量子計算的數學基礎
MA5501*

Chapter 2. Quantum Computing

Introduction

Classical computers carry out logical operations using the "**definite position** of a physical state" (also called classical state). These are usually binary, meaning its operations are based on one of two positions. A single state - such as on or off, up or down, 1 or 0 - is called a bit.

In quantum computing, operations instead use the **quantum state** of an object. These states have indefinite/undetermined positions before they are measured, such as the spin of an electron (電子自旋態) or the polarisation of a photon (光子極化態). Rather than having a clear position, unmeasured quantum states occur in a mixed "superposition", not unlike a coin spinning through the air before it lands in your hand. These superpositions can be **entangled** with those of other objects, meaning their final outcomes will be mathematically related even if we do not know yet what they are.

Introduction

Classical computers carry out logical operations using the "**definite position** of a physical state" (also called classical state). These are usually binary, meaning its operations are based on one of two positions. A single state - such as on or off, up or down, 1 or 0 - is called a bit.

In quantum computing, operations instead use the **quantum state** of an object. These states have indefinite/undetermined positions before they are measured, such as the spin of an electron (電子自旋態) or the polarisation of a photon (光子極化態). Rather than having a clear position, unmeasured quantum states occur in a mixed "superposition", not unlike a coin spinning through the air before it lands in your hand. These superpositions can be **entangled** with those of other objects, meaning their final outcomes will be mathematically related even if we do not know yet what they are.

Introduction

Classical computers carry out logical operations using the "**definite position** of a physical state" (also called classical state). These are usually binary, meaning its operations are based on one of two positions. A single state - such as on or off, up or down, 1 or 0 - is called a bit.

In quantum computing, operations instead use the **quantum state** of an object. These states have indefinite/undetermined positions before they are measured, such as the spin of an electron (電子自旋態) or the polarisation of a photon (光子極化態). Rather than having a clear position, unmeasured quantum states occur in a mixed "superposition", not unlike a coin spinning through the air before it lands in your hand. These superpositions can be **entangled** with those of other objects, meaning their final outcomes will be mathematically related even if we do not know yet what they are.

Introduction

Classical computers carry out logical operations using the "**definite position** of a physical state" (also called classical state). These are usually binary, meaning its operations are based on one of two positions. A single state - such as on or off, up or down, 1 or 0 - is called a bit.

In quantum computing, operations instead use the **quantum state** of an object. These states have indefinite/undetermined positions before they are measured, such as the spin of an electron (電子自旋態) or the polarisation of a photon (光子極化態). Rather than having a clear position, unmeasured quantum states occur in a mixed "superposition", not unlike a coin spinning through the air before it lands in your hand. These superpositions can be **entangled** with those of other objects, meaning their final outcomes will be mathematically related even if we do not know yet what they are.

Introduction

In a classical computer, each number is in classical state. Call these states $|1\rangle, |2\rangle, \cdots, |N\rangle$ (here we treat $|1\rangle, \cdots, |N\rangle$ as N distinct outcomes but not necessarily natural numbers from 1 to N). A superposition of these states is a quantum state

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle,$$

where $\alpha_1, \cdots, \alpha_N$ are complex numbers satisfying $|\alpha_1|^2 + \cdots + |\alpha_N|^2 = 1$ and this particular quantum state, upon measurement, gives $|j\rangle$ with probability $|\alpha_j|^2$. Quantum computers perform calculations based on the probability of an object's quantum state. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. An important objective is to find **quantum algorithms** that are significantly faster than any classical algorithm solving the same problem.

Introduction

In a classical computer, each number is in classical state. Call these states $|1\rangle, |2\rangle, \cdots, |N\rangle$ (here we treat $|1\rangle, \cdots, |N\rangle$ as N distinct outcomes but not necessarily natural numbers from 1 to N). A superposition of these states is a quantum state

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle,$$

where $\alpha_1, \cdots, \alpha_N$ are complex numbers satisfying $|\alpha_1|^2 + \cdots + |\alpha_N|^2 = 1$ and this particular quantum state, upon measurement, gives $|j\rangle$ with probability $|\alpha_j|^2$. Quantum computers perform calculations based on the probability of an object's quantum state. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. An important objective is to find **quantum algorithms** that are significantly faster than any classical algorithm solving the same problem.

Introduction

In a classical computer, each number is in classical state. Call these states $|1\rangle, |2\rangle, \cdots, |N\rangle$ (here we treat $|1\rangle, \cdots, |N\rangle$ as N distinct outcomes but not necessarily natural numbers from 1 to N). A superposition of these states is a quantum state

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle,$$

where $\alpha_1, \cdots, \alpha_N$ are complex numbers satisfying $|\alpha_1|^2 + \cdots + |\alpha_N|^2 = 1$ and this particular quantum state, upon measurement, gives $|j\rangle$ with probability $|\alpha_j|^2$. Quantum computers perform calculations based on the probability of an object's quantum state. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. An important objective is to find **quantum algorithms** that are significantly faster than any classical algorithm solving the same problem.

Introduction

In a classical computer, each number is in classical state. Call these states $|1\rangle, |2\rangle, \cdots, |N\rangle$ (here we treat $|1\rangle, \cdots, |N\rangle$ as N distinct outcomes but not necessarily natural numbers from 1 to N). A superposition of these states is a quantum state

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle,$$

where $\alpha_1, \cdots, \alpha_N$ are complex numbers satisfying $|\alpha_1|^2 + \cdots + |\alpha_N|^2 = 1$ and this particular quantum state, upon measurement, gives $|j\rangle$ with probability $|\alpha_j|^2$. Quantum computers perform calculations based on the probability of an object's quantum state. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles. An important objective is to find **quantum algorithms** that are significantly faster than any classical algorithm solving the same problem.

§2.1 Quantum Mechanics

§2.1.1 Schrödinger equation

In "continuous" quantum mechanics, the Schrödinger equation for a single non-relativistic particle with mass m is given by

$$i\hbar\frac{\partial}{\partial t}\psi = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\}\,, \tag{1}$$

where $\hbar \approx 1.05457181765 \times 10^{-34} J \cdot s$ is the reduced Planck constant, $\psi = \psi(x,t)$ is the **wave function**, a function that assigns a complex number to each point x at each time t, and $V = V(x,t)$ is a real-valued function, called the potential, that represents the environment in which the particle exists. **The square of the absolute value of the wave function** at each point is taken to define a probability density function: given a wave function in position space $\psi(x,t)$ as above, the function $\big|\psi(x,t)\big|^2$ denotes the probability density of the presence of the particle at position x at time t.

§2.1 Quantum Mechanics

§2.1.1 Schrödinger equation

In “continuous” quantum mechanics, the Schrödinger equation for a single non-relativistic particle with mass m is given by

$$i\hbar\frac{\partial}{\partial t}\psi = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\}\,, \tag{1}$$

where $\hbar \approx 1.05457181765 \times 10^{-34} J \cdot s$ is the reduced Planck constant, $\psi = \psi(x, t)$ is the **wave function**, a function that assigns a complex number to each point x at each time t, and $V = V(x, t)$ is a real-valued function, called the potential, that represents the environment in which the particle exists. **The square of the absolute value of the wave function** at each point is taken to define a probability density function: given a wave function in position space $\psi(x, t)$ as above, the function $\big|\psi(x, t)\big|^2$ denotes the probability density of the presence of the particle at position x at time t.

§2.1 Quantum Mechanics

Taking the complex conjugate of the Schrödinger equation (1), we obtain that

$$-i\hbar\frac{\partial}{\partial t}\bar{\psi} = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\bar{\psi}$$

thus

$$i\hbar\,\bar{\psi}\frac{\partial}{\partial t}\psi = \bar{\psi}\Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi\,, \quad i\hbar\,\psi\frac{\partial}{\partial t}\bar{\psi} = -\psi\Big(-\frac{\hbar}{2m}\Delta + V\Big)\bar{\psi}\,.$$

Therefore,

$$i\hbar\frac{\partial}{\partial t}|\psi|^2 = i\hbar\frac{\partial}{\partial t}(\bar{\psi}\psi) = \frac{\hbar}{2m}\big(\psi\Delta\bar{\psi} - \bar{\psi}\Delta\psi\big)$$

so that the divergence theorem implies that

$$\begin{aligned} i\hbar\frac{d}{dt}\int_{\mathbb{R}^3}\big|\psi(x,t)\big|^2 dx &= \frac{\hbar}{2m}\int_{\mathbb{R}^3}\big[\psi(x,t)\Delta\bar{\psi}(x,t) - \bar{\psi}(x,t)\Delta\psi(x,t)\big]\,dx \\ &= 0\,. \end{aligned}$$

§2.1 Quantum Mechanics

Therefore, $\int_{\mathbb{R}^3} |\psi(x,t)|^2 \, dx$ is a constant (which is assumed to be 1 if at a certain time this integral is 1). This shows that the probability of the presence of a particle (whose dynamics is described by (1)) at a certain point in $\mathbb{R}^3$ is 1. The physical interpretation of this identity is "the position at which the particle locates is a superposition of all the points in $\mathbb{R}^3$".

On the other hand, when you try to figure out the location of the particle by implementing some kind of measurements, you always obtain an unambiguous result. The outcome of the measurement follows the probability distribution that the probability density function $|\psi(\cdot,t)|^2$ provides: the probability of that the particle locations in the region $\mathcal{D} \subseteq \mathbb{R}^3$ at time t is given by $\int_{\mathcal{D}} |\psi(x,t)|^2 \, dx$.

§2.1 Quantum Mechanics

Therefore, $\int_{\mathbb{R}^3} |\psi(x,t)|^2\,dx$ is a constant (which is assumed to be 1 if at a certain time this integral is 1). This shows that the probability of the presence of a particle (whose dynamics is described by (1)) at a certain point in $\mathbb{R}^3$ is 1. The physical interpretation of this identity is "the position at which the particle locates is a superposition of all the points in $\mathbb{R}^3$".

On the other hand, when you try to figure out the location of the particle by implementing some kind of measurements, you always obtain an unambiguous result. The outcome of the measurement follows the probability distribution that the probability density function $|\psi(\cdot,t)|^2$ provides: the probability of that the particle locations in the region $\mathcal{D} \subseteq \mathbb{R}^3$ at time t is given by $\int_{\mathcal{D}} |\psi(x,t)|^2\,dx$.

§2.1 Quantum Mechanics

Therefore, $\int_{\mathbb{R}^3} |\psi(x,t)|^2\,dx$ is a constant (which is assumed to be 1 if at a certain time this integral is 1). This shows that the probability of the presence of a particle (whose dynamics is described by (1)) at a certain point in $\mathbb{R}^3$ is 1. The physical interpretation of this identity is "the position at which the particle locates is a superposition of all the points in $\mathbb{R}^3$".

On the other hand, when you try to figure out the location of the particle by implementing some kind of measurements, you always obtain an unambiguous result. The outcome of the measurement follows the probability distribution that the probability density function $|\psi(\cdot,t)|^2$ provides: the probability of that the particle locations in the region $\mathcal{D} \subseteq \mathbb{R}^3$ at time t is given by $\int_{\mathcal{D}} |\psi(x,t)|^2\,dx$.

§2.1 Quantum Mechanics

Therefore, $\int_{\mathbb{R}^3} |\psi(x, t)|^2 \, dx$ is a constant (which is assumed to be 1 if at a certain time this integral is 1). This shows that the probability of the presence of a particle (whose dynamics is described by (1)) at a certain point in $\mathbb{R}^3$ is 1. The physical interpretation of this identity is "the position at which the particle locates is a superposition of all the points in $\mathbb{R}^3$".

On the other hand, when you try to figure out the location of the particle by implementing some kind of measurements, you always obtain an unambiguous result. The outcome of the measurement follows the probability distribution that the probability density function $|\psi(\cdot, t)|^2$ provides: the probability of that the particle locations in the region $\mathcal{D} \subseteq \mathbb{R}^3$ at time t is given by $\int_{\mathcal{D}} |\psi(x, t)|^2 \, dx$.

§2.1 Quantum Mechanics

Definition

A **quantum state** is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a system.

§2.1 Quantum Mechanics

§2.1.2 Superposition

In quantum computing, each data is a superposition of "classical data". Consider some physical system that can be in N different, mutually exclusive classical states $|1\rangle, |2\rangle, \cdots, |N\rangle$. A superposition of these states is described by the wave function

$$\psi(x) = \begin{cases} \alpha_1 & \text{if } x = |1\rangle, \\ \vdots & \\ \alpha_N & \text{if } x = |N\rangle, \end{cases}$$

where α_j is a complex number called the **amplitude** of $|j\rangle$ in $|\psi\rangle$, and $\alpha_1, \cdots, \alpha_N$ satisfy $|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_N|^2 = 1$. The wave function above is a pure quantum state (usually just called state) and is usually written as

$$|\psi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle .$$

§2.1 Quantum Mechanics

§2.1.2 Superposition

In quantum computing, each data is a superposition of "classical data". Consider some physical system that can be in N different, mutually exclusive classical states $|1\rangle$, $|2\rangle$, $\cdots$, $|N\rangle$. A superposition of these states is described by the wave function

$$\psi(x) = \begin{cases} \alpha_1 & \text{if } x = |1\rangle, \\ \vdots & \\ \alpha_N & \text{if } x = |N\rangle, \end{cases}$$

where α_j is a complex number called the **amplitude** of $|j\rangle$ in $|\psi\rangle$, and $\alpha_1, \cdots, \alpha_N$ satisfy $|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_N|^2 = 1$. The wave function above is a pure quantum state (usually just called state) and is usually written as

$$|\psi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle\,.$$

§2.1 Quantum Mechanics

§2.1.2 Superposition

In quantum computing, each data is a superposition of "classical data". Consider some physical system that can be in N different, mutually exclusive classical states $|1\rangle$, $|2\rangle$, $\cdots$, $|N\rangle$. A superposition of these states is described by the wave function

$$\psi(x) = \begin{cases} \alpha_1 & \text{if } x = |1\rangle\,, \\ \vdots & \\ \alpha_N & \text{if } x = |N\rangle\,, \end{cases}$$

where α_j is a complex number called the **amplitude** of $|j\rangle$ in $|\psi\rangle$, and $\alpha_1, \cdots, \alpha_N$ satisfy $|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_N|^2 = 1$. The wave function above is a pure quantum state (usually just called state) and is usually written as

$$|\psi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle\,.$$

§2.1 Quantum Mechanics

Intuitively, a system in quantum state $|\psi\rangle$ is in all classical states at the same time! It is in state $|1\rangle$ with amplitude α_1 (and probability $|\alpha_1|^2$), in state $|2\rangle$ with amplitude α_2 (and probability $|\alpha_2|^2$), and so on. Mathematically, the states $|1\rangle, \cdots, |N\rangle$ form an orthonormal basis of an N-dimensional Hilbert space (that is, an N-dimensional vector space equipped with an inner product), and a quantum state $|\psi\rangle$ is a vector in this space.

Notation: Let $(\mathbb{H}, \langle\cdot,\cdot\rangle)$ be a Hilbert space over field $\mathbb{F}$. Any vectors $\boldsymbol{v}$ in $\mathbb{H}$ is expressed as $|\boldsymbol{v}\rangle$. For example, in "continuous" quantum mechanics every quantum state $|\psi\rangle$ lives in the Hilbert space $L^2(\mathbb{R}^3)$. For a vector $\boldsymbol{v} \in \mathbb{H}$, the notation $\langle\boldsymbol{v}|$ is an element in the **dual space** of $\mathbb{H}$ satisfying $\langle\boldsymbol{v}|\boldsymbol{w}\rangle \equiv \langle\boldsymbol{v}, \boldsymbol{w}\rangle$. In other word, for each $\boldsymbol{w} \in \mathbb{H}$, we write $\boldsymbol{w} = \alpha\boldsymbol{v} + \beta\boldsymbol{v}^\perp$ for some $\alpha \in \mathbb{F}$ so that $\langle\boldsymbol{v}| : \boldsymbol{w} \mapsto \alpha\|\boldsymbol{v}\|^2$.

§2.1 Quantum Mechanics

Intuitively, a system in quantum state $|\psi\rangle$ is in all classical states at the same time! It is in state $|1\rangle$ with amplitude α_1 (and probability $|\alpha_1|^2$), in state $|2\rangle$ with amplitude α_2 (and probability $|\alpha_2|^2$), and so on. Mathematically, the states $|1\rangle, \cdots, |N\rangle$ form an orthonormal basis of an N-dimensional Hilbert space (that is, an N-dimensional vector space equipped with an inner product), and a quantum state $|\psi\rangle$ is a vector in this space.

Notation: Let $(\mathbb{H}, \langle\cdot,\cdot\rangle)$ be a Hilbert space over field $\mathbb{F}$. Any vectors $\boldsymbol{v}$ in $\mathbb{H}$ is expressed as $|\boldsymbol{v}\rangle$. For example, in "continuous" quantum mechanics every quantum state $|\psi\rangle$ lives in the Hilbert space $L^2(\mathbb{R}^3)$. For a vector $\boldsymbol{v} \in \mathbb{H}$, the notation $\langle\boldsymbol{v}|$ is an element in the **dual space** of $\mathbb{H}$ satisfying $\langle\boldsymbol{v}|\boldsymbol{w}\rangle \equiv \langle\boldsymbol{v}, \boldsymbol{w}\rangle$. In other word, for each $\boldsymbol{w} \in \mathbb{H}$, we write $\boldsymbol{w} = \alpha\boldsymbol{v} + \beta\boldsymbol{v}^\perp$ for some $\alpha \in \mathbb{F}$ so that $\langle\boldsymbol{v}| : \boldsymbol{w} \mapsto \alpha\|\boldsymbol{v}\|^2$.

§2.1 Quantum Mechanics

Intuitively, a system in quantum state $|\psi\rangle$ is in all classical states at the same time! It is in state $|1\rangle$ with amplitude α_1 (and probability $|\alpha_1|^2$), in state $|2\rangle$ with amplitude α_2 (and probability $|\alpha_2|^2$), and so on. Mathematically, the states $|1\rangle, \cdots, |N\rangle$ form an orthonormal basis of an N-dimensional Hilbert space (that is, an N-dimensional vector space equipped with an inner product), and a quantum state $|\psi\rangle$ is a vector in this space.

Notation: Let $(\mathbb{H}, \langle\cdot,\cdot\rangle)$ be a Hilbert space over field $\mathbb{F}$. Any vectors $\boldsymbol{v}$ in $\mathbb{H}$ is expressed as $|\boldsymbol{v}\rangle$. For example, in "continuous" quantum mechanics every quantum state $|\psi\rangle$ lives in the Hilbert space $L^2(\mathbb{R}^3)$. For a vector $\boldsymbol{v} \in \mathbb{H}$, the notation $\langle\boldsymbol{v}|$ is an element in the **dual space** of $\mathbb{H}$ satisfying $\langle\boldsymbol{v}|\boldsymbol{w}\rangle \equiv \langle\boldsymbol{v},\boldsymbol{w}\rangle$. In other word, for each $\boldsymbol{w} \in \mathbb{H}$, we write $\boldsymbol{w} = \alpha\boldsymbol{v} + \beta\boldsymbol{v}^\perp$ for some $\alpha \in \mathbb{F}$ so that $\langle\boldsymbol{v}| : \boldsymbol{w} \mapsto \alpha\|\boldsymbol{v}\|^2$.

§2.1 Quantum Mechanics

There are two things we can do with a quantum state: measure it or let it evolve unitarily without measuring it.

§2.1.3 Measurement

- **Measurement in the computational basis**

If we measure state $|\phi\rangle$ we will see one and only one classical state $|j\rangle$. The specific $|j\rangle$ that we will see is not determined in advance; the only thing we can say is that we will see state $|j\rangle$ with probability $|\alpha_j|^2$. This implies $\sum_{j=1}^{N} |\alpha_j|^2 = 1$, so **the vector of amplitudes has (Euclidean) norm** 1. If we measure $|\phi\rangle$ and see classical state $|j\rangle$ as a result, then $|\phi\rangle$ itself has "disappeared", and all that is left is $|j\rangle$. In other words, observing $|\phi\rangle$ "collapses" the quantum superposition $|\phi\rangle$ to the classical state $|j\rangle$ that we saw, and all "information" that might have been contained in the amplitudes α_i is gone.

§2.1 Quantum Mechanics

There are two things we can do with a quantum state: measure it or let it evolve unitarily without measuring it.

§2.1.3 Measurement

- **Measurement in the computational basis**

If we measure state $|\phi\rangle$ we will see one and only one classical state $|j\rangle$. The specific $|j\rangle$ that we will see is not determined in advance; the only thing we can say is that we will see state $|j\rangle$ with probability $|\alpha_j|^2$. This implies $\sum_{j=1}^{N} |\alpha_j|^2 = 1$, so **the vector of amplitudes has (Euclidean) norm** 1. If we measure $|\phi\rangle$ and see classical state $|j\rangle$ as a result, then $|\phi\rangle$ itself has "disappeared", and all that is left is $|j\rangle$. In other words, observing $|\phi\rangle$ "collapses" the quantum superposition $|\phi\rangle$ to the classical state $|j\rangle$ that we saw, and all "information" that might have been contained in the amplitudes α_i is gone.

§2.1 Quantum Mechanics

There are two things we can do with a quantum state: measure it or let it evolve unitarily without measuring it.

§2.1.3 Measurement

- **Measurement in the computational basis**

If we measure state $|\phi\rangle$ we will see one and only one classical state $|j\rangle$. The specific $|j\rangle$ that we will see is not determined in advance; the only thing we can say is that we will see state $|j\rangle$ with probability $|\alpha_j|^2$. This implies $\sum_{j=1}^{N} |\alpha_j|^2 = 1$, so **the vector of amplitudes has (Euclidean) norm** 1. If we measure $|\phi\rangle$ and see classical state $|j\rangle$ as a result, then $|\phi\rangle$ itself has "disappeared", and all that is left is $|j\rangle$. In other words, observing $|\phi\rangle$ "collapses" the quantum superposition $|\phi\rangle$ to the classical state $|j\rangle$ that we saw, and all "information" that might have been contained in the amplitudes α_i is gone.

§2.1 Quantum Mechanics

There are two things we can do with a quantum state: measure it or let it evolve unitarily without measuring it.

§2.1.3 Measurement

- **Measurement in the computational basis**

If we measure state $|\phi\rangle$ we will see one and only one classical state $|j\rangle$. The specific $|j\rangle$ that we will see is not determined in advance; the only thing we can say is that we will see state $|j\rangle$ with probability $|\alpha_j|^2$. This implies $\sum_{j=1}^{N} |\alpha_j|^2 = 1$, so **the vector of amplitudes has (Euclidean) norm** 1. If we measure $|\phi\rangle$ and see classical state $|j\rangle$ as a result, then $|\phi\rangle$ itself has "disappeared", and all that is left is $|j\rangle$. In other words, observing $|\phi\rangle$ "collapses" the quantum superposition $|\phi\rangle$ to the classical state $|j\rangle$ that we saw, and all "information" that might have been contained in the amplitudes α_i is gone.

§2.1 Quantum Mechanics

There are two things we can do with a quantum state: measure it or let it evolve unitarily without measuring it.

§2.1.3 Measurement

- **Measurement in the computational basis**

If we measure state $|\phi\rangle$ we will see one and only one classical state $|j\rangle$. The specific $|j\rangle$ that we will see is not determined in advance; the only thing we can say is that we will see state $|j\rangle$ with probability $|\alpha_j|^2$. This implies $\sum_{j=1}^{N} |\alpha_j|^2 = 1$, so **the vector of amplitudes has (Euclidean) norm** 1. If we measure $|\phi\rangle$ and see classical state $|j\rangle$ as a result, then $|\phi\rangle$ itself has "disappeared", and all that is left is $|j\rangle$. In other words, observing $|\phi\rangle$ "collapses" the quantum superposition $|\phi\rangle$ to the classical state $|j\rangle$ that we saw, and all "information" that might have been contained in the amplitudes α_i is gone.

§2.1 Quantum Mechanics

- **Projective measurement**

A somewhat more general kind of measurement is called *projective measurement*. Such a projective measurement is described by projectors $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_m$ $(m \leqslant N)$ which **sum to identity**. These projectors are then pairwise orthogonal, meaning that $\mathrm{P}_i\mathrm{P}_j = 0$ if $i \neq j$. The projector P_j projects on some subspace $\mathbb{H}_j$ of the total Hilbert space $\mathbb{H}$, and every state $|\phi\rangle \in \mathbb{H}$ can be decomposed in a unique way as $|\phi\rangle = \sum_{j=1}^{N} |\phi_j\rangle$, with $|\phi_j\rangle = \mathrm{P}_j|\phi\rangle \in \mathbb{H}_j$. Because the projectors are orthogonal, the subspaces $\mathbb{H}_j$ are orthogonal as well, as are the states $|\phi_j\rangle$. When we apply this measurement to the pure state $|\phi\rangle$, then we will get outcome in $\mathbb{H}_j$ with probability $\||\phi_j\rangle\|^2 = \mathrm{tr}(\mathrm{P}_j|\phi\rangle\langle\phi|)$ and the state will then "collapse" to the new state $|\phi_j\rangle/\||\phi_j\rangle\| = \mathrm{P}_j|\phi\rangle/\|\mathrm{P}_j|\phi\rangle\|$.

§2.1 Quantum Mechanics

- **Projective measurement**

A somewhat more general kind of measurement is called *projective measurement*. Such a projective measurement is described by projectors P_1, P_2, $\cdots$, P_m $(m \leqslant N)$ which **sum to identity**. These projectors are then pairwise orthogonal, meaning that $\mathrm{P}_i\mathrm{P}_j = 0$ if $i \neq j$. The projector P_j projects on some subspace $\mathbb{H}_j$ of the total Hilbert space $\mathbb{H}$, and every state $|\phi\rangle \in \mathbb{H}$ can be decomposed in a unique way as $|\phi\rangle = \sum_{j=1}^{N} |\phi_j\rangle$, with $|\phi_j\rangle = \mathrm{P}_j|\phi\rangle \in \mathbb{H}_j$. Because the projectors are orthogonal, the subspaces $\mathbb{H}_j$ are orthogonal as well, as are the states $|\phi_j\rangle$. When we apply this measurement to the pure state $|\phi\rangle$, then we will get outcome in $\mathbb{H}_j$ with probability $\||\phi_j\rangle\|^2 = \mathrm{tr}(\mathrm{P}_j|\phi\rangle\langle\phi|)$ and the state will then "collapse" to the new state $|\phi_j\rangle/\||\phi_j\rangle\| = \mathrm{P}_j|\phi\rangle/\|\mathrm{P}_j|\phi\rangle\|$.

§2.1 Quantum Mechanics

- **Projective measurement**

A somewhat more general kind of measurement is called *projective measurement*. Such a projective measurement is described by projectors P_1, P_2, $\cdots$, P_m $(m \leqslant N)$ which **sum to identity**. These projectors are then pairwise orthogonal, meaning that $\mathrm{P}_i\mathrm{P}_j = 0$ if $i \neq j$. The projector P_j projects on some subspace $\mathbb{H}_j$ of the total Hilbert space $\mathbb{H}$, and every state $|\phi\rangle \in \mathbb{H}$ can be decomposed in a unique way as $|\phi\rangle = \sum_{j=1}^{N} |\phi_j\rangle$, with $|\phi_j\rangle = \mathrm{P}_j|\phi\rangle \in \mathbb{H}_j$. Because the projectors are orthogonal, the subspaces $\mathbb{H}_j$ are orthogonal as well, as are the states $|\phi_j\rangle$. When we apply this measurement to the pure state $|\phi\rangle$, then we will get outcome in $\mathbb{H}_j$ with probability $\||\phi_j\rangle\|^2 = \mathrm{tr}(\mathrm{P}_j|\phi\rangle\langle\phi|)$ and the state will then "collapse" to the new state $|\phi_j\rangle/\||\phi_j\rangle\| = \mathrm{P}_j|\phi\rangle/\|\mathrm{P}_j|\phi\rangle\|$.

§2.1 Quantum Mechanics

- **Projective measurement**

A somewhat more general kind of measurement is called *projective measurement*. Such a projective measurement is described by projectors $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_m$ $(m \leqslant N)$ which **sum to identity**. These projectors are then pairwise orthogonal, meaning that $\mathrm{P}_i \mathrm{P}_j = 0$ if $i \neq j$. The projector P_j projects on some subspace $\mathbb{H}_j$ of the total Hilbert space $\mathbb{H}$, and every state $|\phi\rangle \in \mathbb{H}$ can be decomposed in a unique way as $|\phi\rangle = \sum_{j=1}^{N} |\phi_j\rangle$, with $|\phi_j\rangle = \mathrm{P}_j|\phi\rangle \in \mathbb{H}_j$. Because the projectors are orthogonal, the subspaces $\mathbb{H}_j$ are orthogonal as well, as are the states $|\phi_j\rangle$. When we apply this measurement to the pure state $|\phi\rangle$, then we will get outcome in $\mathbb{H}_j$ with probability $\||\phi_j\rangle\|^2 = \mathrm{tr}(\mathrm{P}_j|\phi\rangle\langle\phi|)$ and the state will then "collapse" to the new state $|\phi_j\rangle/\||\phi_j\rangle\| = \mathrm{P}_j|\phi\rangle/\|\mathrm{P}_j|\phi\rangle\|$.

§2.1 Quantum Mechanics

- **Projective measurement**

A somewhat more general kind of measurement is called *projective measurement*. Such a projective measurement is described by projectors $\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_m$ $(m \leqslant N)$ which **sum to identity**. These projectors are then pairwise orthogonal, meaning that $\mathrm{P}_i\mathrm{P}_j = 0$ if $i \neq j$. The projector P_j projects on some subspace $\mathbb{H}_j$ of the total Hilbert space $\mathbb{H}$, and every state $|\phi\rangle \in \mathbb{H}$ can be decomposed in a unique way as $|\phi\rangle = \sum_{j=1}^{N} |\phi_j\rangle$, with $|\phi_j\rangle = \mathrm{P}_j|\phi\rangle \in \mathbb{H}_j$. Because the projectors are orthogonal, the subspaces $\mathbb{H}_j$ are orthogonal as well, as are the states $|\phi_j\rangle$. When we apply this measurement to the pure state $|\phi\rangle$, then we will get outcome in $\mathbb{H}_j$ with probability $\||\phi_j\rangle\|^2 = \mathrm{tr}(\mathrm{P}_j|\phi\rangle\langle\phi|)$ and the state will then "collapse" to the new state $|\phi_j\rangle/\||\phi_j\rangle\| = \mathrm{P}_j|\phi\rangle/\|\mathrm{P}_j|\phi\rangle\|$.

§2.1 Quantum Mechanics

Example

A measurement in the standard basis is the specific projective measurement where $m = N$ and $\mathrm{P}_j = |\,j\rangle\langle j\,|$; that is, P_j projects onto the standard basis state $|\,j\rangle$ and the corresponding subspace $\mathbb{H}_j$ is the space spanned by $|\,j\rangle$. Consider the state $|\phi\rangle = \sum\limits_{j=1}^{N} \alpha_j |\,j\rangle$. Note that $\mathrm{P}_j|\phi\rangle = \alpha_j|\,j\rangle$, so applying our measurement to $|\phi\rangle$ will give outcome in $\mathbb{H}_j$ with probability $\|\alpha_j|\,j\rangle\|^2 = |\alpha_j|^2$, and in that case the state collapses to $\dfrac{\alpha_j|\,j\rangle}{\|\alpha_j|\,j\rangle\|} = \dfrac{\alpha_j}{|\alpha_j|}|\,j\rangle$. The norm-1 factor $\dfrac{\alpha_j}{|\alpha_j|}$ may be disregarded because it has no physical significance, so we end up with the state $|\,j\rangle$ as we saw before.

§2.1 Quantum Mechanics

Example

A measurement that distinguishes between $|j\rangle$ with $j < \frac{N}{2}$ and $|j\rangle$ with $j \geqslant \frac{N}{2}$ corresponds to the two projectors $\mathrm{P}_1 = \sum_{j<N/2} |j\rangle\langle j|$ and $\mathrm{P}_2 = \sum_{j\geqslant N/2} |j\rangle\langle j|$. Applying this measurement to the state

$$|\phi\rangle = \frac{1}{2}|1\rangle + \frac{\sqrt{3}}{\sqrt{8}}|2\rangle + \frac{1}{2}|N-1\rangle + \frac{1}{\sqrt{8}}|N\rangle,$$

where $N \geqslant 4$, will give outcome 1 with probability $\|\mathrm{P}_1|\phi\rangle\|^2 = \frac{5}{8}$, in which case the state collapses to $\frac{\sqrt{2}}{\sqrt{5}}|1\rangle + \frac{\sqrt{3}}{\sqrt{5}}|2\rangle$, and will give outcome 2 with probability $\|\mathrm{P}_2|\phi\rangle\|^2 = \frac{3}{8}$, in which case the state collapses to $\frac{\sqrt{2}}{\sqrt{3}}|N-1\rangle + \frac{1}{\sqrt{3}}|N\rangle$.

§2.1 Quantum Mechanics

§2.1.4 Unitary evolution

We can change the state $|\phi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle$ to some other state

$$|\psi\rangle = \sum_{j=1}^{N} \beta_j |j\rangle = \beta_1 |1\rangle + \beta_2 |2\rangle + \cdots + \beta_N |N\rangle .$$

Quantum mechanics only allows linear operations to be applied to quantum states. What this means is: if we view a state like $|\phi\rangle$ as an N-dimensional vector $[\alpha_1, \alpha_2, \cdots, \alpha_N]^{\mathrm{T}}$ (sometimes called the "**qubit state vector**"), then applying an operation that changes $|\phi\rangle$ to $|\psi\rangle$ corresponds to multiplying $|\phi\rangle$ with an $N \times N$ complex-valued matrix U:

$$\mathrm{U} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_N \end{bmatrix} .$$

§2.1 Quantum Mechanics

§2.1.4 Unitary evolution

We can change the state $|\phi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle$ to some other state

$$|\psi\rangle = \sum_{j=1}^{N} \beta_j |j\rangle = \beta_1|1\rangle + \beta_2|2\rangle + \cdots + \beta_N|N\rangle .$$

Quantum mechanics only allows linear operations to be applied to quantum states. What this means is: if we view a state like $|\phi\rangle$ as an N-dimensional vector $[\alpha_1, \alpha_2, \cdots, \alpha_N]^{\mathrm{T}}$ (sometimes called the "**qubit state vector**"), then applying an operation that changes $|\phi\rangle$ to $|\psi\rangle$ corresponds to multiplying $|\phi\rangle$ with an $N \times N$ complex-valued matrix U:

$$\mathrm{U}\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_N \end{bmatrix} .$$

§2.1 Quantum Mechanics

Note that by linearity we have

$$|\psi\rangle = \mathrm{U}|\phi\rangle = \mathrm{U}\Big(\sum_{j=1}^{N}\alpha_j|j\rangle\Big) = \sum_{j=1}^{N}\alpha_j\mathrm{U}|j\rangle\,.$$

Because measuring $|\psi\rangle$ should also give a probability distribution, we have the constraint $\sum_{j=1}^{N}|\beta_j|^2 = 1$. This implies that the operation U must preserve the norm of vectors, and U always maps a vector of norm 1 to a vector of norm 1. Such a linear map is said to be **unitary** and always has an inverse (since $\mathrm{U}\boldsymbol{x} = \mathbf{0}$ if and only if $\boldsymbol{x} = \mathbf{0}$), and it follows that any (non-measuring) operation on quantum states must be reversible: by applying U^{-1} we can always "undo" the action of U, and nothing is lost in the process. On the other hand, a measurement is clearly non-reversible, because we cannot reconstruct $|\phi\rangle$ from the observed classical state $|j\rangle$.

§2.1 Quantum Mechanics

Note that by linearity we have

$$|\psi\rangle = \mathrm{U}|\phi\rangle = \mathrm{U}\Big(\sum_{j=1}^{N} \alpha_j |j\rangle\Big) = \sum_{j=1}^{N} \alpha_j \mathrm{U}|j\rangle .$$

Because measuring $|\psi\rangle$ should also give a probability distribution, we have the constraint $\sum_{j=1}^{N} |\beta_j|^2 = 1$. This implies that the operation U must preserve the norm of vectors, and U always maps a vector of norm 1 to a vector of norm 1. Such a linear map is said to be **unitary** and always has an inverse (since $\mathrm{U}\boldsymbol{x} = \mathbf{0}$ if and only if $\boldsymbol{x} = \mathbf{0}$), and it follows that any (non-measuring) operation on quantum states must be reversible: by applying U^{-1} we can always "undo" the action of U, and nothing is lost in the process. On the other hand, a measurement is clearly non-reversible, because we cannot reconstruct $|\phi\rangle$ from the observed classical state $|j\rangle$.

§2.1 Quantum Mechanics

Note that by linearity we have

$$|\psi\rangle = \mathrm{U}|\phi\rangle = \mathrm{U}\Big(\sum_{j=1}^{N} \alpha_j |j\rangle\Big) = \sum_{j=1}^{N} \alpha_j \mathrm{U}|j\rangle .$$

Because measuring $|\psi\rangle$ should also give a probability distribution, we have the constraint $\sum_{j=1}^{N} |\beta_j|^2 = 1$. This implies that the operation U must preserve the norm of vectors, and U always maps a vector of norm 1 to a vector of norm 1. Such a linear map is said to be **unitary** and always has an inverse (since $\mathrm{U}\boldsymbol{x} = \mathbf{0}$ if and only if $\boldsymbol{x} = \mathbf{0}$), and it follows that any (non-measuring) operation on quantum states must be reversible: by applying U^{-1} we can always "undo" the action of U, and nothing is lost in the process. On the other hand, a measurement is clearly non-reversible, because we cannot reconstruct $|\phi\rangle$ from the observed classical state $|j\rangle$.

§2.1 Quantum Mechanics

Note that by linearity we have

$$|\psi\rangle = \mathrm{U}|\phi\rangle = \mathrm{U}\Big(\sum_{j=1}^{N}\alpha_j|j\rangle\Big) = \sum_{j=1}^{N}\alpha_j\mathrm{U}|j\rangle .$$

Because measuring $|\psi\rangle$ should also give a probability distribution, we have the constraint $\sum_{j=1}^{N}|\beta_j|^2 = 1$. This implies that the operation U must preserve the norm of vectors, and U always maps a vector of norm 1 to a vector of norm 1. Such a linear map is said to be **unitary** and always has an inverse (since $\mathrm{U}\boldsymbol{x} = \mathbf{0}$ if and only if $\boldsymbol{x} = \mathbf{0}$), and it follows that any (non-measuring) operation on quantum states must be reversible: by applying U^{-1} we can always "undo" the action of U, and nothing is lost in the process. On the other hand, a measurement is clearly non-reversible, because we cannot reconstruct $|\phi\rangle$ from the observed classical state $|j\rangle$.

§2.1 Quantum Mechanics

Note that by linearity we have

$$|\psi\rangle = \mathrm{U}|\phi\rangle = \mathrm{U}\Big(\sum_{j=1}^{N} \alpha_j |j\rangle\Big) = \sum_{j=1}^{N} \alpha_j \mathrm{U}|j\rangle .$$

Because measuring $|\psi\rangle$ should also give a probability distribution, we have the constraint $\sum_{j=1}^{N} |\beta_j|^2 = 1$. This implies that the operation U must preserve the norm of vectors, and U always maps a vector of norm 1 to a vector of norm 1. Such a linear map is said to be **unitary** and always has an inverse (since $\mathrm{U}\boldsymbol{x} = \mathbf{0}$ if and only if $\boldsymbol{x} = \mathbf{0}$), and it follows that any (non-measuring) operation on quantum states must be reversible: by applying U^{-1} we can always "undo" the action of U, and nothing is lost in the process. On the other hand, a measurement is clearly non-reversible, because we cannot reconstruct $|\phi\rangle$ from the observed classical state $|j\rangle$.

§2.2 Qubits and Quantum Gates

In the previous sections, we talked about the superposition

$$|\phi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle$$

of N classical states. In a quantum computer, $|\phi\rangle$ is used to expressed a random numbers. Each such number is created using random bits, called **qubits**, and every qubit can be created with different amplitude (or probability) of the 0 and 1 state. A 1-qubit state is represented in braket notation as $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, and an n-qubit state is represented as

$$|\phi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle \qquad \text{or} \qquad |\phi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j_0 \cdots j_{n-1}\rangle,$$

where $(0\, j_0\, j_1 \cdots j_{n-2}\, j_{n-1})_2$ is the binary representation of j; that is,

$$j = 2^{n-1} j_0 + 2^{n-2} j_1 + \cdots + 2^1 j_{n-2} + 2^0 j_{n-1}\,.$$

§2.2 Qubits and Quantum Gates

In the previous sections, we talked about the superposition

$$|\phi\rangle = \sum_{j=1}^{N} \alpha_j |j\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_N|N\rangle$$

of N classical states. In a quantum computer, $|\phi\rangle$ is used to expressed a random numbers. Each such number is created using random bits, called **qubits**, and every qubit can be created with different amplitude (or probability) of the 0 and 1 state. A 1-qubit state is represented in braket notation as $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, and an n-qubit state is represented as

$$|\phi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle \qquad \text{or} \qquad |\phi\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j_0 \cdots j_{n-1}\rangle,$$

where $(0\, j_0\, j_1 \cdots j_{n-2}\, j_{n-1})_2$ is the binary representation of j; that is,

$$j = 2^{n-1} j_0 + 2^{n-2} j_1 + \cdots + 2^1 j_{n-2} + 2^0 j_{n-1}\,.$$

§2.2 Qubits and Quantum Gates

§2.2.1 Quantum bits

Definition (Qubits)

A qubit is a quantum state with two possible outcomes of measurement. A qubit is usually represented by

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

where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Two qubits $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ are said to be equivalent if there exists $\theta \in \mathbb{R}$ such that $(\alpha_2, \beta_2) = e^{i\theta}(\alpha_1, \beta_1)$.

Remark: A qubit is more than a two-valued random variable.

§2.2 Qubits and Quantum Gates

§2.2.1 Quantum bits

Definition (Qubits)

A qubit is a quantum state with two possible outcomes of measurement. A qubit is usually represented by

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

where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Two qubits $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ are said to be equivalent if there exists $\theta \in \mathbb{R}$ such that $(\alpha_2, \beta_2) = e^{i\theta}(\alpha_1, \beta_1)$.

Remark: A qubit is more than a two-valued random variable.

§2.2 Qubits and Quantum Gates

§2.2.1 Quantum bits

Definition (Qubits)

A qubit is a quantum state with two possible outcomes of measurement. A qubit is usually represented by

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

where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Two qubits $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ are said to be equivalent if there exists $\theta \in \mathbb{R}$ such that $(\alpha_2, \beta_2) = e^{i\theta}(\alpha_1, \beta_1)$.

Remark: A qubit is more than a two-valued random variable.

§2.2 Qubits and Quantum Gates

§2.2.1 Quantum bits

Definition (Qubits)

A qubit is a quantum state with two possible outcomes of measurement. A qubit is usually represented by

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

where $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$. Two qubits $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ are said to be equivalent if there exists $\theta \in \mathbb{R}$ such that $(\alpha_2, \beta_2) = e^{i\theta}(\alpha_1, \beta_1)$.

Remark: A qubit is more than a two-valued random variable.

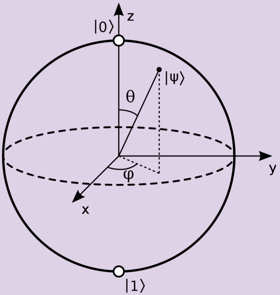
§2.2 Qubits and Quantum Gates

Definition

A Bloch sphere B is a subset of $\mathbb{C}^2$ defined by $(\alpha, \beta) \in B$ if and only if $|\alpha|^2 + |\beta|^2 = 1$. Each point $(\alpha, \beta) \in B$ is represented by

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

where $\theta \in [0, \pi]$ and $\phi \in [0, 2\pi)$.



§2.2 Qubits and Quantum Gates

§2.2.2 Quantum gates

A unitary transformation that acts on a small numer of qubits (say, at most 3) is often called a gate, in analogy to classical logic gates. Two simple but important 1-qubit gates are the **bitflip**-gate X (which negates the bit; that is, swaps $|0\rangle$ and $|1\rangle$) and the **phaseflip** gate Z (which puts a minus sign "$-$" in front of $|1\rangle$). Represented as 2×2 matrices, these are

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Remark: Let $|\psi\rangle = e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big)$ be a 1-qubit quantum state.

§2.2 Qubits and Quantum Gates

§2.2.2 Quantum gates

A unitary transformation that acts on a small numer of qubits (say, at most 3) is often called a gate, in analogy to classical logic gates. Two simple but important 1-qubit gates are the **bitflip**-gate X (which negates the bit; that is, swaps $|0\rangle$ and $|1\rangle$) and the **phaseflip** gate Z (which puts a minus sign "$-$" in front of $|1\rangle$). Represented as 2×2 matrices, these are

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Remark: Let $|\psi\rangle = e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big)$ be a 1-qubit quantum state.

§2.2 Qubits and Quantum Gates

§2.2.2 Quantum gates

A unitary transformation that acts on a small numer of qubits (say, at most 3) is often called a gate, in analogy to classical logic gates. Two simple but important 1-qubit gates are the **bitflip**-gate X (which negates the bit; that is, swaps $|0\rangle$ and $|1\rangle$) and the **phaseflip** gate Z (which puts a minus sign "$-$" in front of $|1\rangle$). Represented as 2×2 matrices, these are

$$\mathrm{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \mathrm{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Remark: Let $|\psi\rangle = e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big)$ be a 1-qubit quantum state.

§2.2 Qubits and Quantum Gates

Then on the Bloch sphere,

1. $\mathrm{X}|\psi\rangle$ is the reflection of $|\psi\rangle$ (or the rotation by angel π) about the x-axis; that is,

$$\begin{aligned}\mathrm{X}|\psi\rangle &= e^{i\delta}\Big(\cos\frac{\pi-\theta}{2}|0\rangle + e^{-i\phi}\sin\frac{\pi-\theta}{2}|1\rangle\Big)\\ &= e^{i(\delta-\phi)}\Big(e^{i\phi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle\Big)\\ &= e^{i(\delta-\phi)}\Big(\cos\frac{\theta}{2}|1\rangle + e^{i\phi}\sin\frac{\theta}{2}|0\rangle\Big).\end{aligned}$$

2. $\mathrm{Z}|\psi\rangle$ is the reflection of $|\psi\rangle$ (or the rotation by angel π) about the z-axis; that is, then

$$\begin{aligned}\mathrm{Z}|\psi\rangle &= e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i(\pi+\phi)}\sin\frac{\theta}{2}|1\rangle\Big)\\ &= e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle - e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big).\end{aligned}$$

§2.2 Qubits and Quantum Gates

Then on the Bloch sphere,

1. $\mathrm{X}|\psi\rangle$ is the reflection of $|\psi\rangle$ (or the rotation by angel π) about the x-axis; that is,

$$\begin{aligned}\mathrm{X}|\psi\rangle &= e^{i\delta}\Big(\cos\frac{\pi-\theta}{2}|0\rangle + e^{-i\phi}\sin\frac{\pi-\theta}{2}|1\rangle\Big) \\ &= e^{i(\delta-\phi)}\Big(e^{i\phi}\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle\Big) \\ &= e^{i(\delta-\phi)}\Big(\cos\frac{\theta}{2}|1\rangle + e^{i\phi}\sin\frac{\theta}{2}|0\rangle\Big).\end{aligned}$$

2. $\mathrm{Z}|\psi\rangle$ is the reflection of $|\psi\rangle$ (or the rotation by angel π) about the z-axis; that is, then

$$\begin{aligned}\mathrm{Z}|\psi\rangle &= e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i(\pi+\phi)}\sin\frac{\theta}{2}|1\rangle\Big) \\ &= e^{i\delta}\Big(\cos\frac{\theta}{2}|0\rangle - e^{i\phi}\sin\frac{\theta}{2}|1\rangle\Big).\end{aligned}$$

§2.2 Qubits and Quantum Gates

Possibly the most important 1-qubit gate is the **Hadamard** transform, specified by:

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{and} \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The Hadamard transform is represented as

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

If we apply H to initial state $|0\rangle$ and then measure, we have equal probability of observing $|0\rangle$ or $|1\rangle$. Similarly, applying H to $|1\rangle$ and observing gives equal probability of $|0\rangle$ or $|1\rangle$. However, if we apply H to the superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ then we obtain $|0\rangle$: the positive and negative amplitudes for $|1\rangle$ cancel out! This effect is called **interference**, and is analogous to interference patterns between light or sound waves.

§2.2 Qubits and Quantum Gates

Possibly the most important 1-qubit gate is the **Hadamard** transform, specified by:

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{and} \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The Hadamard transform is represented as

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

If we apply H to initial state $|0\rangle$ and then measure, we have equal probability of observing $|0\rangle$ or $|1\rangle$. Similarly, applying H to $|1\rangle$ and observing gives equal probability of $|0\rangle$ or $|1\rangle$. However, if we apply H to the superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ then we obtain $|0\rangle$: the positive and negative amplitudes for $|1\rangle$ cancel out! This effect is called **interference**, and is analogous to interference patterns between light or sound waves.

§2.2 Qubits and Quantum Gates

Possibly the most important 1-qubit gate is the **Hadamard** transform, specified by:

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{and} \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The Hadamard transform is represented as

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

If we apply H to initial state $|0\rangle$ and then measure, we have equal probability of observing $|0\rangle$ or $|1\rangle$. Similarly, applying H to $|1\rangle$ and observing gives equal probability of $|0\rangle$ or $|1\rangle$. However, if we apply H to the superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ then we obtain $|0\rangle$: the positive and negative amplitudes for $|1\rangle$ cancel out! This effect is called **interference**, and is analogous to interference patterns between light or sound waves.

§2.2 Qubits and Quantum Gates

Possibly the most important 1-qubit gate is the **Hadamard** transform, specified by:

$$\mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{and} \quad \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

The Hadamard transform is represented as

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

If we apply H to initial state $|0\rangle$ and then measure, we have equal probability of observing $|0\rangle$ or $|1\rangle$. Similarly, applying H to $|1\rangle$ and observing gives equal probability of $|0\rangle$ or $|1\rangle$. However, if we apply H to the superposition $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ then we obtain $|0\rangle$: the positive and negative amplitudes for $|1\rangle$ cancel out! This effect is called **interference**, and is analogous to interference patterns between light or sound waves.

§2.2 Qubits and Quantum Gates

Let us also consider the reflection (or the rotation by angle π) about the y-axis. This rotation is denoted by Y and is given by

$$\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \overset{\mathrm{Y}}{\mapsto} \cos\frac{\pi-\theta}{2}|0\rangle + e^{i(\pi-\phi)}\sin\frac{\pi-\theta}{2}|1\rangle$$

so that the matrix representation of Y is

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

These three gates X, Y, Z are called the **Pauli gates**. We note that if A and B are two different Pauli gates, then $AB + BA = 0$.

Remark: In principle, the matrix representation of a quantum gate can differ by a multiple of a constant whose modulus is 1 because these representations give equivalent quantum states. We choose X, Y and Z in such a way that $\mathrm{X}^2 = \mathrm{Y}^2 = \mathrm{Z}^2 = \mathrm{I}$.

§2.2 Qubits and Quantum Gates

Let us also consider the reflection (or the rotation by angle π) about the y-axis. This rotation is denoted by Y and is given by

$$\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \overset{\mathrm{Y}}{\mapsto} \cos\frac{\pi-\theta}{2}|0\rangle + e^{i(\pi-\phi)}\sin\frac{\pi-\theta}{2}|1\rangle$$

so that the matrix representation of Y is

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

These three gates X, Y, Z are called the **Pauli gates**. We note that if A and B are two different Pauli gates, then $AB + BA = 0$.

Remark: In principle, the matrix representation of a quantum gate can differ by a multiple of a constant whose modulus is 1 because these representations give equivalent quantum states. We choose X, Y and Z in such a way that $\mathrm{X}^2 = \mathrm{Y}^2 = \mathrm{Z}^2 = \mathrm{I}$.

§2.2 Qubits and Quantum Gates

Let us also consider the reflection (or the rotation by angle π) about the y-axis. This rotation is denoted by Y and is given by

$$\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \overset{\mathrm{Y}}{\mapsto} \cos\frac{\pi-\theta}{2}|0\rangle + e^{i(\pi-\phi)}\sin\frac{\pi-\theta}{2}|1\rangle$$

so that the matrix representation of Y is

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

These three gates X, Y, Z are called the **Pauli gates**. We note that if A and B are two different Pauli gates, then $AB + BA = 0$.

Remark: In principle, the matrix representation of a quantum gate can differ by a multiple of a constant whose modulus is 1 because these representations give equivalent quantum states. We choose X, Y and Z in such a way that $\mathrm{X}^2 = \mathrm{Y}^2 = \mathrm{Z}^2 = \mathrm{I}$.

§2.2 Qubits and Quantum Gates

In general, we can consider the rotation by angle τ about the *x*-axis, *y*-axis and *z*-axis. These rotations are denoted by $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$, respectively.

Theorem

For $\tau \in \mathbb{R}$, the matrix representations of $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ are respectively given by

$$\mathrm{R}_x(\tau) = \begin{bmatrix} \cos\frac{\tau}{2} & -i\sin\frac{\tau}{2} \\ -i\sin\frac{\tau}{2} & \cos\frac{\tau}{2} \end{bmatrix}, \tag{2a}$$

$$\mathrm{R}_y(\tau) = \begin{bmatrix} \cos\frac{\tau}{2} & -\sin\frac{\tau}{2} \\ \sin\frac{\tau}{2} & \cos\frac{\tau}{2} \end{bmatrix}, \tag{2b}$$

$$\mathrm{R}_z(\tau) = \begin{bmatrix} e^{-i\tau/2} & 0 \\ 0 & e^{i\tau/2} \end{bmatrix}. \tag{2c}$$

§2.2 Qubits and Quantum Gates

Proof.

Let $|\psi\rangle$ be a 1-qubit quantum state

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

whose Cartesian coordinate on the Bloch sphere is

$$\overrightarrow{\psi} \equiv \cos\phi\sin\theta\boldsymbol{i} + \sin\phi\sin\theta\boldsymbol{j} + \cos\theta\boldsymbol{k}\,.$$

1. On the unit sphere, the rotation of the vector $\overrightarrow{\psi}$ by angle τ about the x-axis leaves the x-coordinate unchanged, while the y-coordinate and the z-coordinate are obtained, using the rotation matrix, by

$$\begin{bmatrix} \cos\tau & -\sin\tau \\ \sin\tau & \cos\tau \end{bmatrix}\begin{bmatrix} \sin\phi\sin\theta \\ \cos\theta \end{bmatrix} = \begin{bmatrix} \cos\tau\sin\phi\sin\theta - \sin\tau\cos\theta \\ \sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta \end{bmatrix}.$$

□

§2.2 Qubits and Quantum Gates

Proof.

Let $|\psi\rangle$ be a 1-qubit quantum state

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

whose Cartesian coordinate on the Bloch sphere is

$$\overrightarrow{\psi} \equiv \cos\phi\sin\theta\boldsymbol{i} + \sin\phi\sin\theta\boldsymbol{j} + \cos\theta\boldsymbol{k}\,.$$

1. On the unit sphere, the rotation of the vector $\overrightarrow{\psi}$ by angle τ about the x-axis leaves the x-coordinate unchanged, while the y-coordinate and the z-coordinate are obtained, using the rotation matrix, by

$$\begin{bmatrix}\cos\tau & -\sin\tau\\ \sin\tau & \cos\tau\end{bmatrix}\begin{bmatrix}\sin\phi\sin\theta\\ \cos\theta\end{bmatrix} = \begin{bmatrix}\cos\tau\sin\phi\sin\theta - \sin\tau\cos\theta\\ \sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta\end{bmatrix}. \qquad \square$$

§2.2 Qubits and Quantum Gates

Proof.

Let $|\psi\rangle$ be a 1-qubit quantum state

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

whose Cartesian coordinate on the Bloch sphere is

$$\overrightarrow{\psi} \equiv \cos\phi\sin\theta\boldsymbol{i} + \sin\phi\sin\theta\boldsymbol{j} + \cos\theta\boldsymbol{k}\,.$$

1. On the unit sphere, the rotation of the vector $\overrightarrow{\psi}$ by angle τ about the x-axis leaves the x-coordinate unchanged, while the y-coordinate and the z-coordinate are obtained, using the rotation matrix, by

$$\begin{bmatrix} \cos\tau & -\sin\tau \\ \sin\tau & \cos\tau \end{bmatrix}\begin{bmatrix} \sin\phi\sin\theta \\ \cos\theta \end{bmatrix} = \begin{bmatrix} \cos\tau\sin\phi\sin\theta - \sin\tau\cos\theta \\ \sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta \end{bmatrix}. \quad \square$$

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Suppose that in Cartesian coordinate the state $\mathrm{R}_x(\tau)|\psi\rangle$ on the Bloch sphere is given by

$$\begin{aligned}\big[\mathrm{R}_x(\tau)|\psi\rangle\big] &= \cos\phi\sin\theta\,\boldsymbol{i} + (\cos\tau\sin\phi\sin\theta - \sin\tau\cos\theta)\boldsymbol{j} \\ &\quad + (\sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta)\boldsymbol{k} \\ &= \cos\varphi\sin\vartheta\,\boldsymbol{i} + \sin\varphi\sin\vartheta\,\boldsymbol{j} + \cos\vartheta\,\boldsymbol{k}\end{aligned}$$

for some φ and ϑ. Then

$$\cos^2\frac{\vartheta}{2} = \frac{1+\sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta}{2}. \tag{3}$$

Next we show that $\mathrm{R}_x(\tau)$ with matrix representation given by (2a) indeed has the property that for some $\delta \in \mathbb{R}$,

$$\mathrm{R}_x(\tau)|\psi\rangle = e^{i\delta}\Big(\cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle\Big).$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Suppose that in Cartesian coordinate the state $\mathrm{R}_x(\tau)|\psi\rangle$ on the Bloch sphere is given by

$$\begin{aligned}[\mathrm{R}_x(\tau)|\psi\rangle] &= \cos\phi\sin\theta\boldsymbol{i} + (\cos\tau\sin\phi\sin\theta - \sin\tau\cos\theta)\boldsymbol{j} \\ &\quad + (\sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta)\boldsymbol{k} \\ &= \cos\varphi\sin\vartheta\boldsymbol{i} + \sin\varphi\sin\vartheta\boldsymbol{j} + \cos\vartheta\boldsymbol{k}\end{aligned}$$

for some φ and ϑ. Then

$$\cos^2\frac{\vartheta}{2} = \frac{1 + \sin\tau\sin\phi\sin\theta + \cos\tau\cos\theta}{2}. \tag{3}$$

Next we show that $\mathrm{R}_x(\tau)$ with matrix representation given by (2a) indeed has the property that for some $\delta \in \mathbb{R}$,

$$\mathrm{R}_x(\tau)|\psi\rangle = e^{i\delta}\Big(\cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle\Big).$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Expanding the product

$$\begin{bmatrix} \cos\frac{\tau}{2} & -i\sin\frac{\tau}{2} \\ -i\sin\frac{\tau}{2} & \cos\frac{\tau}{2} \end{bmatrix} \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix},$$

it is to show that there exists $\delta \in \mathbb{R}$ such that

$$\cos\frac{\tau}{2}\cos\frac{\theta}{2} - i\sin\frac{\tau}{2}e^{i\phi}\sin\frac{\theta}{2} = e^{i\delta}\cos\frac{\vartheta}{2}, \tag{4a}$$

$$-i\sin\frac{\tau}{2}\cos\frac{\theta}{2} + \cos\frac{\tau}{2}e^{i\phi}\sin\frac{\theta}{2} = e^{i(\delta+\varphi)}\sin\frac{\vartheta}{2}, \tag{4b}$$

or

$$\cos\frac{\tau}{2}\cos\frac{\theta}{2} + \sin\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2} - i\cos\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2} = e^{i\delta}\cos\frac{\vartheta}{2},$$

$$\cos\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2} + i\Big(\sin\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2} - \cos\frac{\theta}{2}\sin\frac{\tau}{2}\Big) = e^{i(\delta+\varphi)}\sin\frac{\vartheta}{2}. \quad \square$$

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Using (3),

$$\begin{aligned}
&\Big(\cos\frac{\tau}{2}\cos\frac{\theta}{2}+\sin\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2}\Big)^2+\cos^2\phi\sin^2\frac{\tau}{2}\sin^2\frac{\theta}{2}\\
&\quad=\cos^2\frac{\tau}{2}\cos^2\frac{\theta}{2}+\sin^2\frac{\tau}{2}\sin^2\frac{\theta}{2}+2\cos\frac{\tau}{2}\cos\frac{\theta}{2}\sin\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2}\\
&\quad=\frac{(1+\cos\tau)(1+\cos\theta)+(1-\cos\tau)(1-\cos\theta)}{4}+\frac{\sin\phi\sin\tau\sin\theta}{2}\\
&\quad=\frac{1+\cos\tau\cos\theta+\sin\phi\sin\tau\sin\theta}{2}=\cos^2\frac{\vartheta}{2}\,;
\end{aligned}$$

thus there exists $\delta\in\mathbb{R}$ such that

$$\cos\frac{\tau}{2}\cos\frac{\theta}{2}+\sin\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2}-i\cos\phi\sin\frac{\tau}{2}\sin\frac{\theta}{2}=e^{i\delta}\cos\frac{\vartheta}{2}\,;$$

thus (4a) holds. □

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Moreover, by the fact that $\mathrm{R}_x(\tau)$ given by (2a) is unitary,

$$\left|\cos\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}+i\Big(\sin\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}-\cos\frac{\theta}{2}\sin\frac{\tau}{2}\Big)\right|^2=\sin^2\frac{\vartheta}{2}\,.$$

Therefore, for some $\eta\in\mathbb{R}$ we have

$$\cos\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}+i\Big(\sin\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}-\cos\frac{\theta}{2}\sin\frac{\tau}{2}\Big)=e^{i\eta}\sin\frac{\vartheta}{2}. \quad (5)$$

To show (4b) it suffices to extract the phase information. Computing the product of (5) and the complex conjugate of (4a), we obtain that

$$\begin{aligned}\frac{1}{2}e^{i(\eta-\delta)}\sin\vartheta &= e^{i\eta}\sin\frac{\vartheta}{2}\,e^{-i\delta}\cos\frac{\vartheta}{2}\\ &=\frac{1}{2}\Big[\cos\phi\sin\theta+i(\sin\phi\cos\tau\sin\theta-\cos\theta\sin\tau)\Big]\,.\end{aligned}$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Moreover, by the fact that $\mathrm{R}_x(\tau)$ given by (2a) is unitary,

$$\Big|\cos\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}+i\big(\sin\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}-\cos\frac{\theta}{2}\sin\frac{\tau}{2}\big)\Big|^2=\sin^2\frac{\vartheta}{2}\,.$$

Therefore, for some $\eta\in\mathbb{R}$ we have

$$\cos\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}+i\big(\sin\phi\cos\frac{\tau}{2}\sin\frac{\theta}{2}-\cos\frac{\theta}{2}\sin\frac{\tau}{2}\big)=e^{i\eta}\sin\frac{\vartheta}{2}. \quad (5)$$

To show (4b) it suffices to extract the phase information. Computing the product of (5) and the complex conjugate of (4a), we obtain that

$$\begin{aligned}\frac{1}{2}e^{i(\eta-\delta)}\sin\vartheta &= e^{i\eta}\sin\frac{\vartheta}{2}\,e^{-i\delta}\cos\frac{\vartheta}{2}\\ &=\frac{1}{2}\big[\cos\phi\sin\theta+i(\sin\phi\cos\tau\sin\theta-\cos\theta\sin\tau)\big]\,.\end{aligned}$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Comparing with the first two component of $[\mathrm{R}_x(\tau)|\psi\rangle]$,

$$\begin{aligned} e^{i(\eta-\delta)}\sin\vartheta &= \cos\phi\sin\theta + i(\sin\phi\cos\tau\sin\theta - \cos\theta\sin\tau) \\ &= \cos\varphi\sin\vartheta + i\sin\varphi\sin\vartheta = e^{i\varphi}\sin\vartheta\,; \end{aligned}$$

thus $e^{i\eta} = e^{i(\delta+\varphi)}$ in (5) so that (4b) holds.

2. The proof of this part is similar to the one in the first part, and the proof is left as an exercise.
3. It is clear that $\mathrm{R}_z(\tau)$ maps $|\psi\rangle$ to the quantum state

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

Therefore, the matrix representations of $\mathrm{R}_z(\tau)$ is given by

$$\mathrm{R}_z(\tau) = \begin{bmatrix} e^{-i\tau/2} & 0 \\ 0 & e^{i\tau/2} \end{bmatrix}.$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Comparing with the first two component of $[\mathrm{R}_x(\tau)|\psi\rangle]$,

$$e^{i(\eta-\delta)}\sin\vartheta = \cos\phi\sin\theta + i(\sin\phi\cos\tau\sin\theta - \cos\theta\sin\tau)$$
$$= \cos\varphi\sin\vartheta + i\sin\varphi\sin\vartheta = e^{i\varphi}\sin\vartheta\,;$$

thus $e^{i\eta} = e^{i(\delta+\varphi)}$ in (5) so that (4b) holds.

2. The proof of this part is similar to the one in the first part, and the proof is left as an exercise.

3. It is clear that $\mathrm{R}_z(\tau)$ maps $|\psi\rangle$ to the quantum state

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

Therefore, the matrix representations of $\mathrm{R}_z(\tau)$ is given by

$$\mathrm{R}_z(\tau) = \begin{bmatrix} e^{-i\tau/2} & 0 \\ 0 & e^{i\tau/2} \end{bmatrix}.$$

□

§2.2 Qubits and Quantum Gates

Proof (cont'd).

Comparing with the first two component of $[\mathrm{R}_x(\tau)|\psi\rangle]$,

$$e^{i(\eta-\delta)}\sin\vartheta = \cos\phi\sin\theta + i(\sin\phi\cos\tau\sin\theta - \cos\theta\sin\tau)$$
$$= \cos\varphi\sin\vartheta + i\sin\varphi\sin\vartheta = e^{i\varphi}\sin\vartheta\,;$$

thus $e^{i\eta} = e^{i(\delta+\varphi)}$ in (5) so that (4b) holds.

2. The proof of this part is similar to the one in the first part, and the proof is left as an exercise.
3. It is clear that $\mathrm{R}_z(\tau)$ maps $|\psi\rangle$ to the quantum state

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

Therefore, the matrix representations of $\mathrm{R}_z(\tau)$ is given by

$$\mathrm{R}_z(\tau) = \begin{bmatrix} e^{-i\tau/2} & 0 \\ 0 & e^{i\tau/2} \end{bmatrix}.$$

□

§2.2 Qubits and Quantum Gates

For a 2×2 matrix A (with complex entries) satisfying $A^2 = \mathrm{I}$,

$$e^{iAx} = \sum_{k=0}^{\infty} \frac{(iAx)^k}{k!} = \sum_{k=0}^{\infty} \frac{i^{2k} A^{2k} x^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{i^{2k+1} A^{2k+1} x^{2k+1}}{(2k+1)!}$$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!} \mathrm{I} + i \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!} A = \cos x \mathrm{I} + i \sin x A\,.$$

Using the notation of exponential, we find the matrix representation of $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ given in (2) in fact can be expressed as

$$\mathrm{R}_x(\tau) = \exp\Big(\frac{-i\tau \mathrm{X}}{2}\Big), \ \mathrm{R}_y(\tau) = \exp\Big(\frac{-i\tau \mathrm{Y}}{2}\Big), \ \mathrm{R}_z(\tau) = \exp\Big(\frac{-i\tau \mathrm{Z}}{2}\Big).$$

Note that for a unit vector $\boldsymbol{a} = (a_x, a_y, a_z)$ in $\mathbb{R}^3$,

$$\begin{aligned}(a_x \mathrm{X} + a_y \mathrm{Y} + a_z \mathrm{Z})^2 &= a_x^2 \mathrm{X}^2 + a_y^2 \mathrm{Y}^2 + a_z^2 \mathrm{Z}^2 + a_x a_y (\mathrm{XY} + \mathrm{YX}) \\ &\quad + a_x a_z (\mathrm{XZ} + \mathrm{ZX}) + a_y a_x (\mathrm{YZ} + \mathrm{ZY}) \\ &= (a_x^2 + a_y^2 + a_z^2)\mathrm{I} = \mathrm{I}\,.\end{aligned}$$

§2.2 Qubits and Quantum Gates

For a 2×2 matrix A (with complex entries) satisfying $A^2 = \mathrm{I}$,

$$e^{iAx} = \sum_{k=0}^{\infty} \frac{(iAx)^k}{k!} = \sum_{k=0}^{\infty} \frac{i^{2k}A^{2k}x^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{i^{2k+1}A^{2k+1}x^{2k+1}}{(2k+1)!}$$

$$= \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!}\mathrm{I} + i\sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!}A = \cos x\,\mathrm{I} + i\sin x\,A\,.$$

Using the notation of exponential, we find the matrix representation of $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ given in (2) in fact can be expressed as

$$\mathrm{R}_x(\tau) = \exp\Big(\frac{-i\tau\mathrm{X}}{2}\Big),\ \mathrm{R}_y(\tau) = \exp\Big(\frac{-i\tau\mathrm{Y}}{2}\Big),\ \mathrm{R}_z(\tau) = \exp\Big(\frac{-i\tau\mathrm{Z}}{2}\Big).$$

Note that for a unit vector $\boldsymbol{a} = (a_x, a_y, a_z)$ in $\mathbb{R}^3$,

$$(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})^2 = a_x^2\mathrm{X}^2 + a_y^2\mathrm{Y}^2 + a_z^2\mathrm{Z}^2 + a_xa_y(\mathrm{XY}+\mathrm{YX})$$
$$+a_xa_z(\mathrm{XZ}+\mathrm{ZX}) + a_ya_x(\mathrm{YZ}+\mathrm{ZY})$$
$$= (a_x^2 + a_y^2 + a_z^2)\mathrm{I} = \mathrm{I}\,.$$

§2.2 Qubits and Quantum Gates

For a 2×2 matrix A (with complex entries) satisfying $A^2 = \mathrm{I}$,

$$e^{iAx} = \sum_{k=0}^{\infty} \frac{(iAx)^k}{k!} = \sum_{k=0}^{\infty} \frac{i^{2k}A^{2k}x^{2k}}{(2k)!} + \sum_{k=0}^{\infty} \frac{i^{2k+1}A^{2k+1}x^{2k+1}}{(2k+1)!}$$
$$= \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k}}{(2k)!}\mathrm{I} + i\sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!}A = \cos x\,\mathrm{I} + i\sin x\,A\,.$$

Using the notation of exponential, we find the matrix representation of $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ given in (2) in fact can be expressed as

$$\mathrm{R}_x(\tau) = \exp\Big(\frac{-i\tau\mathrm{X}}{2}\Big),\ \mathrm{R}_y(\tau) = \exp\Big(\frac{-i\tau\mathrm{Y}}{2}\Big),\ \mathrm{R}_z(\tau) = \exp\Big(\frac{-i\tau\mathrm{Z}}{2}\Big).$$

Note that for a unit vector $\boldsymbol{a} = (a_x, a_y, a_z)$ in $\mathbb{R}^3$,

$$(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})^2 = a_x^2\mathrm{X}^2 + a_y^2\mathrm{Y}^2 + a_z^2\mathrm{Z}^2 + a_xa_y(\mathrm{XY} + \mathrm{YX})$$
$$+ a_xa_z(\mathrm{XZ} + \mathrm{ZX}) + a_ya_x(\mathrm{YZ} + \mathrm{ZY})$$
$$= (a_x^2 + a_y^2 + a_z^2)\mathrm{I} = \mathrm{I}\,.$$

§2.2 Qubits and Quantum Gates

We now define the rotation about any axis.

Definition

For a general unit vector $\boldsymbol{a} = (a_x, a_y, a_z)$ in $\mathbb{R}^3$, the rotation of an 1-qubit state by angle ϕ about an axis in direction $\boldsymbol{a}$, denoted by $R_{\boldsymbol{a}}(\phi)$, is a 1-qubit quantum gate given by

$$\begin{aligned} R_{\boldsymbol{a}}(\phi) &= \exp\Big(-\frac{i\phi}{2}(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})\Big) \\ &= \cos\frac{\phi}{2}\mathrm{I} - i\sin\frac{\phi}{2}(a_x\mathrm{X} + a_y\mathrm{Y} + a_z\mathrm{Z})\,. \end{aligned}$$

The matrix representation of $R_{\boldsymbol{a}}(\phi)$ is given by

$$R_{\boldsymbol{a}}(\phi) = \begin{bmatrix} \cos\frac{\phi}{2} - ia_z\sin\frac{\phi}{2} & -(a_y + ia_x)\sin\frac{\phi}{2} \\ (a_y - ia_x)\sin\frac{\phi}{2} & \cos\frac{\phi}{2} + ia_z\sin\frac{\phi}{2} \end{bmatrix}.$$

§2.2 Qubits and Quantum Gates

Next we consider quantum gates acting on more than one qubit. An example of a 2-qubit gate is the the controlled-not gate **CNOT**. It negates the second bit of its input if the first bit is 1, and does nothing if first bit is 0:

$$\mathbf{CNOT}|ab\rangle = |a\rangle \otimes |a \oplus b\rangle \qquad \forall\, a, b \in \{0, 1\}\,.$$

Since the first qubit controls what action is applied to the second qubit, the first qubit is called the ***control qubit***, and the second qubit is called the ***target qubit***.

The matrix form of $\mathbf{CNOT}$ gate is $\mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ since

$$\mathbf{CNOT}|00\rangle = |00\rangle\,, \quad \mathbf{CNOT}|01\rangle = |01\rangle\,,$$
$$\mathbf{CNOT}|10\rangle = |11\rangle\,, \quad \mathbf{CNOT}|11\rangle = |10\rangle\,.$$

§2.2 Qubits and Quantum Gates

Next we consider quantum gates acting on more than one qubit. An example of a 2-qubit gate is the the controlled-not gate **CNOT**. It negates the second bit of its input if the first bit is 1, and does nothing if first bit is 0:

$$\mathbf{CNOT}|ab\rangle = |a\rangle \otimes |a \oplus b\rangle \qquad \forall\, a, b \in \{0, 1\}\,.$$

Since the first qubit controls what action is applied to the second qubit, the first qubit is called the ***control qubit***, and the second qubit is called the ***target qubit***.

The matrix form of $\mathbf{CNOT}$ gate is $\mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ since

$$\mathbf{CNOT}|00\rangle = |00\rangle\,, \quad \mathbf{CNOT}|01\rangle = |01\rangle\,,$$
$$\mathbf{CNOT}|10\rangle = |11\rangle\,, \quad \mathbf{CNOT}|11\rangle = |10\rangle\,.$$

§2.2 Qubits and Quantum Gates

Next we consider quantum gates acting on more than one qubit. An example of a 2-qubit gate is the the controlled-not gate **CNOT**. It negates the second bit of its input if the first bit is 1, and does nothing if first bit is 0:

$$\mathbf{CNOT}|ab\rangle = |a\rangle \otimes |a \oplus b\rangle \qquad \forall\, a, b \in \{0, 1\}\,.$$

Since the first qubit controls what action is applied to the second qubit, the first qubit is called the ***control qubit***, and the second qubit is called the ***target qubit***.

The matrix form of $\mathbf{CNOT}$ gate is $\mathbf{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ since

$$\mathbf{CNOT}|00\rangle = |00\rangle\,, \quad \mathbf{CNOT}|01\rangle = |01\rangle\,,$$
$$\mathbf{CNOT}|10\rangle = |11\rangle\,, \quad \mathbf{CNOT}|11\rangle = |10\rangle\,.$$

§2.2 Qubits and Quantum Gates

More generally, if U is some 1-qubit gate, the 2-qubit controlled-U gate given by

$$|ab\rangle \mapsto |a\rangle \otimes \big((1 \oplus a)|b\rangle + aU|b\rangle\big) \qquad \forall\, a, b \in \{0, 1\}$$

or more precisely,

$$|0b\rangle \mapsto |0b\rangle \quad \text{and} \quad |1b\rangle \mapsto |1\rangle \otimes U|b\rangle \qquad \forall\, b \in \{0, 1\}$$

corresponds to the following 4×4 matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}.$$

§2.2 Qubits and Quantum Gates

Adding another control qubit to **CNOT**, we get the 3-qubit Toffoli gate, also called controlled-controlled-not (**CCNOT**) gate, which negates the third bit of its input if both of the first two bits are 1:

$$\mathbf{CCNOT}|abc\rangle = |ab\rangle \otimes |ab \oplus c\rangle \qquad \forall\, a, b, c \in \{0, 1\}\,.$$

The matrix form of $\mathbf{CCNOT}$ gate is

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

The Toffoli gate is important because it is complete for classical reversible computation. We will see other quantum gates later.

§2.2 Qubits and Quantum Gates

Adding another control qubit to **CNOT**, we get the 3-qubit Toffoli gate, also called controlled-controlled-not (**CCNOT**) gate, which negates the third bit of its input if both of the first two bits are 1:

$$\mathbf{CCNOT}|abc\rangle = |ab\rangle \otimes |ab \oplus c\rangle \qquad \forall\, a, b, c \in \{0, 1\}\,.$$

The matrix form of $\mathbf{CCNOT}$ gate is

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

The Toffoli gate is important because it is complete for classical reversible computation. We will see other quantum gates later.

§2.2 Qubits and Quantum Gates

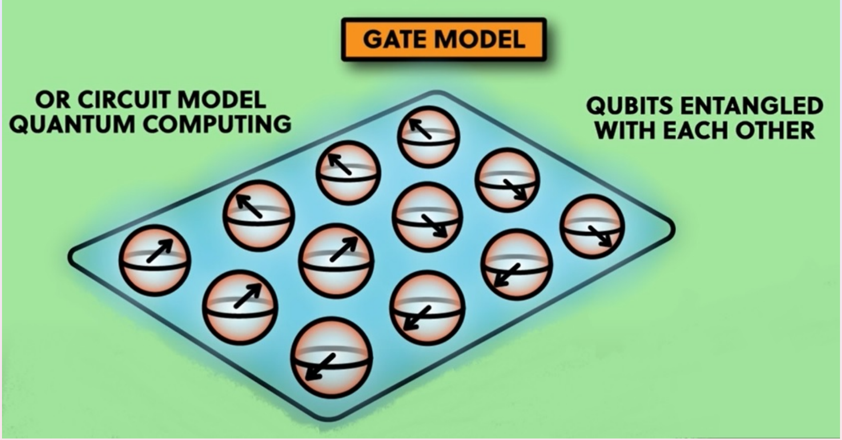


Figure 1: Gate model or circuit model of quantum computing - it consists of a lot of qubits, each qubit represents a digit of a number, and qubits are manipulated using quantum gates.

§2.3 Quantum Registers

A quantum register is a system comprising multiple qubits. It is the quantum analog of the classical processor register. Quantum computers perform calculations by manipulating qubits within a quantum register.

Classically, information is represented by finite chunks of bits. These are essentially words $(x_1, x_2, x_3, \cdots, x_n)$ built from the alphabet $\{0, 1\}$; that is, $x_\ell \in \{0, 1\}$ for all $1 \leqslant \ell \leqslant n$. Hence, we need 2^n classical storage configurations in order to represent all such words.

Remark: There is a conceptual difference between the quantum and classical register. A classical register of n bits refers to an array of n flip flops (flip flops - 可儲存 0 或 1 狀態的電路), while a quantum register of n qubits is merely a collection of n qubits.

§2.3 Quantum Registers

A quantum register is a system comprising multiple qubits. It is the quantum analog of the classical processor register. Quantum computers perform calculations by manipulating qubits within a quantum register.

Classically, information is represented by finite chunks of bits. These are essentially words $(x_1, x_2, x_3, \cdots, x_n)$ built from the alphabet $\{0, 1\}$; that is, $x_\ell \in \{0, 1\}$ for all $1 \leqslant \ell \leqslant n$. Hence, we need 2^n classical storage configurations in order to represent all such words.

Remark: There is a conceptual difference between the quantum and classical register. A classical register of n bits refers to an array of n flip flops (flip flops - 可儲存 0 或 1 狀態的電路), while a quantum register of n qubits is merely a collection of n qubits.

§2.3 Quantum Registers

A classical two-bit word (x_1, x_2) is an element of the set $\{0,1\} \times \{0,1\} = \{0,1\}^2$, and classically we can represent the words 00, 01, 10, 11 by storing the first letter x_1 (the first bit or the highest bit) and the second letter x_2 (the second bit) accordingly. If we represent each of these bits quantum mechanically by qubits, we are dealing with a two-qubit quantum system composed of two quantum mechanical sub-systems. A two-qubit word in a two-quit quantum system is in superposition

$$\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$, and $|x_1x_2\rangle$ denotes the state that the first qubit is in state $|x_1\rangle$ and the second qubit is in state $|x_2\rangle$.

§2.3 Quantum Registers

A classical two-bit word (x_1, x_2) is an element of the set $\{0,1\} \times \{0,1\} = \{0,1\}^2$, and classically we can represent the words 00, 01, 10, 11 by storing the first letter x_1 (the first bit or the highest bit) and the second letter x_2 (the second bit) accordingly. If we represent each of these bits quantum mechanically by qubits, we are dealing with a two-qubit quantum system composed of two quantum mechanical sub-systems. A two-qubit word in a two-quit quantum system is in superposition

$$\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$, and $|x_1x_2\rangle$ denotes the state that the first qubit is in state $|x_1\rangle$ and the second qubit is in state $|x_2\rangle$.

§2.3 Quantum Registers

A classical two-bit word (x_1, x_2) is an element of the set $\{0,1\} \times \{0,1\} = \{0,1\}^2$, and classically we can represent the words 00, 01, 10, 11 by storing the first letter x_1 (the first bit or the highest bit) and the second letter x_2 (the second bit) accordingly. If we represent each of these bits quantum mechanically by qubits, we are dealing with a two-qubit quantum system composed of two quantum mechanical sub-systems. A two-qubit word in a two-quit quantum system is in superposition

$$\alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle,$$

where $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$, and $|x_1 x_2\rangle$ denotes the state that the first qubit is in state $|x_1\rangle$ and the second qubit is in state $|x_2\rangle$.

§2.3 Quantum Registers

More generally, a quantum register of n qubits has 2^n basis states of the form $|b_1 b_2 \cdots b_n\rangle$. Since bitstrings of length n can be viewed as numbers between 0 and 2^n-1, we can also write the basis states as numbers $|0\rangle$, $|1\rangle$, $|2\rangle$, $\cdots$, $|2^n-1\rangle$. In other words, for $b = b_1 b_2 \cdots b_n \in \{0,1\}^n$ we often use $|b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n\rangle$ to identify $|b_1 b_2 \cdots b_n\rangle$ (recall that $b_1 b_2 \cdots b_n$ in binary equals $b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n$ in decimal). A quantum register of n qubits can be in any superposition

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n-1\rangle = \sum_{j=0}^{2^n-1} \alpha_j|j\rangle,$$

where $\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$. The superposition above sometimes is also written as $\sum_{j\in\{0,1\}^n} \alpha_j|j\rangle$.

§2.3 Quantum Registers

More generally, a quantum register of n qubits has 2^n basis states of the form $|b_1 b_2 \cdots b_n\rangle$. Since bitstrings of length n can be viewed as numbers between 0 and $2^n - 1$, we can also write the basis states as numbers $|0\rangle$, $|1\rangle$, $|2\rangle$, $\cdots$, $|2^n - 1\rangle$. In other words, for $b = b_1 b_2 \cdots b_n \in \{0,1\}^n$ we often use $|b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n\rangle$ to identify $|b_1 b_2 \cdots b_n\rangle$ (recall that $b_1 b_2 \cdots b_n$ in binary equals $b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n$ in decimal). A quantum register of n qubits can be in any superposition

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n - 1\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle,$$

where $\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$. The superposition above sometimes is also written as $\sum_{j \in \{0,1\}^n} \alpha_j |j\rangle$.

§2.3 Quantum Registers

More generally, a quantum register of n qubits has 2^n basis states of the form $|b_1 b_2 \cdots b_n\rangle$. Since bitstrings of length n can be viewed as numbers between 0 and 2^n-1, we can also write the basis states as numbers $|0\rangle$, $|1\rangle$, $|2\rangle$, $\cdots$, $|2^n-1\rangle$. In other words, for $b = b_1 b_2 \cdots b_n \in \{0,1\}^n$ we often use $|b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n\rangle$ to identify $|b_1 b_2 \cdots b_n\rangle$ (recall that $b_1 b_2 \cdots b_n$ in binary equals $b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n$ in decimal). A quantum register of n qubits can be in any superposition

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n-1\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle,$$

where $\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$. The superposition above sometimes is also written as $\sum_{j\in\{0,1\}^n} \alpha_j |j\rangle$.

§2.3 Quantum Registers

More generally, a quantum register of n qubits has 2^n basis states of the form $|b_1 b_2 \cdots b_n\rangle$. Since bitstrings of length n can be viewed as numbers between 0 and 2^n-1, we can also write the basis states as numbers $|0\rangle$, $|1\rangle$, $|2\rangle$, $\cdots$, $|2^n-1\rangle$. In other words, for $b = b_1 b_2 \cdots b_n \in \{0,1\}^n$ we often use $|b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n\rangle$ to identify $|b_1 b_2 \cdots b_n\rangle$ (recall that $b_1 b_2 \cdots b_n$ in binary equals $b_1 2^{n-1} + b_2 2^{n-2} + \cdots + b_n$ in decimal). A quantum register of n qubits can be in any superposition

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n-1\rangle = \sum_{j=0}^{2^n-1} \alpha_j |j\rangle,$$

where $\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$. The superposition above sometimes is also written as $\sum_{j\in\{0,1\}^n} \alpha_j |j\rangle$.

§2.3 Quantum Registers

In an n-qubit quantum system, one can perform measurement on certain qubits. A measuement of m qubits, where $m < n$, is a projective measurement, and the quantum register

$$\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n - 1\rangle$$

under such a projective measurement collapses to another quantum register

$$\beta_0|0\rangle + \beta_1|1\rangle + \cdots + \beta_{2^n-1}|2^n - 1\rangle,$$

where at most 2^{n-m} β_j's are non-zero, and $\beta_0, \beta_1, \cdots, \beta_{2^n-1}$ are determined by the outcomes of the measurement, the exact position of the qubits on which the measurement is performed, and α_0, α_1, $\cdots$, α_{2^n-1}.

§2.3 Quantum Registers

Example

Suppose we perform a (projective) measurement on the second qubit of the 3-qubit register

$$\alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle$$
$$+\alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle$$

and obtain value 0, then the 3-qubit register above collapses to the quantum register

$$\frac{\alpha_0}{\|\boldsymbol{\alpha}\|}|000\rangle + \frac{\alpha_1}{\|\boldsymbol{\alpha}\|}|001\rangle + \frac{\alpha_4}{\|\boldsymbol{\alpha}\|}|100\rangle + \frac{\alpha_5}{\|\boldsymbol{\alpha}\|}|101\rangle$$

where $\|\boldsymbol{\alpha}\| = \sqrt{|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_4|^2 + |\alpha_5|^2}$.

§2.3 Quantum Registers

§2.3.1 Tensor products - preview

Suppose that two single qubit states $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ are given, and a quantum register of two qubits is formed from these two single qubits: the output of the first and the second qubit of the quantum register upon measurement follows the distribution given by states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively. Therefore, measuring this quantum register of two qubits gives $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ with probability $|\alpha_0\beta_0|^2$, $|\alpha_0\beta_1|^2$, $|\alpha_1\beta_0|^2$ and $|\alpha_1\beta_2|^2$, respectively. This motivates us to consider the quantum state of two qubits

$$|\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\,.$$

We will write the quantum state $|\psi\rangle$ above as $|\psi_1\rangle \otimes |\psi_2\rangle$, called the **tensor product** of states $|\psi_1\rangle$ and $|\psi_2\rangle$.

§2.3 Quantum Registers

§2.3.1 Tensor products - preview

Suppose that two single qubit states $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ are given, and a quantum register of two qubits is formed from these two single qubits: the output of the first and the second qubit of the quantum register upon measurement follows the distribution given by states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively. Therefore, measuring this quantum register of two qubits gives $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ with probability $|\alpha_0\beta_0|^2$, $|\alpha_0\beta_1|^2$, $|\alpha_1\beta_0|^2$ and $|\alpha_1\beta_2|^2$, respectively. This motivates us to consider the quantum state of two qubits

$$|\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle .$$

We will write the quantum state $|\psi\rangle$ above as $|\psi_1\rangle \otimes |\psi_2\rangle$, called the **tensor product** of states $|\psi_1\rangle$ and $|\psi_2\rangle$.

§2.3 Quantum Registers

§2.3.1 Tensor products - preview

Suppose that two single qubit states $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$ are given, and a quantum register of two qubits is formed from these two single qubits: the output of the first and the second qubit of the quantum register upon measurement follows the distribution given by states $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively. Therefore, measuring this quantum register of two qubits gives $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ with probability $|\alpha_0\beta_0|^2$, $|\alpha_0\beta_1|^2$, $|\alpha_1\beta_0|^2$ and $|\alpha_1\beta_2|^2$, respectively. This motivates us to consider the quantum state of two qubits

$$|\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle .$$

We will write the quantum state $|\psi\rangle$ above as $|\psi_1\rangle \otimes |\psi_2\rangle$, called the **tensor product** of states $|\psi_1\rangle$ and $|\psi_2\rangle$.

§2.3 Quantum Registers

In general, let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two quantum states of n qubits and m qubits, respectively. The tensor product of $|\psi_1\rangle$ and $|\psi_2\rangle$ is a quantum state of $(n+m)$ qubits. Let us first consider the "continuous" case to illustrate the idea of the tensor product. Suppose that the states of two non-relativistic particles of the same mass m, labeled as particle 1 and particle 2, are described by Schrödinger equations

$$i\hbar\frac{\partial}{\partial t}\psi_1 = \Big(-\frac{\hbar}{2m}\Delta + V_1\Big)\psi_1 \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\}$$

and

$$i\hbar\frac{\partial}{\partial t}\psi_2 = \Big(-\frac{\hbar}{2m}\Delta + V_2\Big)\psi_2 \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\},$$

respectively. Then at time t the probability of the presence of particle 1 at location x and particle 2 at location y is given by $\big|\psi_1(x,t)\big|^2\big|\psi_2(y,t)\big|^2 = \big|\psi_1(x,t)\psi_2(y,t)\big|^2$.

§2.3 Quantum Registers

In general, let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two quantum states of n qubits and m qubits, respectively. The tensor product of $|\psi_1\rangle$ and $|\psi_2\rangle$ is a quantum state of $(n+m)$ qubits. Let us first consider the "continuous" case to illustrate the idea of the tensor product. Suppose that the states of two non-relativistic particles of the same mass m, labeled as particle 1 and particle 2, are described by Schrödinger equations

$$i\hbar\frac{\partial}{\partial t}\psi_1 = \Big(-\frac{\hbar}{2m}\Delta + V_1\Big)\psi_1 \qquad \text{in} \quad \mathbb{R}^n \times \{t>0\}$$

and

$$i\hbar\frac{\partial}{\partial t}\psi_2 = \Big(-\frac{\hbar}{2m}\Delta + V_2\Big)\psi_2 \qquad \text{in} \quad \mathbb{R}^n \times \{t>0\}\,,$$

respectively. Then at time t the probability of the presence of particle 1 at location x and particle 2 at location y is given by $\big|\psi_1(x,t)\big|^2\big|\psi_2(y,t)\big|^2 = \big|\psi_1(x,t)\psi_2(y,t)\big|^2$.

§2.3 Quantum Registers

In general, let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two quantum states of n qubits and m qubits, respectively. The tensor product of $|\psi_1\rangle$ and $|\psi_2\rangle$ is a quantum state of $(n+m)$ qubits. Let us first consider the "continuous" case to illustrate the idea of the tensor product. Suppose that the states of two non-relativistic particles of the same mass m, labeled as particle 1 and particle 2, are described by Schrödinger equations

$$i\hbar\frac{\partial}{\partial t}\psi_1 = \Big(-\frac{\hbar}{2m}\Delta + V_1\Big)\psi_1 \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\}$$

and

$$i\hbar\frac{\partial}{\partial t}\psi_2 = \Big(-\frac{\hbar}{2m}\Delta + V_2\Big)\psi_2 \qquad \text{in} \quad \mathbb{R}^n \times \{t > 0\}\,,$$

respectively. Then at time t the probability of the presence of particle 1 at location x and particle 2 at location y is given by $\big|\psi_1(x,t)\big|^2\big|\psi_2(y,t)\big|^2 = \big|\psi_1(x,t)\psi_2(y,t)\big|^2$.

§2.3 Quantum Registers

This motivates of considering the function $\psi(x, y, t) = \psi_1(x, t)\psi_2(y, t)$. This function ψ satisfies

$$i\hbar \frac{\partial}{\partial t}\psi = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi \qquad \text{in} \quad \mathbb{R}^n \times \mathbb{R}^n \times \{t > 0\}\,,$$

where $V(x, y, t) = V_1(x, t) + V_2(y, t)$ and

$$(\Delta\psi)(x, y, t) = (\Delta_x + \Delta_y)\psi(x, y, t)\,.$$

If there is no interference between the two particles (which is the case if V_1 and V_2 satisfy certain conditions), then the state of the "combined system" (meaning that we use $(x, y) \in \mathbb{R}^n \times \mathbb{R}^n$ to write the position of these two particles) is described by the wave function ψ. In other words, the state of the combined system is simply the "product" (which is exactly the tensor product) of the individual states.

§2.3 Quantum Registers

This motivates of considering the function $\psi(x, y, t) = \psi_1(x, t)\psi_2(y, t)$. This function ψ satisfies

$$i\hbar\frac{\partial}{\partial t}\psi = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi \qquad \text{in} \quad \mathbb{R}^n \times \mathbb{R}^n \times \{t > 0\},$$

where $V(x, y, t) = V_1(x, t) + V_2(y, t)$ and

$$(\Delta\psi)(x, y, t) = (\Delta_x + \Delta_y)\psi(x, y, t).$$

If there is no interference between the two particles (which is the case if V_1 and V_2 satisfy certain conditions), then the state of the "combined system" (meaning that we use $(x, y) \in \mathbb{R}^n \times \mathbb{R}^n$ to write the position of these two particles) is described by the wave function ψ. In other words, the state of the combined system is simply the "product" (which is exactly the tensor product) of the individual states.

§2.3 Quantum Registers

This motivates of considering the function $\psi(x, y, t) = \psi_1(x, t)\psi_2(y, t)$. This function ψ satisfies

$$i\hbar \frac{\partial}{\partial t}\psi = \Big(-\frac{\hbar}{2m}\Delta + V\Big)\psi \qquad \text{in} \quad \mathbb{R}^n \times \mathbb{R}^n \times \{t > 0\}\,,$$

where $V(x, y, t) = V_1(x, t) + V_2(y, t)$ and

$$(\Delta\psi)(x, y, t) = (\Delta_x + \Delta_y)\psi(x, y, t)\,.$$

If there is no interference between the two particles (which is the case if V_1 and V_2 satisfy certain conditions), then the state of the "combined system" (meaning that we use $(x, y) \in \mathbb{R}^n \times \mathbb{R}^n$ to write the position of these two particles) is described by the wave function ψ. In other words, the state of the combined system is simply the "product" (which is exactly the tensor product) of the individual states.

§2.3 Quantum Registers

Now suppose the states of two qubits are given by $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. Recall that this is a shorthand notation for the quantum states

$$\psi_1(x_1) = \begin{cases} \alpha_0 & \text{if } x_1 = 0\,, \\ \alpha_1 & \text{if } x_1 = 1\,, \end{cases} \quad \text{and} \quad \psi_2(x_2) = \begin{cases} \beta_0 & \text{if } x_2 = 0\,, \\ \beta_1 & \text{if } x_2 = 1\,, \end{cases}$$

Then the state of the combined system (which can be used to describe for random numbers $(0)_{10} = (00)_2$, $(1)_{10} = (01)_2$, $(2)_{10} = (10)_2$ and $(3)_{10} = (11)_2$) is given by

$$\psi(x_1, x_2) \equiv \psi_1(x_1)\psi_2(x_2) = \begin{cases} \alpha_0\beta_0 & \text{if } (x_1, x_2) = (0,0)\,, \\ \alpha_0\beta_1 & \text{if } (x_1, x_2) = (0,1)\,, \\ \alpha_1\beta_0 & \text{if } (x_1, x_2) = (1,0)\,, \\ \alpha_1\beta_1 & \text{if } (x_1, x_2) = (1,1)\,, \end{cases}$$

which is abbreviated as

$$|\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\,.$$

§2.3 Quantum Registers

Now suppose the states of two qubits are given by $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$. Recall that this is a shorthand notation for the quantum states

$$\psi_1(x_1) = \begin{cases} \alpha_0 & \text{if } x_1 = 0\,, \\ \alpha_1 & \text{if } x_1 = 1\,, \end{cases} \quad \text{and} \quad \psi_2(x_2) = \begin{cases} \beta_0 & \text{if } x_2 = 0\,, \\ \beta_1 & \text{if } x_2 = 1\,, \end{cases}$$

Then the state of the combined system (which can be used to describe for random numbers $(0)_{10} = (00)_2$, $(1)_{10} = (01)_2$, $(2)_{10} = (10)_2$ and $(3)_{10} = (11)_2$) is given by

$$\psi(x_1, x_2) \equiv \psi_1(x_1)\psi_2(x_2) = \begin{cases} \alpha_0\beta_0 & \text{if } (x_1, x_2) = (0,0)\,, \\ \alpha_0\beta_1 & \text{if } (x_1, x_2) = (0,1)\,, \\ \alpha_1\beta_0 & \text{if } (x_1, x_2) = (1,0)\,, \\ \alpha_1\beta_1 & \text{if } (x_1, x_2) = (1,1)\,, \end{cases}$$

which is abbreviated as

$$|\psi\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle\,.$$

§2.3 Quantum Registers

In general, if

$$|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n - 1\rangle$$

and

$$|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle + \cdots + \beta_{2^m-1}|2^m - 1\rangle$$

are two quantum states, then

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle &= \Big(\sum_{k=0}^{2^n-1} \alpha_k|k\rangle\Big) \otimes \Big(\sum_{\ell=0}^{2^m-1} \beta_\ell|\ell\rangle\Big) \\ &= \sum_{k=0}^{2^n-1} \sum_{\ell=0}^{2^m-1} \alpha_k\beta_\ell|k\rangle \otimes |\ell\rangle, \end{aligned}$$

where by writing $k = (k_1 k_2 \cdots k_n)_2$ and $\ell = (\ell_1\ell_2 \cdots \ell_m)_2$,

$$|k\rangle \otimes |\ell\rangle = |k_1 k_2 \cdots k_n \ell_1 \ell_2 \cdots \ell_m\rangle .$$

Sometimes $|\psi_1\rangle \otimes |\psi_2\rangle$ is written as $|\psi_1\rangle|\psi_2\rangle$.

§2.3 Quantum Registers

In general, if

$$|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{2^n-1}|2^n - 1\rangle$$

and

$$|\psi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle + \cdots + \beta_{2^m-1}|2^m - 1\rangle$$

are two quantum states, then

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle &= \Big(\sum_{k=0}^{2^n-1} \alpha_k|k\rangle\Big) \otimes \Big(\sum_{\ell=0}^{2^m-1} \beta_\ell|\ell\rangle\Big) \\ &= \sum_{k=0}^{2^n-1}\sum_{\ell=0}^{2^m-1} \alpha_k\beta_\ell|k\rangle \otimes |\ell\rangle, \end{aligned}$$

where by writing $k = (k_1k_2\cdots k_n)_2$ and $\ell = (\ell_1\ell_2\cdots\ell_m)_2$,

$$|k\rangle \otimes |\ell\rangle = |k_1k_2\cdots k_n\ell_1\ell_2\cdots\ell_m\rangle.$$

Sometimes $|\psi_1\rangle \otimes |\psi_2\rangle$ is written as $|\psi_1\rangle|\psi_2\rangle$.

§2.3 Quantum Registers

§2.3.2 Entanglements

An important property that deserves to be mentioned is entanglement, which refers to quantum correlations between different qubits. For instance, consider a 2-qubit register that is in the state

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

Initially neither of the two qubits has a classical value $|0\rangle$ or $|1\rangle$; however, if we measure the first qubit and observe, say, a $|0\rangle$, then the whole state collapses to $|00\rangle$. Thus observing the first qubit immediately fixes also the second, unobserved qubit to a classical value. This example illustrates some of the non-local effects that quantum systems can exhibit. In general, a bipartite state $|\phi\rangle$ is called entangled if it cannot be written as a tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$, where $|\phi_A\rangle$ lives in the first space and $|\phi_B\rangle$ lives in the second.

§2.3 Quantum Registers

§2.3.2 Entanglements

An important property that deserves to be mentioned is entanglement, which refers to quantum correlations between different qubits. For instance, consider a 2-qubit register that is in the state

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

Initially neither of the two qubits has a classical value $|0\rangle$ or $|1\rangle$; however, if we measure the first qubit and observe, say, a $|0\rangle$, then the whole state collapses to $|00\rangle$. Thus observing the first qubit immediately fixes also the second, unobserved qubit to a classical value. This example illustrates some of the non-local effects that quantum systems can exhibit. In general, a bipartite state $|\phi\rangle$ is called entangled if it cannot be written as a tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$, where $|\phi_A\rangle$ lives in the first space and $|\phi_B\rangle$ lives in the second.

§2.3 Quantum Registers

§2.3.2 Entanglements

An important property that deserves to be mentioned is entanglement, which refers to quantum correlations between different qubits. For instance, consider a 2-qubit register that is in the state

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

Initially neither of the two qubits has a classical value $|0\rangle$ or $|1\rangle$; however, if we measure the first qubit and observe, say, a $|0\rangle$, then the whole state collapses to $|00\rangle$. Thus observing the first qubit immediately fixes also the second, unobserved qubit to a classical value. This example illustrates some of the non-local effects that quantum systems can exhibit. In general, a bipartite state $|\phi\rangle$ is called entangled if it cannot be written as a tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$, where $|\phi_A\rangle$ lives in the first space and $|\phi_B\rangle$ lives in the second.

§2.3 Quantum Registers

§2.3.2 Entanglements

An important property that deserves to be mentioned is entanglement, which refers to quantum correlations between different qubits. For instance, consider a 2-qubit register that is in the state

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

Initially neither of the two qubits has a classical value $|0\rangle$ or $|1\rangle$; however, if we measure the first qubit and observe, say, a $|0\rangle$, then the whole state collapses to $|00\rangle$. Thus observing the first qubit immediately fixes also the second, unobserved qubit to a classical value. This example illustrates some of the non-local effects that quantum systems can exhibit. In general, a bipartite state $|\phi\rangle$ is called entangled if it cannot be written as a tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$, where $|\phi_A\rangle$ lives in the first space and $|\phi_B\rangle$ lives in the second.

§2.3 Quantum Registers

At this point, a comparison with classical probability distributions may be helpful. Suppose we have two probability spaces, A and B, the first with 2^n possible outcomes, the second with 2^m possible outcomes. A distribution on the first space can be described by 2^n parameters (non-negative reals summing to 1; actually there are only $2^n - 1$ degrees of freedom here) and a distribution on the second by 2^m parameters. Accordingly, a product distribution on the joint space can be described by $2^n + 2^m$ parameters. However, an arbitrary (non-product) distribution on the joint space takes 2^{n+m} numbers, since there are 2^{n+m} possible outcomes in total. Analogously, an n-qubit state $|\phi_A\rangle$ can be described by 2^n parameters (complex numbers whose squared moduli sum to 1), an m-qubit state $|\phi_B\rangle$ by 2^m parameters, and their tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$ by $2^n + 2^m$ parameters.

§2.3 Quantum Registers

At this point, a comparison with classical probability distributions may be helpful. Suppose we have two probability spaces, A and B, the first with 2^n possible outcomes, the second with 2^m possible outcomes. A distribution on the first space can be described by 2^n parameters (non-negative reals summing to 1; actually there are only $2^n - 1$ degrees of freedom here) and a distribution on the second by 2^m parameters. Accordingly, a product distribution on the joint space can be described by $2^n + 2^m$ parameters. However, an arbitrary (non-product) distribution on the joint space takes 2^{n+m} numbers, since there are 2^{n+m} possible outcomes in total. Analogously, an n-qubit state $|\phi_A\rangle$ can be described by 2^n parameters (complex numbers whose squared moduli sum to 1), an m-qubit state $|\phi_B\rangle$ by 2^m parameters, and their tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$ by $2^n + 2^m$ parameters.

§2.3 Quantum Registers

At this point, a comparison with classical probability distributions may be helpful. Suppose we have two probability spaces, A and B, the first with 2^n possible outcomes, the second with 2^m possible outcomes. A distribution on the first space can be described by 2^n parameters (non-negative reals summing to 1; actually there are only 2^n-1 degrees of freedom here) and a distribution on the second by 2^m parameters. Accordingly, a product distribution on the joint space can be described by $2^n + 2^m$ parameters. However, an arbitrary (non-product) distribution on the joint space takes 2^{n+m} numbers, since there are 2^{n+m} possible outcomes in total. Analogously, an n-qubit state $|\phi_A\rangle$ can be described by 2^n parameters (complex numbers whose squared moduli sum to 1), an m-qubit state $|\phi_B\rangle$ by 2^m parameters, and their tensor product $|\phi_A\rangle \otimes |\phi_B\rangle$ by $2^n + 2^m$ parameters.

§2.3 Quantum Registers

However, an arbitrary (possibly entangled) state in the joint space takes 2^{n+m} numbers, since it lives in a 2^{n+m}-dimensional space. We see that the number of parameters required to describe quantum states is the same as the number of parameters needed to describe probability distributions. Also note the analogy between statistical independence of two random variables A and B and non-entanglement of the product state $|\phi_A\rangle \otimes |\phi_B\rangle$. However, despite the similarities between probabilities and amplitudes, quantum states are much more powerful than distributions, because amplitudes may have negative parts which can lead to interference effects. Amplitudes only become probabilities when we square them. The art of quantum computing is to use these special properties for interesting computational purposes.

§2.3 Quantum Registers

However, an arbitrary (possibly entangled) state in the joint space takes 2^{n+m} numbers, since it lives in a 2^{n+m}-dimensional space. We see that the number of parameters required to describe quantum states is the same as the number of parameters needed to describe probability distributions. Also note the analogy between statistical independence of two random variables A and B and non-entanglement of the product state $|\phi_A\rangle \otimes |\phi_B\rangle$. However, despite the similarities between probabilities and amplitudes, quantum states are much more powerful than distributions, because amplitudes may have negative parts which can lead to interference effects. Amplitudes only become probabilities when we square them. The art of quantum computing is to use these special properties for interesting computational purposes.

§2.3 Quantum Registers

However, an arbitrary (possibly entangled) state in the joint space takes 2^{n+m} numbers, since it lives in a 2^{n+m}-dimensional space. We see that the number of parameters required to describe quantum states is the same as the number of parameters needed to describe probability distributions. Also note the analogy between statistical independence of two random variables A and B and non-entanglement of the product state $|\phi_A\rangle \otimes |\phi_B\rangle$. However, despite the similarities between probabilities and amplitudes, quantum states are much more powerful than distributions, because amplitudes may have negative parts which can lead to interference effects. Amplitudes only become probabilities when we square them. The art of quantum computing is to use these special properties for interesting computational purposes.

§2.3 Quantum Registers

However, an arbitrary (possibly entangled) state in the joint space takes 2^{n+m} numbers, since it lives in a 2^{n+m}-dimensional space. We see that the number of parameters required to describe quantum states is the same as the number of parameters needed to describe probability distributions. Also note the analogy between statistical independence of two random variables A and B and non-entanglement of the product state $|\phi_A\rangle \otimes |\phi_B\rangle$. However, despite the similarities between probabilities and amplitudes, quantum states are much more powerful than distributions, because amplitudes may have negative parts which can lead to interference effects. Amplitudes only become probabilities when we square them. The art of quantum computing is to use these special properties for interesting computational purposes.

§2.4 Quantum Circuits

A quantum circuit (also called quantum network or quantum gate array) generalizes the idea of classical circuit families, replacing the **AND**, **OR**, and **NOT** gates by elementary quantum gates. A quantum gate is a unitary transformation on a small (usually 1, 2, or 3) number of qubits. We saw a number of examples already in Section 2.2: the bitflip-gate X, the phaseflip gate Z, the Hadamard gate H. Mathematically, these gates can be composed by taking tensor products (if gates are applied in parallel to different parts of the register) and ordinary products (if gates are applied sequentially). Simple examples of such circuits of elementary gates are given in the next section.

§2.4 Quantum Circuits

A quantum circuit (also called quantum network or quantum gate array) generalizes the idea of classical circuit families, replacing the **AND**, **OR**, and **NOT** gates by elementary quantum gates. A quantum gate is a unitary transformation on a small (usually 1, 2, or 3) number of qubits. We saw a number of examples already in Section 2.2: the bitflip-gate X, the phaseflip gate Z, the Hadamard gate H. Mathematically, these gates can be composed by taking tensor products (if gates are applied in parallel to different parts of the register) and ordinary products (if gates are applied sequentially). Simple examples of such circuits of elementary gates are given in the next section.

§2.4 Quantum Circuits

For example, if we apply the Hadamard gate H to each bit in a register of n zeroes, we obtain $\frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle$ which is a superposition of all n-bit strings. More generally, if we apply $\mathrm{H}^{\otimes n}$ to an initial state $|i\rangle$, with $i \in \{0,1\}^n$, we obtain

$$\mathrm{H}^{\otimes n}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\bullet j}|j\rangle, \tag{6}$$

where $i \bullet j = \sum_{k=1}^{n} i_k j_k$ denotes the bitwise product of the n-bit strings $i, j \in \{0,1\}^n$. For instance,

$$\mathrm{H}^{\otimes 2}|01\rangle \equiv (\mathrm{H}|0\rangle)\otimes(\mathrm{H}|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2}\sum_{j\in\{0,1\}^2} (-1)^{01\bullet j}|j\rangle.$$

The n-fold Hadamard transform $\mathrm{H}^{\otimes n}$ will be very useful for all the quantum algorithms explained later.

§2.4 Quantum Circuits

For example, if we apply the Hadamard gate H to each bit in a register of n zeroes, we obtain $\frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle$ which is a superposition of all n-bit strings. More generally, if we apply $\mathrm{H}^{\otimes n}$ to an initial state $|i\rangle$, with $i \in \{0,1\}^n$, we obtain

$$\mathrm{H}^{\otimes n}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\bullet j}|j\rangle, \tag{6}$$

where $i \bullet j = \sum_{k=1}^{n} i_k j_k$ denotes the bitwise product of the n-bit strings $i, j \in \{0,1\}^n$. For instance,

$$\mathrm{H}^{\otimes 2}|01\rangle \equiv (\mathrm{H}|0\rangle) \otimes (\mathrm{H}|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2} \sum_{j\in\{0,1\}^2} (-1)^{01\bullet j}|j\rangle.$$

The n-fold Hadamard transform $\mathrm{H}^{\otimes n}$ will be very useful for all the quantum algorithms explained later.

§2.4 Quantum Circuits

For example, if we apply the Hadamard gate H to each bit in a register of n zeroes, we obtain $\frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} |j\rangle$ which is a superposition of all n-bit strings. More generally, if we apply $\mathrm{H}^{\otimes n}$ to an initial state $|i\rangle$, with $i \in \{0,1\}^n$, we obtain

$$\mathrm{H}^{\otimes n}|i\rangle = \frac{1}{\sqrt{2^n}} \sum_{j\in\{0,1\}^n} (-1)^{i\bullet j}|j\rangle, \tag{6}$$

where $i \bullet j = \sum_{k=1}^{n} i_k j_k$ denotes the bitwise product of the n-bit strings $i, j \in \{0,1\}^n$. For instance,

$$\mathrm{H}^{\otimes 2}|01\rangle \equiv (\mathrm{H}|0\rangle)\otimes(\mathrm{H}|1\rangle) = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2}\sum_{j\in\{0,1\}^2} (-1)^{01\bullet j}|j\rangle.$$

The n-fold Hadamard transform $\mathrm{H}^{\otimes n}$ will be very useful for all the quantum algorithms explained later.

§2.4 Quantum Circuits

Theorem

For each $n \in \mathbb{N}$ *and* $j = (j_1 j_2 \cdots j_n)_2$,

$$\mathrm{H}^{\otimes n}|j\rangle \equiv \mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{j \bullet k} |k\rangle, \tag{6}$$

where we recall that with $k = (k_1 k_2 \cdots k_n)_2$, $j \bullet k \equiv j_1 k_1 + \cdots j_n k_n$.

Proof.

Note that for $j_\ell \in \{0, 1\}$, $\mathrm{H}|j_\ell\rangle = \frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} (-1)^{j_\ell k_\ell} |k_\ell\rangle$. Therefore,

$$\begin{aligned}
\mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle &\equiv (\mathrm{H}|j_1\rangle) \otimes \cdots \otimes (\mathrm{H}|j_n\rangle) \\
&= \left(\frac{1}{\sqrt{2}} \sum_{k_1=0}^{1} (-1)^{j_1 k_1} |k_1\rangle \right) \otimes \cdots \otimes \left(\frac{1}{\sqrt{2}} \sum_{k_n=0}^{1} (-1)^{j_n k_n} |k_n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} (-1)^{j_1 k_1 + \cdots + j_n k_n} |k_1\rangle \otimes \cdots \otimes |k_n\rangle .
\end{aligned}$$

□

§2.4 Quantum Circuits

Theorem

For each $n \in \mathbb{N}$ *and* $j = (j_1 j_2 \cdots j_n)_2$,

$$\mathrm{H}^{\otimes n}|j\rangle \equiv \mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{j \bullet k}|k\rangle, \qquad (6)$$

where we recall that with $k = (k_1 k_2 \cdots k_n)_2$, $j \bullet k \equiv j_1 k_1 + \cdots j_n k_n$.

Proof.

Note that for $j_\ell \in \{0,1\}$, $\mathrm{H}|j_\ell\rangle = \frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} (-1)^{j_\ell k_\ell}|k_\ell\rangle$. Therefore,

$$\begin{aligned}\mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle &\equiv (\mathrm{H}|j_1\rangle) \otimes \cdots \otimes (\mathrm{H}|j_n\rangle)\\ &= \Big(\frac{1}{\sqrt{2}} \sum_{k_1=0}^{1} (-1)^{j_1 k_1}|k_1\rangle\Big) \otimes \cdots \otimes \Big(\frac{1}{\sqrt{2}} \sum_{k_n=0}^{1} (-1)^{j_n k_n}|k_n\rangle\Big)\\ &= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} (-1)^{j_1 k_1 + \cdots + j_n k_n}|k_1\rangle \otimes \cdots \otimes |k_n\rangle .\end{aligned}$$

□

§2.4 Quantum Circuits

Theorem

For each $n \in \mathbb{N}$ *and* $j = (j_1 j_2 \cdots j_n)_2$,

$$\mathrm{H}^{\otimes n}|j\rangle \equiv \mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{j\bullet k}|k\rangle, \tag{6}$$

where we recall that with $k = (k_1 k_2 \cdots k_n)_2$, $j \bullet k \equiv j_1 k_1 + \cdots j_n k_n$.

Proof.

Note that for $j_\ell \in \{0,1\}$, $\mathrm{H}|j_\ell\rangle = \frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} (-1)^{j_\ell k_\ell}|k_\ell\rangle$. Therefore,

$$\mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle \equiv (\mathrm{H}|j_1\rangle) \otimes \cdots \otimes (\mathrm{H}|j_n\rangle)$$

$$= \Big(\frac{1}{\sqrt{2}} \sum_{k_1=0}^{1} (-1)^{j_1 k_1}|k_1\rangle\Big) \otimes \cdots \otimes \Big(\frac{1}{\sqrt{2}} \sum_{k_n=0}^{1} (-1)^{j_n k_n}|k_n\rangle\Big)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} (-1)^{j_1 k_1 + \cdots + j_n k_n}|k_1\rangle \otimes \cdots \otimes |k_n\rangle .$$ □

§2.4 Quantum Circuits

Theorem

For each $n \in \mathbb{N}$ *and* $j = (j_1 j_2 \cdots j_n)_2$,

$$\mathrm{H}^{\otimes n}|j\rangle \equiv \mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{j\bullet k}|k\rangle, \qquad (6)$$

where we recall that with $k = (k_1 k_2 \cdots k_n)_2$, $j \bullet k \equiv j_1 k_1 + \cdots j_n k_n$.

Proof.

Note that for $j_\ell \in \{0,1\}$, $\mathrm{H}|j_\ell\rangle = \frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} (-1)^{j_\ell k_\ell}|k_\ell\rangle$. Therefore,

$$\begin{aligned}
\mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle &\equiv (\mathrm{H}|j_1\rangle) \otimes \cdots \otimes (\mathrm{H}|j_n\rangle) \\
&= \Big(\frac{1}{\sqrt{2}} \sum_{k_1=0}^{1} (-1)^{j_1 k_1}|k_1\rangle\Big) \otimes \cdots \otimes \Big(\frac{1}{\sqrt{2}} \sum_{k_n=0}^{1} (-1)^{j_n k_n}|k_n\rangle\Big) \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} (-1)^{j_1 k_1 + \cdots + j_n k_n}|k_1\rangle \otimes \cdots \otimes |k_n\rangle . \qquad \square
\end{aligned}$$

§2.4 Quantum Circuits

Theorem

For each $n \in \mathbb{N}$ *and* $j = (j_1 j_2 \cdots j_n)_2$,

$$\mathrm{H}^{\otimes n}|j\rangle \equiv \mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{j \bullet k} |k\rangle, \tag{6}$$

where we recall that with $k = (k_1 k_2 \cdots k_n)_2$, $j \bullet k \equiv j_1 k_1 + \cdots j_n k_n$.

Proof.

Note that for $j_\ell \in \{0,1\}$, $\mathrm{H}|j_\ell\rangle = \frac{1}{\sqrt{2}} \sum_{k_\ell=0}^{1} (-1)^{j_\ell k_\ell} |k_\ell\rangle$. Therefore,

$$\begin{aligned}
\mathrm{H}^{\otimes n}|j_1 j_2 \cdots j_n\rangle &\equiv (\mathrm{H}|j_1\rangle) \otimes \cdots \otimes (\mathrm{H}|j_n\rangle) \\
&= \Big(\frac{1}{\sqrt{2}} \sum_{k_1=0}^{1} (-1)^{j_1 k_1} |k_1\rangle\Big) \otimes \cdots \otimes \Big(\frac{1}{\sqrt{2}} \sum_{k_n=0}^{1} (-1)^{j_n k_n} |k_n\rangle\Big) \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} (-1)^{j_1 k_1 + \cdots + j_n k_n} |k_1\rangle \otimes \cdots \otimes |k_n\rangle.
\end{aligned}$$

□

§2.4 Quantum Circuits

A quantum circuit is a finite directed acyclic graph of input nodes, gates, and output nodes. There are n nodes that contain the input; in addition we may have some more input nodes that are initially $|0\rangle$ ("workspace"). The internal nodes of the quantum circuit are quantum gates that each operate on at most 2 qubits of the state. The gates in the circuit transform the initial state vector into a final state, which will generally be a superposition. We measure some dedicated output bits of this final state to (probabilistically) obtain an answer.

§2.4 Quantum Circuits

A quantum circuit is a finite directed acyclic graph of input nodes, gates, and output nodes. There are n nodes that contain the input; in addition we may have some more input nodes that are initially $|0\rangle$ ("workspace"). The internal nodes of the quantum circuit are quantum gates that each operate on at most 2 qubits of the state. The gates in the circuit transform the initial state vector into a final state, which will generally be a superposition. We measure some dedicated output bits of this final state to (probabilistically) obtain an answer.

§2.4 Quantum Circuits

To draw such circuits, we typically let time progress from left to right: we start with the initial state on the left. Each qubit is pictured as a wire, and the circuit prescribes which gates are to be applied to which wires. Single-qubit gates like X and H just act on one wire, while multi-qubit gates such as the **CNOT** act on multiple wires simultaneously. When one qubit "controls" the application of a gate to another qubit, then the controlling wire is drawn with a dot linked vertically to the gate that is applied to the target qubit. This happens for instance with the **CNOT**, where the applied single-qubit gate is X (sometimes drawn as '$\oplus$').

§2.4 Quantum Circuits

To draw such circuits, we typically let time progress from left to right: we start with the initial state on the left. Each qubit is pictured as a wire, and the circuit prescribes which gates are to be applied to which wires. Single-qubit gates like X and H just act on one wire, while multi-qubit gates such as the **CNOT** act on multiple wires simultaneously. When one qubit "controls" the application of a gate to another qubit, then the controlling wire is drawn with a dot linked vertically to the gate that is applied to the target qubit. This happens for instance with the **CNOT**, where the applied single-qubit gate is X (sometimes drawn as '$\oplus$').

§2.4 Quantum Circuits

To draw such circuits, we typically let time progress from left to right: we start with the initial state on the left. Each qubit is pictured as a wire, and the circuit prescribes which gates are to be applied to which wires. Single-qubit gates like X and H just act on one wire, while multi-qubit gates such as the **CNOT** act on multiple wires simultaneously. When one qubit "controls" the application of a gate to another qubit, then the controlling wire is drawn with a dot linked vertically to the gate that is applied to the target qubit. This happens for instance with the **CNOT**, where the applied single-qubit gate is X (sometimes drawn as '$\oplus$').

§2.4 Quantum Circuits

Figure 2 gives a simple example on two qubits, initially in basis state $|00\rangle$: first apply the Hadamard gate H to the first qubit, then **CNOT** to both qubits (with the first qubit acting as the control), and then Z to the last qubit.

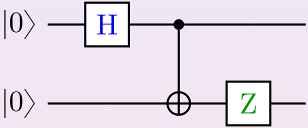


Figure 2: Simple circuit for turning $|00\rangle$ into an entangled state

Let $A \otimes B$ be defined by $(A \otimes B)(|a\rangle \otimes |b\rangle) = (A|a\rangle) \otimes (B|b\rangle)$:

$$|00\rangle \overset{\mathrm{H}\otimes\mathrm{I}}{\longmapsto} \mathrm{H}|0\rangle \otimes \mathrm{I}|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\mathrm{CNOT}}{\longmapsto} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\overset{\mathrm{I}\otimes\mathrm{Z}}{\longmapsto} \frac{1}{\sqrt{2}}(\mathrm{I}|0\rangle \otimes \mathrm{Z}|0\rangle + \mathrm{I}|1\rangle \otimes \mathrm{Z}|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) .$$

Therefore, the resulting state of the circuit above is $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

§2.4 Quantum Circuits

Figure 2 gives a simple example on two qubits, initially in basis state $|00\rangle$: first apply the Hadamard gate H to the first qubit, then **CNOT** to both qubits (with the first qubit acting as the control), and then Z to the last qubit.

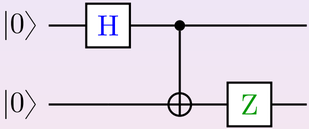


Figure 2: Simple circuit for turning $|00\rangle$ into an entangled state

Let $A \otimes B$ be defined by $(A \otimes B)(|a\rangle \otimes |b\rangle) = (A|a\rangle) \otimes (B|b\rangle)$:

$$|00\rangle \overset{\mathrm{H}\otimes\mathrm{I}}{\mapsto} \mathrm{H}|0\rangle \otimes \mathrm{I}|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{\mathbf{CNOT}}{\mapsto} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\overset{\mathrm{I}\otimes\mathrm{Z}}{\mapsto} \frac{1}{\sqrt{2}}(\mathrm{I}|0\rangle \otimes \mathrm{Z}|0\rangle + \mathrm{I}|1\rangle \otimes \mathrm{Z}|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)\,.$$

Therefore, the resulting state of the circuit above is $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

§2.4 Quantum Circuits

Example

One possible implementation of a 2-bit full adder (using **CNOT** gates and TOFFOLI gates):

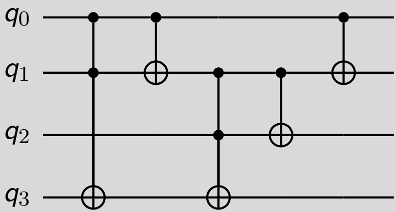


Figure 3: Circuit diagram of a quantum full adder

where the inputs are $q_0 = A$, $q_1 = B$, $q_2 = \mathrm{C}_{\text{in}}$, and the ouputs are $q_0 = A$, $q_1 = B$, $q_2 = \text{Sum}_{\text{out}}$, $q_3 = \mathrm{C}_{\text{out}}$.

§2.4 Quantum Circuits

Example (cont.)

The validity of that the quantum circuit above is indeed a full adder can be verified by the following truth table:

INPUT				OUTPUT			
q_3	q_2 C_{in}	q_1 B	q_0 A	q_3 C_{out}	q_2 S	q_1 B	q_0 A
0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0
0	0	1	0	0	1	1	0
0	1	1	0	1	0	1	0
0	0	0	1	0	1	0	1
0	1	0	1	1	0	0	1
0	0	1	1	1	0	1	1
0	1	1	1	1	1	1	1

§2.4 Quantum Circuits

§2.4.1 Quantum Teleportation

As an example of the use of elementary gates, we will explain teleportation. Suppose there are two parties, Alice and Bob. Alice has a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ that she wants to send to Bob via a classical channel. Without further resources this would be impossible, but Alice also shares an EPR-pair

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

with Bob (say Alice holds the first qubit and Bob the second). Initially, their joint state is

$$(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha_0}{\sqrt{2}}(|000\rangle+|011\rangle)+\frac{\alpha_1}{\sqrt{2}}(|100\rangle+|111\rangle).$$

The first two qubits belong to Alice, the third to Bob.

§2.4 Quantum Circuits

§2.4.1 Quantum Teleportation

As an example of the use of elementary gates, we will explain teleportation. Suppose there are two parties, Alice and Bob. Alice has a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ that she wants to send to Bob via a classical channel. Without further resources this would be impossible, but Alice also shares an EPR-pair

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

with Bob (say Alice holds the first qubit and Bob the second). Initially, their joint state is

$$(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}}=\frac{\alpha_0}{\sqrt{2}}(|000\rangle+|011\rangle)+\frac{\alpha_1}{\sqrt{2}}(|100\rangle+|111\rangle).$$

The first two qubits belong to Alice, the third to Bob.

§2.4 Quantum Circuits

§2.4.1 Quantum Teleportation

As an example of the use of elementary gates, we will explain teleportation. Suppose there are two parties, Alice and Bob. Alice has a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ that she wants to send to Bob via a classical channel. Without further resources this would be impossible, but Alice also shares an EPR-pair

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

with Bob (say Alice holds the first qubit and Bob the second). Initially, their joint state is

$$(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha_0}{\sqrt{2}}(|000\rangle+|011\rangle)+\frac{\alpha_1}{\sqrt{2}}(|100\rangle+|111\rangle).$$

The first two qubits belong to Alice, the third to Bob.

§2.4 Quantum Circuits

§2.4.1 Quantum Teleportation

As an example of the use of elementary gates, we will explain teleportation. Suppose there are two parties, Alice and Bob. Alice has a qubit $\alpha_0|0\rangle + \alpha_1|1\rangle$ that she wants to send to Bob via a classical channel. Without further resources this would be impossible, but Alice also shares an EPR-pair

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

with Bob (say Alice holds the first qubit and Bob the second). Initially, their joint state is

$$(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha_0}{\sqrt{2}}(|000\rangle+|011\rangle)+\frac{\alpha_1}{\sqrt{2}}(|100\rangle+|111\rangle).$$

The first two qubits belong to Alice, the third to Bob.

§2.4 Quantum Circuits

Alice performs a CNOT on her two qubits to obtain

$$\frac{\alpha_0}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\alpha_1}{\sqrt{2}}(|110\rangle + |101\rangle)$$

and then a Hadamard transform on her first qubit so that their joint state now becomes

$$\begin{aligned}
&\frac{\alpha_0}{2}\Big[(|0\rangle+|1\rangle)\otimes(|00\rangle+|11\rangle)\Big] + \frac{\alpha_1}{2}\Big[(|0\rangle-|1\rangle)\otimes(|10\rangle+|01\rangle)\Big] \\
&\quad = \frac{\alpha_0}{2}(|000\rangle+|011\rangle+|100\rangle+|111\rangle) \\
&\qquad + \frac{\alpha_1}{2}(|010\rangle+|001\rangle-|110\rangle-|101\rangle) \\
&\quad = \frac{1}{2}|00\rangle\otimes(\alpha_0|0\rangle+\alpha_1|1\rangle) + \frac{1}{2}|01\rangle\otimes(\alpha_0|1\rangle+\alpha_1|0\rangle) \\
&\qquad + \frac{1}{2}|10\rangle\otimes(\alpha_0|0\rangle-\alpha_1|1\rangle) + \frac{1}{2}|11\rangle\otimes(\alpha_0|1\rangle-\alpha_1|0\rangle).
\end{aligned}$$

§2.4 Quantum Circuits

Alice then measures her two qubits in the computational basis and sends the result $b_1 b_2$, a 2 random classical bits, to Bob over a classical channel. In order to recover Alice's qubit, Bob applies the transformation $\mathrm{Z}^{b_1}\mathrm{X}^{b_2}$, where X is the bitflip-gate and Z is the phaseflip gate, to the qubit he has now. For example, if Alice sent 11 to Bob over a classical channel, Bob then applies ZX to the qubit $\alpha_0|1\rangle - \alpha_1|0\rangle$ (which is the qubit Bob has now since Alice's two qubits has been measured) and obtain $\alpha_0|0\rangle + \alpha_1|1\rangle$ which is the qubit Alice has originally. In fact, if Alice's qubit had been entangled with other qubits, then teleportation preserves this entanglement: Bob then receives a qubit that is entangled in the same way as Alice's original qubit was.

§2.4 Quantum Circuits

Alice then measures her two qubits in the computational basis and sends the result $b_1 b_2$, a 2 random classical bits, to Bob over a classical channel. In order to recover Alice's qubit, Bob applies the transformation $\mathrm{Z}^{b_1}\mathrm{X}^{b_2}$, where X is the bitflip-gate and Z is the phaseflip gate, to the qubit he has now. For example, if Alice sent 11 to Bob over a classical channel, Bob then applies ZX to the qubit $\alpha_0|1\rangle - \alpha_1|0\rangle$ (which is the qubit Bob has now since Alice's two qubits has been measured) and obtain $\alpha_0|0\rangle + \alpha_1|1\rangle$ which is the qubit Alice has originally. In fact, if Alice's qubit had been entangled with other qubits, then teleportation preserves this entanglement: Bob then receives a qubit that is entangled in the same way as Alice's original qubit was.

§2.4 Quantum Circuits

Alice then measures her two qubits in the computational basis and sends the result $b_1 b_2$, a 2 random classical bits, to Bob over a classical channel. In order to recover Alice's qubit, Bob applies the transformation $\mathrm{Z}^{b_1}\mathrm{X}^{b_2}$, where X is the bitflip-gate and Z is the phaseflip gate, to the qubit he has now. For example, if Alice sent 11 to Bob over a classical channel, Bob then applies ZX to the qubit $\alpha_0|1\rangle - \alpha_1|0\rangle$ (which is the qubit Bob has now since Alice's two qubits has been measured) and obtain $\alpha_0|0\rangle + \alpha_1|1\rangle$ which is the qubit Alice has originally. In fact, if Alice's qubit had been entangled with other qubits, then teleportation preserves this entanglement: Bob then receives a qubit that is entangled in the same way as Alice's original qubit was.

§2.4 Quantum Circuits

Note that the qubit on Alice's side has been destroyed: teleporting moves a qubit from A to B, rather than copying it. In fact, copying an unknown qubit is impossible. This can be seen as follows. Suppose C were a 1-qubit copier; that is, $C|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for every qubit $|\phi\rangle$. In particular, $C|0\rangle|0\rangle = |0\rangle|0\rangle$ and $C|1\rangle|0\rangle = |1\rangle|1\rangle$. But then C would not copy $|\phi\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ correctly, since by linearity

$$C|\phi\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(C|0\rangle|0\rangle + C|1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \neq |\phi\rangle|\phi\rangle .$$

Remark: The fact that copying an unknown qubit is impossible implies that not all the Boolean function can be implemented by current quantum computers. The lack of the ability of performing all Boolean functions will put a lot of constraints to the use of quantum computers.

§2.4 Quantum Circuits

Note that the qubit on Alice's side has been destroyed: teleporting moves a qubit from A to B, rather than copying it. In fact, copying an unknown qubit is impossible. This can be seen as follows. Suppose C were a 1-qubit copier; that is, $C|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for every qubit $|\phi\rangle$. In particular, $C|0\rangle|0\rangle = |0\rangle|0\rangle$ and $C|1\rangle|0\rangle = |1\rangle|1\rangle$. But then C would not copy $|\phi\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ correctly, since by linearity

$$C|\phi\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(C|0\rangle|0\rangle + C|1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \neq |\phi\rangle|\phi\rangle .$$

Remark: The fact that copying an unknown qubit is impossible implies that not all the Boolean function can be implemented by current quantum computers. The lack of the ability of performing all Boolean functions will put a lot of constraints to the use of quantum computers.

§2.4 Quantum Circuits

Note that the qubit on Alice's side has been destroyed: teleporting moves a qubit from A to B, rather than copying it. In fact, copying an unknown qubit is impossible. This can be seen as follows. Suppose C were a 1-qubit copier; that is, $C|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for every qubit $|\phi\rangle$. In particular, $C|0\rangle|0\rangle = |0\rangle|0\rangle$ and $C|1\rangle|0\rangle = |1\rangle|1\rangle$. But then C would not copy $|\phi\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ correctly, since by linearity

$$C|\phi\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(C|0\rangle|0\rangle + C|1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \neq |\phi\rangle|\phi\rangle\,.$$

Remark: The fact that copying an unknown qubit is impossible implies that not all the Boolean function can be implemented by current quantum computers. The lack of the ability of performing all Boolean functions will put a lot of constraints to the use of quantum computers.

§2.4 Quantum Circuits

Note that the qubit on Alice's side has been destroyed: teleporting moves a qubit from A to B, rather than copying it. In fact, copying an unknown qubit is impossible. This can be seen as follows. Suppose C were a 1-qubit copier; that is, $C|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$ for every qubit $|\phi\rangle$. In particular, $C|0\rangle|0\rangle = |0\rangle|0\rangle$ and $C|1\rangle|0\rangle = |1\rangle|1\rangle$. But then C would not copy $|\phi\rangle = \mathrm{H}|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ correctly, since by linearity

$$C|\phi\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(C|0\rangle|0\rangle + C|1\rangle|0\rangle\big) = \frac{1}{\sqrt{2}}\big(|0\rangle|0\rangle + |1\rangle|1\rangle\big) \neq |\phi\rangle|\phi\rangle\,.$$

Remark: The fact that copying an unknown qubit is impossible implies that not all the Boolean function can be implemented by current quantum computers. The lack of the ability of performing all Boolean functions will put a lot of constraints to the use of quantum computers.

§2.5 Universality of Various Sets of Elementary Gates

Definition

Let $\{U_1, \cdots, U_k\}$ be a collection of quantum gates. The collection of all quantum gates that can be constructed from U_1, U_2, $\cdots$, U_k, denoted by $\mathcal{F}[U_1, \cdots, U_k]$, is the set satisfying the following construction rules:

1. For any $1 \leqslant j \leqslant k$, $U_j \in \mathcal{F}[U_1, \cdots, U_k]$.
2. For any $n \in \mathbb{N}$, $\mathbf{1}^{\otimes n} \in \mathcal{F}[U_1, \cdots, U_k]$, where $\mathbf{1}$ denotes the identity gate.
3. For any n-qubit quantum gates V_1, V_2, we have
$$V_1, V_2 \in \mathcal{F}[U_1, \cdots, U_k] \quad \Rightarrow \quad V_1 V_2 \in \mathcal{F}[U_1, \cdots, U_k] .$$
4. For any two quantum gates V_1, V_2, we have
$$V_1, V_2 \in \mathcal{F}[U_1, \cdots, U_k] \quad \Rightarrow \quad V_1 \otimes V_2 \in \mathcal{F}[U_1, \cdots, U_k] .$$

§2.5 Universality of Various Sets of Elementary Gates

Definition (Cont.)

A collection of quantum gates $\mathcal{U} = \{U_1, \cdots, U_k\}$ is called universal if any quantum gate U can be constructed with gates from $\mathcal{U}$; that is, for every quantum gate U, $U \in \mathcal{F}[U_1, \cdots, U_k]$.

Proposition

For quantum gates $V_1, \cdots, V_\ell$, $U_1, \cdots, U_k$, we have

$$V_1, \cdots, V_\ell \in \mathcal{F}[U_1, \cdots, U_k] \;\Rightarrow\; \mathcal{F}[V_1, \cdots, V_\ell] \subseteq \mathcal{F}[U_1, \cdots, U_k] .$$

In particular, $\mathcal{F}\big[\mathcal{F}[U_1, \cdots, U_k]\big] = \mathcal{F}[U_1, \cdots, U_k]$.

§2.5 Universality of Various Sets of Elementary Gates

Definition (Cont.)

A collection of quantum gates $\mathcal{U} = \{U_1, \cdots, U_k\}$ is called universal if any quantum gate U can be constructed with gates from $\mathcal{U}$; that is, for every quantum gate U, $U \in \mathcal{F}[U_1, \cdots, U_k]$.

Proposition

For quantum gates $V_1, \cdots, V_\ell$, $U_1, \cdots, U_k$, we have

$$V_1, \cdots, V_\ell \in \mathcal{F}[U_1, \cdots, U_k] \;\Rightarrow\; \mathcal{F}[V_1, \cdots, V_\ell] \subseteq \mathcal{F}[U_1, \cdots, U_k]\,.$$

In particular, $\mathcal{F}\big[\mathcal{F}[U_1, \cdots, U_k]\big] = \mathcal{F}[U_1, \cdots, U_k]$.

§2.5 Universality of Various Sets of Elementary Gates

Which set of elementary gates should we allow? There are several reasonable choices.

1. The set of all 1-qubit operations together with the 2-qubit **CNOT** gate is universal, meaning that any other unitary transformation can be built from these gates.

Allowing all 1-qubit gates is not very realistic from an implementational point of view, as there are uncountably many of them. However, the model is usually restricted, only allowing a small finite set of 1-qubit gates from which all other 1-qubit gates can be efficiently approximated.

§2.5 Universality of Various Sets of Elementary Gates

Theorem (Solovay-Kitaev)

Let $\mathcal{G}$ be a finite set of elements in $\mathrm{SU}(2)$ containing its own inverses and such that the group $\langle \mathcal{G} \rangle$ they generate is dense in $\mathrm{SU}(2)$. There exists $c > 0$ such that for any $\varepsilon > 0$ and $U \in \mathrm{SU}(2)$, there is a sequence S of gates from $\mathcal{G}$ of length $\mathcal{O}(\log^c(1/\varepsilon))$ such that $\|S - U\| \leqslant \varepsilon$.

2. The set consisting of **CNOT**, Hadamard, and the R_z gate $\mathrm{R}_z(\frac{\pi}{4})$ is universal in the sense of approximation, meaning that any other unitary can be arbitrarily well approximated using circuits of only these gates. The Solovay-Kitaev Theorem says that this approximation is quite efficient: we can approximate any gate on 1 or 2 qubits up to error ε using polylog$(1/\varepsilon)$ gates from our small set.

§2.5 Universality of Various Sets of Elementary Gates

Theorem (Solovay-Kitaev)

Let $\mathcal{G}$ be a finite set of elements in $\mathrm{SU}(2)$ containing its own inverses and such that the group $\langle \mathcal{G} \rangle$ they generate is dense in $\mathrm{SU}(2)$. There exists $c > 0$ such that for any $\varepsilon > 0$ and $U \in \mathrm{SU}(2)$, there is a sequence S of gates from $\mathcal{G}$ of length $\mathcal{O}(\log^c(1/\varepsilon))$ such that $\|S - U\| \leqslant \varepsilon$.

2. The set consisting of **CNOT**, Hadamard, and the R_z gate $\mathrm{R}_z(\frac{\pi}{4})$ is universal in the sense of approximation, meaning that any other unitary can be arbitrarily well approximated using circuits of only these gates. The Solovay-Kitaev Theorem says that this approximation is quite efficient: we can approximate any gate on 1 or 2 qubits up to error ε using $\mathrm{polylog}(1/\varepsilon)$ gates from our small set.

§2.5 Universality of Various Sets of Elementary Gates

Theorem (Solovay-Kitaev)

Let $\mathcal{G}$ be a finite set of elements in $\mathrm{SU}(2)$ containing its own inverses and such that the group $\langle \mathcal{G} \rangle$ they generate is dense in $\mathrm{SU}(2)$. There exists $c > 0$ such that for any $\varepsilon > 0$ and $U \in \mathrm{SU}(2)$, there is a sequence S of gates from $\mathcal{G}$ of length $\mathcal{O}(\log^c(1/\varepsilon))$ such that $\|S - U\| \leqslant \varepsilon$.

2. The set consisting of **CNOT**, Hadamard, and the R_z gate $\mathrm{R}_z(\frac{\pi}{4})$ is universal in the sense of approximation, meaning that any other unitary can be arbitrarily well approximated using circuits of only these gates. The Solovay-Kitaev Theorem says that this approximation is quite efficient: we can approximate any gate on 1 or 2 qubits up to error ε using polylog$(1/\varepsilon)$ gates from our small set.

§2.5 Universality of Various Sets of Elementary Gates

Recall that $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ denote 1-qubit gates that rotate a 1-qubit state, on the Bloch sphere, by angle τ about the x-axis, y-axis, and the z-axis, respectively. The matrix representation of $\mathrm{R}_x(\tau)$, $\mathrm{R}_y(\tau)$ and $\mathrm{R}_z(\tau)$ are

$$\mathrm{R}_x(\tau) = \begin{bmatrix} \cos\frac{\tau}{2} & -i\sin\frac{\tau}{2} \\ -i\sin\frac{\tau}{2} & \cos\frac{\tau}{2} \end{bmatrix}, \mathrm{R}_y(\tau) = \begin{bmatrix} \cos\frac{\tau}{2} & -\sin\frac{\tau}{2} \\ \sin\frac{\tau}{2} & \cos\frac{\tau}{2} \end{bmatrix}, \mathrm{R}_z(\tau) = \begin{bmatrix} e^{-i\tau/2} & 0 \\ 0 & e^{i\tau/2} \end{bmatrix}.$$

Then

3. The set of Hadamard H, $\mathbf{CNOT}$, $\mathrm{R}_y(\tau)$, $\mathrm{R}_z(\tau)$ (for all $\tau \in \mathbb{R}$) and **SWAP** is universal.

§2.6 Quantum Parallelism

One uniquely quantum-mechanical effect that we can use for building quantum algorithms is quantum parallelism. Suppose we can build a quantum circuit to represent a boolean function $f\colon \{0,1\}^n \to \{0,1\}^m$. Then we can build a quantum circuit U that maps $|x\rangle|0\rangle$ to $|x\rangle|f(x)\rangle$ for every $x \in \{0,1\}^n$ and we have

$$\mathrm{U}\Big(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle\,.$$

We applied U just once, but the final superposition contains $f(x)$ for all 2^n input values x! However, by itself this is not very useful and does not give more than classical randomization, since observing the final superposition will give just one random $|x\rangle|f(x)\rangle$ and all other information will be lost. As we will see below, quantum parallelism needs to be combined with the effects of interference and entanglement in order to get something that is better than classical.

§2.6 Quantum Parallelism

One uniquely quantum-mechanical effect that we can use for building quantum algorithms is quantum parallelism. Suppose we can build a quantum circuit to represent a boolean function $f\colon \{0,1\}^n \to \{0,1\}^m$. Then we can build a quantum circuit U that maps $|x\rangle|0\rangle$ to $|x\rangle|f(x)\rangle$ for every $x \in \{0,1\}^n$ and we have

$$\mathrm{U}\Big(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle\,.$$

We applied U just once, but the final superposition contains $f(x)$ for all 2^n input values x! However, by itself this is not very useful and does not give more than classical randomization, since observing the final superposition will give just one random $|x\rangle|f(x)\rangle$ and all other information will be lost. As we will see below, quantum parallelism needs to be combined with the effects of interference and entanglement in order to get something that is better than classical.

§2.6 Quantum Parallelism

One uniquely quantum-mechanical effect that we can use for building quantum algorithms is quantum parallelism. Suppose we can build a quantum circuit to represent a boolean function $f\colon \{0,1\}^n \to \{0,1\}^m$. Then we can build a quantum circuit U that maps $|x\rangle|0\rangle$ to $|x\rangle|f(x)\rangle$ for every $x \in \{0,1\}^n$ and we have

$$\mathrm{U}\Big(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle\Big) = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle\,.$$

We applied U just once, but the final superposition contains $f(x)$ for all 2^n input values x! However, by itself this is not very useful and does not give more than classical randomization, since observing the final superposition will give just one random $|x\rangle|f(x)\rangle$ and all other information will be lost. As we will see below, quantum parallelism needs to be combined with the effects of interference and entanglement in order to get something that is better than classical.

§2.7 The Early Algorithms

Virtually all quantum algorithms work with **queries** in some form or other. For a given N-bit data $x = (x_0, \cdots, x_{N-1}) \in \{0,1\}^N$, where $N = 2^n$, let O_x be a linear map on $n+1$ qubits given by

$$\mathrm{O}_x : |i\rangle|b\rangle \mapsto |i\rangle|b \oplus x_i\rangle ,$$

where $i \in \{0,1\}^n$, $b \in \{0,1\}$, $\oplus$ denotes exclusive-or (addition modulo 2), and the value of x_i is obtained through a memory access via a so-called "black-box", which is equipped to output the bit x_i on input i. The first n qubits of the state are called the address bits (or address register), while the $(n+1)$-th qubit is called the target bit.

Since O_x is equivalent to a swap of basis, it is unitary. Note that a quantum computer can apply O_x on a superposition of various i, something a classical computer cannot do.

§2.7 The Early Algorithms

Virtually all quantum algorithms work with **queries** in some form or other. For a given N-bit data $x = (x_0, \cdots, x_{N-1}) \in \{0,1\}^N$, where $N = 2^n$, let O_x be a linear map on $n+1$ qubits given by

$$\mathrm{O}_x : |i\rangle|b\rangle \mapsto |i\rangle|b \oplus x_i\rangle,$$

where $i \in \{0,1\}^n$, $b \in \{0,1\}$, $\oplus$ denotes exclusive-or (addition modulo 2), and the value of x_i is obtained through a memory access via a so-called "black-box", which is equipped to output the bit x_i on input i. The first n qubits of the state are called the address bits (or address register), while the $(n+1)$-th qubit is called the target bit.

Since O_x is equivalent to a swap of basis, it is unitary. Note that a quantum computer can apply O_x on a superposition of various i, something a classical computer cannot do.

§2.7 The Early Algorithms

Virtually all quantum algorithms work with **queries** in some form or other. For a given N-bit data $x = (x_0, \cdots, x_{N-1}) \in \{0,1\}^N$, where $N = 2^n$, let O_x be a linear map on $n+1$ qubits given by

$$\mathrm{O}_x : |i\rangle|b\rangle \mapsto |i\rangle|b \oplus x_i\rangle\,,$$

where $i \in \{0,1\}^n$, $b \in \{0,1\}$, $\oplus$ denotes exclusive-or (addition modulo 2), and the value of x_i is obtained through a memory access via a so-called "black-box", which is equipped to output the bit x_i on input i. The first n qubits of the state are called the address bits (or address register), while the $(n+1)$-th qubit is called the target bit.

Since O_x is equivalent to a swap of basis, it is unitary. Note that a quantum computer can apply O_x on a superposition of various i, something a classical computer cannot do.

§2.7 The Early Algorithms

Given the ability to make a query of the above type, we can also make a query of the form $|i\rangle \mapsto (-1)^{x_i}|i\rangle$ by setting the target bit to the state $|-\rangle \equiv \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$:

$$\mathrm{O}_x(|i\rangle|-\rangle) = |i\rangle\frac{1}{\sqrt{2}}\big(|x_i\rangle - |1-x_i\rangle\big) = (-1)^{x_i}|i\rangle|-\rangle\,.$$

This $\pm$-kind of query puts the output variable in the phase of the state: if x_i is 1 then we get a -1 in the phase of basis state $|i\rangle$; if $x_i = 0$ then nothing happens to $|i\rangle$. This "phase-oracle" is sometimes more convenient than the standard type of query. We sometimes denote the corresponding n-qubit unitary transformation (ignoring the last qubit $|-\rangle$) by $\mathrm{O}_{x,\pm}$.

§2.7 The Early Algorithms

Given the ability to make a query of the above type, we can also make a query of the form $|i\rangle \mapsto (-1)^{x_i}|i\rangle$ by setting the target bit to the state $|-\rangle \equiv \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$:

$$\mathrm{O}_x(|i\rangle|-\rangle) = |i\rangle\frac{1}{\sqrt{2}}\big(|x_i\rangle - |1 - x_i\rangle\big) = (-1)^{x_i}|i\rangle|-\rangle\,.$$

This $\pm$-kind of query puts the output variable in the phase of the state: if x_i is 1 then we get a -1 in the phase of basis state $|i\rangle$; if $x_i = 0$ then nothing happens to $|i\rangle$. This "phase-oracle" is sometimes more convenient than the standard type of query. We sometimes denote the corresponding n-qubit unitary transformation (ignoring the last qubit $|-\rangle$) by $\mathrm{O}_{x,\pm}$.

§2.7 The Early Algorithms

Given the ability to make a query of the above type, we can also make a query of the form $|i\rangle \mapsto (-1)^{x_i}|i\rangle$ by setting the target bit to the state $|-\rangle \equiv \mathrm{H}|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$:

$$\mathrm{O}_x(|i\rangle|-\rangle) = |i\rangle\frac{1}{\sqrt{2}}\big(|x_i\rangle - |1-x_i\rangle\big) = (-1)^{x_i}|i\rangle|-\rangle\,.$$

This $\pm$-kind of query puts the output variable in the phase of the state: if x_i is 1 then we get a -1 in the phase of basis state $|i\rangle$; if $x_i = 0$ then nothing happens to $|i\rangle$. This "phase-oracle" is sometimes more convenient than the standard type of query. We sometimes denote the corresponding n-qubit unitary transformation (ignoring the last qubit $|-\rangle$) by $\mathrm{O}_{x,\pm}$.

§2.7 The Early Algorithms

§2.7.1 Deutsch-Jozsa Algorithm

Deutsch-Jozsa problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ such that either

1. all x_i have the same value ("constant"), or
2. $N/2$ of the x_i are 0 and $N/2$ of the x_i are 1 ("balanced").

The goal is to find out whether x is constant or balanced.

The algorithm of Deutsch and Jozsa is as follows. We start in the n-qubit zero state $|0^n\rangle$, apply a Hadamard transform to each qubit, apply a query (in its $\pm$-form), apply another Hadamard to each qubit, and then measure the final state. As a unitary transformation, the algorithm would be $\mathrm{H}^{\otimes n}\mathrm{O}_{\pm}\mathrm{H}^{\otimes n}$. We have drawn the corresponding quantum circuit in Figure 4 (where time progresses from left to right).

§2.7 The Early Algorithms

§2.7.1 Deutsch-Jozsa Algorithm

Deutsch-Jozsa problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ such that either

1. all x_i have the same value ("constant"), or
2. $N/2$ of the x_i are 0 and $N/2$ of the x_i are 1 ("balanced").

The goal is to find out whether x is constant or balanced.

The algorithm of Deutsch and Jozsa is as follows. We start in the n-qubit zero state $|0^n\rangle$, apply a Hadamard transform to each qubit, apply a query (in its $\pm$-form), apply another Hadamard to each qubit, and then measure the final state. As a unitary transformation, the algorithm would be $\mathrm{H}^{\otimes n}\mathrm{O}_{\pm}\mathrm{H}^{\otimes n}$. We have drawn the corresponding quantum circuit in Figure 4 (where time progresses from left to right).

§2.7 The Early Algorithms

§2.7.1 Deutsch-Jozsa Algorithm

Deutsch-Jozsa problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ such that either

1. all x_i have the same value ("constant"), or
2. $N/2$ of the x_i are 0 and $N/2$ of the x_i are 1 ("balanced").

The goal is to find out whether x is constant or balanced.

The algorithm of Deutsch and Jozsa is as follows. We start in the n-qubit zero state $|0^n\rangle$, apply a Hadamard transform to each qubit, apply a query (in its $\pm$-form), apply another Hadamard to each qubit, and then measure the final state. As a unitary transformation, the algorithm would be $\mathrm{H}^{\otimes n}\mathrm{O}_{\pm}\mathrm{H}^{\otimes n}$. We have drawn the corresponding quantum circuit in Figure 4 (where time progresses from left to right).

§2.7 The Early Algorithms

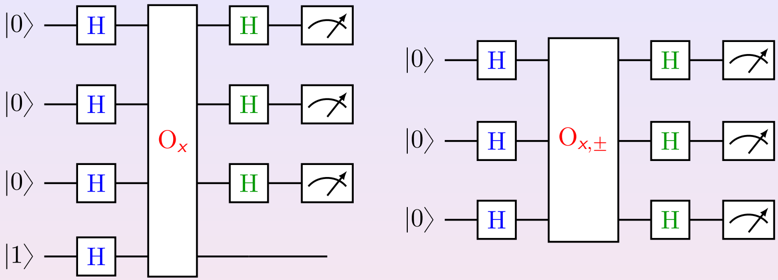


Figure 4: The Deutsch-Jozsa algorithm for $n = 3$

Let us follow the state through these operations. Initially we have the state $|0^n\rangle$. After the first Hadamard transforms we have obtained the uniform superposition of all i:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle .$$

§2.7 The Early Algorithms

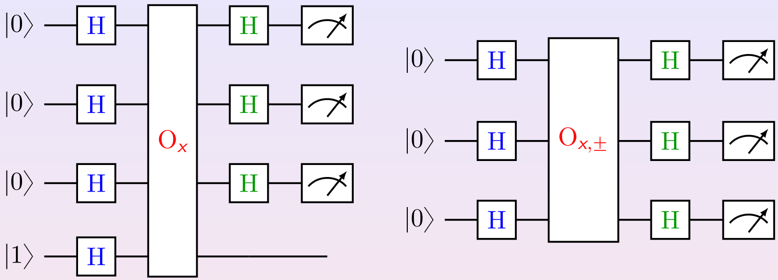


Figure 4: The Deutsch-Jozsa algorithm for $n = 3$

Let us follow the state through these operations. Initially we have the state $|0^n\rangle$. After the first Hadamard transforms we have obtained the uniform superposition of all i:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle .$$

§2.7 The Early Algorithms

The $\mathrm{O}_{\pm}$-query turns this into

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle .$$

Applying the second batch of Hadamards gives the final superposition

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \sum_{j \in \{0,1\}^n} (-1)^{i \bullet j} |j\rangle ,$$

where $i \bullet j = \sum_{k=1}^{n} i_k j_k$ is the bitwise dot product of i and j as before.

Since $i \bullet 0^n = 0$ for all $i \in \{0,1\}^n$, we see that the amplitude of the $|0^n\rangle$-state in the final superposition is

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{if } x_i = 0 \text{ for all } i , \\ -1 & \text{if } x_i = 1 \text{ for all } i , \\ 0 & \text{if } x \text{ is balanced} . \end{cases}$$

§2.7 The Early Algorithms

The $\mathrm{O}_{\pm}$-query turns this into

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle \,.$$

Applying the second batch of Hadamards gives the final superposition

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \sum_{j \in \{0,1\}^n} (-1)^{i \bullet j} |j\rangle \,,$$

where $i \bullet j = \sum_{k=1}^{n} i_k j_k$ is the bitwise dot product of i and j as before.

Since $i \bullet 0^n = 0$ for all $i \in \{0,1\}^n$, we see that the amplitude of the $|0^n\rangle$-state in the final superposition is

$$\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} = \begin{cases} 1 & \text{if } x_i = 0 \text{ for all } i \,, \\ -1 & \text{if } x_i = 1 \text{ for all } i \,, \\ 0 & \text{if } x \text{ is balanced} \,. \end{cases}$$

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output "constant" if those bits are the same and "balanced" if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output "constant" if those bits are the same and "balanced" if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output "constant" if those bits are the same and "balanced" if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output “constant” if those bits are the same and “balanced” if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output "constant" if those bits are the same and "balanced" if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Hence the final observation will yield $|0^n\rangle$ if x is constant and will yield some other state if x is balanced. Accordingly, the Deutsch-Jozsa problem can be solved with certainty using only 1 quantum query and $\mathcal{O}(n)$ other operations. In contrast, it is easy to see that any classical deterministic algorithm needs $N/2+1$ queries in the worst case scenario: if it has made only $N/2$ queries and seen only 0s, the correct output is still undetermined. However, a classical algorithm can solve this problem efficiently if we allow a small error probability: just query x at two random positions, output "constant" if those bits are the same and "balanced" if they are different. This algorithm outputs the correct answer with probability 1 if x is constant and outputs the correct answer with probability $1/2$ if x is balanced. Thus the quantum-classical separation of this problem only holds if we consider algorithms without error probability.

§2.7 The Early Algorithms

Remark: In a lot of literatures, the Deutsch-Jozsa problem is formulated as: Let $f : \{0,1\}^n \to \{0,1\}$ satisfy either f is a constant function or $\#f^{-1}(\{0\}) = \#f^{-1}(\{1\}) = 2^{n-1}$ (such f is said to be balanced). Determine if f is constant or balanced. In such a case, the O_x operator is usually denoted by U_f, and the quantum circuit for the Deutsch-Jozsa algorithm is usually drawn as

Figure 5: Another way of drawing the quantum circuit for the Deutsch-Jozsa algorithm

§2.7 The Early Algorithms

Remark: In a lot of literatures, the Deutsch-Jozsa problem is formulated as: Let $f : \{0,1\}^n \to \{0,1\}$ satisfy either f is a constant function or $\#f^{-1}(\{0\}) = \#f^{-1}(\{1\}) = 2^{n-1}$ (such f is said to be balanced). Determine if f is constant or balanced. In such a case, the O_x operator is usually denoted by U_f, and the quantum circuit for the Deutsch-Jozsa algorithm is usually drawn as

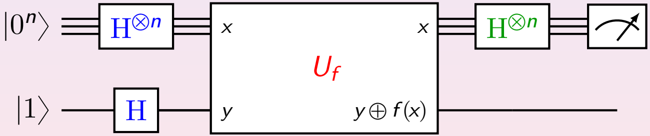


Figure 5: Another way of drawing the quantum circuit for the Deutsch-Jozsa algorithm

§2.7 The Early Algorithms

Remark: In general it is not easy to construct a quantum circuit for the oracle U_f; however, for some specific f a quantum implementation of U_f is possible. For example, let $f\colon \{0,1\}^n \to \{0,1\}$ be given by $f(x) = x_n$ if $x = (x_1, \cdots, x_n)$; that is, the value of f is identical to the lowest digits of the input. Then $U_f = \mathbf{I}_{n-1} \otimes \mathbf{CNOT}$, where $\mathbf{I}_{n-1}$ is the identity map on $(n-1)$ qubit system, since

$$
\begin{aligned}
(\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x\rangle|y\rangle) &= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}x_n\rangle|y\rangle) \\
&= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}\rangle|x_n y\rangle) \\
&= \big(\mathbf{I}_{n-1}|x_1 \cdots x_{n-1}\rangle\big) \otimes \big(\mathbf{CNOT}(|x_n\rangle|y\rangle)\big) \\
&= |x_1 \cdots x_{n-1}\rangle|x_n\rangle|y \oplus x_n\rangle = |x_1 \cdots x_n\rangle|y \oplus x_n\rangle \\
&= |x\rangle|y \oplus f(x)\rangle .
\end{aligned}
$$

§2.7 The Early Algorithms

Remark: In general it is not easy to construct a quantum circuit for the oracle U_f; however, for some specific f a quantum implementation of U_f is possible. For example, let $f\colon \{0,1\}^n \to \{0,1\}$ be given by $f(x) = x_n$ if $x = (x_1, \cdots, x_n)$; that is, the value of f is identical to the lowest digits of the input. Then $U_f = \mathbf{I}_{n-1} \otimes \mathbf{CNOT}$, where $\mathbf{I}_{n-1}$ is the identity map on $(n-1)$ qubit system, since

$$
\begin{aligned}
(\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x\rangle|y\rangle) &= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}x_n\rangle|y\rangle) \\
&= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}\rangle|x_n y\rangle) \\
&= \big(\mathbf{I}_{n-1}|x_1 \cdots x_{n-1}\rangle\big) \otimes \big(\mathbf{CNOT}(|x_n\rangle|y\rangle)\big) \\
&= |x_1 \cdots x_{n-1}\rangle|x_n\rangle|y \oplus x_n\rangle = |x_1 \cdots x_n\rangle|y \oplus x_n\rangle \\
&= |x\rangle|y \oplus f(x)\rangle .
\end{aligned}
$$

§2.7 The Early Algorithms

Remark: In general it is not easy to construct a quantum circuit for the oracle U_f; however, for some specific f a quantum implementation of U_f is possible. For example, let $f\colon \{0,1\}^n \to \{0,1\}$ be given by $f(x) = x_n$ if $x = (x_1, \cdots, x_n)$; that is, the value of f is identical to the lowest digits of the input. Then $U_f = \mathbf{I}_{n-1} \otimes \mathbf{CNOT}$, where $\mathbf{I}_{n-1}$ is the identity map on $(n-1)$ qubit system, since

$$\begin{aligned}(\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x\rangle|y\rangle) &= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}x_n\rangle|y\rangle) \\ &= (\mathbf{I}_{n-1} \otimes \mathbf{CNOT})(|x_1 \cdots x_{n-1}\rangle|x_n y\rangle) \\ &= \big(\mathbf{I}_{n-1}|x_1 \cdots x_{n-1}\rangle\big) \otimes \big(\mathbf{CNOT}(|x_n\rangle|y\rangle)\big) \\ &= |x_1 \cdots x_{n-1}\rangle|x_n\rangle|y \oplus x_n\rangle = |x_1 \cdots x_n\rangle|y \oplus x_n\rangle \\ &= |x\rangle|y \oplus f(x)\rangle .\end{aligned}$$

§2.7 The Early Algorithms

Therefore, U_f can be implemented by the following quantum circuit

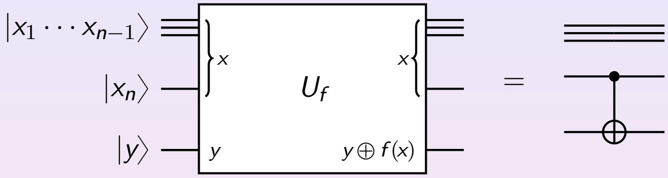


Figure 6: A quantum circuit for U_f with $f(x_1, \cdots, x_n) = x_n$

§2.7 The Early Algorithms

§2.7.2 Bernstein-Vazirani

Bernstein-Vazirani problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ with the property that there is some unknown $a \in \{0,1\}^n$ such that $x_i = (i \bullet a) \bmod 2$. The goal is to find a.

The Bernstein-Vazirani algorithm is exactly the same as the Deutsch-Jozsa algorithm, but now the final observation miraculously yields a. Since $(-1)^{x_i} = (-1)^{(i \bullet a) \bmod 2} = (-1)^{i \bullet a}$, we can write the state obtained after the query as:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{i \bullet a} |i\rangle .$$

Since Hadamard is its own inverse, applying a Hadamard to each qubit will turn this into the classical state $|a\rangle$ and hence solves the problem with 1 query and $\mathcal{O}(n)$ other operations.

§2.7 The Early Algorithms

§2.7.2 Bernstein-Vazirani

Bernstein-Vazirani problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ with the property that there is some unknown $a \in \{0,1\}^n$ such that $x_i = (i \bullet a) \bmod 2$. The goal is to find a.

The Bernstein-Vazirani algorithm is exactly the same as the Deutsch-Jozsa algorithm, but now the final observation miraculously yields a. Since $(-1)^{x_i} = (-1)^{(i \bullet a) \bmod 2} = (-1)^{i \bullet a}$, we can write the state obtained after the query as:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{i \bullet a} |i\rangle .$$

Since Hadamard is its own inverse, applying a Hadamard to each qubit will turn this into the classical state $|a\rangle$ and hence solves the problem with 1 query and $\mathcal{O}(n)$ other operations.

§2.7 The Early Algorithms

§2.7.2 Bernstein-Vazirani

Bernstein-Vazirani problem: For $N = 2^n$, we are given $x \in \{0,1\}^N$ with the property that there is some unknown $a \in \{0,1\}^n$ such that $x_i = (i \bullet a) \bmod 2$. The goal is to find a.

The Bernstein-Vazirani algorithm is exactly the same as the Deutsch-Jozsa algorithm, but now the final observation miraculously yields a. Since $(-1)^{x_i} = (-1)^{(i \bullet a) \bmod 2} = (-1)^{i \bullet a}$, we can write the state obtained after the query as:

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{x_i} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{i \bullet a} |i\rangle .$$

Since Hadamard is its own inverse, applying a Hadamard to each qubit will turn this into the classical state $|a\rangle$ and hence solves the problem with 1 query and $\mathcal{O}(n)$ other operations.

§2.7 The Early Algorithms

In contrast, any classical algorithm (even a randomized one with small error probability) needs to ask n queries for information-theoretic reasons: the final answer consists of n bits and one classical query gives at most 1 bit of information. Bernstein and Vazirani also defined a recursive version of this problem, which can be solved exactly by a quantum algorithm in poly(n) steps, but for which any classical randomized algorithm needs $n^{\Omega(\log n)}$ steps.

§2.7 The Early Algorithms

In contrast, any classical algorithm (even a randomized one with small error probability) needs to ask n queries for information-theoretic reasons: the final answer consists of n bits and one classical query gives at most 1 bit of information. Bernstein and Vazirani also defined a recursive version of this problem, which can be solved exactly by a quantum algorithm in poly(n) steps, but for which any classical randomized algorithm needs $n^{\Omega(\log n)}$ steps.