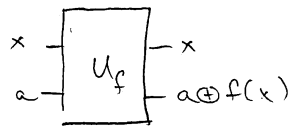
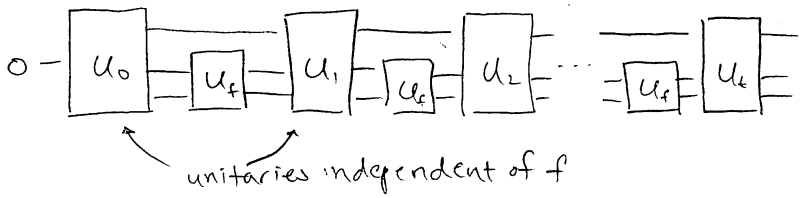
9/30/10 QIC 710 Lecture 6

Last time:

Quantum query model



query complexity = # of times U_f needs to be applied



Example:

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

Note: For applications, the black-box f can be instantiated with a particular efficiently computable function.

eg. $f(x) = \begin{cases} 1 & \text{if } x \text{ is the binary representation of a proof for problem 3} \\ 0 & \text{otherwise} \end{cases}$

- a properly written proof can be efficiently verified, so this is a search over all possible proofs
- ultimate difficulty depends on the instance

Example:

Parity: For $f: \{1,2,\dots,n\} \to \{0,1\}$,

find $f(1) + f(2) + \cdots + f(n) \mod 2$

classical query complexity: n

quantum query complexity: $\lceil \frac{n}{2} \rceil$ Why?

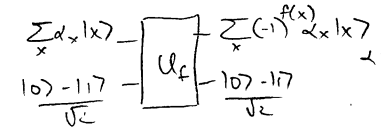
$|1\rangle + |2\rangle \mapsto (-1)^{f(1)}\left(|1\rangle + (-1)^{f(1)+f(2)}|2\rangle\right)$, etc.

Goals in quantum algorithms research:

1. Solve useful problems quickly
2. Show large separations in the power of classical and quantum computers.

Last time:

1. $H^{\otimes n}|a\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{x \cdot a} |x\rangle$
2. "Phase kickback"

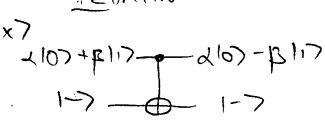


in general: $U|\psi\rangle = \lambda|\psi\rangle$

$|0\rangle + |1\rangle \mapsto |0\rangle + \lambda|1\rangle$

$|\psi\rangle$ — U — $|\psi\rangle$

#2 on hw:



Recursive Fourier Sampling problem [Bernstein & Vazirani]

Base case: Given $f: \{0,1\}^n \to \{0,1\}$

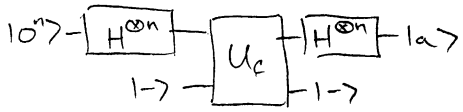
$$\exists\ a : f(x) = a \cdot x = a_1 x_1 + \cdots + a_n x_n \bmod 2$$

Find a.

classical complexity: n queries

quantum complexity: 1 query

want to amplify this separation

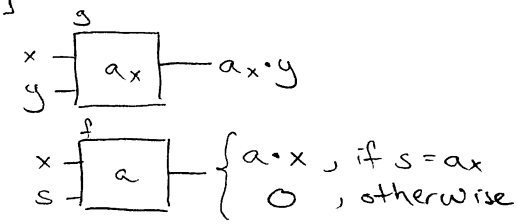


[Hallgren & Harrow, 0805.0007]

2^{nd} level: 2 oracles:

secrets a, $\{a_x : x \in \{0,1\}^n\}$

Find a.



Idea: 2^{nd} oracle is useless unless it is "unlocked" by the secret a_x.

3^{rd} level: 3 oracles: $f(x,s) = \begin{cases} a \cdot x, & \text{if } s = a_x \\ 0, & \text{o.w.} \end{cases}$

$g(x,y,s) = \begin{cases} a_x \cdot y, & \text{if } s = a_{xy} \\ 0, & \text{o.w.} \end{cases}$

$h(x,y,z) = a_{xy} \cdot z$

Quantum algorithm (for 2-level case)

$$\sum_{xy} |xy\rangle \xrightarrow[\text{(one call to } g)]{FS} \sum_x |x, a_x\rangle \xrightarrow[\text{with phase kickback}]{\text{one call to } f} \sum_x (-1)^{a \cdot x} |x, a_x\rangle \xrightarrow[\text{to erase } a_x)]{FS^{-1}, \text{ one call to } g} \sum_x (-1)^{a \cdot x} |x\rangle \xrightarrow{H^{\otimes n}} |a\rangle$$

with $\log n$ levels, halving the length each time, i.e. $x \in \{0,1\}^n$, $y \in \{0,1\}^{n/2}$, $z \in \{0,1\}^{n/4}$, ...

quantum: $T(n) = 2T(n/2) + O(n) = \Theta(n \log n)$

classical: $T(n) = nT(n/2) + O(n) = \Omega(n^{\log_2 n})$

classical lower bound...

[BV]'s construction: 2 levels: $f(x) = a \cdot x$ but can't access f directly!

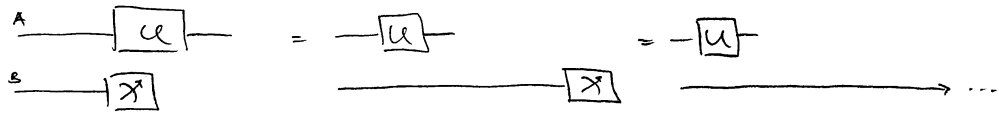
instead, can access $g(x,y) = a_x \cdot y$, and promised that $f(x) = h(a_x)$

Conjecture: RFS & Polynomial Hierarchy (PH).

See [Aaronson, 0910.4698, 1009.5104], [Fefferman & Umans 1007.0305].

Aside: Principle of deferred measurements (hw 2 #4)

$|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$



Example: How to generate randomness for a quantum circuit.

① $|0\rangle$ — H — $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

No good: 0 — H — H — 0

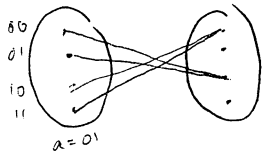
② $|0\rangle$ — H — H — $\frac{1}{\sqrt{2}}: |0\rangle + |1\rangle$ ✓
$\frac{1}{\sqrt{2}}: |0\rangle - |1\rangle$

$|0\rangle$ — ⊕ — M — $\frac{1}{\sqrt{2}}:|00\rangle$
$\frac{1}{\sqrt{2}}:|11\rangle$

③ $|0\rangle$ — H — H — ✓

$|0\rangle$ — ⊕

Simon's algorithm

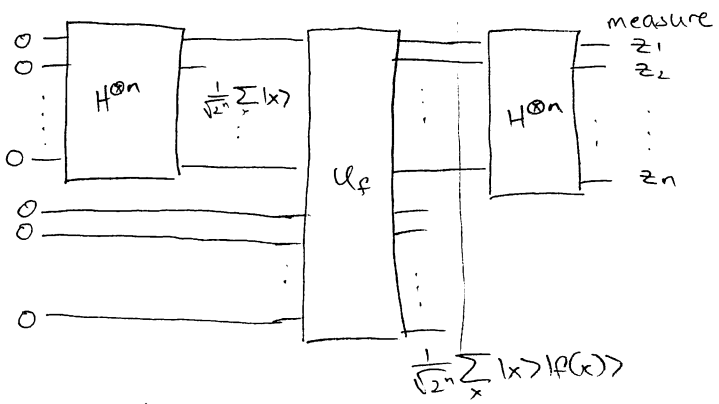


Given $f: \{0,1\}^n \to \{0,1\}^n$

promise: f is exactly 2-to-1, and

$\exists\ a$ s.t. $\forall x,\ f(x) = f(x \oplus a)$

Find a. "Hidden subgroup problem" "Fourier sampling"



Analysis:

1. By principle of deferred measurement, might as well measure 2nd register

   1st register $= \frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|x+a\rangle$ for a uniformly random x (unknown!)

2. $\longrightarrow \frac{1}{2^{\frac{n+1}{2}}} \sum_z (-1)^{x\cdot z}|z\rangle + (-1)^{(x+a)\cdot z}|z\rangle$

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_z \left[(-1)^{x\cdot z} + (-1)^{(x+a)\cdot z}\right]|z\rangle = \frac{1}{2^{\frac{n+1}{2}}} \sum_z (-1)^{x\cdot z}\left(1 + (-1)^{a\cdot z}\right)|z\rangle$$

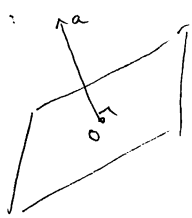
$\Rightarrow$ obtain uniformly random z s.t. $a \cdot z = 0$

Repeat $n-1$ times:

$$\left.\begin{aligned} z_{1,1}a_1 + \cdots + z_{1,n}a_n &= 0 \\ &\vdots \\ z_{n-1,1}a_1 + \cdots + z_{n-1,n}a_n &= 0 \end{aligned}\right\} \text{ - solve for } a_n$$

Claim: $\mathbb{P}[\text{equations have a unique, nonzero solution } a] \geq \frac{1}{4}$.

Proof:



$\mathbb{P}[n-1$ uniform samples from an $(n-1)$-D space over $\mathbb{F}_2$ are linearly independent$]$

$$= \left(1 - \frac{1}{2^{n-1}}\right)\left(1 - \frac{2}{2^{n-1}}\right)\left(1 - \frac{4}{2^{n-1}}\right)\cdots\left(1 - \frac{1}{2}\right) \geq 0.28 \ldots \quad \square$$

(Proof. By union bound, $\left(1 - \frac{1}{2^{n-1}}\right)\cdots\left(1 - \frac{2^{n-2}}{2^{n-1}}\right) \geq 1 - \frac{1}{4} - \frac{1}{8} - \cdots \geq \frac{1}{2}$.)

Classical complexity: $\Omega(2^{n/2})$

why? Intuitively, it must find a collision, two inputs x, y with $f(x) = f(y) \Rightarrow a = x \oplus y$.

Theorem: Any probabilistic algorithm making k queries succeeds with probability $\leq \frac{1}{2^n - \binom{k}{2} - 1} + P[\text{collision}]$

$(\Rightarrow k \approx 2^{n/2})$

Proof: Let f be a random function satisfying the promise.

If after k queries, $\nexists x, y$ with $f(x) = f(y)$

$\Rightarrow$ have eliminated exactly $\binom{k}{2}$ choices for a.

a could be anything else! $\square$

Shor's factoring algorithm:

1. Generalize the hidden subgroup problem from $\mathbb{Z}_2^n$ to $\mathbb{Z}_N$.
2. Instantiate f satisfying the promise.

(Regev et al. 2010)