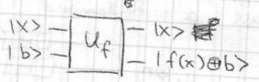
Deutsch's algorithm [82]:

$U_f |x\rangle|b\rangle = |x\rangle|f(x)\oplus b\rangle$

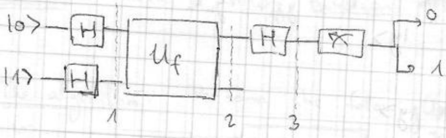


Input: given: $f: \{0,1\} \to \{0,1\}$

Output: 0 - if f is constant, 1 - if f isn't constant.

How many queries to f (U_f)?

-Classically: 2 queries, $f(0)$, $f(1)$.



→ 0 if f is const.

→ 1 if f isn't const.

state 1: $\frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) = \frac{1}{2}(|00\rangle+|10\rangle-|01\rangle-|11\rangle)$

state 2: $\frac{1}{2}(|0f(0)\rangle+|1f(1)\rangle-|0(f(0)\oplus 1)\rangle-|1(f(0)\oplus 1)\rangle) =$

$= \frac{1}{2}\cdot(|0\rangle\cdot(|f(0)\rangle-|f(0)\oplus 1\rangle)+|1\rangle\cdot(|f(1)\rangle-|f(1)\oplus 1\rangle)) =$

if $f(0)=0$: $|0\rangle-|1\rangle$; if $f(0)=1$: $-(|0\rangle-|1\rangle)$ $\Big\} = (-1)^{f(0)}\cdot(|0\rangle-|1\rangle)$

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

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

state 3: $\frac{1}{2}\cdot((-1)^{f(0)}\cdot(|0\rangle+|1\rangle)+(-1)^{f(1)}\cdot(|0\rangle-|1\rangle))\otimes\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) =$

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

- If f is constant $(-1)^{f(0)}-(-1)^{f(1)}=0$, so we measure 0 w.p 100%
- If f isn't constant $(-1)^{f(0)}+(-1)^{f(1)}=0$, so we measure 1 w.p 100%

Deutsch - Jozsa algorithm

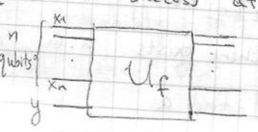
Problem: Given $f: \{0,1\}^n \to \{0,1\}$, such that either f is constant or f is balanced (50% get 0, 50% get 1).
We need do decide if f is constant or balanced.

Classically: - We need to check f on at least $2^{n-1}+1$ different input.

- Randomized algorithm: for an error probability of ε, we need $O(\log(\frac{1}{\varepsilon}))$ inputs.

Quantum: 100% success after calling U_f once!

our black box



$U_f|x_1\ldots x_n\rangle|y\rangle = |x_1\ldots x_n\rangle|f(x_1\ldots x_n)\oplus y\rangle$

We will use a Hadamard gate for n qubits:

$H^{\otimes n}$

$$H^{\otimes n} \underbrace{|x\rangle}_{|x_1,\dots,x_n\rangle} = (H|x_1\rangle) \otimes \dots \otimes (H|x_n\rangle)$$

For $|x_i\rangle = |0\rangle$ or $|1\rangle$: $H|x_i\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_i} \cdot |1\rangle\right)$

So the Hadamard transformation for n qubits:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{y \cdot x \to y_1x_1 + \dots + y_nx_n} |y\rangle$$

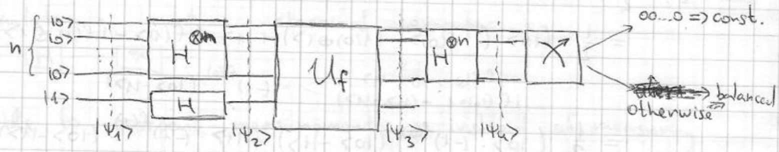
$$\Downarrow$$

$$H^{\otimes n}|00\dots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} |y\rangle$$

Also, notice that (similar to Deutch's algorithm): $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

for $x = 0$ or 1.

The algorithm:



$|\psi_1\rangle = |00\dots0\rangle|1\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|-\rangle$

$|\psi_3\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)}|x\rangle\right)|-\rangle$ (and we discard the $|-\rangle$)

If f is constant: $|\psi_4\rangle = H^{\otimes n}|\psi_3\rangle = H^{\otimes n} \cdot \left(\frac{(-1)^s}{\sqrt{2^n}} \sum_x |x\rangle\right) = |0\dots0\rangle \cdot (-1)^s \to$ We measure $00\dots0$

Because $H^{\otimes n} \cdot H^{\otimes n} = \mathbb{1}$

If f is balanced:

$|\psi_4\rangle = H^{\otimes n}|\psi_3\rangle = H^{\otimes n} \cdot \left(\frac{1}{\sqrt{2^n}} \cdot \sum_x (-1)^{f(x)} \cdot |x\rangle\right) =$ (formula we showed earlier for $H^{\otimes n}|x\rangle$)

$= \frac{1}{2^n} \cdot \sum_x (-1)^{f(x) + x \cdot y} \cdot |y\rangle$.

The coeffitient of $|00\dots0\rangle$ is $\frac{1}{2^n} \sum_x (-1)^{f(x)} = 0 \to$ because f is balanced.

Hence, the probability of measuring $00\dots0$ is 0.

Simon's algorithm - Period finding over $\mathbb{Z}_2^n$ [94]

Problem: Given $f: \{0,1\}^n \to \{0,1\}^n$. We know that there exists $a = (a_1, \dots, a_n) \neq 0$ such that $\forall x, y$ $f(x) = f(y) \iff y = x \oplus a$. Goal: find a.

$G = \mathbb{Z}_2^n$, $\{0, a\} = H \triangleleft G$. We divide G into cosets of G/H ($\{x, x \oplus a\}$)

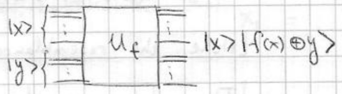
<u>Classically</u>: (1) Choose $x, y \in \{0,1\}^n$ randomly.

(2) Check if $f(x) = f(y)$. If yes: $a = x \oplus y$

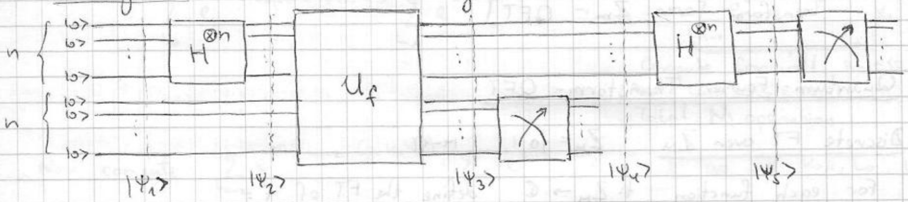
If no: return to (1).

Total time is exponential.

<u>Quantum</u>: Given a unitary function describing f:



<u>The algorithm</u>: Perform the following $O(n)$ times:



$|\psi_1\rangle = |00\ldots0\rangle \otimes |00\ldots0\rangle$

$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |00\ldots0\rangle$

$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$. We have 2^{n-1} possible values for $f(x)$. So measuring the 2^{nd} vector we collapse into one of the cosets.

$|\psi_4\rangle = \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus a\rangle)$ – If we measure now, the result will either be $|x\rangle$ or $|x \oplus a\rangle$, giving no information about a.

$$|\psi_5\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2^n}} \sum_y \left((-1)^{x \cdot y} |y\rangle + (-1)^{(x \oplus a) \cdot y} \cdot |y\rangle \right) = \frac{1}{\sqrt{2^{n+1}}} \sum_y (-1)^{xy} \underbrace{\left(1 + (-1)^{a \cdot y}\right)}_{\text{non-zero} \Leftrightarrow a \cdot y = 0 \Leftrightarrow a \perp y} \cdot |y\rangle =$$

$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{y : y \perp a} (-1)^{xy} |y\rangle$$

Measuring gives us a vector $\vec{y}_1 \perp \vec{a}$. ~~After~~ After $n-1$ runs we have n vectors $y_1, \ldots, y_{n-1}$, all perpendicular to $\vec{a}$. We get a linear system of equations $\vec{y}_i \cdot \vec{a} = 0$. ~~We need~~ To get a unique solution, we need $y_1, \ldots, y_{n-1}$ to be linearly independent.

– If we have $\{\vec{y}_1, \ldots, \vec{y}_k\}$ ~~then~~ ~~poss~~ and $\vec{y} \perp \vec{a}$ is a random vector, then with probability $\geq \frac{1}{2}$, $\vec{y} \notin \mathrm{span}\{\vec{y}_1, \ldots, \vec{y}_k\}$. So we can get $n-1$ such vectors after $O(n)$ runs.