained by rotating the states $|x\rangle$ and $|y\rangle$ by 45°. Suppose that we have a polarization analyzer that allows only one of two orthogonal linear photon polarizations to pass through, absorbing the other. Then an x or y polarized photon has probability $\frac{1}{2}$ of getting through a 45° rotated polarizer, and a 45° polarized photon has probability $\frac{1}{2}$ of getting through an x or y analyzer. But an x photon *never* passes through a y analyzer.

Suppose that a photon beam is directed at an x analyzer, with a y analyzer placed further downstream. Then about half of the photons will pass through the first analyzer, but every one of these will be stopped by the second analyzer. But now suppose that we place a 45°-rotated analyzer between the x and y analyzers. Then about half of the photons pass through each analyzer, and about one in eight will manage to pass all three without being absorbed. Because of this *interference* effect, there is no consistent interpretation in which each photon carries one classical bit of polarization information. Qubits are different than probabilistic classical bits.

A device can be constructed that rotates the linear polarization of a photon, and so applies the transformation Eq. (2.45) to our qubit; it functions by "turning on" a Hamiltonian for which the circular polarization states $|L\rangle$ and $|R\rangle$ are nondegenerate energy eigenstates. This is not the most general possible unitary transformation. But if we also have a device that alters the relative phase of the two orthogonal linear polarization states

$$\begin{aligned} |x\rangle &\rightarrow e^{-i\varphi/2}|x\rangle, \\ |y\rangle &\rightarrow e^{i\varphi/2}|y\rangle \end{aligned} \tag{2.50}$$

(by turning on a Hamiltonian whose nondegenerate energy eigenstates are the linear polarization states), then the two devices can be employed together to apply an arbitrary 2×2 unitary transformation (of determinant 1) to the photon polarization state.

2.3 The density operator

2.3.1 The bipartite quantum system

Having understood everything about a single qubit, we are ready to address systems with two qubits. Stepping up from one qubit to two is a bigger leap than you might expect. Much that is weird and wonderful about quantum mechanics can be appreciated by considering the properties of the quantum states of two qubits.

The axioms of §2.1 provide a perfectly acceptable general formulation of the quantum theory. Yet under many circumstances, we find that the

axioms appear to be violated. The trouble is that our axioms are intended to characterize the quantum behavior of a *closed system* that does not interact with its surroundings. In practice, closed quantum systems do not exist; the observations we make are always limited to a small part of a much larger quantum system.

When we study *open systems*, that is, when we limit our attention to just part of a larger system, then (contrary to the axioms):

1. States are *not* rays.
2. Measurements are *not* orthogonal projections.
3. Evolution is *not* unitary.

To arrive at the laws obeyed by open quantum systems, we must recall our fifth axiom, which relates the description of a composite quantum system to the description of its component parts. As a first step toward understanding the quantum description of an open system, consider a two-qubit world in which we observe only one of the qubits. Qubit A is here in the room with us, and we are free to observe or manipulate it any way we please. But qubit B is locked in a vault where we can't get access to it. The full system AB obeys the axioms of §2.1. But we would like to find a compact way to characterize the observations that can be made on qubit A alone.

We'll use $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ to denote orthonormal bases for qubits A and B respectively. Consider a quantum state of the two-qubit world of the form

$$|\psi\rangle_{AB} = a|0\rangle_A \otimes |0\rangle_B + b|1\rangle_A \otimes |1\rangle_B. \tag{2.51}$$

In this state, qubits A and B are *correlated.* Suppose we measure qubit A by projecting onto the $\{|0\rangle_A, |1\rangle_A\}$ basis. Then with probability $|a|^2$ we obtain the result $|0\rangle_A$, and the measurement prepares the state

$$|0\rangle_A \otimes |0\rangle_B \ ; \tag{2.52}$$

with probability $|b|^2$, we obtain the result $|1\rangle_A$ and prepare the state

$$|1\rangle_A \otimes |1\rangle_B. \tag{2.53}$$

In either case, a definite state of qubit B is picked out by the measurement. If we subsequently measure qubit B, then we are guaranteed (with probability one) to find $|0\rangle_B$ if we had found $|0\rangle_A$, and we are guaranteed to find $|1\rangle_B$ if we had found $|1\rangle_A$. In this sense, the outcomes of the $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ measurements are perfectly correlated in the state $|\psi\rangle_{AB}$.

But now we would like to consider more general observables acting on qubit A, and we would like to characterize the measurement outcomes for A alone (irrespective of the outcomes of any measurements of the inaccessible qubit B). An observable acting on qubit A only can be expressed as

$$\boldsymbol{M}_A \otimes \boldsymbol{I}_B, \tag{2.54}$$

where $\boldsymbol{M}_A$ is a self-adjoint operator acting on A, and $\boldsymbol{I}_B$ is the identity operator acting on B. The expectation value of the observable in the state $|\psi\rangle$ is:

$$\begin{aligned} \langle \boldsymbol{M}_A \rangle &= \langle \psi | \boldsymbol{M}_A \otimes \boldsymbol{I}_B | \psi \rangle \\ &= \left(a^* \langle 00| + b^* \langle 11| \right) \left(\boldsymbol{M}_A \otimes \boldsymbol{I}_B \right) \left(a|00\rangle + b|11\rangle \right) \\ &= |a|^2 \langle 0 | \boldsymbol{M}_A | 0 \rangle + |b|^2 \langle 1 | \mathbf{M}_A | 1 \rangle \end{aligned} \tag{2.55}$$

(where we have used the orthogonality of $|0\rangle_B$ and $|1\rangle_B$). This expression can be rewritten in the form

$$\langle \boldsymbol{M}_A \rangle = \mathrm{tr} \left(\boldsymbol{M}_{\mathrm{A}} \boldsymbol{\rho}_{\mathrm{A}} \right), \quad \boldsymbol{\rho}_{\mathrm{A}} = |a|^2 \ |0\rangle\langle 0| + |b|^2 \ |1\rangle\langle 1| \tag{2.56}$$

and $\mathrm{tr}(\cdot)$ denotes the *trace*. The operator $\boldsymbol{\rho}_A$ is called the *density operator* (or *density matrix*) for qubit A. It is self-adjoint, positive (its eigenvalues are nonnegative) and it has unit trace (because $|\psi\rangle$ is a normalized state.)

Because $\langle \boldsymbol{M}_A \rangle$ has the form eq.(2.56) for *any* observable $\boldsymbol{M}_A$ acting on qubit A, it is consistent to interpret $\boldsymbol{\rho}_A$ as representing an *ensemble* of possible quantum states, each occurring with a specified probability. That is, we would obtain precisely the same result for $\langle \boldsymbol{M}_A \rangle$ if we stipulated that qubit A is in one of two quantum states. With probability $p_0 = |a|^2$ it is in the quantum state $|0\rangle$, and with probability $p_1 = |b|^2$ it is in the state $|1\rangle$. If we are interested in the result of any possible measurement, we can consider $\boldsymbol{M}_A$ to be the projection $\boldsymbol{E}_A(a)$ onto the relevant eigenspace of a particular observable. Then

$$\mathrm{Prob}(a) = p_0 \langle 0 | \boldsymbol{E}_A(a) | 0 \rangle + p_1 \langle 1 | \boldsymbol{E}_A(a) | 1 \rangle, \tag{2.57}$$

which is the probability of outcome a summed over the ensemble, and weighted by the probability of each state in the ensemble.

We have emphasized previously that there is an essential difference between a coherent superposition of the states $|0\rangle$ and $|1\rangle$, and a probabilistic ensemble, in which $|0\rangle$ and $|1\rangle$ can each occur with specified probabilities. For example, for a spin-$\frac{1}{2}$ object we have seen that if we measure $\boldsymbol{\sigma}_1$ in the state $\frac{1}{\sqrt{2}} \left(|\uparrow_z\rangle + |\downarrow_z\rangle \right)$, we will obtain the result $|\uparrow_x\rangle$ with probability one. But the ensemble in which $|\uparrow_z\rangle$ and $|\downarrow_z\rangle$ each occur with probability $\frac{1}{2}$ is represented by the density operator

$$\boldsymbol{\rho} = \frac{1}{2} \left(|\uparrow_z\rangle\langle\uparrow_z| + |\downarrow_z\rangle\langle\downarrow_z| \right) = \frac{1}{2} \boldsymbol{I}, \tag{2.58}$$

and the projection onto $|\uparrow_x\rangle$ then has the expectation value

$$\mathrm{tr}\,(|\uparrow_x\rangle\langle\uparrow_x|\boldsymbol{\rho}) = \langle\uparrow_x|\boldsymbol{\rho}|\uparrow_x\rangle = \frac{1}{2}. \tag{2.59}$$

Similarly, if we measure the spin along any axis labeled by polar angles θ and φ, the probability of obtaining the result "spin up" is

$$\begin{aligned}\langle|\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|\rangle &= \mathrm{tr}\,(|\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|\boldsymbol{\rho}) \\ &= \langle\psi(\theta,\varphi)|\frac{1}{2}\boldsymbol{I}|\psi(\theta,\varphi)\rangle = \frac{1}{2}.\end{aligned} \tag{2.60}$$

Therefore, if in the two-qubit world an equally weighted coherent superposition of $|00\rangle$ and $|11\rangle$ is prepared, the state of qubit A behaves *incoherently* – along any axis it is an equiprobable mixture of spin up and spin down.

This discussion of the correlated two-qubit state $|\psi\rangle_{AB}$ is easily generalized to an arbitrary state of any bipartite quantum system (a system divided into two parts). The Hilbert space of a bipartite system is $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_{A,B}$ are the Hilbert spaces of the two parts. This means that if $\{|i\rangle_A\}$ is an orthonormal basis for $\mathcal{H}_A$ and $\{|\mu\rangle_B\}$ is an orthonormal basis for $\mathcal{H}_B$, then $\{|i\rangle_A \otimes |\mu\rangle_B\}$ is an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$. Thus an arbitrary pure state of $\mathcal{H}_A \otimes \mathcal{H}_B$ can be expanded as

$$|\psi\rangle_{AB} = \sum_{i,\mu} a_{i\mu}|i\rangle_A \otimes |\mu\rangle_B, \tag{2.61}$$

where $\sum_{i,\mu}|a_{i\mu}|^2 = 1$. The expectation value of an observable $\boldsymbol{M}_A \otimes \boldsymbol{I}_B$ that acts only on subsystem A is

$$\begin{aligned}\langle\boldsymbol{M}_A\rangle &= {}_{AB}\langle\psi|\boldsymbol{M}_A \otimes \boldsymbol{I}_B|\psi\rangle_{AB} \\ &= \sum_{j,\nu} a^*_{j\nu}\left({}_A\langle j| \otimes {}_B\langle\nu|\right)(\boldsymbol{M}_A \otimes \boldsymbol{I}_B)\sum_{i,\mu} a_{i\mu}\left(|i\rangle_A \otimes |\mu\rangle_B\right) \\ &= \sum_{i,j,\mu} a^*_{j\mu}a_{i\mu}\langle j|\boldsymbol{M}_A|i\rangle = \mathrm{tr}\left(\boldsymbol{M}_A\boldsymbol{\rho}_A\right),\end{aligned} \tag{2.62}$$

where

$$\boldsymbol{\rho}_A = \mathrm{tr}_B\left(|\psi\rangle\langle\psi|\right) \equiv \sum_{i,j,\mu} a_{i\mu}a^*_{j\mu}|i\rangle\langle j| \tag{2.63}$$

is the density operator of subsystem A.

We may say that the density operator $\boldsymbol{\rho}_A$ for subsystem A is obtained by performing a *partial trace* over subsystem B of the density operator (in this case a pure state) for the combined system AB. We may regard a

dual vector (or bra) ${}_B\langle\mu|$ as a linear map that takes vectors in $\mathcal{H}_A \otimes \mathcal{H}_B$ to vectors of $\mathcal{H}_A$, defined through its action on a basis:

$$ {}_B\langle\mu|i\nu\rangle_{AB} = \delta_{\mu\nu}|i\rangle_A \ ; \tag{2.64}$$

similarly, the ket $|\mu\rangle_B$ defines a map from the $\mathcal{H}_A \otimes \mathcal{H}_B$ dual basis to the $\mathcal{H}_A$ dual basis, via

$$ {}_{AB}\langle i\nu|\mu\rangle_B = \delta_{\mu\nu}\ {}_A\langle i|. \tag{2.65}$$

The partial trace operation is a linear map that takes an operator $\boldsymbol{M}_{AB}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ to an operator on $\mathcal{H}_A$ defined as

$$ \mathrm{tr}_B\ \boldsymbol{M}_{AB} = \sum_\mu {}_B\langle\mu|\boldsymbol{M}_{AB}|\mu\rangle_B. \tag{2.66}$$

We see that the density operator acting on A is the partial trace

$$ \boldsymbol{\rho}_A = \mathrm{tr}_B\left(|\psi\rangle\langle\psi|\right). \tag{2.67}$$

From the definition eq.(2.63), we can immediately infer that $\boldsymbol{\rho}_A$ has the following properties:

1. $\boldsymbol{\rho}_A$ is self-adjoint: $\boldsymbol{\rho}_A = \boldsymbol{\rho}_A^\dagger$.
2. $\boldsymbol{\rho}_A$ is positive: For any $|\varphi\rangle$, $\langle\varphi|\boldsymbol{\rho}_A|\varphi\rangle = \sum_\mu |\sum_i a_{i\mu}\langle\varphi|i\rangle|^2 \geq 0$.
3. $\mathrm{tr}(\boldsymbol{\rho}_A) = 1$: We have $\mathrm{tr}(\boldsymbol{\rho}_A) = \sum_{i,\mu} |a_{i\mu}|^2 = 1$, since $|\psi\rangle_{AB}$ is normalized.

It follows that $\boldsymbol{\rho}_A$ can be diagonalized in an orthonormal basis, that the eigenvalues are all real and nonnegative, and that the eigenvalues sum to one.

If we are looking at a subsystem of a larger quantum system, then, even if the state of the larger system is a ray, the state of the subsystem need not be; in general, the state is represented by a density operator. In the case where the state of the subsystem *is* a ray, and we say that the state is *pure*. Otherwise the state is *mixed*. If the state is a pure state $|\psi\rangle_A$, then the density matrix $\boldsymbol{\rho}_A = |\psi\rangle\langle\psi|$ is the *projection* onto the one-dimensional space spanned by $|\psi\rangle_A$. Hence a pure density matrix has the property $\boldsymbol{\rho}^2 = \boldsymbol{\rho}$. A general density matrix, expressed in the basis $\{|a\rangle\}$ in which it is diagonal, has the form

$$ \boldsymbol{\rho}_A = \sum_a p_a |a\rangle\langle a|, \tag{2.68}$$

where $0 < p_a \leq 1$ and $\sum_a p_a = 1$. If the state is not pure, there are two or more terms in this sum, and $\boldsymbol{\rho}^2 \neq \boldsymbol{\rho}$; in fact, $\mathrm{tr}\ \boldsymbol{\rho}^2 = \sum p_a^2 < \sum p_a = 1$.

We say that $\boldsymbol{\rho}$ is an *incoherent* mixture of the states $\{|a\rangle\}$; "incoherent" means that the relative phases of the $|a\rangle$'s are experimentally inaccessible.

Since the expectation value of *any* observable $\boldsymbol{M}$ acting on the subsystem can be expressed as

$$\langle \boldsymbol{M} \rangle = \text{tr } \boldsymbol{M}\boldsymbol{\rho} = \sum_a p_a \langle a|\boldsymbol{M}|a\rangle, \tag{2.69}$$

we see as before that we may interpret $\boldsymbol{\rho}$ as describing an *ensemble* of pure quantum states, in which the state $|a\rangle$ occurs with probability p_a. We have, therefore, come a long part of the way to understanding how probabilities arise in quantum mechanics when a quantum system A interacts with another system B. A and B become *entangled*, that is, correlated. The entanglement *destroys the coherence* of a superposition of states of A, so that some of the phases in the superposition become inaccessible if we look at A alone. We may describe this situation by saying that the state of system A *collapses* — it is in one of a set of alternative states, each of which can be assigned a probability.

2.3.2 Bloch sphere

Let's return to the case in which system A is a single qubit, and consider the form of the general density matrix. The most general self-adjoint 2×2 matrix has four real parameters, and can be expanded in the basis $\{\boldsymbol{I}, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2, \boldsymbol{\sigma}_3\}$. Since each $\boldsymbol{\sigma}_i$ is traceless, the coefficient of $\boldsymbol{I}$ in the expansion of a density matrix $\boldsymbol{\rho}$ must be $\frac{1}{2}$ (so that $\text{tr}(\boldsymbol{\rho}) = 1$), and $\boldsymbol{\rho}$ may be expressed as

$$\begin{aligned} \boldsymbol{\rho}(\vec{P}) &= \frac{1}{2}\left(\boldsymbol{I} + \vec{P}\cdot\vec{\boldsymbol{\sigma}}\right) \\ &\equiv \frac{1}{2}\left(\boldsymbol{I} + P_1\boldsymbol{\sigma}_1 + P_2\boldsymbol{\sigma}_2 + P_3\boldsymbol{\sigma}_3\right) \\ &= \frac{1}{2}\begin{pmatrix} 1+P_3 & P_1 - iP_2 \\ P_1 + iP_2 & 1 - P_3 \end{pmatrix}, \end{aligned} \tag{2.70}$$

where P_1, P_2, P_3 are real numbers. We can compute $\det\boldsymbol{\rho} = \frac{1}{4}\left(1 - \vec{P}^2\right)$. Therefore, a necessary condition for $\boldsymbol{\rho}$ to have nonnegative eigenvalues is $\det\boldsymbol{\rho} \geq 0$ or $\vec{P}^2 \leq 1$. This condition is also sufficient; since tr $\boldsymbol{\rho} = 1$, it is not possible for $\boldsymbol{\rho}$ to have two negative eigenvalues. Thus, there is a $1-1$ correspondence between the possible density matrices of a single qubit and the points on the *unit 3-ball* $0 \leq |\vec{P}| \leq 1$. This ball is usually called the *Bloch sphere* (although it is really a ball, not a sphere).

The boundary $\left(|\vec{P}| = 1\right)$ of the ball (which really *is* a sphere) contains the density matrices with vanishing determinant. Since tr $\boldsymbol{\rho} = 1$, these

density matrices must have the eigenvalues 0 and 1 — they are one-dimensional projectors, and hence pure states. We have already seen that any pure state of a single qubit is of the form $|\psi(\theta,\varphi)\rangle$ and can be envisioned as a spin pointing in the (θ,φ) direction. Indeed using the property

$$(\hat{n}\cdot\vec{\boldsymbol{\sigma}})^2 = \boldsymbol{I}, \tag{2.71}$$

where $\hat{n}$ is a unit vector, we can easily verify that the pure-state density matrix

$$\boldsymbol{\rho}(\hat{n}) = \frac{1}{2}\left(\boldsymbol{I} + \hat{n}\cdot\vec{\boldsymbol{\sigma}}\right) \tag{2.72}$$

satisfies the property

$$(\hat{n}\cdot\vec{\boldsymbol{\sigma}})\,\boldsymbol{\rho}(\hat{n}) = \boldsymbol{\rho}(\hat{n})\,(\hat{n}\cdot\vec{\boldsymbol{\sigma}}) = \boldsymbol{\rho}(\hat{n}), \tag{2.73}$$

and, therefore is the projector

$$\boldsymbol{\rho}(\hat{n}) = |\psi(\hat{n})\rangle\langle\psi(\hat{n})|\ ; \tag{2.74}$$

that is, $\hat{n}$ is the direction along which the spin is pointing up. Alternatively, from the expression

$$|\psi(\theta,\phi)\rangle = \begin{pmatrix} e^{-i\varphi/2}\cos(\theta/2) \\ e^{i\varphi/2}\sin(\theta/2) \end{pmatrix}, \tag{2.75}$$

we may compute directly that

$$\begin{aligned} \boldsymbol{\rho}(\theta,\phi) &= |\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)| \\ &= \begin{pmatrix} \cos^2(\theta/2) & \cos(\theta/2)\sin(\theta/2)e^{-i\varphi} \\ \cos(\theta/2)\sin(\theta/2)e^{i\varphi} & \sin^2(\theta/2) \end{pmatrix} \\ &= \frac{1}{2}\boldsymbol{I} + \frac{1}{2}\begin{pmatrix} \cos\theta & \sin\theta e^{-i\varphi} \\ \sin\theta e^{i\varphi} & -\cos\theta \end{pmatrix} = \frac{1}{2}(\boldsymbol{I} + \hat{n}\cdot\vec{\boldsymbol{\sigma}}) \end{aligned} \tag{2.76}$$

where $\hat{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. One nice property of the Bloch parametrization of the pure states is that while $|\psi(\theta,\varphi)\rangle$ has an arbitrary overall phase that has no physical significance, there is no phase ambiguity in the density matrix $\boldsymbol{\rho}(\theta,\varphi) = |\psi(\theta,\varphi)\rangle\langle\psi(\theta,\varphi)|$; all the parameters in $\boldsymbol{\rho}$ have a physical meaning.

From the property

$$\frac{1}{2}\mathrm{tr}\ \boldsymbol{\sigma}_i\boldsymbol{\sigma}_j = \delta_{ij} \tag{2.77}$$

we see that

$$\langle\hat{n}\cdot\vec{\boldsymbol{\sigma}}\rangle_{\vec{P}} = \mathrm{tr}\left(\hat{n}\cdot\vec{\boldsymbol{\sigma}}\boldsymbol{\rho}(\vec{P})\right) = \hat{n}\cdot\vec{P}\ . \tag{2.78}$$

We say that the vector $\vec{P}$ in Eq. (2.70) parametrizes the *polarization* of the spin. If there are many identically prepared systems at our disposal, we can determine $\vec{P}$ (and hence the complete density matrix $\boldsymbol{\rho}(\vec{P})$) by measuring $\langle\hat{n}\cdot\vec{\boldsymbol{\sigma}}\rangle$ along each of three linearly independent axes.

2.4 Schmidt decomposition

A bipartite pure state can be expressed in a standard form (*the Schmidt decomposition*) that is often very useful.

To arrive at this form, note that an arbitrary vector in $\mathcal{H}_A \otimes \mathcal{H}_B$ can be expanded as

$$|\psi\rangle_{AB} = \sum_{i,\mu} \psi_{i\mu} |i\rangle_A \otimes |\mu\rangle_B \equiv \sum_i |i\rangle_A \otimes |\tilde{i}\rangle_B. \tag{2.79}$$

Here $\{|i\rangle_A\}$ and $\{|\mu\rangle_B\}$ are orthonormal basis for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively, but to obtain the second equality in eq.(2.79) we have defined

$$|\tilde{i}\rangle_B \equiv \sum_\mu \psi_{i\mu} |\mu\rangle_B. \tag{2.80}$$

Note that the $|\tilde{i}\rangle_B$'s need *not* be mutually orthogonal or normalized.

Now let's suppose that the $\{|i\rangle_A\}$ basis is chosen to be the basis in which $\boldsymbol{\rho}_A$ is diagonal,

$$\boldsymbol{\rho}_A = \sum_i p_i |i\rangle\langle i|. \tag{2.81}$$

We can also compute $\boldsymbol{\rho}_A$ by performing a partial trace,

$$\begin{aligned} \boldsymbol{\rho}_A &= \mathrm{tr}_B(|\psi\rangle\langle\psi|) \\ &= \mathrm{tr}_B\Big(\sum_{i,j} |i\rangle\langle j| \otimes |\tilde{i}\rangle\langle\tilde{j}|\Big) = \sum_{i,j} \langle\tilde{j}|\tilde{i}\rangle \, (|i\rangle\langle j|) \ . \end{aligned} \tag{2.82}$$

We obtained the last equality in eq.(2.82) by noting that

$$\begin{aligned} \mathrm{tr}_B\left(|\tilde{i}\rangle\langle\tilde{j}|\right) &= \sum_k \langle k|\tilde{i}\rangle\langle\tilde{j}|k\rangle \\ &= \sum_k \ \langle\tilde{j}|k\rangle\langle k|\tilde{i}\rangle = \ \langle\tilde{j}|\tilde{i}\rangle, \end{aligned} \tag{2.83}$$

where $\{|k\rangle\}$ is a complete orthonormal basis for $\mathcal{H}_B$. By comparing eq.(2.81) and eq. (2.82), we see that

$${}_B\langle\tilde{j}|\tilde{i}\rangle_B = p_i \delta_{ij}. \tag{2.84}$$

Hence, it turns out that the $\{|\tilde{i}\rangle_B\}$ *are* orthogonal after all. We obtain orthonormal vectors by rescaling,

$$|i'\rangle_B = p_i^{-1/2} |\tilde{i}\rangle_B \tag{2.85}$$

(we may assume $p_i \neq 0$, because we will need eq.(2.85) only for i appearing in the sum eq.(2.81)), and therefore obtain the expansion

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\ |i\rangle_A \otimes |i'\rangle_B, \tag{2.86}$$

in terms of a *particular* orthonormal basis of $\mathcal{H}_A$ and $\mathcal{H}_B$.

Eq.(2.86) is the Schmidt decomposition of the bipartite pure state $|\psi\rangle_{AB}$. Any bipartite pure state can be expressed in this form, but the bases used depend on the pure state that is being expanded. In general, we can't simultaneously expand *both* $|\psi\rangle_{AB}$ and $|\varphi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ in the form eq.(2.86) using the *same* orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$.

It is instructive to compare the Schmidt decomposition of the bipartite pure state $|\psi\rangle_{AB}$ with its expansion in a generic orthonormal basis

$$|\psi\rangle_{AB} = \sum_{a,\mu} \psi_{a\mu} |a\rangle_A \otimes |\mu\rangle_B. \tag{2.87}$$

The orthonormal bases $\{|a\rangle_A\}$ and $\{|\mu\rangle_B\}$ are related to the Schmidt bases $\{|i\rangle_A\}$ and $\{|i'\rangle_B\}$ by unitary transformations $\boldsymbol{U}_A$ and $\boldsymbol{U}_B$, hence

$$|i\rangle_A = \sum_a |a\rangle_A \, (U_A)_{ai}\,, \quad |i'\rangle_B = \sum_\mu |\mu\rangle_B \, (U_B)_{\mu i'}\,. \tag{2.88}$$

By equating the expressions for $|\psi\rangle_{AB}$ in eq.(2.86) and eq.(2.87), we find

$$\psi_{a\mu} = \sum_i (U_A)_{ai}\ \sqrt{p_i}\ \left(U_B^T\right)_{i\mu}. \tag{2.89}$$

We see that by applying unitary transformations on the left and right, any matrix ψ can be transformed to a matrix which is diagonal and non-negative. (The "diagonal" matrix will be rectangular rather than square if the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ have different dimensions.) Eq.(2.89) is said to be the *singular value decomposition* of ψ, and the weights $\{\sqrt{p_i}\}$ in the Schmidt decomposition are ψ's singular values.

Using eq.(2.86), we can also evaluate the partial trace over $\mathcal{H}_A$ to obtain

$$\boldsymbol{\rho}_B = \mathrm{tr}_A \left(|\psi\rangle\langle\psi|\right) = \sum_i p_i |i'\rangle\langle i'|. \tag{2.90}$$

We see that $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ have the *same nonzero eigenvalues*. If $\mathcal{H}_A$ and $\mathcal{H}_B$ do not have the same dimension, the number of *zero* eigenvalues of $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ will differ.

If $\boldsymbol{\rho}_A$ (and hence $\boldsymbol{\rho}_B$) have no degenerate eigenvalues other than zero, then the Schmidt decomposition of $|\psi\rangle_{AB}$ is essentially uniquely determined by $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$. We can diagonalize $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ to find the $|i\rangle_A$'s

and $|i'\rangle_B$'s, and then we pair up the eigenstates of $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ with the same eigenvalue to obtain eq.(2.86). We have chosen the phases of our basis states so that no phases appear in the coefficients in the sum; the only remaining freedom is to redefine $|i\rangle_A$ and $|i'\rangle_B$ by multiplying by opposite phases (which leaves the expression eq.(2.86) unchanged).

But if $\boldsymbol{\rho}_A$ has degenerate nonzero eigenvalues, then we need more information than that provided by $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ to determine the Schmidt decomposition; we need to know which $|i'\rangle_B$ gets paired with each $|i\rangle_A$. For example, if both $\mathcal{H}_A$ and $\mathcal{H}_B$ are d-dimensional and U_{ij} is any $d \times d$ unitary matrix, then

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{i,j=1}^{d} |i\rangle_A U_{ij} \otimes |j'\rangle_B, \tag{2.91}$$

will yield $\boldsymbol{\rho}_A = \boldsymbol{\rho}_B = \frac{1}{d}\boldsymbol{I}$ when we take partial traces. Furthermore, we are free to apply simultaneous unitary transformations in $\mathcal{H}_A$ and $\mathcal{H}_B$; writing

$$|i\rangle_A = \sum_a |a\rangle_A U_{ai}, \quad |i'\rangle_B = \sum_b |b'\rangle_B U^*_{bi}, \tag{2.92}$$

we have

$$\begin{aligned} |\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |i\rangle_A \otimes |i'\rangle_B &= \frac{1}{\sqrt{d}} \sum_{i,j,a} |a\rangle_A U_{ai} \otimes |b'\rangle_B U^\dagger_{ib} \\ &= \frac{1}{\sqrt{d}} \sum_a |a\rangle_A \otimes |a'\rangle_B. \end{aligned} \tag{2.93}$$

This simultaneous rotation preserves the state $|\psi\rangle_{AB}$, illustrating that there is an ambiguity in the basis used when we express $|\psi\rangle_{AB}$ in the Schmidt form.

2.4.1 Entanglement

With any bipartite pure state $|\psi\rangle_{AB}$ we may associate a positive integer, the *Schmidt number*, which is the number of nonzero eigenvalues in $\boldsymbol{\rho}_A$ (or $\boldsymbol{\rho}_B$) and hence the number of terms in the Schmidt decomposition of $|\psi\rangle_{AB}$. In terms of this quantity, we can define what it means for a bipartite pure state to be *entangled*: $|\psi\rangle_{AB}$ is entangled (or nonseparable) if its Schmidt number is greater than one; otherwise, it is *separable* (or unentangled). Thus, a separable bipartite pure state is a direct product of pure states in $\mathcal{H}_A$ and $\mathcal{H}_B$,

$$|\psi\rangle_{AB} = |\varphi\rangle_A \otimes |\chi\rangle_B; \tag{2.94}$$

then the reduced density matrices $\boldsymbol{\rho}_A = |\varphi\rangle\langle\varphi|$ and $\boldsymbol{\rho}_B = |\chi\rangle\langle\chi|$ are pure. Any state that cannot be expressed as such a direct product is entangled; then $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ are mixed states.

When $|\psi\rangle_{AB}$ is entangled we say that A and B have *quantum correlations*. It is not strictly correct to say that subsystems A and B are *uncorrelated* if $|\psi\rangle_{AB}$ is separable; after all, the two spins in the separable state

$$|\uparrow\rangle_A|\uparrow\rangle_B, \tag{2.95}$$

are surely correlated – they are both pointing in the same direction. But the correlations between A and B in an entangled state have a different character than those in a separable state. One crucial difference is that *entanglement cannot be created locally.* The only way to entangle A and B is for the two subsystems to directly interact with one another.

We can prepare the state eq.(2.95) without allowing spins A and B to ever come into contact with one another. We need only send a (classical!) message to two preparers (Alice and Bob) telling both of them to prepare a spin pointing along the z-axis. But the only way to turn the state eq.(2.95) into an entangled state like

$$\frac{1}{\sqrt{2}}\left(|\uparrow\rangle_A|\uparrow\rangle_B + |\downarrow\rangle_A|\downarrow\rangle_B\right), \tag{2.96}$$

is to apply a *collective* unitary transformation to the state. Local unitary transformations of the form $U_A \otimes U_B$, and local measurements performed by Alice or Bob, *cannot increase the Schmidt number* of the two-qubit state, no matter how much Alice and Bob discuss what they do. To entangle two qubits, we *must* bring them together and allow them to interact.

As we will discuss in Chapter 4, it is also possible to make the distinction between entangled and separable bipartite *mixed* states. We will also discuss various ways in which local operations can modify the form of entanglement, and some ways that entanglement can be put to use.

2.5 Ambiguity of the ensemble interpretation

2.5.1 Convexity

Recall that an operator $\boldsymbol{\rho}$ acting on a Hilbert space $\mathcal{H}$ may be interpreted as a density operator if it has the three properties:

(1) $\boldsymbol{\rho}$ is self-adjoint.

(2) $\boldsymbol{\rho}$ is nonnegative.

(3) $\mathrm{tr}(\boldsymbol{\rho}) = 1$.

It follows immediately that, given two density matrices $\boldsymbol{\rho}_1$, and $\boldsymbol{\rho}_2$, we can always construct another density matrix as a convex linear combination of the two:

$$\boldsymbol{\rho}(\lambda) = \lambda\boldsymbol{\rho}_1 + (1-\lambda)\boldsymbol{\rho}_2 \tag{2.97}$$

is a density matrix for any real λ satisfying $0 \leq \lambda \leq 1$. We easily see that $\boldsymbol{\rho}(\lambda)$ satisfies (1) and (3) if $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ do. To check (2), we evaluate

$$\langle\psi|\boldsymbol{\rho}(\lambda)|\psi\rangle = \lambda\langle\psi|\boldsymbol{\rho}_1|\psi\rangle + (1-\lambda)\langle\psi|\boldsymbol{\rho}_2|\psi\rangle \geq 0; \tag{2.98}$$

$\langle\boldsymbol{\rho}(\lambda)\rangle$ is guaranteed to be nonnegative because $\langle\boldsymbol{\rho}_1\rangle$ and $\langle\boldsymbol{\rho}_2\rangle$ are. We have, therefore, shown that in a Hilbert space $\mathcal{H}$ of dimension d, the density operators are a *convex subset* of the real vector space of $d \times d$ hermitian operators. (A subset of a vector space is said to be convex if the set contains the straight line segment connecting any two points in the set.)

Most density operators can be expressed as a sum of other density operators in many different ways. But the pure states are special in this regard – it is *not* possible to express a pure state as a convex sum of two other states. Consider a pure state $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$, and let $|\psi_\perp\rangle$ denote a vector orthogonal to $|\psi\rangle$, $\langle\psi_\perp|\psi\rangle = 0$. Suppose that $\boldsymbol{\rho}$ can be expanded as in eq.(2.97); then

$$\begin{aligned}\langle\psi_\perp|\boldsymbol{\rho}|\psi_\perp\rangle = 0 = \lambda\langle\psi_\perp|\boldsymbol{\rho}_1|\psi_\perp\rangle \\ + (1-\lambda)\langle\psi_\perp|\boldsymbol{\rho}_2|\psi_\perp\rangle.\end{aligned} \tag{2.99}$$

Since the right hand side is a sum of two nonnegative terms, and the sum vanishes, both terms must vanish. If λ is not 0 or 1, we conclude that $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ are orthogonal to $|\psi_\perp\rangle$. But since $|\psi_\perp\rangle$ can be *any* vector orthogonal to $|\psi\rangle$, we see that $\boldsymbol{\rho}_1 = \boldsymbol{\rho}_2 = \boldsymbol{\rho}$.

The vectors in a convex set that cannot be expressed as a linear combination of other vectors in the set are called the *extremal points* of the set. We have just shown that the pure states are extremal points of the set of density matrices. Furthermore, *only* the pure states are extremal, because any mixed state can be written $\boldsymbol{\rho} = \sum_i p_i|i\rangle\langle i|$ in the basis in which it is diagonal, and so is a convex sum of pure states.

We have already encountered this structure in our discussion of the special case of the Bloch sphere. We saw that the density operators are a (unit) ball in the three-dimensional set of 2×2 hermitian matrices with unit trace. The ball is convex, and its extremal points are the points on the boundary. Similarly, the $d \times d$ density operators are a convex subset of the (d^2-1)-dimensional set of $d \times d$ hermitian matrices with unit trace, and the extremal points of the set are the pure states.

However, the 2×2 case is atypical in one respect: for $d > 2$, the points on the boundary of the set of density matrices are not necessarily pure

states. The boundary of the set consists of all density matrices with at least one vanishing eigenvalue (since there are nearby matrices with negative eigenvalues). Such a density matrix need not be pure, for $d > 2$, since the number of nonvanishing eigenvalues can exceed one.

2.5.2 Ensemble preparation

The convexity of the set of density matrices has a simple and enlightening physical interpretation. Suppose that a preparer agrees to prepare one of two possible states; with probability λ, the state $\boldsymbol{\rho}_1$ is prepared, and with probability $1-\lambda$, the state $\boldsymbol{\rho}_2$ is prepared. (A random number generator might be employed to guide this choice.) To evaluate the expectation value of any observable $\boldsymbol{M}$, we average over *both* the choices of preparation *and* the outcome of the quantum measurement:

$$\begin{aligned}\langle \boldsymbol{M} \rangle &= \lambda \langle \boldsymbol{M} \rangle_1 + (1-\lambda)\langle \boldsymbol{M} \rangle_2 \\ &= \lambda \mathrm{tr}(\boldsymbol{M}\boldsymbol{\rho}_1) + (1-\lambda)\mathrm{tr}(\boldsymbol{M}\boldsymbol{\rho}_2) \\ &= \mathrm{tr}\left(\boldsymbol{M}\boldsymbol{\rho}(\lambda)\right). \end{aligned} \tag{2.100}$$

All expectation values are thus indistinguishable from what we would obtain if the state $\boldsymbol{\rho}(\lambda)$ had been prepared instead. Thus, we have an operational procedure, given methods for preparing the states $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$, for preparing any convex combination.

Indeed, for any mixed state $\boldsymbol{\rho}$, there are an infinite variety of ways to express $\boldsymbol{\rho}$ as a convex combination of other states, and hence an infinite variety of procedures we could employ to prepare $\boldsymbol{\rho}$, all of which have exactly the same consequences for any conceivable observation of the system. But a pure state is different; it can be prepared in only one way. (This is what is "pure" about a pure state.) Every pure state is an eigenstate of some observable, e.g., for the state $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$, measurement of the projection $\boldsymbol{E} = |\psi\rangle\langle\psi|$ is guaranteed to have the outcome 1. (For example, recall that every pure state of a single qubit is "spin-up" along some axis.) Since $\boldsymbol{\rho}$ is the only state for which the outcome of measuring $\boldsymbol{E}$ is 1 with 100% probability, there is no way to reproduce this observable property by choosing one of several possible preparations. Thus, the preparation of a pure state is unambiguous (we can infer a unique preparation if we have many copies of the state to experiment with), but the preparation of a mixed state is always ambiguous.

How ambiguous is it? Since any $\boldsymbol{\rho}$ can be expressed as a sum of pure states, let's confine our attention to the question: in how many ways can a density operator be expressed as a convex sum of pure states? Mathematically, this is the question: in how many ways can $\boldsymbol{\rho}$ be written as a sum of *extremal* states?

As a first example, consider the "maximally mixed" state of a single qubit:

$$\boldsymbol{\rho} = \frac{1}{2}\boldsymbol{I}. \tag{2.101}$$

This can indeed be prepared as an ensemble of pure states in an infinite variety of ways. For example,

$$\boldsymbol{\rho} = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle\langle\downarrow_z|, \tag{2.102}$$

so we obtain $\boldsymbol{\rho}$ if we prepare either $|\uparrow_z\rangle$ or $|\downarrow_z\rangle$, each occurring with probability $\frac{1}{2}$. But we also have

$$\boldsymbol{\rho} = \frac{1}{2}|\uparrow_x\rangle\langle\uparrow_x| + \frac{1}{2}|\downarrow_x\rangle\langle\downarrow_x|, \tag{2.103}$$

so we obtain $\boldsymbol{\rho}$ if we prepare either $|\uparrow_x\rangle$ or $|\downarrow_x\rangle$, each occurring with probability $\frac{1}{2}$. Now the preparation procedures are undeniably *different*. Yet there is no possible way to tell the difference by making observations of the spin.

More generally, the point at the center of the Bloch ball is the sum of any two antipodal points on the sphere – preparing either $|\uparrow_{\hat{n}}\rangle$ or $|\downarrow_{\hat{n}}\rangle$, each occurring with probability $\frac{1}{2}$, will generate $\boldsymbol{\rho} = \frac{1}{2}\boldsymbol{I}$.

Only in the case where $\boldsymbol{\rho}$ has two (or more) degenerate eigenvalues will there be distinct ways of generating $\boldsymbol{\rho}$ from an ensemble of *mutually orthogonal* pure states, but there is no good reason to confine our attention to ensembles of mutually orthogonal pure states. We may consider a point in the interior of the Bloch ball

$$\boldsymbol{\rho}(\vec{P}) = \frac{1}{2}(\boldsymbol{I} + \vec{P}\cdot\vec{\sigma}), \tag{2.104}$$

with $0 < |\vec{P}| < 1$, and it too can be expressed as

$$\boldsymbol{\rho}(\vec{P}) = \lambda\boldsymbol{\rho}(\hat{n}_1) + (1-\lambda)\boldsymbol{\rho}(\hat{n}_2), \tag{2.105}$$

if $\vec{P} = \lambda\hat{n}_1 + (1-\lambda)\hat{n}_2$ (or in other words, if $\vec{P}$ lies somewhere on the line segment connecting the points $\hat{n}_1$ and $\hat{n}_2$ on the sphere). Evidently, for any $\vec{P}$, there is a an expression for $\rho(\vec{P})$ as a convex combination of pure states associated with any chord of the Bloch sphere that passes through the point $\vec{P}$; all such chords comprise a two-parameter family.

This highly ambiguous nature of the preparation of a mixed quantum state is one of the characteristic features of quantum information that contrasts sharply with classical probability distributions. Consider, for example, the case of a probability distribution for a single classical bit. The two extremal distributions are those in which either 0 or 1 occurs

with 100% probability. *Any* probability distribution for the bit is a convex sum of these two extremal points. Similarly, if there are d possible states, there are d extremal distributions, and any probability distribution has a *unique* decomposition into extremal ones (the convex set of probability distributions is a *simplex*, the convex hull of its d vertices). If 0 occurs with 21% probability, 1 with 33% probability, and 2 with 46% probability, there is a unique "preparation procedure" that yields this probability distribution.

2.5.3 Faster than light?

Let's now return to our earlier viewpoint — that a mixed state of system A arises because A is *entangled* with system B — to further consider the implications of the ambiguous preparation of mixed states. If qubit A has density matrix

$$\boldsymbol{\rho}_A = \frac{1}{2}|\uparrow_z\rangle\langle\uparrow_z| + \frac{1}{2}|\downarrow_z\rangle\langle\downarrow_z|, \tag{2.106}$$

this density matrix could arise from an entangled bipartite pure state $|\psi\rangle_{AB}$ with the Schmidt decomposition

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle_A|\uparrow_z\rangle_B + |\downarrow_z\rangle_A|\downarrow_z\rangle_B\right). \tag{2.107}$$

Therefore, the ensemble interpretation of $\boldsymbol{\rho}_A$ in which either $|\uparrow_z\rangle_A$ or $|\downarrow_z\rangle_A$ is prepared (each with probability $p = \frac{1}{2}$) can be realized by performing a measurement of qubit B. We measure qubit B in the $\{|\uparrow_z\rangle_B, |\downarrow_z\rangle_B\}$ basis; if the result $|\uparrow_z\rangle_B$ is obtained, we have prepared $|\uparrow_z\rangle_A$, and if the result $|\downarrow_7\rangle_B$ is obtained, we have prepared $|\downarrow_z\rangle_A$.

But as we have already noted, in this case, because $\boldsymbol{\rho}_A$ has degenerate eigenvalues, the Schmidt basis is not unique. We can apply simultaneous unitary transformations to qubits A and B (actually, if we apply U to A we must apply U^* to B as in eq.(2.92)) without modifying the bipartite pure state $|\psi\rangle_{AB}$. Therefore, for *any* unit 3-vector $\hat{n}$, $|\psi\rangle_{AB}$ has a Schmidt decomposition of the form

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\uparrow_{\hat{n}}\rangle_A|\uparrow_{\hat{n}'}\rangle_B + |\downarrow_{\hat{n}}\rangle_A|\downarrow_{\hat{n}'}\rangle_B\right). \tag{2.108}$$

We see that by measuring qubit B in a suitable basis, we can realize *any* interpretation of $\boldsymbol{\rho}_A$ as an ensemble of two pure states.

This property suggests a mechanism for faster-than-light communication. Many copies of $|\psi\rangle_{AB}$ are prepared. Alice takes all of the A qubits to the Andromeda galaxy and Bob keeps all of the B qubits on earth. When Bob wants to send a one-bit message to Alice, he chooses to measure either $\boldsymbol{\sigma}_1$ or $\boldsymbol{\sigma}_3$ for all his spins, thus preparing Alice's spins in either

the $\{|\uparrow_z\rangle_A, |\downarrow_z\rangle_A\}$ or $\{|\uparrow_x\rangle_A, |\downarrow_x\rangle_A\}$ ensembles. (U is real in this case, so $U = U^*$ and $\hat{n} = \hat{n}'$.) To read the message, Alice immediately measures her spins to see which ensemble has been prepared.

This scheme has a flaw. Though the two preparation methods are surely different, both ensembles are described by precisely the same density matrix $\boldsymbol{\rho}_A$. Thus, there is no conceivable measurement Alice can make that will distinguish the two ensembles, and no way for Alice to tell what action Bob performed. The "message" is unreadable.

Why, then, do we confidently state that "the two preparation methods are surely different?" To qualm any doubts about that, imagine that Bob either (1) measures all of his spins along the $\hat{z}$-axis, or (2) measures all of his spins along the $\hat{x}$-axis, and then calls Alice on the intergalactic telephone. He does *not* tell Alice whether he did (1) or (2), but he does tell her the results of all his measurements: "the first spin was up, the second was down," etc. Now Alice performs either (1) or (2) on *her* spins. If both Alice and Bob measured along the same axis, Alice will find that every single one of her measurement outcomes agrees with what Bob found. But if Alice and Bob measured along different (orthogonal) axes, then Alice will find *no correlation* between her results and Bob's. About half of her measurements agree with Bob's and about half disagree. If Bob promises to do either (1) or (2), and assuming no preparation or measurement errors, then Alice will know that Bob's action was different than hers (even though Bob never told her this information) as soon as one of her measurements disagrees with what Bob found. If all their measurements agree, then if many spins are measured, Alice will have very high statistical confidence that she and Bob measured along the same axis. (Even with occasional measurement errors, the statistical test will still be highly reliable if the error rate is low enough.) So Alice does have a way to distinguish Bob's two preparation methods, but in this case there is certainly no faster-than-light communication, because Alice had to receive Bob's phone call before she could perform her test.

2.5.4 Quantum erasure

We had said that the density matrix $\boldsymbol{\rho}_A = \frac{1}{2}\boldsymbol{I}$ describes a spin in an *incoherent* mixture of the pure states $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$. This was to be distinguished from *coherent* superpositions of these states, such as

$$|\uparrow_x, \downarrow_x\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow_z\rangle \pm |\downarrow_z\rangle\right) \ ; \tag{2.109}$$

in the case of a coherent superposition, the *relative phase* of the two states has observable consequences (distinguishes $|\uparrow_x\rangle$ from $|\downarrow_x\rangle$). In the case of an incoherent mixture, the relative phase is completely unobservable.

The superposition becomes incoherent if spin A becomes entangled with another spin B, and spin B is inaccessible.

Heuristically, the states $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$ can *interfere* (the relative phase of these states can be observed) only if we have no information about whether the spin state is $|\uparrow_z\rangle_A$ or $|\downarrow_z\rangle_A$. More than that, interference can occur only if there is *in principle no possible way* to find out whether the spin is up or down along the z-axis. Entangling spin A with spin B destroys interference, (causes spin A to *decohere*) because it is possible in principle for us to determine if spin A is up or down along $\hat{z}$ by performing a suitable measurement of spin B.

But we have now seen that the statement that entanglement causes decoherence requires a qualification. Suppose that Bob measures spin B along the $\hat{x}$-axis, obtaining either the result $|\uparrow_x\rangle_B$ or $|\downarrow_x\rangle_B$, and that he sends his measurement result to Alice. *Now* Alice's spin is a pure state (either $|\uparrow_x\rangle_A$ or $|\downarrow_x\rangle_A$) and in fact a coherent superposition of $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$. We have managed to recover the purity of Alice's spin before the jaws of decoherence could close!

Suppose that Bob allows his spin to pass through a Stern–Gerlach apparatus oriented along the $\hat{z}$-axis. Well, of course, Alice's spin can't behave like a coherent superposition of $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$; all Bob has to do is look to see which way his spin moved, and he will know whether Alice's spin is up or down along $\hat{z}$. But suppose that Bob does not look. Instead, he carefully refocuses the two beams without maintaining any record of whether his spin moved up or down, and *then* allows the spin to pass through a second Stern–Gerlach apparatus oriented along the $\hat{x}$-axis. *This* time he looks, and communicates the result of his $\boldsymbol{\sigma}_1$ measurement to Alice. Now the coherence of Alice's spin has been restored!

This situation has been called a *quantum eraser*. Entangling the two spins creates a "measurement situation" in which the coherence of $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$ is lost because we can find out if spin A is up or down along $\hat{z}$ by observing spin B. But when we measure spin B along $\hat{x}$, this information is "erased." Whether the result is $|\uparrow_x\rangle_B$ or $|\downarrow_x\rangle_B$ does not tell us anything about whether spin A is up or down along $\hat{z}$, because Bob has been careful not to retain the "which way" information that he might have acquired by looking at the first Stern–Gerlach apparatus. Therefore, it is possible again for spin A to behave like a coherent superposition of $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$ (and it does, *after* Alice hears about Bob's result).

We can best understand the quantum eraser from the ensemble viewpoint. Alice has many spins selected from an ensemble described by $\boldsymbol{\rho}_A = \frac{1}{2}\boldsymbol{I}$, and there is no way for her to observe interference between $|\uparrow_z\rangle_A$ and $|\downarrow_z\rangle_A$. When Bob makes his measurement along $\hat{x}$, a particular preparation of the ensemble is realized. However, this has no effect that Alice can perceive – her spin is *still* described by $\boldsymbol{\rho}_A = \frac{1}{2}\boldsymbol{I}$ as before.

But, when Alice receives Bob's phone call, she can select a *subensemble* of her spins that are all in the pure state $|\uparrow_x\rangle_A$. The information that Bob sends allows Alice to distill purity from a maximally mixed state.

Another wrinkle on the quantum eraser is sometimes called *delayed choice*. This just means that the situation we have described is really completely symmetric between Alice and Bob, so it can't make any difference who measures first. (Indeed, if Alice's and Bob's measurements are spacelike separated events, there is no invariant meaning to which came first; it depends on the frame of reference of the observer.) Alice could measure all of her spins today (say along $\hat{x}$) before Bob has made his mind up how he will measure his spins. Next week, Bob can decide to "prepare" Alice's spins in the states $|\uparrow_{\hat{n}}\rangle_A$ and $|\downarrow_{\hat{n}}\rangle_A$ (that is the "delayed choice"). He then tells Alice which were the $|\uparrow_{\hat{n}}\rangle_A$ spins, and she can check her measurement record to verify that

$$\langle\sigma_1\rangle_{\hat{n}} = \hat{n}\cdot\hat{x}\ . \tag{2.110}$$

The results are the same, irrespective of whether Bob "prepares" the spins before or after Alice measures them.

We have claimed that the density matrix $\boldsymbol{\rho}_A$ provides a complete physical description of the state of subsystem A, because it characterizes all possible measurements that can be performed on A. One might object that the quantum eraser phenomenon demonstrates otherwise. Since the information received from Bob enables Alice to recover a pure state from the mixture, how can we hold that everything Alice can know about A is encoded in $\boldsymbol{\rho}_A$?

I prefer to say that quantum erasure illustrates the principle that "information is physical." The state $\boldsymbol{\rho}_A$ of system A is not the same thing as $\boldsymbol{\rho}_A$ accompanied by the information that Alice has received from Bob. This information (which attaches labels to the subensembles) changes the physical description. That is, we should include Alice's "state of knowledge" in our description of her system. An ensemble of spins for which Alice has no information about whether each spin is up or down is a *different* physical state than an ensemble in which Alice knows which spins are up and which are down. This "state of knowledge" need not really be the state of a human mind; any (inanimate) record that labels the subensemble will suffice.

2.5.5 The HJW theorem

So far, we have considered the quantum eraser only in the context of a single qubit, described by an ensemble of equally probable mutually orthogonal states, (*i.e.*, $\boldsymbol{\rho}_A = \frac{1}{2}\boldsymbol{I}$). The discussion can be considerably generalized.

We have already seen that a mixed state of any quantum system can be realized as an ensemble of pure states in an infinite number of different ways. For a density matrix $\boldsymbol{\rho}_A$, consider one such realization:

$$\boldsymbol{\rho}_A = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|, \quad \sum p_i = 1. \tag{2.111}$$

Here the states $\{|\varphi_i\rangle_A\}$ are all normalized vectors, but we do *not* assume that they are mutually orthogonal. Nevertheless, $\boldsymbol{\rho}_A$ can be realized as an ensemble, in which each pure state $|\varphi_i\rangle\langle\varphi_i|$ occurs with probability p_i.

For any such $\boldsymbol{\rho}_A$, we can construct a "purification" of $\boldsymbol{\rho}_A$, a bipartite pure state $|\Phi_1\rangle_{AB}$ that yields $\boldsymbol{\rho}_A$ when we perform a partial trace over $\mathcal{H}_B$. One such purification is of the form

$$|\Phi_1\rangle_{AB} = \sum_i \sqrt{p_i}\ |\varphi_i\rangle_A \otimes |\alpha_i\rangle_B, \tag{2.112}$$

where the vectors $|\alpha_i\rangle_B \in \mathcal{H}_B$ *are* mutually orthogonal and normalized,

$$\langle\alpha_i|\alpha_j\rangle = \delta_{ij}. \tag{2.113}$$

Clearly, then,

$$\mathrm{tr}_B\left(|\Phi_1\rangle\langle\Phi_1|\right) = \boldsymbol{\rho}_A. \tag{2.114}$$

Furthermore, we can imagine performing an orthogonal measurement in system B that projects onto the $|\alpha_i\rangle_B$ basis. (The $|\alpha_i\rangle_B$'s might not span $\mathcal{H}_B$, but in the state $|\Phi_1\rangle_{AB}$, measurement outcomes orthogonal to all the $|\alpha_i\rangle_B$'s never occur.) The outcome $|\alpha_i\rangle_B$ will occur with probability p_i, and will prepare the pure state $|\varphi_i\rangle\langle\varphi_i|$ of system A. Thus, given the purification $|\Phi_1\rangle_{AB}$ of $\boldsymbol{\rho}_A$, there is a measurement we can perform in system B that realizes the $|\varphi_i\rangle_A$ ensemble interpretation of $\boldsymbol{\rho}_A$. When the measurement outcome in B is known, we have successfully extracted one of the pure states $|\varphi_i\rangle_A$ from the mixture $\boldsymbol{\rho}_A$.

What we have just described is a generalization of preparing $|\uparrow_z\rangle_A$ by measuring spin B along $\hat{z}$ (in our discussion of two entangled qubits). But to generalize the notion of a quantum eraser, we wish to see that in the state $|\Phi_1\rangle_{AB}$, we can realize a *different* ensemble interpretation of $\boldsymbol{\rho}_A$ by performing a different measurement of B. So let

$$\boldsymbol{\rho}_A = \sum_\mu q_\mu |\psi_\mu\rangle\langle\psi_\mu|, \tag{2.115}$$

be another realization of the same density matrix $\boldsymbol{\rho}_A$ as an ensemble of pure states. For this ensemble as well, there is a corresponding purification

$$|\Phi_2\rangle_{AB} = \sum_\mu \sqrt{q_\mu}\ |\psi_\mu\rangle_A \otimes |\beta_\mu\rangle_B, \tag{2.116}$$

where again the $\{|\beta_\mu\rangle_B$'s$\}$ are orthonormal vectors in $\mathcal{H}_B$. So in the state $|\Phi_2\rangle_{AB}$, we can realize the ensemble by performing a measurement in $\mathcal{H}_B$ that projects onto the $\{|\beta_\mu\rangle_B\}$ basis.

Now, how are $|\Phi_1\rangle_{AB}$ and $|\Phi_2\rangle_{AB}$ related? In fact, we can easily show that

$$|\Phi_1\rangle_{AB} = (\boldsymbol{I}_A \otimes \boldsymbol{U}_B)\,|\Phi_2\rangle_{AB}; \tag{2.117}$$

the two states differ by a unitary change of basis acting in $\mathcal{H}_B$ alone, or

$$|\Phi_1\rangle_{AB} = \sum_\mu \sqrt{q_\mu}\;|\psi_\mu\rangle_A \otimes |\gamma_\mu\rangle_B, \tag{2.118}$$

where

$$|\gamma_\mu\rangle_B = \boldsymbol{U}_B|\beta_\mu\rangle_B, \tag{2.119}$$

is yet another orthonormal basis for $\mathcal{H}_B$. We see, then, that there is a *single* purification $|\Phi_1\rangle_{AB}$ of $\boldsymbol{\rho}_A$, such that we can realize either the $\{|\varphi_i\rangle_A\}$ ensemble or $\{|\psi_\mu\rangle_A\}$ ensemble by choosing to measure the appropriate observable in system B!

Similarly, we may consider many ensembles that all realize $\boldsymbol{\rho}_A$, where the maximum number of pure states appearing in any of the ensembles is N. Then we may choose a Hilbert space $\mathcal{H}_B$ of dimension N, and a pure state $|\Phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, such that any one of the ensembles can be realized by measuring a suitable observable of B. This is the *HJW theorem* (for Hughston, Jozsa, and Wootters); it expresses the quantum eraser phenomenon in its most general form.

In fact, the HJW theorem is an easy corollary to the Schmidt decomposition. Both $|\Phi_1\rangle_{AB}$ and $|\Phi_2\rangle_{AB}$ have a Schmidt decompositions, and because both yield the same $\boldsymbol{\rho}_A$ when we take the partial trace over B, these decompositions must have the form

$$\begin{aligned} |\Phi_1\rangle_{AB} &= \sum_k \sqrt{\lambda_k}\;|k\rangle_A \otimes |k'_1\rangle_B, \\ |\Phi_2\rangle_{AB} &= \sum_k \sqrt{\lambda_k}\;|k\rangle_A \otimes |k'_2\rangle_B, \end{aligned} \tag{2.120}$$

where the λ_k's are the eigenvalues of $\boldsymbol{\rho}_A$ and the $|k\rangle_A$'s are the corresponding eigenvectors. But since $\{|k'_1\rangle_B\}$ and $\{|k'_2\rangle_B\}$ are both orthonormal bases for $\mathcal{H}_B$, there is a unitary $\boldsymbol{U}_B$ such that

$$|k'_1\rangle_B = \boldsymbol{U}_B|k'_2\rangle_B, \tag{2.121}$$

from which eq.(2.117) immediately follows.

In the ensemble of pure states described by Eq. (2.111), we would say that the pure states $|\varphi_i\rangle_A$ are mixed *incoherently* — an observer in system A cannot detect the relative phases of these states. Heuristically, the

reason that these states cannot interfere is that it is possible in principle to find out which representative of the ensemble is actually realized by performing a measurement in system B, a projection onto the orthonormal basis $\{|\alpha_i\rangle_B\}$. However, by projecting onto the $\{|\gamma_\mu\rangle_B\}$ basis instead, and relaying the information about the measurement outcome to system A, we can extract one of the pure states $|\psi_\mu\rangle_A$ from the ensemble, even though this state may be a coherent superposition of the $|\varphi_i\rangle_A$'s. In effect, measuring B in the $\{|\gamma_\mu\rangle_B\}$ basis "erases" the "which way" information (whether the state of A is $|\varphi_i\rangle_A$ or $|\varphi_j\rangle_A$). In this sense, the HJW theorem characterizes the general quantum eraser. The moral, once again, is that *information is physical* — the information acquired by measuring system B, when relayed to A, changes the physical description of a state of A.

2.6 Summary

Axioms. The arena of quantum mechanics is a Hilbert space $\mathcal{H}$. The fundamental assumptions are:

(1) A *state* is a *ray* in $\mathcal{H}$.

(2) An *observable* is a *self-adjoint operator* on $\mathcal{H}$.

(3) A *measurement* is an orthogonal *projection*.

(4) *Time evolution* is *unitary*.

(5) A *composite system* AB is described by the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$.

Density operator. But if we confine our attention to only a portion of a larger quantum system, assumptions (1)-(4) need not be satisfied. In particular, a quantum state is described not by a ray, but by a density operator $\boldsymbol{\rho}$, a nonnegative operator with unit trace. The density operator is *pure* (and the state can be described by a ray) if $\boldsymbol{\rho}^2 = \boldsymbol{\rho}$; otherwise, the state is *mixed*. An observable $\boldsymbol{M}$ has expectation value $\mathrm{tr}(\boldsymbol{M}\boldsymbol{\rho})$ in this state.

Qubit. A quantum system with a two-dimensional Hilbert space is called a *qubit*. The general density matrix of a qubit is

$$\boldsymbol{\rho}(\vec{P}) = \frac{1}{2}(\boldsymbol{I} + \vec{P} \cdot \vec{\boldsymbol{\sigma}}) \tag{2.122}$$

where $\vec{P}$ is a three-component vector of length $|\vec{P}| \leq 1$. Pure states have $|\vec{P}| = 1$.

Schmidt decomposition. For any pure state $|\psi\rangle_{AB}$ of a bipartite system, there are orthonormal bases $\{|i\rangle_A\}$ for $\mathcal{H}_A$ and $\{|i'\rangle_B\}$ for $\mathcal{H}_B$

such that

$$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\ |i\rangle_A \otimes |i'\rangle_B; \tag{2.123}$$

Eq.(2.123) is called the *Schmidt decomposition* of $|\psi\rangle_{AB}$. In a bipartite pure state, subsystems A and B separately are described by density operators $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$; it follows from eq.(2.123) that $\boldsymbol{\rho}_A$ and $\boldsymbol{\rho}_B$ have the same nonvanishing eigenvalues (the p_i's). The number of nonvanishing eigenvalues is called the *Schmidt number* of $|\psi\rangle_{AB}$. A bipartite pure state is said to be *entangled* if its Schmidt number is greater than one.

Ensembles. The density operators on a Hilbert space form a convex set, and the pure states are the *extremal points* of the set. A mixed state of a system A can be prepared as an *ensemble* of pure states in many different ways, all of which are experimentally indistinguishable if we observe system A alone. Given any mixed state $\boldsymbol{\rho}_A$ of system A, any preparation of $\boldsymbol{\rho}_A$ as an ensemble of pure states can be realized in principle by performing a measurement in another system B with which A is entangled. In fact given many such preparations of $\boldsymbol{\rho}_A$, there is a single entangled state of A and B such that any one of these preparations can be realized by measuring a suitable observable in B (the *HJW theorem*). By measuring in system B and reporting the measurement outcome to system A, we can extract from the mixture a pure state chosen from one of the ensembles.

2.7 Exercises

2.1 Fidelity of a guess

a) A single qubit (spin-$\frac{1}{2}$ object) is in an unknown *pure* state $|\psi\rangle$, selected at random from an ensemble uniformly distributed over the Bloch sphere. We guess at random that the state is $|\varphi\rangle$. On the average, what is the *fidelity* F of our guess, defined by

$$F \equiv |\langle\varphi|\psi\rangle|^2\ . \tag{2.124}$$

b) After randomly selecting a one-qubit pure state as in part (*a*), we perform a measurement of the spin along the $\hat{z}$-axis. This measurement prepares a state described by the density operator

$$\boldsymbol{\rho} = \boldsymbol{E}_\uparrow \langle\psi|\boldsymbol{E}_\uparrow|\psi\rangle + \boldsymbol{E}_\downarrow \langle\psi|\boldsymbol{E}_\downarrow|\psi\rangle \tag{2.125}$$

(where $\boldsymbol{E}_{\uparrow,\downarrow}$ denote the projections onto the spin-up and spin-down states along the $\hat{z}$-axis). On the average, with what fidelity

$$F \equiv \langle\psi|\boldsymbol{\rho}|\psi\rangle \tag{2.126}$$

does this density matrix represent the initial state $|\psi\rangle$?

Remark: The improvement in F in the answer to (b) compared to the answer to (a) is a crude measure of how much we learned by making the measurement.

2.2 Schmidt decomposition

For the two-qubit state

$$\Phi = \frac{1}{\sqrt{2}}|\uparrow\rangle_A \left(\frac{1}{2}|\uparrow\rangle_B + \frac{\sqrt{3}}{2}|\downarrow\rangle_B\right) + \frac{1}{\sqrt{2}}|\downarrow\rangle_A \left(\frac{\sqrt{3}}{2}|\uparrow\rangle_B + \frac{1}{2}|\downarrow\rangle_B\right) \tag{2.127}$$

a) Compute $\boldsymbol{\rho}_A = \mathrm{tr}_B\left(|\Phi\rangle\langle\Phi|\right)$ and $\boldsymbol{\rho}_B = \mathrm{tr}_A\left(|\Phi\rangle\langle\Phi|\right)$.

b) Find the Schmidt decomposition of $|\Phi\rangle$.

2.3 Measurement without disturbance?

Charlie prepares the system A in one of two *nonorthogonal* states, $|\varphi\rangle_A$ or $|\tilde{\varphi}\rangle_A$, and he challenges Alice to collect some information about which state he prepared *without in any way disturbing the state*. Alice has an idea about how to meet the challenge.

Alice intends to prepare a second "ancillary" system B in the state $|\beta\rangle_B$, and then apply to the composite system AB a unitary transformation U that acts according to

$$\begin{aligned} U : |\varphi\rangle_A \otimes |\beta\rangle_B &\rightarrow |\varphi\rangle_A \otimes |\beta'\rangle_B \\ |\tilde{\varphi}\rangle_A \otimes |\beta\rangle_B &\rightarrow |\tilde{\varphi}\rangle_A \otimes |\tilde{\beta}'\rangle_B, \end{aligned} \tag{2.128}$$

which does indeed leave the state of system A undisturbed. Then she plans to perform a measurement on system B that is designed to distinguish the states $|\beta'\rangle_B$ and $|\tilde{\beta}'\rangle_B$.

a) What do you think of Alice's idea? [**Hint**: What does the unitarity of U tell you about how the states $|\beta'\rangle_B$ and $|\tilde{\beta}'\rangle_B$ are related to one another?]

b) Would you feel differently if the states $|\varphi\rangle_A$ and $|\tilde{\varphi}\rangle_A$ were orthogonal?

2.4 Quantum bit commitment

The Yankees are playing the Dodgers in the World Series. Alice is sure that she knows who will win. Alice doesn't like Bob, so she doesn't want to tell him who the winner will be. But after the Series

is over, Alice wants to be able to convince Bob that she knew the outcome all along. What to do?

Bob suggests that Alice write down her choice (0 if the Yankees will win, 1 if the Dodgers will win) on a piece of paper, and lock the paper in a box. She is to give the box to Bob, but she will keep the key for herself. Then, when she is ready to reveal her choice, she will send the key to Bob, allowing him to open the box and read the paper.

Alice rejects this proposal. She doesn't trust Bob, and she knows that he is a notorious safe cracker. Who's to say whether he will be able to open the box and sneak a look, even if he doesn't have the key?

Instead, Alice proposes to certify her honesty in another way, using quantum information. To *commit* to a value $a \in \{0, 1\}$ of her bit, she prepares one of two distinguishable density operators ($\boldsymbol{\rho}_0$ or $\boldsymbol{\rho}_1$) of the bipartite system AB, sends system B to Bob, and keeps system A for herself. Later, to *unveil* her bit, Alice sends system A to Bob, and he performs a measurement to determine whether the state of AB is $\boldsymbol{\rho}_0$ or $\boldsymbol{\rho}_1$. This protocol is called *quantum bit commitment*

We say that the protocol is *binding* if, after commitment, Alice is unable to change the value of her bit. We say that the protocol is *concealing* if, after commitment and before unveiling, Bob is unable to discern the value of the bit. The protocol is *secure* if it is both binding and concealing.

Show that if a quantum bit commitment protocol is concealing, then it is not binding. Thus quantum bit commitment is insecure.

Hint: First argue that without loss of generality, we may assume that the states $\boldsymbol{\rho}_0$ and $\boldsymbol{\rho}_1$ are both pure. Then apply the HJW Theorem.

Remark: Note that the conclusion that quantum bit commitment is insecure still applies even if the shared bipartite state ($\boldsymbol{\rho}_0$ or $\boldsymbol{\rho}_1$) is prepared during many rounds of quantum communication between Alice and Bob, where in each round one party performs a quantum operation on his/her local system and on a shared message system, and then sends the message system to the other party.

2.5 Quantum correlations in a mixed state

Consider a density matrix for two qubits

$$\boldsymbol{\rho} = \frac{1}{8}\boldsymbol{I} + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \,, \tag{2.129}$$

where $\boldsymbol{I}$ denotes the 4×4 unit matrix, and

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle\right) \ . \tag{2.130}$$

Suppose we measure the first spin along the $\hat{n}$ axis and the second spin along the $\hat{m}$ axis, where $\hat{n}\cdot\hat{m} = \cos\theta$. What is the probability that both spins are "spin-up" along their respective axes?

2.6 Completeness of subsystem correlations

Consider a bipartite system AB. Suppose that many copies of the (not necessarily pure) state $\boldsymbol{\rho}_{AB}$ have been prepared. An observer Alice with access only to subsystem A can measure the expectation value of any observable of the form $\boldsymbol{M}_A \otimes \boldsymbol{I}_B$, while an observer Bob with access only to subsystem B can measure the expectation value of any observable of the form $\boldsymbol{I}_A \otimes \boldsymbol{N}_B$. As discussed in class, neither of these observers, working alone, can expect to learn very much about the state $\boldsymbol{\rho}_{AB}$.

But now suppose that Alice and Bob can communicate, exchanging (classical) information about how their measurement outcomes are *correlated*. Thereby, they can jointly determine the expectation value of any observable of the form $\boldsymbol{M}_A \otimes \boldsymbol{N}_B$ (an observable whose eigenstates are separable direct products states of the form $|\varphi\rangle_A \otimes |\chi\rangle_B$).

The point of this exercise is to show that if Alice and Bob have complete knowledge of the nature of the correlations between subsystems A and B (know the expectation values of any tensor product observable $\boldsymbol{M}_A \otimes \boldsymbol{N}_B$), then in fact they know everything about the bipartite state $\boldsymbol{\rho}_{AB}$ – there will be no surprises when they measure entangled observables, those whose eigenstates are entangled states.

a) Let $\{\boldsymbol{M}_a,\ a = 1, 2, \ldots, N^2\}$ denote a set of N^2 linearly independent self-adjoint operators acting on a Hilbert space $\mathcal{H}$ of dimension N. Show that if $\boldsymbol{\rho}$ is a density operator acting on $\mathcal{H}$, and $\mathrm{tr}\,(\boldsymbol{\rho}\boldsymbol{M}_a)$ is known for each a, then $\langle\varphi|\boldsymbol{\rho}|\varphi\rangle$ is known for any vector $|\varphi\rangle$ in $\mathcal{H}$.

b) Show that if $\langle\varphi|\boldsymbol{\rho}|\varphi\rangle$ is known for each vector $|\varphi\rangle$, then $\boldsymbol{\rho}$ is completely known.

c) Show that if $\{\boldsymbol{M}_a\}$ denotes a basis for self-adjoint operators on $\mathcal{H}_A$, and $\{\boldsymbol{N}_b\}$ denotes a basis for self-adjoint operators on $\mathcal{H}_B$, then $\{\boldsymbol{M}_a \otimes \boldsymbol{N}_b\}$ is a basis for the self-adjoint operators on $\mathcal{H}_A \otimes \mathcal{H}_B$.

Remark: It follows from (c) alone that the correlations of the "local" observables determine the expectation values of all the observables. Parts (a) and (b) serve to establish that $\boldsymbol{\rho}$ is completely determined by the expectation values of a complete set of observables.

d) State and prove the result corresponding to (c) that applies to a multipartite system with Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$.

e) Discuss how the world would be different if quantum states resided in a real Hilbert space rather than a complex Hilbert space. Consider, in particular, whether (c) is true for *symmetric* operators acting on a real vector space.

2.7 How far apart are two quantum states?

Consider two quantum states described by density operators $\boldsymbol{\rho}$ and $\tilde{\boldsymbol{\rho}}$ in an N-dimensional Hilbert space, and consider the complete orthogonal measurement $\{\boldsymbol{E}_a, a = 1, 2, 3, \ldots N\}$, where the $\boldsymbol{E}_a$'s are one-dimensional projectors satisfying

$$\sum_{a=1}^{N} \boldsymbol{E}_a = \boldsymbol{I}. \tag{2.131}$$

When the measurement is performed, outcome a occurs with probability $p_a = \mathrm{tr}\, \boldsymbol{\rho}\boldsymbol{E}_a$ if the state is $\boldsymbol{\rho}$ and with probability $\tilde{p}_a = \mathrm{tr}\, \tilde{\boldsymbol{\rho}}\boldsymbol{E}_a$ if the state is $\tilde{\boldsymbol{\rho}}$.

The L^1 *distance* between the two probability distributions is defined as

$$d(p, \tilde{p}) \equiv \|p - \tilde{p}\|_1 \equiv \frac{1}{2} \sum_{a=1}^{N} |p_a - \tilde{p}_a| \; ; \tag{2.132}$$

this distance is zero if the two distributions are identical, and attains its maximum value one if the two distributions have support on disjoint sets.

a) Show that

$$d(p, \tilde{p}) \leq \frac{1}{2} \sum_{i=1}^{N} |\lambda_i| \tag{2.133}$$

where the λ_i's are the eigenvalues of the Hermitian operator $\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}$. **Hint**: Working in the basis in which $\boldsymbol{\rho} - \tilde{\boldsymbol{\rho}}$ is diagonal, find an expression for $|p_a - \tilde{p}_a|$, and then find an upper bound on $|p_a - \tilde{p}_a|$. Finally, use the completeness property eq.(2.131) to bound $d(p, \tilde{p})$.

b) Find a choice for the orthogonal projector $\{\boldsymbol{E}_a\}$ that saturates the upper bound eq.(2.133).

Define a distance $d(\boldsymbol{\rho}, \tilde{\boldsymbol{\rho}})$ between density operators as the maximal L^1 distance between the corresponding probability distributions that can be achieved by any orthogonal measurement. From the results of (*a*) and (*b*), we have found that

$$d(\boldsymbol{\rho}, \tilde{\boldsymbol{\rho}}) = \frac{1}{2} \sum_{i=1}^{N} |\lambda_i|. \tag{2.134}$$

c) The L^1 *norm* $\|\boldsymbol{A}\|_1$ of an operator $\boldsymbol{A}$ is defined as

$$\|\boldsymbol{A}\|_1 \equiv \mathrm{tr}\left[(\boldsymbol{A}\boldsymbol{A}^\dagger)^{1/2}\right]. \tag{2.135}$$

How can the distance $d(\boldsymbol{\rho}, \tilde{\boldsymbol{\rho}})$ be expressed as the L^1 norm of an operator?

Now suppose that the states $\boldsymbol{\rho}$ and $\tilde{\boldsymbol{\rho}}$ are pure states $\boldsymbol{\rho} = |\psi\rangle\langle\psi|$ and $\tilde{\boldsymbol{\rho}} = |\tilde{\psi}\rangle\langle\tilde{\psi}|$. If we adopt a suitable basis in the space spanned by the two vectors, and appropriate phase conventions, then these vectors can be expressed as

$$|\psi\rangle = \begin{pmatrix} \cos\theta/2 \\ \sin\theta/2 \end{pmatrix}, \quad |\tilde{\psi}\rangle = \begin{pmatrix} \sin\theta/2 \\ \cos\theta/2 \end{pmatrix}, \tag{2.136}$$

where $\langle\psi|\tilde{\psi}\rangle = \sin\theta$.

d) Express the distance $d(\boldsymbol{\rho}, \tilde{\boldsymbol{\rho}})$ in terms of the angle θ.

e) Express $\| \, |\psi\rangle - |\tilde{\psi}\rangle\|^2$ (where $\|\cdot\|$ denotes the Hilbert space norm) in terms of θ, and by comparing with the result of (*d*), derive the bound

$$d(|\psi\rangle\langle\psi|, |\tilde{\psi}\rangle\langle\tilde{\psi}|) \leq \| \, |\psi\rangle - |\tilde{\psi}\rangle\|. \tag{2.137}$$

f) Bob thinks that the norm $\| \, |\psi\rangle - |\tilde{\psi}\rangle\|$ should be a good measure of the distinguishability of the pure quantum states $\boldsymbol{\rho}$ and $\tilde{\boldsymbol{\rho}}$. Explain why Bob is wrong. **Hint**: Remember that quantum states are *rays*.

2.8 What probability distributions are consistent with a mixed state?

A density operator $\boldsymbol{\rho}$, expressed in the orthonormal basis $\{|\alpha_i\rangle\}$ that diagonalizes it, is

$$\boldsymbol{\rho} = \sum_i p_i |\alpha_i\rangle\langle\alpha_i|. \tag{2.138}$$

We would like to realize this density operator as an ensemble of pure states $\{|\varphi_\mu\rangle\}$, where $|\varphi_\mu\rangle$ is prepared with a specified probability q_μ. This preparation is possible if the $|\varphi_\mu\rangle$'s can be chosen so that

$$\boldsymbol{\rho} = \sum_\mu q_\mu |\varphi_\mu\rangle\langle\varphi_\mu|. \tag{2.139}$$

We say that a probability vector q (a vector whose components are nonnegative real numbers that sum to 1) is *majorized* by a probability vector p (denoted $q \prec p$), if there exists a *doubly stochastic* matrix D such that

$$q_\mu = \sum_i D_{\mu i}\ p_i. \tag{2.140}$$

A matrix is doubly stochastic if its entries are nonnegative real numbers such that $\sum_\mu D_{\mu i} = \sum_i D_{\mu i} = 1$. That the columns sum to one assures that D maps probability vectors to probability vectors (*i.e.*, is *stochastic*). That the rows sum to one assures that D maps the uniform distribution to itself. Applied repeatedly, D takes any input distribution closer and closer to the uniform distribution (unless D is a permutation, with one nonzero entry in each row and column). Thus we can view majorization as a partial order on probability vectors such that $q \prec p$ means that q is more nearly uniform than p (or equally close to uniform, in the case where D is a permutation).

Show that normalized pure states $\{|\varphi_\mu\rangle\}$ exist such that eq.(2.139) is satisfied if and only if $q \prec p$, where p is the vector of eigenvalues of $\boldsymbol{\rho}$.

Hint: Recall that, according to the HJW Theorem, if eq.(2.138) and eq.(2.139) are both satisfied then there is a unitary matrix $V_{\mu i}$ such that

$$\sqrt{q_\mu}\ |\varphi_\mu\rangle = \sum_i \sqrt{p_i}\ V_{\mu i}|\alpha_i\rangle. \tag{2.141}$$

You may also use (but need not prove) *Horn's Lemma*: if $q \prec p$, then there exists a unitary (in fact, orthogonal) matrix $U_{\mu i}$ such that $q = Dp$ and $D_{\mu i} = |U_{\mu i}|^2$.

2.9 Alice does Bob a favor

Alice, in Anaheim, and Bob, in Boston, share a bipartite pure state $|\Psi\rangle$, which can be expressed in the Schmidt form

$$|\Psi\rangle = \sum_i \sqrt{p_i}\ |\alpha_i\rangle \otimes |\beta_i\rangle, \tag{2.142}$$

where $\{|\alpha_i\rangle\}$ is an orthonormal basis for Alice's system A, $\{|\beta_i\rangle\}$ is an orthonormal basis for Bob's system B, and the $\{p_i\}$ are non-negative real numbers summing to 1. Bob is supposed to perform a complete orthogonal local measurement on B, characterized by the set of projectors $\{\boldsymbol{E}_a^B\}$ — if the measurement outcome is a, then Bob's measurement prepares the state

$$|\Psi\rangle \mapsto |\Psi_a\rangle = \frac{\left(\boldsymbol{I} \otimes \boldsymbol{E}_a^B\right)|\Psi\rangle}{\langle\Psi|\left(\boldsymbol{I} \otimes \boldsymbol{E}_a^B\right)|\Psi\rangle^{1/2}}. \tag{2.143}$$

$|\Psi_a\rangle$ can also be expressed in the Schmidt form if we choose appropriate orthonormal bases for A and B that depend on the measurement outcome. The new Schmidt basis elements can be written as

$$|\alpha'_{a,i}\rangle = \boldsymbol{U}_a^A|\alpha_i\rangle, \quad |\beta'_{a,i}\rangle = \boldsymbol{U}_a^B|\beta_i\rangle, \tag{2.144}$$

where $\boldsymbol{U}_a^A, \boldsymbol{U}_a^B$ are unitary.

Unfortunately, Bob's measurement apparatus is broken, though he still has the ability to perform local unitary transformations on B. Show that Alice can help Bob out by performing a measurement that is "locally equivalent" to Bob's. That is, there are orthogonal projectors $\{\boldsymbol{E}_a^A\}$ and unitary transformations $\boldsymbol{V}_a^A, \boldsymbol{V}_a^B$ such that

$$|\Psi_a\rangle = \boldsymbol{V}_a^A \otimes \boldsymbol{V}_a^B \left(\frac{\left(\boldsymbol{E}_a^A \otimes \boldsymbol{I}\right)|\Psi\rangle}{\langle\Psi|\left(\boldsymbol{E}_a^A \otimes \boldsymbol{I}\right)|\Psi\rangle^{1/2}}\right) \tag{2.145}$$

for each a, and furthermore, both Alice's measurement and Bob's yield outcome a with the same probability. This means that instead of Bob doing the measurement, the same effect can be achieved if Alice measures instead, tells Bob the outcome, and both Alice and Bob perform the appropriate unitary transformations. Construct $\boldsymbol{E}_a^A$ (this is most conveniently done by expressing both $\boldsymbol{E}_a^A$ and $\boldsymbol{E}_a^B$ in the Schmidt bases for $|\Psi\rangle$) and express $\boldsymbol{V}_a^A$ and $\boldsymbol{V}_a^B$ in terms of $\boldsymbol{U}_a^A$ and $\boldsymbol{U}_a^B$.

Remark: This result shows that for any protocol involving local operations and "two-way" classical communication (2-LOCC) that transforms an initial bipartite pure state to a final bipartite pure state, the same transformation can be achieved by a "one-way" (1-LOCC) protocol in which all classical communication is from Alice to Bob (the *Lo-Popescu Theorem*). In a two-way LOCC protocol, Alice and Bob take turns manipulating the state for some finite (but arbitrarily large) number of rounds. In each round, one party or the other performs a measurement on her/his local system and

broadcasts the outcome to the other party. Either party might use a local "ancilla" system in performing the measurement, but we may include all ancillas used during the protocol in the bipartite pure state $|\Psi\rangle$. Though a party might discard information about the measurement outcome, or fail to broadcast the information to the other party, we are entitled to imagine that the complete information about the outcomes is known to both parties at each step (incomplete information is just equivalent to the special case in which the parties choose not to use all the information). Thus the state is pure after each step.

The solution to the exercise shows that a round of a 2-LOCC protocol in which Bob measures can be simulated by an operation performed by Alice and a local unitary applied by Bob. Thus, we can allow Alice to perform all the measurements herself. When she is through she sends all the outcomes to Bob, and he can apply the necessary product of unitary transformations to complete the protocol.

2.10 The power of noncontextuality

We may regard a quantum state as an assignment of probabilities to projection operators. That is, according to Born's rule, if $\boldsymbol{\rho}$ is a density operator and $\boldsymbol{E}$ is a projector, then $p(\boldsymbol{E}) = \mathrm{tr}\,(\boldsymbol{\rho}\boldsymbol{E})$ is the probability that the outcome $\boldsymbol{E}$ occurs, if $\boldsymbol{E}$ is one of a complete set of orthogonal projectors associated with a particular quantum measurement. A notable feature of this rule is that the assignment of a probability $p(\boldsymbol{E})$ to $\boldsymbol{E}$ is *noncontextual*. This means that, while the probability $p(\boldsymbol{E})$ depends on the state $\boldsymbol{\rho}$, it does not depend on how we choose the rest of the projectors that complete the orthogonal set containing $\boldsymbol{E}$.

In a *hidden variable theory*, the probabilistic description of quantum measurement is derived from a more fundamental and complete deterministic description. The outcome of a measurement could be perfectly predicted if the values of the hidden variables were precisely known – then the probability $p(\boldsymbol{E})$ could take only the values 0 and 1. The standard probabilistic predictions of quantum theory arise when we average over the unknown values of the hidden variables. The purpose of this exercise is to show that such deterministic assignments conflict with noncontextuality. Thus a hidden variable theory, if it is to agree with the predictions of quantum theory after averaging, must be contextual.

Let $\{\boldsymbol{I}, \boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}\}$ denote the single-qubit observables

$$\begin{aligned} \boldsymbol{I} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \boldsymbol{Y} &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \boldsymbol{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \end{aligned} \tag{2.146}$$

and consider the nine two-qubit observables:

$$\begin{array}{ccc} \boldsymbol{X} \otimes \boldsymbol{I} & \boldsymbol{I} \otimes \boldsymbol{X} & \boldsymbol{X} \otimes \boldsymbol{X} \\ \boldsymbol{I} \otimes \boldsymbol{Y} & \boldsymbol{Y} \otimes \boldsymbol{I} & \boldsymbol{Y} \otimes \boldsymbol{Y} \\ \boldsymbol{X} \otimes \boldsymbol{Y} & \boldsymbol{Y} \otimes \boldsymbol{X} & \boldsymbol{Z} \otimes \boldsymbol{Z} \end{array} . \tag{2.147}$$

The three observables in each row and in each column are mutually commuting, and so can be simultaneously diagonalized. In fact the simultaneous eigenstates of any two operators in a row or column (the third operator is not independent of the other two) are a complete basis for the four-dimensional Hilbert space of the two qubits. Thus we can regard the array eq.(2.147) as a way of presenting six different ways to choose a complete set of one-dimensional projectors for two qubits.

Each of these observables has eigenvalues ± 1, so that in a deterministic and noncontextual model of measurement (for a fixed value of the hidden variables), each can be assigned a definite value, either $+1$ or -1.

a) Any noncontextual deterministic assignment has to be consistent with the multiplicative structure of the observables. For example, the product of the three observables in the top row is the identity $\boldsymbol{I} \otimes \boldsymbol{I}$. Therefore, if we assign a value ± 1 to each operator, the number of -1's assigned to the first row must be even. Compute the product of the three observables in each row and each column to find the corresponding constraints.

b) Show that there is no way to satisfy all six constraints simultaneously.

Thus a deterministic and noncontextual assignment does not exist.

2.11 Schmidt-decomposable states

We saw in class that any vector in a bipartite Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed in the *Schmidt form*: Given the vector $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are both N-dimensional, we

can choose orthonormal bases $\{|i\rangle_A\}$ for $\mathcal{H}_A$ and $\{|i\rangle_B\}$ for $\mathcal{H}_B$ so that

$$|\psi\rangle_{AB} = \sum_{i=1}^{N} \sqrt{\lambda_i}\ |i\rangle_A \otimes |i\rangle_B, \tag{2.148}$$

where the λ_i's are real and nonnegative. (We're not assuming here that the vector has unit norm, so the sum of the λ_i's is not constrained.) Eq.(2.148) is called the *Schmidt decomposition* of the vector $|\psi\rangle_{AB}$. Of course, the bases in which the vector has the Schmidt form depend on which vector $|\psi\rangle_{AB}$ is being decomposed.

A unitary transformation acting on $\mathcal{H}_{AB}$ is called a *local unitary* if it is a tensor product $\boldsymbol{U}_A \otimes \boldsymbol{U}_B$, where $\boldsymbol{U}_A$, $\boldsymbol{U}_B$ are unitary transformations acting on $\mathcal{H}_A$, $\mathcal{H}_B$ respectively. The word "local" is used because if the two parts A and B of the system are widely separated from one another, so that Alice can access only part A and Bob can access only part B, then Alice and Bob can apply this transformation by each acting locally on her or his part.

a) Now suppose that Alice and Bob choose standard fixed bases $\{|i\rangle_A\}$ and $\{|i\rangle_B\}$ for their respective Hilbert spaces, and are presented with a vector $|\psi_{AB}\rangle$ that is not necessarily in the Schmidt form when expressed in the standard bases. Show that there is a local unitary $\boldsymbol{U}_A \otimes \boldsymbol{U}_B$ that Alice and Bob can apply so that the resulting vector

$$|\psi\rangle'_{AB} = \boldsymbol{U}_A \otimes \boldsymbol{U}_B |\psi\rangle_{AB} \tag{2.149}$$

does have the form eq.(2.148) when expressed in the standard bases.

b) Let's verify that the result of (*a*) makes sense from the point of view of parameter counting. For a *generic* vector in the Schmidt form, all λ_i's are nonvanishing and no two λ_i's are equal. Consider the *orbit* that is generated by letting arbitrary local unitaries act on one fixed generic vector in the Schmidt form. What is the dimension of the orbit, that is, how many real parameters are needed to specify one particular vector on the orbit? (**Hint**: To do the counting, consider the local unitaries that differ infinitesimally from the identity $\boldsymbol{I}_A \otimes \boldsymbol{I}_B$. Choose a basis for these, and count the number of independent linear combinations of the basis elements that annihilate the Schmidt-decomposed vector.) Compare the dimension of the orbit to the (real) dimension of $\mathcal{H}_{AB}$, and check the consistency with the number of free parameters in eq.(2.148).

A vector $|\psi\rangle_{A_1 \ldots A_r}$ in a Hilbert space $\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_r}$ with r parts is said to be *Schmidt decomposable* if it is possible to choose orthonormal bases for $\mathcal{H}_{A_1}, \ldots \mathcal{H}_{A_r}$ such that vector can be expressed as

$$|\psi\rangle_{A_1 \ldots A_r} = \sum_i \sqrt{\lambda_i}\ |i\rangle_{A_1} \otimes |i\rangle_{A_2} \otimes \cdots \otimes |i\rangle_{A_r}. \tag{2.150}$$

Though every vector in a bipartite Hilbert space is Schmidt decomposable, this isn't true for vectors in Hilbert spaces with three or more parts.

c) Consider a generic Schmidt-decomposable vector in the tripartite Hilbert space of three qubits. Find the dimension of the orbit generated by local unitaries acting on this vector.

d) By considering the number of free parameters in the Schmidt form eq.(2.150), and the result of (*c*), find the (real) dimension of the space of Schmidt-decomposable vectors for three qubits. What is the real *codimension* of this space in the three-qubit Hilbert space $\mathbb{C}^8$?