9/28/10 QIC 710 Lecture 5 Early quantum query algorithms: Deutsch & Deutsch-Josza

Query model

Input: Black-box access to a function f.

Goal: Solve a problem with as few calls to f as possible.

Example: Search

Given $f:\{0,1\}^n \to \{0,1\}$, find x so $f(x)=1$

$\Theta(n)$ queries are needed (classically)

Deutsch's problem

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

Goal: Find $f(0) \oplus f(1) = \begin{cases} 0 & \text{if } f \text{ is constant (0 or 1)} \\ 1 & \text{if } f \text{ is balanced} \end{cases}$

Classically complexity = 2 queries

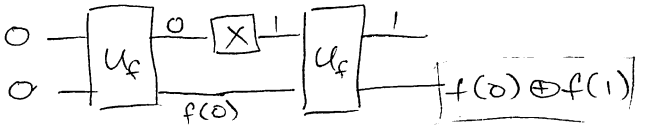
Quantum complexity = 1 query

Def: U_f $\quad a \to a$, $b \to b \oplus f(x)$

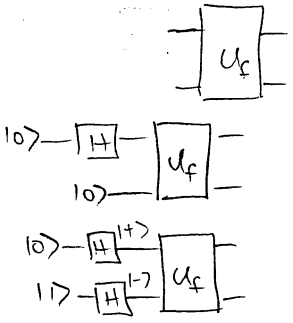
$= \sum_{a,b \in \{0,1\}} |a, b \oplus f(x)\rangle\langle a,b|$ a permutation in the computational basis

$\therefore$ unitary

Classical algorithm:



Quantum algorithm, making one call to U_f:



$\sum_{a,b} \alpha_{ab} |a,b\rangle \to \sum_{ab} \alpha_{ab} |a, b \oplus f(x)\rangle$

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

$|+\rangle \otimes |-\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$

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

$\to \frac{1}{2}\left[|0\rangle \otimes (|f(0)\rangle - |\overline{f(0)}\rangle) + |1\rangle \otimes (|f(1)\rangle - |\overline{f(1)}\rangle)\right]$

$= \begin{cases} |0\rangle - |1\rangle & \text{if } f(0)=0 \\ |1\rangle - |0\rangle & \text{if } f(0)=1 \end{cases}$

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

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

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

Deutsch's algorithm

$|a\rangle \otimes |-\rangle$ an eigenvector of U_f with eigenvalue $(-1)^{f(a)}$.

Is this interesting? "phase kickback" trick

- no, minor savings
- no, how is U_f implemented?

classically, just a simple circuit

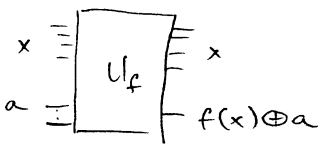
$f(0)=f(1)=0$ $\quad f(0)=f(1)=1$ $\quad f(0)=0, f(1)=1$ $\quad f(0)=1, f(1)=0$

quantumly, more hardware required

Query model

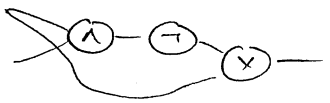
Classically can apply f at cost 1

Quantumly can apply U_f at cost 1

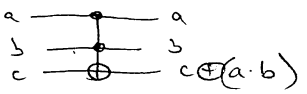


$$\left(\sum_x \alpha_x |x\rangle\right) \otimes |0^m\rangle \xrightarrow{U_x} \sum_x \alpha_x |x\rangle \otimes |f(x)\rangle.$$

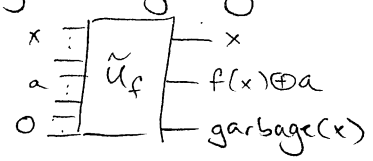
Eg. f given by a circuit of $\wedge, \neg$ gates of size S



same circuit can be implemented using reversible gates

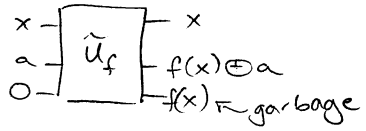


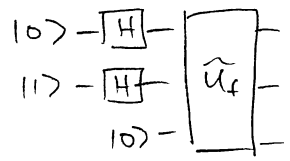
but they leave garbage!



Garbage breaks Deutsch's algorithm & most quantum query algorithms

eg:



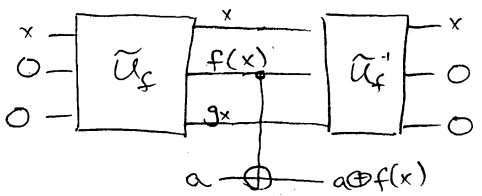


$$\sum_x (-1)^{f(x)} |x\rangle \otimes |-\rangle \otimes |f(x)\rangle$$

works for $f \equiv 0$ or $f \equiv 1$, but otherwise

	now	before
$f(x) = x$:	$\|0\rangle\otimes\|0\rangle - \|1\rangle\otimes\|1\rangle$	$\|0\rangle - \|1\rangle$
$H^{\otimes 1}$	$\|+\rangle\otimes\|0\rangle - \|-\rangle\otimes\|1\rangle$	$\longrightarrow \|+\rangle - \|-\rangle \propto \|1\rangle$

Solution: garbage clean-up



⇒ U_f can be implemented (with extra ancilla qubits) by a circuit of Toffoli gates of size $\leq 2s$.

lost factor of 2.

Deutsch-Jozsa algorithm. '92

Goal: Distinguish between constant and balanced functions

Given: $f : \{0,1\}^n \to \{0,1\}$ black-box

Promise: Either f is constant (0 or 1)

or f is balanced (0 on 2^{n-1} inputs, 1 on 2^{n-1} inputs)

Figure out which.

Query complexity:

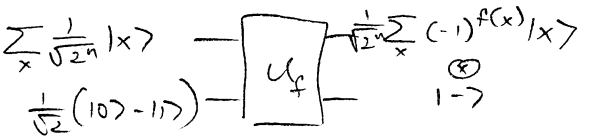
Classically must probe $\geq 2^{n-1}+1$ inputs for certainty

(probing k random inputs gives right answer w/prob. $1-\frac{1}{2^k}$)

Claim: Exact quantum query complexity is 1. ($\Rightarrow$ exp. separation)

Pf:

version 1 of the algorithm:



f constant

$$\pm \frac{1}{\sqrt{2^n}} \sum_x |x\rangle \otimes |-\rangle$$

f balanced

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \otimes |-\rangle$$

orthogonal? $\Rightarrow$ distinguishable in principle

Remark: Hadamard gate H and $H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$

$$H \to \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad H|x\rangle = \sum_{y=0}^{1} (-1)^{x \cdot y} |y\rangle / \sqrt{2}$$

$$H \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

Theorem: $H^{\otimes n}|x\rangle = \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$ where $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$

Proof:

$$\begin{aligned} H^{\otimes n}|x\rangle &= H^{\otimes n}|x_1 x_2 \cdots x_n\rangle \\ &= (H|x_1\rangle) \otimes (H|x_2\rangle) \otimes \cdots \otimes (H|x_n\rangle) \\ &= \frac{1}{\sqrt{2^n}} \left(\sum_{y_1=0}^{1} (-1)^{x_1 y_1} |y_1\rangle\right) \otimes \cdots \otimes \left(\sum_{y_n=0}^{1} (-1)^{x_n y_n} |y_n\rangle\right) \\ &= \frac{1}{\sqrt{2^n}} \sum_y (-1)^{x_1 y_1 + \cdots + x_n y_n} |y_1 \cdots y_n\rangle \end{aligned}$$

□

Corollary: $H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$ uniform superposition over all inputs

Corollary: $H^{\otimes n} \sum_x (-1)^{f(x)} |x\rangle = \sum_{xy} (-1)^{f(x)+x\cdot y} |y\rangle$

case $f(x)$ constant: $H^{\otimes n} \sum_x |x\rangle = |0^n\rangle$

case $f(x)$ balanced:

$$\mathbb{P}[\text{measure } 0^n] = \left| \langle 0^n | \frac{1}{2^n} \sum_{xy} (-1)^{f(x)+x\cdot y} |y\rangle \right|^2$$

$$= \frac{1}{2^{2n}} \left| \sum_x (-1)^{f(x)} \right|^2 = 0.$$

Next time: Bernstein-Vazirani & Simon's algorithms:
superpolynomial & exponential gaps in bounded-error model