From Nakahara and Ohmi

5

Simple Quantum Algorithms

Before we start presenting "useful" but rather complicated quantum algorithms, we introduce a few simple quantum algorithms which will be of help for readers to understand how quantum algorithms are different from and superior to classical algorithms. We follow closely Meglicki [1].

5.1 Deutsch Algorithm

The **Deutsch algorithm** is one of the first quantum algorithms which showed quantum algorithms may be more efficient than their classical counterparts. In spite of its simplicty, full use of the superposition principle has been made here.

Let $f : \{0,1\} \to \{0,1\}$ be a binary function. Note that there are only four possible f, namely

$$f_1 : 0 \mapsto 0,\ 1 \mapsto 0, \quad f_2 : 0 \mapsto 1,\ 1 \mapsto 1,$$
$$f_3 : 0 \mapsto 0,\ 1 \mapsto 1, \quad f_4 : 0 \mapsto 1,\ 1 \mapsto 0.$$

The first two cases, f_1 and f_2, are called *constant*, while the rest, f_3 and f_4, are *balanced*. If we only have classical resources, we need to evaluate f twice to tell if f is constant or balanced. There is a quantum algorithm, however, with which it is possible to tell if f is constant or balanced with a single evaluation of f, as was shown by Deutsch [2].

Let $|0\rangle$ and $|1\rangle$ correspond to classical bits 0 and 1, respectively, and consider the state $|\psi_0\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$. We apply f on this state in terms of the unitary operator $U_f : |x,y\rangle \mapsto |x, y \oplus f(x)\rangle$, where $\oplus$ is an addition mod 2. To be explicit, we obtain

$$\begin{aligned}|\psi_1\rangle &= U_f|\psi_0\rangle \\ &= \frac{1}{2}(|0, f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, f(1)\rangle - |1, 1 \oplus f(1)\rangle) \\ &= \frac{1}{2}(|0, f(0)\rangle - |0, \neg f(0)\rangle + |1, f(1)\rangle - |1, \neg f(1)\rangle),\end{aligned}$$

where $\neg$ stands for negation. Therefore this operation is nothing but the CNOT gate with the control bit $f(x)$; the target bit y is flipped if and only if

$f(0) - f(1) = \begin{cases} 0 & \text{if } f \text{ a constant} \\ = \pm 1 \neq 0 & \text{if } f \text{ is balanced} \end{cases}$

So classical 1 bit is also enough to tell.

$f(x) = 1$ and left unchanged otherwise. Subsequently we apply a Hadamard gate on the first qubit to obtain

$$|\psi_2\rangle = (U_{\rm H} \otimes I)|\psi_1\rangle$$
$$= \frac{1}{2\sqrt{2}}\left[(|0\rangle + |1\rangle)(|f(0)\rangle - |\neg f(0)\rangle) + (|0\rangle - |1\rangle)(|f(1)\rangle - |\neg f(1)\rangle)\right].$$

The wave function reduces to

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle(|f(0)\rangle - |\neg f(0)\rangle) \tag{5.1}$$

in case f is constant, for which $|f(0)\rangle = |f(1)\rangle$, and

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|1\rangle(|f(0)\rangle - |\neg f(0)\rangle) \tag{5.2}$$

if f is balanced, for which $|\neg f(0)\rangle = |f(1)\rangle$. Therefore the measurement of the first qubit tells us whether f is constant or balanced.

Let us consider a quantum circuit which implements the Deutsch algorithm. We first apply Walsh-Hadamard transformation $W_2 = U_{\rm H} \otimes U_{\rm H}$ on $|01\rangle$ to obtain $|\psi_0\rangle$. We need to introduce a conditional gate U_f, i.e., the controlled-NOT gate with the control bit $f(x)$, whose action is $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$. Then a Hadamard gate is applied on the first qubit before it is measured. Figure 5.1 depicts this implementation.

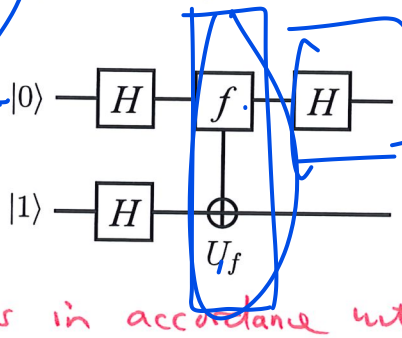

FIGURE 5.1
Implementation of the Deutsch algorithm.

In the quantum circuit, we assume the gate U_f is a black box for which we do not ask the explicit implementation. We might think it is a kind of subroutine. Such a black box is often called an **oracle**. The gate U_f is called the Deutsch oracle. Its implementation is given only after f is specified.

Then what is the merit of the Deutsch algorithm? Suppose your friend gives you a unitary matrix U_f and asks you to tell if f is constant or balanced. Instead of applying $|0\rangle$ and $|1\rangle$ separately, you may construct the circuit in Fig. 5.1 with the given matrix U_f and apply the circuit on the input state $|01\rangle$. Then you can tell your friend whether f is constant or balanced with a single use of U_f.

5.2 Deutsch-Jozsa Algorithm and Bernstein-Vazirani Algorithm

The Deutsch algorithm introduced in the previous section may be generalized to the **Deutsch-Jozsa algorithm** [3].

Let us first define the **Deutsch-Jozsa problem**. Suppose there is a binary function

$$f : S_n \equiv \{0, 1, \ldots, 2^n - 1\} \to \{0, 1\}. \tag{5.3}$$

We require that f be either *constant* or *balanced* as before. When f is constant, it takes a constant value 0 or 1 irrespetive of the input value x. When it is balanaced the value $f(x)$ for the half of $x \in S_n$ is 0, while it is 1 for the rest of x. In other words, $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$, where $|A|$ denotes the number of elements in a set A, known as the cardinality of A. Although there are functions which are neither constant nor balanced, we will not consider such cases here. Our task is to find an algorithm which tells if f is constant or balanced with the least possible number of evaluations of f.

It is clear that we need at least $2^{n-1} + 1$ steps, in the worst case with classical manipulations, to make sure if $f(x)$ is constant or balanced with 100% confidence. It will be shown below that the number of steps reduces to a single step if we are allowed to use a quantum algorithm.

The algorithm is divided into the following steps:

1. Prepare an $(n+1)$-qubit register in the state $|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$. First n qubits work as input qubits, while the $(n+1)$st qubit serves as a "scratch pad." Such qubits, which are neither input qubits nor output qubits, but work as a scratch pad to store temporary information are called **ancillas** or **ancillary qubits**.

2. Apply the Walsh-Hadamard transforamtion to the register. Then we have the state

$$|\psi_1\rangle = U_{\mathrm{H}}^{\otimes n+1}|\psi_0\rangle = \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n} \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5.4}$$

3. Apply the $f(x)$-controlled-NOT gate on the register, which flips the $(n+1)$st qubit if and only if $f(x) = 1$ for the input x. Therefore we need a U_f gate which evaluates $f(x)$ and acts on the register as $U_f|x\rangle|c\rangle = |x\rangle|c \oplus f(x)\rangle$, where $|c\rangle$ is the one-qubit state of the $(n+1)$st qubit. Observe that $|c\rangle$ is flipped if and only if $f(x) = 1$ and left

unchanged otherwise. We then obtain a state

$$\begin{aligned}|\psi_2\rangle &= U_f|\psi_1\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle - |\neg f(x)\rangle) \\ &= \frac{1}{\sqrt{2^n}}\sum_{x}(-1)^{f(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{5.5}$$

Although the gate U_f is applied once for all, it is applied to *all* the n-qubit states $|x\rangle$ simultaneously.

4. The Walsh-Hadamard transformation (4.11) is applied on the first n qubits next. We obtain

$$|\psi_3\rangle = (W_n \otimes I)|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}U_{\rm H}^{\otimes n}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5.6}$$

It is instructive to write the action of the one-qubit Hadamard gate in the following form,

$$U_{\rm H}|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) = \frac{1}{\sqrt{2}}\sum_{y\in\{0,1\}}(-1)^{xy}|y\rangle,$$

where $x \in \{0,1\}$, to find the resulting state. The action of the Walsh-Hadamard transformation on $|x\rangle = |x_{n-1}\ldots x_1x_0\rangle$ yields

$$\begin{aligned}W_n|x\rangle &= (U_{\rm H}|x_{n-1}\rangle)(U_{\rm H}|x_{n-2}\rangle)\ldots(U_{\rm H}|x_0\rangle) \\ &= \frac{1}{\sqrt{2^n}}\sum_{y_{n-1},y_{n-2},\ldots,y_0\in\{0,1\}}(-1)^{x_{n-1}y_{n-1}+x_{n-2}y_{n-2}+\ldots+x_0y_0} \\ &\quad\times|y_{n-1}y_{n-2}\ldots y_0\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle, \end{aligned} \tag{5.7}$$

where $x\cdot y = x_{n-1}y_{n-1}\oplus x_{n-2}y_{n-2}\oplus\ldots\oplus x_0y_0$. Substituting this result into Eq. (5.6), we obtain

$$|\psi_3\rangle = \frac{1}{2^n}\left(\sum_{x,y=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}|y\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5.8}$$

5. The first n qubits are measured. Suppose $f(x)$ is constant. Then $|\psi_3\rangle$ is put in the form

$$|\psi_3\rangle = \frac{1}{2^n}\sum_{x,y}(-1)^{x\cdot y}|y\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

up to an overall phase. Now let us consider the summation

$$\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{x\cdot y}$$

with a fixed $y \in S_n$. Clearly it vanishes since $x \cdot y$ is 0 for half of x and 1 for the other half of x unless $y = 0$. Therefore the summation yields δ_{y0}. Now the state reduces to

$$|\psi_3\rangle = |0\rangle^{\otimes n}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

and the measurement outcome of the first n qubits is always $00\ldots0$. Suppose $f(x)$ is balanced next. The probability amplitude of $|y = 0\rangle$ in $|\psi_3\rangle$ is proportional to

$$\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot 0} = \sum_{x=0}^{2^n-1}(-1)^{f(x)} = 0.$$

Therefore the probability of obtaining measurement outcome $00\ldots0$ for the first n qubits vanishes. In conclusion, the function f is constant if we obtain $00\ldots0$ upon the meaurement of the first n qubits in the state $|\psi_3\rangle$, and it is balanced otherwise.

EXERCISE 5.1 Let us take $n = 2$ for definiteness. Consider the following cases and find the final wave function $|\psi_3\rangle$ and evaluate the measurement outcomes and their probabilities for each case.
(1) $f(x) = 1\ \forall x \in S_2$.
(2) $f(00) = f(01) = 1, f(10) = f(11) = 0$.
(3) $f(00) = 0, f(01) = f(10) = f(11) = 1$. (This function is neither constant nor balanced.)

The above exercise shows that the measurement gives $|00\rangle$ with probability 1 if f is constant and with probability 0 if balanced. If f is neither constant nor balanced $|\psi_3\rangle$ is a superposition of several states including $|00\rangle$, which is attributed to "incomplete" interference.

A quantum circuit which implements the Deutsch-Jozsa algorithm is given in Fig. 5.2. The gate U_f is called the **Deutsch-Jozsa oracle**.

The **Bernstein-Vazirani algorithm** is a special case of the Deutsch-Jozsa algorithm, in which $f(x)$ is given by $f(x) = c \cdot x$, where $c = c_{n-1}c_{n-2}\cdots c_0$ is an n-bit binary number [4]. Our aim is to find c with the smallest number of evaluations of f. If we apply the Deutsch-Jozsa algorithm with this f, we obtain

$$|\psi_3\rangle = \frac{1}{2^n}\left[\sum_{x,y=0}^{2^n-1}(-1)^{c\cdot x}(-1)^{x\cdot y}|y\rangle\right]\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

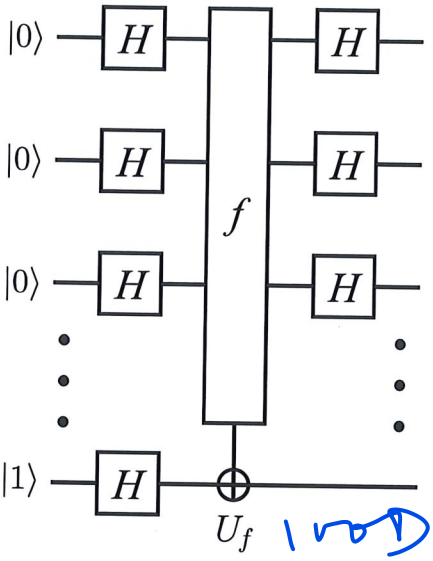

FIGURE 5.2
Quantum circuit implementing the Deutsch-Jozsa algorithm. The gate U_f is the Deutsch-Jozsa oracle.

Let us fix y first. If we take $y = c$, we obtain

$$\sum_x (-1)^{c\cdot x}(-1)^{x\cdot c} = \sum_x (-1)^{2c\cdot x} = 0$$

If $y \neq c$, on the other hand, there will be the same number of x such that $c \cdot x = 0$ and x such that $c \cdot x = 1$ in the summation over x and, as a result, the probability amplitude of $|y \neq c\rangle$ vanishes. By using these results, we end up with

$$|\psi_3\rangle = |c\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (5.9)$$

We are able to tell what c is by measuring the first n qubits. Note that this is done by a single application of the circuit in Fig. 5.2.

EXERCISE 5.2 Consider the Bernstein-Vazirani algorithm with $n = 3$ and $c = 101$. Work out the quantum circuit depicted in Fig. 5.2 to show that the measurement outcome of the first three qubits is $c = 101$.

5.3 Simon's Algorithm

The final example of simple quantum algorithms is **Simon's algorithm**. Let us consider a function (oracle) $f : \{0,1\}^n \to \{0,1\}^n$ such that

1. f is 2 to 1; namely, for any x_1, there is one and only one $x_2 \neq x_1$ such that $f(x_1) = f(x_2)$.
2. f is periodic; namely, there exists $p \in \{0,1\}^n$ such that $f(x \oplus p) = f(x)$, $\forall x \in \{0,1\}^n$, where $\oplus$ is a bitwise addition mod 2.

The function f is made of n component functions $f_k : \{0,1\}^n \to \{0,1\}$ as $f = (f_1, f_2, \ldots, f_n)$.

Suppose we want to find the period p, given an unknown oracle f. Since p can be any number between $00\ldots0$ and $11\ldots1$, we have to try $\sim 2^n$ possibilities classically before we hit the right number. It is shown below that the number of trials required to find p is reduced to $O(n)$ if Simon's algorithm is employed.

The algorithm is decomposed into the following steps:

1. Prepare two sets of n-qubit regiters in the state $|\psi_0\rangle = |0\rangle|0\rangle$. Then the Walsh-Hadamard transformation W_n is applied on the first register to yield
$$|\psi_1\rangle = (W_n \otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle.$$
2. Introduce n controlled-NOT gates with control qubits $f_k(x)$ $(1 \leq k \leq n)$ and the target bit is the kth qubit of the second register. We write
$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle,$$
where $|0\rangle$ is an n-qubit register state and $|f(x)\rangle = |f_1(x)\rangle|f_2(x)\rangle \ldots |f_n(x)\rangle$. Linearity implies the state $|\psi_2\rangle$ after the U_f gate operation on $|\psi_1\rangle$ is
$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle. \tag{5.10}$$
3. Now we measure the second register. In fact, we do not need to know the measurement outcome. What we have to do is to project the second register to a certain state $|f(x_0)\rangle$, for example. After one of these operations, the state is now projected to
$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus p\rangle)|f(x_0)\rangle, \tag{5.11}$$
where we noted that there are exactly two states $|x_0\rangle$ and $|x_0 \oplus p\rangle$ that give the second register state $|f(x_0)\rangle$ in step 2.

4. Now we apply W_n again on the first register to obtain

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}\left[(-1)^{x_0\cdot y} + (-1)^{(x_0\oplus p)\cdot y}\right]|y\rangle \otimes |f(x_0)\rangle$$

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x_0\cdot y}\left[1 + (-1)^{p\cdot y}\right]|y\rangle \otimes |f(x_0)\rangle. \quad (5.12)$$

The inner product $p\cdot y$ takes two values 0 and 1. We immediately notice that such y which satisfies $1+(-1)^{p\cdot y}=0$, namely, $p\cdot y = 1$ does not contribute to the summation in Eq. (5.12). Now we are left with

$$|\psi_4\rangle = \frac{2}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\left[\sum_{p\cdot y=0}(-1)^{x_0\cdot y}|y\rangle\right]\otimes|f(x_0)\rangle. \quad (5.13)$$

5. Finally we measure the first register. Upon this measurement, we obtain $|y\rangle$ such that $p\cdot y = 0$. Of course, this equation is not enough to identify the period p. Now we repeat the algorithm many times to obtain

$$p\cdot y_1 = p\cdot y_2 = \ldots = p\cdot y_m = 0. \pmod 2 \quad (5.14)$$

It should be clear that we need at least n trials since not all equations are linearly independent. For a sufficiently large number of trials m, we are able to solve Eq. (5.14) for p classically. The number of trials necessary for this is $O(n)$ with a good probability.

Figure 5.3 shows the quantum circuit to implement Simon's algorithm for the case $n = 3$.

Simon's algorithm has been improved so that it may be executed in deterministic polynomial time [6].

References

[1] Z. Meglicki, `http://beige.ucs.indiana.edu/M743/index.html`

[2] D. Deutsch, Proc. Roy. Soc. Lond. A, **400**, 97 (1985).

[3] D. Deutsch and R. Jozsa, Proc. Roy. Soc. Lond. A, **439**, 553 (1992).

[4] E. Bernstein and U. Vazirani, SIAM J. Comput., **26**, 1411 (1997).

[5] D. R. Simon, Proc. 35th Annual Sympo. Found. Comput. Science, IEEE Comput. Soc. Press, Los Alamitos, 116 (1994).

[6] T. Mihara and S. C. Sung, Comput. Complex. **12**, 162 (2003).