PHY265 Lecture notes: Introducing Quantum Systems, Measurement and the Qubit!

A. C. Quillen

February 8, 2024

Contents

1 Introduction

The goal of these notes is not to teach quantum mechanics but introduce the frame work for quantum mechanics well enough that we can explore concepts of quantum computing, quantum information and quantum simulation. Quantum computers are now a reality, and they continue to be improved. A significant fraction of research effort in physics is now devoted to various aspects of quantum computing. They have inspired new ideas in information theory and new types of algorithms. Quantum computers may turn out to be useful.

2 Basis vectors and quantum states

For our purpose, a Hilbert space is a **complex vector space** that has an **inner product**. A Hilbert space has in addition a requirement that it is a complete metric space, but as we will primarily be working with finite dimensional Hilbert spaces, we are essentially working with complex vector spaces that have an inner product. Because it is more concise, we will refer to a "N-dimensional complex vector space with an inner product" as an "N-dimensional Hilbert space". A set of vectors B for which every element of a complex vector space V can be written uniquely as a linear combination of vectors in B is called a **basis** for V. An orthogonal basis in our Hilbert space is one where the basis vectors $|a_i\rangle$ satisfy

$$\langle a_i|a_j\rangle = 0 \qquad \text{if} \qquad i \neq j$$

Here we are indexing the different basis vectors with an integer index i and $i \in \{0, 1, ..., N-1\}$ where N is the dimension of the Hilbert space. I have immediately introduced the inner product, denoted $\langle|\rangle$, which is a bilinear function that takes two vectors and gives a complex number.

With an **orthonormal** basis

$$\langle a_i|a_j\rangle = \delta_{ij}$$

where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$.

A quantum state (which we often call a state vector) is a vector

$$|\psi\rangle = \sum_i c_i |a_i\rangle ,$$

where c_i are a series of complex numbers which specify the state. Here the sum is over $i = 0$ to $i = N - 1$ where N is the dimension of the vector space.

The symbol $|\psi\rangle$ we call a ket. The symbol $\langle\psi|$ is called a bra. Both are vectors. The notation is called Dirac notation. We can map a ket into a bra vector by taking its complex conjugate

$$\langle\psi| = \sum_i \langle a_i| c_i^*.$$

Here c_i^* is the complex conjugate of the complex number c_i. If $c_i = x + iy$ then $c_i^* = x - iy$ for x, y real numbers.

Suppose we have two states

$$|\psi\rangle = \sum_i c_i |a_i\rangle$$
$$|\phi\rangle = \sum_i d_i |a_i\rangle$$

The inner product is a bra-ket and is

$$\langle\phi|\psi\rangle = \sum_i d_i^* c_i \tag{1}$$

An **inner product** is a map from $V \times V$ (where V is our vector space) to $\mathbb{C}$ such that for all vectors $|\psi\rangle, |\phi\rangle$ (not necessarily normalized), the map is

- Linear in the second argument. That means that $\langle\psi|\lambda\phi\rangle = \lambda\langle\psi|\phi\rangle$ for any complex number λ and all vectors $|\psi\rangle, |\phi\rangle$. Also $\langle\psi|\phi+\phi'\rangle = \langle\psi|\phi\rangle + \langle\psi|\phi'\rangle$.
- Satisfies $\langle\psi|\phi\rangle = (\langle\phi|\psi\rangle)^*$. This is known as conjugate symmetry. Reversing the order of the arguments is equivalent to taking the complex conjugate.
- Satisfies $\langle\phi|\phi\rangle \geq 0$. Because of conjugate symmetry, this must be a real number. Also, you get zero only when $|\phi\rangle = 0$. The inner product of a vector with itself is positive. You can assign a length to a vector by computing the inner product of the vector with itself and taking the square root of the result. The inner product is said to be **positive definite**.

To show the inner product. I have used $\langle|\rangle$, which is called a *bra-ket*.

In summary, with an orthonormal basis for a Hilbert space with basis vectors the set $\{\langle a_i|\}$, (satisfying $\langle a_i|a_j\rangle = \delta_{ij}$ and with $i \in \{0, 1, ..., N-1\}$) we can write

$$\begin{aligned} |\psi\rangle &= \sum_i c_i |a_i\rangle \\ \langle\psi| &= \sum_i \langle a_i| c_i^*. \end{aligned} \tag{2}$$

Here the c_i are complex numbers and c_i^* are their complex conjugates. We use $\{\}$ to denote a set.

A **wave-vector** or **quantum state** or a **state vector** $|\psi\rangle$ (as defined in equation 2) is a normalized vector;

$$\langle\psi|\psi\rangle = \sum_i c_i c_i^* = 1.$$

In other words, it is a vector that has length 1. Each real number $c_i c_i^*$ must be greater or equal to zero and is associated with the **probability** to be in state $|a_i\rangle$. Quantum mechanics postulates that the world is described with probabilities of knowing something rather than absolutely knowing the position or state in which that object resides.

The ket or $|\psi\rangle = \sum_i c_i |a_i\rangle$ can also be written as a vertical or column vector

$$|\psi\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ . \\ c_{N-1} \end{pmatrix}$$

where N is the dimension of the Hilbert space. The bra or $\langle\psi|$ can be written as horizontal or row vector

$$\langle\psi| = \begin{pmatrix} c_0^* & c_1^* & c_2^* & ...c_{N-1}^* & . \end{pmatrix}$$

The inner product resembles a dot product

$$\begin{aligned} \langle\psi|\psi\rangle &= \begin{pmatrix} c_0^* & c_1^* & c_2^* & ...c_{N-1}^* \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ . \\ . \\ c_{N-1} \end{pmatrix} \\ &= (c_0^*, c_1^*, c_2^*...) \cdot (c_0, c_1, c_2...) \\ &= \sum_{i=0}^{N-1} c_i^* c_i \end{aligned}$$

A state vector can be normalized by computing the inner product. If $|\phi\rangle = \sum_j d_i |a_i\rangle$ is not normalized then to normalized it we divide by its length

$$\frac{|\phi\rangle}{\sqrt{\langle\phi|\phi\rangle}} = \sum_i \frac{d_i}{\sqrt{\sum_j d_j^* d_j}} |a_i\rangle .$$

Here and in many places below the sum over i goes from 0 to $N-1$ where N is the dimension of the vector space.

2.1 Linear operators

A linear operator on a state vector can be written as a matrix. This is called its matrix representation. In a 2-state system, an orthonormal basis

$$|a_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |a_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

In this basis, we can write a vector

$$\begin{aligned} |\psi\rangle &= c_0 |a_0\rangle + c_1 |a_1\rangle \\ &= \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \end{aligned}$$

With $c_0, c_1 \neq 0$, the state $|\psi\rangle$ is described as a **superposition** of two states $|a_0\rangle, |a_1\rangle$.

A linear operator $\mathbf{A}$ in the two state system is a 2×2 matrix,

$$\mathbf{A} = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix}.$$

This form is the matrix representation of $\mathbf{A}$ in the basis $\{|a_0\rangle, |a_1\rangle\}$.

The operator $\mathbf{A}$ operates on a state vector, giving another state vector,

$$\mathbf{A} |\psi\rangle = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} = \begin{pmatrix} A_{00}c_0 + A_{01}c_1 \\ A_{10}c_0 + A_{11}c_1 \end{pmatrix}$$

We can also write

$$\mathbf{A} = \sum_{ij} A_{ij} |a_i\rangle \langle a_j| \tag{3}$$

where A_{ij} is the matrix value in the i-th row and j-th column and the set $\{|a_i\rangle\}$ are vectors from an orthonormal basis. Equivalently to equation 3

$$A_{ij} = \langle a_i| \mathbf{A} |a_j\rangle. \tag{4}$$

If we operate on a state vector $|\psi\rangle = \sum_k c_k |a_k\rangle$ with $\mathbf{A}$

$$\begin{aligned} \mathbf{A} |\psi\rangle &= \sum_{ij} A_{ij} |a_i\rangle \langle a_j| \sum_k c_k |a_k\rangle \\ &= \sum_{ijk} A_{ij} |a_i\rangle c_k \delta_{jk} = \sum_{ij} A_{ij} c_j |a_i\rangle. \end{aligned}$$

We could also write

$$\mathbf{A} |\psi\rangle = \sum_i f_i |a_i\rangle$$

with complex coefficients

$$f_i = \sum_j A_{ij} c_j.$$

In an orthonormal basis with basis vectors $|a_i\rangle$ the identity matrix

$$\mathbf{I} = \sum_{i=0}^{N-1} |a_i\rangle \langle a_i|$$

This makes sense as its coefficients are $I_{ij} = \delta_{ij}$. In 3 dimensions

$$\mathbf{I} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Let state vectors

$$\begin{aligned} |\psi\rangle &= \sum_i c_i |a_i\rangle \\ |\phi\rangle &= \sum_i d_i |a_i\rangle \end{aligned}$$

and linear operator

$$\mathbf{A} = \sum_{ij} A_{ij} |a_i\rangle \langle a_i| .$$

Let's compute the inner product

$$\begin{aligned} \langle\phi| \mathbf{A} |\psi\rangle &= \sum_k d_k^* |a_k\rangle \sum_{ij} A_{ij} c_j |a_i\rangle \\ &= \sum_{ijk} \delta_{ki} d_k^* A_{ij} c_j \\ &= \sum_{ij} d_i^* A_{ij} c_j. \end{aligned} \tag{5}$$

For example, in a two dimensional Hilbert space with

$$\begin{aligned} |\psi\rangle &= \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \\ |\phi\rangle &= \begin{pmatrix} d_0 \\ d_1 \end{pmatrix} \\ \langle\phi| &= \begin{pmatrix} d_0^* & d_1^* \end{pmatrix} \\ \mathbf{A} &= \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \end{aligned}$$

in matrix notation

$$\begin{aligned}\langle\phi|\,\mathbf{A}\,|\psi\rangle &= \begin{pmatrix} d_0^* & d_1^* \end{pmatrix} \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \end{pmatrix} \\ &= d_0^* A_{00} c_0 + d_0^* A_{01} c_1 + d_1^* A_{10} c_0 + d_1^* A_{11} c_1.\end{aligned}$$

For two complex numbers z, w, we can check that $(zw)^* = z^* w^*$. This follows as

$$\begin{aligned}\overline{(a+bi)}\,\overline{(c+di)} &= (a-bi)(c-di) = ac - bd - (ad+bc)i \\ \overline{(a+bi)(c+di)} &= \overline{ac - bd + (ad+bc)i} = ac - bd - (ad+bc)i\end{aligned}$$

where I am using the overline to represent complex conjugation and a, b, c, d are real numbers.

Equivalently we can use a polar form. Let $z = ae^{i\alpha}$ with $|z| = a$ and $w = be^{i\beta}$ with $|w| = b$ and a, b, α, β are real numbers. Then

$$\begin{aligned} z &= ae^{i\alpha} \qquad z^* = ae^{-i\alpha} \\ w &= be^{i\beta} \qquad w^* = be^{-i\beta} \\ (zw)^* &= \overline{ae^{i\alpha}be^{i\beta}} = \overline{abe^{i(\alpha+\beta)}} = abe^{-i(\alpha+\beta)} \\ &= ae^{-i\alpha}be^{-i\beta} = z^* w^*. \end{aligned}$$

What is $\langle(\mathbf{A}\psi)|$?

We note that

$$\langle\phi|\psi\rangle^* = \langle\psi|\phi\rangle$$

for any two vectors. Reversing the order in the inner product is equivalent to computing the complex conjugate of the inner product. Using equation 5.

$$\begin{aligned}\langle(\mathbf{A}\psi)|\phi\rangle &= \langle\phi|\mathbf{A}\psi\rangle^* \\ &= \left(\sum_{ij} d_i^* A_{ij} c_j\right)^* \\ &= \sum_{ij} d_i A_{ij}^* c_j^* \\ &= \sum_{ij} c_j^* A_{ji}^* d_i. \end{aligned} \tag{6}$$

The matrix in the middle is transposed and conjugated. We have a special symbol for it, $\mathbf{A}^\dagger$ is the **complex transpose** (or Hermitian adjoint) of A and it looks like

$$\mathbf{A}^\dagger = \sum_{ij} A_{ji}^* \,|a_i\rangle\,\langle a_j|\,. \tag{7}$$

For example

$$\begin{pmatrix}1 & i\\ 0 & 1+i\end{pmatrix}^{\dagger} = \begin{pmatrix}1 & 0\\ -i & 1-i\end{pmatrix}.$$

You transpose the matrix (flip it across its diagonal) and take the complex conjugate of every entry. Note that $(\mathbf{A}^{\dagger})^{\dagger} = \mathbf{A}$.

Equation 6 implies that

$$\langle (\mathbf{A}\psi) | \phi \rangle = \langle \psi | \, \mathbf{A}^{\dagger} \, | \phi \rangle$$

or

$$\left\langle (\mathbf{B}^{\dagger}\psi) \middle| \phi \right\rangle = \langle \psi | \, \mathbf{B} \, | \phi \rangle$$

for any linear operators $\mathbf{A}, \mathbf{B}$ and any two state-vectors $|\psi\rangle$ and $|\phi\rangle$.

You can move an operator from one side of an inner product to the other side by taking the Hermitian adjoint (transpose conjugate) of the operator. Often the bra form of the vector $|\mathbf{A}\psi\rangle$ is written as $\langle \psi | \, \mathbf{A}^{\dagger}$.

2.2 Hermitian operators

A Hamiltonian matrix is a **Hermitian** or **self-adjoint** matrix. A Hermitian matrix satisfies

$$\mathbf{A}^{\dagger} = \mathbf{A}$$

where the dagger means taking both the transpose and complex conjugate of the matrix. A Hermitian matrix is equal to the complex conjugate of its transpose.

For example with

$$\mathbf{A} = \begin{pmatrix}A_{00} & A_{01}\\ A_{10} & A_{11}\end{pmatrix} \tag{8}$$

the transpose is

$$\mathbf{A}^{t} = \begin{pmatrix}A_{00} & A_{10}\\ A_{01} & A_{11}\end{pmatrix} \tag{9}$$

and the transpose and complex conjugate of the matrix is

$$\mathbf{A}^{\dagger} = \begin{pmatrix}A_{00}^{*} & A_{10}^{*}\\ A_{01}^{*} & A_{11}^{*}\end{pmatrix} \tag{10}$$

If the matrix is Hermitian then the diagonal entries must be real, $A_{00} = A_{00}^{*}$, $A_{11} = A_{11}^{*}$ and the off-diagonals must be related via $A_{10} = A_{01}^{*}$.

For any state vector $|\psi\rangle$, the inner product $\langle\psi| \mathbf{A} |\psi\rangle$ is always a real number if $\mathbf{A}$ is Hermitian. This follows because

$$\begin{aligned}(\langle\psi|\mathbf{A}\psi\rangle)^* &= \langle\mathbf{A}\psi|\psi\rangle \\ &= \left\langle\psi\middle|\mathbf{A}^\dagger\psi\right\rangle) \\ &= \langle\psi|\mathbf{A}\psi\rangle).\end{aligned}$$

Since $\langle\psi| \mathbf{A} |\psi\rangle$ equals its own complex conjugate it must be a real number.

Observables or **quantum measurements** are represented by Hermitian matrices.

Some useful relations for linear transformations (aka operators or square matrices) for a finite dimensional Hilbert space.

- $(\mathbf{AB})^\dagger = \mathbf{B}^\dagger\mathbf{A}^\dagger$ for operators $\mathbf{A}, \mathbf{B}$.
- If $\mathbf{A}, \mathbf{B}$ are Hermitian, their product $\mathbf{AB}$ is not necessarily Hermitian.
- For any operator $\mathbf{A}$, the operator $\mathbf{AA}^\dagger$ is Hermitian, and the operator $\mathbf{A} + \mathbf{A}^\dagger$ is Hermitian.

2.3 Unitary matrices

A **unitary** matrix $\mathbf{U}$ is a complex square matrix that satisfies

$$\mathbf{UU}^\dagger = \mathbf{U}^\dagger\mathbf{U} = \mathbf{I}$$

with $\mathbf{I}$ the identity matrix. A unitary transformation preserves the norm of the state vector $|\psi\rangle$. In other words, with $\langle\psi|\psi\rangle = 1$ and $|\psi'\rangle = \mathbf{U}|\psi\rangle$ and $\mathbf{U}$ unitary, then

$$\begin{aligned}\left\langle\psi'\middle|\psi'\right\rangle &= \langle\mathbf{U}\psi|\mathbf{U}\psi\rangle \\ &= \langle\psi| \mathbf{U}^\dagger\mathbf{U} |\psi\rangle \\ &= \langle\psi| \mathbf{I} |\psi\rangle = \langle\psi|\psi\rangle = 1.\end{aligned}$$

Consider the product $\mathbf{W} = \mathbf{UV}$ where $\mathbf{U}$ and $\mathbf{V}$ are unitary. We compute

$$\begin{aligned}\mathbf{WW}^\dagger &= (\mathbf{UV})(\mathbf{UV})^\dagger \\ &= \mathbf{UVV}^\dagger\mathbf{U}^\dagger = \mathbf{UU}^\dagger = \mathbf{I}\end{aligned}$$

Likewise

$$\begin{aligned}\mathbf{W}^\dagger\mathbf{W} &= (\mathbf{UV})^\dagger(\mathbf{UV}) \\ &= \mathbf{V}^\dagger\mathbf{U}^\dagger\mathbf{UV} = \mathbf{I}\end{aligned}$$

This means that **W** is also unitary. The space of unitary operators on a finite dimensional complex vector space forms a *group*.

Evolution of a quantum state vector is often described in terms of a Hamiltonian operator. Hamiltonian evolution gives **unitary** evolution of a state vector. However a Hamiltonian is not necessarily a unitary matrix, it is Hermitian.

Hamiltonian evolution is done using the exponential of the Hamiltonian via

$$|\psi(t)\rangle = e^{-i\mathbf{H}t/\hbar} |\psi(t=0)\rangle \,, \tag{11}$$

as this is consistent with Schrödinger's equation

$$i\hbar\frac{\partial}{\partial t} |\psi\rangle = \mathbf{H} |\psi\rangle \,. \tag{12}$$

An isolated quantum mechanical system would evolve via a Hamiltonian operator **H**. We will discuss exponentials of matrices in section 3.4 below.

Unitary evolution is not random but deterministic. The coefficients of the state-vector are not randomly varied but vary in such a way that can be computed as a function of time using a unitary operator that is constructed from a Hamiltonian operator.

2.4 Expectation value

In a particular orthonormal basis, the coefficients c_i of a state vector $|\psi\rangle = \sum_i c_i |a_i\rangle$ are directly related to probabilities, with the probability of being in basis state $|a_i\rangle$ equal to $p_i = c_i c_i^*$. Even though the state vector is described as a complex vector, the probabilities are real numbers.

The expectation value of an observable **A**

$$\langle \mathbf{A} \rangle = \langle \psi | \mathbf{A} | \psi \rangle = \sum_{ij} c_i^* A_{ij} c_j .$$

The expectation value of an observable should be a real number and this implies observables should be Hermitian.

What is meant by the expectation value? Expectation values are mean values measured from of an ensemble of systems all with state vector $|\psi\rangle$. A system with the same state vector must be measured many times to find an expectation value.

For example, for state $|\psi\rangle = a|0\rangle + b|1\rangle$, aa_* can be interpreted as the probability that the state is in the $|0\rangle$ state and bb^* the probability that the state is in the $|1\rangle$ state. Consider the Hermitian matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

The expectation of $\mathbf{A}$ would be

$$\begin{aligned}\langle \mathbf{A} \rangle &= \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \\ &= a^*(a+2b) + b^*(2a+b) \\ &= a^*a + b^*b + 2(a^*b + b^*a)\end{aligned}$$

We notice that a^*a is real and b^*b is real. For any two complex numbers a, b the expression $a^*b + b^*a$ is also real. The final result is real. The expectation value of $\mathbf{A}$ would be the result of averaging measurements from many experiments of a system with this same state vector.

2.5 Projection operators

A projection operator $\mathbf{P}$ satisfies

$$\mathbf{P}^2 = \mathbf{P}.$$

The probability p_i, that a state vector ψ is in state $|a_i\rangle$ can be computed with the projection operator

$$\mathbf{P}_i = |a_i\rangle \langle a_i|$$

with $\psi = \sum_i c_i |a_i\rangle$,

$$\begin{aligned}\langle \psi | \mathbf{P}_i | \psi \rangle &= \sum_{jk} \langle a_j| \, c_j^* \ \mathbf{P}_{i,jk} \ c_k \, |a_k\rangle \\ &= \sum_{ij} \langle a_j| \, c_j^* \ \ |a_i\rangle \langle a_i| \ \ c_k \, |a_k\rangle \\ &= \sum_{ij} c_j^* \delta_{ji} \delta_{ki} c_k \\ &= c_i^* c_i = p_i.\end{aligned}$$

For example, in a 2 state system two projection operators are

$$\mathbf{P}_0 = |0\rangle \langle 0| \qquad\qquad \mathbf{P}_1 = |1\rangle \langle 1| \tag{13}$$

In matrix form

$$\mathbf{P}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad\qquad \mathbf{P}_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The set of these two projection operators $\{\mathbf{P}_0, \mathbf{P}_1\}$ is *complete* in the sense that their sum is equal to the identity matrix

$$\mathbf{P}_0 + \mathbf{P}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}.$$

These two projection operators are *orthogonal* in the sense that

$$\mathbf{P}_0\mathbf{P}_1 = \mathbf{P}_1\mathbf{P}_0 = 0.$$

We will talk more about sets of projection operators when we discuss what is meant by measurement in more detail.

2.6 Changing basis

We have been assuming that there is a specific orthonormal basis $\{|a_i\rangle\}$. Given any unitary matrix $\mathbf{U}$ we can transform each element in this orthonormal basis to give us a new set of vectors

$$|b_i\rangle = \mathbf{U}\,|a_i\rangle\,.$$

The new set of vectors is also an orthonormal set of basis vectors!

$$\begin{aligned}\langle b_i|b_j\rangle &= \langle \mathbf{U}a_i|\,\mathbf{U}a_j\rangle \\ &= \langle a_i|\,\mathbf{U}^\dagger\mathbf{U}\,|a_j\rangle \\ &= \langle a_i|a_j\rangle \\ &= \delta_{ij}\end{aligned}$$

Any two sets of orthonormal basis vectors that span a complex vector space can be related via a unitary transformation. Suppose we have two sets of orthonormal basis vectors $\{|a_i\rangle\}, \{|b_i\rangle\}$. We want to find $\mathbf{U}$ such that $|b_i\rangle = \mathbf{U}\,|a_i\rangle$. We compute the inner product

$$\langle a_j|b_i\rangle = \langle a_j|\,\mathbf{U}\,|a_i\rangle \tag{14}$$

With the two sets of orthonormal vectors, we can compute the left hand side for all i, j. Recall that we can write in bra-ket notation as $\mathbf{U} = \sum_{ij} U_{ij}\,|a_i\rangle\,\langle a_j|$. The right hand side of equation 14 gives us the components of $\mathbf{U}$ in the $|a_i\rangle$ basis.

2.7 The spectral theorem

The spectral theorem (which we are not proving here) states that a Hermitian matrix is diagonalizable. This means that for any Hermitian matrix $\mathbf{A}$ it is possible to find a unitary matrix $\mathbf{U}$ such that

$$\mathbf{A} = \mathbf{U}\mathbf{\Lambda}\mathbf{U}^\dagger \tag{15}$$

where $\mathbf{\Lambda}$ is a matrix that only has values on the diagonal.

An eigenvalue λ_i and an eigenvector $|b_i\rangle$ of a matrix $\mathbf{A}$ satisfy

$$\mathbf{A}\,|b_i\rangle = \lambda_i\,|b_i\rangle\,.$$

Given unitary matrix $\mathbf{U}$ that diagonalizes $\mathbf{A}$ in an orthonormal basis $\{|a_i\rangle\}$, we show that the eigenvectors of $\mathbf{A}$ are

$$|b_i\rangle = \mathbf{U}\,|a_i\rangle\,. \tag{16}$$

Apply $\mathbf{A}$ onto this vector (and use equation 15)

$$\begin{aligned}\mathbf{A}\,|b_i\rangle &= \mathbf{U\Lambda U}^\dagger\mathbf{U}\,|a_i\rangle\\ &= \mathbf{U\Lambda}\,|a_i\rangle\\ &= \mathbf{U}\lambda_i\,|a_i\rangle\\ &= \lambda_i\,|b_i\rangle\,.\end{aligned}$$

Here we assume that the diagonal matrix is in order λ_0, λ_1..... We have shown that $|b_i\rangle$ are eigenvectors.

Looking again at equation 16 for the eigenvectors:

$$|b_i\rangle = \mathbf{U}\,|a_i\rangle\,.$$

This implies that the rows of $\mathbf{U}$ are the eigenvectors. To see this another way consider

$$\begin{pmatrix}\text{first} & .. & \text{row}\\ \text{second} & .. & \text{row}\\ \text{third} & .. & \text{row}\\ \text{fourth} & .. & \text{row}\\ . & . & .\\ . & . & .\\ . & . & .\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\\0\\.\\.\end{pmatrix}$$

In an orthogonal basis $|a_i\rangle$ is a column vector that is all zeros with a single 1 at the i-th row. U times this vector gives the i-th row of U.

Since $\mathbf{U}$ gives an orthonormal basis, we know that the eigenvectors found from the rows of a unitary matrix are all perpendicular and normalized so that they have length 1. In the orthonormal basis given by these eigenvectors, the operator $\mathbf{A}$ is diagonal.

In summary, for $\mathbf{A}$ Hermitian, and $\mathbf{U}$ the unitary matrix that diagonalizes it with $\mathbf{\Lambda}$ the diagonal matrix in equation 15, the values on the diagonal in $\mathbf{\Lambda}$ are the eigenvalues of $\mathbf{A}$ and the rows of the unitary matrix $\mathbf{U}$ are the eigenvectors.

Two eigenvectors of a Hermitian matrix with different eigenvalues are always perpendicular. However if the diagonal matrix $\mathbf{\Lambda}$ has two eigenvectors that are the same, then there are multiple ways to chose linearly independent eigenvectors.

The spectral theorem extends to a more general class of matrices than Hermitian matrices. The spectral theorem more generally applies to **normal matrices** which satisfy $\mathbf{AA}^\dagger = \mathbf{A}^\dagger\mathbf{A}$. This means that for any normal matrix $\mathbf{A}$, there is a unitary matrix $\mathbf{U}$ that gives $\mathbf{A} = \mathbf{U\Lambda U}^\dagger$ with $\mathbf{\Lambda}$ a diagonal matrix. Unitary matrices are not necessarily

Hermitian but they are normal matrices. This means that unitary matrices themselves can be diagonalized.

The spectral theorem is related to the Schur decomposition and the singular value decomposition. The Schur decomposition states that an arbitrary complex square matrix is unitarily equivalent to an upper triangular matrix whose diagonal elements are the eigenvalues of the original matrix. The singular value decomposition of an $m \times n$ complex matrix $\mathbf{M}$ is a factorization of the form $\mathbf{M} = \mathbf{U\Sigma V}^\dagger$ where $\mathbf{U}$ is a unitary $m \times m$ matrix, $\mathbf{V}$ is a unitary $n \times n$ matrix and $\mathbf{\Sigma}$ is an $m \times n$ rectangular diagonal matrix with non-negative real numbers on the diagonal.

3 The qubit

A two state quantum system can be described with state vector

$$\begin{aligned} |\psi\rangle &= a\,|0\rangle + b\,|1\rangle \\ \langle\psi| &= \langle 0|\,a^* + \langle 1|\,b^* \end{aligned}$$

where $|0\rangle$ and $|1\rangle$ are the two energy states. You can also think of a particle with spin up and spin down as a two energy state object. Here we take $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$. This is a building block for many quantum computer designs and is called a qubit or q-bit.

In vector notation the first state and second states are

$$|0\rangle = \left(\begin{array}{c} 1 \\ 0 \end{array} \right) \qquad |1\rangle = \left(\begin{array}{c} 0 \\ 1 \end{array} \right).$$

Consider the operator

$$\boldsymbol{\sigma}_z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\,\langle 0| - |1\rangle\,\langle 1| \tag{17}$$

which is called the Pauli-Z matrix. Note that

$$\begin{aligned} \boldsymbol{\sigma}_z\,|0\rangle &= |0\rangle \\ \boldsymbol{\sigma}_z\,|1\rangle &= -\,|1\rangle \end{aligned}$$

The eigenvalues of the Pauli Z matrix are 1,-1 and its eigenvectors are $|0\rangle\,, |1\rangle$.

We look at a state vector in this basis

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \left(\begin{array}{c} a \\ b \end{array} \right). \tag{18}$$

Coefficients a, b are both complex numbers, but the vector is normalized so that

$$aa^* + bb^* = 1.$$

A state ψ is described by two complex numbers a, b. Each one has a real and a complex part. This gives a four dimensional space. As $\langle\psi|\psi\rangle = 1$, the sum

$$\mathrm{Re}(a)^2 + \mathrm{Im}(a)^2 + \mathrm{Re}(b)^2 + \mathrm{Im}(b)^2 = 1$$

restricting the space to a 3d spherical surface in this 4d space.

3.1 Global phase

We consider two quantum states $|\psi\rangle$ and $|\psi'\rangle$ which are related by a phase ϕ;

$$\left|\psi'\right\rangle = e^{i\phi}\left|\psi\right\rangle$$

We make a measurement, for example, by computing the expectation value of an observable $\mathbf{A}$,

$$\begin{aligned} \left\langle\psi'\right|\mathbf{A}\left|\psi'\right\rangle &= e^{-i\phi}\left\langle\psi\right|\mathbf{A}\left|\psi\right\rangle e^{i\phi} && (19)\\ &= \left\langle\psi\right|\mathbf{A}\left|\psi\right\rangle && (20) \end{aligned}$$

The expectation value is not changed by the factor $e^{i\phi}$ which we call a global phase.

Global phase is unobservable whereas *relative phase* is observable. Global means we can multiply the entire state by $e^{i\phi}$ and we would not see any difference in our measurements. By *relative phase* we mean one component in a superposition state is multiplied by a phase.

3.2 The Bloch Sphere

For a qubit it is convenient to define

$$\begin{aligned} \left|+\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)\\ \left|-\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)\\ \left|i\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle + i\left|1\right\rangle)\\ \left|-i\right\rangle &= \frac{1}{\sqrt{2}}(\left|0\right\rangle - i\left|1\right\rangle) \end{aligned}$$

The two states $\frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$ and $\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$ have different *relative* phases. We could rotate the states and then measure their spin. We would measure different spin values in these rotated states. Relative phase is observable.

By adjusting the global phase we can take a state vector

$$\left|\psi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$$

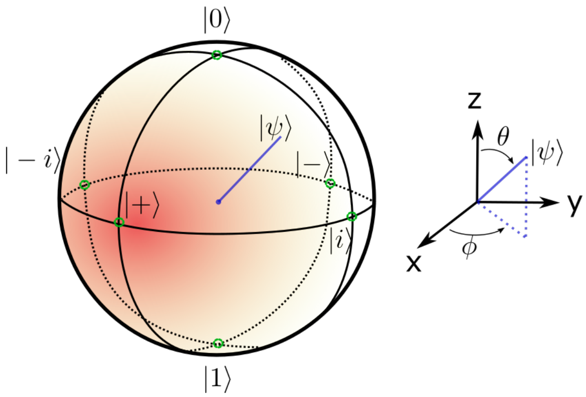

Figure 1: The Bloch sphere.

and write it as

$$\left|\psi'\right\rangle = a' \left|0\right\rangle + b' e^{i\phi} \left|1\right\rangle$$

with a', b' both real and $a' \geq 0$. We do this by multiplying by $a^*/|a|$.

The map onto the Bloch sphere

$$|\psi\rangle \xrightarrow{\boldsymbol{\pi}} |\psi'\rangle$$

with map $\boldsymbol{\pi}$

$$a, b \xrightarrow{\boldsymbol{\pi}} a', b'$$

given by

$$\begin{aligned} a' &= |a| \\ b' &= \frac{|ba^*|}{|a|} \\ \phi &= \operatorname{arctan2}(\operatorname{Im}(ba^*), \operatorname{Re}(ba^*)) \end{aligned}$$

The map is a projection as $\boldsymbol{\pi}^2 = \boldsymbol{\pi}$. In other words $\boldsymbol{\pi}(\boldsymbol{\pi}(|\psi\rangle)) = \boldsymbol{\pi}(|\psi\rangle)$.

The state vector has a norm of 1 so we we can find an angle θ with

$$\left|\psi'\right\rangle = \cos(\theta/2) \left|0\right\rangle + \sin(\theta/2) e^{i\phi} \left|1\right\rangle . \tag{21}$$

The factor of 2 within the cosine and sine lets us associate θ with a **co-latitude** on a sphere. The angles

$$\theta \in [0, \pi] \qquad \phi \in [0, 2\pi)$$

with ϕ acting like a **longitude**. With $\theta \in [0, \pi]$ the factor $\cos(\theta/2)$ ranges from 1 to 0. This means we have chosen a global phase that keeps a' positive!

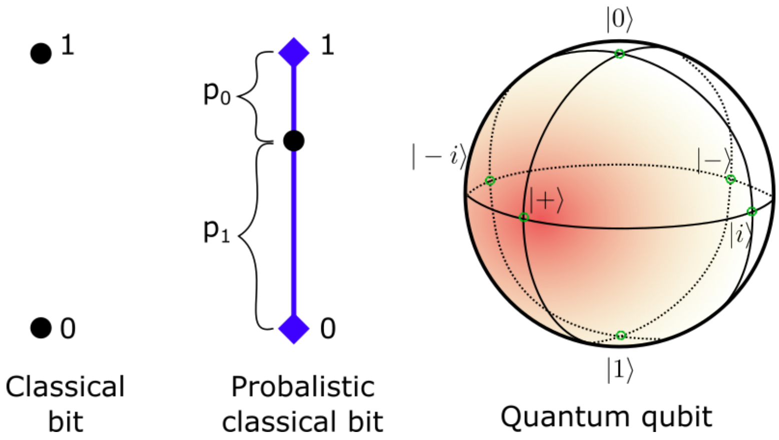

Figure 2: We compare the degrees of freedom in a classical bit to a quantum bit. A classical bit can be one of two states, 0 or 1. A more complex but still classical setting might be a **probabilistic classical bit** which is described by a probability p_0 that the bit is 0 and a probability p_1 that the bit is 1 with $p_0 + p_1 = 1$. The bit spans the unit interval as $p_0 \in [0, 1]$. The quantum qubit spans the Bloch sphere.

Any point on the Bloch sphere can be written in the form of equation 21. You can always find angles $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$ to describe any point on the Bloch sphere in the form of equation 21.

We can describe the state vector as a point on the sphere, or with unit vector

$$(x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta). \tag{22}$$

This makes it clear that we can directly relate any qubit state vector to a point on a sphere. The projection $\boldsymbol{\pi}$ to the Bloch sphere can also described as a map from complex numbers a, b that are normalized so that $aa^* + bb* = 1$ to angles θ, ϕ,

$$a, b \xrightarrow{\boldsymbol{\pi}} \theta, \phi$$

given by

$$\frac{\theta}{2} = \text{arctan2}(b', a') = \text{arctan2}(|b|, |a|)$$
$$\phi = \text{arctan2}(\text{Im}(ba^*), \text{Re}(ba^*)).$$

A general qubit state $|\psi\rangle$ depends on two complex numbers, giving 4 degrees of freedom, when counting each real and complex part of the two complex numbers. However $\langle\psi|\psi\rangle = 1$ reduces the degrees of freedom by 1. There is a redundant phase. If we drop it by projecting onto the Bloch sphere, then this reduces the dimension again. This is why the Bloch sphere is a 2-d object, and is a sphere in 3d rather than a 3-sphere embedded in 4-dimensions, like the qubit prior to projection onto the Bloch sphere.

Points 180° apart on the Bloch sphere are orthogonal states. Two points that are 180° are called **antipodal**. The spin up/down pair $|0\rangle, |1\rangle$ are orthogonal states. Likewise $|+\rangle, |-\rangle$ and $|i\rangle, |-i\rangle$ are pairs of orthogonal states. These six states are 6 equidistant poles on the Bloch sphere. We could also rotate into another basis and find a different set of 3 pairs of points.

Question: What are the θ, ϕ angles and x, y, z coordinates for the 6 states $|0\rangle, |1\rangle$, $|+\rangle, |-\rangle$, $|i\rangle, |-i\rangle$, on the Bloch sphere?

Answer: Here is a table:

Points on the Bloch sphere				
State		θ	ϕ	(x,y,z)
$\|0\rangle$		0	-	(0,0,1)
$\|1\rangle$		π	0	(0,0,-1)
$\|+\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\pi/2$	0	(1,0,0)
$\|-\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\pi/2$	π	(-1,0,0)
$\|i\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\pi/2$	$\pi/2$	(0,1,0)
$\|-i\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$	$\pi/2$	$-\pi/2$	(0,-1,0)

The spin up and down states $|0\rangle, |1\rangle$ are eigenvectors of $\boldsymbol{\sigma}_z$.

Question: How do the Pauli spin matrices, $\boldsymbol{\sigma}_x, \boldsymbol{\sigma}_y, \boldsymbol{\sigma}_z$ operate on the 6 states $|0\rangle, |1\rangle$, $|+\rangle, |-\rangle$, $|i\rangle, |-i\rangle$?

$$\boldsymbol{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \boldsymbol{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \boldsymbol{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Answer: here is a table:

	Action of Pauli Matrices		
$\|\psi\rangle$	$\boldsymbol{\sigma}_x\|\psi\rangle$	$\boldsymbol{\sigma}_y\|\psi\rangle$	$\boldsymbol{\sigma}_z\|\psi\rangle$
$\|0\rangle$	$\|1\rangle$	$i\|1\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$-i\|0\rangle$	$-\|1\rangle$
$\|+\rangle$	$\|+\rangle$	$-i\|-\rangle$	$\|-\rangle$
$\|-\rangle$	$-\|-\rangle$	$i\|+\rangle$	$\|+\rangle$
$\|i\rangle$	$i\|-i\rangle$	$\|i\rangle$	$\|-i\rangle$
$\|-i\rangle$	$-i\|i\rangle$	$-\|-i\rangle$	$\|i\rangle$

This table illustrates that each antipodal pair is either rotated by a Pauli matrix to another pair of antipodal points, or are eigenvectors of the Pauli matrix.

Question: Find a matrix for which the complex states $|i\rangle$ and $|-i\rangle$ are eigenvectors.
The answer is the Pauli-Y or $\boldsymbol{\sigma}_y$.

Question: Find a matrix for which the states $|+\rangle$ and $|-\rangle$ are eigenvectors.
Answer is the Pauli-X or $\boldsymbol{\sigma}_x$.

Question: Is there a way to figure this out without guessing?

Answer: Yes. Make a unitary transformation $\mathbf{U}$ to transfer from $|0\rangle, |1\rangle$ basis to $|+\rangle, |-\rangle$. This can be done with the states themselves as the pairs of states are orthonormal and rows of unitary matrices are orthonormal. Then compute $\mathbf{U}\boldsymbol{\sigma}_z\mathbf{U}^\dagger$.

3.3 Single qubit Gates

Quantum **gates** are unitary transformations. I give some examples of common quantum gates that operate on a single qubit.

Hadamard	$-\boxed{\mathrm{H}}-$	$\mathbf{H}$	$= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
NOT or Pauli-X	$-\boxed{\mathrm{X}}-$	$\boldsymbol{\sigma}_x$	$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli-Y	$-\boxed{\mathrm{Y}}-$	$\boldsymbol{\sigma}_y$	$= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli-Z	$-\boxed{\mathrm{Z}}-$	$\boldsymbol{\sigma}_z$	$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Phase $= \sqrt{\mathbf{Z}}$	$-\boxed{\mathrm{S}}-$	$\mathbf{S}$	$= \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$
$\pi/8 = \sqrt{\mathbf{S}}$	$-\boxed{\frac{\pi}{8}}-$	$\frac{\pi}{8}$	$= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

I have also include the quantum circuit symbols. The Hadamard gate takes a $|0\rangle$ and returns a $|+\rangle$ and takes a $|1\rangle$ and returns a $|-\rangle$. The Hadamard gate obeys $\mathbf{H}^2 = \mathbf{I}$. The Hadamard gate introduces **superposition** as $|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

The NOT interchanges the $|0\rangle, |1\rangle$ states. The $\pi/8$ is the square root of the Phase Gate which itself is the square root of the Pauli-Z gate.

Unitary matrices satisfy $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I}$. The rows and columns of a unitary matrix are orthonormal. The above gates are unitary matrices.

The phase gate is sometimes called P or $P_{\frac{\pi}{2}}$. The $\frac{\pi}{8}$ gate is sometimes called $P_{\frac{\pi}{4}}$. The ambiguity of a factor of 2 in the naming convention arises because of the difference between taking an exponential of a Pauli matrix and the equivalent rotation on the Bloch sphere (compare equation 25 to equation 28).

3.4 Exponentials of matrices

The exponential of a matrix $\mathbf{A}$ is

$$e^{\mathbf{A}} = \mathbf{I} + \mathbf{A} + \frac{1}{2}\mathbf{A}^2 + \frac{1}{3!}\mathbf{A}^3 .... \frac{1}{i!}\mathbf{A}^i ... \tag{23}$$

We can generate a smooth trajectory in the space of matrices with

$$e^{t\mathbf{A}} = \mathbf{I} + \sum_{i=1}^{\infty} \frac{t^i \mathbf{A}^i}{i!}, \tag{24}$$

where real number t is like time. At $t = 0$ we recover the identity matrix $\mathbf{I}$ as

$$\lim_{t \to 0} e^{t\mathbf{A}} = \mathbf{I}.$$

When applied on a vector $|\psi(t)\rangle = e^{t\mathbf{A}} |\psi\rangle$, and starting at $t = 0$, the initial condition returns $|\psi\rangle$ itself. Then as t varies we have a trajectory in the Hilbert space in which $|\psi\rangle$ lives. Unitary evolution for quantum mechanical systems is more commonly written as $e^{-it\mathbf{H}/\hbar}$ where $\mathbf{H}$ is a Hermitian matrix. Note that if operator $\mathbf{A}$ is Hermitian, then $e^{i\mathbf{A}}$ is unitary. This is easiest to see if you transfer into the basis of H where it is diagonal and all of its eigenvalues are real.

Let us compute the exponentials of the Pauli matrices. Because $\boldsymbol{\sigma}_x^2 = \boldsymbol{\sigma}_y^2 = \boldsymbol{\sigma}_z^2 = \mathbf{I}$ the exponentials of the Pauli matrices can be evaluated from the expansion in equation 23. The exponentials of the Pauli matrices are sometimes described like rotations $S_x(\alpha)$, $S_y(\alpha)$, $S_z(\alpha)$,

$$S_x(\alpha) = e^{i\alpha\boldsymbol{\sigma}_x} = \cos\alpha \; \mathbf{I} + i \sin\alpha \; \boldsymbol{\sigma}_x = \begin{pmatrix} \cos\alpha & i\sin\alpha \\ i\sin\alpha & \cos\alpha \end{pmatrix} \tag{25}$$

$$S_y(\alpha) = e^{i\alpha\boldsymbol{\sigma}_y} = \cos\alpha \; \mathbf{I} + i \sin\alpha \; \boldsymbol{\sigma}_y = \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \tag{26}$$

$$S_z(\alpha) = e^{i\alpha\boldsymbol{\sigma}_z} = \cos\alpha \; \mathbf{I} + i \sin\alpha \; \boldsymbol{\sigma}_z = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \tag{27}$$

and they are functions of an angle α. They can be considered rotations in $U(2)$, the group of 2 dimensional unitary matrices, that are generated exponentially from infinitesimal operators, the Pauli spin matrices.

The matrices $S_x(\alpha)$, $S_y(\alpha)$, $S_z(\alpha)$ are unitary transformations but they are not Hermitian.

How do these rotation matrices rotate a state on the Bloch sphere? A state on the Bloch sphere can be described in terms of two angles $\phi \in [0, 2\pi]$, $\theta \in [0, \pi)$.

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle\,.$$

We operate on it with $S_z(\alpha)$;

$$S_z(\alpha)\,|\psi\rangle = e^{i\alpha}\left(\cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i(\phi-2\alpha)}\,|1\rangle\right).$$

This is equivalent to a rotation of -2α about the z axis on the Bloch sphere. Because of the factor of two and the minus size, rotation transformations on the Bloch sphere are often defined as

$$R_x(\alpha) = e^{-i\alpha\boldsymbol{\sigma}_x/2} = \begin{pmatrix} \cos\frac{\alpha}{2} & -i\sin\frac{\alpha}{2} \\ -i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix} \tag{28}$$

$$R_y(\alpha) = e^{-i\alpha\boldsymbol{\sigma}_y/2} = \begin{pmatrix} \cos\frac{\alpha}{2} & -\sin\frac{\alpha}{2} \\ \sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix} \tag{29}$$

$$R_z(\alpha) = e^{-i\alpha\boldsymbol{\sigma}_z/2} = \begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \tag{30}$$

Here $R_x(\alpha)$ is a rotation on the Bloch sphere by angle α about the x-axis. Similarly R_y and R_z correspond give rotations about the y and z axes, respectively.

3.5 Properties of unitary transformations

Some properties of *unitary transformations* and unitary evolution of quantum states:

- Reversible. They have an inverse. If $\mathbf{U}$ is a unitary transformation $\mathbf{U}^{-1} = \mathbf{U}^\dagger$.
- Deterministic. No random choices are required when a state vector transforms via unitary transformation.
- A unitary matrix can be written as $\mathbf{U} = e^{i\mathbf{H}}$ where $\mathbf{H}$ is a Hermitian matrix.
- They can be applied in a time continuous way with an exponential matrix.
- They preserve the state vector norm, $\langle\psi|\psi\rangle = \langle \mathbf{U}\psi|\mathbf{U}\psi\rangle = \langle\psi|\,\mathbf{U}^\dagger\mathbf{U}\,|\psi\rangle = 1$.
- A unitary matrix has columns that are orthonormal and rows that are orthonormal.
- The determinant of a unitary matrix $|\det(\mathbf{U})| = 1$.

- They can be diagonalized and their eigenvalues are complex numbers on the unit circle.
- They can be used to change basis.
- In an N-dimensional space, the set of them is a group called $U(N)$.

4 Measurements

Measurements are

- Irreversible.
- Information is lost.
- Probabilistic.
- Involve what is called 'collapse of the wave-function'. The measurement changes the quantum state vector. They can be discontinuous. (Though not necessarily in the setting of weak measurements).

Measurements can be described as a projection of the quantum state vector with a Hermitian projection operator that is chosen using a probability.

In contrast, unitary transformations are reversible, and do not involve random choices.

Measurements involve a sum of probabilities that equal 1.

As an example, we consider a measurement of a qubit that is associated with the Pauli spin matrix

$$\boldsymbol{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The expectation

$$\langle \boldsymbol{\sigma}_z \rangle = \langle \psi | \, \boldsymbol{\sigma}_z \, | \psi \rangle$$

gives us the expectation value of the spin value with a measured 1 being spin up and a measured -1 being spin down. (For a spin 1/2 particle the spin operator is $\mathbf{J} = \hbar \boldsymbol{\sigma}_z / 2$ so a measurement of spin in the z direction actually gives $\pm\hbar/2$). With $|\psi\rangle = |0\rangle$ the spin is up and with $|\psi\rangle = |1\rangle$ the spin is down. With $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, the probability of measuring spin up is aa^* and the probability of measure spin down is $bb^* = 1 - aa^*$. After measuring a spin up, the state vector collapses and becomes a complex number of magnitude 1 times $|0\rangle$. After measuring a spin down, the state vector collapses and becomes $|1\rangle$ times a complex number of magnitude 1. Is the phase important? If you are later on carrying out an interference experiment, the phase could be important. The expectation value is the mean value measured from a series of measurements on the same state vector.

A **projection operator** $\mathbf{P}$ satisfies

$$\mathbf{P}^2 = \mathbf{P}. \tag{31}$$

We can collapse the state vector with two projection operators

$$\mathbf{P}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \mathbf{P}_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

The projection operators can also be written

$$\mathbf{P}_0 = |0\rangle \langle 0| \qquad \mathbf{P}_1 = |1\rangle \langle 1| \, . \tag{32}$$

We can see that the two operators $\mathbf{P}_0, \mathbf{P}_1$ are projection operators as they satisfy equation 31; $\mathbf{P}_0^2 = \mathbf{P}_0$, $\mathbf{P}_1^2 = \mathbf{P}_1$.

Since $|0\rangle, |1\rangle$ are the eigenvectors of the Pauli spin matrix $\boldsymbol{\sigma}_z$, the two projection operators are constructed as ket/bra from these eigenvectors.

After a measurement giving spin up, the new state vector must be normalized

$$|\psi'\rangle = \frac{\mathbf{P}_0 |\psi\rangle}{\sqrt{\langle\psi| \mathbf{P}_0 |\psi\rangle}}$$

Similarly after a measurement giving spin down, the new state vector would become

$$|\psi'\rangle = \frac{\mathbf{P}_1 |\psi\rangle}{\sqrt{\langle\psi| \mathbf{P}_1 |\psi\rangle}}$$

The probability that a state vector $|\psi\rangle$ is in the spin up state is $\langle\psi|\mathbf{P}_0|\psi\rangle$ and that it is in the spin down state is $\langle\psi|\mathbf{P}_1|\psi\rangle$.

The measurement operator $\boldsymbol{\sigma}_z$ can be written as

$$\boldsymbol{\sigma}_z = m_0\mathbf{P}_0 + m_1\mathbf{P}_1$$
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = 1 \times \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + (-1) \times \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

where $m_0 = 1$ is the measurement associated with the $\mathbf{P}_0$ projection operator and $m_1 = -1$ is the measurement associated with the $\mathbf{P}_1$ projection operator.

To simulate measurement of a single quantum state, you need a set of projection operators, $\mathbf{P}_i$ each associated with each possible measurement value m_i. To simulate a measurement, you chose the measurement value, based on its probability, and then project the state with the appropriate projection operator. For example if $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ then

$$\mathbf{P}_0 \,|\psi\rangle = a\,|0\rangle$$
$$\mathbf{P}_1 \,|\psi\rangle = b\,|1\rangle$$

The probability of getting spin up is $aa*$ and the probability of getting spin down is $bb*$. You would choose a possible measurement value randomly, using these two probabilities. After you know what state resulted from the measurement you then would normalize the state vector. If spin up was measured then the resulting state-vector after measurement is $\frac{a}{|a|} |0\rangle$, otherwise it is $\frac{b}{|b|} |1\rangle$. Here I am keeping track of the phase. If you don't want to keep track of the phase then after measurement the state would be $|0\rangle$ or $|1\rangle$.

Simulation of measurement on a single state involves making a random choice. A series of measurements would then be a series of random choices each giving you a new state vector. Mimicking a series of measurements is a Markov chain Monte Carlo (MCMC) model.

If you have an experiment that you run many times taking a series of measurements of a state $|\psi\rangle$, then the expectation value of the spin would be

$$\langle\psi| \boldsymbol{\sigma}_z |\psi\rangle$$

with 1 corresponding to spin up and -1 corresponding measuring spin down. This expectation value would be the average over many possible measurements of the specific state vector $|\psi\rangle$.

4.1 Measurement Postulates of Quantum Mechanics

- A measurement can be specified via a Hermitian operator $\mathbf{A}$ which can also be called an *observable.*

- The eigenvalues m_i of the operator are the possible measured values. Because $\mathbf{A}$ is Hermitian, the measurement values m_i are real numbers.

- Because $\mathbf{A}$ is Hermitian, it is possible to find a set of normalized, orthogonal eigenvectors that span the Hilbert space. The normalized eigenvectors $|v_i\rangle$ of the operator can be used to construct a set of orthogonal projection operators $\mathbf{P}_i = |v_i\rangle \langle v_i|$. Because the eigenvectors are orthogonal, so too are these projection operators

  $$\mathbf{P}_i\mathbf{P}_j = |v_i\rangle \langle v_i| |v_j\rangle \langle v_j| = \delta_{ij}\mathbf{P}_i.$$

  The measurement operator can be written as

  $$\mathbf{A} = \sum_i m_i\mathbf{P}_i$$

  where m_i are the possible measurement values m_i is the eigenvalue associated with eigenvector $|v_i\rangle$.

- The inner product of a normalized eigenvector $|v_i\rangle$ with the wave function $|\psi\rangle$ gives the probability of a particular measurement value.

  $$p_i = | \langle v_i|\psi\rangle |^2 = | \langle\psi|v_i\rangle \langle v_i|\psi\rangle | = \langle\psi| \mathbf{P}_i |\psi\rangle .$$

This postulate is called **Born's rule**.

- The expectation value of the measurement $\langle \mathbf{A} \rangle = \langle \psi | \mathbf{A} | \psi \rangle$. If you redid the measurement many times on the same state vector, the expectation value is the average of all the measurements.
$$\langle \mathbf{A} \rangle = \sum_i m_i p_i.$$
- After a single measurement the state vector is collapsed using one of the projection operators. If the measured value is m_i then the wave function becomes
$$|\psi\rangle \to \frac{\mathbf{P}_i |\psi\rangle}{\sqrt{\langle \psi | \mathbf{P}_i | \psi \rangle}}.$$
After measurement, the state vector is a normalized eigenvector of the measurement operator.

These postulates are known as the *Hermitian operator formalism for measurement.*

4.2 Measurement operators and projective measurements

In our above list for postulates of quantum measurement we derived a set of projection operators from the eigenvectors of a Hermitian operator. For a Hermitian operator, it is always possible to find a set of orthogonal eigenvectors that span the whole Hilbert space. In other words given a Hermitian operator $\mathbf{A}$ in an N-dimensional Hilbert space you can always find N linearly independent eigenvectors of $\mathbf{A}$ and with these eigenvectors you can always make a set of projection operators. Because the eigenvectors are orthogonal, so too are the projection operators constructed from them.

Instead of defining measurement in terms of a Hermitian operator, we can describe measurements in terms of a set of Hermitian projection operators $\mathbf{P}_i$. They should span the space so we require that
$$\sum_i \mathbf{P}_i = \mathbf{I}. \tag{33}$$
This is known as a **completeness relation**. We require that the projection operators are orthogonal
$$\mathbf{P}_i \mathbf{P}_j = \delta_{ij} \mathbf{P}_i. \tag{34}$$

A measurement is then written as an operator
$$\mathbf{A} = \sum_i m_i \mathbf{P}_i$$
where the m_i are real numbers that are the possible measurement values.

Given a state $|\psi\rangle$, the probability that you would measure m_i is

$$p_i = \langle\psi|\,\mathbf{P}_i\,|\psi\rangle\,.$$

Likewise after measurement the state becomes

$$|\psi'\rangle = \frac{\mathbf{P}_i\,|\psi\rangle}{\langle\psi|\,\mathbf{P}_i\,|\psi\rangle}.$$

The completeness relation of equation 33 ensures that these probabilities sum to 1.

Instead of requiring measurements to be derived from the eigenvectors of a Hermitian operator we can postulate that quantum measurements are described by a complete set of Hermitian, orthogonal projection operators. This means they satisfy equations 33 and 34. Measurements that are based on Hermitian projection operators that satisfy these two equations (completeness and orthogonality) are called **projective measurements**. This is a bit more general than basing a measurement on a Hermitian operator, as the real numbers m_i (the possible measurement values) could be anything.

Definition: A **projective measurement** is a set of Hermitian projection operators that are complete (they satisfy equation 33) and orthogonal (they satisfy equation 34). If there are N projection operators, where N is the dimension of the Hilbert space, then the measurement is called a **Von Neumann measurement**. For a projective measurement, the total number of projection operators could be smaller than N.

We often say we are **measuring in a particular basis**. What is meant is that we are carrying out a von Neumann measurement; which is a projective measurement with N projection operators, where N is the dimension of the quantum space. The measurement values are irrelevant, but following measurement, the quantum state is in one of the basis elements and we know which one.

There are more general types of measurements. For example, the projection operators need not be be orthogonal. It is possible to measure only part of a quantum system. More general types of measurements are called **POVM measurements** where POVM is short for Positive Operator Value Measure and we will discuss them later.

In our above definition of a projective measurement, we did not specify how many of the projection operators are required. If projection operators are derived from a Hermitian operator or observable, how do we create projection operators if two of the eigenvalues of the Hermitian operator are the same? We discuss this in the next section.

4.3 Subspace decomposition and operators with eigenvalues that are not all unique

What happens if two eigenvalues of an observable are the same? For example? Consider the observable

$$\mathbf{M} = \begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

There are two possible measurements: 4 or 2.

This operator is in a 4 dimensional Hilbert space and we call the basis vectors $|0\rangle, |1\rangle, |2\rangle, |3\rangle$. In terms of vectors these are

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

We could construct a set of projection operators $\mathbf{P}_i = |i\rangle\langle i|$ in this basis;

$$\mathbf{P}_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{P}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathbf{P}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{P}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Our observable $\mathbf{M}$ can be written in terms of these projection operators as

$$\mathbf{M} = 4\mathbf{P}_0 + 4\mathbf{P}_1 + 2\mathbf{P}_2 + 2\mathbf{P}_2. \tag{35}$$

The expectation value is computed as before

$$\langle \mathbf{M} \rangle = 4\langle\psi|\,\mathbf{P}_0\,|\psi\rangle + 4\langle\psi|\,\mathbf{P}_1\,|\psi\rangle + 2\langle\psi|\,\mathbf{P}_2\,|\psi\rangle + 2\langle\psi|\,\mathbf{P}_3\,|\psi\rangle$$

How do we simulate a measurement? If a 4 is measured do we collapse the state vector using $\mathbf{P}_0$ or $\mathbf{P}_1$ or some combination of these two? The subspace S_1 spanned by $|0\rangle, |1\rangle$ is preserved during a measurement of 4, but we don't learn anything more about the vector within this subspace. The part of the vector in the subspace S_2 spanned by $|2\rangle, |3\rangle$ is removed by the measurement. With state vector

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle + c\,|2\rangle + d\,|3\rangle$$

a measurement of 4 removes the part of the vector in the subspace spanned by $|2\rangle, |3\rangle$ so after measurement of 4 the new state vector would become

$$|\psi\rangle \rightarrow \frac{a|0\rangle + b|1\rangle}{\sqrt{aa^* + bb*}}$$

If a 2 is measured then

$$|\psi\rangle \rightarrow \frac{c|2\rangle + d|3\rangle}{\sqrt{cc^* + dd*}}$$

We can describe the measurement with two different projection operators

$$\mathbf{P}_{\lambda 4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{P}_{\lambda 2} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where I am labelling the operators by the eigenvalues related to the measurement. The measurement can be written in terms of these operators

$$\mathbf{M} = 4\mathbf{P}_{\lambda 4} + 2\mathbf{P}_{\lambda 2}.$$

The operators $\mathbf{P}_{\lambda 4}, \mathbf{P}_{\lambda 2}$ are projection operators as $\mathbf{P}_{\lambda 2}^2 = \mathbf{P}_{\lambda 2}$ and $\mathbf{P}_{\lambda 4}^2 = \mathbf{P}_{\lambda 4}$. These projection operators are perpendicular or orthogonal, as

$$\mathbf{P}_{\lambda 2}\mathbf{P}_{\lambda 4} = \mathbf{P}_{\lambda 4}\mathbf{P}_{\lambda 2} = 0.$$

They also satisfy the completeness relation as

$$\mathbf{P}_{\lambda 2} + \mathbf{P}_{\lambda 4} = \mathbf{I}.$$

The operators are Hermitian, projective and satisfy equations 33 and 34 for completeness and orthogonality. However there are only 2 projection operators instead of 4 which is the dimension of the Hilbert space. The operator **M** gives us a **projective measurement** but it is not a **von-Neumann measurement** because there are fewer projection operators than the dimension of the quantum space.

In this example, there are only 2 possible measurement values. When you make a measurement with **M** you gain less **information** than if there were 4 possible measurement values. The measurement gives you information with respect to a subspace decomposition of the full Hilbert space $\mathcal{H} = S_1 \otimes S_2$ where the subspaces are S_1, S_2. Here S_1 is spanned by the basis $|0\rangle, |1\rangle$ and S_2 is spanned by the basis $|2\rangle, |3\rangle$. The action of measurement projects the eigenvector into a subspace. If the measurement gives you more information, then the resulting state after measurement is restricted to a smaller subspace.

4.3.1 Notes on projections

- Projection operators have eigenvalues that are 0 or 1.
- Projection operators are **positive semidefinite** which means that $\langle v| \mathbf{P} |v\rangle \geq 0$ for all nonzero $|v\rangle$ in the Hilbert space.
- A projective operator is not necessarily Hermitian. An example is

  $$\mathbf{P} = \begin{pmatrix} \frac{1}{2} & 1 \\ \frac{1}{4} & \frac{1}{2} \end{pmatrix}$$

  It is a projection operator because $\mathbf{P}^2 = \mathbf{P}$. Because it is real and not symmetric, it is not Hermitian. Its eigenvalues are 0,1 but its eigenvectors are not perpendicular.
- Vector spaces U, W are *orthogonal subspaces* if every vector $v \in V$ is orthogonal to every vector $u \in U$. An 'orthogonal projection' is one with range U and null space W that are orthogonal subspaces. A projection is an 'orthogonal' projection if and only if it is Hermitian (self-adjoint).
- I think that if a set of projection operators satisfies completeness and orthogonality that they must be Hermitian and if a set of projection operators is Hermitian and complete, that they must be orthogonal.

4.4 Can quantum systems be isolated?

We have described a quantum state in terms of a normalized state-vector in a finite dimensional space. This is equivalent to pretending that the system is isolated and does not interact with the outside world except in terms of idealized measurements which we described above as projective. However, in the real world a quantum subsystem would interact with the outside world. Due to interactions with the external world, evolution of the subsystem might not be unitary. If we only focus on the subsystem alone, then measurements on it might not be projective.

4.5 The Quantum Zeno effect

The **Quantum Zeno** effect describes what happens if you measure a state over and over again. It is nearly frozen into a single measured state. With a slowly drifting system, the process of repeated measurement and state vector collapse keeps the probability low that the system can evolve into a different state and that a subsequent measurement will give a different value.

Consider a single qubit that is initially in the spin up state $|\psi\rangle = |0\rangle$. We operate on it with a smoothly varying unitary operation that depends upon time t and a small

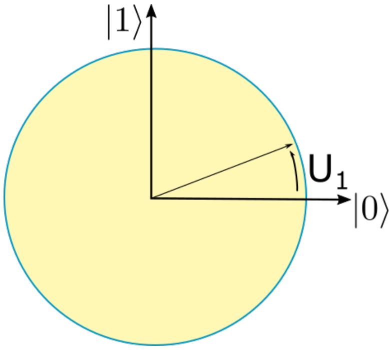

Figure 3: A qubit drifts in the counter clockwise due to continuous unitary evolution. Measurement by $\boldsymbol{\sigma}_z$ projects the state either into $|0\rangle$ or $|1\rangle$. If the state originates at $|0\rangle$ repeated measurements tend to keep it near $|0\rangle$. This is called the Quantum Zeno effect.

parameter β

$$\begin{aligned}\mathbf{U}(t) = \mathbf{S}_y(-\beta t) &= e^{-i\beta\boldsymbol{\sigma}_y t} \\ &= \begin{pmatrix}\cos\beta t & \sin\beta t \\ \sin\beta t & \cos\beta t\end{pmatrix}\end{aligned} \tag{36}$$

and we have used equation 26 for the exponential. After time $T = 2\pi/\beta$, the system returns to its initial state. We divide T in to N pieces giving us a time interval

$$\delta t = \frac{2\pi}{N\beta}. \tag{37}$$

Here N is the number of time intervals required for a complete revolution of 2π. At time interval $j\delta t$, the unitary transformation $U_j = e^{\frac{-i2\pi j\boldsymbol{\sigma}_y}{N}}$ rotates the state by angle $\alpha = \frac{2\pi j}{N}$. We evaluate this matrix using equation 36 to find

$$U_j = \begin{pmatrix}\cos\frac{2\pi j}{N} & -\sin\frac{2\pi j}{N} \\ \sin\frac{2\pi j}{N} & \cos\frac{2\pi j}{N}\end{pmatrix}. \tag{38}$$

With a single time interval δt the unitary transformation is

$$U_1 = \begin{pmatrix}\cos\frac{2\pi}{N} & -\sin\frac{2\pi}{N} \\ \sin\frac{2\pi}{N} & \cos\frac{2\pi}{N}\end{pmatrix}. \tag{39}$$

We evolve with U_1, then measure the state, then evolve it again, and so on, alternating between continuous unitary evolution and measurement.

After evolving via U_1 the state vector becomes

$$|\psi\rangle = \cos\frac{2\pi}{N}|0\rangle + \sin\frac{2\pi}{N}|1\rangle$$

We measure it with $\boldsymbol{\sigma}_z$. The probability that the state has a spin up (corresponding to $|0\rangle$) is $\cos^2 \frac{2\pi}{N} = 1 - \sin^2 \frac{2\pi}{N}$ and that the state has spin down is $\sin^2 \frac{2\pi}{N}$. Let

$$\epsilon = \sin \frac{2\pi}{N}$$

assuming that ϵ is small, which is equivalent to assuming that N is large. The probability that a spin down is measured is ϵ^2 and that a spin-up is measured is $1 - \epsilon^2$.

Suppose we alternate between unitary evolution by δt and measurement by $\boldsymbol{\sigma}_z$. We do this M times. We estimate the probability that a spin up is measured after M repeats is

$$P_{UM} \sim (1-\epsilon^2)^M \sim 1 - M\epsilon^2. \qquad \text{probability of measuring 0 after M repeated measurements} \tag{40}$$

The probability that a spin up is measured after M unitary evolutions by U_1 and measurements by $\boldsymbol{\sigma}_z$ is actually higher than this since one of the intermediate measurements could have been spin down, and then followed by a spin up measurement.

Suppose instead the system is allowed to evolve without measurement during the M time intervals. Using equation 38 with $j = M$, the state vector becomes

$$|\psi\rangle = \cos \frac{2\pi M}{N} |0\rangle + \sin \frac{2\pi M}{N} |1\rangle$$

The probability that spin up is measured after time $T = M\delta t$ is

$$P_U \sim \cos^2 \frac{2\pi M}{N}. \tag{41}$$

Suppose we chose number of evolution steps to be $M = N/4$. This gives probably of spin up $P_U = \cos^2 \frac{\pi}{2} = 0$ (without measurement) because the state evolves to $|1\rangle$. In contrast the probability of spin up when measurements are taken

$$P_{UM} \sim 1 - M\frac{4\pi^2}{N^2} \sim 1 - \frac{\pi^2}{N}.$$

This is much higher than 0 if N is large. The probability can be high that the spin up is measured after the evenly spaced M measurements. The frequent measurements keep the system near the spin up position! The **Quantum Zeno effect** is when rapid measurements keep a system from evolving.

Procedure	Probability of $|0\rangle$ measurement
After $M = N/4$ times alternating measurement and U_1	$1 - \frac{\pi^2}{N}$
After $M = N/4$ times unitary evolution by U_1	0

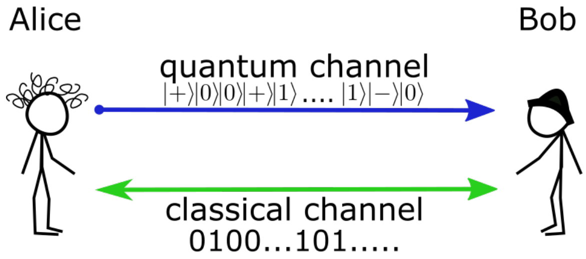
Alice
Bob
quantum channel
$|+\rangle|0\rangle|0\rangle|+\rangle|1\rangle$ .... $|1\rangle|-\rangle|0\rangle$
classical channel
0100...101.....

Figure 4: The BB84 protocol for quantum key distribution involves a unidirectional quantum communication channel and a bidirectional classical communication channel. Alice and Bob want to create a common key that is not known to a potential eavesdropper, Eve. Alice and Bob share which basis they use, not which values are measured or are discarded.

4.6 Quantum Key Distribution, the BB84 protocol

In communication protocols, sender and receiver are often called Alice and Bob. A third party who might be trying to listen in (or eavesdrop) on the communication is called Eve.

BB84 refers to a key generation protocol proposed by Bennett and Brassard (1984). The goal is to establish a secret key, which is a sequences of 0s and 1s, that only Alice and Bob know about. Alice and Bob then can use this key to encrypt and decrypt messages.

Alice and Bob communicate with two channels, a classical one and a quantum one. In the bidirectional classical channel, they send regular messages back and forth. In the quantum communication channel, Alice sends a single qubit to Bob and Bob performs measurements on it. The qubit is actually a photon or a 2 state object. If the object is a photon, Alice and Bob make polarization measurements. The idea of the protocol is that Alice and Bob would notice if there was an eavesdropper (Eve) on the quantum line.

Alice randomly choose 0 or 1. She also randomly chooses a basis which is either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. She sends a quantum state to Bob that depends on both of these random choices.

If she has a 0 and choses basis $\{|0\rangle, |1\rangle\}$, then she sends $|0\rangle$.
If she has a 1 and chooses basis $\{|0\rangle, |1\rangle\}$ then she sends $|1\rangle$.
If she has a 0 and choses basis $\{|+\rangle, |-\rangle\}$, then she sends $|+\rangle$.
If she has a 1 and choses basis $\{|+\rangle, |-\rangle\}$, then she sends $|-\rangle$.

What Alice sends				
Bit/basis	0, $\{|0\rangle, |1\rangle\}$	1, $\{|0\rangle, |1\rangle\}$	0, $\{|+\rangle, |-\rangle\}$	1, $\{|+\rangle, |-\rangle\}$
Alice sends	$|0\rangle$	$|1\rangle$	$|+\rangle$	$|-\rangle$

Bob receives the quantum state (or photon) and then measures it. He randomly choose either the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis in which to do his measurement. If he is using the $\{ |0\rangle, |1\rangle \}$ basis for measurement he associates a 0 with a measurement giving $|0\rangle$ and a 1 with a measurement giving $|1\rangle$. Similarly if he is using the $\{|+\rangle, |-\rangle\}$

basis for measurement he associates a 0 with a measurement giving $|+\rangle$ and a 1 with a measurement giving $|-\rangle$. Measurements could be associated with the following Hermitian matrix (a measurement operator with eigenvalues 0,1) in either basis

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

If the object sent is a photon, the basis is chosen by rotating a polarizer and the photon either passes through or it is absorbed giving a 1 or 0 result. If the object sent is a two-state quantum system, then you assign 0 to measurement of $|0\rangle$ and you assign 1 to a measurement of $|1\rangle$.

			Basis for Bob's measurement	
			$\{\|0\rangle, \|1\rangle\}$	$\{\|+\rangle, \|-\rangle\}$
Alice's bit	Alice's basis	Bob receives	Bob records	Bob records
0	$\{\|0\rangle, \|1\rangle\}$	$\|0\rangle$	0	0 or 1
1	$\{\|0\rangle, \|1\rangle\}$	$\|1\rangle$	1	0 or 1
0	$\{\|+\rangle, \|-\rangle\}$	$\|+\rangle$	0 or 1	0
1	$\{\|+\rangle, \|-\rangle\}$	$\|-\rangle$	0 or 1	1

After Bob makes his measurements, Alice and Bob share which bases they used and discard all measurements where they did not use the same basis.

Alice and Bob now share a series of randomly generated bits which we call a key. This involves sending about twice as many bits as they need in the key because about 50% are discarded. Because the bits are initially chosen randomly by Alice, the key's sequence is randomly generated. Over the classical communication channel, Alice and Bob discuss the bases, not the actual values of the bits themselves. Eve would not gain information about the key by listening in on the classical channel.

To gain information Eve must intercept the photons on the quantum channel. However, she will not know what basis is used to send or receive the photons when she intercepts the photons. That means she cannot figure out which basis to use to measure/intercept the photons. If she uses the wrong basis then she will incorrectly measure and then resend the photon.

What happens if the qubit is measured by Eve and then she sends her measured state to Bob? There is a 50% chance that Eve guesses the correct basis for her measurement. In this case Bob's measurement is still correct. There is a 50% chance that Eve uses the wrong basis to make her measurement. Her measurement projects the state into the wrong basis. For example, suppose the photon is in the $|+\rangle$ state and Eve choses the $\{|0\rangle, |1\rangle\}$ basis for measurement. Afterwards her measurement the photon will be either $|0\rangle$ or $|1\rangle$ and that is what she sends to Bob. Bob will measure her photon in the $\{|+\rangle, |-\rangle\}$ basis and will measure the incorrect result 50% of the time. Taking into account the 1/2 probability that Eve guesses the basis incorrectly, we find that 1/4 of the time Bob will measure the wrong result. If Eve is eavesdropping, then 25% of the photons in the key will be incorrectly measured by Bob. When Alice and Bob try to use the key, they will notice a high error rate.

As we will see later on, Eve cannot make a copy of the qubit to keep while sending the original on to Bob. This would be called *cloning* and it is impossible.

Of course Eve could impersonate Bob. This makes the protocol vulnerable to what is known as is a man-in-the-middle attack. To guard against such an attack, in additional to a key protocol, Alice and Bob would also want to use an authentication protocol.

4.7 Mutually unbiased bases

Two orthonormal bases $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ are **mutually unbiased** if $|\langle u_i|v_j\rangle| = c$ is the same real number c for every i, j.

For example the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle\, |-\rangle\}$ bases are mutually unbiased. We check that this is true:

$$|\langle 0|+\rangle| = |\langle 1|+\rangle| = |\langle 0|+\rangle| = |\langle 1|-\rangle| = \frac{1}{\sqrt{2}}$$

Suppose you measure in the $\{|0\rangle, |1\rangle\}$ basis. If the state is $|+\rangle$ then you have equal probability of measuring a $|0\rangle$ or a $|1\rangle$. Likewise if the state is $|-\rangle$ then you have equal probability of measuring a $|0\rangle$ or a $|1\rangle$. If you measure a $|0\rangle$ you cannot tell if the state was $|+\rangle$ or $|-\rangle$. Even if you made many measurements of the same state, you would not be able to tell if the state you are measuring is $|+\rangle$ or $|-\rangle$. The measurement gives you no information.

Use the $\{|u_i\rangle\}$ basis for measurement and measure a basis element from the $\{|v_i\rangle\}$ basis. If the two bases are mutually unbiased, then you do not learn anything about the measured basis element from the measurement.

The BB84 quantum key distribution(QKD) protocol leverages the fact that the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases are **mutually unbiased**.

4.8 Beyond BB84

For a single qubit, is it possible to have a third basis that is also mutually unbiased with respect to the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases?

Yes, the three bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ and $\{|i\rangle, |-i\rangle\}$ are all mutually unbiased. In other words each possible pair of bases from this set is mutually unbiased.

The Chau02 protocol[1] uses the three mutually unbiased bases for a single qubit to create a protocol that is remarkably robust to errors. Alice and Bob each choose between the three possible bases for measurement and after Bob makes his measurements, they share their basis choices.

[1] H. F. Chau. "Practical scheme to share a secret key through a quantum channel with a 27.6 percent bit error rate". In: Phys. Rev. A 66 (2002), p. 060302.

In a qubit system, the largest number of mutually unbiased bases is three.

Larger quantum systems have larger sets of mutually unbiased bases. See the recent review[2] `https://arxiv.org/pdf/2402.01319.pdf` on using qudits in quantum key distribution protocols.

5 Product spaces and 2 qubits

With two qubits we have a Hilbert space H_{AB} that is a product of two Hilbert spaces H_A and H_B.

A state in the Hilbert space $H_{AB} = H_A \otimes H_B$ can be written in terms of basis vectors for H_A and H_B,

$$|\psi\rangle = \sum_{ij} a_{ij} |i\rangle_A \otimes |j\rangle_B .$$

where $|i\rangle_A$ is in H_A and $|j\rangle_B$ is in H_B. Shorthand includes

$$|i\rangle_A \otimes |j\rangle_B = |i\rangle |j\rangle = |ij\rangle .$$

With two qubits, a state looks like this

$$|\psi\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |10\rangle + a_{11} |11\rangle$$

with four complex coefficients. Our Hilbert space has 4 elements in its basis and must be normalized so that $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.

We could also write $|00\rangle$ as $|0\rangle \otimes |0\rangle$ making it clearer that our Hilbert space is a product of two complex vector spaces. The product space contains elements like $a_{ij} |i\rangle \otimes |j\rangle$ or $a_{ij} |ij\rangle$. The product is known as a *tensor* product.

A single qubit has state vector in the form $|\psi\rangle = a|0\rangle + b|1\rangle$. We can make a tensor product with two single qubits (each in their own 2d Hilbert space) with

$$\begin{aligned}(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) &= ac|0\rangle|0\rangle + bd|1\rangle|1\rangle + ad|0\rangle|1\rangle + bc|1\rangle|0\rangle \\ &= ac|00\rangle + bd|11\rangle + ad|01\rangle + bc|10\rangle . \qquad (42)\end{aligned}$$

However not every state in the product space can be written in the form on the left hand side. In others words, there are state vectors $|\psi\rangle_{AB} \in H_A \otimes H_B$ where there does not exist $|\phi\rangle_A \in H_A$ and $|\phi\rangle_B \in H_B$ such that $|\psi\rangle_{AB} = |\phi\rangle_A \otimes |\phi_B\rangle$.

[2] A Review of Quantum communication using high-dimensional Hilbert spaces, Yuval Idan and Avihai Didi (2024) arxiv.org/2402.01319.

5.1 Entanglement

We consider the product space of 2 qubits. Not all states in the full 2-qubit Hilbert space can be written as a tensor product. For example consider the state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Can we find a, b, c, d

$$(a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle)$$

that would allow us to write the state vector as a tensor product? We need to find a, b, c, d that would satisfy

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle)$$

Using equation 42 we find that gives $ac = 1/\sqrt{2} = bd$ and $ad = bc = 0$. The second condition implies that one of a, d must be zero but neither can be zero according to the first condition. There is no solution.

States that cannot be written as a tensor product are called **entangled**.

We consider a state-vector $|\psi\rangle = \sum_{ij} a_{ij}\,|i\rangle\,|j\rangle$. There might be a basis $\left|\tilde{i}\right\rangle \otimes \left|\tilde{j}\right\rangle$ in which we can write the state-vector as

$$|\psi\rangle = \sum_{ij} a_i a_j\,|i\rangle\,|j\rangle = \left(\sum_i b_i\,\left|\tilde{i}\right\rangle\right) \otimes \left(\sum_j c_j\,\left|\tilde{j}\right\rangle\right).$$

If there is no-such basis, then the state is described as **entangled**.

Are there states that are more entangled than others? The definition for entanglement given here does not give us a quantitative way to discuss the level of entanglement. We will discuss this issue in more detail when we look at measures of quantum information.

5.2 The Bell pair state

The state

$$|\psi\rangle_{\text{Bell}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

is called a **Bell pair** or EPR pair state. Consider making a Bell pair state and then sending the first qubit to Alice and the second qubit to Bob. Alice and Bob perform measurements on their qubits. We now consider creating a sequence of Bell pair states and sending the first qubit in each pair to Alice and the second qubit in each pair to Bob. Alice makes a series of measurements and so does Bob. Looking at her results, Alice sees a sequence that appears to be randomly distributed with 0 and 1 states given with equal probability. Similarly Bob measures a sequence that appears to be random. However, when Alice and Bob compare their sequences they notice that they are highly *correlated.* Alice and Bob measure the same value at each iteration in the sequence.

5.3 Operations on two qubits

For the product of two qubits, we can order matrices and vectors using the order above so

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \qquad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{43}$$

The order of these states is consecutive in base two: 00 is 0, 01 is 1, 10 is 2 and 11 is 3.

The identity for the 2 qubit system can be written as $\mathbf{I} \otimes \mathbf{I}$,

$$\mathbf{I} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Many operators can be written as direct products, like $\mathbf{A} \otimes \mathbf{I}$ where $\mathbf{I}$ is the identity for a single qubit and $\mathbf{A}$ is an operator for a single qubit. We can construct operators (or gates) in the full space that are products of gates in the subspaces. For example $\mathbf{H} \otimes \mathbf{H}$ where $\mathbf{H}$ is the Hadamard gate or $\mathbf{H} \otimes \mathbf{I}$.

$$\mathbf{I} \otimes \mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\mathbf{H} \otimes \mathbf{I} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

For example

$$\begin{aligned} \mathbf{H} \otimes \mathbf{I}\, |00\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ \mathbf{H} \otimes \mathbf{I}\, |01\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \\ \mathbf{H} \otimes \mathbf{I}\, |10\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \mathbf{H} \otimes \mathbf{I}\, |11\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle). \end{aligned}$$

The product of $\mathbf{I} \otimes \mathbf{H}$ and $\mathbf{H} \otimes \mathbf{I}$ is

$$\mathbf{H} \otimes \mathbf{H} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

It may help to know that unitary matrices have rows and columns that have norm 1 and are orthogonal. It is also useful to check that the conjugate transpose of the matrix times itself gives the identity.

5.4 Controlled NOT gate

An interesting new gate that operates on 2 qubits is the **Controlled NOT** or **CNOT** where the second bit is flipped only if the first bit is 1.

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

With basis as defined in equation 43.

$$\begin{aligned} \text{CNOT}\,|00\rangle &= |00\rangle \\ \text{CNOT}\,|01\rangle &= |01\rangle \\ \text{CNOT}\,|10\rangle &= |11\rangle \\ \text{CNOT}\,|11\rangle &= |10\rangle\,. \end{aligned}$$

The CNOT *cannot* be written as a tensor product.

The CNOT can also be written as

$$\text{CNOT}\,|xy\rangle = |x, x+y\rangle$$

where x, y are either 0 or 1 and the sum $x + y$ is mod 2. Treating the states as classical bits, $x + y$ mod 2 is also **XOR** applied to bit x, y, which gives 0 if both bits are the same but 1 otherwise. The XOR is sometimes written as $x \oplus y$.

I can start with a state that is a tensor product and apply the CNOT

$$\begin{aligned} \text{CNOT}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle &= \text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

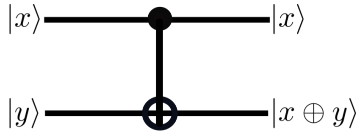

Figure 5: Common convention (though there are exceptions to this rule) with quantum circuit drawings is that the first qubit is on the top. The operation is the CNOT but with first (top) bit as control and second (bottom) bit as target. The CNOT looks like a plus on the second qubit because the CNOT can be written as $|x, x+y\rangle$ with $x, y \in \{0, 1\}$.

The result is an entangled state (as we showed above that this state could not be written as a tensor product). So the CNOT takes a tensor product state that is not entangled, and turns it into an entangled state.

The CNOT is said to induce **correlations**. With $|+0\rangle$ the original state, there is 50% chance for the first qubit to be measured in the 0 state, 50% chance of it being measured in the 1 state and 100% chance that the second qubit is measured in the 0 state. There is a 50% chance that measurements of the two qubits would agree. With the final entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, there is a 50% chance of both qubits being measured in the zero state and a 50% chance of both qubits being measured in the 1 state. The probability is zero that that one qubit would be measured to be in the zero state and other qubit would be measured to be in the 1 state. The probability that the measurements of the two qubits agree is 100%. This is what is meant by inducing correlations.

Example: Starting from $|00\rangle$ construct a Bell pair state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ using simple gates. See Figure 6 for an illustration.

Here's how we do it.

- Apply $\mathbf{H} \otimes \mathbf{I}$, the Hadamard gate to the first qubit.

$$\mathbf{H} \otimes \mathbf{I}\,|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

- Then apply the CNOT where the control bit is the first qubit and the 2nd qubit is the target

$$\text{CNOT}\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

A diagram of the quantum circuit for the creating the Bell pair state is shown in Figure 6. Common convention for quantum circuits seems to be putting the first qubit on the top of the diagram. Inputs are on the left and outputs are on the right.

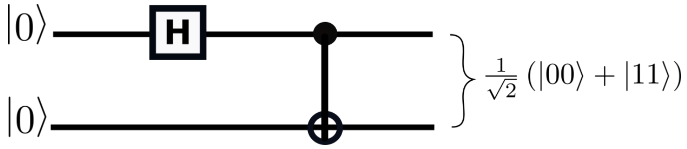

Figure 6: The first quantum operation is a Hadamard on the top qubit. This corresponds to the unitary transformation $\mathbf{H} \otimes \mathbf{I}$. The second operation (on the right) is the CNOT but with first (top) bit as control and second (bottom) bit as target. The CNOT looks like a plus on the second qubit because the CNOT can be written as $|x, x+y\rangle$. Starting with state $|00\rangle$ on the left, the result, on the right is the Bell pair state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

5.5 Other controlled 2 qubit operators

We can consider a 2 qubit gate with the first bit a control bit and the second bit a target bit. Instead of flipping the target bit if the first bit is 1, we can execute a gate on the target bit if the first bit is 1 and not change it if the first bit is 0. Any one bit gate can be controlled. We write the CNOT gate as $\Lambda(\mathbf{X})$, where $\mathbf{X}$ is the NOT gate and equivalent to the Pauli-X gate. We can use the Λ symbol to denote other types of controlled gates.

For the first qubit we use projection operators

$$\mathbf{P}_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad \mathbf{P}_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

In the tensor product space

$$\mathbf{P}_0 \otimes \mathbf{I} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \mathbf{P}_1 \otimes \mathbf{I} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{44}$$

We can write CNOT gate as

$$\begin{aligned} \text{CNOT} = \Lambda(\mathbf{X}) &= \mathbf{P}_0 \otimes \mathbf{I} + \mathbf{P}_1 \otimes \mathbf{X} \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|. \end{aligned}$$

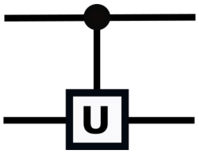

Figure 7: A controlled gate. The control bit is the top one and if it is 1 then the gate U operates on the bottom bit.

For example a controlled phase gate $\Lambda(\mathbf{S})$ gate operates on the second bit with the phase gate if the first bit is 1. Recall that the phase gate looks like

$$\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The controlled phase gate

$$\begin{aligned}\Lambda(\mathbf{S}) &= \mathbf{P}_0 \otimes \mathbf{I} + \mathbf{P}_1 \otimes \mathbf{S} \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + i\,|11\rangle\langle 11| \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}.\end{aligned}$$

5.6 Partial measurement on two qubits

Supose we have

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

Question: We measure the first qubit. What is the probability to get a 0 (or spin up)?
Answer: The probability to get 0 in a measurement of the first qubit is $|\alpha|^2 + |\beta|^2$.
Question: We measure a 0. What does the state vector look like now?
Answer:

$$|\psi'\rangle = \alpha'\,|00\rangle + \beta'\,|01\rangle$$

with coeffcients

$$\alpha' = \frac{\alpha}{|\alpha|^2 + |\beta|^2} \qquad \beta' = \frac{\beta}{|\alpha|^2 + |\beta|^2}.$$

What are the projection operators associated with measuring the first bit? They look like $\mathbf{P}_0 \otimes \mathbf{I}$ and $\mathbf{P}_1 \otimes \mathbf{I}$ as shown in equation 44.

5.7 The no-cloning theorem

Cloning means taking taking an arbitrary state in the first qubit, a specific state in the second one and making the second qubit the same as the first qubit and keeping the state unentangled. In other words finding a transformation

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle \to (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle)$$

with a unitary transformation and for **any** α, β.

In matrix form, the transformation would satisfy

$$U \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^2 \\ \alpha\beta \\ \alpha\beta \\ \beta^2 \end{pmatrix}$$

The transformation is non-linear. There is no way to solve for a matrix U that does not depend on α, β. So, it is not possible to do this with a unitary transformation.

Can you make a copy of a state with a CNOT? Let's recall Figure 5 showing the CNOT operation $|x, y\rangle \to |x, x+y\rangle$ with $x, y \in \{0, 1\}$. Let's apply the CNOT operation to $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle$

$$\text{CNOT}(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle = \alpha|00\rangle + \beta|11\rangle .$$

This result is not the same as $(\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$.

We wanted to clone any state, meaning we wanted an operation that worked for any α, β. However, could we clone a subset of possible input states?

In general a cloning device can only simultaneously clone a set of states which are orthogonal to one another and a general quantum cloning device is impossible. In other words suppose we have two states $|\psi\rangle$ and $|\phi\rangle$ in H_A and a state $|s\rangle \in H_B$ giving states in $H_A \times H_B$

$$|\psi\rangle \otimes |s\rangle \qquad \text{and} \qquad |\phi\rangle \otimes |s\rangle .$$

Now suppose we have a unitary transformation U that does the cloning

$$\begin{aligned} U|\psi\rangle \otimes |s\rangle &= |\psi\rangle \otimes |\psi\rangle \\ U|\phi\rangle \otimes |s\rangle &= |\phi\rangle \otimes |\phi\rangle . \end{aligned}$$

We take the inner product of these two equations

$$\begin{aligned} \langle\psi| \otimes \langle s| U^\dagger U |\phi\rangle \otimes |s\rangle &= (\langle\psi| \otimes \langle\psi|)(|\phi\rangle \otimes |\phi\rangle) \\ (\langle\psi| \otimes \langle s|)(|\phi\rangle \otimes |s\rangle) &= \langle\psi|\phi\rangle \langle\phi|\psi\rangle \\ \langle\psi|\phi\rangle &= |\langle\psi|\phi\rangle|^2. \end{aligned}$$

The only solutions of $x = x^2$ are 0, 1. So if $|\psi\rangle \neq |\phi\rangle$ then $\langle\psi|\phi\rangle = 0$ and they are orthogonal. The states can only be simultaneously cloned if they are orthogonal. As long as we are willing to only accept a small set of orthogonal initial possible states, we could find a **U** that would make it possible to clone them.

5.8 Qutrits instead of Qubits

So far we have discussed bipartite systems of two qubits. A **qutrit** is a three state system with $|0\rangle, |1\rangle, |2\rangle$. We could make a Hilbert space that is a product of a qubit and a qutrit or a product of a qutrit and a quitrit. And so on!

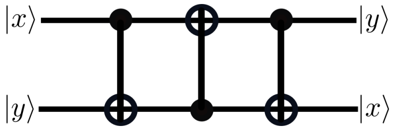

Figure 8: A Quantum circuit that swaps two bits. Here $x, y \in \{0, 1\}$.

5.9 Some quantum circuits

5.9.1 A swap circuit

Let's construct a quantum circuit that flips the states of 2 qubits. The first qubit becomes whatever the other one was and vice versa. In other words we want a circuit that does this transformation

$$\begin{aligned} \text{SWAP}: \qquad & |00\rangle \to |00\rangle \\ & |11\rangle \to |11\rangle \\ & |10\rangle \to |01\rangle \\ & |01\rangle \to |10\rangle \,. \end{aligned} \tag{45}$$

As a matrix the SWAP (in our standard basis, with standard order) is

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

A circuit that does this is shown in Figure 8 and involves 3 CNOTs applied consecutively. Let's show that it works. We start with $|x, y\rangle$ where x can be 0 or 1 and y can be 0 or 1. The first CNOT changes the second bit if the first one is 1. This can be written as

$$\text{First CNOT} \qquad |x, y\rangle \to |x, x + y\rangle$$

where $x + y$ is addition mod 2. The sum $x + y$ is 1 if one of x or y is 1 and is 0 if both are 1 or both are 0. The second CNOT flips the first bit if the second one is 1.

$$\text{Second CNOT} \qquad |x, x + y\rangle \to |x + x + y, x + y\rangle \,.$$

Let's look at $x + x$. If $x = 0$ then $x + x$ is 0. If $x = 1$ then $x + x$ is 0 mod 2. So the second CNOT does this

$$\text{Second CNOT} \qquad |x, x + y\rangle \to |y, x + y\rangle \,.$$

Now we apply the third CNOT which flips the second bit if the first one is 1.

$$\text{Third CNOT} \qquad |x, x + y\rangle \to |y, y + x + y\rangle = |y, x\rangle \,.$$

Altogeter our circuit does this

$$\text{SWAP}: \qquad |x, y\rangle \rightarrow |y, x\rangle$$

which is consistent with our desired transformation in equation 45.

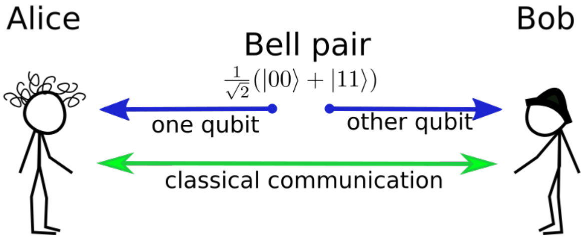

Figure 9: Alice and Bob share a series of Bell pairs. Each of them indepenently choose either the $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$ bases in which to make measurements. They then share over a classical communication channel which bases they used for their measurements. They do not share the values of their measurements. This is a protocol for creating a quantum key using entangled states (Ekert91).

5.10 Quantum key distribution using entangled states

Quantum key distribution is a secure communication method which uses a cryptographic protocol involving quantum states. It enables two parties (Alice and Bob) to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages.

We describe the 1991 quantum key distribution scheme by Artur Ekert.

The protocol starts by creating a series of entangled two qubit states in the Bell state.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{46}$$

Alice gets the first qubit. Bob gets the second.

They each independently chose either the basis $\{|0\rangle, |1\rangle\}$ or the basis $\{|+\rangle, |-\rangle\}$ to perform a measurement.

After they measure a bit, they let each other know what basis they used to make a measurement. If they chose the same basis, then they keep their measurements, otherwise they discard it.

If they both chose the $\{|0\rangle, |1\rangle\}$ basis, then if Alice measures 0, so did Bob and if Alice measured 1, then so did Bob.

If they both chose the $\{|+\rangle, |-\rangle\}$ basis, then what happens? Recall that

$$\begin{aligned}|0\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)\\ |1\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)\end{aligned}$$

$$\begin{aligned}|00\rangle &= |0\rangle \otimes |0\rangle\\ &= \frac{1}{2}(|+\rangle + |-\rangle) \otimes (|+\rangle + |-\rangle)\\ &= \frac{1}{2}(|{+}{+}\rangle + |{-}{-}\rangle + |{+}{-}\rangle + |{-}{+}\rangle)\\ |11\rangle &= |1\rangle \otimes |1\rangle\\ &= \frac{1}{2}(|+\rangle - |-\rangle) \otimes (|+\rangle - |-\rangle)\\ &= \frac{1}{2}(|{+}{+}\rangle + |{-}{-}\rangle - |{+}{-}\rangle - |{-}{+}\rangle)\end{aligned}$$

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\\ &= \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)\end{aligned}$$

If they both choose the $\{|+\rangle, |-\rangle\}$ basis then they will both measure $|+\rangle$ or they will both measure $|-\rangle$. If Alice measures 0, so did Bob and if Alice measured 1, then so did Bob.

So as long as they measure in the same basis, they both will measure the same bits and can securely create a shared key.

The security of the scheme relies on adding extra steps to the protocol to test the fidelity of the Bell states (aka the EPR pairs).

5.11 Dense Coding. Sending two classical bits via sending one qubit and sharing a Bell pair

Alice wishes to send two classical bits of information to Bob. She and Bob start with a Bell pair state that is shared between them (Alice has the first qubit and Bob has the second)

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

The datum Alice wants to send to Bob has one of 4 values: 00, 01, 10, or 11 in base 2 — or 0, 1, 2, or 3 in base 10. The operation she applies to the Bell pair depend upon

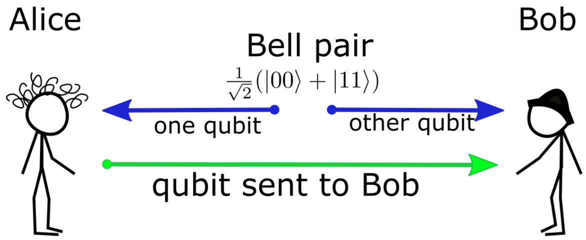

Figure 10: Alice performs operations on one qubit of a Bell pair and then sends her qubit to Bob. Bob performs operations on both qubits and then measures both qubits. Two classical bits of information are sent by Alice to Bob. This is known as *dense coding*.

which datum number she wants to send. She operates on her half of the Bell pair using the following recipe:

Alice's Data and Operations		
Value	Operation	Resulting state
00	$\mathbf{I} \otimes \mathbf{I}$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	$\boldsymbol{\sigma}_x \otimes \mathbf{I}$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
10	$\boldsymbol{\sigma}_z \otimes \mathbf{I}$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
11	$\boldsymbol{\sigma}_y \otimes \mathbf{I}$	$\frac{i}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$

Alice then sends her qubit to Bob. Bob applies the following operations to the 2 qubits, $(H \otimes I)\text{CNOT}\,|\psi\rangle$. In other words, he first applies a CNOT with control bit the first one and target the second qubit, and then he performs a Hadamard op on the first qubit. Bob's operations are shown in quantum circuit form in Figure 11, Afterwards he measures both qubits.

Bob's Operations and Measurements			
$\|\psi\rangle_{\text{received}}$	CNOT(0,1) $\|\psi\rangle$	$\mathbf{H}\otimes\mathbf{I}$ CNOT(0,1)$\|\psi\rangle$	Measurement
$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle+\|10\rangle)=\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)\otimes\|0\rangle$	$\|0\rangle\otimes\|0\rangle$	00
$\frac{1}{\sqrt{2}}(\|10\rangle+\|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle+\|01\rangle)=\frac{1}{\sqrt{2}}(\|1\rangle+\|0\rangle)\otimes\|1\rangle$	$\|0\rangle\otimes\|1\rangle$	01
$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle-\|10\rangle)=\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)\otimes\|0\rangle$	$\|1\rangle\otimes\|0\rangle$	10
$\frac{i}{\sqrt{2}}(-\|10\rangle+\|01\rangle)$	$\frac{i}{\sqrt{2}}(-\|11\rangle+\|01\rangle)=\frac{i}{\sqrt{2}}(-\|1\rangle+\|0\rangle)\otimes\|1\rangle$	$i\,\|1\rangle\otimes\|1\rangle$	11

Here CNOT(0,1) is the CNOT with control bit 0 (the first qubit) that operates on bit 1(the second qubit). I am using the order and notation for the control and operation bits that is used in the `addgate` routine in the python package `qutip`.

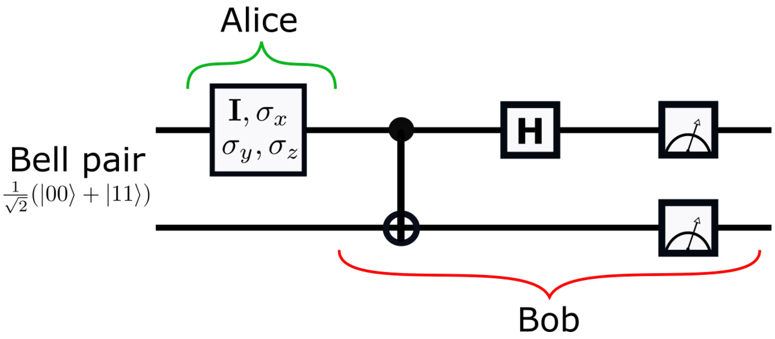

Figure 11: Initially Bob and Alice each have 1 qubit of a Bell pair. Bob receives Alice's qubit after she performs an operation on it. Bob's operations are on the right. This is known as dense coding.

Why is this called *dense coding*? We used 2 qubits to send 2 classical bits of information. Notice that Alice only operated on one of the qubits. The original Bell pair could have been created and then a single qubit sent to Alice and the other sent to Bob. Then Alice operates on her qubit. She does not perform any measurements on it so it remains entangled. She then sends her qubit to Bob who decodes the information she wanted to send by measuring both qubits. Technically Alice only sent 1 qubit to Bob, though a Bell pair was shared prior to the information transfer.

We give another interpretation of the dense coding circuit shown in Figure 11. Each of Alice's operations $\mathbf{I}$, $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_y$, $\boldsymbol{\sigma}_z$ operate on the the Bell pair state and give another maximally entangled state that is perpendicular to the Bell pair state. The set of resulting states is an orthogonal basis known as the Bell basis. Each of the elements of this basis is maximally entangled. Bob's CNOT and Hadamard gate transform from the Bell basis back into the conventional basis. This is why his measurement determines exactly which operation was done by Alice. The Bell basis is discussed in more detail below when we discuss quantum teleportation.

6 Interpretations of Quantum Mechanics

6.1 Thoughts on the EPR paradox

The **EPR paradox** refers to a paper by Albert Einstein, Boris Podolsky, and Nathan Rosen entitled "Can quantum-mechanical description of physical reality be considered complete?"

We start with two particles in a locally generated Bell pair state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Then the two qubits are spit up and Alice is given one of them and Bob is given the other. If Alicee measures 0 then Bob's particle must instantaneously be put in the state $|0\rangle$ and she would then also measure 0. This could be interpreted as transfer of information over large distances in an infinitely small period of time. It may seem like the particles are communicating faster than the speed of light.

What if both Alice and Bob are given a newspaper? They both can simultaneously know the same information. In both cases the information is not actually transferred instantaneously. Hence information is not necessarily transmitted faster than the speed of light. The experimental results can be explained equally well by Bob measuring first and then Alice as in the opposite order. This symmetry shows while there is a correlation between the two measurements, it is not *causal* and Alice and Bob are not communicating faster than the speed of light. This conundrum is known as the **EPR paradox**.

What if particles are not really described by probabilities but rather the uncertainty arises due to local **hidden variables**. In this case particles have an internal hidden state that determines the result of measurements. The hidden state is identical in two particles when the Bell pair is generated. However, the hidden variable is not the same for each generated Bell pair.

This local hidden variables interpretation can be ruled out via Bell's inequalities which we discuss below.

So far we have divided up our operations on quantum states into two categories

1. Unitary evolution. Nobody is watching. No information loss.

2. Measurement. The wave-function is collapsed to a state which is chosen based on a probability described by the wave-function.

This division also presents some paradoxes. If physical laws are based on quantum mechanics why can't everything be described via unitary evolution only? When can we approximate coupling between systems as a measurement?

6.2 Copenhagen interpretation

It's not all that easy to pin down the Copenhagen interpretation. It is more like a set of guiding principles.

In the appropriate limit, quantum theory should resemble classical physics and reproduces the classical predictions. Quantum mechanics obeys different rules than classical physics. The results provided by measuring devices are essentially classical. Measurement involves an interaction between the system and a laboratory device and this interaction 'collapses' the wave function. A wave function is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a system.

The **Born rule**: The wave function gives probabilities for the outcomes of measurements.

The **correspondence principle**: In the appropriate limit, quantum theory should give predictions consistent with classical mechanics.

Complementarity: Certain properties cannot be simultaneously measured on a particular system (this is related to the Heisenberg uncertainty principle).

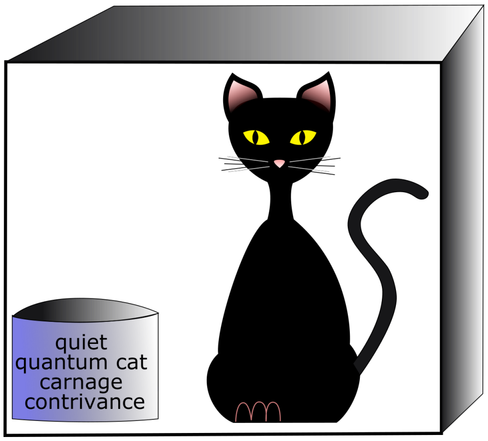

Figure 12: Shrödinger's cat is in a box. A mechanism, here the 'quiet quantum cat carnage contrivance', has probability 1/2 that it will kill the cat. The state of the cat is $|\psi\rangle_{\text{cat}} = \frac{1}{\sqrt{2}}(|\text{dead}\rangle + |\text{alive}\rangle)$. The observer cannot see into the box until after the experiment is done. The observer cannot tell from listening (or any other probe) what is going on inside the box until he or she opens it.

There are now numerous other *interpretations*.

6.3 The many worlds interpretation

For example the *many worlds interpretation* describes the universe with a single wave function that evolves deterministically via unitary evolution. Interactions of objects within the universe can behave like measurements. The subjective appearance of wavefunction collapse is explained by the mechanism of *quantum decoherence*.

The universe's wave function then describes probabilities for ensembles of many universes. Universes diverge after measurements. Apparently it does not matter if entire universes diverge instantaneously or if they diverge only locally with differences between them propagating at the speed of light.

As the idea of multiple universes is not testable (we can only inhabit one), some people think that the many worlds intepretation is not really a theory. In contrast, quantum mechanics is accurately predictive and has been overwhelmingly verified experimentally. In this sense quantum mechanics is a very good theory.

6.4 Shrödinger's cat

Schrödinger's cat is a thought experiment that illustrates an apparent paradox caused by quantum superposition. A cat is in an opaque box. There is a Geiger counter next to some radioactive material. In a single hour, the probability that the Geiger counter counts 1 radioactive decay is 1/2 and counts 0 decays is 1/2. If the Geiger counter counts a decay, then the cat is automatically killed.[3] After the hour is up, the box is opened to see if the cat is alive or dead. During this hour, the cat can be considered to be in a superposition of dead and alive states;

$$|\psi\rangle_{\text{cat}} = \frac{1}{\sqrt{2}} \left(|\text{dead}\rangle + |\text{alive}\rangle\right).$$

In the Copenhagen interpretation, the superposition of states exists only while the box is closed. Only when the box is opened and the cat inside is observed is the cat's wave function collapsed.

However Niels Bohr suggested instead that effectively irreversible processes causes the decay of quantum coherence which imparts the classical behavior of *observation* to the cat. The cat is either alive or dead before the box is opened.

In the many worlds interpretation the universe with the observer and the possibly-dead cat split into a universe with an observer looking at a box with a dead cat, and a universe with an observer looking at a box with a live cat. Since the dead and alive states are decoherent, there is no effective communication or interaction between the two universes.

6.5 EPR polarization measurements

Bell's inequalities which are used to rule out hidden variable interpretations are often discussed in terms of photon polarization. The polarization of a single photon can be described in terms of basis states $|\uparrow\rangle$, corresponding to vertical polarization and $|\rightarrow\rangle$ corresponding to horizontal polarization. A photon can be in a superposition $|\psi\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ where aa^* is the probability that a vertical polarizer allow the photon to pass through it. A photon that passes through a vertical polarizer becomes vertically polarized, $|\psi\rangle \rightarrow \frac{a}{\sqrt{aa^*}}\,|\uparrow\rangle$.

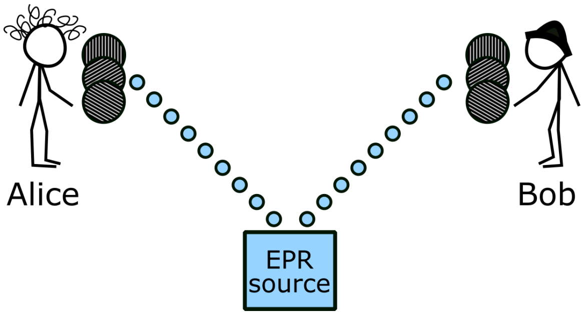

Figure 13: An EPR source of photons generates pairs entangled photons. From each pair, one is sent to Alice and the other is sent to Bob. Alice and Bob individually make polarization measurements.

[3] Apparently Shrödinger's version involved hydrocyanic acid whereas Einstein's version involved gunpowder.

Consider a photon source, called an EPR source (for the Einstein-Podolsky-Rosen paradox) that generates two entangled photons,

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|{\uparrow\uparrow}\rangle + |{\rightarrow\rightarrow}\rangle \right).$$

One photon travels to Alice and the other travels to Bob. Both Alice and Bob can measure the photon polarization, but each of them can measure the polarization in one of three orientations. They can measure the polarization in the vertical direction, at 60° from vertical or at −60° from vertical. The different directions are chosen by changing the orientation of the polarizer.

If they both measure polarization in the same orientation, they will 100% of the time measure the same polarization (whether the photon passes through or is absorbed by the polarizer). This follows if we consider rotations of the Bell state, $R(\theta) \otimes R(\theta)$, for both qubits by the same angle θ. This rotation transfers both qubits to the same new basis. To make a polarization measurement that is an angle, we can rotate the measurement and projection operators and keep the state vector in the same basis or equivalently we can rotate the basis of the state vector and use diagonal matrices for measuring the polarization.

We describe photon polarization with basis vectors $|{\uparrow}\rangle, |{\rightarrow}\rangle$ and in vector form

$$|{\uparrow}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |{\rightarrow}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

$|{\uparrow}\rangle$ is a photon that passes through a vertical polarizer but is absorbed by horizontal polarizer. $|{\rightarrow}\rangle$ is a photon that passes through a horizontal polarizer but is absorbed by vertical polarizer.

A photon that passes through a vertical polarizer is in the state $|{\uparrow}\rangle$. Afterwards what happens if we try to measure it through a polarizer that is rotated by θ? We can rotate the basis with

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Notice that if $\theta = \pi/2$ that this rotation matrix sends $|{\uparrow}\rangle \to |{\rightarrow}\rangle$ and $|{\rightarrow}\rangle \to -|{\uparrow}\rangle$ as we might expect. Rotating the basis (by θ) prior to measurement is equivalent to measuring in a basis that is rotated by θ.

If the state is $|{\uparrow}\rangle$ and we rotate the basis by θ

$$\begin{aligned} |\psi\rangle &= R(\theta)\,|{\uparrow}\rangle \\ &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} \\ &= \cos\theta\,|{\uparrow}\rangle + \sin\theta\,|{\rightarrow}\rangle. \end{aligned}$$

When measured through a polarizer at angle θ we have a probability of $\cos^2\theta$ of the polarizer passing the photon and a probability of $\sin^2\theta$ that the polarizer will absorb the photon.

We now return to discussing Bell pair state for two photons. What happens if Alice measures the polarization of the first qubit in the vertical direction and Bob measures it at angle θ? We rotate the basis of the second qubit

$$\begin{aligned}
|\psi\rangle' &= \mathbf{I} \otimes R(\theta) \frac{1}{\sqrt{2}} \left(|{\uparrow\uparrow}\rangle + |{\rightarrow\rightarrow}\rangle \right) \\
&= \mathbf{I} \otimes \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \frac{1}{\sqrt{2}} \left(|{\uparrow\uparrow}\rangle + |{\rightarrow\rightarrow}\rangle \right) \\
&= \frac{1}{\sqrt{2}} \left(\cos\theta \, |{\uparrow\uparrow}\rangle + \sin\theta \, |{\rightarrow\uparrow}\rangle - \sin\theta \, |{\uparrow\rightarrow}\rangle + \cos\theta \, |{\rightarrow\rightarrow}\rangle \right).
\end{aligned}$$

This rotation lets us mimic measurement of the second photon with a polarizer rotated by angle θ.

We label photons that pass through a polarizer as P and those that are absorbed by A.

We measure the first photon with a vertical polarizer. The probability is $1/2$ that the polarization of the first photon is vertical (passing through the polarizer, giving P) and after measurement the state vector is $|\psi\rangle = \cos\theta \, |{\uparrow\uparrow}\rangle - \sin\theta \, |{\uparrow\rightarrow}\rangle$. Afterwards we measure the second photon. The probability is $\cos^2\theta$ that the second qubit passes (P) through the polarizer aligned with θ and $\sin^2\theta$ that it is absorbed (A).

Polarization Measurements of the EPR source (Quantum)					
State	$\frac{1}{\sqrt{2}} \left(\cos\theta \, \lvert{\uparrow\uparrow}\rangle + \sin\theta \, \lvert{\rightarrow\uparrow}\rangle - \sin\theta \, \lvert{\uparrow\rightarrow}\rangle + \cos\theta \, \lvert{\rightarrow\rightarrow}\rangle \right)$				
Measurement First photon	New Wavevector	Probability	Measurement Second photon	New Wavevector	Probability
P	$\cos\theta \, \lvert{\uparrow\uparrow}\rangle - \sin\theta \, \lvert{\uparrow\rightarrow}\rangle$	$\frac{1}{2}$	P	$\cos\theta \, \lvert{\uparrow\uparrow}\rangle$	$\cos^2\theta$
P	$\cos\theta \, \lvert{\uparrow\uparrow}\rangle - \sin\theta \, \lvert{\uparrow\rightarrow}\rangle$	$\frac{1}{2}$	A	$-\sin\theta \, \lvert{\uparrow\rightarrow}\rangle$	$\sin^2\theta$
A	$\sin\theta \, \lvert{\rightarrow\uparrow}\rangle + \cos\theta \, \lvert{\rightarrow\rightarrow}\rangle$	$\frac{1}{2}$	P	$\sin\theta \, \lvert{\rightarrow\uparrow}\rangle$	$\sin^2\theta$
A	$\sin\theta \, \lvert{\rightarrow\uparrow}\rangle + \cos\theta \, \lvert{\rightarrow\rightarrow}\rangle$	$\frac{1}{2}$	A	$\cos\theta \, \lvert{\rightarrow\rightarrow}\rangle$	$\cos^2\theta$

Similarly the probability is $1/2$ that the polarization of the first photon is horizontal and is absorbed (giving A) by the polarizer. After measurement $|\psi\rangle = \sin\theta \, |{\rightarrow\uparrow}\rangle + \cos\theta \, |{\rightarrow\rightarrow}\rangle$ and the probability is $\sin^2\theta$ that the second photon has polarization aligned with θ (giving a P).

The probability that Alice and Bob's measurements agree (either both passing through PP or both absorbed by the polarizers AA) is

$$P_{\text{agree}} = \frac{1}{2}\cos^2\theta + \frac{1}{2}\cos^2\theta = \cos^2\theta. \tag{47}$$

If $\theta = 60°$, the probability that their measurements agree is 1/4. Here we asserted that the polarizers were like this $\uparrow\nearrow$ as Alice's was up and Bob's was at 60°. We summarize:

$$\text{QM : for Polarizers } \uparrow\nearrow,\ p_{\text{agree}} = \frac{1}{4}. \tag{48}$$

Exploiting the symmetry of the problem, we make a table of the possible orientations for Alice and Bob's polarizers and the probability that their measurements agree. Here $\nearrow, \nwarrow$ are the ±60° orientations.

Quantum EPR Measurements		
Alice's polarizer	Bob's polarizer	probability meas. agree
$\uparrow$	$\uparrow$	1
$\uparrow$	$\nearrow$	1/4
$\uparrow$	$\nwarrow$	1/4
$\nearrow$	$\uparrow$	1/4
$\nearrow$	$\nearrow$	1
$\nearrow$	$\nwarrow$	1/4
$\nwarrow$	$\uparrow$	1/4
$\nwarrow$	$\nearrow$	1/4
$\nwarrow$	$\nwarrow$	1

To fill this table, notice that the angle between $\nwarrow$ and $\nearrow$ is 120°. We compute $\cos^2 120° = \cos^2 60° = \frac{1}{4}$.

What if Alice and Bob randomly choose orientations for their polarizers? Then each row of the above table is equally likely. One third of the possible rows in this table always give agreement. The probability is 1/3 that they will measure have the same polarizer orientation and it is 2/3 that they will not. Altogether the probability that their measurements agree is

$$p_{agree} = \frac{1}{3} + \frac{2}{3} \times \frac{1}{4} = \frac{4}{12} + \frac{2}{12} = \frac{1}{2}.$$

Alice's and Bob's measurements should agree half of the time!

6.6 EPR polarization measurements with hidden variables

Suppose there is some hidden state associated with each photon that determines the result of measuring the photon with a polarizer in each of the three possible settings. We list the possible polarization measurements with P for pass and A for absorb. We can refer to these possibilities as covering the possible range of hidden states.

The idea is that the choice of the hidden variables determines the polarization measurement results ahead of time. We choose three possible polarization orientations $\nwarrow, \nearrow, \uparrow$.

The hidden variables determine the measurement outcomes P or A for each of these three possible orientations.

Later on Alice and Bob each separately chose an orientation and measure the polarization of their photons but the outcome of these measurements would have been determined ahead of time from the hidden variables. The hidden variables are created or fixed when the two photons are created.

As Alice and Bob can chose three different orientations $\nwarrow, \nearrow, \uparrow$ for their polarizers we fill the following table. Whether the photon passes or is absorbed is set by the hidden variables.

Hidden variables states			
$\nearrow$	$\uparrow$	$\nwarrow$	p_{agree}
P	P	P	1
P	P	A	
P	A	P	
P	A	A	
A	P	P	
A	P	A	
A	A	P	
A	A	A	1

We expect that two polarization measurements will agree for the two photon Bell state if the measurements of individual photons are the same or if the hidden states give PPP or AAA. I added a third column in the above table giving $p_{agree} = 1$ for these two possible hidden variable states.

Let us consider the second line with PPA and list the possibilities for each possible measurement.

Hidden variables are PPA for $\nearrow \uparrow \nwarrow$			
Alice's polarizer	Bob's polarizer	PPA meas. Al/Bob	meas. agree
$\uparrow$	$\uparrow$	PP	yes
$\uparrow$	$\nearrow$	PP	yes
$\uparrow$	$\nwarrow$	PA	no
$\nearrow$	$\uparrow$	PP	yes
$\nearrow$	$\nearrow$	PP	yes
$\nearrow$	$\nwarrow$	PA	no
$\nwarrow$	$\uparrow$	AP	no
$\nwarrow$	$\nearrow$	AP	no
$\nwarrow$	$\nwarrow$	AA	yes

We see that there are 5 cases where the measurements agree so the probability is 5/9 of measurements agreeing if the photon variables were in the PPA state. Using the symmetry of the problem, we can fill in the table of hidden states.

Hidden variable states			
$\nearrow$	$\uparrow$	$\nwarrow$	p_{agree}
P	P	P	1
P	P	A	5/9
P	A	P	5/9
P	A	A	5/9
A	P	P	5/9
A	P	A	5/9
A	A	P	5/9
A	A	A	1

What is the probability that the measurements agree?

$$p_{agree} = \frac{1}{8}\left(2 \times 1 + 6 \times \frac{5}{9}\right) = \frac{1}{8}\left(\frac{6}{3} + \frac{10}{3}\right) = \frac{16}{3 \times 8} = \frac{2}{3}$$

This exceeds the 1/2 expected (and verified experimentally) from the Quantum measurement in section 6.5.

6.7 Bell's inequality

Bell's inequality is a generalization of the preceding two sections. Polarizers can be set at any triple of three distinct angles a, b, and c. P_{ab} is the sum of the probability that both photons both pass through or both are absorbed with the first polarizer at angle a and the second at angle b, and the probability that both photons both pass or both are absorbed with the first polarizer at angle b and the second at angle a.

For any local hidden variable (HV) theory,

$$HV: \qquad P_{ab} + P_{ac} + P_{bc} \geq 1. \tag{49}$$

This is **Bell's inequality**.

Quantum mechanics allows Bell's inequality to be violated. For example, in section 6.5 we determined that the probability that Alice's and Bob's polarization measurements agree if Alice's polarizer is vertical and Bob's polarizer is at 60° is 1/4 (see equation 48). This means that $P_{\uparrow\nearrow} = \frac{1}{4}$. Because of symmetry, $P_{\uparrow\nwarrow} = \frac{1}{4}$. With the two polarizers separated by angle θ, the probability that the two measurements agree is equal to $\cos^2\theta$

(equation 47). For $P_{\nearrow\nwarrow}$ the two polarizers differ by 120° and the probability is also 1/4 as $\cos 120^\circ = -1/2$.

The sum of

$$QM: \qquad P_{\uparrow\nearrow} + P_{\uparrow\nwarrow} + P_{\nearrow\nwarrow} = 3/4, \tag{50}$$

and as this is less than 1, the inequality of equation 49 is violated.

We now show how equation 49 is derived. According to a local hidden-variable theory, the result of measuring a photon by a polarizer in each of the three possible settings is determined by a local hidden state h of the photon. Any measurement has only two possible outcomes P (for pass) and A (for absorb). We assume if Alice and Bob's polarizers are oriented the same, their measurements or outcomes will agree on an EPR pair. This implies that for an EPR pair, the hidden state is the same for both photons.

Let P^h_{ab} be 1 if the measurements agree for hidden state h and be zero otherwise. The two photons in the EPR pair are assumed to be in the same hidden state h. Outcomes can only be P or A. We have three things a, b, c that can be P or A. There are 8 ways to choose P or A for a, b or c. P^h_{ab}, P^h_{bc} and P^h_{ac} can either be 1 or 0, corresponding to agreeing or disagreeing. With three things a, b, c that can be P or A, one pair of ab, bc, ac must have two values that agree. This means that one of P_{ab}, P_{bc}, P_{ac} must be 1. This implies that for the state h

$$HV: \qquad P^h_{ab} + P^h_{bc} + P^h_{ac} \geq 1.$$

Consider a probability distribution for the hidden variable states h, where $w_h \geq 0$ is the probability that the EPR source emits photons of kind h. As w_h gives the probability of each kind of hidden variable,

$$\sum_h w_h = 1.$$

The sum

$$P_{ab} + P_{bc} + P_{ac} = \sum_h w_h (P^h_{ab} + P^h_{bc} + P^h_{ac}).$$

The weighted average (where weights are positive and sum to 1) of a sum of terms, each of which is greater than 1, must also be greater than 1. Hence

$$HV: \qquad P_{ab} + P_{bc} + P_{ac} \geq 1. \tag{51}$$

We have shown that a local hidden variable theory satisfies Bell's inequality.

Let's check how this relates to the hidden variable assumptions we made in section 6.6.

Hidden variable states - Probabilities for pairs						
Hidden vars $\nwarrow\uparrow\nearrow$	a b $\uparrow\nearrow$	agree	b c $\nwarrow\nearrow$	agree	c a $\nwarrow\uparrow$	agree
PPP	PP	y	PP	y	PP	y
PPA	PA	n	PA	n	PP	y
PAP	AP	n	PP	y	PA	n
PAA	AA	y	PA	n	PA	n
APP	PP	y	AP	n	AP	n
APA	PA	n	AA	y	AP	n
AAP	AP	n	AP	n	AA	y
AAA	AA	y	AA	y	AA	y
	P_{ab}		P_{bc}		P_{ca}	
	$\frac{1}{2}$		$\frac{1}{2}$		$\frac{1}{2}$	

For the hidden variable states we assumed in section 6.6

$$HV: \qquad P_{ab} + P_{bc} + P_{ac} = \frac{3}{2} \tag{52}$$

which exceeds 1, as expected from Bell's inequality (eqn 49).

So which description is correct, the hidden variable inequality (equation 52) or the quantum mechanical one (equation 50)? The quantum mechanical description has been experimentally verified. Bell's inequality is in fact violated in laboratory experiments.

7 Teleportation with a Bell pair

We describe how an unknown state can be transferred from one qubit to another with a series of measurements and two qubits in an entangled state.

We have three qubits. Two of them are in an entangled Bell pair state. Alice has a single qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ where a, b are not known. She wants to teleport its state to Bob. Alice can measure 1 qubit of the Bell pair and Bob can measure the other qubit in the Bell pair.

- Alice performs a transformation on a qubit $|\psi\rangle$ that entangles it with the Bell pair.
- Alice measures the transformed qubit **and** her qubit that is part of the entangled pair.
- Alice tells Bob (via classical communication) what she has measured.
- Bob performs a transformation on his half of the entangled qubit pair that depends on these measurements.
- Bob now holds the information that was in $|\psi\rangle$.

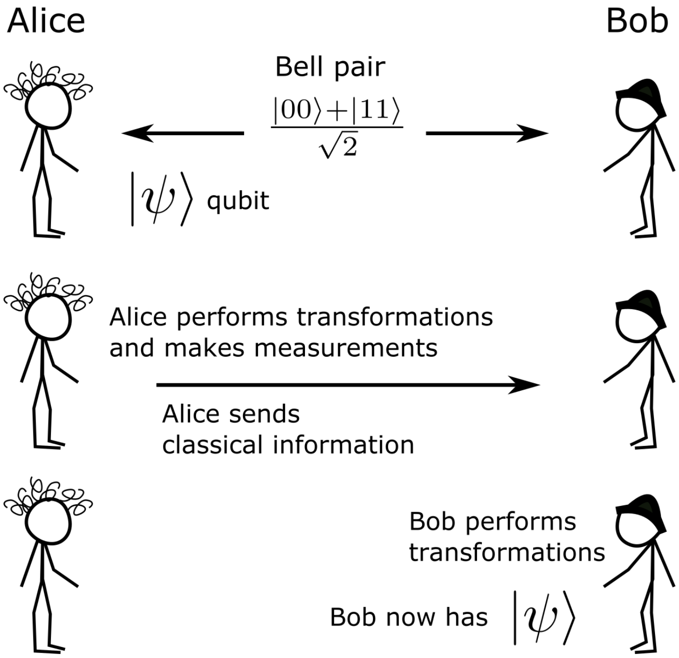
Alice
Bob
Bell pair
$\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
$|\psi\rangle$ qubit
Alice performs transformations and makes measurements
Alice sends classical information
Bob performs transformations
Bob now has $|\psi\rangle$

Figure 14: Teleportation of an unknown qubit state $|\psi\rangle$.

- Alice no longer holds the information that was in $|\psi\rangle$.
- The information that was in $|\psi\rangle$ (the values of a, b) has teleported to Bob.

We assume that the first qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. The second and third qubits are in a Bell pair state. Initial the state taking into account all three qubits

$$|\psi\rangle_{ABC} = (a\,|0\rangle + b\,|1\rangle) \otimes \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$$

This can be written as

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\,(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle)\,. \tag{53}$$

Alice performs the CNOT gate on the total state with target the second qubit and control the first qubit. The CNOT gate flips the second qubit if the first one is 1. The total state becomes

$$\frac{1}{\sqrt{2}}\,(a\,|000\rangle + a\,|011\rangle + b\,|110\rangle + b\,|101\rangle)\,.$$

Alice performs a Hadamard operation on the first qubit. The total state becomes

$$\frac{1}{2}\,(a\,|000\rangle + a\,|100\rangle + a\,|011\rangle + a\,|111\rangle - b\,|110\rangle + b\,|010\rangle - b\,|101\rangle + b\,|001\rangle)\,.$$

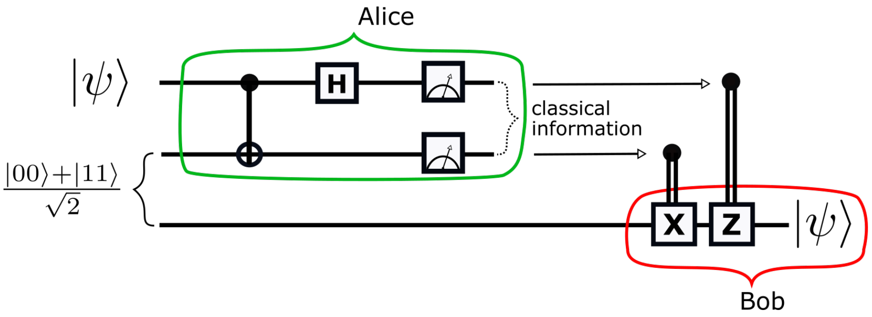

Figure 15: A recipe for teleporting a qubit $|\psi\rangle$ using two additional entangled qubits, a CNOT, a Hadamard operation and two measurements. Alice and Bob share an entangled state. The transmitter (Alice) applies the CNOT and the Hadamard and makes the two measurements. The transmitter then tells the receiver the results of the two measurements. The receiver (Bob) applies a transformation on the third qubit that is based on the measurements of the first two qubits. The receiver then holds the third qubit which has become identical to $|\psi\rangle$, the original state of the first qubit.

Alice now measures the first two bits. She can measure 0,0 with a probability of $1/4(aa^* + bb^*) = 1/4$. If this happens the state becomes

$$a\,|000\rangle + b\,|001\rangle\,.$$

All her possible measurements are equally likely.

Let's make a table summarizing all possible measurements.

Alice measures the first two qubits				
Alice measures	00	01	10	11
The state becomes	$a\,\|000\rangle + b\,\|001\rangle$	$a\,\|011\rangle + b\,\|010\rangle$	$a\,\|100\rangle - b\,\|101\rangle$	$a\,\|111\rangle - b\|110\rangle$

Alice sends her measurements to Bob who then performs the following transformations on the last qubit.

If the second bit that Alice measures is 1, Bob applies $\boldsymbol{\sigma}_x$ to his qubit,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This swaps $|1\rangle \rightarrow |0\rangle$ and vice versa.

If the first bit that Alice measures is 1, Bob applies $\boldsymbol{\sigma}_z$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

to the last qubit. This flips the sign of $|1\rangle$.

The order that Bob performs these operations is not all important. However as $\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z = -\boldsymbol{\sigma}_z\boldsymbol{\sigma}_x$, there is a difference in the sign of the state vector that depends on the order of the operations which only occurs if if both bits are measured to be 1. This is a global phase, so it is not necessarily important.

Let's apply these transformations to the above table:

Alice measures	00	01	10	11
The state is now	$a\,\|000\rangle + b\,\|001\rangle$	$a\,\|011\rangle + b\,\|010\rangle$	$a\,\|100\rangle - b\,\|101\rangle$	$a\,\|111\rangle - b\,\|110\rangle$
Bob applies	$\mathbf{I}\otimes\mathbf{I}\otimes\mathbf{I}$	$\mathbf{I}\otimes\mathbf{I}\otimes\boldsymbol{\sigma}_x$	$\mathbf{I}\otimes\mathbf{I}\otimes\boldsymbol{\sigma}_z$	$\mathbf{I}\otimes\mathbf{I}\otimes(\boldsymbol{\sigma}_z\boldsymbol{\sigma}_x)$
The state becomes	$a\,\|000\rangle + b\,\|001\rangle$	$a\,\|010\rangle + b\,\|011\rangle$	$a\,\|100\rangle + b\,\|101\rangle$	$a\,\|110\rangle + b\,\|111\rangle$
Which is equal to	$\|00\rangle\otimes(a\|0\rangle+b\|1\rangle)$	$\|01\rangle\otimes(a\|0\rangle+b\|1\rangle)$	$\|10\rangle\otimes(a\|0\rangle+b\|1\rangle)$	$\|11\rangle\otimes(a\|0\rangle+b\|1\rangle)$

Examining this table we see that the state vector that was initially in the first bit has been transported (teleported) to the third bit.

Note: Alice never knew what a, b were. At the end, there is nothing left of interest in the first two bits as both Alice and Bob know what they are. The Bell pair is 'used up'.

With more Bell pairs, more qubit states can be teleported. If two qubits are teleported and they are initially entangled, the resulting teleported state will also be entangled.

7.1 The Bell basis

For a two qubit system it is possible to create a basis from states that are like the Bell pair.

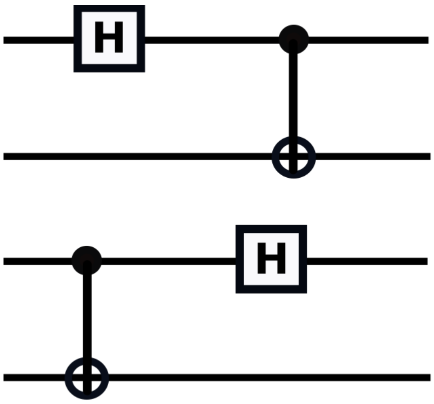

Figure 16: For the top circuit and starting with state $|00\rangle$ input on the left, the result on the right is the Bell pair state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The bottom circuit shows the inverse transformation of that given in the top circuit.

Consider the top circuit in Figure 16. We compute

$$\begin{aligned}
|00\rangle &\to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \equiv \left|\Phi^+\right\rangle \\
|01\rangle &\to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \equiv \left|\Psi^+\right\rangle \\
|10\rangle &\to \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \equiv \left|\Phi^-\right\rangle \\
|11\rangle &\to \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \equiv \left|\Psi^-\right\rangle .
\end{aligned} \tag{54}$$

The resulting 4 states are orthogonal to each other. They form a basis of entangled states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$ which is called the Bell basis. The top circuit in Figure 16 transforms between the conventional basis and the Bell basis.

What is the inverse transform? The inverse of the Hadamard gate is itself and the inverse of the CNOT is also itself. That means that if you reverse the order of the Hadamard and the CNOT gates you will have the inverse transformation, as shown in the bottom of Figure 16. The inverse transformation

$$\begin{aligned}
\frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle) &= |00\rangle \\
\frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle) &= |11\rangle \\
\frac{1}{\sqrt{2}}(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle) &= |01\rangle \\
\frac{1}{\sqrt{2}}(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle) &= |10\rangle .
\end{aligned} \tag{55}$$

What if we measure both bits after transferring to the Bell basis? Consider the circuit shown in Figure 17.

It is convenient to notice that

$$\begin{aligned}
\mathbf{X}_1 \left|\Phi^+\right\rangle &= \mathbf{X}_1 \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = \left|\Psi^+\right\rangle \\
\mathbf{Z}_1 \left|\Phi^+\right\rangle &= \mathbf{X}_1 \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \left|\Phi^-\right\rangle \\
\mathbf{Z}_1\mathbf{X}_1 \left|\Phi^+\right\rangle &= \mathbf{Z}_1 \left|\Psi^+\right\rangle = \mathbf{Z}_1 \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \left|\Psi^-\right\rangle .
\end{aligned}$$

Here $\mathbf{X}_1$ refers to operating with a Pauli X gate on the first qubit. The Pauli matrices can be used to convert one Bell basis vector to another. The Bell basis states also satisfy

$$\begin{aligned}
\mathbf{X}_1 \left|\Phi^+\right\rangle &= \mathbf{X}_2 \left|\Phi^+\right\rangle \\
\mathbf{Z}_1 \left|\Phi^+\right\rangle &= \mathbf{Z}_2 \left|\Phi^+\right\rangle \\
\mathbf{Z}_1\mathbf{X}_1 \left|\Phi^+\right\rangle &= -\mathbf{Z}_2\mathbf{X}_2 \left|\Phi^+\right\rangle ,
\end{aligned}$$

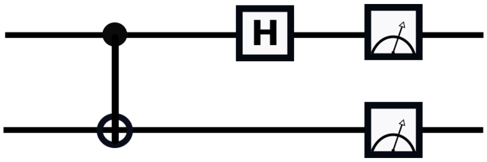

Figure 17: This circuit makes measurements in the Bell basis with $|\Phi^+\rangle$ giving 00, $|\Psi^+\rangle$ giving 01, $|\Phi^-\rangle$ giving 10, and $|\Psi^-\rangle$ giving 11.

If the initial state is a Bell basis state then the measurements are

$$\begin{array}{ll} \left|\Phi^+\right\rangle \to |00\rangle & \text{00 measured} \\ \left|\Psi^+\right\rangle \to |10\rangle & \text{01 measured} \\ \left|\Phi^-\right\rangle \to |10\rangle & \text{10 measured} \\ \left|\Psi^-\right\rangle \to |11\rangle & \text{11 measured} \end{array}$$

where $\mathbf{Z}_2$ is the Pauli Z gate operating on the second qubit. The last statement can also be written as $\mathbf{Y}_1 |\Phi^+\rangle = -\mathbf{Y}_2 |\Phi^+\rangle$ because $\mathbf{ZX} = i\mathbf{Y}$. By applying additional Pauli gates it is possible to show that

$$\mathbf{V}_1 |\Phi\rangle = \pm \mathbf{V}_2 |\Phi\rangle \tag{56}$$

where $|\Phi\rangle$ is *any* of the Bell basis states and $\mathbf{V}$ is *any* of the single bit Pauli matrices. Except for a global phase, a single Pauli operation $(X, Y$ or $Z)$ in one qubit on a Bell basis state, is equivalent to the same operation on the other qubit.

7.2 Teleportation with the Bell basis

The Bell basis is useful for understanding the teleportation protocol shown in Figure 15. Notice that the Hadamard and CNOT applied on the first two qubits transform the Bell basis into the conventional basis.

The initial state is (from equation 53)

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \left(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle \right). \tag{57}$$

We write the first two qubits in terms of the Bell basis for the first two qubits using equation 55

$$
\begin{aligned}
a\,|000\rangle &= \frac{a}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{AB} + |\Phi_{-}\rangle_{AB}) \otimes |0\rangle_C \\
a\,|011\rangle &= \frac{a}{\sqrt{2}}(\left|\Psi^{+}\right\rangle_{AB} + |\Psi_{-}\rangle_{AB}) \otimes |1\rangle_C \\
b\,|100\rangle &= \frac{b}{\sqrt{2}}(\left|\Psi^{+}\right\rangle_{AB} - |\Psi_{-}\rangle_{AB}) \otimes |0\rangle_C \\
b\,|111\rangle &= \frac{b}{\sqrt{2}}(\left|\Phi^{+}\right\rangle_{AB} - |\Phi_{-}\rangle_{AB}) \otimes |1\rangle_C \,.
\end{aligned}
$$

We insert these into equation 57 and group terms by the Bell basis states for the first two qubits

$$
\begin{aligned}
|\psi\rangle_{ABC} = \frac{1}{2}\Big[\, &\left|\Phi^{+}\right\rangle_{AB} \otimes (a\,|0\rangle_C + b\,|1\rangle_C) + \left|\Phi^{-}\right\rangle_{AB} \otimes (a\,|0\rangle_C - b\,|1\rangle_C) \\
&+ \left|\Psi^{+}\right\rangle_{AB} \otimes (a\,|1\rangle_C + b\,|0\rangle_C) + \left|\Psi^{-}\right\rangle_{AB} \otimes (a\,|1\rangle_C - b\,|0\rangle_C)\Big]. \qquad (58)
\end{aligned}
$$

With the application of the CNOT and the Hadamard, the Bell basis for the first two qubits is transformed into the conventional basis. That means $|\Phi^{+}\rangle_{AB} \to |00\rangle_{AB}$. The measurements made by Alice depend on the Bell basis vector in the first two qubits in $|\psi\rangle_{ABC}$.

The new state-vector becomes

$$
\begin{aligned}
\mathbf{H}_0 \boldsymbol{\Lambda}_{t=1}^{c=0}(\mathbf{X})\,|\psi\rangle_{ABC} = \frac{1}{2}\Big[\, &|00\rangle_{AB} \otimes (a\,|0\rangle_C + b\,|1\rangle_C) + |10\rangle_{AB} \otimes (a\,|0\rangle_C - b\,|1\rangle_C) \\
&+ |01\rangle_{AB} \otimes (a\,|1\rangle_C + b\,|0\rangle_C) + |11\rangle_{AB} \otimes (a\,|1\rangle_C - b\,|0\rangle_C)\Big]. \qquad (59)
\end{aligned}
$$

Here the Hadamard operating on the first qubit (with index 0) is $\mathbf{H}_0$ and $\boldsymbol{\Lambda}_{t=1}^{c=0}(\mathbf{X})$ refers to the CNOT with control the first qubit (with index 0) and target the second one (with index 1). The order of the operations is right to left in the above equation but left to right in Figure 15.

If 00 is measured by Alice, corresponding to the initial $|\Phi^{+}\rangle_{AB}$ in the first two qubits, then the third qubit has $a\,|0\rangle_C + b\,|1\rangle_C$ which is equal to $|\psi\rangle$.

If 01 is measured, corresponding to the initial $|\Psi^{+}\rangle_{AB}$ in the first two qubits, then the bits are flipped with $\mathbf{X}$ (swap on the third bit) and the third qubit again becomes $|\psi\rangle$.

If 10 is measured, corresponding to the initial $|\Phi^{-}\rangle_{AB}$ in the first two qubits, then a $\mathbf{Z}$ is applied on the third bit and the third qubit again becomes $|\psi\rangle$.

If 11 is measured, corresponding to the initial $|\Psi^{-}\rangle_{AB}$ in the first two qubits, then a $\mathbf{XZ}$ is applied on the third bit and the third qubit again becomes $|\psi\rangle$.

The teleportation circuit makes measurements in the Bell basis in the first 2 qubits. We denote the bits as ABC. Let the first qubit $|\psi\rangle_A = \sum_{i=0}^{1} a_i\,|i\rangle_A$. The Bell pair state in the second two qubits can be written as

$$\left|\Phi^+\right\rangle_{BC} = \sum_{j=0}^{1} \left|j\right\rangle_B \left|j\right\rangle_C .$$

The initial state

$$\begin{aligned} \left|\psi\right\rangle_{ABC,init} &= \left|\psi\right\rangle_A \left|\Phi^+\right\rangle_{BC} \\ &= \sum_{i,j} a_i \left|i\right\rangle_A \left|j\right\rangle_B \left|j\right\rangle_C . \end{aligned}$$

In the teleportation protocol, as measurement is done in the Bell basis, after measurement the first two qubits are in one of the Bell basis states and we know which one it is in. That means the first two qubits have been projected into the state $\mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}$ where $\mathbf{V}_1^{mn}$ is a gate (either $\mathbf{I}$, $\mathbf{X}_1$, $\mathbf{Z}_1$ or $\mathbf{Z}_1\mathbf{X}_1$) operating on the first qubit that depends upon which Bell basis state was measured. Here mn are the measured bit values.

If bits mn are measured, then the measured state in the first two qubits is

$$\left|\psi\right\rangle_{AB,measured}^{mn} = \mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB} = \mathbf{V}_1^{mn} \sum_{i=0}^{1} \left|i\right\rangle_A \left|i\right\rangle_B .$$

We form a projection operator for measurements of the first two qubits in the Bell basis

$$\begin{aligned} \mathbf{P}^{mn} &= \left|\psi\right\rangle_{AB,measured}^{mn} \left\langle\psi\right|_{AB,measured}^{mn} \\ &= \mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right|_{AB}\mathbf{V}_1^{\dagger,mn}. \end{aligned} \tag{60}$$

What does the final state look like for all three qubits? We project using the measured state constructed from the 2 qubit projection operator

$$\begin{aligned} \left|\psi\right\rangle_{ABC,measured}^{mn} &= \mathbf{P}^{mn}\left|\psi\right\rangle_{ABC,init} \\ &= \mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right|_{AB}\mathbf{V}_1^{\dagger,mn}\left|\psi\right\rangle_A\left|\Phi^+\right\rangle_{BC} \\ &= \pm\mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right|_{AB}\mathbf{V}_2^{\dagger,mn}\left|\psi\right\rangle_A\left|\Phi^+\right\rangle_{BC} \\ &= \pm\mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right|_{AB}\left|\psi\right\rangle_A\mathbf{V}_2^{\dagger,mn}\left|\Phi^+\right\rangle_{BC} \\ &= \pm\mathbf{V}_1^{mn}\left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right|_{AB}\left|\psi\right\rangle_A\mathbf{V}_3^{\dagger,mn}\left|\Phi^+\right\rangle_{BC} , \end{aligned} \tag{61}$$

where we have used the relation in equation 56 multiple times. Let us compute

$$\begin{aligned}
\left\langle\Phi^+\right|_{AB} \left|\psi\right\rangle_A &= \sum_{i=0}^{1} \left\langle i\right|_A \left\langle i\right|_B \sum_{j=0}^{1} a_j \left|j\right\rangle_A \\
&= \sum_{i,j=0}^{1} \left\langle i\right|_A \left\langle i\right|_B \sum_{j=0}^{1} a_j \left|j\right\rangle_A \delta_{ij} \\
&= \sum_{i=0}^{1} a_i \left\langle i\right|_B . \qquad (62)
\end{aligned}$$

This illustrates that it is possible to transfer information from one qubit to another using the Bell pair state.

Insert this into equation 61

$$\begin{aligned}
\left|\psi\right\rangle_{ABC,measured}^{mn} &= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \sum_{i=0}^{1} a_i \left\langle i\right|_B \mathbf{V}_3^{\dagger,mn} \left|\Phi^+\right\rangle_{BC} \\
&= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \mathbf{V}_3^{\dagger,mn} \sum_{i=0}^{1} a_i \left\langle i\right|_B \left|\Phi^+\right\rangle_{BC} \\
&= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \mathbf{V}_3^{\dagger,mn} \sum_{i,j=0}^{1} a_i \left\langle i\right|_B \left|j\right\rangle_B \left|j\right\rangle_C \\
&= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \mathbf{V}_3^{\dagger,mn} \sum_{i,j=0}^{1} a_i\delta_{ij} \left|j\right\rangle_C \\
&= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \mathbf{V}_3^{\dagger,mn} \sum_{i=0}^{1} a_i \left|i\right\rangle_C \\
&= \pm\mathbf{V}_1^{mn} \left|\Phi^+\right\rangle_{AB} \mathbf{V}_3^{\dagger,mn} \left|\psi\right\rangle_C .
\end{aligned}$$

Since Alice tells Bob which Bell pair state is measured in the first two qubits, Bob can chose to apply the inverse of $\mathbf{V}_3^{\dagger,mn}$ to the third qubit. He applies $[\mathbf{V}_3^{\dagger,mn}]^{-1}$ to the third qubit and the result is $\left|\psi\right\rangle_C$ up to a global phase.

The algorithm uses the fact that Bell basis states can be used to transfer information from one qubit to another (as in equation 62). The algorithm also exploits the fact that the single qubit Pauli gates operate on all qubits in Bell basis states in a similar manner.