Quantum Computing (量子计算)

Get ready to grasp the leading edge technologies

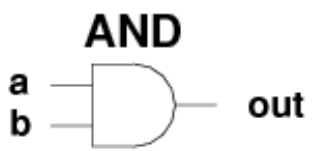
Driss BOUTAT

Institut National des Sciences Appliquées Centre Val de Loire .

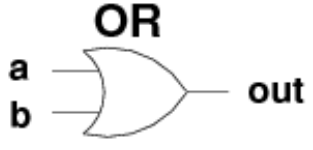
Binary logical gates

Let's provide some logical gates used for binary computers that enable us to communicate with or computer.

- Operator AND outputs the value $1 =$ TRUE if inputs are both 1,
- Operator OR outputs the value $1 =$ TRUE if one or more of its inputs 1.



a	b	out
0	0	0
0	1	0
1	0	0
1	1	1



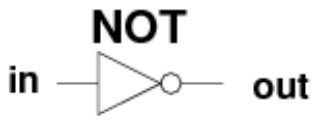
a	b	out
0	0	0
0	1	1
1	0	1
1	1	1

Figure: Logical AND and OR.

Binary logical gates

- Operator XOR outputs the value $1 =$ TRUE if either, but not both, one of its two inputs is true 1.
- Operator NOT reverses the values $1 =$ TRUE and $0 =$ False.

a	b	out
0	0	0
0	1	1
1	0	1
1	1	0



in	out
0	1
1	0

Figure: Logical XOR and NOT (bits).

Binary logical gates

we have also NOR gate and NAND gate

- NOR gate which is a 2-input OR gate followed with a NOT gate,
- NAND gate which is a 2-input AND gate followed with a NOT gate.

NAND and NOR are known as universal gates since they can be used to devise any digital circuit without using any other gate.This means that every gate can be designed only by NAND or NOR gates.
Unlike the NOT gate, the others are not reversible gates. Indeed, the inputs cannot be unambiguously reconstructed from its single output.

Qubit Gates: NOT gate

Qubit Gates are **unitary** and **reversible**. The Not gate acting on one qubit is implemented by the matrix $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. It behaves as the logic NOT operator in the binary computation. Therefore, for a state $|a\rangle = \alpha|0\rangle + \beta|1\rangle$, we have $X|a\rangle = \beta|0\rangle + \alpha|1\rangle$.

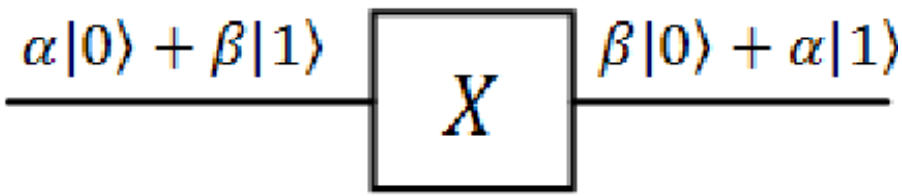


Figure: Quantum circuit diagram of a NOT-gate

Qubit Gates : NOT Gate

Realization of X gate in IBM Q Experience by grabbing and dropping green tab (or box) on wire as well as the measurement pink tab:

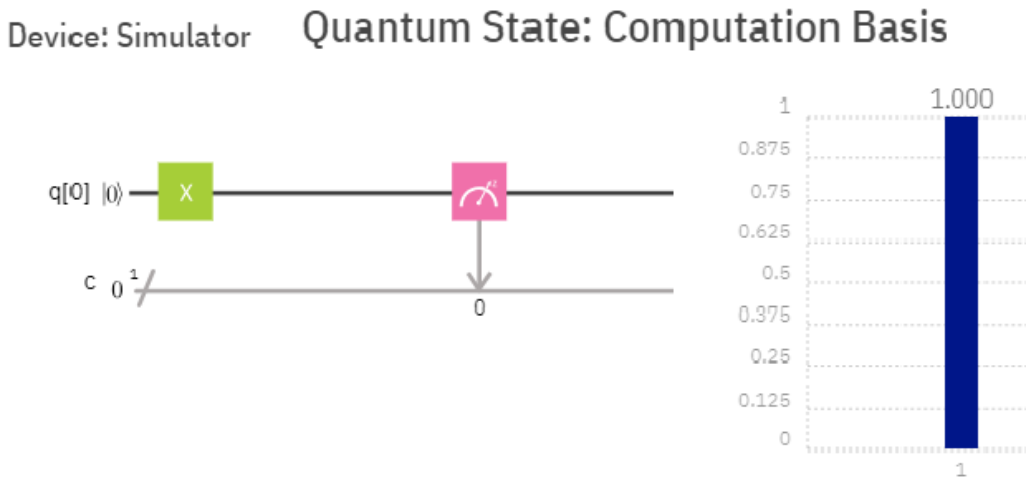


Figure: IBM Q Experience

This means that we apply X (green tab or box) to the state $|0\rangle$. Measurement on the right represented by the blue bar chart is a probability of obtaining the state $|1\rangle$.

Qubit Gates: Hadamard's gate (superposition)

The Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, acts on a single qubit.

It maps the basis states as follows

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

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

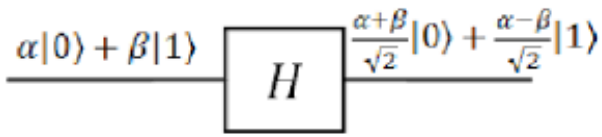


Figure: Quantum circuit diagram of a NOT-gate

Qubit Gates: Hadamard's gate (superposition)

Realization of H gate in IBM Q Experience

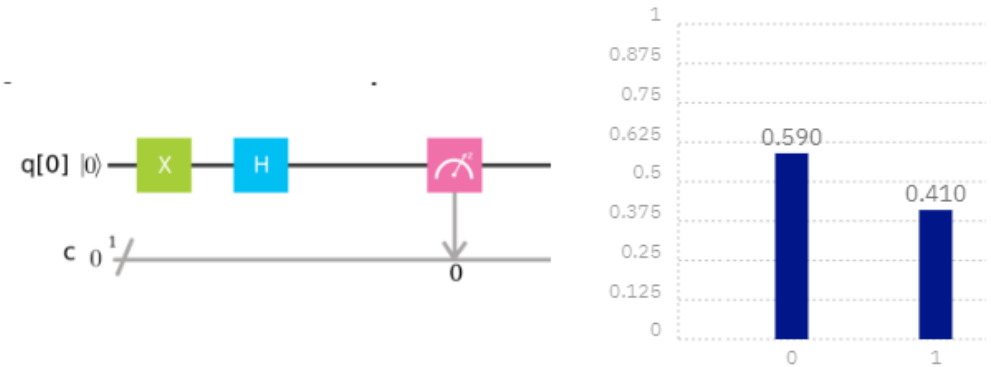


Figure: Hadamard's IBM Q Experience

Here we apply H to $X|0\rangle = |1\rangle$. The result shows that the probability of obtaining the state $|0\rangle$ and $|1\rangle$ are 0.59 and 0.41 respectively. You must not be supervised if you don't see $-|1\rangle$. This is the point, we measure probabilities and not coefficients !

Controlled Not gate : CNOT

Denote U_{CN} as a matrix acting on double qubits :

$$U_{CN}\left|00\right\rangle = \left|00\right\rangle, U_{CN}\left|01\right\rangle = \left|01\right\rangle, U_{CN}\left|10\right\rangle = \left|11\right\rangle, U_{CN}\left|11\right\rangle = \left|10\right\rangle$$

which doesn't change the first qubit and change the second if the first is 1 otherwise left it invariant. Therefore its matrix is given by

$$U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

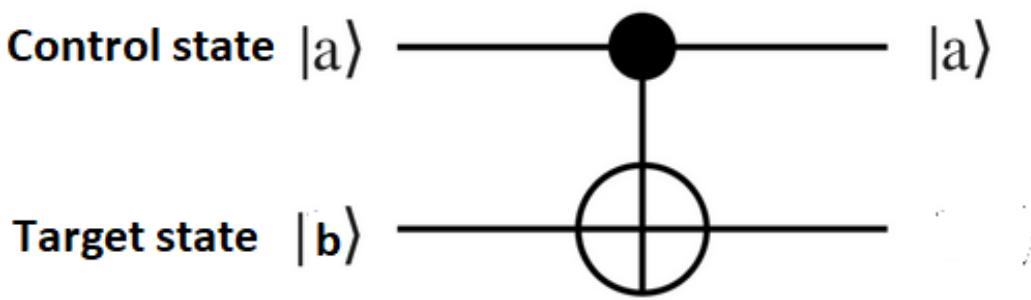


Figure: Quantum circuit diagram of a Controlled NOT gate

Controlled Not gate : CNOT

Realization of CNOT gate in IBM Q Experience

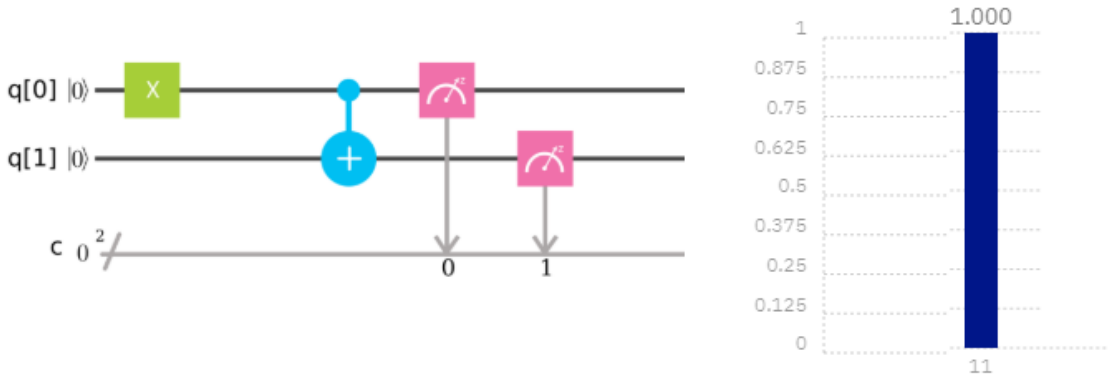


Figure: CNOT IBM Q Experience

Here we have two wires which represents a tensor product of tow states: $X|0\rangle \otimes |0\rangle$. As, $X|0\rangle = |1\rangle$. We obtain $U_{CN}|10\rangle = |11\rangle$ with probability 1.

Swap gate

Swap gate is a matrix that acts on double qubits as follows $S|00\rangle = |00\rangle$, $S|01\rangle = |10\rangle$, $S|10\rangle = |01\rangle$ and $S|11\rangle = |11\rangle$. Thus it switch the qubit if they are different. Therefore its matrix is given by $U_{CN} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

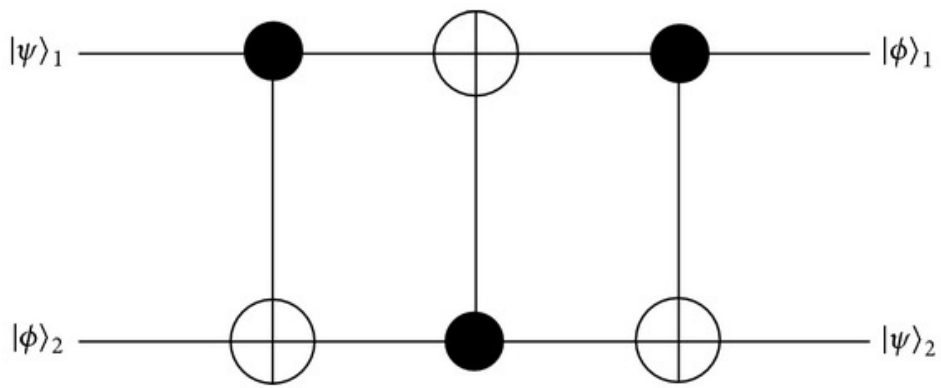


Figure: Quantum circuit diagram of a Swap gate

Swap gate

From the figure bellow; we see that swap gate is a composition of three C-Not gates. The first and the third are controlled by means of the first qubit and the second is controlled by means of the second qubit. Indeed we will show that $S = U_1U_2U_1$ where U_i stands for controlled by the i^{th} qubit. Indeed, we have

- $U_1U_2U_1 |00\rangle = |00\rangle$,
- $U_1U_2U_1 |11\rangle = U_1U_2 |10\rangle = U_1 |10\rangle = |11\rangle$
- $U_1U_2U_1 |01\rangle = U_1U_2 |01\rangle = U_1 |11\rangle = |10\rangle$
- $U_1U_2U_1 |10\rangle = U_1U_2 |11\rangle = U_1 |01\rangle = |01\rangle$

Swap gate

You can check this in IBM Q Experience. Beware, here I took the first measurement on second line and the second measurement in the first line to get result as provided by the notations used in this document.

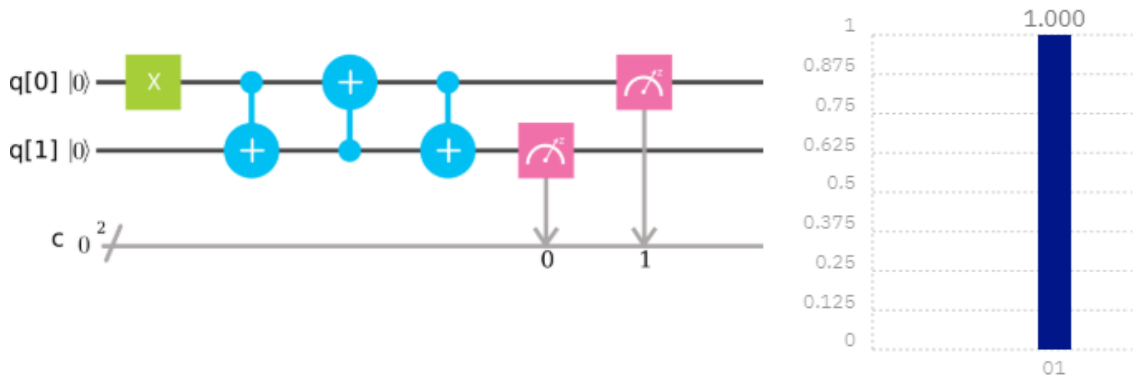


Figure: IBM Q Experience swap realization.

Here we test it for the state $|10\rangle$. The quantum state that appears in the right: in the bottom the output state $|01\rangle$ with the probability 1 which appears in the top.

No cloning problem

Given a state $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ and consider $|a\rangle \otimes |0\rangle$. Is there any unitary operator U such that:

$$U(|a\rangle \otimes |0\rangle) = |a\rangle \otimes |a\rangle?$$

that means U copies $|a\rangle$ in the slot $|0\rangle$.

The answer is NO. There is no operator that cloning (克隆) all state. Indeed, if we assume that is possible then we will have in one hand $U(|a\rangle \otimes |0\rangle) = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$, and by linearity in other hand we have $U(|a\rangle \otimes |0\rangle) = \alpha|00\rangle + \beta|11\rangle$. Be aware with this particular case: $U_{CN}|00\rangle = |00\rangle$ and $U_{CN}|10\rangle = |11\rangle$. Thus U_{CN} copies states $|0\rangle$ and $|1\rangle$

Deutsch-Josza Algorithm

The Deutsch-Josza algorithm consists of determining if a given a function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is **constant** or **balanced**.

Deutsch 's is diagram is as follows

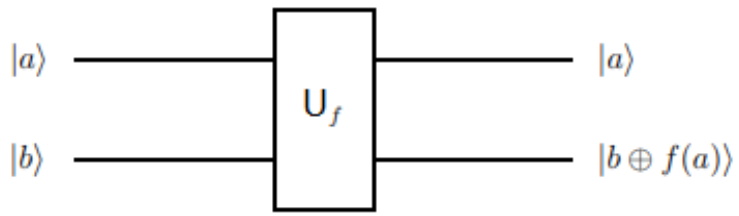


Figure: Deutsch' s circuit diagram

U_f a controlled operator

$\oplus$ stands for $+$ together with $\mod 2$ in binary basis. Therefore, $U_f\left(|a\rangle \otimes |b\rangle\right) = |a\rangle \otimes |b \oplus f(a)\rangle$ is an unitary controlled operator where $|a\rangle$ is the control state and $|b\rangle$ is the target state.

Deutsch-Josza Algorithm

Let's $k = k_1 ... k_n$ in its binary writing, be an integer ranging from 0 to $2^n - 1$. Let's use the Hadamard's operator

$$U_f \left(|k\rangle \otimes H |1\rangle \right) = \frac{1}{\sqrt{2}} |k\rangle \otimes \left(|0 \oplus f(k)\rangle - |1 \oplus f(k)\rangle \right).$$

According to the case where $f(k) = 0 \mod 2$ or $1 \mod 2$, we deduce that:

$$U_f \left(|k\rangle \otimes H |1\rangle \right) = \frac{(-1)^{f(k)}}{\sqrt{2}} |k\rangle \otimes \left(|0\rangle - |1\rangle \right).$$

Now, we normalize and sum up all terms over all k to obtain

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{k=0}^{2^n - 1} (-1)^{f(k)} |k\rangle \otimes \left(|0\rangle - |1\rangle \right).$$

Deutsch-Josza Algorithm

Now if f is constant then

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{k=0}^{2^n-1} (-1)^{f(k)} |k\rangle \otimes (|0\rangle - |1\rangle) .$$

becomes

$$\frac{\pm 1}{\sqrt{2^{n+1}}} \sum_{k=0}^{2^n-1} |k\rangle \otimes (|0\rangle - |1\rangle) .$$

A straightforward calculation shows that $\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle = H^{\otimes n} |0\rangle$.

Deutsch-Josza Algorithm

Thereby, by applying $(n+1)\otimes$ copies of $H^{-1} = H$ we get $\pm |0\rangle^{n\otimes} \otimes |1\rangle$. Thus we have

$$|0\rangle^{n\otimes} \otimes |1\rangle \overset{H^{\otimes(n+1)} \times U_f \times H^{\otimes(n+1)}}{\longrightarrow} \pm |0\rangle^{n\otimes} \otimes |1\rangle .$$

Thus the output is related to the input by a phase factor.

Deutsch-Josza Algorithm

Now if f is balanced then we apply the operator $H^{\otimes(n+1)}$ to

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{k=0}^{2^n-1}(-1)^{f(k)}\left|k\right\rangle\otimes\left(\left|0\right\rangle-\left|1\right\rangle\right).$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{k=0}^{2^n-1}(-1)^{f(k)}H^{\otimes(n)}\left|k\right\rangle\otimes\left|1\right\rangle=\frac{1}{2^{n+1}}\sum_{k=0}^{2^n-1}(-1)^{f(k)}\left(\left|0\right\rangle+(-1)^{k_i}\left|1\right\rangle\right)^{\otimes n}\otimes\left|1\right\rangle.$$

Now, we can see that the amplitude of $\left|0\right\rangle^{\otimes n}\otimes\left|1\right\rangle$ is

$$\sum_{k=0}^{2^n-1}(-1)^{f(k)}=0$$

because f is assumed to be balanced.

Deutsch-Josza Algorithm

To keep in mind

f is constant if and only if

$$H^{\otimes n+1} U_f H^{\otimes n+1} \left(|0\rangle \otimes |1\rangle \right) = \pm |0\rangle \otimes |1\rangle .$$

Thus, the input appears in the measurement (the output) with probability 1. The circuit doesn't change up to a factor (phase) the input.

Remark

If the input $|0\rangle \otimes |1\rangle$ appears in the measurement with a probability $0 < p < 1$, then f is neither constant nor balance.

Deutsch-Josza Algorithm

Let's do simulations in the case of one qubit where $f : \{0,1\} \longrightarrow \{0,1\}$. We have the following four cases. .

Input	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Construct U_f operator for each case. For **constant maps**, we have:

- for $f_0 \equiv 0$ it clear that $U_f = \mathrm{Id} \otimes \mathrm{Id}$ on $\mathcal{H}_2 \otimes \mathcal{H}_2$.
- for $f_3 \equiv 1$ it clear that $U_f = X \otimes X$ operator on $\mathcal{H}_2 \otimes \mathcal{H}_2$. Because $U_f\left(|a\rangle \otimes |b\rangle\right) = |a\rangle \otimes |b \oplus 1\rangle$

Deutsch-Josza Algorithm

Let's do simulations for the case $f_3 \equiv 1$ thus $U_f = X \otimes X$ operator on $\mathcal{H}_2 \otimes \mathcal{H}_2$

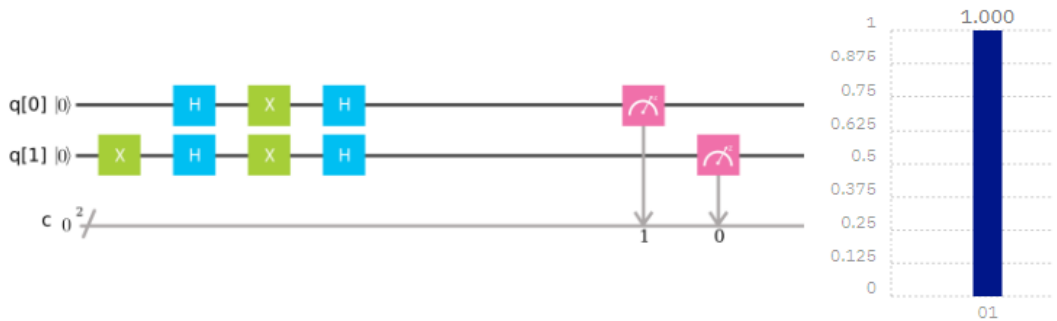


Figure: Deutsch' s circuit for $f \equiv 1$

the input is $|0\rangle \otimes |1\rangle$ and the measurement (the output) gives the amplitude of $|0\rangle \otimes |1\rangle$ with probability 1. A simple hand calculation leads to $-|0\rangle \otimes |1\rangle$. For the case $f_0 \equiv 0$, just remove the X gates in the above circuit.

Deutsch-Josza Algorithm

Interpretation

the output is equal to input up to a factor (phase) $e^{i\pi} = -1$. The input appears with probity 1 in the measurement.

In the previous circuit I change the order of measurement to get the good presentation of the tensor product.

Deutsch-Josza Algorithm

Now let's deal with the balanced maps operator U_f. Let's start with $f_1 \equiv \mathrm{Id}$. It is clear that $U_f = \mathrm{Id} \otimes X$ which is the CNOT operator on $\mathcal{H}_2 \otimes \mathcal{H}_2$ where X is the Pauli's NOT operator.

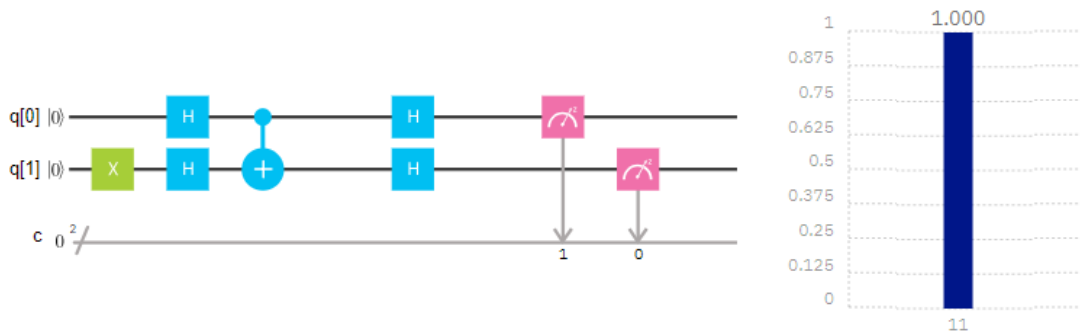


Figure: Deutsch' s circuit for $f \equiv \mathrm{Id}$

The measurement (the output) gives the amplitude of $|1\rangle \otimes |1\rangle$ with probability 1.

Read out

The input state appears in the measurement with 0 probability which means that f is balanced.

Deutsch-Josza Algorithm

For the balanced case $f \equiv \text{Not}$, we have $U_f = X \otimes \text{Id}$ in $\mathcal{H}_2 \otimes \mathcal{H}_2$ thus the quantum circuits are as follows:

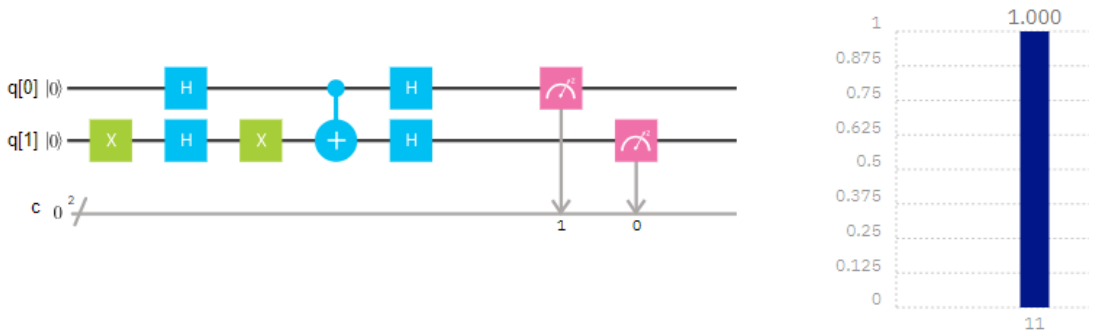


Figure: Deutsch' s circuit for $f \equiv \text{Not}$

The measurement (the output) gives the amplitude of $|1\rangle \otimes |1\rangle$ with probability 1.

Read out

The input state appears in the measurement with 0 probability which means that f is balanced.

Algorithm of phase estimation

Phase estimation (相位估计)

Let U an unitary operator and let $|\varphi\rangle$ an eigenvector of U, thus

$$U|\varphi\rangle = e^{2i\pi\theta}|\varphi\rangle.$$

The objective is to estimate

$$\theta \in [0,1) \Rightarrow \text{the eigenvalue} \lambda = e^{2i\pi\theta}.$$

Since $|e^{2i\pi\theta}| = 1$ doesn't appear in the measurement, we need another way to achieve this. For this, assume we have

$$\theta = \frac{x}{2^n}, \quad \lambda = e^{2i\pi\theta}$$

where $x = x_1 ... x_n$ in binary basis. The algorithm goes as follows :

Algorithm of phase estimation

Algorithm

- we prepare the following state $|0^{\otimes n}\rangle |\varphi\rangle$
- we apply the Hadamard $H^{\otimes n}$ to the first state $|0^{\otimes n}\rangle$ to obtain $\frac{1}{\sqrt{2^n}} \left(\sum_{k=0}^{2^n-1} |k\rangle \right) |\varphi\rangle$
- we apply controlled U as follows $U |k\rangle |\varphi\rangle = |k\rangle U^k |\varphi\rangle$ to obtain $\frac{1}{\sqrt{2^n}} \left(\sum_{k=0}^{2^n-1} |k\rangle \right) \lambda^k |\varphi\rangle$, which can be written as

$$\frac{1}{\sqrt{2^n}} \left(\sum_{k=0}^{2^n-1} e^{2i\pi\theta k} |k\rangle \right) |\varphi\rangle .$$

Algorithm of phase estimation

This last equation is in the form of $\frac{1}{\sqrt{2^n}}\left(\sum_{k=0}^{2^n-1} e^{2i\pi\theta k}\left|k\right\rangle\right)\left|\varphi\right\rangle = \mathfrak{F}\left|2^n\theta\right\rangle \otimes \left|\varphi\right\rangle$. Thus to get θ we need apply the inverse QFT on the state $\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2i\pi\theta k}\left|k\right\rangle$.

The diagram looks like this

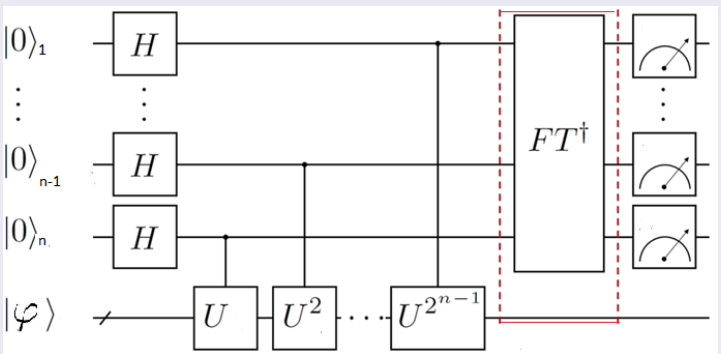


Figure: Diagram of phase estimation.

Phase estimation on IBM Q 5 Tenerife

We consider $U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ with the eigenstate

$$|\varphi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + i\,|1\rangle)$$

and its eigenvalue

$$\lambda = e^{\frac{3}{2}i\pi} = -i.$$

To prepare the eigenstate $|\varphi\rangle$, we use

$$|\varphi\rangle = SH\,|0\rangle$$

where $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

Phase estimation on IBM Q 5 Tenerife

2 qubits estimation

To simulate control U we use $CU3$ from IBM's advanced gates.

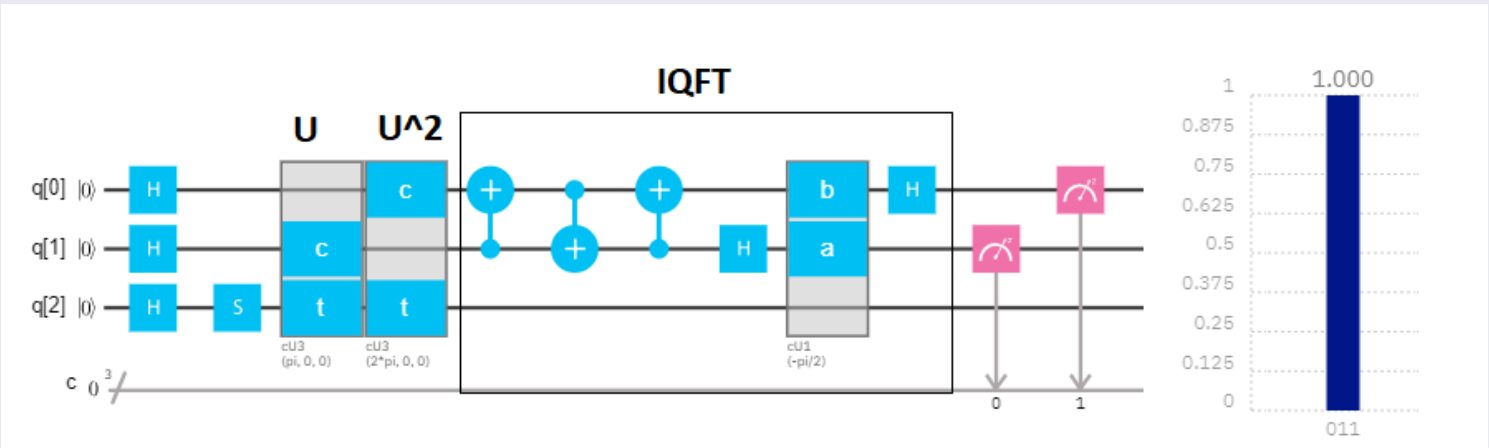


Figure: Phase estimation using two qubits.

We obtain the state 011 with probability 1. In binary basis this is $0 \times 2^2 + 1 \times 2 + 1 \times 2^0 = 3$ Thus $2^2\theta = 3$ the power 2 because we used two qubits. Therefore we get $\theta = \frac{3}{4} \Rightarrow \lambda = e^{2i\pi\theta} = -i$.

Phase estimation IBM IBM Q 5 Tenerife

3 qubits estimation

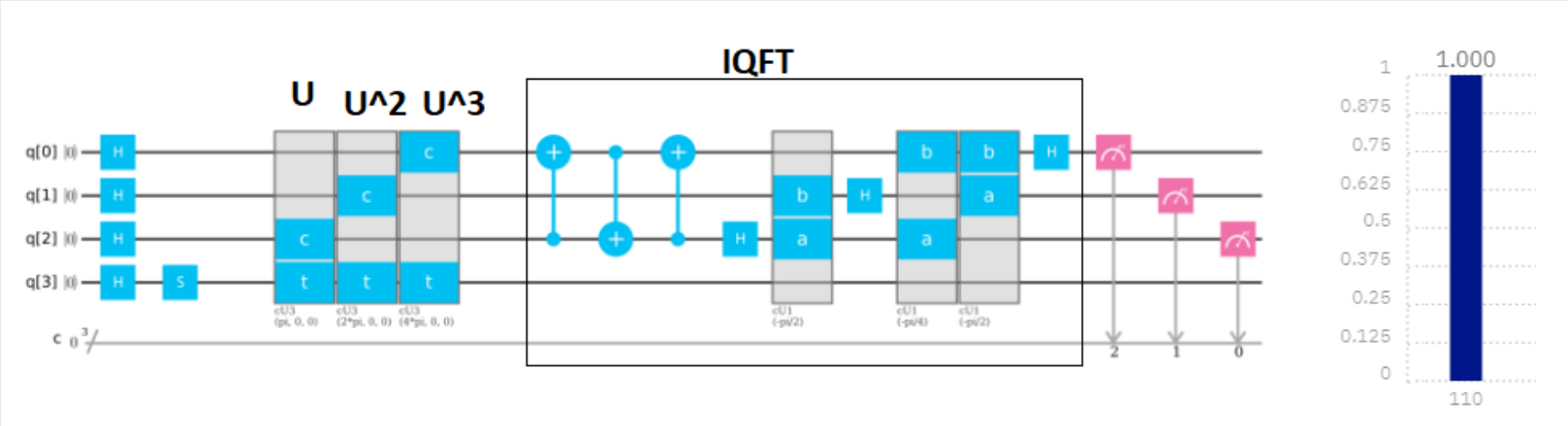


Figure: Phase estimation using three qubits.

We obtain the state 110 with probability 1. In binary basis this is $1 \times 2^2 + 1 \times 2 + 0 \times 2^0 = 6$ Thus $2^3\theta = 6$ the power 3 because we used three qubits. Therefore we get $\theta = \frac{3}{4} \Rightarrow \lambda = e^{2i\pi\theta} = -i$. Thus, we reach the same result.

Grover's algorithm: research

For example, we want to find $|w\rangle = |11\rangle$ from the list $\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\}$. First we write,

$$|\psi\rangle = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$$

then we use an oralacle to flag $|w\rangle$

$$\begin{aligned} O\_\omega|\psi\rangle &= \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle) \\ &= |\psi\rangle - |11\rangle \end{aligned}$$

Finally, we apply the following operator to increase the amplitude of state $|w\rangle$

$$R = 2|\psi\rangle\langle\psi| - I_d = H(2|0\rangle\langle 0| - I_d)H = HZH$$

$$\begin{aligned} RO\_\omega \left|\psi\right\rangle &= \left|\psi\right\rangle + \left|11\right\rangle - 2\left|\psi\right\rangle\left\langle\psi\right|\left|01\right\rangle \\ &= \left|11\right\rangle \end{aligned}$$

The Grover's diffusion operator

$$G = HZHO$$

Grover's algorithm: research

Grover' s algorithm provides a trick to **exponentially** speed up an unstructured search problem. It enables to find an item among a list of $N = 2^n$ items.

The Oracle

The Oracle flags the desired item ω as follows

$$O\_\omega(|x\rangle) = \begin{cases} |x\rangle \text{ if } x \neq \omega \\ -|x\rangle \text{ if } x = \omega \end{cases}$$

For example $|\psi\rangle = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle + |11\rangle)$ and $|\omega\rangle = |01\rangle$ then

$$O\_\omega|\psi\rangle = \frac{1}{2}(|00\rangle + |10\rangle - |01\rangle + |11\rangle)$$

Amplitude amplification

To be continued! And I will give references used to write the present presentation.

Reflection Gate

Grover's diffusion operator (or mean inversion). Let $R_0 = 2\left|0\right\rangle\left\langle 0\right| - I_d$

$$R_0 = -\begin{pmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} = -X \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix} X$$