MATH 5390 - Quantum Computing Notes

Libao Jin

October 28, 2020

Contents

1 Introduction

- Quantum computing is a beautiful combination of quantum physics, computer science, and information theory.
- We take care to distinguish a quantum state from a vector that represents it.
- We make clear which notions are basis dependent (e.g., superposition) and which are not (e.g., entanglement), and emphasize the dependence of certain notions (e.g., entanglement) on a particular tensor decomposition.
- Tensor decompositions vs. direct sum decompositions.
- Fundamental concepts
  - Quantum state spaces
  - Quantum measurement
  - Entanglement
- Tensor product spaces and the relation to component spaces are fundamental to quantum information processing.
- Combintation of information theory and quantum mechanics gave rise to a new view of computation and information.
- Information theory can determine the efficiency of an algorithm or the robustness of a communication protocol without understanding details of the physical devices used for the computation or the communication. Information sicences have been firmly rooted in classical mechanics, e.g., the Turing machine is a classical mechanical model that behaves according to purely classical mechanical principles.
- Quantum mechanics underlies the working of traditional, classical computers and communication devices, from the transistor through the laser to the latest hardware advances that increase the speed and power and decrease the size of computer and communications components.
- Charles Bennett, Gilles Brassard, Stephne Wiesner: nonclassical properties of quantum measurement provided a probably secure mechanism for establishing a cryptographic key.
- Richard Feynman, Yuri Manin: entangled particles could not be simulated efficiently by a Turing machine.
- Quantum information processing, a field that includes quantum computing, quantum cryptography, quantum communications, and quantum games, explores the implications of using quantum mechanics instead of classical mechanics to model information and its processing. Placing computation on a quantum mechanical foundation led to the discovery of faster algorithms, novel cryptographic mechanisms, and improved communication protocols.
- The phrase *quantum computing* is closer in character to *analog computing* because the computational model for analog computing differs from that of standard computing: a continuum of values, rather than only a discrete set, is allowed. However, the analog computation does not support entanglement, a key resource or quantum computation, and measurements of a quantum computer's registers can yield only a small, discrete set of values.
- David Deutsch developed a notion of a quantum mechanical Turing machine. Daniel Bernstein, Vijay Vazirani, And Andrew Yao improved upon his model and showed that a quantum Turing machine could simulate a classical Turing machine, and hence any classical computation, with at most a polynomial time slowdown.
- Peter Shor surprised the world with his polynomial-time quantum algorithm for factoring integers.
- Quantum systems are notoriously fragile. Key properties, such as quantum entanglement,

are easily distributed by environmental influences that cause the quantum states to *decohere*.
- Shor and Robert Calderbank, quantum error correction techniques.
- Part I: basic building blocks of quantum information processing: quantum bits (qubits) and quantum gates. Quantum measurement, quantum state transformations, and entanglement between quantum subsystems. Quantum key distribution, quantum teleportation, and quantum dense coding.
- Part II: quantum algorithms. Shor's algorithm and Grover's algorithm.
- Part III explore entanglement and robust quantum computation. Quantum algorithms and protocols, adiabatic, cluster state, holonomic, and topological quantum computing, and the impact quantum information processing has had on classical computer science and physics.

2 Single-Qubit Quantum Systems

- Quantum bits are the fundamental units of information in quantum information processing in much the same way that bits (two voltage levels) are the fundamental units of information for classical processing.
- The behavior polarized photons under measurement: one of many possible realizations of quantum bits.
- Dirac's bra/ket notation, the standard notation used throughout quantum information processing as well as quantum mechanics.
- Quantum key distribution: an application of quantum information processing.

2.1 The Quantum Mechanics of Photon Polarization

This experiment can be performed by the reader using only minimal equipment: a laser pointer and three polaroids (polarization filters).

2.1.1 A Simple Experiment

Shine a beam of light on a projection screen. When polaroid A is placed between the light source and the screen, the intensity of the light reaching the screen is reduced. Let us suppose that the polarization of polaroid A is horizontal. Next, place a polaroid C between polaroid A and the projection screen. If polaroid C is rotated so that its polarization is orthogonal (vertical) to the polarization of A, no light reaches the screen. Finally, place polaroid B between polaroids A and C, surprisingly, at most polarization angles of B, light shines on the screen. The intensityof this light will be maximal if the polarization of B is at 45 degrees to both A and C.

2.1.2 A Quantum Explanation

The results of single photon experiments can be explained only using quantum mechanics. The quantum mechanical explanation of the experiment consists of two parts: a model of a photon's polarization state and a model of the interaction between a polaroid and a photon.

Quantum mechanics models a photon's polarization state by a unit vector, a vector of length 1, pointing in the appropriate direction. We write $|\uparrow\rangle$ and $|\rightarrow\rangle$ for the unit vectors that represent vertical and horizontal polarization respectively. Let $|v\rangle$ be a vector with some arbitrary label v. In quantum mechanics, the standard notation for a vector representing a quantum state is $|v\rangle$ which can be expressed as a linear combination $|v\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ of the two basis vectors, where a and b are called *amplitudes* of $|v\rangle$ in the directions $|\uparrow\rangle$ and $|\rightarrow\rangle$ respectively. If both a and b are both non-zero, then $|v\rangle$ is said to be a *superposition* of $|\uparrow\rangle$ and $|\rightarrow\rangle$.

Quantum mechanics models the interaction between a photon and a polaroid as follows. When a photon with polarization $|v\rangle = a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ meets a polaroid with preferred axis $|\uparrow\rangle$, the photon will get through with probability $|a|^2$ and will be absorbed with probability $|b|^2$. Furthermore, any photon that passes through the polaroid will now be polarized in the direction of the polaroid's preferred axis.

In summary, the polarization state of a photon is modeled as a unit vector. Its interaction with a polaroid is probabilistic and depends on the amplitude of the photon's polarization in the direction of the polaroid's preferred axis.

2.2 Single Quantum Bits

The space of possible polarization states of a photon is an example of a *quantum bit*, or *qubit*. A qubit has a continuum of possible values: any state represented by a unit vector $a\,|\uparrow\rangle + b\,|\rightarrow\rangle$ is a legitimate qubit value, where $a, b \in \mathbb{C}$.
In general, the set of all possible states of a physical system is called the *state space* of the system. Any quantum mechanical system that can be modeled by a two-dimensional complex vector space can be viewed as a qubit. Such systems, called *two-state quantum systems*, include photon polarization, electron spin, and the ground state together with an excited state of an atom. For a two-dimensional complex vector space to be viewed as a qubit, two linearly independent states, labeled $|0\rangle$ and $|1\rangle$, must be distinguished.
In Dirac's bra/ket notation, a *ket* such as $|x\rangle$, where x is an arbitrary label, refers to a vector representing a state of a quantum system. A vector $|v\rangle$ is a *linear combination* of vectors $|s_1\rangle, |s_2\rangle, \ldots, |s_n\rangle$ if there exist complex numbers a_i such that $|v\rangle = a_1\,|s_1\rangle + a_2\,|s_2\rangle + \cdots + a_n\,|s_n\rangle$. A set of vectors S *generates* a complex vector space V if every element $|v\rangle$ of V can be written as a complex linear combination of vectors in the set: every $|v\rangle \in V$ can be written as $|v\rangle = a_1\,|s_1\rangle + a_2\,|s_2\rangle + \cdots + a_n\,|s_n\rangle$ for some elements $|s_i\rangle \in S$ and complex numbers a_i. Given a set of vectors S, the subspace of all linear combinations of vectors in S is called the *span* of S and is denoted span(S). A set of vectors B for which every element of V can be written *uniquely* as a linear combination of vectors in B is called a basis for V. In a two-dimensional vector space, any two vectors that are not multiples of each other form a basis. In quantum mechanics, bases are usually required to be *orthonormal*.
An *inner product* $\langle v_2|v_1\rangle$, or *dot product*, on a complex vector space V is a complex function defined on pairs of vectors $|v_1\rangle$ and $|v_2\rangle$ in V, satisfying

- $\langle v|v\rangle$ is non-negative real,
- $\langle v_2|v_1\rangle = \overline{\langle v_1|v_2\rangle}$, and
- $(a\,\langle v_2| + b\,\langle v_3|)\,|v_1\rangle = a\,\langle v_2|v_1\rangle + b\,\langle v_3|v_1\rangle$,

where $\overline{z}$ is the complex conjugate $\overline{z} = a - \mathbf{i}b$ of $z = a + \mathbf{i}b$.
Two vectors $|v_1\rangle$ and $|v_2\rangle$ are said to be *orthogonal* if $\langle v_1|v_2\rangle = 0$. The *length*, or norm, of a vector $|v\rangle$ is $||v\rangle| = \sqrt{\langle v|v\rangle}$. Since all vectors $|x\rangle$ representing quantum states are of unit length, $\langle x|x\rangle = 1$ for any state vector $|x\rangle$. A set of vectors is said to be *orthonormal* if all of its elements are of length one and orthogonal to each other: a set of vectors $B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_n\rangle\}$ is orthonormal if $\langle\beta_i|\beta_j\rangle = \delta_{ij}$ for all i, j, where

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

For the state space of a two-state system to represent a quantum bit, two orthonormal distinguished states, labeled $|0\rangle$ and $|1\rangle$, must be specified. For instance, in the case of photon polarization, we may choose $|0\rangle$ and $|1\rangle$ to correspond to the states $|\uparrow\rangle$ and $|\rightarrow\rangle$, or to $|\nearrow\rangle$ and $|\nwarrow\rangle$. We follow the convention that $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\rightarrow\rangle$, which implies that $|\nearrow\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|\nwarrow\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. In the case of electron spin, $|0\rangle$ and $|1\rangle$ could correspond to the spin-up and spin-down states, or spin-left and spin-right. Bits vs. qubits: bits can take on only two values, 0 and 1, while qubits can take on not only the values $|0\rangle$ and $|1\rangle$ but also any superposition of these values, $a\,|0\rangle + b\,|1\rangle$, where a and b are complex numbers such that $|a|^2 + |b|^2 = 1$.
If basis $\{|\beta_1\rangle, |\beta_2\rangle\}$ is specified, a ket $|v\rangle = a\,|\beta_1\rangle + b\,|\beta_2\rangle$ can be written $\begin{bmatrix} a \\ b \end{bmatrix}$. Then conjugate

transpose $v^\dagger$ of a ket

$$|v\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} \text{is} v^\dagger = \begin{bmatrix} \overline{a_1} & \cdots & \overline{a_n} \end{bmatrix} = \langle v| .$$

In Dirac's notation, the conjugate transpose of a ket $|v\rangle$ is called a *bra* and is written $\langle v|$. Then the standard *inner product* $\langle a|b\rangle$ is defined to be the scalar obtained by multiplying the conjugate transpose $\langle a| = \begin{bmatrix} \overline{a}_1, \ldots, \overline{a}_n \end{bmatrix}$ with $|b\rangle$:

$$\langle a|b\rangle = \langle a| \, |b\rangle = \begin{bmatrix} \overline{a}_1 & \cdots & \overline{a}_n \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = \sum_{i=1}^{n} \overline{a}_i b_i.$$

Let $|v\rangle = a\,|0\rangle + b\,|1\rangle$, where $a, b \in \mathbb{R}^n$, then $\langle 0|0\rangle = 1$, $\langle 1|1\rangle = 1$, $\langle 0|1\rangle = 0$, $\langle 1|0\rangle = 1$, $\langle v|0\rangle = a$, $\langle v|1\rangle = b$.
In the standard basis, with ordering $\{|0\rangle, |1\rangle\}$, the basis elements $|0\rangle$ and $|1\rangle$ can be expressed as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.
Instead of qubits, physical systems with states modeled by three- or n-dimensional vector spaces could be used as fundamental units of computation. Three-valued units are called *qutrits*, and n-valued units re called *qudits*, which can be modeled using multiple qubits, a model of quantum information based on qudits has the same computational power as one based on qubits.

2.3 Single-Qubit Measurement

The measurement of more complicated systems retains many of the features of single-qubit measurement: the probabilistic outcomes and the effect measurement has on the state of the system. Quantum theory postulates that any device that measures a two-state quantum system must have two preferred states whose representative vectors, $\{|u\rangle, |u^\perp\rangle\}$, form an orthonormal basis for the associated vector space. Measurement of a state transforms the state into one of the measuring device's associated basis vectors $|u\rangle$ or $|u^\perp\rangle$. The probability that the state is measured as basis vector $|u\rangle$ is the square of the magnitude of the amplitude of the component of the state in the direction of the basis vector $|u\rangle$. For example, given a device for measuring the polarization of photons with associated basis $\{|u\rangle, |u^\perp\}$, the state $|v\rangle = a\,|u\rangle + b\,|u^\perp\rangle$ is measured as $|u\rangle$ with probability $|a|^2$ and as $|u^\perp\rangle$ with probability $|b|^2$.
Measurement of a quantum state changes the state. If a state $|v\rangle = a\,|u\rangle + b\,|u^\perp\rangle$ is measured as $|u\rangle$, then the state $|v\rangle$ changes to $|u\rangle$. A second measurement with respect to the same basis will return $|u\rangle$ with probability 1. The notion of superposition is basis-dependent; all states are superpositions with respect to some bases and not with respect to others. For instance, $a\,|0\rangle + b\,|1\rangle$ is a superposition with respect to the basis $\{|0\rangle, |1\rangle\}$ but not with respect to $\{a\,|0\rangle + b\,|1\rangle, \bar{b}\,|0\rangle - \overline{a}\,|1\rangle\}$. $|v\rangle = a\,|0\rangle + b\,|1\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results: a photon with polarization $|\nearrow\rangle = 1/\sqrt{2}(|\uparrow\rangle + |\rightarrow\rangle)$ behaves deterministically when measured with respect to the Hadamard basis $\{|\nearrow\rangle, |\nwarrow\rangle\}$, but it gives random results when measured with respect to the standard basis $\{|\uparrow\rangle, |\rightarrow\rangle\}$.
Though qubits can take on any one of infinitely many states, the properties of quantum measurement severely restrict the amount of information that can be extracted from a qubit. Information about a quantum bit can be obtained only by measurement, and any measurement results in one of the only two states, the two basis states associated with the measuring device: thus a single measurement yields at most a single classical bit of information.

2.4 A Quantum Key Distribution Protocol

The quantum theory introduced so far is sufficient to describe a first application of quantum information processing: a key distribution protocol that relies on quantum effects for its security and for which there is no classical analog.
Keys – binary strings or numbers chosen randomly from a sufficiently large set – provide the security for most cryptographic protocols, from encryption to authentication to secret sharing. Two general classes of keys exist: symmetric keys and public-private keys pairs.

- Public-private key pairs consist of a public key, knowable by all, and a corresponding private key whose secrecy must be carefully guarded by the owner.
- symmetric keys consist of a single key (or a pair of keys easily computable from one another) that are known to all of the legitimate parties and no one else. In the symmetric key case, multiple parties are responsible for guarding the security of the key.

Quantum key distribution protocols can be used securely anywhere classical key agreement protocols such as Diffie-Hellman can be used. The security of quantum key distribution rests on fundamental properties of quantum mechanics, whereas classical key agreement protocols rely on the computational intractability of a certain problem. The aim of the BB84 protocol is to establish a secret key, a random sequence of bit values 0 and 1, known only to the two parties, who may use this key to support a cryptographic task such as exchanging secret messages or detecting tampering. The bb84 protocol enables two parties to be sure that if they detect no problems while attempting to establish a key, then with high probability it is secret. The protocol does not guarantee, however, that they will succeed in establishing a private key.
Suppose Alice and Bob are connected by two public channels: an ordinary bidirectional classical channel and a unidirectional quantum channel. The quantum channel allows Alice to send a sequence of single qubits to Bob; we suppose the qubits are encoded in the polarization states of individual photons. Both channels can be observed by an eavesdropper Eve. To begin the process of establishing a private key, Alice uses quantum or classical means to generate a random sequence of classical bit values. As we will see, a random subset of this sequence will be the final private key. Alice then randomly encodes each bit of this sequence in the polarization state of a photon by randomly choosing for each bit one of the following two agreed-upon bases in which to encode it: the standard basis, $0 \mapsto |\uparrow\rangle, 1 \mapsto |\rightarrow\rangle$, or the Hadamard basis, $0 \mapsto |\nearrow\rangle = 1/\sqrt{2}(|\uparrow\rangle + |\rightarrow\rangle)$, $1 \mapsto |\nwarrow\rangle = 1/\sqrt{2}(|\uparrow\rangle - |\rightarrow\rangle)$. She sends this sequence of photons to Bob through the quantum channel. Bob measures the state of each photon he receives by randomly picking either basis. Over the classical channel, Alice and Bob check that Bob has received a photon for ever one Alice has sent, and only then do Alice and Bob tell each other the bases they used for encoding and decoding (measuring) each bit. When the choice of bases agree, Bob's measured bit value agrees with the bit value that Alice sent. When they chose different bases, the chance that Bob's bit matches Alice's is only 50 percent. Without revealing the bit values themselves, which would also reveal the values to Eve, there is no way for Alice and Bob to figure out which of these bit values agree and which do not. So they simply discard all the bits on which their choice of bases differed. An average of 50 percent of all bits transmitted remain. Then, depending on the level of assurance they require, Alice and Bob compare a certain number of bit values to check that no eavesdropping has occurred. These bits will also be discarded, and only the remaining bits will be used as their private key.
The no-cloning principle of quantum mechanics means that it is impossible to reliably copy quantum information unless a basis in which it is encoded is known; all quantum copying machines are basis dependent.

2.5 The State Space of a Single-Qubit System

The *state space* of a classical or quantum physical system is the set of all possible states of the system. A state of the system consists of any combination of the positions, momenta, polarizations, spins, energy, and so on of the particles in the system. More generally, the state space for a single qubit, no matter how it is realized, is the set of possible qubit values, $\{a|0\rangle + b|1\rangle\}$, where $|a|^2+|b|^2= 1$ and $a|0\rangle+b|1\rangle$ and $a'|0\rangle+b'|1\rangle$ are considered the same qubit value if $a|0\rangle+b|1\rangle = c(a'|0\rangle+b'|1\rangle)$ for some modulus one complex number c.

2.5.1 Relative Phases versus Global Phases

The same quantum state can be represented by more than one vector means that there is a critical distinction between the complex vector space and the quantum state space: unit vectors equivalent up to multiplication by a complex number of modulus one represent the same state. The multiple by which two vectors representing the same quantum state differ is called the *global phase*. We use the equivalence relation $|v\rangle \sim |v'\rangle$ to indicate that $|v\rangle = c|v'\rangle$ for some complex global phase $c = e^{\mathbf{i}\phi}$. The space in which two two-dimensional complex vectors are considered equivalent if they are multiples of each other is called *complex projective space* of dimension one. This *quotient space* is a space obtained by identifying sets of equivalent vectors with a single point in the space:

$$\mathbf{CP}^1 = \{a|0\rangle + b|1\rangle\}/\sim .$$

So the quantum state space for a single-qubit system is in one-to-one correspondence with the points of the complex projective space $\mathbf{CP}^1$.
The *relative phase* (in the standard basis) of a superposition $a|0\rangle + b|1\rangle$ is a measure of the angle in the complex plane between the two complex numbers a and b. More precisely, the relative phase is the modulus one complex number $e^{\mathbf{i}\phi}$ satisfying $a/b = e^{\mathbf{i}\phi}|a|/|b|$. While multiplication with a unit constant does not change a quantum state vector, relative phases in a superposition do represent distinct quantum state: even though $|v_1\rangle \sim e^{\mathbf{i}\phi}|v_1\rangle$, the vectors $1/\sqrt{2}(e^{\mathbf{i}\phi}|v_1\rangle + |v_2\rangle)$ and $1/\sqrt{2}(|v_1\rangle + |v_2\rangle)$ do *not* represent the same state.
A few single-qubit states:

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

The basis $\{|+\rangle, |-\rangle\}$ is referred to as the Hadamard basis.

2.5.2 Geometric Views of the State Space of a Single Qubit

- Extended Complex Plane $C\cup\{\infty\}$. A correspondence between the set of all complex numbers and single-qubit states is given by

$$a|0\rangle + b|1\rangle \mapsto b/a = \alpha; \alpha \mapsto \frac{1}{\sqrt{1+|\alpha|^2}}|0\rangle + \frac{\alpha}{\sqrt{1+|\alpha|^2}}|1\rangle .$$

It is not defined for the state with $a = 0$ and $b = 1$. To make this correspondence one-to-one we need to add a single point, which we label ∞, to the complex plane and define $\infty \leftrightarrow |1\rangle$. For example, we have

$$\begin{aligned} |0\rangle &\mapsto 0, \\ |1\rangle &\mapsto \infty, \\ |+\rangle &\mapsto 1, \\ |-\rangle &\mapsto -1, \\ |\mathbf{i}\rangle &\mapsto \mathbf{i}, \\ |-\mathbf{i}\rangle &\mapsto -\mathbf{i}. \end{aligned}$$

- Block Sphere. We can map each state, represented by the complex number $\alpha = s + \mathbf{i}t$, onto the unit sphere in three real dimensions, the points $(x, y, z) \in \mathbb{C}$ satisfying $|x|^2+|y|^2+|z|^2= 1$, via the standard *stereographic projection*

$$(s, t) \mapsto \left(\frac{2s}{|\alpha|^2+1}, \frac{2t}{|\alpha|^2+1}, \frac{1 - |\alpha|^2}{|\alpha|^2+1} \right).$$

further requiring that $\infty \mapsto (0, 0, -1)$.

$$\begin{aligned} |0\rangle &\mapsto (0, 0, 1), \\ |1\rangle &\mapsto (0, 0, -1), \\ |+\rangle &\mapsto (1, 0, 0), \\ |-\rangle &\mapsto (-1, 0, 0), \\ |\mathbf{i}\rangle &\mapsto (0, 1, 0), \\ |-\mathbf{i}\rangle &\mapsto (0, -1, 0. \end{aligned}$$

Three representation of the quantum state space for a single-qubit system.

(a) Vectors written in ket notation: $a\,|0\rangle + b\,|1\rangle$ with complex coefficients a and b, subject to $|a|^2+|b|^2= 1$, where a and b are unique up to a unit complex factor. Because of this factor, the global phase, this representation is not one-to-one.
(b) Extended complex plane: a single complex number $\alpha \in \mathbb{C}$ or ∞. This representation is one-to-one.
(c) Block sphere: points (x, y, z) on the unit sphere. This representation is also one-to-one.

2.5.3 Comments on General Quantum State Spaces

3 Multiple-Qubit Systems

The state space of a quantum system grows exponentially with the number of particles. The state of the classical system can be completely characterized by describing the state of each of its component pieces separately. A surprising and unintuitive aspect of quantum systems is that often the state of a system cannot be described in terms of the states of its component pieces. States that cannot be so described are called *entangled states*, which are a uniquely quantum phenomenon. Most states in a multiple-qubit system are entangled states. Section 3.1: the difference between the *direct sum* of two or more vector spaces and the *tensor product* of a set of vector spaces.

3.1 Quantum State Spaces

- Classical state spaces combine through the direct sum, i.e., the direct sum of individual states (a vector in a two-dimensional vector space) of a system of n objects gives a vector space of $2n$ dimensions.
- Quantum systems spaces combine through the tensor product, which results in a vectors space of 2^n dimensions.

3.1.1 Direct Sums of Vector Spaces

The *direct sum* $V \oplus W$ of two vector spaces V and W with bases $A = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle\}$ and $B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_m\rangle\}$ respectively is the vector space with basis

$$A \cup B = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle, |\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_m\rangle\}.$$

The order of the basis is arbitrary. Every element $|x\rangle \in V \oplus W$ can be written as $|x\rangle = |v\rangle \oplus |w\rangle$ for some $|v\rangle \in V$ and $|w\rangle \in W$. For V and W of dimension n and m respectively, $V \oplus W$ has dimension $n + m$:

$$\dim(V \oplus W) = \dim(V) + \dim(W).$$

When V and W are inner product spaces, the standard inner product on $V \oplus W$ is given by

$$(\langle v_2| \oplus \langle w_2|)(|v_1\rangle \oplus |w_1\rangle) = \langle v_2|v_1\rangle + \langle w_2|w_1\rangle.$$

Suppose that the state of each of three classical objects O_1, O_2, and O_3 is fully described by two parameters, the positions x_i and the momentum p_i. Then the state of the system can be described by the direct sum of the states of the individual objects:

$$\begin{bmatrix} x_1 \\ p_1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \\ p_2 \end{bmatrix} \oplus \begin{bmatrix} x_3 \\ p_3 \end{bmatrix} = \begin{bmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \\ x_3 \\ p_3 \end{bmatrix}.$$

3.1.2 Tensor Products of Vector Spaces

The *tensor product* $V \otimes W$ of two vector spaces V and W with bases $A = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle\}$ and $B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_m\rangle\}$ respectively is an nm-dimensional vector space with a basis consisting of

the nm elements of the form $|\alpha_i\rangle \otimes |\beta_j\rangle$ where $\otimes$ is the tensor product, an abstract binary operator that satisfies the following relations:

$$\begin{aligned}(|v_1\rangle + |v_2\rangle) \otimes |w\rangle &= |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \\ |v\rangle \otimes (|w_1\rangle + |w_2\rangle) &= |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \\ (a\,|v\rangle) \otimes |w\rangle &= |v\rangle \otimes (a\,|w\rangle) = a(|v\rangle \otimes |w\rangle).\end{aligned}$$

Taking $k = \min(n, m)$, all elements of $V \otimes W$ have form

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle + \cdots + |v_k\rangle \otimes |w_k\rangle$$

for some $v_i \in V$ and $w_i \in W$. Due to the relations defining the tensor product, such a representation is not unique. Furthermore, while all elements of $V \otimes W$ can be written

$$a_1(|\alpha_1\rangle \otimes |\beta_1\rangle) + a_2(|\alpha_2\rangle \otimes |\beta_1\rangle) + \cdots + a_{nm}(|\alpha_n\rangle \otimes |\beta_m\rangle),$$

most elements of $V \otimes W$ cannot be written as $|v\rangle \otimes |w\rangle$, where $v \in V$ and $w \in W$. It's common to write $|v\rangle\,|w\rangle$ for $|v\rangle \otimes |w\rangle$.
If V and W are inner product spaces, then $V \otimes W$ can be given an inner product by taking the product of the inner products on V and W; the inner product of $|v_1\rangle \otimes |w_1\rangle$ and $|v_2\rangle \otimes |w_2\rangle$ is given by

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_2\rangle \langle w_2|w_1\rangle,$$

Given orthonormal bases $\{|\alpha_i\rangle\}$ for V and $\{|\beta_j\rangle\}$ for W, the basis $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ for $V \otimes W$ is also orthonormal. The tensor product $V \otimes W$ has dimension $\dim(V) \times \dim(W)$, so the tensor product of n two-dimensional vector spaces has 2^n dimensions. States of $V \otimes W$ that cannot be written as the tensor product of a vector in V and a vector in W are called *entangled* states, which cannot be written as the tensor product of a vector in V and a vector in W.

3.1.3 The State Space of an n-Qubit System

Given two quantum systems with states represented by unit vectors in V and W respectively, the possible states of the joint quantum system are represented by unit vector space $V \otimes W$. For $0 \le i < n$, let V_i be the vector space, with basis $\{|0\rangle_i, |1\rangle_i\}$, corresponding to a single qubit. The standard basis for the vector space $V_{n-1} \otimes \cdots \otimes V_1 \otimes V_0$ for an n-qubit system consists of the 2^n vectors

$$\begin{aligned}\{\,&|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0, \\ &|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0, \\ &\vdots \\ &|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0\}.\end{aligned}$$

More compact and readable notation uses $|b_{n-1} \ldots b_0\rangle$ to represent $|b_{n-1}\rangle \otimes \cdots \otimes |b_0\rangle$. In this notation the standard basis for an n-qubit system can be written

$$\{|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle\}.$$

We will represent the state $|b_{n-1} \ldots b_0\rangle$ more compactly as $|x\rangle$, where b_i are the digits of the binary representation for the decimal number x. In this notation, the standard basis for an n-qubit system is written

$$\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}.$$

To use matrix notation for state vectors of an n-qubit system, the order of basis vectors must be established, basis vectors with numbers are assumed to be sorted numerically. Using this convection, the two qubit state will have the following matrix representation:

$$\frac{1}{2}|00\rangle + \frac{\mathbf{i}}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|0\rangle + \frac{\mathbf{i}}{2}|1\rangle + \frac{1}{\sqrt{2}}|3\rangle \implies \begin{bmatrix} 1/2 \\ \mathbf{i}/2 \\ 0 \\ 1/\sqrt{2} \end{bmatrix}.$$

Bell basis for a two-qubit system, $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, where

$$\begin{aligned} |\Phi^+\rangle &= 1/\sqrt{2}(|00\rangle + |11\rangle), \\ |\Phi^-\rangle &= 1/\sqrt{2}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= 1/\sqrt{2}(|01\rangle + |10\rangle), \\ |\Psi^-\rangle &= 1/\sqrt{2}(|01\rangle - |10\rangle). \end{aligned}$$

Bell basis is important for various applications of quantum information processing including quantum teleportation. In the multiple-qubit case, not only do vectors that are multiples of each other refer to the same quantum state, but properties of the tensor product also mean that phase factors distribute over tensor products, the same phase factor in different qubits of a tensor product represent the same state:

$$|v\rangle \otimes (e^{\mathbf{i}\phi}|w\rangle) = e^{\mathbf{i}\phi}(|v\rangle \otimes |w\rangle) = (e^{\mathbf{i}\phi}|v\rangle) \otimes |w\rangle.$$

If we write every quantum state as

$$a_0|0\ldots00\rangle + a_1|0\ldots01\rangle + \cdots + a_{2^n-1}|1\ldots11\rangle$$

and require the first non-zero a_i to be real and non-negative, then every quantum state has a unique representation. The quantum state space of an n-qubit system has $2^n - 1$ complex dimensions. The space of distinct quantum states of an n-qubit system is a *complex projective space* of dimension $2^n - 1$.

3.2 Entangled States

Any tensor product of n individual single-qubit states can be specified by n complex numbers. However, it takes $2^n - 1$ complex numbers to describe states of an n-qubit system, the vast majority of n-qubit states cannot be described in terms of the state of n separate single-qubit systems. States that cannot be written as the tensor product of n single-qubit states are called *entangled* states. Strictly speaking, entanglement is always with respect to a specified tensor product decomposition of the state space. Given a state $|\psi\rangle$ of some quantum system with associated vector space V and a tensor decomposition of V, $V = V_1 \otimes \cdots \otimes V_n$, the state $|\psi\rangle$ is *separable*, or *unentangled*, with respect to that decomposition if it can be written as

$$|\psi\rangle = |v_1\rangle \otimes \cdots \otimes |v_n\rangle.$$

where $|v_i\rangle$ is contained in V_i. Entanglement is not basis dependent, it depends on the tensor decomposition.

3.3 Basics of Multi-Qubit Measurement

Let V be the $N = 2^n$ dimensional vector space associated with an n-qubit system. Any device that measures this system has an associated direct sum decomposition into orthogonal subspaces

$$V = S_1 \oplus \cdots \oplus S_k$$

for some $k \leq N$. The number k corresponds to the maximum number of possible measurement outcomes for a state measured with that particular device. That any device has an associated direct sum decomposition is a direct generalization of the single-qubit case. Every device measuring a single-qubit system has an associated orthonormal basis $\{|v_1\rangle, |v_2\rangle\}$ for the vector space V associated with the single-qubit system; the vectors $|v_i\rangle$ each generate a one-dimensional subspace S_i (consisting of all multiples $a|v_i\rangle$ where a is a complex number), and $V = S_1 \oplus S_2$. Furthermore, the only nontrivial decompositions of the vector space V are into two one-dimensional subspaces, and any choice of unit length vectors, one from each of the subspaces, yields an orthonormal basis. When a measuring device with associated direct sum decomposition $V = S_1 \oplus \cdots \oplus S_k$ interacts with an n-qubit system in state $|\psi\rangle$, the interaction changes the state to one entirely contained within one of the subspaces, and chooses the subspace with probability equal to the square of the absolute value of the amplitude of the component of $|\psi\rangle$ in that subspace. More formally, the state $|\psi\rangle$ has a unique direct sum decomposition $|\psi\rangle = a_1|\psi_i\rangle \oplus \cdots \oplus a_k|\psi_k\rangle$, where $|\psi_i\rangle$ is a unit vector in S_i and a_i is real and non-negative. When $|\psi\rangle$ is measured, the state $|\psi_i\rangle$ is obtained with probability $|a_i|^2$. That any measuring device has an associated direct sum decomposition, and that interaction can be modeled in this way, is an axiom of quantum mechanics.

3.4 Quantum Key Distribution Using Entangled States

The Ekert 91 protocol resembles the BB84 protocol. In this protocol, Alice and Bob establish a shared key by separately performing random measurements on their halves of an EPR pair and then comparing which bases they used over a classical channel. The protocol begins with the creation of a sequence of pairs of qubits, all in the entangled state $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. Alice receives the first qubit of each pair, while Bob receives the second. When they wish to create a secrete key, for each qubit they both independently and randomly choose either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ in which to measure, just as in the BB84 protocol. After they have made their measurements, they compare bases and discard those bits for which their bases differ.

4 Measurement of Multiple-Qubit States

The non-classical behavior of quantum measurement is critical to quantum information processing application.

4.1 Dirac's Bra/Ket Notation for Linear Transformations

Dirac's bra/ket notation provides a convenient way of specifying linear transformations on quantum states. The conjugate transpose of the vector denoted by ket $|\psi\rangle$ is denoted by bra $\langle\psi|$, and the inner product of vectors $|\psi\rangle$ and $|\phi\rangle$ is given by $\langle\psi|\phi\rangle$. The notation $|x\rangle\langle y|$ represents the outer product of the vectors $|x\rangle$ and $\langle y|$. Matrix multiplication is associative, and scalars commute with everything, so relations such as the following hold:

$$(|a\rangle\langle b|)|c\rangle = |a\rangle(\langle b|c\rangle) = (\langle b|c\rangle)|a\rangle.$$

Let V be a vector space associated with a single-qubit system. The matrix for the operator $|0\rangle\langle 0|$ with respect to the standard basis in the standard order $\{|0\rangle, |1\rangle\}$ is

$$|0\rangle\langle 0| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}.$$

The notation $|0\rangle\langle 1|$ represents the linear transformation that maps $|1\rangle$ to $|0\rangle$ and $|0\rangle$ to the null vector, a relationship suggested by the notation:

$$(|0\rangle\langle 1|)|1\rangle = |0\rangle(\langle 1|1\rangle) = |0\rangle(1) = |0\rangle,$$
$$(|0\rangle\langle 1|)|0\rangle = |0\rangle(\langle 1|0\rangle) = |0\rangle(0) = 0.$$

Similarly,

$$|1\rangle\langle 0| = \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}, |1\rangle\langle 1| = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}.$$

Thus, all two-dimensional linear transformations on V can be written in Dirac's notation:

$$\begin{bmatrix}a & b\\c & d\end{bmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|.$$

An operator on an n-qubit system that maps the basis vector $|j\rangle$ to $|i\rangle$ and all other standard basis elements to 0 can be written

$$O = |i\rangle\langle j|$$

is the standard basis; the matrix for O has a single non-zero entry 1 in the ij-th place. A general operator O with entries a_{ij} in the standard basis can be written

$$O = \sum_i \sum_j a_{ij}|i\rangle\langle j|.$$

Similarly, the ij-th entry of the matrix for O in the standard basis is given by $\langle i|O|j\rangle$. Given a vector $|\psi\rangle = \sum_k b_k|k\rangle$, applying operator O gives:

$$O|\psi\rangle = \left(\sum_i \sum_j a_{ij}|i\rangle\langle j|\right)\left(\sum_k b_k|k\rangle\right) = \sum_i \sum_j \sum_k a_{ij}b_k|i\rangle\langle j|k\rangle = \sum_i \sum_j a_{ij}b_j|i\rangle.$$

More generally, if $\{|\beta_j\rangle\}$ is a basis for an N-dimensional vector space V, then an operator $O : V \to V$ can be written as

$$\sum_{i=1}^{N}\sum_{j=1}^{N} b_{ij} |\beta_i\rangle |\beta_j\rangle$$

with respect to this basis. In particular, the matrix for O with respect to basis $\{|\beta_i\rangle\}$ has entries $O_{ij} = b_{ij}$.

4.2 Projection Operators for Measurement

For any subspace S of V, the subspace $S^\perp$ satisfy $V = S \oplus S^\perp$; thus, any vector $|v\rangle \in V$ can be written uniquely as the sum of a vector $\mathbf{s}_1 \in S$ and a vector $\mathbf{s}_2 \in S^\perp$. For any S, the *projection operator* P_S is the linear operator $P_S : V \to S$ that sends $|v\rangle \mapsto \mathbf{s}_1$ where $|v\rangle = \mathbf{s}_1 + \mathbf{s}_2$ with $\mathbf{s}_1 \in S_1$ and $\mathbf{s}_2 \in S_2$. We use the notation $\mathbf{s}_1$ and $\mathbf{s}_2$ are generally not unit vectors. The operator $|\psi\rangle \langle\psi|$ is the projection operator onto the subspace spanned by $|\psi\rangle$. Projection operators are sometimes called *projectors* for short. For any direct sum decomposition of $V = S_1 \oplus \cdots \oplus S_k$ into orthogonal subspaces S_i there are k related projection operators $P_i : V \to S_i$ where $P_i |v\rangle = \mathbf{s}_i$ where $|v\rangle = \mathbf{s}_1 + \cdots + \mathbf{s}_k$ with $s_i \in S_i$. In this terminology, a measuring device with associated decomposition $V = S_1 \oplus \cdots \oplus S_k$ acting on a state $|\psi\rangle$ results in the state

$$|\phi\rangle = \frac{P_i |\psi\rangle}{|P_i |\psi\rangle|}$$

with probability $|P_i |\psi\rangle|^2$.
Let P_S be the projection operator from an n-dimensional vector space V onto an s-dimensional subspace S with basis $\{|\alpha_0\rangle, \ldots, |\alpha_{s-1}\rangle\}$. Then

$$P_S = \sum_{i=1}^{s-1} |\alpha_i\rangle \langle\alpha_i| = |\alpha_0\rangle \langle\alpha_0| + \cdots + |\alpha_{s-1}\rangle \langle\alpha_{s-1}| .$$

Let V and W be two vector spaces with inner product. The *adjoint operator* or *conjugate transpose* $O^\dagger : V \to W$ of an operator $O : W \to V$ is defined to be the operator that satisfies the following inner product relation. For any $\mathbf{v} \in V$ and $O\mathbf{w} \in W$, the inner product between $O^\dagger\mathbf{v}$ and $\mathbf{w}$ is the same as the inner product between $\mathbf{v}$ and $O\mathbf{w}$:

$$O^\dagger\mathbf{v} \cdot \mathbf{w} = \mathbf{v} \cdot O\mathbf{w}.$$

The definition of a projection operator P implies that applying a projection operator many times in succession has the same effect as just applying it once: $PP = P$. Furthermore, any projection operator is its own adjoint: $P = P^\dagger$. Thus

$$|P |v\rangle|^2 = (\langle v| P^\dagger)(P |v\rangle) = \langle v| P |v\rangle$$

for any projection operator P and all $|v\rangle \in V$.

Example 4.1 (Formal treatment of single-qubit measurement in the standard basis)**.** Let V be the vector space associated with a single-qubit system. The direct sum decomposition for V associated with measurement in the standard basis is $V = S \oplus S'$, where S is the subspace generated and $P' : V \to S$, where $P = |0\rangle \langle 0|$ and $P' = |1\rangle \langle 1|$. Measurement of the state $|\psi\rangle = a |0\rangle + b |1\rangle$ results in the state $P |\psi\rangle / |P |\psi\rangle|$ with probability $|P |\psi\rangle|^2$. Since

$$P |\psi\rangle = (|0\rangle \langle 0|) |\psi\rangle = |0\rangle \langle 0|\psi\rangle = a |0\rangle .$$

and

$$|P|\psi\rangle|^2 = \langle\psi|P|\psi\rangle = \langle\psi|(|0\rangle\langle 0|)|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = \overline{a}a = |a|^2.$$

the result of the measurement is $a|0\rangle/|a|$ with probability $|a|^2$.

Example 4.2 (Measuring a two-qubit state with respect to the full standard basis decomposition)**.** Let V be the vector space associated with a two-qubit system and $|\phi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|01\rangle + a_{11}|11\rangle$ an arbitrary two-qubit state. Consider a measurement with decomposition $V = S_{00} \oplus S_{01} \oplus S_{10} \oplus S_{11}$, where S_{ij} is the one-dimensional complex subspace spanned by $|ij\rangle$. The related projection operators $P_{ij} : V \to S_{ij}$ are $P_{00} = |00\rangle\langle 00|$, $P_{01} = |01\rangle\langle 01|$, $P_{10} = |10\rangle\langle 10|$, and $P_{11} = |11\rangle\langle 11|$. The state after measurement will be $P_{ij}|\psi\rangle/|P_{ij}|\psi\rangle|$ with probability $|P_{ij}|\psi\rangle|^2$. The state after measurement is either

$$\frac{P_{00}|\psi\rangle}{|P_{00}|\psi\rangle|} = \frac{a_{00}|00\rangle}{|a_{00}|} \sim |00\rangle.$$

with probability $\langle\psi|P_{00}|\psi\rangle = |a_{00}|^2$, or $|01\rangle$ with probability $|a_{01}|^2$, or $|10\rangle$ with probability $|a_{10}|^2$, or $|11\rangle$ with probability $|a_{11}|^2$.

4.3 Hermitian Operator Formalism for Measurement

Let $O : V \to V$ be a linear operator. If $O\mathbf{v} = \lambda\mathbf{v}$ for some non-zero vector $\mathbf{v} \in V$, then λ is an *eigenvalue* and $\mathbf{v}$ is a λ-*eigenvector* of O. If both $\mathbf{v}$ and $\mathbf{w}$ are λ-eigenvectors of O, then $\mathbf{v} + \mathbf{w}$ is also a λ-eigenvector, so the set of all λ-eigenvectors forms a subspace of V called the λ-eigenspace of O. For an operator with a diagonal matrix representation, the eigenvalues are simply the values along the diagonal.
An operator $O : V \to V$ is *Hermitian* if it is equal to its adjoint, $O^\dagger = O$. Suppose λ is an eigenvalue of an Hermitian operator O with eigenvector $|x\rangle$. Since

$$\lambda\langle x|x\rangle = \langle x|\lambda|x\rangle = \langle x_\lambda|(O|x_\lambda\rangle) = (\langle x|O^\dagger)|x\rangle = \overline{\lambda}\langle x|x\rangle,$$

$\lambda = \overline{\lambda}$, which means that all eigenvalues of a Hermitian operator are real.
The eigenspaces $S_{\lambda_1}, S_{\lambda_2}, \ldots, S_{\lambda_k}$ of a Hermitian operator are orthogonal and satisfy $S_{\lambda_1} \oplus S_{\lambda_2} \oplus \cdots \oplus S_{\lambda_k} = V$. For any operator, two distinct eigenvalues have disjoint eigenspaces since, for any unit vector $|x\rangle$, $O|x\rangle = \lambda_0|x\rangle$ and $O|x\rangle = \lambda_1|x\rangle$ imply $(\lambda_0 - \lambda_1)|x\rangle = 0$, which implies that $\lambda_0 = \lambda_1$. For any Hermitian operator, the eigenvectors for distinct eigenvalues must be orthogonal. Suppose $|v\rangle$ is a λ-eigenvector and $|w\rangle$ is a μ-eigenvector with $\lambda \neq \mu$. Then

$$\lambda\langle v|w\rangle = (\langle v|O^\dagger)|w\rangle = \langle v|(O|w\rangle) = \mu\langle v|w\rangle.$$

Since λ and μ are distinct eigenvalues, $\langle v|w\rangle = 0$. Thus, S_{λ_i} and S_{λ_j} are orthogonal for $\lambda_i \neq \lambda_j$.
Let V be an N-dimensional vector space, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the $k \leq N$ distinct eigenvalues of an Hermitian operator $O : V \to V$. Also, $V = S_{\lambda_1} \oplus \cdots \oplus S_{\lambda_k}$, where S_{λ_i} is the eigenspace of O with eigenvalue λ_i. This direct sum decomposition of V is called the *eigenspace decomposition* of V for the hermitian operator O. Thus, any Hermitian operator $O : V \to V$ uniquely determines a subspace decomposition for V. Furthermore, any decomposition of a vector space V into the direct sum of subspaces $S_1, \ldots, S_k$ can be realized as the eigenspace decomposition of Hermitian operator $O : V \to V$: let P_i be the projectors onto the subspaces S_i, and let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be any set of distinct real values; then $O = \sum_{i=1}^k \lambda_i P_i$ is a Hermitian operator with the desired direct sum decomposition.

Any Hermitian operator with the appropriate direct sum decomposition can be used to specify a given measurement. It is important to recognize, however, that quantum measurement is not modeled by the *action* of a Hermitian operator on a state. The projectors P_j associated with a Hermitian operator O, not O itself, act on a state. Which projector acts on the state depends on the probabilities $p_j = \langle\psi| P_j |\psi\rangle$.

4.3.1 The measurement Postulate

It is only the results of measurements that we can directly observe. For this reason, the Hermitian operators we use to specify measurements are called *observables*. The measurement postulate of quantum mechanics states that:

- Any quantum measurement can be specified by a Hermitian operator O called an observable.
- The possible outcomes of measuring a state $|\psi\rangle$ with an observable O are labeled by the eigenvalues of O. Measurement of sate $|\psi\rangle$ results in the outcome labeled by the eigenvalue λ_i of O with probability $|P_i |\psi\rangle|^2$ where P_i is the projector onto the λ_i-eigenspace.
- (Projection) The state after measurement is the normalized projection $P_i |\psi\rangle / |P_i |\psi\rangle|$ of $|\psi\rangle$ onto the λ_i-eigenvspace.

Any Hermitian operator O with eigenvalues λ_j can be written as $O = \sum_j \lambda_j P_j$, where P_j are the projectors for the λ_j-eigenspaces of O. Every projector is Hermitian with eigenvalues 1 and 0 where the 1-eigenspace is the image of the operator. For an m-dimensional subspace S of V spanned by the basis $\{|i_1\rangle, \ldots, |i_m\rangle\}$, the associated projector

$$P_S = \sum_{j=1}^{m} |i_j\rangle \langle i_j|$$

maps vectors in V into S. If P_S and P_T are projectors for orthogonal subspaces S and T, the projector for the direct sum $S \oplus T$ is $P_S + P_T$. If P is a projector onto subspace S then $\mathrm{tr}(P)$, the sum of the diagonal elements of any matrix representing P, is the dimension of S. This argument applies to any basis since the trace is basis independent.
Given linear operator A and B on vector spaces V and W respectively, the *tensor product* $A \otimes B$ acts on elements $v \otimes w$ of the tensor product space $V \otimes W$ as follows:

$$(A \otimes B)(v \otimes w) = Av \otimes Bw.$$

It follows from this definition that

$$(A \otimes B)(C \otimes D) = AC \otimes BD.$$

Let O_0 and O_1 be Hermitian operators on spaces V_0 and V_1 respectively. Then $O_0 \otimes O_1$ is a Hermitian operator on the space $V_0 \otimes V_1$. Furthermore, if O_i has eigenvalues λ_{ij} with associated eigenspaces S_{ij}, then $O_0 \otimes O_1$ has eigenvalues $\lambda'_{jk} = \lambda_{0j}\lambda 1k$. If an eigenvalue $\lambda'_{jk} = \lambda_{0j}\lambda 1k$ is unique, then its associated eigenspaces S'_{jk} is the tensor product of S_{0j} and S_{1k}. In general, the eigenvalues λ'_{jk} need not be distinct. An eigenvalue λ' of $O_0 \otimes O_1$ that is the product of eigenvalues of O_0 and O_1 in multiple ways, $\lambda'_i = \lambda'_{j_1 k_1} = \cdots = \lambda'_{j_m k_m}$, has eigenspace $S = (S_{0j_1} \otimes S_{1k_1}) \oplus \cdots \oplus (S_{0j_m} \otimes S_{1k_m})$.
Any Hermitian operator $Q_1 \otimes Q_2$ on a two-qubit system is said to be composed of single-qubit measurements if Q_q and Q_2 are Hermitian operators on the single-qubit systems. Furthermore, any Hermitian operator of the form $Q \otimes I$ or $I \otimes Q'$ on a two-qubit system is said to be a measurement on a single qubit of the system. More generally, a Hermitian operator of the form

$$I \otimes \cdots \otimes I \otimes Q \otimes I \otimes \cdots \otimes I$$

on an n-qubit system is said to be a single-qubit measurement of the system. Any Hermitian operator of the form $A \otimes I$ on a system $V \otimes W$, where A is a Hermitian operator acting on V is said to be a measurement of subsystem V.

4.4 EPR Paradox and Bell's Theorem

In 1935, Albert Einstein, Boris Podolsky, and Nathan Rose had a thought experiment which involves a pair of photons (EPR pairs) in the state $1/\sqrt{2}(|00\rangle + |11\rangle)$: Imagine a source that generates EPR pairs $1/\sqrt{2}(|00\rangle + |11\rangle)$ and sends the first particle to Alice and to the second to Bob. Alice can use only observables of the form $O \otimes I$ to measure the system, and Bob can use only observables of the form $I \otimes O'$, where O and O' are single-qubit observables.

4.4.1 Setup for Bell's Theorem

Imagine an EPR source that emits pairs of photons whose polarizations are in an entangled state $|\psi\rangle = 1/\sqrt{2}(|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$, where we are using the notation $|\uparrow\rangle$ and $|\rightarrow\rangle$ for photon polarization. We suppose that the two photons travel in opposite directions, each towards a polaroid (polarization filter).

4.4.2 What Quantum Mechanics Predicts

Let O_θ be a single-qubit observable with 1-eigenspace generated by $|v\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and -1-eigenspace generated by $\left|v^\perp\right\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$. Quantum mechanics predicts that measurement of $|\psi\rangle$ with $O_{\theta_1} \otimes O_{\theta_2}$ results in a state with eigenvalue 1 with probability $\cos^2(\theta_1 - \theta_2)$. In other words, the probability that the state ends up in the subspace generated by $\{|v_1\rangle\,|v_2\rangle\,, \left|v_1^\perp\right\rangle \left|v_2^\perp\right\rangle\}$, and not the -1-eigenspace generated by $\{|v_1\rangle \left|v_2^\perp\right\rangle, \left|v_1^\perp\right\rangle |v_2\rangle\}$, is $\cos^2(\theta_1 - \theta_2)$.
If the polaroids are set randomly for a series of EPR pairs emanating from the source, then

- with probability 1/3 the polaroid orientation will be the same and the measurements will agree, and
- with probability 2/3 the polaroid orientation will differ and the measurements will agree with probability 1/4.

Thus, overall, the measurements will agree half the time and disagree half the time.

4.4.3 Special Case of Bell's Theorem: What Any Local Hidden Variable Theory Predicts

Suppose there is some hidden state associated with each photon that determines the result of measuring the photon with a polaroid in each of the three possible settings. We do not know the nature of such it state, but there are only 2^3 binary combinations in which these states can respond to measurement by polaroids in the 3 orientations.

4.4.4 Bell's Inequality

Consider polaroids that can be set at any triple of three distinct angles a, b, and c. If we record the results of repeated measurements at random settings of the polaroids, chosen from the settings above, we an count the number of times that the measurements match for any pair of settings. Let P_{xy} denote the sum of the observed probability that either

- the two photons interact in the same way with both polaroids (either both pass through, or both are absorbed) when the first polaroid is set at angle x and the second at angle y, or
- the two photons interact in the same way with both polaroids when the first polaroid is set at angle y and the second at angle x.

Since whenever the two polaroids are on the same setting, the measurement of the photons will always give the same result $P_{xx} = 1$ for any setting x. We now show that the inequality,

$$P_{ab} + P_{ac} + P_{bc} \geq 1,$$

known as *Bell's inequality*, holds for any local hidden-variable theory and any sequence of settings for each of the polaroids.

5 Quantum State Transformations

Computation on Quantum information takes place through dynamic transformation of quantum systems. In order to understand quantum computation, we must understand which sorts of transformations nature allows and which it does not. The transformations that map the state space of the quantum system to itself are called the transformations of a closed quantum system. The no-cloning restriction is central to both the limitations and the advantages of encoding information in quantum states. All quantum transformations on n-qubit quantum systems can be expressed as a sequence of transformations on single-qubit and two-qubit subsystems.

5.1 Unitary Transformations

Nature does not allow arbitrary transformations of a quantum system. Nature forces these transformation to respect properties connected to quantum measurement and quantum superposition. The transformations must be linear transformations of the vector space associated with the state space so that a state that is a superposition of other states goes to the superposition of their images; more precisely, linearity means that for any quantum transformation U,

$$U(a_1 |\psi_1\rangle + \cdots + a_k |\psi_k\rangle) = a_1 U |\psi_1\rangle + \cdots + a_k U |\psi_k\rangle$$

on any superposition $|\psi\rangle = a_1 |\psi_1\rangle + \cdots + a_k |\psi_k\rangle$. This property holds if U preserves the inner product; for any $|\psi\rangle$ and ϕ, the inner product of their images, $U |\psi\rangle$ and $U |\phi\rangle$, must be the same as the inner product between $|\psi\rangle$ and $|\phi\rangle$:

$$|\phi\rangle U^\dagger U |\psi\rangle = \langle\phi|\psi\rangle \implies U^\dagger U = I \iff U^\dagger = U^{-1}.$$

Therefore, U is said to be unitary. Unitary operators preserve the inner product, they map orthonormal bases to orthonormal bases; and its converse is also true. U is unitary if and only if the set of columns of its matrix representation are orthonormal, so are the rows of U. The product $U_1 U_2$ or tensor product $U_1 \otimes U_2$ of two unitary transformations is again unitary.
In the standard circuit model of quantum computation, all computation is carried out by quantum transformations, with measurement used only at the end to read out the results.

5.1.1 Impossible Transformations: The No-Cloning Principle

Suppose U is a unitary transformation that *clones*, in that $U(|a\rangle |0\rangle) = |a\rangle |a\rangle$ for all quantum states $|a\rangle$. Let $|a\rangle$ and $|b\rangle$ be two orthogonal quantum states. That U clones means $U(|a\rangle |0\rangle) = |a\rangle |a\rangle$ and $U(|b\rangle |0\rangle) = |b\rangle |b\rangle$. Consider $|c\rangle = 1/\sqrt{2}(|a\rangle + |b\rangle)$. By linearity,

$$U(|c\rangle |0\rangle) = 1/\sqrt{2}[U(|a\rangle |0\rangle) + U(|b\rangle |0\rangle)] = 1/\sqrt{2}(|a\rangle |a\rangle + |b\rangle |b\rangle),$$

But if U is a cloning transformation then

$$U(|c\rangle |0\rangle) = |c\rangle |c\rangle = 1/2(|a\rangle |a\rangle + |a\rangle |b\rangle + |b\rangle |a\rangle + |b\rangle |b\rangle),$$

which is not equal to $1/\sqrt{2}(|a\rangle |a\rangle + |b\rangle |b\rangle)$. Thus, there is no unitary operation that can reliably clone all quantum states.

5.2 Some Simple Quantum Gates

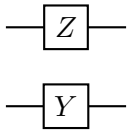
Any quantum state transformation that acts on only a small number of qubits is called a *quantum gate*. Sequences of quantum gates are called *quantum gate arrays* or *quantum circuits*. In the quantum-information-processing literature, gates are mathematical abstractions useful for describing quantum algorithms. Graphical notation, representing series of quantum state transformations acting on various combinations of qubits, is commonly used to describe sequences of transformations and to analyze the resulting algorithms. Simple transformations are graphically represented by appropriately labeled boxes which are connected to form more complex circuits. Each horizontal line corresponds to a qubit. The transformations on the left are performed first, and the processing proceeds from left to right. When we apply an operator U to qubit i of an n-qubit quantum system, we mean that we apply the operator $I \otimes \cdots \otimes I \otimes U \otimes I \otimes \cdots \otimes I$ to the entire system, where I is the single-qubit identity operator, applied to each of the other qubits of the system.

5.2.1 The Pauli Transformations

The Pauli transformations are the most commonly used single-qubit transformations:

$$\begin{aligned}
I &: |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \\
X &: |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\
Y &: -|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \\
Z &: |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.
\end{aligned}$$

where I is the identity transformation, X is negation (the classical NOT operation on $|0\rangle$ and $|1\rangle$ viewed as classical bits), Z changes the relative phase of a superposition in the standard basis, and $Y = ZX$ is a combination of negation and phase change. In graphical notation, these gates are represented by boxes labeled appropriately.



5.2.2 The Hadamard Transformation

The Hadamard transformation is

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|),$$

or

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

which produces an even superposition of $|0\rangle$ and $|1\rangle$ from either of the standard basis elements. Note $HH = I$. In the standard basis, the matrix for the Hadamard transformation is

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

5.2.3 Multiple-Qubit Transformations from Single-Qubit Transformations

Multiple-qubit transformations can be constructed as tensor products of single-qubit transformations which are equivalent to performing the single-qubit transformations on each of the qubits separately in some order. For example, $U \otimes V$ can be obtained by first apply $U \otimes I$ and then $I \otimes V$. Let $|\psi\rangle$ be a two-qubit state and U and V be single-qubit unitary transformations. Then $(U \otimes V)|\psi\rangle$ is entangled if and only if $|\psi\rangle$ is.

5.2.4 The Controlled-not and Other Singly Controlled Gates

The controlled-NOT gate, C_{not}, acts on the standard basis for a two-qubit system, with $|0\rangle$ and $|1\rangle$ viewed as classical bits, as follows: it flips the second bit if the first bit is 1 and leaves it unchanged otherwise. The C_{not} transformation has representation

$$\begin{aligned} C_{not} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ &= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|, \end{aligned}$$

from which it is easy to read off its effect on the standard basis elements:

$$\begin{aligned} C_{not} : |00\rangle &\to |00\rangle, \\ |01\rangle &\to |01\rangle, \\ |10\rangle &\to |11\rangle, \\ |11\rangle &\to |10\rangle. \end{aligned}$$

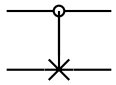
The matrix representation (in the standard basis) for C_{not} is

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

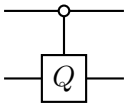
Observe that C_{not} is unitary and is its own inverse. Furthermore, the C_{not} gate cannot be decomposed into a tensor product of two single-qubit transformations.
The importance of the C_{not} gate for quantum computation stems from its ability to change to entanglement between two qubits. For example, it takes the unentangled two-qubit state $1/\sqrt{2}(|0\rangle + |1\rangle)|0\rangle$ to the entangled state $1/\sqrt{2}(|00\rangle + |11\rangle)$:

$$C_{not}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right] = C_{not}\left[\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right] = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Similarly, since it is its own inverse, it can take an entangled state to an unentangled one. The controlled-NOT gate is so common that is has its own graphical notation. The open circle indicates the control bit, the $\times$ indicates negation of the target bit, and the line between them indicates



that the negation is conditional, depending on the value of the control bit. A useful class of two-qubit controlled gates, which generalizes the C_{not} gate, consists of gates that perform a single-qubit transformation Q on the second qubit when the first qubit is $|1\rangle$ and do nothing when it is $|0\rangle$. These controlled gates have graphical representation We use the following shorthand for these



transformations:

$$\bigwedge Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q.$$

The transformation C_{not}, for example, becomes $\bigwedge X$ in this notation. In the standard computational basis, the two-qubit operator $\bigwedge Q$ is represented by the 4×4 matrix

$$\begin{bmatrix} I & 0 \\ 0 & Q \end{bmatrix}.$$

The controlled phase shift $\bigwedge e^{\mathbf{i}\theta}$, where $e^{\mathbf{i}\theta}$ is shorthand for $e^{\mathbf{i}\theta} I$. In the standard basis, the controlled phase shift changes the phase of the second bit if and only if the control bit is one:

$$\bigwedge e^{\mathbf{i}\theta} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{\mathbf{i}\theta}|10\rangle\langle 10| + e^{\mathbf{i}\theta}|11\rangle\langle 11|.$$

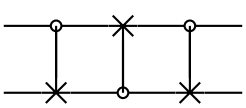
Its effect on the standard basis elements is as follows:

$$\begin{aligned} \bigwedge e^{\mathbf{i}\theta} : |00\rangle &\to |00\rangle, \\ |01\rangle &\to |01\rangle, \\ |10\rangle &\to e^{\mathbf{i}\theta}|10\rangle, \\ |11\rangle &\to e^{\mathbf{i}\theta}|11\rangle, \end{aligned}$$

and it has matrix representation

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{\mathbf{i}\theta} & 0 \\ 0 & 0 & 0 & e^{\mathbf{i}\theta} \end{bmatrix}.$$

Graphical icons can be combined into quantum circuits. The following circuit, for instance, swaps the value of the two bits. In other words, this *swap circuit* take



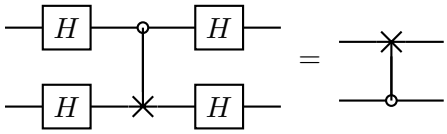
$$
\begin{aligned}
|00\rangle &\mapsto |00\rangle\,, \\
|01\rangle &\mapsto |10\rangle\,, \\
|10\rangle &\mapsto |01\rangle\,, \\
|11\rangle &\mapsto |11\rangle\,,
\end{aligned}
$$

and $|\psi\rangle\,|\phi\rangle \mapsto |\phi\rangle\,|\psi\rangle$ for all single-qubit states $|\psi\rangle$ and $|\phi\rangle$.

1. Phases in Specifications of Transformations. A unitary transformation on the complex vector space is completely determined by its action on a basis. The unitary transformation is not completely determined by specifying what sates the states corresponding to basis states are sent to, a subtle distinction.
2. Basis Dependence of the Notion of Control. The notion of the *control bit* and the *target bit* is a carryover from the classical gate and should not be taken too literally. in the standard basis, the C_{not} operator behaves exactly as the classical gate does on classical bits. However, one should not conclude that the *control bit* is never changed. When the input qubits are not one of the standard basis elements, the effect of the controlled gate can be somewhat counterintuitive. For example, consider C_{not} gate in the Hadamard basis $\{|+\rangle\,, |-\rangle\}$:

   $$
   \begin{aligned}
   C_{not}: |++\rangle &\to |++\rangle\,, \\
   |+-\rangle &\to |--\rangle\,, \\
   |-+\rangle &\to |-+\rangle\,, \\
   |--\rangle &\to |+-\rangle\,.
   \end{aligned}
   $$

   In the Hadamard basis, it is the state of the second qubit that remains unchanged, and the state of the first qubit that is flipped depending on the state of the second bit. Thus, in this basis the sense of which bit is the *control bit* and which the *target bit* has been reversed.
   A related fact, which we will use in constructing algorithms and in quantum error correction, is that the following two circuits are equivalent:

3. Reading circuit diagrams. The graphical representation of quantum circuits can be misleading if one is not careful to interpret it properly. In particular, one cannot determine the effect the transformation has on the input qubits, even if they are all in standard basis states, by simply looking at the line in the diagram corresponding to that qubit.

5.3 Applications of Simple Gates

Dense coding uses one quantum bit together with a shared EPR pair to encode and transmit two classical bits. Since EPR pairs can be distributed ahead of time, only one qubit needs to be physically transmitted to communicate two bits of information. Teleportation is the opposite of dense coding in that it uses two classical bits to transmit the state of a single qubit. The key to both dense coding and teleportation is the use of entangled particles. The initial setup is the same for both processes. Alice and Bob wish to communicate. Each is sent one of the entangled particles making up an EPR pair

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Suppose Alice is sent the first particle, and Bob the second:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0_A\rangle\,|0_B\rangle + |1_A\rangle\,|1_B\rangle).$$

Alice can perform transformations only on her particle, and Bob can perform transformations only on his, until Alice sends Bob her particle or vice versa. In other words, until a particle is transmitted between them, Alice can perform transformations only of the form $Q \otimes I$ on the EPR pair, where Q is a single-qubit transformation, and Bob transformations only of the form $I \otimes Q$. More generally, for $K = 2^k$, let $I^{(K)}$ be the $2^k \times 2^k$ identity matrix. If Alice has n qubits and Bob has m qubits, then Alice can perform transformations only of the form $U \otimes I^{(M)}$, where U is an n-qubit transformation, and Bob can perform transformations only of the form $I^{(N)} \otimes U$.

5.3.1 Dense Coding

- Alice. Alice wishes to transmit the state of two classical bits encoding one of the numbers 0 through 3. Depending on this number, Alice performs one of the Pauli transformations $\{I, X, Y, Z\}$ on her qubit of the entangled pair $|\psi_0\rangle$. The resulting state is shown in the following table.

Value	Transformation	New state
0	$\|\psi_0\rangle = (I \otimes I)\,\|\psi_0\rangle$	$1/\sqrt{2}(\|00\rangle + \|11\rangle)$
1	$\|\psi_1\rangle = (X \otimes I)\,\|\psi_0\rangle$	$1/\sqrt{2}(\|10\rangle + \|01\rangle)$
2	$\|\psi_2\rangle = (Z \otimes I)\,\|\psi_0\rangle$	$1/\sqrt{2}(\|00\rangle - \|11\rangle)$
3	$\|\psi_3\rangle = (Y \otimes I)\,\|\psi_0\rangle$	$1/\sqrt{2}(-\|10\rangle + \|01\rangle)$

- Bob. To decode the information, Bernsteinb applies a controlled-NOT to the two qubits of the entangled pair and then applies the Hadamard transformation H to the first qubit:

$$\begin{bmatrix} 1/\sqrt{2}(|00\rangle + |11\rangle) \\ 1/\sqrt{2}(|10\rangle + |01\rangle) \\ 1/\sqrt{2}(|00\rangle - |11\rangle) \\ 1/\sqrt{2}(-|10\rangle + |01\rangle) \end{bmatrix} \overset{C_{not}}{\rightarrow} \begin{bmatrix} 1/\sqrt{2}(|00\rangle + |10\rangle) \\ 1/\sqrt{2}(|11\rangle + |01\rangle) \\ 1/\sqrt{2}(|00\rangle - |10\rangle) \\ 1/\sqrt{2}(-|11\rangle + |01\rangle) \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2}(|0\rangle + |1\rangle) \otimes |0\rangle \\ 1/\sqrt{2}(|1\rangle + |0\rangle) \otimes |1\rangle \\ 1/\sqrt{2}(|0\rangle - |1\rangle) \otimes |0\rangle \\ 1/\sqrt{2}(-|1\rangle + |0\rangle) \otimes |1\rangle \end{bmatrix} \overset{H\otimes I}{\rightarrow} \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix}.$$

  Bob then measures the two qubits in the standard basis to obtain the two-bit binary encoding of the number Alice wished to send.

5.3.2 Quantum Teleportation

The objective of teleportation is to transmit enough information, using only classical bits, about the quantum state of a particle that a receiver can reconstruct the exact quantum state. Since the no-cloning principle of quantum mechanics means that a quantum state cannot be copied, the quantum state of the original particle cannot be preserved. It is this property – that the original state at the source must be destroyed in the course of creating the state at the target – that gives quantum teleportation its name.

- Alice has a qubit whose state $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$ she does not know. She wants to send this state to Bob through classical channels. As in the setup for the dense coding application, Alice and Bob each possess one qubit of an entangled pair

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

State	Bits received	Decoding
$a\|0\rangle + b\|1\rangle$	00	I
$a\|1\rangle + b\|1\rangle$	01	X
$a\|0\rangle - b\|1\rangle$	10	Z
$a\|1\rangle - b\|0\rangle$	11	Y

The starting state is the three-qubit quantum state

$$\begin{aligned}|\phi\rangle \otimes |\psi_0\rangle &= \frac{1}{\sqrt{2}}[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)] \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle).\end{aligned}$$

Alice controls the first two qubits and Bob controls the last one. Alice applies the decoding step used by Bob in the dense coding scenario to the combined state of the qubit $|\phi\rangle$ to be transmitted and her half of the entangled pair. In other words, Alice now applies $C_{not} \otimes I$ followed by $H \otimes I \otimes I$ to this state to obtain

$$\begin{aligned}&(H \otimes I \otimes I)(C_{not} \otimes I)(|\phi\rangle \otimes |\psi_0\rangle) \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\ &= \frac{1}{2}[a(|000\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)] \\ &= \frac{1}{2}[|00\rangle (a|0\rangle + b|1\rangle) + |01\rangle (a|1\rangle + b|0\rangle) + |10\rangle (a|0\rangle - b|1\rangle) + |11\rangle (a|1\rangle - b|0\rangle)].\end{aligned}$$

Alice measures the first two qubits and obtains one of the four standard basis state $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ with equal probability. Depending on the result of her measurement, the quantum state of Bob's qubit is projected to $a|0\rangle+b|1\rangle$, $a|1\rangle+b|0\rangle$, $a|0\rangle-b|1\rangle$, or $a|1\rangle-b|0\rangle$. Alice sends the result of her measurement as two classical bits to Bob.
After these transformations, crucial information about the original state $|\phi\rangle$ is contained in Bob's qubit. There now nothing Alice can do on her own to reconstruct the original state of her qubit. In fact, the no-cloning principle implies that at any given time, only one of Alice or Bob can reconstruct the original quantum state.

- Bob. When Bob receives the two classical bits from Alice, he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit. Bob can reconstruct the original state of Alice's qubit, $|\phi\rangle$, by applying the appropriate decoding transformation to his qubit, originally part of the entangled pair. The following table show the state of Bob's qubit before the decoding has taken place and the decoding operator Bob should use depending on the value of the bits he received from Alice. After decoding, Bob's qubit will be in the quantum state, $a|0\rangle+b|1\rangle$, in which Alice's qubit started. This decoding step is the encoding step of dense coding, and the encoding step was the decoding step of dense coding, so teleportation and dense coding are in some sense inverse of each other.

5.4 Realizing Unitary Transformation as Quantum Circuits

Any arbitrary unitary transformations can be implemented from a set of primitive transformations which includes the two-qubit C_{not} gate, in addition to three kinds of single-qubit gates.

5.4.1 Decomposition of Single-Qubit Transformations

This section show that all single-qubit transformations can be written as a combination of three types of transformations, phase shift $K(\delta)$, rotations $R(\beta)$, and phase rotations $T(\alpha)$:

$$K(\delta) = e^{\mathbf{i}\delta} \qquad \text{A phase shift by } \delta,$$
$$R(\beta) = \begin{bmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{bmatrix} \qquad \text{A rotation by } \beta,$$
$$T(\alpha) = \begin{bmatrix} e^{\mathbf{i}\alpha} & 0 \\ 0 & e^{-\mathbf{i}\alpha} \end{bmatrix} \qquad \text{A phase rotation by } \alpha.$$

Note that

$$K(\delta_1+\delta_2) = K(\delta_1)K(\delta_2), R(\beta_1+\beta_2) = R(\beta_1)R(\beta_2), T(\alpha_1+\alpha_2) = T(\alpha_1)T(\alpha_2),$$

and that the operator K commutes with K, T, and R. Note that $K(\delta)$ performs a global phase change, and thus is equivalent to the identity on the single-qubit system. The transformation $R(\alpha)$ and $T(\alpha)$ are rotations by 2α about the y- and z-axis of the Bloch sphere respectively.
Any single-qubit unitary transformation Q can be decomposed into a sequence of transformations of the form $Q = K(\delta)T(\alpha)R(\beta)T(\gamma)$. Since the $K(\delta)$ is a global phase shift with no physical effect, the space of all single-qubit transformations has only three real dimensions. Given the transformation

$$Q = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix},$$

it follows immediately from the unitary condition $QQ^\dagger = I$ that $|u_{00}|^2+|u_{01}|^2= 1$, $u_{00}\overline{u_{10}}+u_{01}\overline{u_{11}} = 0$, and $|u_{11}|^2+|u_{10}|^2= 1$. A short calculation gives $|u_{00}|= |u_{11}|$ and $|u_{01}|= |u_{10}|$. We can write Q as

$$Q = \begin{bmatrix} e^{\mathbf{i}\theta_{00}}\cos\beta & e^{\mathbf{i}\theta_{01}}\sin\beta \\ -e^{\mathbf{i}\theta_{10}}\sin\beta & e^{\mathbf{i}\theta_{11}}\cos\beta \end{bmatrix}.$$

Furthermore, the phases are not independent: $u_{10}\overline{u_{00}}+u_{11}\overline{u_{01}} = 0$ implies that $\theta_{10}-\theta_{00} = \theta_{11}-\theta_{01}$. Since

$$K(\delta)T(\alpha)R(\beta)T(\gamma) = \begin{bmatrix} e^{\mathbf{i}(\delta+\alpha+\gamma)}\cos\beta & e^{\mathbf{i}(\delta+\alpha-\gamma)}\sin\beta \\ -e^{\mathbf{i}(\delta-\alpha+\gamma)}\sin\beta & e^{\mathbf{i}(\delta-\alpha-\gamma)}\cos\beta \end{bmatrix},$$

we can find δ, α, γ for a given Q by solving the equations

$$\delta+\alpha+\gamma = \theta_{00}, \delta+\alpha-\gamma = \theta_{01}, \delta-\alpha+\gamma = \theta_{10}.$$

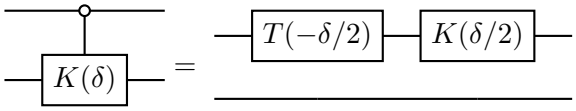
Using $\theta_{11} = \theta_{10}-\theta_{00}+\theta_{01}$, it is easy to see that this solution also satisfies $\delta-\alpha-\gamma = \theta_{11}$.

5.4.2 Singly-Controlled Single-Qubit Transformations

Let $Q = K(\delta)T(\alpha)R(\beta)T(\gamma)$ be an arbitrary single-qubit unitary transformation. The controlled gate $\bigwedge Q$ can be implemented by first constructing $\bigwedge K(\delta)$ and implementing $\bigwedge Q'$ for $Q' = T(\alpha)R(\beta)T(\gamma)$. Then $\bigwedge Q = (\bigwedge K(\delta))(\bigwedge Q')$. The conditional phase shift can be implemented by primitive single-qubit operations:

$$\begin{aligned} \bigwedge K(\delta) &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes K(\delta) \\ &= |0\rangle\langle 0| \otimes I + e^{\mathbf{i}\delta}|1\rangle\langle 1| \otimes I \\ &= (K(\delta/2)T(-\delta/2)) \otimes I. \end{aligned}$$

Graphically, the implementation look like



(5.1)

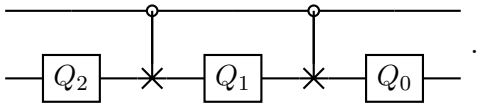
The reason that transformations on the first qubit suffice is that a phase shift affects the whole quantum state, not just a single qubit. In particular, $|x\rangle \otimes a\,|y\rangle = a\,|x\rangle \otimes |y\rangle$. Implementing $\bigwedge Q'$ is slightly more involved. For $Q' = T(\alpha)R(\beta)T(\gamma)$, define the following transformations:

$$Q_0 = T(\alpha)R(\beta/2), Q_1 = R(-\beta/2)T\left(\frac{-\gamma-\alpha}{2}\right), Q_2 = T\left(\frac{\gamma-\alpha}{2}\right).$$

The claim is that $\bigwedge Q'$ can be defined as

$$\bigwedge Q' = (I \otimes Q_0)C_{not}(I \otimes Q_1)C_{not}(I \otimes Q_2),$$

or graphically



.

It is easy to see that this circuit performs the following transformation:

$$|0\rangle \otimes |x\rangle \to |0\rangle \otimes Q_0Q_1Q_2\,|x\rangle\,,$$
$$|1\rangle \otimes |x\rangle \to |1\rangle \otimes Q_0XQ_1XQ_2\,|x\rangle\,.$$

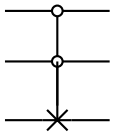
Using $R(\beta)R(-\beta) = I$ and $T(\alpha)T(\gamma) = T(\alpha+\gamma)$, the property $Q_0Q_1Q_2 = I$ follows immediately from the definition of the Q_i. To show that $Q_0XQ_1XQ_2 = Q'$, use $XR(\beta)X = R(-\beta)$ and $XT(\alpha)X = T(-\alpha)$. Then

$$Q_0XQ_1XQ_2 = T(\alpha)R(\beta/2)(XR(-\beta/2)X)\left[XT\left(-\frac{\gamma+\alpha}{2}\right)X\right]T\left(\frac{\gamma-\alpha}{2}\right) = Q'.$$

In this way, we can realize a version of an arbitrary single-qubit transformation controlled by a single qubit.

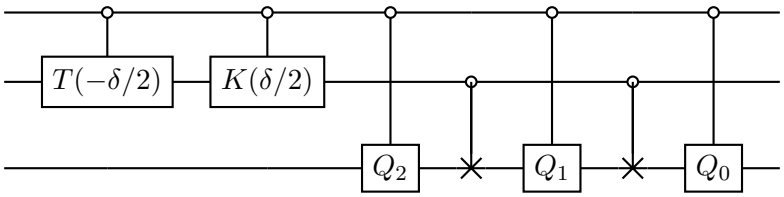
5.4.3 Multiply-Controlled Single-Qubit Transformations

Let $\bigwedge_k Q$ be the $(k+1)$-qubit transformation that applies Q to qubit 0 when qubits 1 through k are all 1. For example, the *controlled-controlled-NOT gate* or *Toffoli gate* $\bigwedge_2 X$, which negates the last bit of three if and only if the first two are both 1, has the following graphical representations.

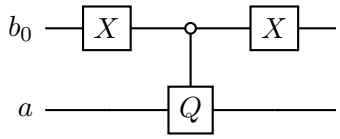


The subscript 2 is the notation $\bigwedge_2 X$ indicates that there are two control bits. We are the C_{not} gate as both $\bigwedge X$ and $\bigwedge_1 X$. To implement $\bigwedge_2 Q$, a three-qubit gate that applies Q controlled by two

qubits, start by replacing each of Q_0, Q_1, and Q_2 in the previous construction with a single-qubit controlled version.



This circuit can be expanded, as in the previous section, into single-qubit and controlled-NOT gates, for a total of twenty five single-qubit gates and 12 controlled-NOT gates. Repeating this process leads to circuits for controlled versions of single-qubit transformations with k control bits, $\bigwedge_k Q$, with 5^k single-qubit transformations and $1/2(5^k - 1)$ controlled-NOT gates.
All of the controlled gates seen so far are executed when the control bits are 1. To implement a singly controlled gate that is executed when the control bit is 0, the control bit can be negated, as in



For any length k bit-string s, temporarily negating the appropriate control qubits in this way, enables the realization of a controlled gate that applies Q to qubit 0 exactly when the other k qubits are in the pattern s. More precisely, let $|s\rangle$ be the k qubit standard basis vector labeled with bit-string s. This construction implements the $(k+1)$-qubit controlled gate that applies the single-qubit transformation Q to qubit 0 when qubits 1 through k are in a different basis state. Such constructions can be further generalized to $(k+1)$-qubit controlled gates that apply the single-qubit transformation Q to qubit i when the other qubits are in a specific basis state and do nothing when they are in a different basis state. In other words, this transformation applies Q to the two-dimensional subspace spanned by the two basis vectors $|x_k \dots x_i \dots x_0\rangle$ and $|x_k \dots \hat{x}_i \dots x_0\rangle$, where $\hat{x}_i = x_i \oplus 1$, that differ only in bit i, and it leaves the orthogonal subspace invariant.
Section 5.4.4 uses such gates to exhibit an explicit implementation of an arbitrary unitary transformation. The construction of section 5.4.4 uses two different transformations related to a pair consisting of a k-bit bit-string s and a single-qubit transformation Q: the first applies Q to the ith qubit with the standard ordering of the basis $\{|0\rangle, |1\rangle\}$ when the other k qubits are in state $|s\rangle$, and the second applies Q to the ith qubit with the basis in the other order. In other words, this second transformation applies XQX to qubit i when the other qubits are in state $|s\rangle$. We use the notation $\bigwedge_x^i Q$, where x is a $(k+1)$-bit bit-string such that $x_k \dots x_{i+1} x_{i-1} \dots x_0 = s_{k-1} \dots s_0$, to represent both of these transformations depending on the value of x_i. When x_i is 0, the single-qubit transformation Q is applied. When x_i is 1, the transformation XQX is applied. When i is specified, the notation $\hat{x}$ means that the ith bit of a bit-string x has been flipped: $\hat{x} = x \oplus 2^i$. For any single-qubit transformation Q, the transformation $\bigwedge_{\hat{x}}^i Q = \hat{x}^i \hat{Q}$, where $\hat{Q} = XQX$. Geometrically $\bigwedge_x^i Q$ is a rotation in the two-dimensional complex subspace spanned by standard basis vectors $|x\rangle$ and $|\hat{x}\rangle$.

5.4.4 General Unitary Transformations

This section presents a symmetric way to implement an arbitrary unitary transformation on the 2^n-dimensional vector space associated with the state space of an n-qubit system. The intuitive idea

behind the construction is that any unitary transformation is simply a rotation of the 2^n-dimensional complex vector space underlying the n-qubit quantum state space, and that any rotation can be obtained by a sequence of rotations in two-dimensional subspaces.

Let $N = 2^n$. This section writes all matrices in the standard basis, but with a *nonstandard ordering* $\{|x_0\rangle, \ldots, |x_{N-1}\rangle$ such that successive basis elements differ by only one bit. Such a sequence of binary numbers is called a *Gray code*. Any Gray code will do. For $0 \leq i \leq N-2$, let j_i be the bit on which $|x_i\rangle$ and $|x_{i+1}\rangle$ differ, and B_i be the shared pattern of all the other bits in $|x_i\rangle$ and $|x_{i+1}\rangle$. The next few paragraphs show how to realize an arbitrary unitary operator U as a sequence of multiply controlled single-qubit operators $\bigwedge_{x_i}^{j_i} Q$ that perform a series of rotations, each in a two-dimensional subspace spanned by successive basis elements.

Consider transformations U_m of the form

$$U_m = \begin{bmatrix} I^{(m)} & 0 \\ 0 & V_{N-m} \end{bmatrix},$$

where $I^{(m)}$ is the $m \times m$ identity matrix and V_{N-m} is an $(N-m) \times (N-m)$-unitary matrix with $0 \leq m \leq N-2$. We wish to show that given any $(N \times N)$-matrix U_{m-1}, $0 < m \leq N-2$, of this form there exist operators C_m, the product of multiply controlled single-qubit operators, and a U_m, now with a larger identity component $I^{(m)}$, such that $U_{m-1} = C_m U_m$. Then, taking $V_N = U$, the unitary operator U can be written as

$$U = U_0 = C_1 \cdots C_{N-2} U_{N-2}.$$

The transformation U_{N-2} has the form

$$U_{N-2} = \begin{bmatrix} I^{(N-2)} & 0 \\ 0 & V_2 \end{bmatrix},$$

which is simply the operation $\bigwedge_x^j V_2$ where $x = x_{N-2}$ and, using the Gray code condition, $j = j_{N-2}$ is the bit in which the last two basis vectors $|x_{N-2}\rangle$ and $|x_{N-1}\rangle$ differ. So once we show how to implement the C_m using multiply controlled single-qubit operators, we will have succeeded in showing that any unitary operator can be expressed in terms of such operators, and thus can be implemented using only C_{not}, $K(\delta)$, $R(\beta)$, and $T(\alpha)$.

The basis vector $|x_m\rangle$ is the first basis vector on which U_{m-1} acts non-trivially. Write

$$|v_m\rangle = U_{m-1} |x_m\rangle = a_m |x_m\rangle + \cdots + a_N |x_N\rangle .$$

We may assume that a_N is real, since we can multiply U_{m-1} by a global phase. If we can find a unitary transformation W_m, composed only of multiply controlled single-qubit transformations, that takes $|v_m\rangle$ to $|x_m\rangle$ and does not affect any of the first m elements of the basis, $W_m U_{m-1}$ would have the desired form, so we would take $U_m = W_m U_{m-1}$ and $C_m = W_m^{-1}$. To define W_m, begin by rewriting the coefficients of the last two components of $|v_m\rangle$:

$$|v_m\rangle = a_m |x_m\rangle + \cdots + c_{N-1} \cos(\theta_{N-1}) e^{\mathbf{i}\phi_{N-1}} |x_{N-1}\rangle + c_{N-1} \sin(\theta_{N-1}) |x_N\rangle ,$$

where $a_{N-1} = |a_{N-1}| e^{\mathbf{i}\theta_{N-1}}$, $c_{N-1} = \sqrt{(}|a_{N-1}|^2 + |a_N|^2)$, $\cos(\theta_{N-1}) = |a_{N-1}/c_{N-1}$, $\sin(\theta_{N-1}) = |a_N|/c_{N-1}$. Then

$$\bigwedge_{x_{N-1}}^{j_{N-1}} R(\theta_{N-1}) \bigwedge_{x_{N-1}}^{j_{N-1}} K(-\phi_{N-1})$$

takes $|v_m\rangle$ to $a_m|v_m\rangle + \cdots + a'_{N-1}|x_{N-1}\rangle$, where $a'_{N-1} = c_{N-1}$, since $\bigwedge_{x_{N-1}}^{j_{N-1}} K(-\phi_{N-1})$ cancels the $e^{\mathbf{i}\phi_{N-1}}$ factor, and $\bigwedge_{x_{N-1}}^{j_{N-1}} R(\theta_{N-1})$ rotates so that all of the amplitude that was in $|x_N\rangle$ is now in $|x_{N-1}\rangle$. None of the other basis vectors are affected because the controlled part of the operators ensure that only basis vectors with bits in pattern B_{N-1} are affected. To obtain the rest of W_m, we iterate this procedure over all pairs of coordinates $\{a_{N-2}, a'_{N-1}$ through $\{a_m, a'_{m+1}\}$ to obtain the operator

$$W_m = \bigwedge_{x_m}^{j_m} R(\theta_m) \bigwedge_{x_m}^{j_m} K(-\phi_m) \cdots \bigwedge_{x_{N-1}}^{j_{N-1}} R(\theta_{N-1}) \bigwedge_{x_{N-1}}^{j_{N-1}} K(-\phi_{N-1}),$$

which takes $|v_m\rangle$ to $a'_m|x_m\rangle$, where $a_i = |a_i|e^{\mathbf{i}\phi_i}$, $a'_i = c_i = \sqrt{|a_i|^2+|a_{i+1}|^2}$, $\cos(\theta_i) = |a_i|/c_i$, $\sin(\theta_i) = |a'_{i+1}|/c_i$. The coefficient $a'_m = 1$, since the image of $|v_m\rangle$ must be a unit vector, and the final $\bigwedge_{x_m}^{j_m} K(-\phi_m)$ ensures that it is a positive real.

5.5 A Universally Approximating Set of Gates

All unitary transformations can be realized as a sequence of single-qubit transformations and controlled-NOT gates. From a practical point of view, we would prefer to deal with a finite set of gates. For any finite set of gates there are unitary transformations that cannot be realized as a combination of these gates, but there are finite sets of gates that can approximate any unitary transformation to arbitrary accuracy. Furthermore, for any desired level of accuracy 2^{-d}, this approximation can be done efficiently; there is a polynomial $p(d)$ such that any single-qubit unitary transformation can be approximated to within 2^{-d} by a sequence of no more than $p(d)$ gates from the finite set (solovay-Kitaev theorem).
since any unitary transformation can be realized using single-qubit and C_{not} gates, it suffices to find a finite set of gates that can approximate all single-qubit transformations. Consider the set consisting of the Hadamard gate H, the phase gate $P_{\pi/2}$, the $\pi/8$-gate $P_{\pi/4}$, and the C_{not} gate where

$$P_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathbf{i}\pi/2} \end{bmatrix} = |0\rangle\langle 0| + \mathbf{i}\,|1\rangle\langle 1|$$

and

$$P_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathbf{i}\pi/4} \end{bmatrix} = |0\rangle\langle 0| + e^{\mathbf{i}\pi/4}\,|1\rangle\langle 1|\,.$$

Recall that the single-qubit operator $T(\theta) = e^{\mathbf{i}\theta}|0\rangle\langle 0| + e^{-\mathbf{i}\theta}|1\rangle\langle 1|$. The $\pi/8$-gate $P_{\pi/4}$ got its name because, up to a global phase, it acts in the same way as the gate $T(-\pi/8)$,

$$P_{\pi/4} = e^{\mathbf{i}\pi/8} T(-\pi/8).$$

A rotation R is a rational rotation if, for some integer m, $R^m = I$. If no such m exists, then R is an irrational rotation. It may seem surprising that a set of gates consisting only of rational rotation on the Bloch sphere can approximate all single-qubit transformations. The gate $P_{\pi/4}$ is a rotation by $\pi/4$ about the z-axis of the Bloch sphere. The transformation $S = HP_{\pi/4}H$ is a rotation by $\pi/4$ is an irrational rotation. Since V is irrational, any rotation W about the same axis can be approximated to within arbitrary precision 2^{-d} by some power of V. Recall that any single-qubit transformation may be achieved (up to global phase) by combining rotations about the y- and z-axes: for every single-qubit operation W there exist angles α, β, γ, and δ such that

$$W = K(\delta)T(\alpha)R(\beta)T(\gamma),$$

where $T(\alpha)$ rotates by angle α about the z-axis and $R(\alpha)$ rotates by angle α about the y-axis. The set of rotations about any two distinct axes can achieve arbitrary single-qubit transformations. Since HVH has a different axis from V, the two transformations H and V generate all single-qubit operators. Other universally approximating finite sets, with varying advantages and disadvantages, exit.

5.6 The Standard Circuit Model

A *circuit model* for quantum computation describes all computations in terms of a circuit composed of simple gates followed by a sequence of measurements. The simple gates are drawn either from a universal set of simple gates or a universally approximating set of quantum gates. The *standard circuit model* for quantum computation takes as its gate set the C_{not} gate together with all single-qubit transformations, and it takes as its set of measurements single-qubit measurements in the standard basis. So all computations in the standard model consist of a sequence of single-qubit and C_{not} gates followed by a sequence of single-qubit measurements in the standard basis.

6 Quantum Versions of Classical Computations

For any classical computation, a quantum circuit that can perform the same computation with comparable efficiency. The construction of quantum analogs to all classical computations relies on a classical result that constructs a reversible analog to any classical computation. Given a classical reversible circuit composed of reversible Boolean logic gates, simple substitution of the analogous quantum gates for the reversible gates gives the desired quantum circuit.

6.1 From Reversible Classical Computations to Quantum Computations

Any sequence of quantum transforms effects a unitary transformation U on the quantum system. As long as no measurements are made, the initial quantum state of the system prior to a computation can be recovered from the final quantum state $|\psi\rangle$ by running $U^{-1} = U^\dagger$ on $|\psi\rangle$. Thus, any quantum computation is *reversible* prior to measurement in the sense that the input can always be computed from the output.

Classical computations are not in general reversible: it is not usually possible to compute the input from the output, e.g., AND, OR, and NAND are not reversible except for NOT. Every classical computation does, however, have a classical reversible analog that takes only slightly more computational resources.

Any classical reversible computation with n input and n output bits simply permutes the $N = 2^n$ bit strings. Thus, for any such classical reversible computation there is a permutation $\pi : \mathbb{Z}_N \to \mathbb{Z}_N$ sending an input bit string to its output bit string. This permutation can be used to define a quantum transformation

$$U_\pi : \sum_{x=0}^{N-1} a_x |x\rangle \mapsto \sum_{x=0}^{N-1} a_x |\pi(x)\rangle ,$$

that behaves on the standard basis vectors, viewed as classical bit strings, exactly as π did.

Any classical computation on n input and m output bits defines function

$$\begin{aligned} f : \mathbb{Z}_N &\to \mathbb{Z}_M \\ x &\mapsto f(x) \end{aligned}$$

mapping the $N = 2^n$ input bit strings to the $M = 2^m$ output bit strings. Such a function can be extended in a canonical way to a reversible function π_f acting on $n + m$ bits partitioned into two registers, the n-bit input register and the m-bit output register:

$$\begin{aligned} \pi_f : \mathbb{Z}_L &\to \mathbb{Z}_L \\ (x, y) &\mapsto (x, y \oplus f(x)), \end{aligned}$$

where $\oplus$ denotes the bitwise exclusive-OR. The function π_f acts on the $L = 2^{n+m}$ bit strings, each made up of an n-bit bit string x and an m-bit bit string y. For $y = 0$, the function π acts like f, except that the output appears in the output register and the input register retains the input. Since π_f is reversible, there is a corresponding unitary transformation $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$. Graphically the transformation U_f is depicted as While most unitary operators do not have an efficient implementation, U_f has an efficient implementation as long as there is a classical circuit that computes f efficiently. The medtho for constructing an efficient implementation of U_f from an efficient classical circuit for f has two parts:

1. Construct an efficient reversible classical circuit that computes f.
2. Substitute qauntum gates for each of the reversible gates that make up the reversible classical circuit.

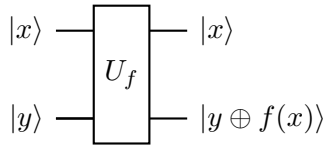


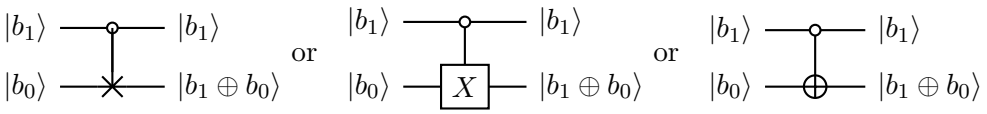
Figure 1: U_f

6.1.1 Reversible and Quantum Versions of Simple Classical Gates

Quantum versions of the Boolean logic gates NOT, XOR, AND, and NAND act like the reversible gates on elements of the standard basis. Their action on other input states is prescribed by the linearity of quantum operations; the action of a gate on a superposition is the linaer combination of the action of the gate on the standard basis elements making up the superposition. In this way, the behavior of a reversible gate fully defines the behavior of its quantum analog, and vice versa.
Let b_1 and b_0 be two binary variables, variables taking on only values 0 or 1. We define the following quantum gates:

NOT Reversible. We use X to refer to both the classical reversible gate and the single-qubit operator $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, which performs a classical NOT operation on classical bits encoded as the standard basis elements.

XOR The controlled negation performed by the $C_{not} = \bigwedge_1 X$ gate amounts to an XOR operation on its input values. It retains the value of the first bit b_1, and replaces the value of the bit b_0 with the XOR of the two values. The quantum version hehaves like the reversible version on the standard basis vectors.



AND Not reversible with only two bits. The three-bit controlled-controlled-NOT gate, or Toffoli gate, $T = \bigwedge_2 X$ can be used to perform a reversible AND operation.

$$T|b_1, b_0, 0\rangle = |b_1, b_0, b_1 \wedge b_0\rangle,$$
$$T|b_1, b_0, 1\rangle = |b_1, b_0, 1 \oplus b_1 \wedge b_0\rangle,$$

where $\wedge$ is notation for the classical AND of the two bit values.

By varying the values of input bits, the Toffoli gate T can be used to construct a complete set of Boolean connectives. Thus, any combinatorial circuit can be constructed from Toffoli gates alone: The Toffoli gate computes NOT, AND, XOR, and NAND in the following way:

$$T|1, 1, x\rangle = |1, 1, \neg x\rangle$$
$$T|x, y, 0\rangle = |x, y, x \wedge y\rangle$$
$$T|1, x, y\rangle = |1, x, x \oplus y\rangle$$
$$T|x, y, 1\rangle = |x, y, \neg(x \wedge y)\rangle.$$

where $\neg$ indicates the classical NOT acting on the bit value.
An alternative to the Toffoli gate, the Fredkin gate F, acts as a controlled *swap*:

$$F = \bigwedge_1 S,$$

where S is the two-bit swap operation

$$S : |xy\rangle \mapsto |yx\rangle .$$

The Fredkin gate F, like the Toffoli gate T, can implement a complete set of classical Boolean operators:

$$\begin{aligned} F\,|x, 0, 1\rangle &= |x, x, \neg x\rangle \\ F\,|x, y, 1\rangle &= |x, y \vee x, y \vee \neg x\rangle \\ F\,|x, 0, y\rangle &= |x, y \wedge x, y \wedge \neg x\rangle , \end{aligned}$$

where $\vee$ is the notation for the classical OR of the two bit values. As the equations for the Toffoli gate illustrate, the operations C_{not} and X can be implemented by Toffoli gates with the addition of one or two bits permanently set to 1. Figure 2 implements a one-bit full adder using Toffoli and controlled-NOT gates, where x and y are the data bits, s is their sum (modulo 2), c is the incoming carry bit, and c' is the new carry bit, Several one-bit adders can be strung together to achieve full n-bit addition.

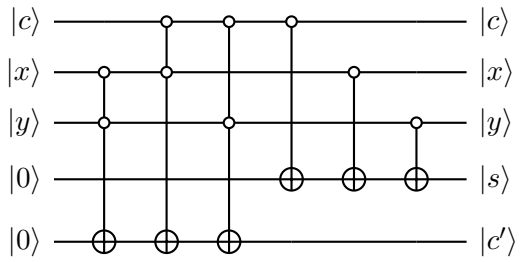


Figure 2: One-bit full adder.

6.2 Reversible Implementations of Classical Circuits

This section develops systematic ways to turn arbitrary classical Boolean circuits into reversible classical circuits of comparable computational efficiency in terms of the number of bits and the number of gates. The resulting reversible circuits are composed entirely of Toffoli and negation gates. A quantum circuit with the same efficiency as the classical reversible circuit is obtained by the trivial substituion of quantum Toffoli and X gates for classical Toffoli and negation gates.

6.2.1 A Naive Reversible Implementation

We consider a classical machine that consists of a register of bits and a processing unit. The processing unit performs simple Boolean operations or gates on one or two of the bits in the register at a time and stores the result in one of the register's bits. We assume that, for a given size input, the sequence of operations and their order of execution are fixed and do not depend on the input data or on other external control. In analogy with quantum circuits, we draw bits of the register as horizontal lines.

An arbitrary Bollean circuit can be transformed into a sequence of operations on a large enough register to hold input, output, and intermediate bits. The space complexity of a circuit is the size of the register. Figure 3 illustrates how the circuit can be made reversible by assigning the results of each operation to a new bit.

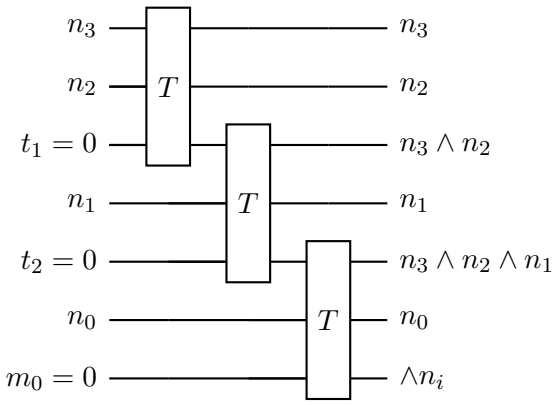


Figure 3: Reversible classical circuit for four-bit conjunction.

Reversible computaiotns cannot reclaim space through a simple *reset* operation. They can, however, *uncompute* any bit set during the course of a reversible computation by reversing the part of the computation that computed the bit. We can reduce the number of qubits needed by uncomputing them and reusing them in the course of the algorithm. The method of uncomputing bits by performing all of the steps in reverse order, except those giving the output, works for any classical Boolean subcircuit.

6.2.2 A General Construction

We show that any classical circuit using t gates and s bits, has a reversible counterpart using only $O(t^{1+\epsilon})$ gates and $O(s \log t)$ bits. For $t \gg s$, this construction uses significantly less space than the $(s + t)$ space of the naive approach.
Let C be a classical circuit, composed of AND and NOT gates, that uses no more than t gates and s bits. The circuit C can be partitioned in time into $r = \lceil t/s \rceil$ subcircuits each containing s or fewer consecutive gates $C = C_1 C_2 \cdots C_r$. Each subcircuit C_i has s input and s output bits, some of which may be unchanged. Each circuit C_i can be replaced by a reversible circuit R_i that uses at most s additional bits. The circuit R_i returns its input as well as the s output values used in the subsequent computation. The input values will be used to uncompute and recompute R_i in order to save space. More than s gates may be required to construct R_i. In general, R_i can be constructed using at most $3s$ gates. While other more efficient constructions are possible, the following three steps always work.

1. Compute all of the output values in a reversible way. For every AND or NOT gate in the original circuit C_i, the circuit R_i has a Toffoli or NOT gate. This step uses the same number of gates, s, as C_i, and uses no more than s additional bits.
2. Copy all of the output values, the values used in subsequent parts of the computation, to the output register, a set of no more than s additional bits.
3. Perform the sequence of gates used to carry out step 1, but this time in reverse order. In this way all bits, except those in the output register, are reset to their original values. Specifically all temporary bits are returned to 0, and we have recovered all of the input values.

The circuits $R_1 \ldots R_r$ perform the computation C in a reversible but space-inefficient way. The subcircuits R_i can be combined in a special way that uses space more efficiently by uncomputing and reusing some of the bits. Uncomputing requires additional gates, so we must choose carefully

when to uncompute in order to reduce the usage of space without needing too many more gates. Fir, we show how to obtain a reversible version using $O(t^{\log_2 3})$ gates and $O(s \log t)$ bits, and then we improve on this method to obtain $O(t^{1+\epsilon})$ gates and $O(s \log t)$ bit bounds.

The basic principle for combining the $r = \lceil t/s \rceil$ circuits R_i is to uncompute and recompute parts of the state selectively to reuse the space. We systematically modify the computation $R_1 R_2 \dots R_r$ to reduce both the total amout of space used and to reset all the temporary bits to zero by the end of the computation.

To simplify the analysis, we take r to be a power of two, $r = 2^k$. For $1 \le i \le k$, let $r_i = 2^i$. We perform the following recursive transformation $\mathcal{B}$ that breaks a sequence into two equal-sized parts, recursively transforms the parts, and the composes them in the way shown:

$$\begin{aligned} \mathcal{B}(R_1, \dots, R_{r_{i+1}}) &= \mathcal{B}(R_1, \dots, R_{r_i}) \mathcal{B}(R_{1+r_i}, \dots, R_{r_{i+1}}) [\mathcal{B}(R_1, \dots, R_{r_i})]^{-1} \\ \mathcal{B}(R) &= R, \end{aligned}$$

where $[\mathcal{B}(R_1, \dots, R_{r_i})]^{-1}$ acts on exactly the same bits as $\mathcal{B}(R_1, \dots, R_{r_i})$ and so requires no additional space.

The transformed computation uncomputes all space except the output of the last step, so the additional space usage is bounded by s. Thus, $\mathcal{B}(R_1, \dots, R_i)$ requires at most s more space than $\mathcal{B}(R_1, \dots, R_{i-1})$. We can write the space $S(i)$ required for each of the $k = \log_2(r)$ steps i in the recursion in terms of the space requirements of the previous step: $S(i) \le s + S(i-1)$ with $S(i) \le 2s$. The recursion ends after $k = \log_2 r$ steps, so the final computation $\mathcal{B}(R_1, \dots, R_r)$ requires at most $S(r) \le (k+1)s = s(\log_2 r + 1)$ space. From the definition of $\mathcal{B}$, it follows immediately that $T(i)$, the number of circuits R_j executed by the computation $\mathcal{B}(R_1, \dots, R_{r_i})$, is $T(i) = 3T(i-1)$ with $T(1) = 1$. By assumption $r = 2^k$, so the reversible version of C we constructed uses

$$T(2^k) = 3T(2^{k-1}) = 3^k = 3^{\log_2 r} = r^{\log_2 3}$$

reversible circuit R_i, each of which requires few than $3s$ gates. Thus, any classical computation of t steps and s bits can be done reversibly in $O(t^{\log_2 3})$ steps and $O(s \log_2 t)$ bits.

To obtain the $O(t^{1+\epsilon})$ bound, instead of using a binary decomposition, consider the following m-ary decomposition. To simplify the analysis, suppose that r is a power of m, $r = m^k$. For $1 \le i \le k$, let $r_i = m^i$. Abbreviating $R_{1+(x-1)r_i}, \dots, R_{xr_i}$ as $\vec{R_{x,i}}$, then

$$\begin{aligned} \mathcal{B}(\vec{R}_{1,i+1}) &= \mathcal{B}(\vec{R}_{1,i}, \vec{R}_{2,i}, \dots, \vec{R}_{m,i}) \\ &= \mathcal{B}(\vec{R}_{1,i}), \mathcal{B}(\vec{R}_{2,i}), \dots, \mathcal{B}(\vec{R}_{m-1,i}), \\ &\quad \mathcal{B}(\vec{R}_{m,i}), \\ &\quad \mathcal{B}(\vec{R}_{m-1,i})^{-1}, \dots, \mathcal{B}(\vec{R}_{2,i})^{-1}, \mathcal{B}(\vec{R}_{1,i})^{-1} \\ \mathcal{B}(R) &= R. \end{aligned}$$

In each step of teh recursion, each block is split into m pieces and replaced with $2m-1$ blocks. We may assume without loss of generality that $r = m^k$ for some k, in which case we stop recursing after k steps. At this point $r = m^k$ subcircuits C_1 have been replaced by $(2m-1)^k$ reversible circuits R_i, so the total number of circuits R_i for the final computation is $(2m-1)^k$, which we rewrite in terms of r:

$$(2m-1)^{\log_m r} = r^{\log_m (2m-1)} \approx r^{\log_m 2m} = r^{1+1/\log_2 m}.$$

The number of primitive gates in R_i is bounded by $3s$ and $r = \lceil t/s \rceil$. The toal number of gates for a reversible circuits of t gates is

$$T(t) \approx 3s \left(\frac{t}{s}\right)^{1+1/\log_2 m} < 3t^{1+1/\log_2 m}.$$

Thus, for any $\epsilon > 0$, it is possible to choose m sufficiently large that the number of gates required for the reversible computation is $O(t^{1+\epsilon})$. The space bound remains the same as before, $O(s \log_2 t)$. Reversible versions of classical Boolean circuits constructed in this manner can be turned directly into quantum circuits consisting entirely of Toffoli and X gates.

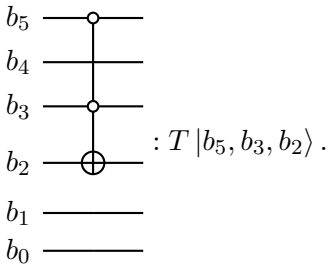
6.3 A Language for Quantum Implementation

The *circuit complexity* is the number of simpole gates in the quantum circuits which can be used to measure the efficiency of the implementations. A single program in this notation can describe precisely a whole class of circuits acting on variable numbers of qubits as input (and classes that depend on other varying classical parameters). The notation uses both classical and quantum variables. Classical control structures such as iterations, recursion, and conditionals are used to define the order in which quantum state transformations are to be applied. Classical information can be used in the construction of a quantum state or as parameters of quantum state transformations, but quantum information cannot be used in classical control structures.

6.3.1 The Basics

Quantum variables are names for registers, subsets of qubits of a single global quantum register. If x is the variable name for an n-qubit register, we may write $x[n]$ if we wish to make the number of qubits in x explicit. We use x_i to refer to the ith qubit of x, and $x_i \dots x_k$ for qubits i through k of the register denoted by x. We will generally order the qubits of a register from highest index to lowest index so that if register x contains a standard basis vector $|b\rangle$, then $b = \sum_i x_i 2^i$. If U is a unitary transformation on n qubits, then the program step $U|x, y, z\rangle = U|x\rangle|y\rangle|z\rangle$ means "apply U to the qubits denoted by the register names in the order given".

Example 6.1.



The notation $(T \otimes C_{not} \otimes H)|x_5 \dots x_3\rangle|x_1, x_0\rangle|x_7\rangle$, for a tranformation acting on six qubits of a ten-qubit register $x = x_9 x_8 \dots x_0$, is just another way of representing the transformation $I \otimes I \otimes H \otimes I \otimes T \otimes I \otimes C_{not}$, where the separate kets indicate which qubits the transformation making up the tensor product is acting upon; the Toffoli gate T acts on qubits x_5, x_4, and x_3, the C_{not} on qubits x_1 and x_0, and the Hadmard gate H on qubit x_7.

Controlled operation: $|b\rangle$ **control** $U|x\rangle$, where b and x are disjoint registers, means that on any standard basis vector the operator U is applied to the contents of register x only if all of the bits in b are 1. Writing $\neg|b\rangle$ **control** $U|x\rangle$ is a convenient shorthand for the sequence

$$\begin{aligned} X \otimes \cdots \otimes X|b\rangle \\ |b\rangle \textbf{ control } U|x, y\rangle \\ X \otimes \cdots \otimes X|b\rangle . \end{aligned}$$

We allow programs to declare local temporary registers using **qubit** $t[n]$, provided that the program restores the qubits in these registers to their initial $|0\rangle$ state. This condition ensures that temporary qubits can be reused for different executions of the program and that the overall storage requirement is bounded. Futhermore, it ensures that the temporary qubits do not remain entangled with the other registers.

6.3.2 Functions

Table 1: Language Summary

Terms	Meaning
U	Name for a unitary transform
U^{-1}	Name for the inverse of U
x	Name for a register of qubits
$x[k]$	Indicates number of qubits in register x
qubit $x[k]$	Indicates x is a name for a register of temporary qubits initially set to $\|0\rangle$
qubit t	Indicates t is a name for a temporary qubit initially set to $\|0\rangle$
x_i	Name for the ith qubit of register x
$x_i \dots x_j$	A sequence of qubits of register x
$\|r\rangle$	Indicates use of qubits named r

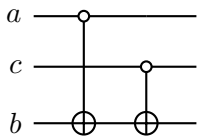
Table 2: Language Summary

Statements	Meaning
$U\|r\rangle$	Apply U to qubits named r
$\|b\rangle$ **control** Γ	Controlled form of statement Γ with control qubits b
$\neg\|b\rangle$ **control** Γ	Statement Γ controlled by negation of qubits b
$\|b_1\rangle\|b_0\rangle$ **control** Γ	Statement Γ controlled by two qubits named b_1 and b_0
for $i \in [a..b]$ $\Gamma(i)$	Perofrm the sequence of statements $\Gamma(a), \Gamma(a+1), \dots, \Gamma(b)$, which depend on the classical paramemter i
define $Name\|x[k]\rangle =$ $\Gamma_0, \Gamma_1, \dots, \Gamma_n$	Introduce $Name$ as a name for a statement that performs statements Γ_0 through Γ_n to a k-qubit register x
$Name\|r\rangle$	Applies the steps described in the definition of $Name$ to register r
$Name^{-1}\|r\rangle$	Appiles the inverse of all the steps described in the definition of $Name$ in reverse order to register r. Since all quantum transformations are reversible, this transformation is always well defined.

Addition modulo 2 with an incoming carry bit can be defined as

$$
\begin{aligned}
Sum : |c, a, b\rangle &\to |c, a, (a + b + c) \mod 2\rangle \\
\textbf{define } Sum\,|c\rangle\,|a\rangle\,|b\rangle &= \\
&|a\rangle \textbf{ control } X\,|b\rangle \\
&|c\rangle \textbf{ control } X\,|b\rangle\,.
\end{aligned}
$$

It operates on three single qubits by adding the value of a and the value of the carry c to the value of b. The program would be drawn as the circuit:



A corresponding carry operator is of the form

$$Carry : \left|c, a, b, c'\right\rangle \rightarrow \left|c, a, b, c' \oplus C(a, b, c)\right\rangle,$$

where the carry $C(a, b, c)$ is 1 if two or more of the bits a, b, c are 1, that is, $C(a, b, c) = (a \wedge b) \oplus [c \wedge (a \oplus b)]$. A program for Carry might look like

$$\begin{aligned}
&\textbf{define } Carry\left|c, a, b, c'\right\rangle = \\
&\qquad |a\rangle\,|b\rangle\,\textbf{control } X\left|c'\right\rangle \\
&\qquad |a\rangle\,\textbf{control } X\,|b\rangle \\
&\qquad |c\rangle\,|b\rangle\,\textbf{control } X\left|c'\right\rangle \\
&\qquad |a\rangle\,\textbf{control } X\,|b\rangle\,.
\end{aligned}$$