Make-up classes: W 1-2:15
M 2-3:15

$\boxed{\text{Ph 452}}$ Lecture 8

1(2) Quick Review

Simon's Problem

O, Ω, Θ

Types of query algs

Corrections:

could be less space or polytime.

Uniform: Each $C_k = C(k)$ has a finite description
(usu. say is generatable by a Turing Machine.)

Reference: Kitaev, Vyali, Shen

1-sided err: $(R_1^p(g))$: has error $\begin{cases} 0 & g(x)=0 \\ 0 \le p \le 1 & g(x)=1 \end{cases}$

2-sided err: $(R_2^p(g))$: has error $0 \le p \le 1/2$

Usually use $R_2(g) := R_2^{1/3}(g)$.

Why? Majority voting $\rightarrow$ "probability amplification"

$2^k = (1+1)^k = \sum \binom{k}{j}$

k trials: $$p_{err} \le \sum_{\substack{S \subseteq \{1,\dots,k\} \\ |S| \le k/2}} (1-p)^{|S|} p^{k-|S|}$$

$\binom{k}{k/2}$ Stirling formula

$$= \left(\sqrt{p(1-p)}\right)^k \sum \left(\frac{p}{1-p}\right)^{k/2-|S|}$$

But $p < 1/2 \Rightarrow 2p < 1$
$p + p < 1$
$p < 1-p$
$\frac{p}{1-p} < 1$

$$p_{err} < \left(\sqrt{p(1-p)}\right)^k \binom{k}{k/2}$$
$$< \left(\sqrt{p(1-p)}\right)^k 2^k$$
$$= \lambda^k, \quad \lambda < 1.$$

constant # trials $\Rightarrow$ exponential error suppression

Ph 452 Lecture 8

General results

$$R_2(f) \le R_1(f) \le R_0(f) \le D(f) \le N$$

$$D(f) \le (R_0(f))^2$$

NAND prob. →

$$D(f) = \Theta((R_2(f))^3) = \Theta((R_1(f))^2)$$

[$D(f) \le 2 R_2(f)^3$ [Nisan 1989]
Biggest gap known: (NAND)
$D(f) = \Theta(R_2(f)^{1.3\ldots})$]

$$Q_2(f) \le R_2(f)$$

$$Q_2^{(\epsilon)} \le Q_\epsilon(f) \le D(f)$$

$$D(f) = O((Q_\epsilon(f))^3) = O((Q_2(f))^6) \qquad [D \le 16 Q_\epsilon^3]$$

<u>Example:</u> Grover / N-bit OR:

$$D = N \qquad Q_\epsilon = \Theta(N)$$

$$R_2^p = \left(\frac{1-2p}{1-\epsilon}\right) N \qquad Q_2 = \Theta(\sqrt{N})$$

Do Deutsch's Problem First.

<u>Physics reason to care</u> about "Monte Carlo" complexity

Any <u>finite</u> set of pgates/angates can at best approximate all possible stochastic/unitary transformations!

("Analog" computation allows a continuum of gates.)

Even though gate complexity only changes for quantum, realistically physicists feel that algorithm is only an approximation

~~Error is $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$,~~

~~$\||\psi\rangle\| := \sqrt{\langle\psi|\psi\rangle}$~~

~~See Box 4.1, Nielsen + Chuang for motivation of $E(U,V)$.~~

$\boxed{\text{Ph 452}}$ ~~Lecture 5~~ Lecture 8

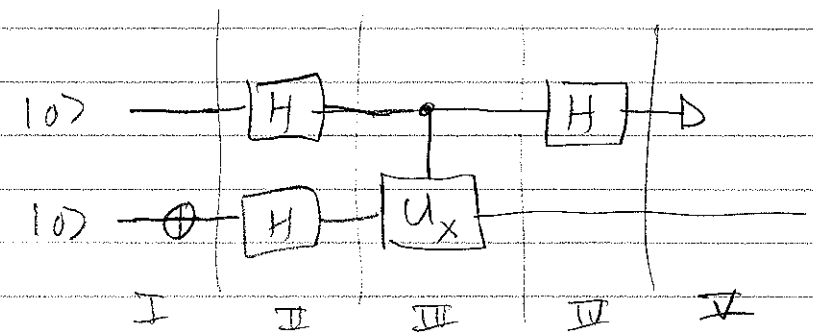
Deutsch's Problem

<u>Example:</u> ~~$X \in \mathbb{B}^2$~~, $g(x) = X_0 \oplus X_1$

$D(g) = 2$, $Q_E(g) = 1$!

~~B(s) case: Same as worst case → always need 2 queries!~~

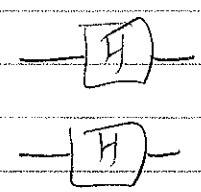
<u>Deutsch's 1-query quantum algorithm:</u>



(I)

$\oplus$: NOT gate : $|00\rangle \to |01\rangle$

(II)



$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ "Hadamard gate" (HW)

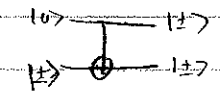
$H|0\rangle = |+\rangle$

$H|1\rangle = |-\rangle$

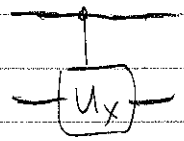
$|01\rangle \to |+-\rangle$

In Lecture 5, Got this far.

Aside: Could show how info propagates "backwards" through a controlled quantum gate



$\boxed{\text{Ph 452}}$ ~~Lecture 5~~ Lecture 8

III 

$$|j\,k\rangle \mapsto |j, k \oplus x_j\rangle$$

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

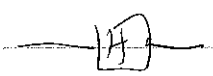
$$\to \tfrac{1}{2}\Big[|0\rangle\underbrace{(|x_0\rangle - |x_0 \oplus 1\rangle)} + |1\rangle\underbrace{(|x_1\rangle - |x_1 \oplus 1\rangle)}\Big]$$

$$= \begin{cases} |0\rangle - |1\rangle & x_0 = 0 \\ -(|0\rangle - |1\rangle) & x_0 = 1 \end{cases} \qquad = \begin{cases} |0\rangle - |1\rangle & x_1 = 0 \\ -(|0\rangle - |1\rangle) & x_1 = 1 \end{cases}$$

$$= \tfrac{1}{\sqrt{2}}\left[(-1)^{x_0}|0-\rangle + (-1)^{x_1}|1-\rangle\right]$$

("absorb a $\frac{1}{\sqrt{2}}$ into def. of $|-\rangle$")

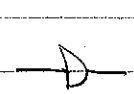
$$= \tfrac{1}{\sqrt{2}}\left[(-1)^{x_0}|0\rangle + (-1)^{x_1}|1\rangle\right] \otimes |-\rangle$$

IV 

$$\to \tfrac{1}{2}\left[(-1)^{x_0}(|0\rangle + |1\rangle) + (-1)^{x_1}(|0\rangle - |1\rangle)\right] \otimes |-\rangle$$

$$= \tfrac{1}{2}\left[\left((-1)^{x_0} + (-1)^{x_1}\right)|0\rangle + \left((-1)^{x_0} - (-1)^{x_1}\right)|1\rangle\right] \otimes |-\rangle$$

$$= \begin{cases} \pm|0-\rangle & \text{if } x_0 = x_1 \quad (x_0 \oplus x_1 = 0) \\ \pm|1-\rangle & \text{if } x_0 \neq x_1 \quad (x_0 \oplus x_1 = 1) \end{cases}$$

V 

$$\Pi_0 = |0\rangle\langle 0| \otimes I \qquad \text{prob}(0) =$$
$$\Pi_1 = |1\rangle\langle 1| \otimes I$$

$$\text{prob}(0 \mid x_0 \oplus x_1 = 0) = (\pm\langle 0-|)(|0\rangle\langle 0| \otimes I)(\pm|0-\rangle)$$
$$= \langle 0|0\rangle\langle 0|0\rangle \otimes \langle -|-\rangle = 1$$

in PS, similar tracing through Simon's algorithm

$$\text{prob}(1 \mid x_0 \oplus x_1 = 1) = 1 \quad \text{similarly.}$$