62
Quantum Computation

Zijian Diao
Ohio University Eastern

Modern computer science emerged when the eminent British mathematician Alan Turing invented the concept of Turing machine (TM) in 1936. Though very simple and primitive, TM serves as the universal model for all known physical computation devices. The principles of quantum mechanics, another revolutionary scientific discovery of the 20^{th} century, had never been incorporated in the theory of computation until the early 1980s. P. Benioff first coined the concept of quantum Turing machine (QTM). Motivated by the problem that classical computers cannot simulate quantum systems efficiently, R. Feynman posed the quantum computer as the solution. The field of quantum computation was born.

Quantum computation mainly studies the construction and analysis of quantum algorithms that outperform the classical counterparts. In terms of computability, quantum computers and classical computers possess exactly the same computational power. But in terms of computational complexity, which measures the efficiency of computation, there are many examples confirming that quantum computers do solve certain problems faster. The two most significant ones are Shor's factorization algorithm and Grover's search algorithm, among other examples such as the Deutsch–Jozsa problem, the Bernstein–Vazirani problem, and Simon's problem.

Quantum computers share many common features of the classical computers. In a classical computer, information is encoded in binary states (for example, 0 denotes the low voltage state and 1 denotes the high voltage state), and processed by various logic gates. In a quantum computer, information is represented by the states of the microscopic quantum systems, called qubits, and manipulated by various quantum gates. A qubit could be a two-level atom in the excited/ground states, a photon with horizontal/vertical polarizations, or a spin-$\frac{1}{2}$ particle with up/down spins. The state of a qubit can be controlled via physical devices such as laser and microwave. The distinctions between quantum and classical computers originate from the special characteristic of quantum mechanics. In contrast to a classical system, a quantum system can exist in different states at the same time, an interesting phenomenon called *superposition*. Superposition enables quantum computers to process data in parallel. That is why a quantum computer can solve certain problems faster than a classical computer. But, when we measure a quantum system, it randomly collapses to one of the basis states. This indeterministic nature makes the design of efficient quantum algorithms highly nontrivial. Another distinctive feature of the quantum computer is that the operations performed by quantum gates must be unitary. This is the natural consequence of the unobserved quantum systems evolving according to the Schrödinger equation.

Throughout this chapter, we will use Dirac's bra-ket notation (see Section 59.4 for more information). In quantum mechanics, the state of a quantum system is described by a unit vector in a complex Hilbert space (a complete inner product vector space). Under Dirac's bra-ket notation, we use $|\psi\rangle$ ("ket") to denote a vector in the Hilbert space and $\langle\psi|$ ("bra") for its dual. The inner product of two vectors $|\psi\rangle$ and $|\phi\rangle$ is denoted $\langle\psi|\phi\rangle$. We also use $|\psi\rangle|\phi\rangle$ and $|\psi\phi\rangle$ interchangeably with the notation for the tensor product $|\psi\rangle \otimes |\phi\rangle$.

62.1 Basic Concepts

Definitions:

A **(classical) Turing machine** (TM) is an abstract computing device consisting of a finite control, a two-way infinite tape, and a read/write head that moves to the left or right on the tape. It can be described by a 6-tuple $(Q, A, B, \delta, q_0, q_a)$, where Q is a finite set of control states, A a finite alphabet, $B \in A$ the blank symbol, q_0, $q_a \in Q$ the initial and accepting states, and δ the transition function

$$\delta : Q \times A \to Q \times A \times \{L, R\}.$$

L and R stand for moving left and right, respectively.

A **quantum Turing machine** (QTM) is an abstract computing device consisting of a finite control, a two-way infinite tape, and a read/write head that moves to the left or right of the tape. It can be described by a 6-tuple $(Q, A, B, \delta, q_0, q_a)$, where Q is a finite set of control states, A a finite alphabet, $B \in A$ the blank symbol, q_0, $q_a \in Q$ the initial and accepting states, and δ the transition amplitude function

$$\delta : Q \times A \times Q \times A \times \{L, R\} \to \mathbb{C}.$$

The transition amplitude function satisfies

$$\sum_{(q_2,a_2,d)\in Q\times A\times\{L,R\}} |\delta(q_1, a_1, q_2, a_2, d)|^2 = 1,$$

for any $(q_1, a_1) \in Q \times A$. L and R stand for moving left and right, respectively.

A **quantum bit** (qubit) is a two-level quantum system, modeled by the two-dimensional Hilbert space H_2, with basis $\{|0\rangle, |1\rangle\}$. For example, for a spin-$\frac{1}{2}$ particle, $|0\rangle$ and $|1\rangle$ denote the spin-down and spin-up states, respectively. They can be mapped to the standard basis for H_2 as $|0\rangle = [1 \quad 0]^T$ and $|1\rangle = [0 \quad 1]^T$.

A **quantum register** of length n is an ordered system of n qubits, modeled by the 2^n-dimensional Hilbert space $H_{2^n} = H_2 \otimes H_2 \otimes \ldots \otimes H_2$ with basis $\{|00\ldots00\rangle, |00\ldots01\rangle, |00\ldots10\rangle, |00\ldots11\rangle, \ldots, |11\ldots11\rangle\}$. The basis states are ordered in lexicographic order. We may also write each basis state as $|i\rangle$ for $0 \le i < 2^n$, interpreting the n-bit string of 0s and 1s as the binary representation of i.

An **one-bit quantum gate** is a unitary map $U : H_2 \to H_2$.

An n**-bit quantum gate** is a unitary map $U : H_2 \otimes H_2 \otimes \ldots \otimes H_2 \to H_2 \otimes H_2 \otimes \ldots \otimes H_2$.

A **quantum circuit** on n bits is a unitary map on H_{2^n}, which can be represented by a concatenation of a finite number of quantum gates.

Facts:

1. [BV93] Any function which is computable by a TM is computable by a QTM.
2. [Fey82] Any function that is computable by a QTM is computable by a TM.
3. [NC00, pp. 13] A general state of a qubit is a unit vector $a|0\rangle + b|1\rangle$, where $a, b \in \mathbb{C}$ and $|a|^2 + |b|^2 = 1$. a and b are the probability amplitudes of $|0\rangle$ and $|1\rangle$, respectively. A measurement of a qubit yields either $|0\rangle$ or $|1\rangle$, with probability $|a|^2$ or $|b|^2$, respectively.
4. [BB02] A general state of n-bit quantum register is a unit vector

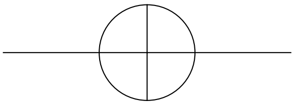
$$\sum_{x=00...0}^{11...1} \psi_x |x\rangle,$$

where $\psi_x \in \mathbb{C}$ and $\sum_{x=00...0}^{11...1} |\psi_x|^2 = 1$. ψ_x is the probability amplitude of $|x\rangle$. A measurement of a quantum register yields $|x\rangle \in \{|00\ldots 0\rangle, |00\ldots 1\rangle, \ldots, |11\ldots 1\rangle\}$, with probability $|\psi_x|^2$.

Examples:

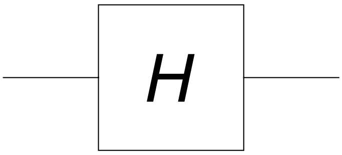
This section contains a list of quantum gates that are frequently used. We provide the description of their effects on the basis states, matrix representations, and circuit diagrams. In the circuit diagrams, the horizontal lines stand for the qubits. When there is no gate on the line, no operation is done, which can be interpreted as the identity operation. When the diagram of a gate shows up on a horizontal line/lines, the corresponding gate operation is applied to the qubit/qubits, with the input coming from the left and the output (result) going out to the right. The entire circuit diagram is read from left to right.

1. NOT gate Λ_0: $\Lambda_0|0\rangle = |1\rangle$, $\Lambda_0|1\rangle = |0\rangle$, or $\Lambda_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.



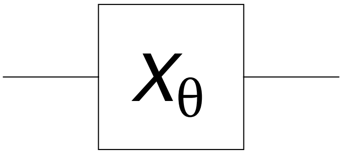
2. The Walsh–Hadamard gate H: $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, or

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



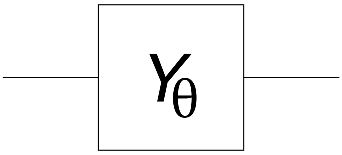
3. The x-rotation gate X_θ: $X_\theta|0\rangle = \cos\frac{\theta}{2}|0\rangle - i\sin\frac{\theta}{2}|1\rangle$, $X_\theta|1\rangle = -i\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$, or

$$X_\theta = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}.$$



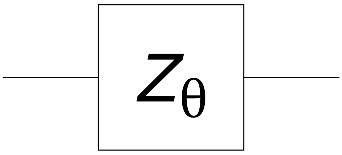
4. The y-rotation gate Y_θ: $Y_\theta|0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$, $Y_\theta|1\rangle = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}|1\rangle$, or

$$Y_\theta = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}.$$



5. The z-rotation gate Z_θ: $Z_\theta|0\rangle = e^{-i\theta/2}|0\rangle$, $Z_\theta|1\rangle = e^{i\theta/2}|1\rangle$, or

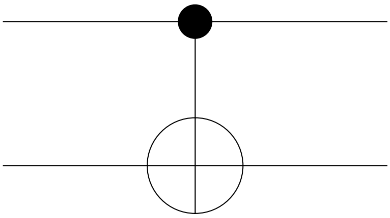
$$Z_\theta = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}.$$



6. Controlled-NOT gate Λ_1: $\Lambda_1|00\rangle = |00\rangle$, $\Lambda_1|01\rangle = |01\rangle$, $\Lambda_1|10\rangle = |11\rangle$, $\Lambda_1|11\rangle = |10\rangle$, or,

$$\Lambda_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

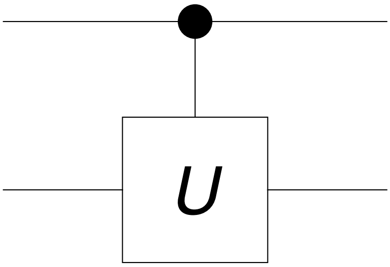
The first qubit acts as the control bit; the operation on the second qubit is controlled by it. If the control bit is $|0\rangle$, no operation is done on the second qubit. If the control bit is $|1\rangle$, the NOT gate is applied to the second qubit. There is no change on the control bit in either case. In the diagram for the Controlled-NOT gate, a black dot denotes the control bit and a vertical line signifies the control action.



7. Two-bit Controlled-U gate $\Lambda_1(U)$, where U is any arbitrary one-bit unitary transform: $\Lambda_1(U)|00\rangle = |00\rangle$, $\Lambda_1(U)|01\rangle = |01\rangle$, $\Lambda_1(U)|10\rangle = |1\rangle U|0\rangle$, $\Lambda_1(U)|11\rangle = |1\rangle U|1\rangle$, or,

$$\Lambda_1(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & & \\ & & & U \\ 0 & 0 & & \end{bmatrix}.$$

The first qubit acts as the control bit; the operation on the second qubit is controlled by it. If the control bit is $|0\rangle$, no operation is done on the second qubit. If the control bit is $|1\rangle$, the one-bit gate U is applied to the second qubit. There is no change on the control bit in either case. In the diagram for the Controlled-U gate, a black dot denotes the control bit and a vertical line signifies the control action.

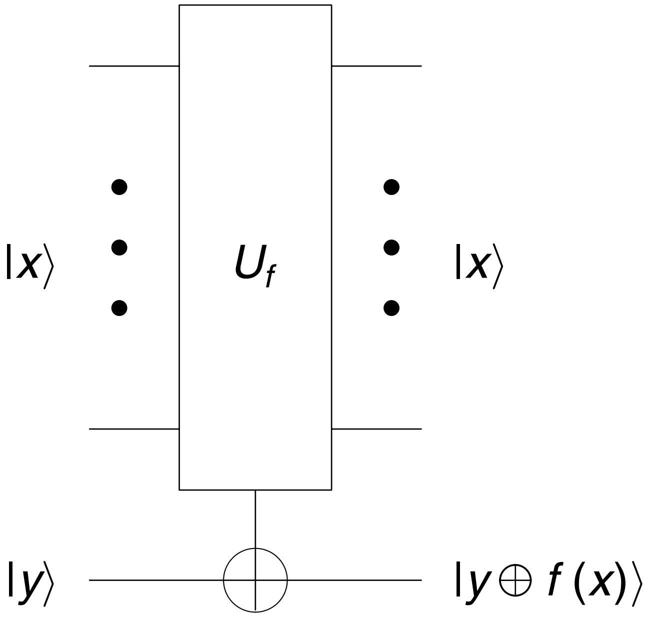


8. Function evaluation operator $U_f : H_{2^n} \otimes H_{2^m} \rightarrow H_{2^n} \otimes H_{2^m}$, where $f : \{0,1\}^n \rightarrow \{0,1\}^m$, $|x\rangle \in H_{2^n}$, and $|y\rangle \in H_{2^m}$, is given by

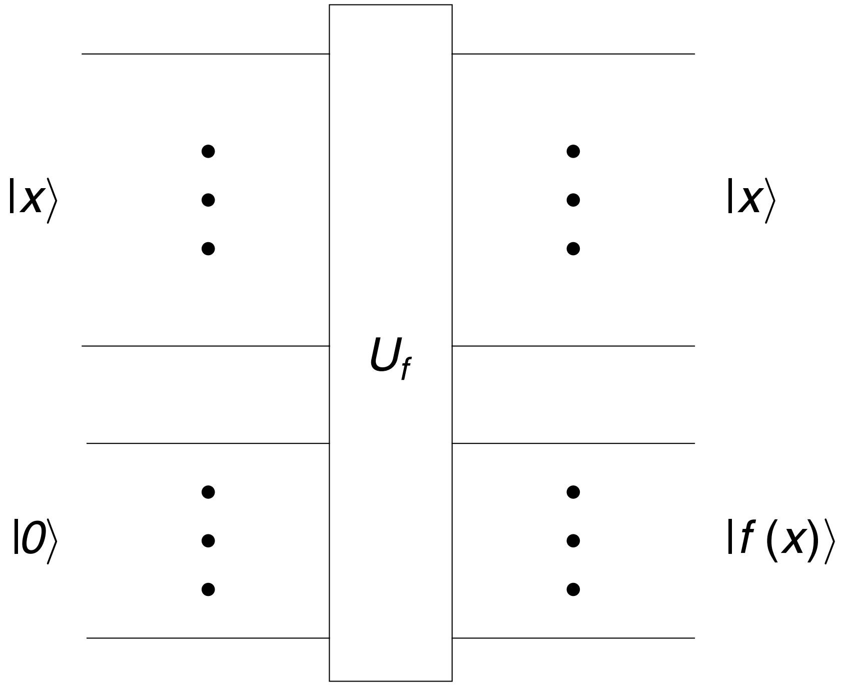
$$|x\rangle|y\rangle \rightarrow |x\rangle|y + f(x)\text{mod}2^m\rangle.$$

Two special cases of this operator will be used in the algorithms discussed later.

- $m = 1$, U_f is given by: $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, where $\oplus$ is the addition mod 2.



- $y = 0$, U_f is given by: $|x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$.



9. Quantum Fourier transform (QFT) (n-bit):

$$|x\rangle \rightarrow \frac{1}{2^{n-1}} \sum_{y=0}^{2^n-1} e^{2\pi i xy/2^n} |y\rangle,$$

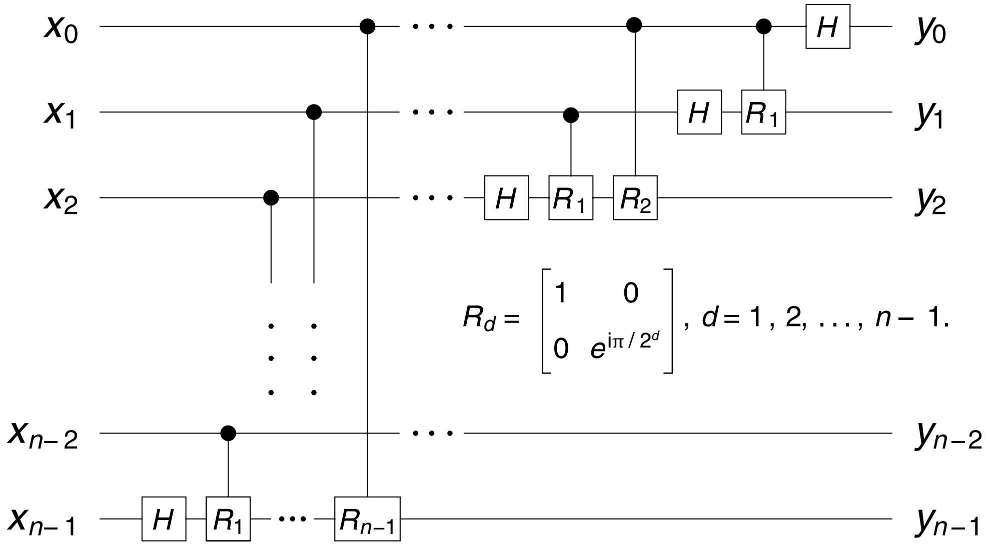
where $x \in \{0, 1, \ldots, 2^n - 1\}$. This operator is a crucial building block of Shor's Factorization Algorithm. The following example manifests the power of QFT.

Example: Define a function $f : \{0, 1, 2, 3\} \rightarrow \{0, \frac{1}{\sqrt{2}}\}$ by $f(1) = f(3) = \frac{1}{\sqrt{2}}$ and $f(0) = f(2) = 0$. This function has period 2. Consider a 2-bit quantum system with state $\frac{1}{\sqrt{2}}(|1\rangle + |3\rangle)$, where the probability amplitudes of the basis states $|0\rangle$, $|1\rangle$, $|2\rangle$, and $|3\rangle$ are specified by the function values of f at 0, 1, 2, and 3. Apply QFT to this state.

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|1\rangle + |3\rangle) \\
&\quad \rightarrow \frac{1}{2\sqrt{2}}(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle) + \frac{1}{2\sqrt{2}}(|0\rangle - i|1\rangle - |2\rangle + i|3\rangle) \\
&\quad = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle).
\end{aligned}$$

Measurement of the result yields 2, the period of f, with probability $\frac{1}{2}$. Thus, QFT provides a tool for period finding.

In the diagram for QFT, $x_{n-1}x_{n-2}\ldots x_2x_1x_0$ and $y_{n-1}y_{n-2}\ldots y_2y_1y_0$ are the binary representations of x and y, respectively.


x_0
x_1
x_2
x_{n-2}
x_{n-1}
y_0
y_1
y_2
y_{n-2}
y_{n-1}
H
R_1
R_2
R_{n-1}
$R_d = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2^d} \end{bmatrix}$, $d = 1, 2, \ldots, n-1$.

62.2 Universal Quantum Gates

Definitions:

A 1-bit gate A is **special** if $\det(A) = 1$.

A 2-bit gate V is **primitive** if V is decomposable, i.e., there exist 1-bit gates S and T such that $V|xy\rangle = S|x\rangle \otimes T|y\rangle$, or $V|xy\rangle = S|y\rangle \otimes T|x\rangle$, for any state $|xy\rangle$.

A 2-bit gate V is **imprimitive** if it is not primitive.

A collection of quantum gates G is **universal** if, for each $n \in \mathbb{N}$, every n-bit quantum gate can be approximated with arbitrary accuracy by a circuit consisting of quantum gates in G.

A collection of quantum gates G is **exactly universal** if, for each $n \in \mathbb{N}$, every n-bit quantum gate can be obtained exactly by a circuit consisting of quantum gates in G.

Facts:

The following facts can be found in [BB02].

1. The collection of all 1-bit gates and any imprimitive 2-bit gate is universal.
2. The collection of all 1-bit gates and any imprimitive 2-bit gate is exactly universal.
3. The collection of all special 1-bit gates and any imprimitive 2-bit gate V with $\det(V)$ not being a root of unity is universal.

Examples:

1. The X_θ, Y_θ, and Z_θ gates are special.
2. The NOT gate and Walsh–Hadamard gate are not special.
3. The 2-bit gate $V = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$ is primitive, $V|xy\rangle = H|x\rangle \otimes |y\rangle$.

4. The Controlled-NOT gate is imprimitive.
5. The collection of all 1-bit gates and Controlled-NOT gate is universal, and exactly universal.
6. The collection of all X_θ, Y_θ, and Z_θ gates and Controlled-phase gate $\Lambda_1(Q_\theta)$, where $Q_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ and $e^{i\theta}$ is not a root of unity, is universal.

62.3 Deutsch's Problem

Definitions:

A **Boolean function** is a function with codomain $\{0, 1\}$.

A Boolean function $f : \{0, 1\} \to \{0, 1\}$ is **constant** if $f(0) = f(1)$.

A Boolean function $f : \{0, 1\} \to \{0, 1\}$ is **balanced** if $f(0) \neq f(1)$.

Problem: Deutsch

Given a Boolean function $f : \{0, 1\} \to \{0, 1\}$, determine whether it is constant or balanced.

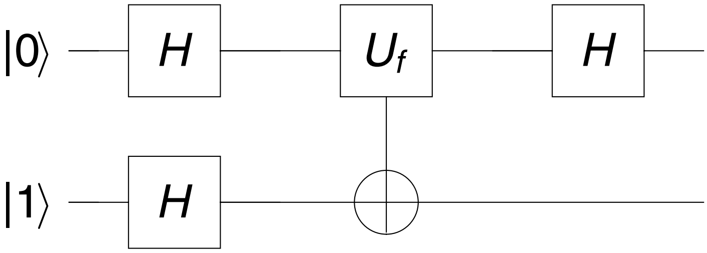
Algorithm: Deutsch

1. Prepare a two-bit quantum register and initialize it to the state $|0\rangle|1\rangle$.
2. Apply the Walsh–Hadamard transform to both qubits.
3. Apply the function evaluation operator U_f

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

4. Apply the Walsh–Hadamard transform to the first qubit.
5. Measure the first qubit. If the outcome is $|0\rangle$, f is constant. If the outcome is $|1\rangle$, f is balanced.

Circuit Diagram: Deutsch



Facts:

The following facts can be found in [CEM98].

1. With the classical computer, we need two evaluations of f to determine whether f is constant or balanced.
2. With the quantum computer, we need only one evaluation of f to determine whether f is constant or balanced.

Examples:

1. Let $f(0) = 0$ and $f(1) = 1$. The following sequence of quantum states shows the result of computation utilizing Deutsch's Algorithm. We start from the initial state $|0\rangle|1\rangle$. Then,

$$\begin{aligned}
&|0\rangle|1\rangle\\
&\to \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|0\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&\to \frac{|0\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\frac{|1\rangle-|0\rangle}{\sqrt{2}}\\
&= \frac{|0\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&\to |1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}.
\end{aligned}$$

   The outcome of measuring the first qubit is $|1\rangle$, hence, f is balanced.

2. Let $f(0) = 0$ and $f(1) = 0$. The following sequence of quantum states shows the result of computation utilizing Deutsch's Algorithm. We start from the initial state $|0\rangle|1\rangle$. Then,

$$\begin{aligned}
&|0\rangle|1\rangle\\
&\to \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|0\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&\to \frac{|0\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&\to |0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}.
\end{aligned}$$

   The outcome of measuring the first qubit is $|0\rangle$, hence, f is constant.

62.4 Deutsch–Jozsa Problem

Definitions:

A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is **constant** if $f(x) = c$, $c \in \{0,1\}$, for all $x \in \{0,1\}^n$.

A Boolean function $f : \{0,1\}^n \to \{0,1\}$ is **balanced** if the function value is 1 (or 0) for exactly half of the input values, i.e., card $\left(f^{-1}(\{1\})\right) =$ card $\left(f^{-1}(\{0\})\right)$.

Problem: Deutsch–Jozsa

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, which is either constant or balanced, determine whether it is constant or balanced.

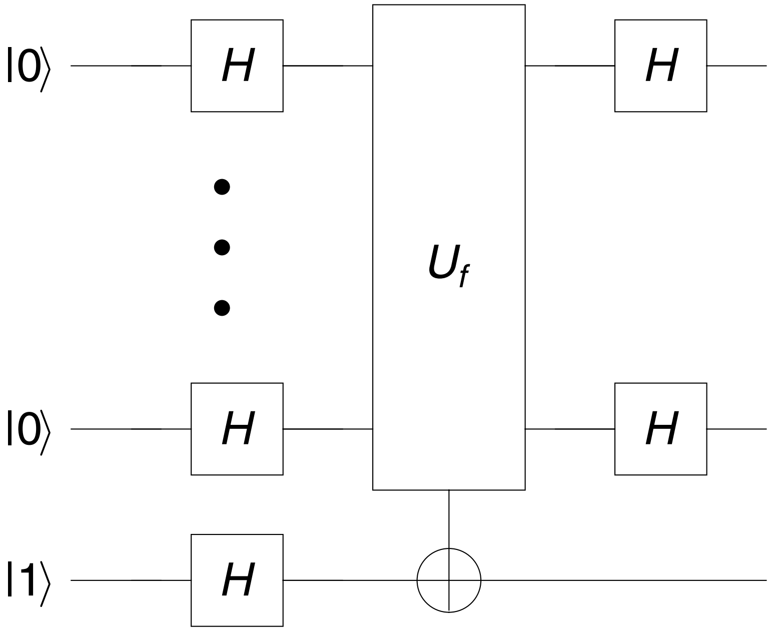
Algorithm: Deutsch–Jozsa

1. Prepare an $(n+1)$-bit quantum register and initialize it to the state $(|0\rangle)^n|1\rangle$.
2. Apply the Walsh–Hadamard transform to all the qubits.
3. Apply the function evaluation operator U_f:

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

4. Apply the Walsh–Hadamard transform to the first n qubits.
5. Measure the first n qubit. If the outcome is $|00\ldots 0\rangle$, f is constant. If the outcome is not $|00\ldots 0\rangle$, f is balanced.

Circuit Diagram: Deutsch–Jozsa



Facts:

The following facts can be found in [CEM98].

1. With the classical computer, we need at least $2^{n-1}+1$ evaluations of f to determine with certainty whether f is constant or balanced.
2. With the quantum computer, we need only one evaluation of f to determine with certainty whether f is constant or balanced.

Examples:

1. Let $n = 2$ and $f(00) = f(01) = f(10) = f(11) = 1$. The following sequence of quantum states shows the result of computation utilizing Deutsch–Jozsa's Algorithm. We start from the initial state $|00\rangle|1\rangle$. Then,

$$
\begin{aligned}
&|00\rangle|1\rangle \\
&\to \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\to \frac{|00\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} \\
&= -\frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{-|00\rangle-|01\rangle-|10\rangle-|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = -\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\to -|00\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}.
\end{aligned}
$$

The outcome of measuring the first 2 qubit is $|00\rangle$, hence, f is constant.

2. Let $n = 2$, $f(00) = f(01) = 0$, and $f(10) = f(11) = 1$. The following sequence of quantum states shows the result of computation utilizing Deutsch–Jozsa's Algorithm. We start from the initial state $|00\rangle|1\rangle$. Then,

$$
\begin{aligned}
&|00\rangle|1\rangle \\
&\to \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\to \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle+|01\rangle-|10\rangle-|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\to |10\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}.
\end{aligned}
$$

The outcome of measuring the first 2 qubit is $|10\rangle$, hence, f is balanced.

62.5 Bernstein–Vazirani Problem

Definitions:

Let $x = x_1x_2\ldots x_n$ and $y = y_1y_2\ldots y_n$ be two n-bit strings from $\{0,1\}^n$. The **dot product** $x \cdot y$ is the mod 2 sum of the bitwise products:

$$x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \ldots \oplus x_ny_n.$$

Problem: Bernstein–Vazirani

Given a Boolean function $f_a : \{0,1\}^n \to \{0,1\}$ defined by $f_a(x) = a \cdot x$, where a is an unknown n-bit string in $\{0,1\}^n$, determine the value of a.

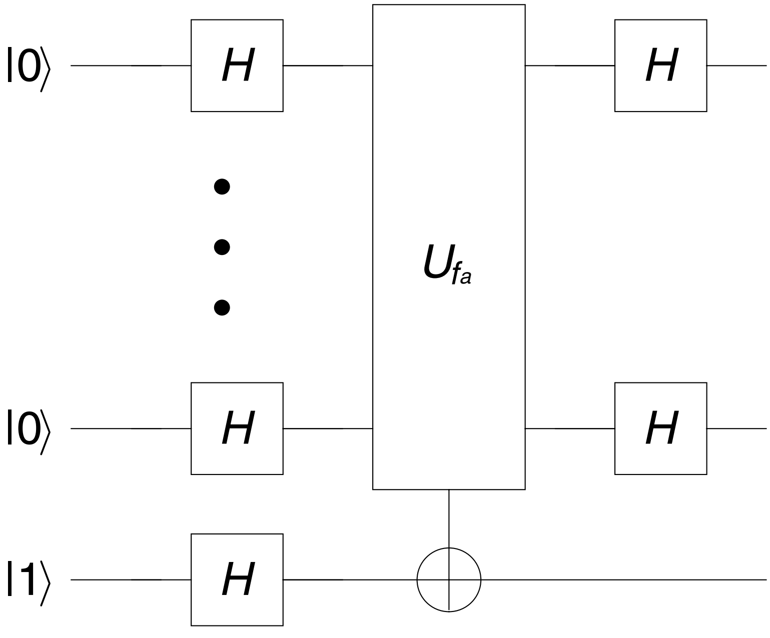
Algorithm: Bernstein–Vazirani

1. Prepare an $(n+1)$-bit quantum register and initialize it to the state $(|0\rangle)^n|1\rangle$.
2. Apply the Walsh–Hadamard transform to all the qubits.
3. Apply the function evaluation operator U_{f_a}:

$$U_{f_a} : |x\rangle|y\rangle \to |x\rangle|y \oplus f_a(x)\rangle.$$

4. Apply the Walsh–Hadamard transform to the first n qubits.
5. Measure the first n qubits. The outcome is $|a\rangle$.

Circuit Diagram: Bernstein–Vazirani



Facts:

The following facts can be found in [BV93].

1. With the classical computer, we need n evaluations of f_a to determine the value of a.
2. With the quantum computer, we need only one evaluation of f_a to determine the value of a.

Examples:

Let $a = 11$, a 2-bit string. The following sequence of quantum states shows the result of computation utilizing Bernstein–Vazirani's Algorithm. We start from the initial state $|00\rangle|1\rangle$. Then,

$$\begin{aligned}
&|00\rangle|1\rangle \\
&\to \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}
\end{aligned}$$

$$
\begin{aligned}
&\to \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}+\frac{|01\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}}+\frac{|10\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}}+\frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&=\frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}-\frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}-\frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}+\frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&=\frac{|00\rangle-|01\rangle-|10\rangle+|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}=\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
&\to |11\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}.
\end{aligned}
$$

The outcome of measuring the first 2 qubits is $|11\rangle$, hence, $a = 11$.

62.6 Simon's Problem

Definitions:

A function $f : \{0,1\}^n \to \{0,1\}^n$ is **2–1** if for each $z \in \text{range}(f)$, there are exactly two distinct n-bit strings x and y such that $f(x) = f(y) = z$.

A function $f : \{0,1\}^n \to \{0,1\}^n$ has a **period** a if $f(x) = f(x \oplus a), \forall x \in \{0,1\}^n$.

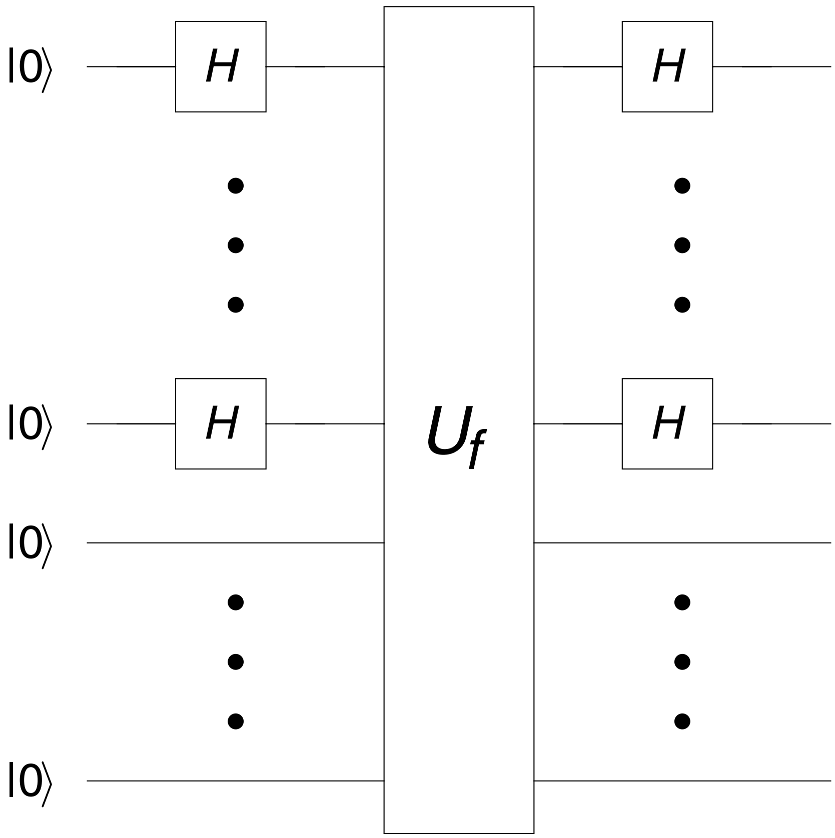
Problem: Simon

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ which is 2-1 and has period a, determine the period a.

Algorithm: Simon

1. Repeat the following procedure for n times.
   (a) Prepare a $2n$-bit quantum register and initialize it to the state $(|0\rangle)^n(|0\rangle)^n$.
   (b) Apply the Walsh–Hadamard transform to the first n qubits.
   (c) Apply the function evaluation operator U_f:
   $$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$
   (d) Apply the Walsh–Hadamard transform to the first n qubits.
   (e) Measure the first n qubits. Record the outcome $|x\rangle$.
2. With the n outcomes $x_1, x_2, \ldots, x_n$, solve the following system of linear equations:
   $$\begin{cases} x_1 \cdot a = 0 \\ x_2 \cdot a = 0 \\ \quad\vdots \\ x_n \cdot a = 0. \end{cases}$$
   The solution a is the period of f.

Circuit Diagram: Simon



Facts:

The following facts can be found in [Sim94].

1. With the classical computer, we need exponentially many evaluations of f to determine the period a.
2. With the quantum computer, we need $O(n)$ evaluations (on average) of f to determine the period a.

Examples:

Let $f(00) = 01$, $f(01) = 11$, $f(10) = 01$, and $f(11) = 11$. The following sequence of quantum states shows the result of computation utilizing Simon's Algorithm. We start from the initial state $|00\rangle|00\rangle$. Then,

$$
\begin{aligned}
&|00\rangle|00\rangle \\
&\rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}} |00\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} |00\rangle \\
&= \frac{|00\rangle|00\rangle}{2} + \frac{|01\rangle|00\rangle}{2} + \frac{|10\rangle|00\rangle}{2} + \frac{|11\rangle|00\rangle}{2} \\
&\rightarrow \frac{|00\rangle|01\rangle}{2} + \frac{|01\rangle|11\rangle}{2} + \frac{|10\rangle|01\rangle}{2} + \frac{|11\rangle|11\rangle}{2}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{|00\rangle + |10\rangle}{2}|01\rangle + \frac{|01\rangle + |11\rangle}{2}|11\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle}{\sqrt{2}}|01\rangle + \frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|1\rangle}{\sqrt{2}}|11\rangle \\
&\to |0\rangle\frac{|0\rangle + |1\rangle}{2}|01\rangle + |0\rangle\frac{|0\rangle - |1\rangle}{2}|11\rangle = \frac{|00\rangle + |01\rangle}{2}|01\rangle + \frac{|00\rangle - |01\rangle}{2}|11\rangle.
\end{aligned}
$$

The outcome of measuring the first 2 qubits yields either $|00\rangle$ or $|01\rangle$. Suppose that we have run the computation above twice and obtained $|00\rangle$ and $|01\rangle$, respectively. We now have a system of linear equations:

$$
\begin{cases} 00 \cdot a = 0 \\ 01 \cdot a = 0. \end{cases}
$$

The solution is $a = 10$, the period of this function.

62.7 Grover's Search Algorithm

Problem: Grover

Given an unsorted database with N items, find a target item w. This problem can be formulated using an oracle function $f : \{0, 1, \dots, N-1\} \to \{0, 1\}$, where

$$
f(x) = \begin{cases} 0, & \text{if } x \neq w, \\ 1, & \text{if } x = w. \end{cases}
$$

Given such an oracle function, find the w such that $f(w) = 1$.

Algorithm: Grover

Without loss of generality, let $N = 2^n$.

1. Prepare an $(n+1)$-bit quantum register and initialize it to the state $(|0\rangle)^n|1\rangle$.
2. Apply the Walsh–Hadamard transform to all the $n+1$ qubits.
3. Repeat the following procedure for about $\frac{\pi}{4}\sqrt{N}$ times. Cf. Figure 62.1.
    (a) Apply the function evaluation operator U_f (selective sign flipping operator):

    $$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle.$$

    This is equivalent to the unitary operator $\mathcal{I}_w = I - 2|w\rangle\langle w|$ on the first n qubits.

    (b) Apply unitary operator (inversion about the average operator) $\mathcal{I}_s = 2|s\rangle\langle s| - I$ on the first n qubits. Cf. Figure 62.2.
4. Measure the first n qubits. We obtain the search target with high probability.

Facts:

1. [Gro97] With the classical computer, on average, we need $O(N)$ oracle calls (evaluations of f) to find the search target.
2. [Gro97] With the quantum computer, on average, we need $O(\sqrt{N})$ oracle calls to find the search target.

Circuit Diagrams: Grover

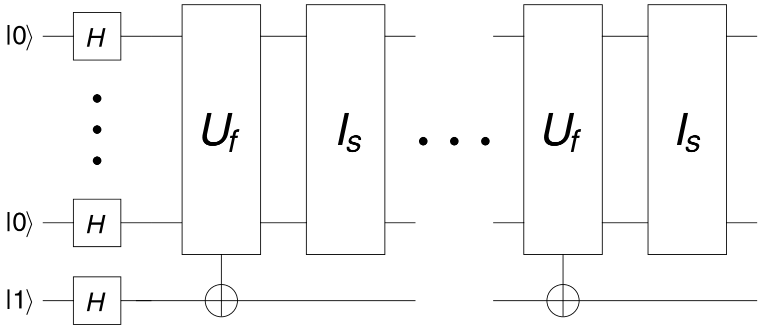


FIGURE 62.1 Grover's Algorithm.

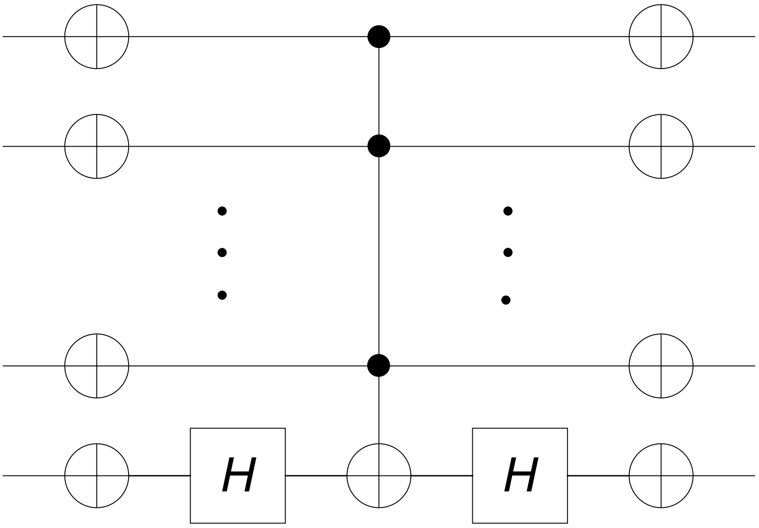


FIGURE 62.2 Inversion about the average operator $\mathcal{I}_s$.

3. [BBH98] When $N = 4$, using Grover's Algorithm, exactly one oracle call suffices to find the search target with certainty.

Examples:

Let $N = 2^2 = 4$ and Item 3 be the search target, which is encoded by the quantum state $|11\rangle$ (11 is the binary representation of 3). The following sequence of quantum states shows the result of computation utilizing Grover's Algorithm. We start from the initial state $|00\rangle|1\rangle$. Then,

$$\begin{aligned}
&|00\rangle|1\rangle\\
\to\ & \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
=\ & \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\
\to\ & \frac{|00\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|11\rangle}{2}\frac{|1\rangle-|0\rangle}{\sqrt{2}}
\end{aligned}$$

$$\begin{aligned}
&= \frac{|00\rangle}{2}\frac{|0\rangle - |1\rangle}{\sqrt{2}} + \frac{|01\rangle}{2}\frac{|0\rangle - |1\rangle}{\sqrt{2}} + \frac{|10\rangle}{2}\frac{|0\rangle - |1\rangle}{\sqrt{2}} - \frac{|11\rangle}{2}\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&= \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2}\frac{|0\rangle - |1\rangle}{\sqrt{2}} \\
&\to |11\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}.
\end{aligned}$$

The outcome of measuring the first 2 qubits yields $|11\rangle$, which is the search target $w = 3$.

Comments:

Grover's Algorithm was discovered by L.K. Grover of Bell Labs in 1996. This algorithm provides a quadratic speedup over classical algorithms. Although it is not exponentially fast (as Shor's Algorithm is), it has a wide range of applications. It could be used to accelerate any algorithms related to searching an unsorted database, including quantum database search, finding the solution of NP problems, finding the median and minimum of a data set, and breaking the Data Encryption Standard (DES) cryptography system.

62.8 Shor's Factorization Algorithm

Integer Factorization Problem:

Given a composite positive integer N, factor it into the product of its prime factors.

Algorithm: Shor

1. Choose a random number $a < N$; make sure that a and N are coprime. This can be done by using a random number generator and Euclidean algorithm on a classical computer.
2. Find the period T of function $f_{a,N}(x) = a^x \ mod \ N$. This step can be further expanded as follows:

   (a) Prepare two L-bit quantum registers in initial state

   $$\left(\frac{1}{\sqrt{2^L}}\sum_{x=0}^{2^L-1}|x\rangle\right)|0\rangle,$$

   where L is chosen such that $N^2 \leq 2^L < 2N^2$.

   (b) Apply the function evaluation operator $U_f : |x\rangle|0\rangle \to |x\rangle|f_{a,N}(x)\rangle$:

   $$\frac{1}{\sqrt{2^L}}\sum_{x=0}^{2^L-1}|x\rangle|0\rangle \to \frac{1}{\sqrt{2^L}}\sum_{x=0}^{2^L-1}|x\rangle|f_{a,N}(x)\rangle.$$

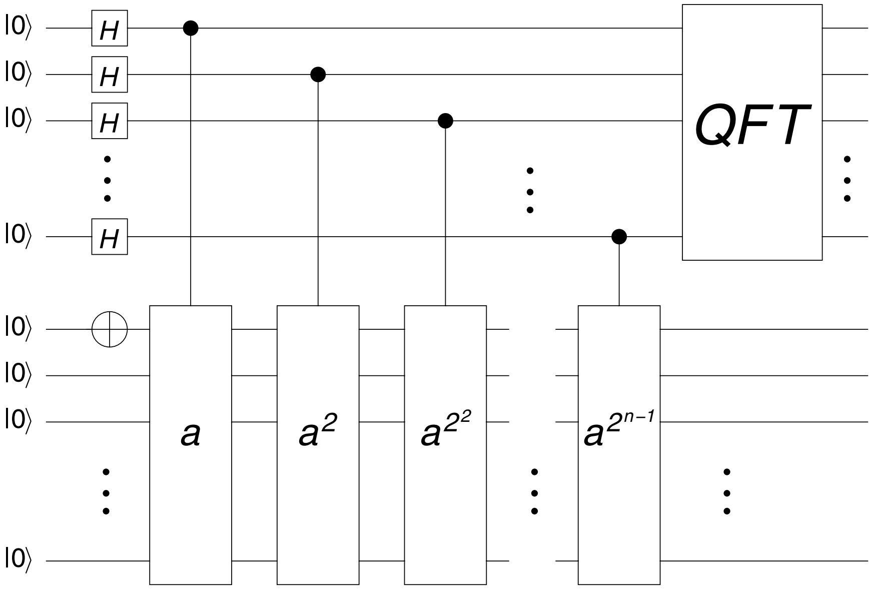
   (c) Apply QFT to the first register:

   $$\frac{1}{\sqrt{2^L}}\sum_{x=0}^{2^L-1}|x\rangle|f_{a,N}(x)\rangle \to \frac{1}{2^L}\sum_{y=0}^{2^L-1}\left(\sum_{x=0}^{2^L-1}e^{2\pi ixy/2^L}|y\rangle\right)|f(x)\rangle.$$

   (d) Make a measurement on the first register, obtaining y.

   (e) Find T from y via the continued fraction for $\frac{y}{2^L}$. This step might fail; in that case, repeat from 2a.
3. If T is odd, repeat from Step 1. If T is even and $N \mid (a^{T/2} + 1)$, repeat from Step 1. If T is even and $N \nmid (a^{T/2} + 1)$, compute $d = gcd(a^{T/2} - 1, N)$, which is a nontrivial factor of N.

Circuit Diagrams: Shor



Facts:

The following facts can be found in [Sho94].

1. The integer factorization problem is classically *intractable*. The most efficient classical algorithm to date, a *number field sieve*, has a time complexity of $O(\exp(\log N)^{1/3}(\log\log N)^{2/3})$.
2. Shor's quantum factorization algorithm has a time complexity of $O((\log N)^2 \log\log N \log\log\log N)$. Hence, it is a polynomial time algorithm.

Examples:

Let $N = 15$. Choose $L = 8$ such that $N^2 = 225 < 2^L < 450 = 2N^2$. Choose a random integer $a = 2$, which is coprime with 15. Thus, $f_{a,N}(x) = 2^x \bmod 15$. The following sequence of quantum states shows the result of computation utilizing Shor's Algorithm:

$$\begin{aligned}
|0\rangle|0\rangle &\rightarrow \frac{1}{2^4}\sum_{x=0}^{2^8-1}|x\rangle|0\rangle \\
&\rightarrow \frac{1}{2^4}\sum_{x=0}^{2^8-1}|x\rangle|f_{a,N}(x)\rangle \\
&= \frac{1}{2^4}(|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle \\
&+ |4\rangle|1\rangle + |5\rangle|2\rangle + |6\rangle|4\rangle + |7\rangle|8\rangle + \cdots + |2^8-2\rangle|4\rangle + |2^8-1\rangle|8\rangle) \\
&\rightarrow \frac{1}{2^4}\sum_{x=0}^{2^8-1}\frac{1}{2^4}\sum_{y=0}^{2^8-1}\omega^{xy}|y\rangle|2^x \bmod 15\rangle \\
&\rightarrow \frac{1}{2^8}\sum_{y=0}^{2^8-1}|y\rangle\sum_{x=0}^{2^8-1}\omega^{xy}|2^x \bmod 15\rangle,
\end{aligned}$$

where $\omega = e^{2\pi i/2^8}$. Suppose that the outcome of measuring the first n qubits is $|56\rangle$. We can compute the continued fraction of $\frac{56}{256}$ to be $[0, 4, \ldots]$. The second number 4 satisfies $2^4 = 1 \bmod 15$. So 4 is the period of $f_{a,N}$. $2^{4/2} - 1 = 3$ yields a factor of 15 and $15 = 3 \times 5$.

Comments:

Shor's Algorithm was discovered by P. Shor of AT&T Labs in 1994. It is the most important breakthrough in the research of quantum computation so far. It solves the integer factorization problem, an extremely hard problem for classical computers, in polynomial time. The security of the RSA cryptographic system, which is widely used nowadays over the Internet, is based on the difficulty of factoring large integers. Equipped with a quantum computer, one could easily break the RSA codes with Shor's Algorithm.

References

[BV93] E. Bernstein and U. Vazirani. Quantum complexity theory. *Proc. of the 25th Annual ACM Symposium on the Theory of Computing*, San Diego, CA, 11–20, 1993.

[BBH98] M. Boyer, G. Brassard, P. Hoyer, and A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys.* 46:493–506, 1998.

[BB02] J. L. Brylinski and R. Brylinski. Universal quantum gates. *Mathematics of Quantum Computation* (R. Brylinski and G. Chen, Eds.). Chapman & Hall/CRC Press, Boca Raton, FL, 101–116, 2002.

[CEM98] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. London A*, 454:339–354, 1998.

[Fey82] R. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[Gro97] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 78:325–328, 1997.

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, U.K., 2000.

[Sho94] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proc. of the 35th Annual IEEE Symposium on the Foundations of Computer Science*, Santa Fe, NM, 124–134, 1994.

[Sim94] D. Simon. On the power of quantum computation. *Proc. of the 35th Annual IEEE Symposium on Foundations of Computer Science*, Santa Fe, NM, 116–123, 1994.