Chapter 1

Deutsch Algorithm

1.1 The Deutch Problem

Consider a Boolean function f that maps a binary input $\{0,1\}$ to a binary output $\{0,1\}$, i.e., $f:\{0,1\}\to\{0,1\}$. Based on these inputs, we can think of four possible scenarios:

1. $f(0)=f(1)=0$.
2. $f(0)=f(1)=1$.
3. $f(0)=0$ and $f(1)=1$.
4. $f(0)=1$ and $f(1)=0$.

The first two cases can be classified as *constant* and the other two cases as *balanced*. Based on this setup, we have the following problem.

Problem 1: Deutsch Query

Given a binary input $\{0,1\}$, determine whether the function $f:\{0,1\}\to\{0,1\}$ is constant $[f(0)=f(1)]$ or balanced $[f(0)\neq f(1)]$ with minimum number of function evaluations.

To address the above the problem, let us look into the truth-table for $f(0)\oplus f(1)$:

Class	$f(0)$	$f(1)$	$f(0)\oplus f(1)$
Constant	0	0	0
Constant	1	1	0
Balanced	0	1	1
Balanced	1	0	1

Table 1.1: Truth table for $f(0)\oplus f(1)$.

From Table 1.1, we clearly notice that just knowing the value of $f(0)\oplus f(1)$ is sufficient to infer whether f is constant or balanced. To find out this classically, we need to make two queries for f as we require to determine both $f(0)$ and $f(1)$. However, using quantum circuits, this can be reduced to a merely a single query by exploiting quantum superposition and quantum parallelism. Before understanding how it works, let us digress to *phase kickback* first.

1.2 Phase Kickback and ancilla

Consider a two-qubit system where the first qubit is in an quantum interference (or superposition) state $|+\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)$ or $|-\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$ and the second qubit is in a state $|u\rangle$. Now there is a controled unitary operator $\hat{U}^C$ which operates on $|u\rangle$ (target bit) (see Fig. 1.1). The operation on the state $|u\rangle\,|\pm\rangle$ by $\hat{U}^C$ can be found as

$$\begin{aligned}\hat{U}^C(0,1)\,|u\rangle\,|\pm\rangle &= \frac{1}{\sqrt{2}}\big[\,|u\rangle\,|0\rangle + \hat{U}\,|u\rangle\,|1\rangle\,\big]\\ &= \frac{1}{\sqrt{2}}\big[\,|u\rangle\,|0\rangle + e^{i\phi}\,|u\rangle\,|1\rangle\,\big]\end{aligned}$$

The above can be reorganized as

$$\boxed{\hat{U}^C(0,1)\,|u\rangle\,|\pm\rangle = |u\rangle\,\big[\,|0\rangle + e^{i\phi}\,|1\rangle\,\big]\,.} \tag{1.1}$$

Though the operator $\hat{U}^C(0,1)$ acts on the target bit $|u\rangle$ and yields the eigenvalue $e^{i\phi}$, the eigenvalue or the phase-factor can be placed in front of one the states in the intereference $|\pm\rangle$. It looks like the target qubit remains unchanged while its phase *kicks back* the control bit. Since the second qubit on the circuit remains unaltered and only serves to modify the first quibit, it is often dubbed *ancilliary qubit* or *ancilla*. However, to see the phase kickback, the first qubit does not necessarily need to be a superposition state while the second qubit must have to be an eigenstate of the operator $\hat{U}$. For instance, we know that $|\pm\rangle$ are eigenstates of a *CNOT* gate. Let us select $|u\rangle = |-\rangle$. If we choose the first qubit as $|1\rangle$,

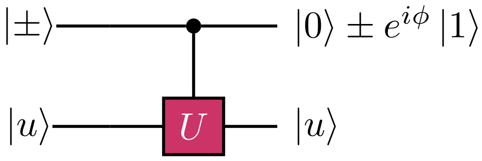

Figure 1.1: Phase kickback on $|\pm\rangle$ by the controlled unitary operator $\hat{U}$.

$$\begin{aligned}\hat{X}^C(0,1)\,|-\rangle\,|1\rangle &= \hat{X}\frac{1}{\sqrt{2}}\big[\,|0\rangle - |1\rangle\,\big]\,|1\rangle\\ &= \hat{X}\frac{1}{\sqrt{2}}\big[\,|1\rangle - |0\rangle\,\big]\,|1\rangle\\ &= -\,|-\rangle\,|1\rangle\ . \end{aligned} \tag{1.2}$$

while it does not affect the $|-\rangle\,|0\rangle$ at all:

$$\hat{X}^C(0,1)\,|-\rangle\,|0\rangle = |-\rangle\,|0\rangle \ . \tag{1.3}$$

Eq. (1.2) and Eq. (1.3) can be generalized as

$$\hat{X}^C(0,1)\,|-\rangle\,|n\rangle = (-1)^n\,|-\rangle\,|n\rangle \ , \tag{1.4}$$

where $n \in \{0,1\}$. Thus for any two qubit interference state $a\,|0\rangle + b\,|1\rangle$,

$$\boxed{\hat{X}^C(0,1)\,|-\rangle\,\big[a\,|0\rangle + b\,|1\rangle\,\big] = |-\rangle\,\big[a\,|0\rangle - b\,|1\rangle\,\big] = |-\rangle\,\hat{Z}\big[a\,|0\rangle + b\,|1\rangle\,\big]\,.} \tag{1.5}$$

Thus the phase kickback on the control bit generates a relative phase (or sign change) between $|0\rangle$ and $|1\rangle$.

1.3 Oracle

A quantum oracle is a blackbox that performs a desired unitary operation required for a quantum algorithm. For the purpose of the algorithm, we do not need to know how an oracle function, rather we bother on what outputs it generates. Once we set up the algorithm, we may figure out the way to construct an oracle at the quantum circuit implementation level. For a function $f : \{0,1\} \to \{0,1\}$, let us consider a 2-qubit oracle $\hat{O}_f$ that operates on a 2-qubit state $|x,y\rangle$ as

Figure 1.2: Gloria Foster as the Oracle in the film Matrix (1999). (Image courtesy: *imgflip.com*)

$$\hat{O}_f\,|y,x\rangle = |y \oplus f(x), x\rangle \ . \tag{1.6}$$

A circuit diagram for the oracle is show in Fig. 1.3.

Now let us check the action of $\hat{O}_f$ when the target qubit is $|-\rangle$.

$$\begin{aligned}
\hat{O}_f\,|-,x\rangle &= \frac{1}{\sqrt{2}}\big[\,|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle\,\big]\,|x\rangle \\
&= \frac{1}{\sqrt{2}}\big[\,|f(x)\rangle - |\overline{f(x)}\rangle\,\big]\,|x\rangle \\
&\equiv |Q\rangle\,|x\rangle \ . \qquad (1.7)
\end{aligned}$$

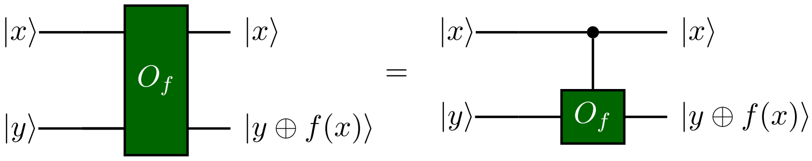

Figure 1.3: A quantum oracle $\hat{O}_f$ that works as a blackbox for the reversible unitary operation $\hat{O}_f\,|y,x\rangle = |y \oplus f(x), y\rangle$.

Now notice that

$$|Q\rangle = \begin{cases} \frac{1}{\sqrt{2}}\big[\,|0\rangle - |1\rangle\,\big] = |-\rangle & \text{for } f(x) = 0 \\ \frac{1}{\sqrt{2}}\big[\,|1\rangle - |0\rangle\,\big] = -\,|-\rangle & \text{for } f(x) = 1\,. \end{cases} \tag{1.8}$$

The above two possible states differ by a negative sign depending on the value of $f(x)$. This can be generically written as

$$|Q\rangle = (-1)^{f(x)}\,|-\rangle\ . \tag{1.9}$$

Thus Eq. (1.7) reads

$$\hat{O}_f\,|-,x\rangle = (-1)^{f(x)}\,|-,x\rangle = |-\rangle\,(-1)^{f(x)}\,|x\rangle\ . \tag{1.10}$$

Thus the operation of $\hat{O}_f$ can be considered as modifying the control qubit $|x\rangle$ instead of the target qubit $|-\rangle$ with a phase factor $(-1)^{f(x)}$. Thus again a phase kickback on the control bit is noticed. Now when the first qubit is a generic superposition state: $|x\rangle = a\,|0\rangle + b\,|1\rangle$, we have

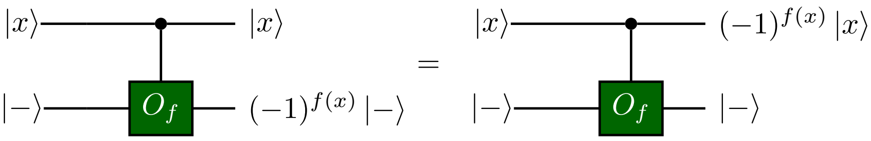

Figure 1.4: Phase kickback on $|x\rangle$ by the oracle $\hat{O}_f$.

$$\boxed{\hat{O}^C_f(0,1)\,|-\rangle\,\big[a\,|0\rangle + b\,|1\rangle\,\big] = |-\rangle\,\big[a(-1)^{f(0)}\,|0\rangle + b(-1)^{f(1)}\,|1\rangle\,\big]\,.} \tag{1.11}$$

1.4 Deutsch algorithm

Let us consider the circuit below (Fig. 1.5). We label various stages of the circuit with states $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$. Let us examine these states step by step below.

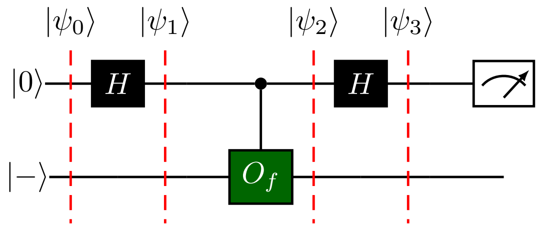

Figure 1.5: Deutsch algorithm circuit diagram.

$$|\psi_0\rangle = |-\rangle\,|0\rangle\ . \tag{1.12}$$

$$|\psi_1\rangle = |-\rangle\,\hat{H}\,|0\rangle = |-\rangle\,|+\rangle = \frac{1}{\sqrt{2}}|-\rangle\,\big[\,|0\rangle + |1\rangle\,\big]\,. \tag{1.13}$$

Now the oracle acts on ψ_1 and modifies it to

$$\boxed{|\psi_2\rangle = \frac{1}{\sqrt{2}}|-\rangle\,\big[(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\,\big]\,.} \tag{1.14}$$

Digression

Note that the value of $(-1)^x$ depends only to the fact that x is even or odd. We know

$$(-1)^x = \begin{cases} 1 & \text{if } x \text{ is even} \\ -1 & \text{if } x \text{ is odd}\,. \end{cases} \tag{1.15}$$

The above can be simplified as

$$(-1)^x = (-1)^{x \mod 2}\,. \tag{1.16}$$

Following this, we can also write

$$(-1)^a(-1)^b = (-1)^{a+b} = (-1)^{(a+b) \mod 2} = (-1)^{a\oplus b}\,. \tag{1.17}$$

Thus

$$\begin{aligned}(-1)^{f(1)} &= (-1)^{2f(0)}(-1)^{f(1)} \quad [\because 2f(0) \text{ is an even power}]\\ &= (-1)^{f(0)}(-1)^{f(0)+f(1)}\\ &= (-1)^{f(0)}(-1)^{f(0)\oplus f(1)}\,. \end{aligned} \tag{1.18}$$

By applying Eq. (1.18), we can rewrite Eq. (1.14) as

$$\boxed{|\psi_2\rangle = (-1)^{f(0)}\frac{1}{\sqrt{2}}\,|-\rangle\,\big[\,|0\rangle + (-1)^{f(0)\oplus f(1)}\,|1\rangle\,\big]\,.} \tag{1.19}$$

Now let us examine our cases again:

- **Case I:** $f(0) \oplus f(1) = 0$ (f is constant):

$$|\psi_2\rangle = (-1)^{f(0)}\frac{1}{\sqrt{2}}\,|-\rangle\,\big[\,|0\rangle - |1\rangle\,\big] = (-1)^{f(0)}\frac{1}{\sqrt{2}}\,|-\rangle\,|-\rangle\,,. \tag{1.20}$$

- **Case II:** $f(0) \oplus f(1) = 1$ (f is balanced):

$$|\psi_2\rangle = (-1)^{f(0)}\frac{1}{\sqrt{2}}\,|-\rangle\,\big[\,|0\rangle - |1\rangle\,\big] = (-1)^{f(0)}\frac{1}{\sqrt{2}}\,|-\rangle\,|+\rangle\,,. \tag{1.21}$$

Hence after the final Hadamard gate operation on the first qubit, we get

- **Case I:** $f(0) \oplus f(1) = 0$ (f is constant):

$$\boxed{|\psi_3\rangle = \hat{H}(0)(-1)^{f(0)}\,|-\rangle\,|-\rangle = (-1)^{f(0)}\,|-\rangle\,|1\rangle\,,.} \tag{1.22}$$

- **Case II:** $f(0) \oplus f(1) = 1$ (f is balanced):

$$\boxed{|\psi_3\rangle = \hat{H}(0)(-1)^{f(0)}\,|-\rangle\,|+\rangle = (-1)^{f(0)}\,|-\rangle\,|0\rangle\,,.} \tag{1.23}$$

Thus the last Hadamard gate operation leaves the first qubit in the state $\pm\,|1\rangle$ or $\pm\,|1\rangle$ for the constant or balanced f. Performing a quantum measurement on the first qubit reveals the nature of f and hence the Deutch problem is solved. The sign before the state is determined by the factor $(-1)^{f(0)}$ and it is immaterial in the measurement.

1.5 Coding the oracle

So far we treated the oracle as a blackbox. Now the question arises: How to construct the oracle for the real implementation. We can figure out the possible gates to design the desired oracle for the four possible combined values of $f(0)$ and $f(1)$. Let us look into the table below.

1.6 FAQs

- **Q. Why do you require an oracle when it returns the same on the first qubit and you are measuring only the first qubit's wire?** A. Because the change on the second wire kicks back a phase and hence modifies the first qubit.

1.7 Deutsch-Jozsa algorithm

The Deutsch problem can be readlily extended to a more generic function that maps a n-bit string to a single bit:

$$f : \{0,1\}^n \to \{0,1\} \,. \tag{1.24}$$

Like in the previous case, f is promised to be either *constant* (here for all bits, f takes a constant value of 0 or 1) or *balanced* (here out of all bits, for half of the bits, $f(x) = 0$ and for other half of the bits, $f(x) = 1$. To

Problem 2: Deutsch-Jozsa Problem

Given a string of n-bit inputs, determine whether the function $f : \{0,1\}^n \to \{0,1\}$ is constant [$f(x)$ is the same $\forall\ x$] or balanced [$f(x) = 0$ for half of the inputs, $f(x) = 1$ for other half of the inputs] with minimum number of queries.

Let us first try to solve the problem classical. For an n-bit input string, we have 2^n possible inputs. In the worst case scenario, we remain inconclusive about f if we do not see $f(x)$ to alter values until we query half plus one extra ($2^n/2 + 1 = 2^{n-1} + 1$) bits. Now let us examine what if we use a quantum algorithm for this. Like in the single bit case, we construct an oracle:

$$\hat{O}_f : |y\rangle\,|\mathbf{x}\rangle \to |y \oplus f(\mathbf{x})\rangle\,|\mathbf{x}\rangle \ . \tag{1.25}$$

$f(0)$	$f(1)$	$y \oplus f(x)$	$\hat{O}_f$
0	0	y	$\hat{I}$
0	1	$\begin{cases} y \text{ for } x = 0 \\ \bar{y} \text{ for } x = 1 \end{cases}$	$\hat{X}^C$
1	0	$\begin{cases} \bar{y} \text{ for } x = 0 \\ y = \bar{\bar{y}} \text{ for } x = 1 \end{cases}$	$\hat{X}\hat{X}^C$ or $\hat{X}^C\hat{X}$
1	1	$\bar{y}$	$\hat{X}$

Table 1.2: A chart to figure out the Deutsch oracle $\hat{O}_f : |y, x\rangle \to |y \oplus f(x), x\rangle$. Note when $f(x) = 1$, we use the identity $y \oplus f(x) = y \oplus 1 = \bar{y}$.

Now let us look into the modified circuit below (see Fig. 1.6). In this modified circuit, n copies of the first quantum wire of the Deutsch circuit are created (the '$/^n$' notation signifies n copies of the same qubit). All qubits except the last ($n+1$-th) one become the control bit. We figure out the evolution of the quantum states below.

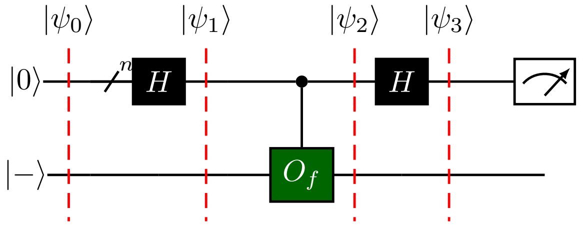

Figure 1.6: Deutsch-Jozsa algorithm circuit diagram. [modification in diagram needed]

$$|\psi_0\rangle = |-\rangle\,|0\rangle^{\otimes n}\ . \tag{1.26}$$

$$|\psi_1\rangle = |-\rangle\,\hat{H}^{\otimes n}\,|0\rangle^{\otimes n}\ . \tag{1.27}$$

Now

$$\begin{aligned}
\hat{H}^{\otimes n}\,|0\rangle^{\otimes n} = |+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}\right)^{n} & \underbrace{\big[\,|0\rangle + |1\rangle\big] \otimes \cdots \big[\,|0\rangle + |1\rangle\big]}_{n \text{ times}} \\
= \frac{1}{\sqrt{2^n}} & \sum_{x_1\in\{0,1\},x_2\in\{0,1\},\cdots,x_n\in\{0,1\}} |x_n\rangle \cdots |x_2\rangle\,|x_1\rangle \\
= \frac{1}{\sqrt{2^n}} & \sum_{\mathbf{x}\in\{\mathbf{0},\mathbf{1}\}^{\mathbf{n}}} |\mathbf{x}\rangle\ ,
\end{aligned} \tag{1.28}$$

where

$$|\mathbf{x}\rangle \equiv |x_n\rangle \cdots |x_2\rangle\,|x_1\rangle\ . \tag{1.29}$$

Thus the state after the first Hadamard operation on each of the first n qubits:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{\mathbf{0},\mathbf{1}\}} |-\rangle\,|\mathbf{x}\rangle\ . \tag{1.30}$$

Now the oracle acts on all the states in $|\psi_1\rangle$' and modifies it to

$$\boxed{|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\,|-\rangle\,\Big[\sum_{\mathbf{x}\in\{\mathbf{0},\mathbf{1}\}} (-1)^{f(\mathbf{x})}\,|\mathbf{x}\rangle\,\Big]\,.} \tag{1.31}$$

Now recall

$$\begin{aligned}\hat{H}\left|x\right\rangle &= \frac{1}{\sqrt{2}}\big[\left|z\right\rangle + (-1)^{x}\left|1\right\rangle\big] \\ &= \frac{1}{\sqrt{2}}\sum_{z\in\{0,1\}}(-1)^{xz}\left|z\right\rangle \; . \end{aligned} \tag{1.32}$$

Then

$$\begin{aligned}\hat{H}^{\otimes n}\left|\mathbf{x}\right\rangle &= \hat{H}^{\otimes n}\left|x_n\cdots x_2x_1\right\rangle \\ &= \hat{H}\left|x_n\right\rangle\cdots\hat{H}\left|x_2\right\rangle\left|x_1\right\rangle \\ &= \frac{1}{\sqrt{2^n}}\big[\left|1\right\rangle + (-1)^{x_n}\left|0\right\rangle\big]\cdots\big[\left|1\right\rangle + (-1)^{x_2}\left|0\right\rangle\big]\big[\left|1\right\rangle + (-1)^{x_1}\left|0\right\rangle\big] \\ &= \frac{1}{\sqrt{2^n}}\sum_{z_1\in\{0,1\},z_2\in\{0,1\},\cdots,z_n\in\{0,1\}}(-1)^{x_1z_1+x_2z_2+\cdots x_nz_n}\left|z_n\right\rangle\cdots\left|z_2\right\rangle\left|z_1\right\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{\mathbf{z}\in\{\mathbf{0,1}\}^{\mathbf{n}}}(-1)^{\mathbf{x.z}}\left|\mathbf{z}\right\rangle \; . \end{aligned} \tag{1.33}$$

Thus

$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{2^n}}\left|-\right\rangle\Big[\sum_{\mathbf{x}\in\{\mathbf{0,1}\}}(-1)^{f(\mathbf{x})}\frac{1}{\sqrt{2^n}}\sum_{\mathbf{z}\in\{\mathbf{0,1}\}^{\mathbf{n}}}(-1)^{\mathbf{x.z}}\left|\mathbf{z}\right\rangle\Big] \, . \tag{1.34}$$

After rearraning the terms, we have

$$\boxed{\left|\psi_3\right\rangle = \frac{1}{2^n}\left|-\right\rangle\sum_{\mathbf{z}\in\{\mathbf{0,1}\}^{\mathbf{n}}}\;\sum_{\mathbf{x}\in\{\mathbf{0,1}\}^{\mathbf{n}}}(-1)^{f(\mathbf{x})+\mathbf{x.z}}\left|\mathbf{z}\right\rangle \; .} \tag{1.35}$$

Now note that there are total 2^n states for a n-qubit state and they can be represented sequentially by a decimal number starting from 0 to 2^{n-1}. For example, a 3-qubit state can have the $2^3 = 8$ possible configurations and they can be represented by decimal numbers from 0 to 7 as shown in Table 1.3. Note Table 1.3 is merely for a demonstration. In practice, we have always have even number of qubits (2^n), else the balanced function will become ill-defined.

Qubit state: $\lvert b_2b_1b_0\rangle$	**Decimal value** $= 2^0b_0 + 2^1b_1 + 2^2b_1$	**State** **representation**
$\lvert 000\rangle$	0	$\lvert 0\rangle$
$\lvert 001\rangle$	1	$\lvert 1\rangle$
$\lvert 010\rangle$	2	$\lvert 2\rangle$
$\lvert 011\rangle$	3	$\lvert 3\rangle$
$\lvert 100\rangle$	4	$\lvert 4\rangle$
$\lvert 101\rangle$	5	$\lvert 5\rangle$
$\lvert 110\rangle$	6	$\lvert 6\rangle$
$\lvert 111\rangle$	7	$\lvert 7\rangle$

Table 1.3: Representation of 3-qubit states with single decimal integers.

Following new representation, $\lvert\psi_3\rangle$ can be written with further simplified notation:

$$\boxed{\lvert\psi_3\rangle = \frac{1}{2^n}\lvert -\rangle \sum_{l=0}^{2^n-1}\sum_{m=0}^{2^n-1}(-1)^{f(l)+lm}\lvert m\rangle\ .} \tag{1.36}$$

Let us look into the probability amplitude of the state $m = 0$ when measurement is done:

$$A_0 = \frac{1}{2^n}\sum_{l=0}^{2^n-1}(-1)^{f(l)}\,. \tag{1.37}$$

- **Case I: f is constant:** In this case, we always have $f(l) = 0$ or $f(l) = 1$, following which $(-1)^{f(l)}$ becomes $+1$ or -1 respectively and hence $A_0 = \pm 1$. So the probability of observing $\lvert 0\rangle^n$ becomes $\lvert A_0\rvert^2 = 1$.

- **Case II: f is balanced:** On the other hand, if f is balanced, in the sum $\sum_{l=0}^{2^n-1}(-1)^{f(l)}$, there arise equal number of $f(l) = 0$ and $f(l) = 1$, making the sum 0 and hence $A_0 = 0$. Thus the probability of seeing $\lvert 0\rangle^n$ becomes $\lvert A_0\rvert^2 = 0$.

1.8 Python codes

Python based codes (using *Qiskit SDK*) are available online:

- Click ☞ Deutsch algorithm.
- Click ☞ Deutsch-Jozsa algorithm.

Suggested reading

1. Cleve *et al.*, Quantum Algorithms Revisited, https://arxiv.org/pdf/quant-ph/9708016.

2. *An Introduction to Quantum Computing* by Phillip Kaye, Raymond Laflamme, and Michele Mosca , Oxford University Press, New York (2007).

3. *Quantum Computer Science* by N. David Mermin, Cambridge University Press, New York (2007) (read specifically for the oracle construction).

4. Deutsch and Jozsa, Rapid solution of problems by quantum computation, https://royalsocietypublishing.org/doi/10.1098/rspa.1992.0167.

5. https://young.physics.ucsc.edu/150/deutsch.pdf.

6. Peter Shor's notes.

7. Chapter 6, *Quantum Information* by John Preskill.