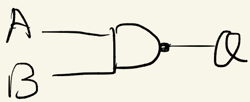
# Classical Circuit VS. Quantum Circuit

Any boolean function $f: \{0,1\}^m \to \{0,1\}^n$ can be computed by a reversible quantum circuit.

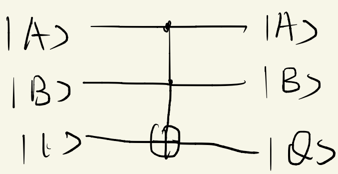
① The NAND gate is universal for classical circuits and acts as below




| A | B | Q |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

NAND gate is not a reversible gate: whe $Q = 1$ we do not know what exact values for input A and B.

② We can perform the same operation using a Toffoli gate. (CCNOT gate).




| A | B | Q |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Toffoli gate is known as universal for classical circuits, not yet for quantum circuits.

Recall: Toffoli can be constructed with $2H + 7T + 6CNOT$

③ we can convert any classical algorithm into a quantum algorithm, replacing the NAND gates with Toffolis and keeping the extra qubits.

⇒ Key message: Quantum can do classical work.

Classical circuits look like a special case of quantum circuits.

Any boolean function $f: \{0,1\}^m \to \{0,1\}^n$ can be efficiently computed by a reversible quantum circuit.

Efficiency: # Gates: 1 NAND → 1 Toffoli

# inputs: n → ? # gates + # inputs

Theoretically, the minimum number of extra inputs we need to use indeed is 1.

① A = how many different binary functions are there that can take n-bit inputs and give n-bit output?

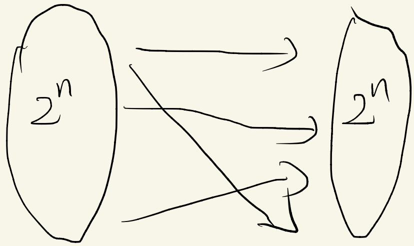
$$A = (2^n)^{2^n}$$

Think of the truth table

- # rows $= 2^n$
- # different output for each row $= 2^n$

② $B$ = how many different reversible boolean functions are there that can take n-bit inputs and give n-bit output?

$B = (2^n)!$




\# input     \# output

key: ① If $x \neq y \Rightarrow f(x) \neq f(y)$

in other words, $f(x) = f(y)$ implies $x = y$.

Otherwise, f will not be reversible.

② Given # input = # output

f just works as a permutation of the input.

$\Rightarrow B = \# f = (2^n)!$

Compare A and B: $A \gg B$

$n = 1 \quad A = 2^2 = 2 \cdot 2$

$B = (2)! = 2 \cdot 1$

$n = k \quad A = (2^k)^{2^k} = \underbrace{2^k \cdot 2^k \cdot 2^k \cdots 2^k}_{2^k}$

$B = (2^k)! = \underbrace{2^k \cdot (2^k - 1) \cdot (2^k - 2) \cdots 1}_{2^k}$

③ $C$ = how many reversible boolean functions are there that can map a $(n+1)$-bit input to a $(n+1)$-bit output

Or in other words, # $(n+1)$ bit reversible boolean functions.

$$C = (2^{n+1})!$$

Compare $A$ and $C$

$n=1$ $\quad A = 2^2 = 2 \cdot 2$

$C = (4)! = 4 \cdot 3 \cdot 2 \cdot 1$

$n=k$ $\quad A = (2^k)^{2^k} = \underbrace{2^k \cdot 2^k \cdot \cdots 2^k}_{2^k}$

$$C = (2^{k+1})! = \underbrace{2^{k+1}(2^{k+1}-1)\cdots(2^k+1)}_{2^k} \cdot \underbrace{2^k \cdots 1}_{2^k}$$

$C \gg A$

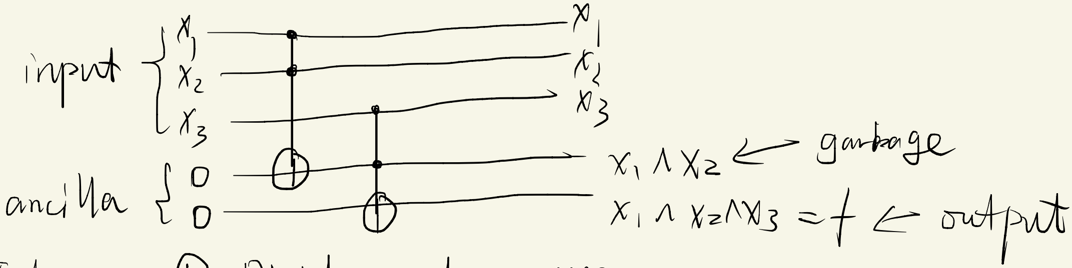
$\Rightarrow$ Key message: Reversibility will hurt the expressiveness, but not a lot.

Theoretically, we only need one extra qubit.

But pratically, it may be hard and would also incurs lots of extra gates.

## Some common tricks to reduce # extra qubits (ancilla qubits)

Example: $f = \text{AND}(x_1, x_2, x_3)$




Idea: ① Divide and conquer
② clean up garbage frequently

Key: we can not directly reuse the garbage qubits. because of the entanglement, and superposition

✓ $|x_1 x_2 x_3\rangle |00\rangle \longrightarrow |x_1 x_2 x_3\rangle |x_1 \wedge x_2\rangle |f\rangle$

It seems that we can simply measure ↗ and set it to $|0\rangle$ and reuse it for follow-up computation.

It work like there is no garbage qubit

$|x_1 x_2 x_3\rangle |0\rangle \rightarrow |x_1 x_2 x_3\rangle |f\rangle$

✓ Now take $|x\rangle$ as a special superposition state

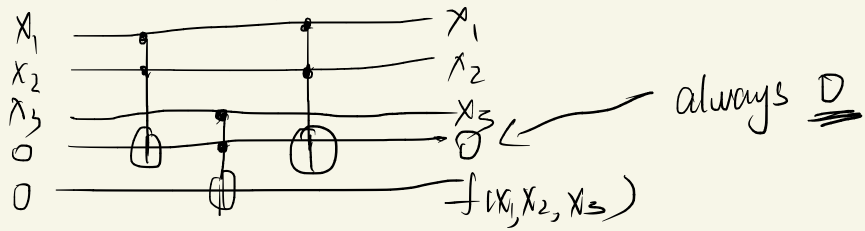
$$\frac{|000\rangle + |110\rangle}{\sqrt{2}}$$

The circuit will take it to $\frac{|000\rangle}{\sqrt{2}}|0\rangle|0\rangle + \frac{|110\rangle}{\sqrt{2}}|1\rangle|0\rangle$

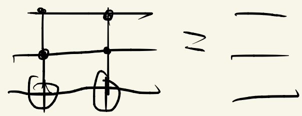
If we measure the garbage qubit, the other qubits will also be affected because of the entanglement. In this case, we can only keep the result for part of the superposition state.

High-level solution: Uncomputation.

Example:

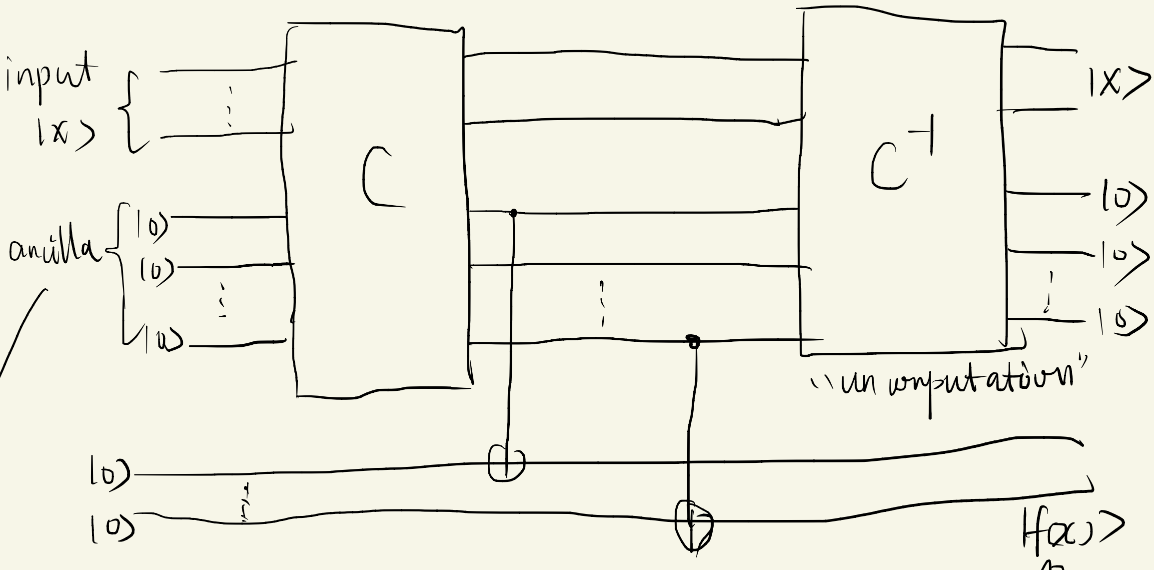



Key: Toffoli gate cancels each other.




or $(x_1 \wedge x_2) \oplus (x_1 \wedge x_2) = 0$

In general, we can perform uncomputation as follows.



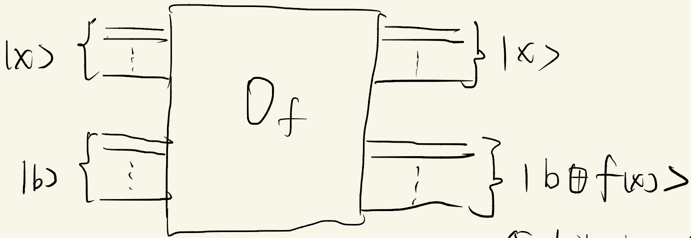

We only need to direct those output related information from the ancilla qubits.

Better strategy for uncomputation? Research problem.

Practice: Let's see how to do that for general $f$.

$$f: \{0,1\}^m \to \{0,1\}^n$$

① "Bit oracle" (XOR oracle): $O_f$




↖ bitwise XOR

key: storing $f(x)$ out-of-place.

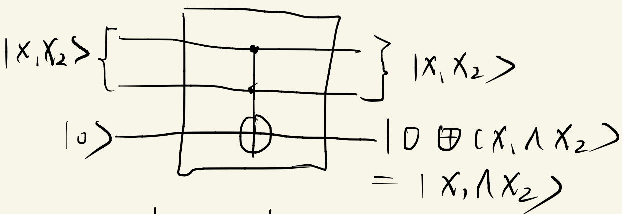
When $|b\rangle = |0\rangle$, then $|b \oplus f(x)\rangle = |f(x)\rangle$

$$\Rightarrow \quad |x\rangle|0\rangle \xrightarrow{O_f} |x\rangle|f(x)\rangle$$

Remark: with superposition

$$\sum_x \alpha_x |x\rangle|0\rangle \xrightarrow{O_f} \sum_x \alpha_x |x\rangle|f(x)\rangle$$

Example: $f = \text{AND}: \{0,1\}^2 \to \{0,1\}$

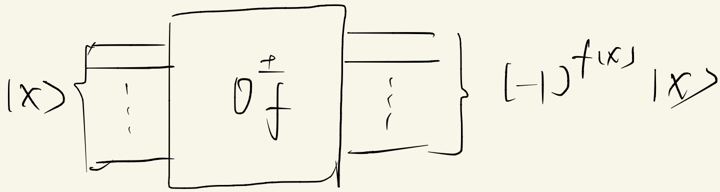



classical vs. Quantum

✓ classical: Each time, we only evaluate some pairs of $x_1x_2$: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

✓ Quantum: With superposition, we may evaluate all of them once.

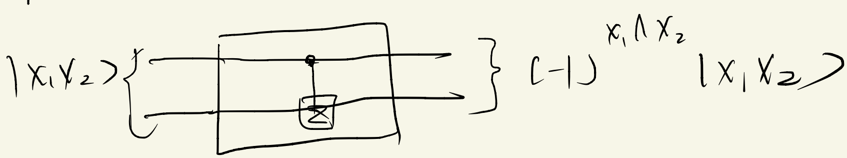
## ② "phase oracle" : $O_f^{\pm}$ (only for $n=1$)

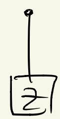



**Key:** storing the result in the phase.

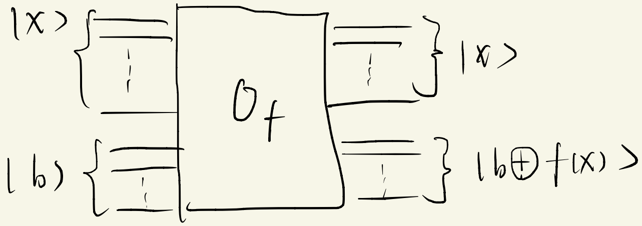
**Remark:** Superposition $\sum_x \alpha_x |x\rangle \xrightarrow{O_f^{\pm}} \sum_x \alpha_x (-1)^{f(x)} |x\rangle$

**Example:** Again for AND:




Recall  $= \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix} = \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |10\rangle \\ |11\rangle \to -|11\rangle \end{cases}$

③ We can use $O_f$ to implement $O_f^{\pm}$. Accutally, we can take $O_f^{\pm}$ as a special case of $O_f$.




✓ $f(x)$ is only 1 bit ✓ set $|b\rangle$ to $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

Input : $|x\rangle|-\rangle = \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle)$

$$\downarrow O_f$$

Output :

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

$$= \frac{1}{\sqrt{2}}(|x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle)$$

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

$$= (-1)^{f(x)}|x\rangle|-\rangle$$

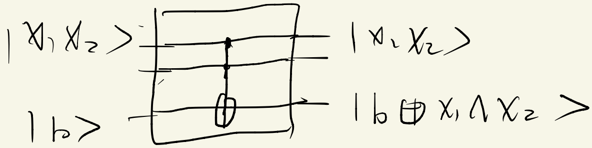
Remark : If we take $|x\rangle$ in a superposition state

$$\left(\sum_x a_x|x\rangle\right)|-\rangle \xrightarrow{O_f} \left(\sum_x a_x(-1)^{f(x)}|x\rangle\right)|-\rangle$$

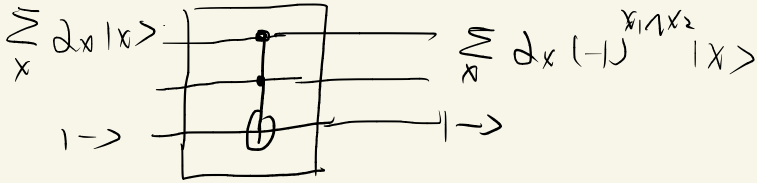
If we ~~measure~~ measure $|b\rangle$ in X basis after $O_f$, then $O_f$ works exactly as a $O_f^{\pm}$. and the output is $\sum_x a_x(-1)^{f(x)}|x\rangle$.

**Example :** still the AND example

Recall $O_f$ :

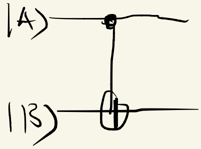



$\Longrightarrow$




It seems that we have changed the control bits.

**Phase kickback**




① Take both $|A\rangle |B\rangle$ in $Z$ basis

$$|z_1, z_2\rangle \xrightarrow{CNOT} |z_1, z_1 \oplus z_2\rangle$$

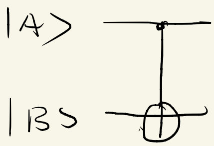
$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle$$

② Take both $|A\rangle |B\rangle$ in $X$ basis

$$|x_1 x_2\rangle \xrightarrow{CNOT} |x_1 \oplus x_2, x_2\rangle$$

$$|++\rangle \rightarrow |++\rangle$$
$$|-+\rangle \rightarrow |-+\rangle$$
$$|+-\rangle \rightarrow |--\rangle$$
$$|--\rangle \rightarrow |+-\rangle$$

A easy way to remember these rules is to take $\begin{cases} |+\rangle \rightarrow |0\rangle \\ |-\rangle \rightarrow |1\rangle \end{cases}$



③ Take $|A\rangle$ in $Z$ basis and set $|B\rangle$ to $|-\rangle$.

$$|x\rangle|-\rangle \xrightarrow{CNOT} ?$$

$$\begin{cases} |0\rangle|-\rangle \xrightarrow{CNOT} |0\rangle|-\rangle \\ |1\rangle|-\rangle \xrightarrow{CNOT} -|1\rangle|-\rangle \end{cases}$$

$$\Rightarrow \quad |x\rangle|-\rangle \xrightarrow{CNOT} (-1)^x|x\rangle|-\rangle$$

Control bit gets a phase.

# Quantum Speedup:

**Query model**

- classical: $x \rightarrow \boxed{f} \rightarrow f(x)$
- Quantum: $|x\rangle \rightarrow \boxed{f} \rightarrow |f(x)\rangle$

$|x\rangle$ ↓ superpositions

$$\sum_x \alpha_x |x\rangle \rightarrow \sum_x \alpha_x |f(x)\rangle$$

classically, you can only query one $x$ at a time, but with quantum, you can have such an parallelism with superposition.

## ① How to create superposition?

$|0\rangle - \boxed{H}$
$|0\rangle - \boxed{H}$
⋮
$|0\rangle - \boxed{H}$

$$|000\cdots0\rangle_n \xrightarrow{H^{\otimes n}} \frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$H^{\otimes 2}|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{(\sqrt{2})^2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

$$= \frac{1}{(\sqrt{2})^2} \sum_{x \in \{0,1\}^2} |x\rangle$$

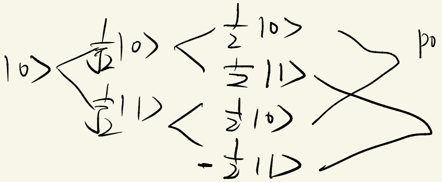
We have uniform distribution of all these "classical" states. but are they useful?

Measurement is how we interact with a quantum system. → randomly collapse to some $|f(x)\rangle$.

② Instead of random collapse, can we create some interference so that we can extract more information from the results.

From an interference perspective to look at the H transformation

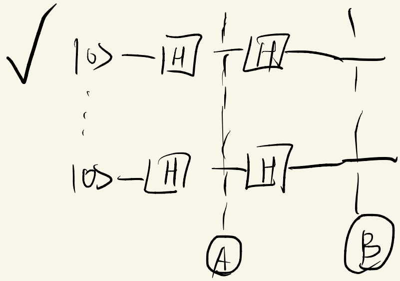
√ $|0\rangle - \boxed{H} - \boxed{H} - |0\rangle$




positive interference $1 \cdot |0\rangle$

negative interference $0 \cdot |1\rangle$

√




Ⓐ: $\frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} |x\rangle$

Ⓑ: ? from the interference perspective

Q: $|x\rangle \xrightarrow{H^{\otimes n}}$ ?

where $x \in \{0,1\}^n$

Example

$$|01\rangle = \frac{1}{(\sqrt{2})^2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

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

$$|10\rangle = \frac{1}{(\sqrt{2})^2}(|0\rangle - |1\rangle)\cdot(|0\rangle + |1\rangle)$$

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

They have the same terms, but different sign.

Define $x \cdot y = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n$

For exaple $\begin{cases} x = 00 \\ y = 01 \end{cases} \Rightarrow x \cdot y = 0$

$\begin{cases} x = 01 \\ y = 01 \end{cases} \Rightarrow x \cdot y = 1$

$$H^{\otimes n} |01\rangle = \frac{1}{(\sqrt{2})^2} \sum_{y \in \{0,1\}^n} (-1)^{[01] \cdot y} |y\rangle$$

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

Now, we are ready to calculate (B) with interference.

$$\frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} |x\rangle \xrightarrow{H^{\otimes n}} \sum_{y = \{0,1\}^n} a_y |y\rangle$$

we first calculate the coeffecient $a_y$ for $y = |00\cdots0\rangle$

$y = 00\cdots0 \Rightarrow x \cdot y = 0$ for whatever $x \Rightarrow (-1)^{x \cdot y} = 1$

As such $a_y = \frac{1}{(\sqrt{2})^n} \sum_{x \in \{0,1\}^n} \frac{1}{(\sqrt{2})^n} \cdot 1 = 1$

We can calculate the coeffecients $a_y$ for other $y$.

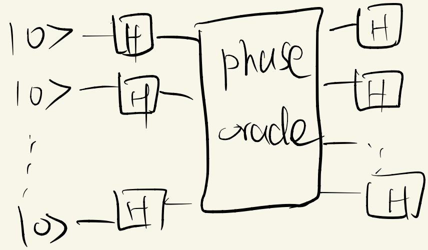
for example $y = |10\cdots01\rangle$

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

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

You can prove that the amplitude for other $|x\rangle$ are all 0.

③




?

The phase for different $|x\rangle$ could disturb the original interference pattern.