CSCE 785
10/12/2023

Deutsch-Jozsa problem
Simon's problem

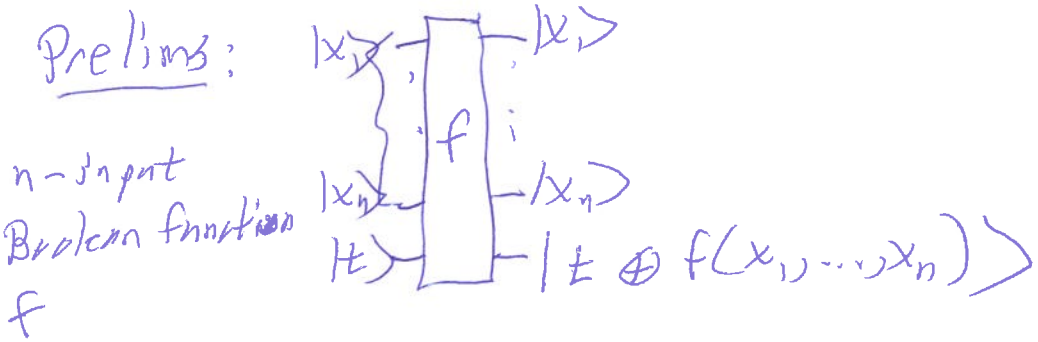
D-J problem: Given a Boolean function $f:\{0,1\}^n \to \{0,1\}$ can make queries to f.

Promise: f is either constant or balanced

$$|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$$

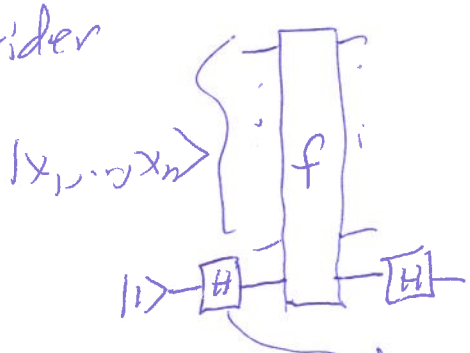
Output: Determine which (constant or balanced)

Prelims:



Notes: U_f for f

Consider



$$|x_1 \cdots x_n\rangle \otimes |1\rangle \xrightarrow{H_{n+1}} \frac{1}{\sqrt{2}}\left(|\vec{x}\rangle \otimes (|0\rangle - |1\rangle)\right)$$

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

$$\xrightarrow{f} \frac{1}{\sqrt{2}}\left(|\vec{x}, f(\vec{x})\rangle - |\vec{x}, \overline{f(\vec{x})}\rangle\right)$$

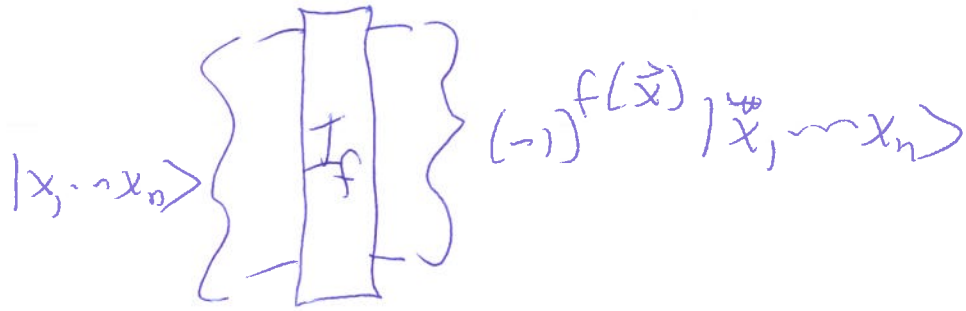
$(\oplus 0)$

$$\xrightarrow{H_{n+1}} \frac{1}{2}\left(|\vec{x}\rangle \otimes \left(|0\rangle + (-1)^{f(\vec{x})}|1\rangle\right) - |\vec{x}\rangle\left(|0\rangle + (-1)^{\overline{f(\vec{x})}}|1\rangle\right)\right)$$

$$= \frac{1}{2}|\vec{x}\rangle \otimes \left((-1)^{f(\vec{x})} - (-1)^{\overline{f(\vec{x})}}\right)|1\rangle$$

$$= \frac{1}{2}|\vec{x}\rangle \otimes \left((-1)^{f(\vec{x})} + (-1)^{f(\vec{x})}\right)|1\rangle$$

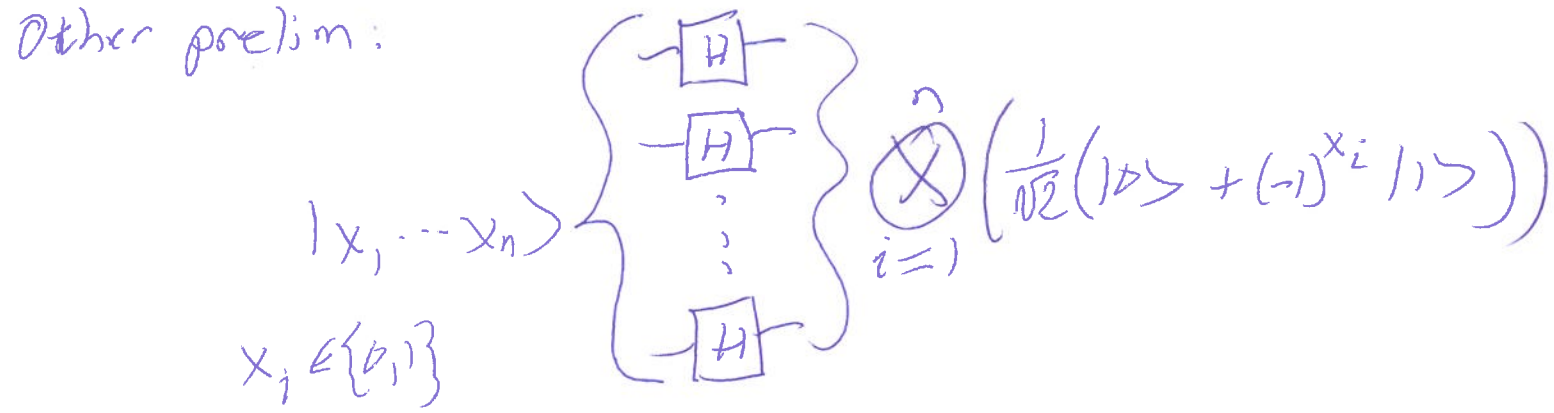
$$= (-1)^{f(\vec{x})}|\vec{x}, 1\rangle$$



"Phase Inversion by f"

Use I_f gate instead of f (a bit cleaner arguments)

Other prelim:

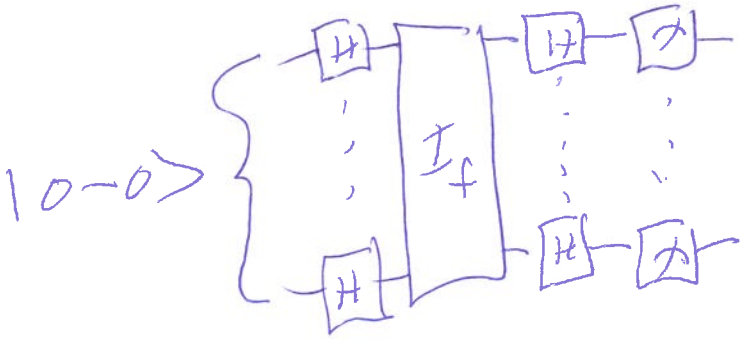


$$= \frac{1}{2^{n/2}} \sum_{\vec{y}=y_1 \cdots y_n \in \{0,1\}^n} (-1)^{x_1y_1 + x_2y_2 + \cdots + x_ny_n}|\vec{y}\rangle = \frac{1}{2^{n/2}} \sum_{\vec{y}} (-1)^{\vec{x}\cdot\vec{y}}|\vec{y}\rangle$$

Back to D-J problem: f is either const. or balanced.

Classically need ~~$2^{n/2}$~~ $2^{n-1}+1$ many queries to be 100% sure of the answer.

Quantum algo that queries f once (one I_f gate) (in superposition):



Step through the circuit

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

$$\xrightarrow{I_f} \frac{1}{2^{n/2}}\sum_x (-1)^{f(x)}|x\rangle$$

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

$$= \frac{1}{2^n}\sum_{x,y}\left((-1)^{f(x)+x\cdot y}\right)|y\rangle$$

Consider $y=0$: what is the coeff on $|0\rangle$?

$$= \frac{1}{2^n}\left(\sum_x (-1)^{f(x)}\right)|0^n\rangle + \frac{1}{2^n}\sum_{y\neq 0}\sum_x (-1)^{f(x)+x\cdot y}|y\rangle$$

f is balanced; $\sum_x (-1)^{f(x)} = 0$ so Prob of seeing 0^n after measuring is 0

f constant: $\sum_x (-1)^{f(x)} = \pm 2^n$

$$\frac{1}{2^n}\sum_x (-1)^{f(x)} = \pm 1$$

$$\left|\frac{1}{2^n}\sum_x (-1)^{f(x)}\right|^2 = 1$$

∴ Final state is $\pm|0^n\rangle$

∴ Prob of 0^n is 1.

After measurement, if 0^n is seen then conclude that f is constant; else conclude f is balanced.

Simon's Problem

Given $f : \{0,1\}^n \to \{0,1\}^m$ for some $m \geq n$ as a black box.

Promise: There exists an $s \in \{0,1\}^n$ such that for all distinct $x, y \in \{0,1\}^n$, $f(x) = f(y)$ iff $x \oplus y = s$ ($y = x \oplus s$)

($\oplus$: bitwise XOR)

Goal: find s. (s is unique given the promise:

$f(x) = f(b)$ iff $x = s$

s is the unique x such that $f(x) = f(b)$).

Notice: If $s = 0$ then f is 1-1.

If $s \neq 0$, then f is 2-1. $\forall x \; f(x) = f(x \oplus s)$.

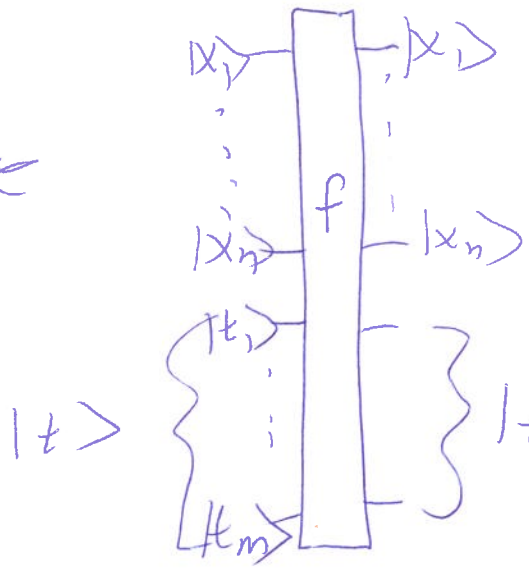
Classically: Deterministic algo needs $2^{n-1} + 1$ queries to find s with certainty.

A randomized algo needs $\approx 2^{n/2}$ queries to f to find s with high prob.

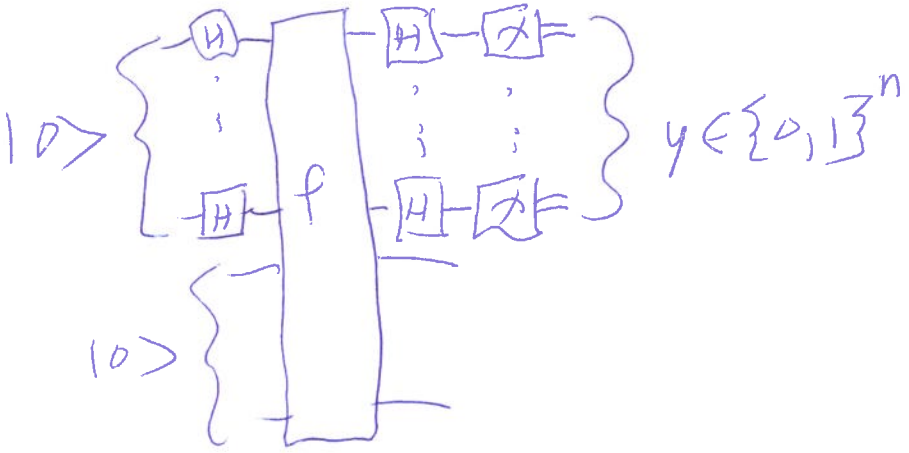
Quantum algo finds with high prob using about $2n$ many queries.

~~Circuit:~~

f-gate



Circuit:



Claim (for next time): Get a uniformly randomly distributed $y \in \{0,1\}^n$ such that $y \cdot s = 0 \mod 2$