Quantum Information and Quantum Computation

Vibhav Aggarwal*

April 2020

Contents

*Mentored by Neeraj Sohani

0 Introduction

Quantum computation and quantum information is the study of the information processing tasks that can be accomplished using quantum mechanical systems. It is relatively a newer field of research and much work is going on to actually make a functional quantum computer. Big tech companies like Google, Microsoft, Hitachi, Mitsubishi, Nokia, etc. are investing huge amounts of money in research and development of quantum computers.

But why? What is so special about this field that so many people are interested in it? Turns out, quantum computers offer an essential speed advantage over classical computers. This speed advantage is so significant that many researchers believe that no conceivable amount of progress in classical computation would be able to overcome the gap between the power of a classical computer and the power of a quantum computer!

For example, the RSA cryptosystem used for transferring data in secure manner is just based on the fact that it is very difficult for a classical computer to factorize large numbers (order of 2048 bits) quickly. Till date there is simply no known algorithm to that efficiently on a classical computer. However, there is an algorithm known as Shor's algorithm which can just do that really quickly on a quantum computer.

There are many other algorithms based upon quantum computers and one class of such algorithms is the *quantum search algorithms*. The quantum search algorithm solves the following problem: Given a search space of size N, and no prior knowledge about the structure of the information in it, we want to find an element of that search space satisfying a known property. How long does it take to find an element satisfying that property? Classically, this problem requires approximately N operations, but the quantum search algorithm allows it to be solved using approximately $\sqrt{N}$ operations.

Another important use is *quantum simulation*. Simulation of quantum systems on classical machines is difficult and the space requirement grows exponentially with increasing number of components in the system. But in case of quantum computers, this growth is linear and therefore they can be used in quantum chemistry to simulate large molecules and study the inter-atomic interactions.

1 Quantum bits (qubits)

The *bit* is the fundamental concept of classical computation. It has only two possible states: 0 and 1. Any information can be represented by a combination of bits. Using n bits, a total of 2^n different messages can be represented/conveyed.

Quantum computation and quantum information are built upon an analogous concept, the *quantum bit*, or *qubit* for short. Qubits are mathematical objects with certain properties. While it is true that qubits, like bits, are realized as actual physical systems, we are going to treat them as abstract mathematical objects.

A qubit has a state, just like a bit, represent by $|\psi\rangle$. Two possible states are $|0\rangle$ and $|1\rangle$. However it can also have a state which is a linear combination of these two. Thus:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

The numbers α and β are complex numbers. Put another way, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an *orthonormal* basis for this vector space.

Since α and β can take infinitely many different complex values, one might be tempted to think that infinite different messages can be conveyed using a single qubit! But there's a catch. When we make a measurement of a qubit, its state *collapses* into either $|0\rangle$ with probability $|\alpha|^2$ or $|0\rangle$ with probability $|\beta|^2$. So every time we observe only one of the two possible states. Naturally, $|\alpha|^2 + |\beta|^2 = 1$.

Geometrically, we can interpret this as the condition that the qubit's state be normalized to length 1. Thus, in general a qubit's state is a unit vector in a two-dimensional complex vector space.

Since α and β are complex numbers with the only constraint that $|\alpha|^2 + |\beta|^2 = 1$, we may represent the state of qubit as:

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

In fact, we can ignore the factor $e^{i\gamma}$ because it has no observable effects. Thus we can effectively write:

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

The numbers θ and ϕ define a point on the unit three-dimensional sphere, as shown in the figure below. This sphere is often called the *Bloch sphere*.

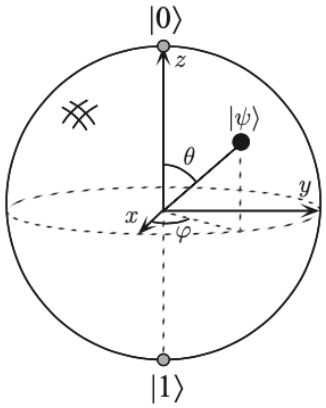

Figure 1: Bloch sphere

2 Introduction to Quantum Mechanics

To understand the concepts of quantum information and computing, a thorough understanding of quantum mechanics is required. Thus we must first get familiar with the mathematics involved and later we will see the postulates of quantum mechanics.

2.1 Linear Algebra

Linear algebra is the study of vector spaces and of linear operations on those vector spaces. A good understanding of quantum mechanics is based upon a solid grasp of elementary linear algebra.

Definition 2.1. A *spanning set* for a vector space is a set of vectors $|v_1\rangle, \ldots, |v_n\rangle$ such that any vector $|v\rangle$ in the vector space can be written as a linear combination $|v\rangle = \sum_i a_i |v_i\rangle$ of vectors in that set.

Definition 2.2. A *linear operator* between vector spaces V and W is defined to be any function $A\colon V \to W$ which is linear in its inputs,

$$A\left(\sum_i a_i |v_i\rangle\right) = \sum_i a_i A(|v_i\rangle)$$

The most convenient way to understand linear operators is in terms of their *matrix representation*. Suppose $A\colon V \to W$ is a linear operator between vector spaces V and W. Suppose $|v_1\rangle, \ldots, |v_m\rangle$ is a basis for V and $|w_1\rangle, \ldots, |w_n\rangle$ is a basis for W . Then for each j in the range $1, \ldots, m$, there exist complex numbers A_{1j} through A_{nj} such that

$$A|v_j\rangle = \sum_{i=1}^{n} A_{ij} |w_i\rangle$$

The $n \times m$ matrix whose entries are the values A_{ij} is said to form a matrix representation of the operator A. Matrix representation is very helpful in the way that applying operator A to a vector $|v\rangle$ is equivalent to multiplying the matrix of A by the column vector representation of $|v\rangle$.

The Pauli matrics

Four extremely useful matrices are the Pauli matrices. They are defined as:

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

2.1.1 Inner Products

An *inner product* is a function which takes as input two vectors $|v\rangle$ and $|w\rangle$ from a vector space and produces a complex number as output. For the time being, it will be convenient to write the inner product of $|v\rangle$ and $|w\rangle$ as $(|v\rangle, |w\rangle)$ although the standard quantum mechanical notation is $\langle v|w\rangle$.

A function $(\cdot, \cdot)$ from $V \times V$ to C is an inner product if it satisfies the requirements that:

1. $(\cdot, \cdot)$ is linear in the second argument,

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle)$$

2. $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$
3. $(|v\rangle, |v\rangle) \geq 0$ with equality if and only if $|v\rangle = 0$

A vector space having an inner product is called an *inner product space*.
For example, $\mathbb{C}^n$ has an inner product defined by

$$((y_1,\ldots,y_n),(z_1,\ldots,_n)) = \sum_i y_i^* z_i = \begin{bmatrix} y_1^* & \ldots & y_n^* \end{bmatrix} \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

In the finite dimensional complex vector spaces that come up in quantum computation and quantum information, a *Hilbert space* is *exactly the same thing* as an inner product space. From now on we may use the two terms interchangeably.

Definition 2.3. Vectors $|v\rangle$ and $|w\rangle$ are *orthogonal* if their inner product is zero.

Definition 2.4. The *norm* of a vector is defined as,

$$\||v\rangle\| = \sqrt{\langle v|v\rangle}$$

Definition 2.5. A *unit vector* is a vector $|v\rangle$ such that $\||v\rangle\| = 1$.

2.1.2 Eigenvectors and eigenvalues

Definition 2.6. An *eigenvector* of a linear operator A on a vector space is a non-zero vector $|v\rangle$ such that $A|v\rangle = v|v\rangle$, where v is a complex number known as the *eigenvalue* of A corresponding to $|v\rangle$.

Definition 2.7. A *diagonal representation* for an operator A on a vector space V is a representation $A = \sum_i \lambda_i |i\rangle\langle i|$, where the vectors $|i\rangle$. form an orthonormal set of eigenvectors for A, with corresponding eigenvalues λ_i. Diagonal representations are sometimes also known as *orthonormal decompositions*.

Definition 2.8. An operator is said to be *diagonalizable* if it has a diagonal representation.

2.1.3 Adjoint and Hermitian operators

Definition 2.9. Suppose A is any linear operator on a Hilbert space, V. There exists a unique operator $A^\dagger$ on V such that for all vectors $|v\rangle, |w\rangle \in V$, $(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle)$. The linear operator $A^\dagger$ is known as the *adjoint* or *Hermitian conjugate* of the operator A.

It can be proved that $A^\dagger = (A^*)^T$

Definition 2.10. An operator A is said to be *normal* if $AA^\dagger = A^\dagger A$.

Definition 2.11. An operator A is said to be *unitary* if $AA^\dagger = I$.

Theorem 2.1. (Spectral decomposition) Any normal operator M on a vector space V is diagonal with respect to some orthonormal basis for V. Conversely, any diagonalizable operator is normal.

Exercise 2.1. Show that a normal matrix is Hermitian if and only if it has real eigenvalues.

Solution. ($\Longrightarrow$) Let $A|v\rangle = \lambda|v\rangle$. We have,

$$\begin{aligned} (|v\rangle, A|V\rangle) &= (A^\dagger|v\rangle, |v\rangle) \\ (|v\rangle, \lambda|v\rangle) &= (\lambda|v\rangle, |v\rangle) \\ \lambda(|v\rangle, |v\rangle) &= \lambda^*(|v\rangle, |v\rangle) \\ \lambda &= \lambda^* \end{aligned}$$

($\Longleftarrow$) By the spectral theorem, if A is normal, then it is diagonalizable. Hence, $A = UDU^\dagger$ for some unitary operator matrix U and a diagonal matrix D containing eigenvalues of A. Taking adjoint on both sides,

$$\begin{aligned} A^\dagger &= \left(UDU^\dagger\right)^\dagger \\ &= UD^*U^\dagger \\ &= UDU^\dagger \\ &= A \end{aligned}$$

Exercise 2.2. Show that all eigenvalues of a unitary matrix have modulus 1, that is, can be written in the form $e^{i\theta}$ for some real θ.

Solution.

$$\begin{aligned} U\left|v\right\rangle &= \lambda\left|v\right\rangle \\ \implies \left\langle v\right| U^\dagger &= \left\langle v\right| \lambda^* \end{aligned}$$

By multiplying the above equations, we get

$$\begin{aligned} \left\langle v\right| U^\dagger U\left|v\right\rangle &= \left\langle v\right| \lambda^*\lambda\left|v\right\rangle \\ \left\langle v|v\right\rangle &= \left\|\lambda\right\|^2\left\langle v|v\right\rangle \\ \left\|\lambda\right\|^2 &= 1 \\ \left\|\lambda\right\| &= 1 \end{aligned}$$

Definition 2.12. A positive operator A is defined to be an operator such that for any vector $|v\rangle$, $(|v\rangle, A|v\rangle)$ is a real, non-negative number.

Exercise 2.3. Show that a positive operator is necessarily Hermitian.

Solution. Let

$$B = \frac{A + A^\dagger}{2} \qquad\qquad C = \frac{-iA + iA^\dagger}{2}$$

Then B and C are Hermitian and $A = B + iC$ Hence

$$\left\langle v\right| A\left|v\right\rangle = \left\langle v\right| B\left|v\right\rangle + i\left\langle v\right| C\left|v\right\rangle$$

Any Hermitian X can be represent as $X = \sum_i \lambda_i \left|i\right\rangle\left\langle i\right|$ where $|i\rangle$ are its eigenvectors and λ_i are corresponding eigenvalues. For any vector $|v\rangle$, $\left\langle v\right| X\left|v\right\rangle = \sum_i \lambda_i \left\langle v|i\right\rangle\left\langle i|v\right\rangle$ which is always real. Hence $\left\langle v\right| C\left|v\right\rangle = 0$ for all vectors $|v\rangle$ and this combined with the fact that C is Hermitian yields that C is identically 0. Therefore, A must be Hermitian.

2.1.4 Tensor products

The *tensor product* is a way of putting vector spaces together to form larger vector spaces. This construction is crucial to understanding the quantum mechanics of multiparticle systems.

In layman terms, tensor product of two vectors *from different vector spaces* is simply the "concatenation" of these vectors (i.e. placing next to each other).

Suppose V and W are vector spaces of dimension m and n respectively. For convenience we also suppose that V and W are Hilbert spaces. Then $V \otimes W$ (read 'V tensor W') is an mn dimensional vector space. The elements of $V \otimes W$ are linear combinations of 'tensor products' $|v\rangle \otimes |w\rangle$ of elements $|v\rangle$ of V and $|w\rangle$ of W. In particular, if $|i\rangle$ and $|j\rangle$ are orthonormal bases for the spaces V and W then $|i\rangle \otimes |j\rangle$ is a basis for $V \otimes W$.

Tensor product can be defined for operators too. Let A and B be linear operators acting on vector spaces V and W respectively. Then the operator $A \otimes B$ acting on $V \otimes W$ is defined as

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv (A|v\rangle) \otimes (B|w\rangle)$$

The inner products on the spaces V and W can be used to define a natural inner product on $V \otimes W$. Define

$$\left(\sum_i a_i |v_i\rangle \otimes |w_i\rangle, \sum_j b_j \left|v'_j\right\rangle \otimes \left|w'_j\right\rangle \right) \equiv = \sum_{ij} a_i^* b_j \left\langle v_i | v'_j \right\rangle \left\langle w_i | w'_j \right\rangle$$

It can be shown that the function so defined is a well-defined inner product.

Now we discuss the *Kroneckar product* which is a convenient matrix representation of $A \otimes B$. Suppose A is an $m \times n$ matrix, and B is a $p \times q$ matrix. Then we have the matrix representation:

$$A \otimes B = \overbrace{\left.\begin{bmatrix} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{bmatrix}\right\} mp}^{nq}$$

We use $|\psi\rangle^{\otimes k}$ to denote $|\psi\rangle$ tensored with itself k times.

2.1.5 Operator functions

There are many important functions which can be defined for operators and matrices. Generally speaking, given a function f from the complex numbers to the complex numbers, it is possible to define a corresponding matrix function on normal matrices by the following construction. Let A $= \sum_a a |a\rangle \langle a|$ be a spectral decomposition for a normal operator A. Define $f(A) \equiv \sum_a f(a) |a\rangle \langle a|$. This procedure can be used, for example, to define the square root of a positive operator, the logarithm of a positive-definite operator, or the exponential of a normal operator.

Exercise 2.4. (Exponential of the Pauli matrices) Let $\vec{v}$ be any real, three-dimensional unit vector and θ a real number. Prove that

$$\exp(i\theta \vec{v} \cdot \vec{\sigma}) = \cos(\theta) I + i \sin(\theta) \vec{v} \cdot \vec{\sigma},$$

where $\vec{v} \cdot \vec{\sigma} = \sum_{i=1}^{3} v_i \sigma_i$.

Solution. Note that $\sigma_i \sigma_j = \begin{cases} I, & if\ i = j \\ -\sigma_j \sigma_i, & if\ i \neq j \end{cases}$

Hence, $(\vec{v} \cdot \vec{\sigma})^2 = (v_1^2 + v_2^2 + v_3^2) I = I$

$$\begin{aligned} \exp(i\theta \vec{v} \cdot \vec{\sigma}) &= \sum_{k=0}^{\infty} \frac{(i\theta \vec{v} \cdot \vec{\sigma})^k}{k!} \\ &= \sum_{k=0}^{\infty} \frac{(i\theta \vec{v} \cdot \vec{\sigma})^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{(i\theta \vec{v} \cdot \vec{\sigma})^{2k+1}}{(2k+1)!} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k (\theta)^{2k} I}{(2k)!} + i\vec{v} \cdot \vec{\sigma} \sum_{k=0}^{\infty} \frac{(-1)^k (\theta)^{2k+1}}{(2k+1)!} \\ &= \cos(\theta) I + i \sin(\theta) \vec{v} \cdot \vec{\sigma} \end{aligned}$$

An important matrix function is the *trace* of a matrix.

Definition 2.13. The trace of A is defined to be the sum of its diagonal elements,

$$tr(A) \equiv \sum_i A_{ii}$$

The following properties can easily be proved for the trace of a matrix:

1. $\mathrm{tr}(AB) = \mathrm{tr}(BA)$
2. $\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B)$
3. $\mathrm{tr}(zA) = z\,\mathrm{tr}(A)$

2.1.6 The commutator and anti-commutator

Definition 2.14. The *commutator* between two operators A and B is defined to be

$$[A, B] = AB - BA$$

Definition 2.15. The *anti-commutator* between two operators A and B is defined to be

$$\{A, B\} = AB + BA$$

If $[A, B] = 0$, we say that A *commutes* with B. Similarly, If $A, B = 0$, we say that A *ant-commutes* with B.

Theorem 2.2. (Simultaneous diagonalization theorem) Suppose A and B are Hermitian operators. Then $[A, B] = 0$ if and only if there exists an orthonormal basis such that both A and B are diagonal with respect to that basis. We say that A and B are *simultaneously diagonalizable* in this case.

Proof. It can be easily verified that if A and B are diagonal in the same orthonormal basis then $[A, B] = 0$. To show the converse, let $|a, j\rangle$ be an orthonormal basis for the eigenspace V_a of A with eigenvalue a; the index j is used to label possible degeneracies. Note that

$$AB\,|a, j\rangle = BA\,|a, j\rangle = aB\,|a, j\rangle$$

and therefore $B\,|a, j\rangle$ is an element of the eigenspace V_a. Let P_a denote the projector onto the space V_a and define $B_a \equiv P_a B P_a$. It is easy to see that the restriction of B_a to the space V_a is Hermitian on V_a, and therefore has a spectral decomposition in terms of an orthonormal set of eigenvectors which span the space V_a. Let's call these eigenvectors $|a, b, k\rangle$, where the indices a and b label the eigenvalues of A and B_a, and k is an extra index to allow for the possibility of a degenerate B_a. Note that $B\,|a, b, k\rangle$ is an element of V_a, so $B\,|a, b, k\rangle = P_a B\,|a, b, k\rangle$. Moreover we have $P_a\,|a, b, k\rangle = |a, b, k\rangle$, so

$$B\,|a, b, k\rangle = P_a B P_a\,|a, b, k\rangle = b\,|a, b, k\rangle$$

It follows that $|a, b, k\rangle$ is an eigenvector of B with eigenvalue b, and therefore $|a, b, k\rangle$ is an orthonormal set of eigenvectors of both A and B, spanning the entire vector space on which A and B are defined. That is, A and B are simultaneously diagonalizable. □

2.1.7 The polar and singular value decompositions

The *polar* and *singular value* decompositions are useful ways of breaking linear operators up into simpler parts. In particular, these decompositions allow us to break general linear operators up into products of unitary operators and positive operators. While we don't understand the structure of general linear operators terribly well, we do understand unitary operators and positive operators in quite some detail. The polar and singular value decompositions allow us to apply this understanding to better understand general linear operators.

Theorem 2.3. (Polar decomposition) Let A be a linear operator on a vector space V. Then there exists unitary U and positive operators J and K such that

$$A = UJ = KU,$$

where the unique positive operators J and K satisfying these equations are defined by $J \equiv \sqrt{A^\dagger A}$ and $K \equiv \sqrt{AA^\dagger}$. Moreover,if A is invertible then U is unique.

Corollary 2.4. (Singular value decomposition) Let A be a square matrix. Then there exist unitary matrices U and V, and a diagonal matrix D with non-negative entries such that

$$A = UDV$$

The diagonal elements of D are called the singular values of A.

2.2 The postulates of quantum mechanics

Quantum mechanics is a mathematical framework for the development of physical theories. On its own quantum mechanics doesn't tell you what laws a physical system must obey, but it does provide a mathematical and conceptual framework for the development of such laws. In the next few sections we give a complete description of the basic postulates of quantum mechanics. These postulates provide a connection between the physical world and the mathematical formalism of quantum mechanics.

2.2.1 State space

Postulate 1. Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

Quantum mechanics does *not* tell us, for a given physical system, what the state space of that system is, nor does it tell us what the state vector of the system is. Figuring that out for a *specific* system is a difficult problem for which physicists have developed many intricate and beautiful rules.

The simplest quantum mechanical system, and the system which we will be most concerned with, is the *qubit*. A qubit has a two-dimensional state space. Suppose $|0\rangle$ and $|1\rangle$ form an orthonormal basis for that state space. Then an arbitrary state vector in the state space can be written

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where a and b are complex numbers. The condition that $|\psi\rangle$ be a unit vector, $\langle\psi|\psi\rangle = 1$, is therefore equivalent to $|a|^2 + |b|^2 = 1$. The condition $\langle\psi|\psi\rangle = 1$ is often known as the *normalization condition* for state vectors.

2.2.2 Evolution

How does the state, $|\psi\rangle$, of a quantum mechanical system change with time? The following postulate gives a prescription for the description of such state changes.

Postulate 2. The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle$$

Just as quantum mechanics does not tell us the state space or quantum state of a *particular* quantum system, it does not tell us which unitary operators U describe real world quantum dynamics. Quantum mechanics merely assures us that the evolution of any closed quantum system may be described in such a way. An obvious question to ask is: what unitary operators are natural to consider? In the case of single qubits, it turns out that *any* unitary operator at all can be realized in realistic systems.

2.2.3 Quantum measurement

We postulated that closed quantum systems evolve according to unitary evolution. The evolution of systems which don't interact with the rest of the world is all very well, but there must also be times when the experimentalist and their experimental equipment – an external physical system in other words – observes the system to find out what is going on inside the system, an interaction which makes the system no longer closed, and thus not necessarily subject to unitary evolution. To explain what happens when this is done, we introduce Postulate 3, which provides a means for describing the effects of measurements on quantum systems.

Postulate 3. Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I$$

The completeness equation expresses the fact that probabilities sum to one:

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle$$

A simple but important example of a measurement is the *measurement of a qubit in the computational basis*. This is a measurement on a single qubit with two outcomes defined by the two measurement operators $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Observe that each measurement operator is Hermitian, and that $M_0^2 = M_0$, $M_1^2 = M_1$. Thus the completeness relation is obeyed, $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Suppose the state being measured is $|\psi\rangle = a|0\rangle + b|1\rangle$. Then the probability of obtaining measurement outcome 0 is

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2$$

Similarly, the probability of obtaining the measurement outcome 1 is $p(1) = |b|^2$. The state after measurement in the two cases is therefore

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle$$
$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle$$

The multipliers like $a/|a|$, which have modulus one, can effectively be ignored because they don't have any observable effect, so the two post-measurement states are effectively $|0\rangle$ and $|1\rangle$.

2.2.4 Composite systems

Postulate 4. The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$

Exercise 2.5. Show that the average value of the observable $X_1 Z_2$ for a two qubit system measured in the state $(|00\rangle + |11\rangle)/2$ is zero.

Solution. Let $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$
The average value of operator $X_1 Z_2$ is given by $\langle\psi| X_1 Z_2 |\psi\rangle$

$$\begin{aligned}
\langle\psi| X_1 Z_2 |\psi\rangle &= \langle\psi| X_1 \left(\frac{|00\rangle - |11\rangle}{\sqrt{2}}\right) \\
&= \left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right)\left(\frac{|10\rangle - |01\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{2}\left(\langle 00|10\rangle - \langle 00|01\rangle + \langle 11|10\rangle - \langle 11|01\rangle\right) \\
&= 0
\end{aligned}$$

(since the four states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are orthogonal)

Postulate 4 also enables us to define one of the most interesting and puzzling ideas associated with composite quantum systems – *entanglement*.

Formally, any multiple qubit state which cannot be factorized into single qubit states is called an *entangled state*.

For example, consider the state $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. We are now going to show that it is entangled by contradiction.

Let $|\psi\rangle = |a\rangle |b\rangle$, where $|a\rangle$ and $|b\rangle$ are single qubit states. Further let $|a\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$ and $|b\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$. Then,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\psi\rangle = |a\rangle |b\rangle = \alpha_1\alpha_2 |00\rangle + \alpha_1\beta_2 |01\rangle + \beta_1\alpha_2 |10\rangle + \beta_1\beta_2 |11\rangle$$

Therefore, we have,

$$\begin{aligned}
\alpha_1\alpha_2 &= \frac{1}{\sqrt{2}}, \\
\alpha_1\beta_2 &= 0, \\
\beta_1\alpha_2 &= 0, \\
\beta_1\beta_2 &= \frac{1}{\sqrt{2}}
\end{aligned}$$

By multiplying first and fourth equations and second and third equations, we get two different values for the product $\alpha_1\alpha_2\beta_1\beta_2$ which is clearly a contradiction. Hence, the given state is entangled.

The entangled states show some very weird phenomenon which we shall cover in the final report.