Quantum Mechanics in Quantum Computing

Mathew Johnson

Mathew Johnson is a Ball State junior majoring in Mathematics (Option 1) with a minor in Physics. In his sophomore year, he participated in the student-faculty colloquium, where he explored quantum computing with several other students and faculty.

Quantum mechanics is a scientific theory that seeks to describe atomic and subatomic particles (or quantum particles) as well as the interaction among them. Such particles include electrons, protons, neutrons, and photons. In classical mechanics, a particle's future state is described with certainty once its present state is known. At any given moment, its momentum and position are determined with certainty. In quantum mechanics, its future state is described probabilistically. Instead of a single momentum, a particle can assume a simultaneous range of momenta, and instead of a single position, it can take a simultaneous range of positions. Since the product of these ranges is no less than a specific positive universal constant, a decrease in the range of its position forces an increase in the range of momentum and vice versa. It is precisely this effect of quantum particles that quantum computing seeks to exploit in order to manipulate a huge amount of information simultaneously. Quantum computing is a mathematical theory currently being developed to give a theoretical basis for building a "quantum computer," which is envisioned to be faster than any classical computer to date. Quantum computing is based on the principles of quantum mechanics. In this article we will look at the postulates of quantum mechanics upon which quantum computing is based.

A physical system consisting of one or more quantum particles will be called a *quantum system*. A quantum system will be called *isolated* if it does not interact with other quantum systems.

At any given instant, a quantum system will be in a certain "state." The first postulate deals with a way of representing states of a quantum system:

Postulate 1. *Associated with any isolated quantum system is a complex Hilbert space. A "state" in the system is represented by a unit vector in this vector space.*

While an infinite dimensional Hilbert space may be needed to model a quan-

tum system completely, for simplicity we will only use finite dimensional Hilbert spaces to describe quantum systems that will be used in quantum computations. In quantum mechanics, the so called Dirac notation is used to represent vectors. In this notation a vector u in a complex Hilbert space H is denoted by a *Dirac ket* $|u\rangle$. The simplest quantum mechanical system is the two-dimensional complex Hilbert space $\mathbb{C}^2$. In this vector space, the inner product between two vectors $z = (z_1, z_2)$ and $w = (w_1, w_2)$, denoted $\langle z|w\rangle$, is given by

$$\langle z|w\rangle = \bar{z}_1 w_1 + \bar{z}_2 w_2.$$

If we let

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{and} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

then the vectors $|0\rangle$ and $|1\rangle$ form an orthonormal basis of $\mathbb{C}^2$. An arbitrary state $|\Psi\rangle$ can be realized as a linear combination (or *superposition*) of $|0\rangle$ and $|1\rangle$. Thus, $|\Psi\rangle = a|0\rangle + b|1\rangle$ for some complex numbers a and b satisfying $|a|^2 + |b|^2 = 1$. This represents a quantum analogue of the classical bit called a quantum bit, or *qubit*, and is used as the smallest unit of quantum information.

Before we go any farther, we recall some definitions from Linear Algebra. Consider an $n \times n$ matrix A over the complex field $\mathbb{C}$. The complex conjugate of A, denoted by A^*, is obtained by taking the complex conjugate of every entry in A. If A is real, then $A = A^*$. We shall let $A^\dagger$ stand for the transpose of the complex conjugate.

Definition.

1. A is said to be *normal* if and only if $AA^\dagger = A^\dagger A$.
2. A is said to be *Hermitian* if and only if $A^\dagger = A$. All eigenvalues of a Hermitian matrix are real.
3. A is said to be *unitary* if $AA^\dagger = I$. All eigenvalues of a unitary matrix have absolute value one.

   We note that Hermitian and unitary matrices are normal matrices. As an example, note that the following matrix is both unitary and Hermitian.

$$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

4. While the tensor product of vector spaces will be useful in a subsequent discussion, here we will confine ourselves to the computational definition of the tensor product between two qubits, and refer the reader to the references [2] and [1] instead. The *tensor product* between two quibits

$$|x\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \qquad |y\rangle = \begin{bmatrix} c \\ d \end{bmatrix},$$

   denoted by $|x\rangle \otimes |y\rangle$, or $|xy\rangle$ for short, is the vector in $\mathbb{C}^4$ given as

$$|x\rangle \otimes |y\rangle = \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix}.$$

The following is a standard theorem in Linear Algebra and we will need it to describe one of the postulates below. To this end let us recall the following concept from Linear Algebra. An $n \times n$ matrix B is said to be *orthogonally diagonalizable* if and only if $\mathbb{C}^n$ has an orthogonal basis consisting of eigenvectors of B.

Spectral Decomposition Theorem

An $n \times n$ matrix A is orthogonally diagonalizable if and only if A is normal.

We will be primarily interested in Hermitian matrices. Let A be a Hermitian matrix and suppose $\{w_j : j = 1, 2, \cdots n\}$ is an orthonormal basis of $\mathbb{C}^n$ consisting of egenvectors of A. Then

$$A = \sum_{j=1}^{n} \lambda_j |w_j\rangle\langle w_j|, \tag{1}$$

where λ_j is the eigenvalue of A corresponding to the eigenvector w_j. Here we have used the "bra" notation $\langle w|$ of Dirac to denote the map $\langle w| : \mathbb{C}^n \to \mathbb{C}$ given by

$$\langle w|(|u\rangle) := \langle w|u\rangle, \qquad \text{for any vector } \ u \in \mathbb{C}^n.$$

Note that

$$\sum_{j=1}^{n} |w_j\rangle\langle w_j| = I,$$

where I is the $n \times n$ identity matrix. Also note that for each unit vector $|w\rangle$, the matrix (operator) $|w\rangle\langle w|$ is a projection of $\mathbb{C}^n$ onto the subspace spanned by the single vector $|w\rangle$. As an example, if $|w\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$, then

$$|w\rangle\langle w| = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} \bar{a} & \bar{b} \end{bmatrix} = \begin{bmatrix} |a|^2 & a\bar{b} \\ \bar{a}b & |b|^2 \end{bmatrix}.$$

Thus, the decomposition (1) of A given above expresses A as a linear combination of (orthogonal) projections P_j of $\mathbb{C}^n$ onto appropriate eigenspaces of A.

As an example we have the spectral decomposition

$$\begin{aligned} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} &= 1 \cdot P_1 + (-1) \cdot P_2 \\ &= 1 \cdot \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + (-1) \cdot \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \end{aligned}$$

The second postulate deals with observables and their measurements. An *observable* is a property of a quantum system which in principle can be measured. This postulate highlights one of the basic features of quantum mechanics: outcomes of measurements can only be predicted probabilistically.

Postulate 2. *In quantum mechanics, an observable is represented by a Hermitian matrix in a complex Hilbert space. The numerical outcome of a measurement of an observable A is an eigenvalue λ_k of A.*

Suppose the observable A is decomposed into appropriate projections as in the Spectral Decomposition Theorem:

$$A = \lambda_1 P_1 + \cdots + \lambda_n P_n.$$

Since A is Hermitian, recall that all its eigenvalues are real. Immediately following a measurement, the quantum state becomes an eigenvector of A. If the pre-measurement quantum state is $|\psi\rangle$, then after the measurement, the outcome λ_k is obtained with probability

$$\text{Prob}(\lambda_k) = \langle\psi|P_k|\psi\rangle$$

where $\langle\psi|P_k|\psi\rangle$ denotes the inner product between $|\psi\rangle$ and $P_k|\psi\rangle$.

If the outcome λ_k is realized, then the post measurement quantum state becomes

$$\frac{P_k|\psi\rangle}{\sqrt{\text{Prob}(\lambda_k)}}.$$

The expected value of the measurement is therefore

$$E(A) = \sum_k \lambda_k \text{Prob}(\lambda_k) = \sum_k \lambda_k \langle\psi|P_k|\psi\rangle = \langle\psi|(\sum_k \lambda_k P_k)|\psi\rangle = \langle\psi|A|\psi\rangle$$

by the spectral decomposition theorem.

As an example, we consider the observable in $\mathbb{C}^2$ given by

$$A = \begin{bmatrix} 2 & 0 \\ 0 & -3 \end{bmatrix} = 2P_1 + (-3)P_2 = 2|0\rangle\langle 0| + (-3)|1\rangle\langle 1|.$$

The outcomes of a measurement of this observable are $\lambda_1 = 2$ and $\lambda_2 = -3$. If the pre-measurement quantum state is $|\Psi\rangle = a|0\rangle + b|1\rangle$, then the outcomes are obtained with probabilities

$$\text{Prob}(2) = |a|^2, \quad \text{Prob}(-3) = |b|^2,$$

and the expected value of the measurement is

$$E(A) = 2|a|^2 - 3|b|^2.$$

The third postulate deals with the evolution of a system over time.

Postulate 3. *The evolution of a closed quantum system is described by a unitary operator. The state $|\psi\rangle$ of a system at time t_1 is related to the state $|\psi'\rangle$ of a system at time t_2 by a unitary operator U, which depends only on the times t_1 and t_2, by $|\psi'\rangle = U|\psi\rangle$.*

The above version of Postulate 3 deals with the evolution of a system over discrete time. A more refined version can be given to describe the evolution

of a quantum system in continuous time. This is described by the Schrödinger equation

$$i\hbar \frac{d\,|\psi(t)\rangle}{d\,t} = H|\psi(t)\rangle$$

where H is a Hermitian matrix known as the *Hamiltonian* of the quantum system, $\hbar = h/(2\pi)$, and h is Planck's constant. If H is a time independent Hamiltonian, then $|\psi(t)\rangle = \exp(-\frac{i}{\hbar}Ht)|C\rangle$, where $|C\rangle$ is a constant vector, is a general solution of the Schrödinger equation. Thus at times t_1 and t_2 we obtain $|\psi(t_2)\rangle = U|\psi(t_1)\rangle$ where U is the unitary matrix $\exp(-\frac{i}{\hbar}H(t_2 - t_1))$. This shows that the Schrödinger equation models the way a state at time t_1 is related to the state at a later time t_2, as given in Postulate 3. The Hamiltonian H encodes the energy configuration of a given quantum system. Being Hermitian, H has a spectral decomposition $H = \sum_{k=1}^{n} \tau_k P_k$ with eigenvalues (energy) τ_k. The corresponding eigenvectors are called the *eigenstates* of the Hamiltonian. The smallest eigenvalue corresponds to the smallest energy level, and its associated eigenvectors are called ground states.

Consider the example of a single qubit system with a Hamiltonian given by

$$H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

It can easily be seen that the eigenvalues of H are $\tau_k = \pm 1$ with corresponding energy eigenstates

$$\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}.$$

The eigenstate which corresponds to the energy level $\tau_k = -1$ is the ground state of the Hamiltonian.

The fourth and final postulate that will be presented deals with being able to combine multiple systems.

Postulate 4. *If n physical systems are represented by n complex Hilbert spaces $H_1, H_2, ..., H_n$, then the composite physical system is represented by the tensor product $H_1 \otimes H_2 \otimes ... \otimes H_n$.*

If, for example, we consider n physical systems each of which is a two-state system, and the k^{th} physical system is prepared in the qubit $|\psi_k\rangle$, then the joint state of the composite system is prepared in the state $|\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$. In the composite system we consider all possible superpositions of such states.

When we start dealing with composite physical systems and superpositions, we begin to see how a quantum computer is much more efficient than a classical computer. In a classical memory register, n bits can represent one integer k with $0 \leq k \leq 2^n - 1$. Due to superposition, however, it is possible for n qubits to represent all of the 2^n integers in that range simultaneously as $|\psi_1\rangle \otimes ... \otimes |\psi_n\rangle$. Such a tensor product of n qubits is called a *quantum memory register* of size n. Information is stored in these registers in binary form.

Let $|a\rangle$ stand for the tensor product

$$|a_{k-1}\rangle \otimes |a_{k-2}\rangle \otimes ... \otimes |a_1\rangle \otimes |a_0\rangle,$$

which represents the number

$$a = \sum_{j=0}^{k-1} a_j 2^j$$

where each $a_j \in \{0, 1\}$. From this definition, a quantum register of size three can store individual numbers such as 6 and 7 as

$$|1\rangle \otimes |1\rangle \otimes |0\rangle = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 = 6,$$

$$|1\rangle \otimes |1\rangle \otimes |1\rangle = 1 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 = 7.$$

Utilizing superposition, the memory register can store both of these integers simultaneously as

$$|1\rangle \otimes |1\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

In fact, a quantum memory register of size three can store the eight integers 0 to 7 at the same time by putting each qubit into the above superposition, thus obtaining the memory register

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

The above preparations, as well as other manipulations on qubits, must be performed by unitary operations. An example of this is a *quantum logic gate*, which is a device that performs a fixed unitary operation on selected qubits. Some examples of quantum logic gates which operate on a single qubit are the Hadmarad gate H and the Phase Shift gate θ. These gates are defined respectively as

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

and their respective unitary operations on the qubit $|x\rangle$ are represented schematically as

$$|x\rangle \text{ ——— } \boxed{\text{H}} \text{ ——— } \frac{1}{\sqrt{2}} \left((-1)^x |x\rangle + |1 - x\rangle \right),$$

$$|x\rangle \text{ ——— } \overset{\theta}{\bullet} \text{ ——— } e^{ix\theta}|x\rangle.$$

Equipped with the above definitions, as well as Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$, a little computation shows that

$$|0\rangle \text{ ——— } \boxed{\text{H}} \text{ ——— } \overset{2\theta}{\bullet} \text{ ——— } \boxed{\text{H}} \text{ ——— } \overset{\frac{\pi}{2}+\alpha}{\bullet} \text{ ——— } \cos\theta|0\rangle + e^{i\alpha}\sin\theta|1\rangle.$$

Thus, these two gates are enough to perform any unitary operation on a single qubit (modulo a global phase - this global phase can be seen explicitly when one carries out the computation to get the above transformation).

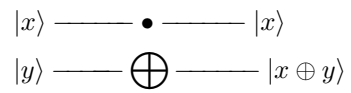
Therefore, the Hadamard gate and the Phase Shift gate can be used in combination to transform the input state $|0\rangle \otimes \cdots \otimes |0\rangle$ of the n-qubit register into any state of the type $|\psi_1\rangle \otimes ... \otimes |\psi_n\rangle$ where $|\psi_k\rangle$ is any arbitrary superposition of $|0\rangle$ and $|1\rangle$. These are special n-qubit states, called *separable states*, i.e., the register can be written as a tensor product of single qubits.

In general, however, a quantum register of size greater than or equal to two can be prepared in states that are not separable - these are known as *entangled states*. As an example, consider the two-qubit states given by $\alpha|00\rangle + \beta|01\rangle$ and $\alpha|00\rangle + \beta|11\rangle$. The first state is separable since it can be written in the form $|0\rangle \otimes (\alpha|0\rangle + \beta|1\rangle)$, which is simply a tensor product between two single qubits. The second state, however, is entangled as it can not be written as a tensor product between single qubits.

Entangled states have many important applications in quantum teleportation and cryptography. So, it would be useful to create a quantum logic gate which would be able to entangle any separable two-qubit system. An example of such an operator is the Controlled-Not (C-Not) gate, given by the unitary matrix

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

A schematic representation of the C-Not gate acting on qubit $|xy\rangle,\ x, y \in \{0, 1\}$ is shown below.



The operation $\oplus$ denotes addition modulo 2 (exclusive or). Given any two qubits, the C-Not gate flips the second (target) qubit if the first (control) qubit is $|1\rangle$, and does nothing if the control qubit is $|0\rangle$. As a result of this behavior, the C-Not gate transforms the two-qubit separable state $|00\rangle + |01\rangle$ into the entangled state $|00\rangle + |11\rangle$.

This article is a brief introduction to the postulates of quantum mechanics as they relate to quantum computing. It was based on a presentation given by the author, in collaboration with Dr. Ahmed Mohammed, for the student-faculty colloquium (Maths 497) during the fall semester of 2002 at Ball State University. Based on these postulates, we later explored in our seminar how a quantum computer might one day be built and what it might be able to do that classical computers cannot. For more information, see the references below.

References

[1] S. Gudder, *Quantum Computation*, Amer. Math. Monthly **110** (2003) 181–201.

[2] N. Nielsen and I. Chuang, Quantum Computations and Quantum Information, Cambridge University Press (2000).

[3] A.O. Pittenger, Introduction to Quantum Computing Algorithms, Birkhauser (1999).

[4] C. Williams and S. Clearwater, Explorations in Quantum Computing, Springer-Verlag (1997).