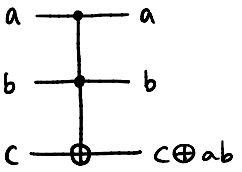
7-1 Deutsch's Algorithm

§1.4 Quantum algorithms

classical computations on a quantum computer

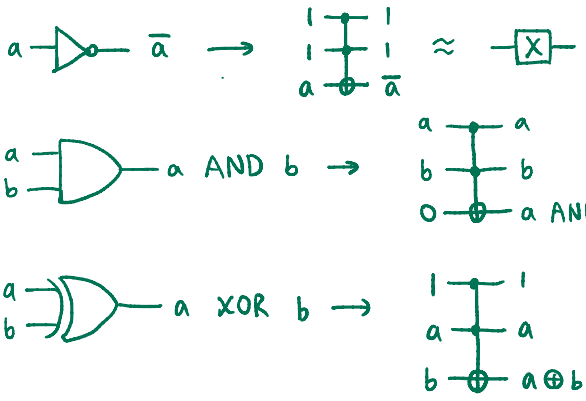
Toffoli gate: controlled-controlled-NOT



$$\begin{cases} c \to \bar{c} & \text{if } a = b = 1 \\ c \to c & \text{otherwise} \end{cases}$$

Toffoli gates with variable input can simulate any classical gates!

The Toffoli gate alone is a universal set for classical computation.



XOR

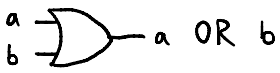
$00 \to 0$

$01 \to 1$

$10 \to 1$

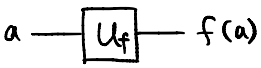
$11 \to 0$

HW7-1 Using Toffoli gates, simulate the following.



(hint) You need multiple Toffoli gates.

quantum parallelism

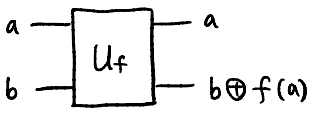


To be reversible, inverse function $f^{-1}(x)$ should exist!

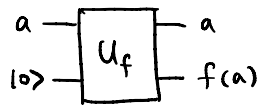
two cases: $\begin{cases} f(0) = 0, & f(1) = 1 \\ f(0) = 1, & f(1) = 0 \end{cases}$

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{U_f} \alpha|f(0)\rangle + \beta|f(1)\rangle$$

what if $f(x)$ is non-invertible?



reversible!

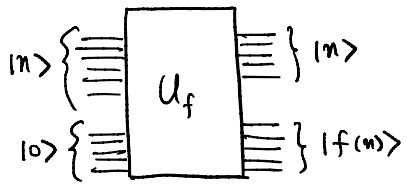


$$|a\rangle|0\rangle \to |a\rangle|f(a)\rangle$$

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle \xrightarrow{U_f} \alpha|0\rangle|f(0)\rangle + \beta|1\rangle|f(1)\rangle$$

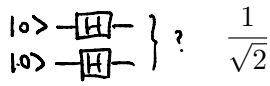
large numbers?

$0 = 0000_2,\ 1 = 0001_2,\ 2 = 0010_2,\ 3 = 0011_2,\ \cdots$

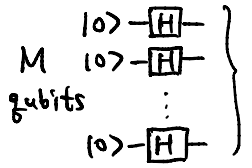


$$(c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + \ldots)|0\rangle \xrightarrow{U_f} \sum_n c_n|n\rangle|f(n)\rangle$$

how to make $\frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \cdots + |N-1\rangle)$?



$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$\qquad\qquad 0 \qquad\quad 1 \qquad\quad 2 \qquad\quad 3$$



$$\left(\frac{1}{\sqrt{2}}\right)^M (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\cdots(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^M}}\left(|0\rangle + |1\rangle + |2\rangle + \cdots + |2^M - 1\rangle\right)$$

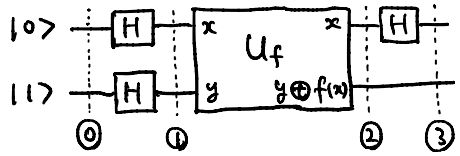
💬 However, measurement destroys the state!

Deutsch's algorithm

objective one-bit function $f(x) \in \{0, 1\}$

determine whether $f(0) = f(1)$ or $f(0) \neq f(1)$

classically, you have to evaluate $f(x)$ twice!



⓪ $|0\rangle|1\rangle$

① $(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |00\rangle - |01\rangle + |10\rangle - |11\rangle$ (unnormalized)

② $|0\rangle|f(0)\rangle - |0\rangle|f(0) \oplus 1\rangle + |1\rangle|f(1)\rangle - |1\rangle|f(1) \oplus 1\rangle$

if $f(0) = f(1)$: $(|0\rangle + |1\rangle)|f(0)\rangle - (|0\rangle + |1\rangle)|f(0) \oplus 1\rangle$

if $f(0) \neq f(1)$: $(|0\rangle - |1\rangle)|f(0)\rangle - (|0\rangle - |1\rangle)|f(0) \oplus 1\rangle$

③ if $f(0) = f(1)$: $|0\rangle(|f(0)\rangle - |f(0) \oplus 1\rangle)$

if $f(0) \neq f(1)$: $|1\rangle(|f(0)\rangle - |f(0) \oplus 1\rangle)$

You can find the answer by only one evaluation of $f(x)$!

HW7-2 Deutsch's algorithm

(a) For $f(0) = 1$ and $f(1) = 1$, draw the quantum circuit of U_f.

(b) For $f(0) = 1$ and $f(1) = 0$, draw the quantum circuit of U_f.

Deutsch-Jozsa algorithm

$f(x) \in \{0,1\}$ $\quad 0 \le x \le 2^n - 1$ (n-bit input)

$f(x)$ is either constant or balanced.

• constant $f(x)$: $f(0) = f(1) = \cdots = f(2^n - 1)$

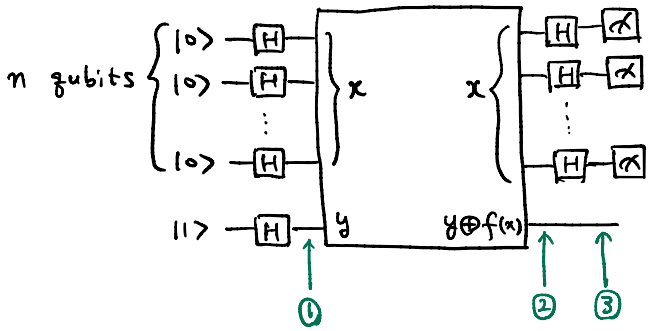
• balanced $f(x)$: $f(x) = 0$ for half of x's

$f(x) = 1$ for the other half

classically: in the best case, $f(x)$ is calculated twice.

in the worst case, $f(x)$ is calculated $2^n/2 + 1$ times.

DJ algorithm: $f(x)$ is calculated only once!



①: $(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\cdots(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$ (unnormalized)

$$= \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle)$$

②: $\sum_x |x\rangle(|f(x)\rangle - |f(x)\oplus 1\rangle)$

$f(x) = 0 \to |0\rangle - |1\rangle$

$f(x) = 1 \to |1\rangle - |0\rangle = -(|0\rangle - |1\rangle)$

$\Big\} (-1)^{f(x)}(|0\rangle - |1\rangle)$

$$= \sum_x (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle)$$

case 1 $f(x)$ is constant.

$f(x) = 0 \to \sum_x |x\rangle(|0\rangle - |1\rangle)$

$f(x) = 1 \to -\sum_x |x\rangle(|0\rangle - |1\rangle)$

③: $|0\rangle|0\rangle \ldots |0\rangle(|0\rangle - |1\rangle) \to$ You measure 000···0.

case 2 $f(x)$ is balanced.

$\sum_x (-1)^{f(x)} |x_1 x_2 \ldots x_n\rangle(|0\rangle - |1\rangle)$ $\qquad |x_1\rangle \xrightarrow{H} |0\rangle + (-1)^{x_1}|1\rangle = \sum_{z_1=0}^{1} (-1)^{x_1 z_1} |z_1\rangle$

③: $\sum_x \sum_z (-1)^{f(x)+x_1z_1+x_2z_2+\cdots+x_nz_n} |z_1 z_2 \ldots z_n\rangle(|0\rangle - |1\rangle)$

$$= \sum_x \cancel{(-1)^{f(x)} |0\rangle(|0\rangle - |1\rangle)} + \sum_x \sum_{z\neq 0} (-1)^{f(x)+x_1z_1+\cdots+x_nz_n} |z\rangle(|0\rangle - |1\rangle)$$

You never measure 000···0.

⇒ If you measure 000···0, $f(x)$ is constant. Otherwise, $f(x)$ is balanced.