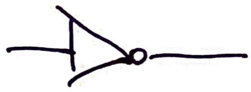
Classical gates:



NOT

$$\equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

if the input is $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

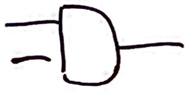
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

if the input is $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$



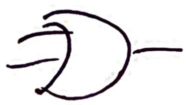
AND

$$\equiv \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\left.\begin{aligned} AND|\underbrace{11}\rangle &= \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ 1 \otimes 1 &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned}\right\} \Rightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \equiv |1\rangle$$

i.e. $AND|11\rangle = |1\rangle$

$$AND|01\rangle = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \equiv |0\rangle$$



OR

$$\equiv \begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 0 \\ 1 \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

NAND

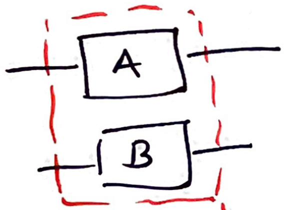
$$\equiv \begin{array}{c c} & \overbrace{\begin{array}{cccc} 00 & 01 & 10 & 11 \end{array}}^{\text{inputs}} \\ \text{outputs}\left\{\begin{array}{c} 0 \\ 1 \end{array}\right. & \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

NAND = AND + NOT

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

seq. combination

and also parallel combination



$A \otimes B$

Reversible gates: gates that are invertible:

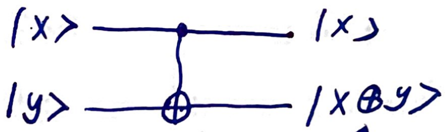
Q: given the output can you find the input?

A: yes, only if the corresponding matrix is invertible (must be square).

examples: NOT gate : $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

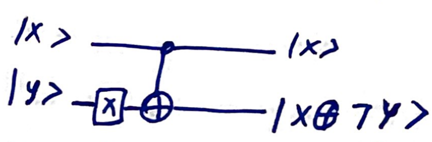
Identity gate : $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

CNOT gate:



exclusive OR

$$= \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array}$$



$$= \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 0 & 1 & 0 & 0 \\ 01 & 1 & 0 & 0 & 0 \\ 10 & 0 & 0 & 1 & 0 \\ 11 & 0 & 0 & 0 & 1 \end{array}$$

Quantum parallelism (by Deutsh's algorithm)

$x \longrightarrow \boxed{?} \longrightarrow f(x)$

"black-box"

assume $x \in \{0,1\}$ (input is a bit) and $f(x) \in \{0,1\}$ (output is a bit)

possibilities:

$f(0) \to 0$, $f(1) \to 0$; $f(0) \to 1$, $f(1) \to 1$ — constant functions (i.e. $f(0) = f(1)$)

$f(0) \to 1$, $f(1) \to 0$; $f(0) \to 0$, $f(1) \to 1$ — balanced functions (i.e. $f(0) \neq f(1)$)

in classical computing to find out what the black-box is we have to make two queries.

1) $f(0) \longrightarrow ?$

2) $f(1) \longrightarrow ?$

* in quantum computing we can have a superposition of two states at the same time.

and we can think of f as a matrix that is multiplied by a vector x s.t. $f(x) = A_f x$ where $A = \left(\begin{smallmatrix} \cdot & \cdot \\ \cdot & \cdot \end{smallmatrix}\right)_{2\times 2}$

invertible

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \cancel{1} \\ 0 \end{pmatrix} \to \begin{pmatrix} \cancel{1} \\ 0 \end{pmatrix}$: $f(x) = x$

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cancel{1} \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 \\ \cancel{1} \end{pmatrix}$: $f(x) = \neg x$

} reversible

not invertible

$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 0 \\ 1 \end{pmatrix}$: $f(x) = 1$

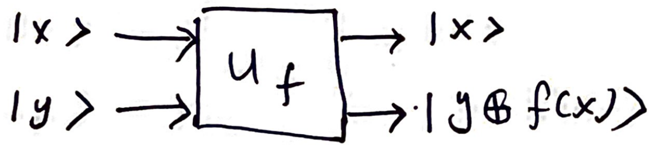
$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 1 \\ 0 \end{pmatrix}$: $f(x) = 0$

} not reversible

Let us define an invertible unitary transformation such that.

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

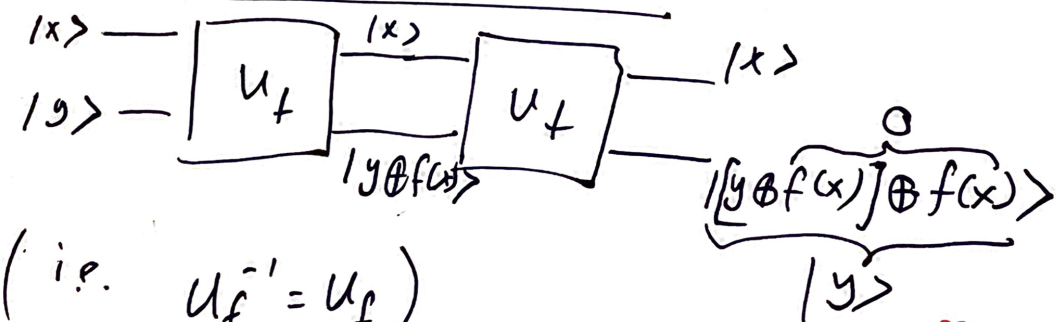
i.e.



Where $\oplus$ is XOR (binary addition modulo 2)

if $y=0 \Rightarrow |x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$

<u>It is reversible because:</u>



(i.e. $U_f^{-1} = U_f$)

Where $U_f = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 0 & 1 & 0 & 0 \\ 01 & 1 & 0 & 0 & 0 \\ 10 & 0 & 0 & 1 & 0 \\ 11 & 0 & 0 & 0 & 1 \end{array}$ (for $f(x) = \neg x$

or $U_f = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & 1 & 0 & 0 & 0 \\ 01 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 0 & 1 \\ 11 & 0 & 0 & 1 & 0 \end{array}$ (for $f(x) = x$)

$U_f = \begin{array}{c|cccc} & 00 & 01 & 10 & 11 \\ \hline 00 & & & & \\ 01 & & & & \\ 10 & & & & \\ 11 & & & & \end{array}$

for $f(x) = 0$

$U_f = \left[\quad \right]$

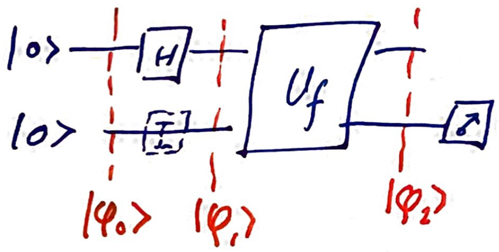
for $f(x) = 1$

Exercise

Task: We are given such a matrix U_f but we can not look inside matrix. We can only compute the output for a given input. Let's try $|x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ as a superposition of states as the input.

$$H|0\rangle = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

and let us choose $|y\rangle = |0\rangle$



$$|00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |\varphi_0\rangle$$

$$\underbrace{U_f(H \otimes I)(|0\rangle \otimes |0\rangle)}$$

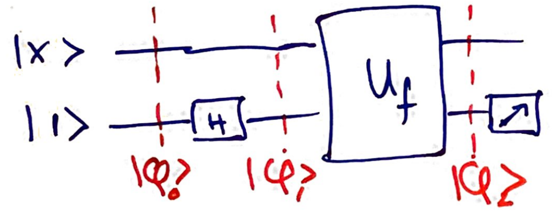
$$\Rightarrow |\varphi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}$$

$$\Rightarrow |\varphi_2\rangle = \frac{|0\,\underline{f(0)}\rangle + |1\,\underline{f(1)}\rangle}{\sqrt{2}}$$

if we measure the top qubit it is 50% 0 and %50 1, there is not much information here.

Another try:

Let the bottom qubit be $\frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$



$\equiv U_f (I \otimes H) |x\,1\rangle$

$|\varphi_0\rangle = |x\,1\rangle$

$|\varphi_1\rangle = |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{|x\,0\rangle - |x\,1\rangle}{\sqrt{2}}$

$U_f|\varphi_1\rangle = |x\rangle\left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}\right)$

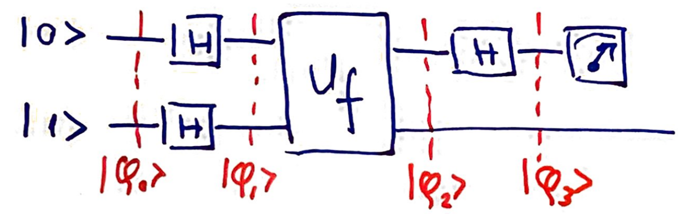
$|\varphi_2\rangle = |x\rangle\left(\frac{|f(x)\rangle - |\neg f(x)\rangle}{\sqrt{2}}\right)$

$\Rightarrow |\varphi_2\rangle = \begin{cases} |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(x) = 0 \\ |x\rangle\left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right) & \text{if } f(x) = 1 \end{cases}$

$\Rightarrow |\varphi_2\rangle = (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

top quibit is in state $|x\rangle$ and the bottom qubit is either in state $|0\rangle$ or $|1\rangle$. This does not help us much.

Final try (Deutsch's algorithm)



$$\equiv \; (H \otimes I) U_f (H \otimes H) \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}}_{|\varphi_0\rangle = |01\rangle}$$

$$|\varphi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{+|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2} = \begin{bmatrix} +\frac{1}{2} \\ -\frac{1}{2} \\ +\frac{1}{2} \\ -\frac{1}{2} \end{bmatrix}$$

We saw from the previous attempt that when the bottom qubit is in superposition:

$$(-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

now $|x\rangle$ is also in superposition

$$|\varphi_2\rangle = \left[\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

for example if $f(0) = 1$ and $f(1) = 0$ the top qubit becomes:

$$(-1)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

if f is constant ~~it is either~~:

$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$ is either

$+(|0\rangle + |1\rangle)$ or $-(|0\rangle + |1\rangle)$

if f is balanced

$(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$ is either

$+(|0\rangle - |1\rangle)$ or $-(|0\rangle - |1\rangle)$

therefore:

$$|\varphi_2\rangle = \begin{cases} (\pm)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if constant} \\ (\pm)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if balanced} \end{cases}$$

remember Hadamard matrix is its of inverse that takes $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ to $|0\rangle$ and takes $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ to $|1\rangle$, then we apply Hadamard gate to the top qubit and obtain,

$$|\varphi_3\rangle = \begin{cases} (\pm)|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if constant} \\ (\pm)|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if balanced.} \end{cases}$$

for example if $f(0)=1$ and $f(1)=0$ then we get,

$$|\varphi_3\rangle = -|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

We measure the top qubit if $|0\rangle$ it is constant if $|1\rangle$ it is balanced.

The sign here tells us more about the function but we don't capture the sign when we make the measurement.

Note: even though the top qubit is the same qubit that comes in however via Hadamard gates top and bottom qubits are entangled.

Created with Scanner Pro