Last time:

**Quantum query model**

\[ x \xrightarrow{U_f} x \xrightarrow{a \otimes f(x)} \]

query complexity = # of times \( U_f \) needs to be applied

Example:

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

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

\[ f(x) = \begin{cases} 1 & \text{if } x \text{ is the binary representation of a proof for problem } i \\ 0 & \text{otherwise} \end{cases} \]

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 \( f : \{1,2,\ldots,n\} \rightarrow \{0,1\} \),

\[ f(x) = \text{parity of } x \]

classical query complexity: \( n \)

quantum query complexity: \( \lceil \frac{\pi}{2} \rceil \)

Why?

\[ 1^n + 1^n \rightarrow (-1)^{s(x_1,x_2)}1^n + (-1)^{s(x_1,x_2)}1^n, \text{ etc.} \]

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. \( H^\otimes n |a> = \frac{1}{2^n} \sum_x (-1)^{x \cdot a} |x> \)

2. "Phase kickback" \[ \sum_x |x> \rightarrow \sum_x \frac{U_f |x>}{\langle x|U_f|x>}, \quad \text{for } x \neq 0,1^n \]

in general: \[ U_{1^n} = 1^n \]

\[ 1^n + 1^n \rightarrow 1^n + 1^n \]

4. MHW:
Recursive Fourier Sampling problem [Bernstein & Vazirani]

Base case: Given $f: [0,1]^{n} \rightarrow [0,1]^{n}$

$$\exists a : f(x) = a \cdot x = a_{1}x_{1} + \cdots + a_{n}x_{n} \mod 2$$

Find $a$.

classical complexity: $n$ queries
quantum complexity: 1 query
want to amplify this separation

[Hallgren & Harrow, 0805.0004]

2nd level: 2 oracles:

secrets $a_{j} \{a_{j} : x \in [0,1]^{n}, j \}$

Find $a$.

Idea: 2nd oracle is useless unless it is "unlocked" by
the secret $a_{j}$.

3rd level: 3 oracles:

$f(x,s) = 1_{s \neq a_{j}x}$

$g(x,y,s) = 1_{s \neq a_{j}y}$

$h(x,y,z) = 1_{z \neq a_{j}x \cdot y}$

Quantum algorithm (for 2-level case)

$$\sum_{x,y} f(x,y) \rightarrow \sum_{x} 1_{x', a_{j}x} \rightarrow \sum_{x} (-1)^{a_{j}x} 1_{x', a_{j}x} \rightarrow \sum_{x} (-1)^{a_{j}x} 1_{x} \rightarrow H_{[n]} \rightarrow a_{j}^{2}$$

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

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...

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

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

Conjecture: RES & Polynomial Hierarchy (PH)

See [Aaronson, 0910.4698, 1009.5104], [Fefferman & Umans 1007.0305]
Aside: Principle of deferred measurements (hw 2 #4)

\[ \Psi \in \mathcal{H}_4 \otimes \mathcal{H}_5 \quad \overset{A}{\rightarrow} \quad \Psi = \quad \overset{A}{\Psi} \quad \overset{B}{\rightarrow} \quad \Psi \]

Example: How to generate randomness for a quantum circuit.

1. \( 107 - \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)
   - No good: \( 0 - \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)

2. \( 107 - \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)
   - \( \frac{1}{2} : 107 + 117 \) \( \frac{1}{2} : 107 - 117 \)

3. \( 107 - \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)
   - True
Simon's algorithm

Given \( f : \{0,1\}^n \rightarrow \{0,1\}^n \)

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
\( \text{1st register} = \frac{1}{2^n} |x\rangle + \frac{1}{\sqrt{2}} |x + a\rangle \) for a uniformly random \( x \)

\( \sum z \) \( \frac{1}{2^{\frac{n^2}{2}} \cdot \mathbb{E}} \sum \mathbb{E} \left[ (-1)^{x \cdot z} + (-1)^{(x \oplus a) \cdot z} \right] \mathbb{E} \)

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

Repeat \( n - 1 \) times:
\( z_1, a_1 + \cdots + a_n = 0 \) \( \text{solve for } an \)
\( z_{n+1}, a_1 + \cdots + a_n = 0 \)

Claim: these equations have a unique, nonzero solution \( a \neq 0 \).

Proof:
\( a \cdot \mathbb{E} = \mathbb{E} \sum a \cdot z \in \{0,1\}^n \) uniform samples from an \( (n-1) \)-D space
\( (a, z) \) \( \text{over } \mathbb{F}_2 \) are linearly independent

\( = (1 - \frac{1}{2^n})(1 - \frac{2}{2^n})(1 - \frac{4}{2^n}) \cdots (1 - \frac{2^{n-1}}{2^n}) \geq 0.28 \). \( \square \)

(Proof: By union bound, \( (1 - \frac{1}{2^n}) \cdots (1 - \frac{2^{n-1}}{2^n}) \geq 1 - \frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} \).)
Classical complexity: $2^{n/2}$

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 $\leq \frac{1}{2^n - (\frac{k}{3}) - 1 + P[\text{collision}]}$ 

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

**Proof**: Let $f$ be a random function satisfying the promise. If after $k$ queries, $f(x, y)$ with $f(x) = f(y)$ 

$\Rightarrow$ have eliminated exactly $(\frac{k}{3})$ choices for $a$. 

$a$ could be anything else! \[ \square \]

Shor’s factoring algorithm:

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

(Regev et al. 2010)