DEVELOPING A BASIC UNDERSTANDING OF QUANTUM COMPUTING

John Basil

PREFACE

This paper was produced as part of an independent study. No active assistance, neither human nor artificial, was sought in the preparation of this paper. The author of this paper is an undergraduate student lacking formal academic training on the subject of quantum computing. Learning tools consisted of online articles and tutorials. Knowledge on the part of the reader of basic concepts in linear algebra, physical science and computer science is assumed. The paper begins by defining a logical basis of terms and concepts; then explores states, gates, and related computations; and lastly, concludes with an overview of real world implications.

Because of the open-ended nature of this paper and the vastness of quantum computing, these discussions could have been far more verbose; particularly the final section which ends abruptly due to the possibility of eclipsing a word limit. In the future the author would like to explore this subject in greater detail; breadthwise, as it relates to different physical models of quantum computing such as quantum annealing and different applications such as quantum machine learning; as well as depth wise, as it relates to developing intuition with advanced gates and how these manipulations can be applied in different contexts in order to produce a desired result.

DISCUSSION

A bit is the most basic unit of information in computing. Each bit stores no more than a single binary unit of information. A computer algorithm utilizes circuits that perform operations, called gates, on input bits in order to produce output bits. The design of a circuit defines the nature and sequence of gates applied to bits. This paper, for the purpose of discussion, generalizes the definition for, the terms, circuit width and for circuit depth, where circuit width refers to the total number of bits within the same circuit, and circuit depth refers to the minimum number of gates required by any bit within the same circuit.

Classical computing is a paradigm of computing that was developed from the principles of classical mechanics. The bit in classical computing is called a classical bit, which this paper truncates to clabit. A clabit possesses a state that can be described by a binary value corresponding to the state of a switch that is either off or on.

Quantum computing is a paradigm of computing that was developed from the principles of quantum mechanics. The bit in quantum computing is called a qubit. The remainder of this section describes a qubit in the context of the gate-based one-way model of quantum computing. The design of the qubit is motivated by the conditions under which quantum phenomena, such as superposition and entanglement, are repeatable and observable. These phenomena enable qubits to be manipulated in ways that clabits cannot, availing new gates and expanding algorithm design.

A qubit possesses a state that can be described by a binary value as well as by a probability distribution corresponding to the state of a quantum object with respect to the state of a measurement apparatus. This quantum object is herein referred to as, quantum (*pl.* quanta). This measurement

apparatus is herein referred to as, apparatus. The point at which the quantum crosses the spatial plane of the apparatus is, herein, referred to as, measurement. This physical system, one of a plurality of physical systems that can serve as the basis for qubit state, is demonstrated by a quantum, such as a photon or an electron, directed at an apparatus, such as a light filter or a calcite crystal. Terms referring to aspects of this physical system, such as quantum, apparatus, and measurement, are herein defined within the context of this physical system and may be defined differently in other contexts.

In such a physical system, the state of the quantum and the state of the apparatus are, both, characterized by a respective degree of polarization from a baseline axis. A quantum can be observed as either a particle or a wave, depending on the context; polarization in this context relates to the quantum mechanical description of a wave. The degree of polarization of a quantum refers to the degree to which an observed property of the quantum differs from a baseline axis. The degree of polarization of an apparatus is the degree of polarization of a quantum that the apparatus yields.

A quantum is always either yielded or polarized upon measurement. An aligned quantum is always yielded, and an antialigned quantum is always polarized, by the apparatus. A quantum is considered to be aligned with, and thus yielded by, the apparatus if the quantum has the equivalent (0° apart) polarization to the polarization of the apparatus. For example, a quantum polarized at 90° is always yielded by an apparatus polarized at 90°. A quantum is considered to be antialigned with, and thus polarized by, the apparatus if the quantum has the orthogonal (90° apart) polarization to the polarization of the apparatus. For example, a quantum polarized at 0° is always polarized by an apparatus polarized at 90°.

The polarization of a quantum can be characterized by the probability of the quantum existing in one of two polarization states (*e.g.* 0° or 90°); in this context, each polarization state also

corresponds to a spin state: 0° polarization is spin up, and 90° polarization is spin down. Hence, qubits can be characterized by the probability of a quantum existing in one of two spin states – up or down – or a combination of probabilities of a quantum existing in either state.

During measurement, a quantum that is polarized with a particular spin is directed at an apparatus that is polarized with a particular spin, where the spin of the apparatus is the state being measured. An apparatus yields a quantum when the polarization of the quantum is unaffected by measurement with the apparatus. The apparatus polarizes a quantum when the polarization of the quantum, upon measurement, is changed to the polarization of the apparatus.

For example, an apparatus polarized at 45° always yields a quantum polarized at 45°; an apparatus polarized at 90° always polarizes a quantum polarized at 0°. When a quantum is either aligned or antialigned with the apparatus, the correspondence between initial and final quantum state is absolute, so the behavior of the quantum is characterized as deterministic. A quantum with deterministic behavior when measured by the apparatus is either yielded with the same spin (same polarization) as the apparatus spin or are polarized with the opposite spin (orthogonal polarization) to the apparatus spin. The probability that a quantum with deterministic behavior is either yielded or polarized by the apparatus is always equal to 0% or 100% (as a boolean: 0 or 1). Quantum properties do not manifest when a quantum behaves deterministically. **[0]**

When a quantum is neither aligned nor antialigned with the apparatus, the correspondence between initial and final quantum state is random, so the behavior of the quantum is characterized as probabilistic. A quantum with probabilistic behavior when measured by the apparatus loses its initial spin state. A quantum that is yielded by the apparatus inherits the same spin (same polarization) as the

apparatus spin, while a quantum that is polarized by the apparatus inherits the opposite spin (orthogonal polarization) to the apparatus spin. **[0]**

The probability that a quantum with probabilistic behavior is either yielded or polarized by the apparatus is always greater than 0% and less than 100%. This probability can be expressed as a linear combination ($c_0 v_0 + c_1 v_1 + \ldots + c_n v_n$ for scalars c, vectors v) of possible states (up or down). This linear combination is also called a superposition of states. After measurement, the quantum is either aligned (same polarization) or antialigned (orthogonal polarization) with the apparatus, so its behavior becomes deterministic; superposition is lost, and subsequent measurements with the same apparatus produce the same result. **[0]**

The reason for the use of the probability distribution in describing the state of a quantum is that the polarization of the quantum, before measurement with the apparatus, is uncertain. **[0]** The uncertainty principle asserts that a predicted value for a quantity associated with a quantum has limited accuracy prior to measurement (due to the loss of information in the frame of reference used when measuring with absolute precision the observed property of the quantum). The observer effect asserts that measurement itself is capable of changing the state of a quantum. Due to the resulting uncertainty, the state of the qubit is described not by a single value but by a collection of values, with each value corresponding to the probability of the quantum being either polarized or yielded, respectively, by the apparatus.

A quantum state is an element of the vector space representing the distribution of probabilities spanned by all possible states (those possible states, in terms of spin, being up and down). Quantum state is described by a column vector called a statevector. Given that the probabilities for the possible states (up and down) sum to one, the entries of the statevector are normalized. **[1]** For a single qubit

system, the first entry of the statevector is a probability amplitude that the measured spin will be up, and the second entry of the statevector is a probability amplitude that the measured spin will be down.

This probability amplitude is a complex number whose modulus squared (or, square of the absolute value) computes a probability that the quantum will either be polarized or yielded, respectively, by the apparatus. The use of probability amplitudes in quantum mechanics extends beyond the scope of quantum computing; infinitely many wavefunctions, with different positive and negative phase shifts between amplitudes resulting in either constructive or destructive interference, yield the same measurement probabilities. **[2]**

Because of this, a wavefunction can not only be represented as a matrix of real functions, but also as a single linear complex function where probability amplitudes represent coefficients to the states of the wavefunction. **[2]** A quantum can be observed as a wave so quantum state is correlated to the wavefunction, which is also the linear combination of superposition where, for $c_0 v_0 + c_1 v_1 + \ldots + c_n v_n$, each scalar c is a probability amplitude, and each vector v is a statevector.

In order to discuss statevectors and their related computations, matrices are utilized. For a quantum that is aligned with the apparatus (*e.g.* both quantum and apparatus polarized at either 0° or 90°), the probability that the measured spin will be up is 100% and down is 0%. so the statevector entries are $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$. For a quantum that is antialigned with the apparatus (*e.g.* quantum polarized at 0° and apparatus polarized at 90°, or vice versa), the probability that the measured spin will be up is 0% and down is 100%, so the statevector entries are $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

For a quantum that is neither aligned nor antialigned with the apparatus (*e.g.* quantum polarized at 0° or 90°, apparatus polarized at 45°) the probability that the measured spin will be either up or down is 50%, so the statevector entries are the square root of ±50%, or

$$\begin{bmatrix} \sqrt{\pm\frac{1}{2}} \\ \sqrt{\pm\frac{1}{2}} \end{bmatrix}.$$

The qubit associated with such a quantum exists as the simultaneous superposition of states, with each state represented as the square root of the probability that a spin direction will result from measurement.

Bra-ket is a notation that associates a measurement state with a quantum state using a bra (denoted as $\langle\beta|$) and a ket (denoted as $|\Psi\rangle$). A ket describes the quantum state of a quantum using a column vector in the complex vector space. A bra describes the measurement state of an apparatus using the adjoint (transpose of the complex conjugate) of a column vector (*i.e.* a row vector) in the ket dual space.

The inner product between measurement state β and quantum state Ψ (the sum of products of vectors corresponding bra and ket entries denoted as $\langle\beta|\Psi\rangle$) is a linear transformation (transformation preserving vector addition and scalar multiplication) that maps a vector in ket vector space to a number in the complex plane *i.e.* a number that can be expressed in the form $a+bi$; i being imaginary. This complex number is a probability amplitude that is the coefficient for the projection of state Ψ onto state β. Where $i^2=-1$, squaring the magnitude of the probability amplitude (*i.e.* $|\langle\beta|\Psi\rangle|^2$) computes a real-valued probability that a quantum in a particular state Ψ will measure with a particular spin β or, in other words, that state Ψ will collapse into state β upon measurement.

Take as examples, for an apparatus that is polarized with spin β: a quantum with quantum state Ψ equal to β will always be yielded by the apparatus upon measurement, so $|\langle\beta|\Psi\rangle|^2=1$; a quantum with quantum state Ψ orthogonal to β is never yielded by the apparatus upon measurement, so $|\langle\beta|\Psi\rangle|^2=0$; a quantum with quantum state Ψ neither equal nor orthogonal to β will only sometimes be yielded upon measurement, so $|\langle\beta|\Psi\rangle|^2$ computes a probability greater than 0 but less than 1. The closer the polarization of the quantum to the polarization of the apparatus, the greater the probability of the quantum being yielded upon measurement.

The statevectors of $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ form an orthonormal (orthogonal unit) basis for the vector space spanned by, and as such can be scaled to compose, all possible statevectors. The orthonormal base states of $\begin{bmatrix}1\\0\end{bmatrix}$ and $\begin{bmatrix}0\\1\end{bmatrix}$ are represented in ket form as $|0\rangle$ and $|1\rangle$, respectively. These bases, which are also called the computational bases, may be used to compute an inner product:

e.g. $\langle1|0\rangle=0$; $\langle0|1\rangle=0$; $\langle0|0\rangle=1$; $\langle1|1\rangle=1$;

or an outer product:

e.g. $|0\rangle\langle1|=\begin{bmatrix}0&1\\0&0\end{bmatrix}$; $|1\rangle\langle0|=\begin{bmatrix}0&0\\1&0\end{bmatrix}$; $|0\rangle\langle0|=\begin{bmatrix}1&0\\0&0\end{bmatrix}$; $|1\rangle\langle1|=\begin{bmatrix}0&0\\0&1\end{bmatrix}$.

A qubit in ket form comprises a linear combination of bases (*i.e.* measured states), each scaled by a corresponding probability amplitude (*i.e.* $|\Psi\rangle=m|B_1\rangle+n|B_2\rangle$, where $|m|^2+|n|^2=1$). The probability amplitudes reduce to pure probabilities of 0 and 1 for qubits $|0\rangle$ and $|1\rangle$, eliminating the probability distribution given that these states behave deterministically (*i.e.* $|0\rangle=1|0\rangle+0|1\rangle$ and $|1\rangle=0|0\rangle+1|1\rangle$). Otherwise, the qubit is in a superposition of states.

For example:

$$\text{statevector} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \text{ is ket } |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle; \text{ statevector} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \text{ is ket } |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle;$$

$$\text{statevector} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix} \text{ is ket } |+i\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle; \text{ statevector} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{i}{\sqrt{2}} \end{bmatrix} \text{ is ket } |-i\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle.$$

Measurement is not restricted to the computational bases; an infinite number of valid combinations of bases exist (so long as the measurement probabilities associated with the bases add to 1); as such, either of these ket pairs: $\{|+\rangle, |-\rangle\}$ or $\{|+i\rangle, |-i\rangle\}$ could become bases (as opposed to $\{|0\rangle, |1\rangle\}$) in the statevector of a qubit.

A qubit statevector can be mapped from two-dimensional complex space into three-dimensional real space using a Bloch vector. A Bloch vector, which always has a magnitude of one, corresponds to a point on the perimeter of a Bloch sphere compring two angles in spherical polar coordinates: an azimuth θ and a zenith ϕ. The θ angle corresponds to probability amplitude and rotates 180° counterclockwise about y-axis. Where $y = 0$, angle θ starts at the polar coordinates

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

The ϕ angle corresponds to relative phase and rotates 360° counterclockwise about the *z*-axis. Where $z = 0$, angle ϕ starts at the polar coordinates

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}. \textbf{ [1]}$$

In order to utilize these angles, a formula for a Bloch state must be derived. Starting with the generic form of a qubit statevector (*i.e.* $|\Psi\rangle = m|0\rangle - m|1\rangle$; m, $n \in \mathbb{C}$; $|m|^2+|n|^2=1$), probability amplitudes m and n are recognized as both being complex (of the form $a+bi$). Given that the real and complex components of the probability amplitudes can be distinghuished by Euler's formula, $re^{i\varphi} = a+bi$ for a real numbered r, the qubit statevector becomes:

$$|\Psi\rangle = pe^{i\varphi 1}|0\rangle + qe^{i\varphi 2}|1\rangle;\ p, q \in \Re;\ |p|^2+|q|^2=1;$$

which can be restated as $|\Psi\rangle = e^{i\varphi 1}(m|0\rangle + ne^{i(\varphi 2-\varphi 1)}|1\rangle)$.

Because a baseline phase angle cannot be measured (called global phase), $e^{i\varphi 1}$ is assigned an arbitrary value of 1 so that this statevector can be further restated as $|\Psi\rangle = p|0\rangle + qe^{i(\varphi 2-\varphi 1)}|1\rangle$. Letting $\phi = \varphi_2 - \varphi_1$, the complex term for m and for n has been factored into a single coefficient which describes the relative phase between $|0\rangle$ and $|1\rangle$: $|\Psi\rangle = p|0\rangle + e^{i\phi}q|1\rangle$; $p, q, \phi \in \Re$. **[3]**

Applying a trigonometric identity, the equation $|p|^2+|q|^2=1$ is transformed into $\sqrt{p^2+q^2} = \sqrt{\sin^2 p + \cos^2 q} = 1$. Applying a trigonometric identity, real p and q can be expressed in terms of one variable by $p = \cos(\frac{\theta}{2})$ and $q = \sin(\frac{\theta}{2})$. These values can be substituted into the equation for a qubit statevector (*i.e.* $|\Psi\rangle = p|0\rangle + e^{i\phi}q|1\rangle$) in order to form an equation for a Bloch vector expressed in terms of θ and ϕ: $|\Psi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$, where $\theta, \phi \in \Re$. **[3]**

A Bloch sphere is useful for visualizing a change to the state of a qubit. This state change corresponds to a change to the state of a quantum, which may be demonstrated in a physical system by directing the quantum at an additional polarizer before the quantum is measured. A polarizer changes the polarization state of a quantum. Such a state change can be represented by a gate applied to a single

qubit that changes the Bloch vector of a qubit. Examples of a quantum gate include the Pauli gates, whose operations are represented by the Pauli matrices (*X*, *Y* and *Z*), the Hadamard gate, the Parameterized gates, and the Universal gate. Each gate hereafter is initially described by a statevector that is transformed, by outer products and vector addition, into a single matrix. Multiplying this gate matrix by a statevector demonstrates the effect of the gate, mathematically. The effect is visualized by changes in orientation to a Bloch vector.

The operation of a Pauli gate expands upon that of a NOT gate in classical computing, performing not only bit flips (*X* and *Y* gates) but also phase flips (*Y* and *Z* gates).

For example,

the *X* gate ($X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$),

the *Y* gate ($Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = \begin{bmatrix} 0 & -i \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ i & 0 \end{bmatrix} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$), and

the *Z* gate ($Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$)

can, each, be represented three-dimensionally on a Bloch sphere as a reflection of a Bloch vector about the same-named axis (*i.e. X* gate::*x*-axis; *Y* gate::*y*-axis; *Z* gate::*z*-axis).

As such, a gate applied to a state whose Bloch vector is aligned with the same-named axis (*i.e. X*-gate applied to $|+\rangle$ or $|-\rangle$; *Y*-gate applied to $|+i\rangle$ or $|-i\rangle$; Z-gate applied to $|0\rangle$ or $|1\rangle$) does nothing. A state $|\Psi\rangle$ that is not affected by a gate *G*, where $G|\Psi\rangle = \lambda|\Psi\rangle$ for a real-numbered scalar λ, is called an eigenstate of *G*.

Multiplying a state column vector by each of these gate matrices demonstrates the effect of each gate, mathematically:

$$X|0\rangle=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}0\\ 1\end{bmatrix}=|1\rangle;\ X|1\rangle=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}=|0\rangle;$$

$$Y|0\rangle=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}i\\ 1\end{bmatrix}=i|1\rangle;\ Y|1\rangle=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\begin{bmatrix}0\\ -i\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}=|0\rangle;$$

$$Z|0\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\begin{bmatrix}1\\ 0\end{bmatrix}=|0\rangle;\ Z|1\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\begin{bmatrix}0\\ -1\end{bmatrix}=-|1\rangle.$$

The Hadamard gate does not operate like any gate in classical computing. This gate has the effect of placing a qubit in one of the computational bases ($|0\rangle$ or $|1\rangle$) into a superposition of states. For example, a qubit with state $|0\rangle$ becomes state $|+\rangle$, and a qubit with state $|1\rangle$ becomes state $|-\rangle$. The equation for the statevector of this gate can be represented as the addition of two outer products:

$$H=|0\rangle\langle+|+|1\rangle\langle-|$$

Computing the two outer products in vector form and extracting the common factor reduces the equation to addition between two matrices:

$$H=\frac{1}{\sqrt{2}}\left(\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}+\begin{bmatrix}0 & 1\\ 0 & -1\end{bmatrix}\right)=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Multiplying a state column vector by this gate matrix demonstrates the effect of the gate mathematically:

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

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

This effect is represented three-dimensionally on a Bloch sphere as a reflection about polar coordinates

$$\begin{bmatrix}1\\ 0\\ 1\end{bmatrix},$$

so that the Bloch vector aligned with the positive (or negative) *z*-axis becomes the Bloch vector aligned with the positive (or negative) *x*-axis (and vice versa), whereas the Bloch vector aligned with the positive *y*-axis becomes the Bloch vector aligned with the negative *y*-axis (and vice versa).

The Parameterized gate ($P(\phi)=|0\rangle\langle 0|+|1\rangle\begin{bmatrix}0\\e^{i\phi}\end{bmatrix}=\begin{bmatrix}1&0\\0&e^{i\phi}\end{bmatrix}$; $\phi \in \Re$) changes the phase of a qubit already in superposition. The ϕ parameter specifies the angle by which the phase should be rotated. For example, a 180° phase rotation transforms $|+\rangle$ into $|-\rangle$. Recalling that phase rotations occur on the *xy*-plane (around the *z*-axis) of the Bloch sphere, the effect of *P*(180°) is equivalent to the effect of a *Z* gate. Other named gates, such as the *S* and *T* gates, are *P* gates where ϕ is specified as 90° and 45°, respectively. Another example of a parameterized gate, which encompasses all other single qubit gates including the *P* gate, is the Universal gate:

$$U(\theta,\phi,\lambda)=\begin{bmatrix}\cos(\frac{\theta}{2}) & -e^{i\phi}\cos(\frac{\theta}{2})\\ e^{i\phi}\cos(\frac{\theta}{2}) & e^{i(\phi+\lambda)}\cos(\frac{\theta}{2})\end{bmatrix}$$

(The effect of $U(0, 0, \lambda)$ is equivalent to the effect of $P(\lambda)$.)

Not only can gates represent other gates, but sequences of gates can represent gates. For example, starting from state $|0\rangle$, applying an *H* gate transforms the qubit state into $|+\rangle$, appying a *P*(180°) or *Z* gate transforms the qubit state into $|-\rangle$, and applying another *H* gate transforms the qubit state into $|1\rangle$. By transforming $|0\rangle$ into $|1\rangle$, this *HZH* circuit identity has the same effect as the *X* gate. Alternately, applying the *H* gate followed by a second *H* gate has the effect of reversing the first *H* gate. **[1]** The same follows for the *X*, *Y*, and Z gates; applying the same two gates in succession reverses the first gate. For the *P* gates, setting the parameter angle of the second gate to negate the parameter angle of the first gate reverses the first gate. Thus, quantum gates are reversible (whereas classical gates are not).

A system of qubits has 2^n possible spin states with corresponding probability amplitudes and statevector entries. The single qubit system discussed thus far is described by two spin states:

i.e. $n=1\,;2^n=2.$

A two-qubit system is described by four spin states:

e.g. {00, 01, 10, 11}; $|\Psi\rangle=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle=\begin{bmatrix}a\\b\\c\\d\end{bmatrix}.$

The number of possible states increases exponentially for each additional qubit added to this system. The additional possible states for a multi-qubit system affect the composition of a gate. The matrix representation of such a gate is computed by a kronecker product (which this paper reperesents with the symbol, ж) of the gate applied to each qubit at a computational step. **[1]** For example, if, at a computational step, an X gate (*i.e.* $\begin{bmatrix}0&1\\1&0\end{bmatrix}$) is applied to both qubits of a two-qubit system, the kronecker product is:

$$X|q_1\rangle \text{ ж } X|q_0\rangle=\begin{bmatrix}0&X\\X&0\end{bmatrix}=\begin{bmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{bmatrix}.$$

In contrast, if, at a computational step, the X gate is applied to only the first qubit (called the control qubit) of a two-qubit system, the kronecker product is $I|q_1\rangle \text{ ж } X|q_0\rangle=\begin{bmatrix}X&0\\0&X\end{bmatrix}$, where I represents the identity matrix (*i.e.* $\begin{bmatrix}1&0\\0&1\end{bmatrix}$) signifying no operation on the second qubit (called the target qubit).

Conditional gates are a class of gates applied to multiple qubits, where the state of one qubit is correlated to the state of another qubit, and vice versa. For example, a CNOT gate observes whether the

state of the control qubit is $|1\rangle$; if so, then an X gate is applied to the target qubit. For a control q_0 and target q_1 with qubit statevector of $|q_1 q_0\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$, this relationship between input and output can be modeled by prepositional logic: $00 \rightarrow 00$; $01 \rightarrow 11$; $10 \rightarrow 10$; $11 \rightarrow 01$. In this case, the gate causes the probability amplitudes a_{01} and a_{11} to swap:

$$CNOT\,|q_1 q_0\rangle = a_{00}|00\rangle + a_{11}|01\rangle + a_{10}|10\rangle + a_{01}|11\rangle.$$

For a deterministic system where, for example, the control is $|0\rangle$ and the target is $|1\rangle$, the result is always:

$$CNOT\,|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}.$$

Likewise, for: $CNOT\,|01\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$; $CNOT\,|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$; $CNOT\,|11\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$.

For a probabilistic system where the control is $|+\rangle$ and the target is $|1\rangle$, with form $|1+\rangle = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$:

if $|+\rangle$ is $|1\rangle$ then $|1\rangle$ is $|0\rangle$, and if $|+\rangle$ is $|0\rangle$ then $|1\rangle$ is $|1\rangle$.

Given that $|+\rangle$ has a 50% probability of either result: $CNOT\,|1+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. **[1]**

Likewise, for $|0+\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix}$: $CNOT\,|0+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

In each case, measuring the state of the control always indicates the state of the target, and the state of the target cannot be described independent of the state of the control.

This correlation is called an entanglement of states. This effect corresponds to the entanglement of the states of quanta, which can be demonstrated in a physical system by generating a single quantum of higher energy that, when polarized, produces a pair of quanta with lower energies; or alternately, by mixing existing quanta using a coupler. Entangling qubit states enables multiple inputs at a computational step to be solved for simultaneously, where one output determines all other possible outputs.

Entangling qubits can not only increase the number of possible states in a system but also the types of operations possible with gates. For example, in addition to applying an H gate to the control (causing transformation to the state $|+\rangle$), applying an XH circuit identity to the target (causing transformation to the state $|1\rangle$, then $|-\rangle$) transforms the pair into:

$$|-+\rangle=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle-|11\rangle).$$

Appying the CNOT gate to $|-+\rangle$ causes the probability amplitudes a_{01} and a_{11} to swap:

$$CNOT\,|-+\rangle=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)=|--\rangle. \textbf{ [1]}$$

Likewise, applying the XH circuit identity to the control and the H gate to the target tranforms the pair into:

$$|+-\rangle=\frac{1}{2}(-|00\rangle-|01\rangle+|10\rangle+|11\rangle); \text{ then,}$$

$$CNOT\,|+-\rangle=\frac{1}{2}(-|00\rangle+|01\rangle+|10\rangle-|11\rangle)=|++\rangle.$$

In these cases, the gates changed the state of the control, applying the relative phase of the target eigenvalue introduced by the additional X gate, without affecting the target.

Additional gates such as the controlled-T, -Y, and -Z gates similarly cause the control to rotate about an axis without affecting the target, a Toffoli is a CNOT that adds a second control which must be in state $|1\rangle$ in order to apply an X gate to the target, and SWAP gate can swap the states of qubits in a two qubit system. While a Bloch sphere is not designed to visualize the phase or probability amplitude of combined states, a different visualization called a Q-sphere indicates the magnitude of probability amplitude by the size of the endpoints of a vector and indicates phase by the color of the vector corresponding to an angle, making it possible to visualize the above transformations on a single sphere. **[1]**

Adding entangled qubits to a computation is an example of short-circuit computing, which expands the width, without changing the depth, of a circuit. In classical computing, expanding the width requires also expanding the depth of a circuit. For an algorithm that factors all possible prime numbers up to a number *n*, the classical computing approach identifies prime numbers sequentially, exponentially adding circuits the larger that *n* is, while the quantum computing approach adds qubits to a single circuit and factors for additional prime numbers concurrently instead of sequentially, exponentially reducing the amount of time required to find all prime numbers up to n. This advantage is also applies to the context of search algorithms, reducing worst-case time complexity from O(N) to $O(N^{1/2})$. However, these results do not account for the instability of qubits so the hypothesized advantage has not yet been proven.

Quantum algorithms are currently designed with shorter circuit depths than classical algorithms due to the instability of qubits. Typically, the environment of the physical system that supports quantum

computing must be cooled to near absolute zero and isolated from external noise. Slight variations in such conditions causes noise and errors collectively referred to as decoherence. Computations may therefore rely on a histogram in order to identify and isolate the effect of decoherence. Real-time error detection and correction is relatively more costly for quantum computers than for classical computers so approaches to prevent decoherence are being developed in order to preserve quantum advantage. Some preventative approaches include computation optimization accounting for predicted decoherence based on environmental analyses, as well as shared processing of quantum computations between classical and quantum computers. **[4]** A classical computer can run quantum computations using algorithms, which add time complexity as compared with a quantum computer that models physical states in O(1) time.

Because qubits cannot be measured without information loss due to state collapse, qubits cannot currently be cloned. This quality, coupled with instability, represents a disadvantage when compared to clabits in most contexts, except for the field of encryption. Classical encryption depends on a two-way channel in order to transmit encoded secret messages which can be intercepted, cloned, and decoded.

Quantum encryption depends on a one-way quantum channel in order to transmit encoded secret messages. In the latter arrangement, the receiver does not know and attempts to guess the encoding. Once the message reaches the receiver, and dissimilar from classical encryption, the message can no longer be intercepted and cloned without the message becoming corrupted. The receiver verifies with checksum, and then informs the sender via classical two-way channel, if the message is corrupted. If the message is corrupted, the process is repeated; if not, the sender sends their encoding schema to the receiver, and the receiver sends their guess at the encoding schema back to the sender, by which both sender and receiver acknowledge that the bits that were successfully decoded. Those decoded bits become the revised secret message. Undecoded bits are discarded. **[0]**

While quantum computers may promote stronger encryption, they also threaten the strongest encryption models. For example, enhanced parallel processing capabilities applied to the prime number factorization problem could break prime-factor-based encryption like that used by RSA. **[5]** For now, the instability of qubits, which factors into the design of quantum encryption, deters effective quantum decryption, and positions quantum encryption as an effective present-day application of quantum computing. Other applications seem years away from widespread industrial use due to the cost of producing a stable quantum computing environment. For this reason, the first industrial uses will likely leverage a cloud computing environment in order to access resources served by a handful of companies vested in quantum computing.

REFERENCES

[0] Ramanathan, Kumarasan. "Quantum Computing and Quantum Physics for Beginners." Udemy, https://www.udemy.com/course/qc101-introduction-to-quantum-computing-quantum-physics-for-beginners/, 2020.

[1] “Qiskit Textbook.” Qiskit. https://learn.qiskit.org/course/, 2023.

[2] Physics Teacher. “What is probability amplitude and why is it complex?” Physics Stack Exchange. https://physics.stackexchange.com/questions/491706/what-is-probability-amplitude-and-why-is-it-complex/, 2019.

[3] Siddhant Singh. “What is the difference between a relative phase and a global phase? In particular, what is a phase?” Quantum Computing Stack Exchange. https://quantumcomputing.stackexchange.com/questions/5125/what-is-the-difference-between-a-relative-phase-and-a-global-phase-in-particula/, 2019.

[4] Patkin, Scott, Et. Al. “The Problem with Quantum Computers.” Scientific American, https://blogs.scientificamerican.com/observations/the-problem-with-quantum-computers/, 2019.

[5] Mone, Gregory. “The Quantum Threat: Cryptographers are Developing Algorithms to Ensure Security in a World of Quantum Computing.” Communications of the ACM, vol. 63, no. 7, 2020, pp. 12-14.