Lecture 9

Oct 24, 2024

Today: Quantum speedups when structure exists.

The optimality of Grover's search was proven in the "query model". This is where we will be mostly working for the next few lectures. Two reasons.

① We can prove lower bounds "easily" in the query model.

② It is easier to construct oracles which have structure than find them "naturally".

Eventually, we will find one in factoring.

Bernstein-Vazirani's observation.

Let $f : \{0,1\}^n \to \{0,1\}$ be a function s.t.

there is a "secret" pattern. For some $s \in \{0,1\}^n$.

$$f(x) = s \cdot x \quad \leftarrow \text{inner product over } \mathbb{F}_2$$

i.e. f is a linear function for some slope s.

They showed there is a quantum algorithm for extracting s using 1 query (query in superposition)!

Classically, it takes n queries at least since each query learns 1 bit of s.

"Query e_j and learn bit $s_j \in \{0,1\}$.".

The q. algorithm:

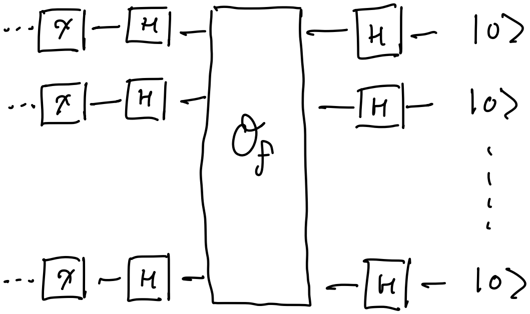
First note $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \sum_{\substack{x,y \\ \in \{0,1\}}} (-1)^{x \cdot y} |y\rangle\langle x|$.

So, $$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\substack{x_1 \cdots x_n \\ y_1 \cdots y_n}} (-1)^{x_1 y_1 + \cdots + x_n y_n} |y_1 \cdots y_n\rangle\langle x_1 \cdots x_n|$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x,y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle\langle x|.$$

This is the finite-dimensional Fourier Transform over $\mathbb{F}_2$.

Bernstein-Vazirani (1994):



$$H^{\otimes n} O_f H^{\otimes n} |0^n\rangle$$

$$= H^{\otimes n} O_f \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

$$= H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_x (-1)^{x \cdot s} |x\rangle$$

$$= \frac{1}{\sqrt{2^n}} \cdot \frac{1}{\sqrt{2^n}} \sum_y \sum_x (-1)^{x \cdot s + x \cdot y} |y\rangle$$

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

$$= \frac{1}{2^n} \Bigg(2^n |s\rangle + \sum_{y \neq s} \Big(\underbrace{\sum_x (-1)^{x \cdot \overset{y+s}{y'}}}_{0 \text{ due to interference.}} \Big) |y\rangle$$

$= |s\rangle$.

The information about s is being hidden in the Fourier basis. By rotating to the Fourier basis, we can access the information faster!

We can also convert this to a decision problem of whether a fn f is a linear fn or far from it.

This is a n vs. $\underline{1}$ query separation.

We can actually find a $\sqrt{2^n}$ vs $O(n)$ separation due to Daniel Simon 1994.

Simon's separation and a key component of Shor's algorithm are special cases of a general phenomenon called Abelian Hidden Subgroup Problem which we will explore today.

Simon's problem:

Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a fn s.t. $\forall\, x, y \in \{0,1\}^n$ with $x \neq y$, $f(x) = f(y)$ iff $x = y \oplus s$ for some hidden secret $s \neq 0^n$. Find s. ← "hidden shift"

Classical lower bound:

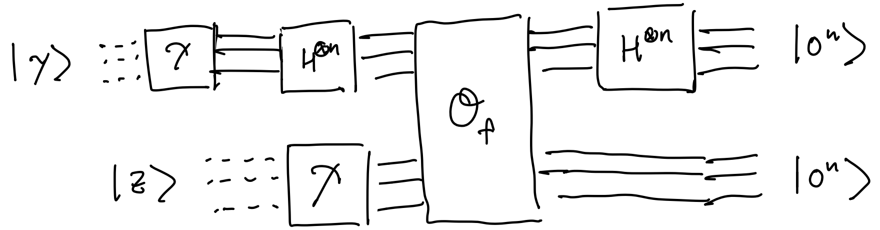
Consider the problem of distinguishing such functions f from permutations $\pi : \{0,1\}^n \rightarrow \{0,1\}^n$. This is an easier problem than finding s.

But until queries find a collision (x, y s.t. $f(x) = f(y)$), f is indistinguishable from some π. Birthday paradox tells us that we find a collision after $\Theta(\sqrt{2^n})$ random queries.

Quantum algorithm:

Construct a subroutine which reveals a random linear eq. of s. Repeat $O(n)$ times and solve equations to extract s.

Access: $O_f |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$.



Before O_f query: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|0^n\rangle$

After O_f query: $\frac{1}{\sqrt{2^n}} \sum_{x} |x\rangle|f(x)\rangle$

Let the measurement collapse to $z \in \{0,1\}^n$. Each z occurs uniformly randomly, and the resulting state will be

$$\frac{1}{\sqrt{2}} \sum_{x : f(x) = z} |x\rangle = \frac{1}{\sqrt{2}} \left(|x\rangle + |x \oplus s\rangle \right)$$

for some $x \in \{0,1\}^n$.

Apply $H^{\otimes n}$ to this state gives,

$$\frac{1}{\sqrt{2}} \left(H^{\otimes n} |x\rangle + H^{\otimes n} |x \oplus s\rangle \right)$$

$$= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2^n}}\sum_y (-1)^{x\cdot y}|y\rangle + \frac{1}{\sqrt{2^n}}\sum_y (-1)^{(x\oplus s)\cdot y}|y\rangle\right)$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_y (-1)^{x\cdot y}\left(1+(-1)^{s\cdot y}\right)|y\rangle$$

$$= \frac{1}{\sqrt{2^{n+1}}}\sum_{y:s\cdot y=0} 2|y\rangle = \frac{1}{\sqrt{2^{n-1}}}\sum_{y:s\cdot y=0}|y\rangle.$$

So measurement yields a uniformly random y amongst $s\cdot y = 0$.

Also, note measurement of z not needed.

Repeating $O(n)$ times will yield n linearly indep. eqs. w pr 99%.

$\Rightarrow$ s can be extracted.

Given a s, we can also check if it is correct by testing if

$f(x) = f(x\oplus s)$ for a random s.

Decision problem: Decide if f is a hidden shift or a permutation.

If we run this algorithm with a permutation it just outputs

random y each time leading to $s = 0^n$.

Group theory: A group is a set G with an action $\cdot : G \times G \to G$ s.t.

① $\exists$ an element $\in G$ s.t.

$$e \cdot g = g \cdot e = g \quad \forall g \in G.$$

② $g_1 \cdot (g_2 \cdot g_3) = (g_1 g_2) \cdot g_3 \quad \forall g_1, g_2, g_3 \in G.$

③ $\forall g \in G$, $\exists$ a unique element $h \in G$ s.t.

$g \cdot h = h \cdot g = e$. So, we denote h by g^{-1}.

Let H be a non-empty subset of G. H is a subgroup if

① $\forall g, h \in H$, $g \cdot h \in H$

② $\forall h \in H$, $h^{-1} \in H$.

A group is abelian if $\forall g, h \in G$, $g \cdot h = h \cdot g$ (commutes).

For abelian groups, the group action $\cdot$ is often represented as $+$. So $g + h = h + g \in G$. And the identity is expressed as 0. And h^{-1} as $-h$.

For $h_1, \ldots, h_k \in G$, let $\langle h_1, \ldots, h_k \rangle$ be the subgroup of elements expressible by combining $h_1, \ldots, h_k$ and $h_1^{-1}, \ldots, h_k^{-1}$.

For a subgroup $H \leq G$, $\{h_1 \ldots h_k\}$ is a generating set for H if $H = \langle h_1, \ldots, h_k \rangle$.

Think of a generating set as a basis in the case of abelian groups.

<u>Def</u>. Given an abelian group G and a subgroup $H \leq G$, a fn $f: G \to \{0,1\}^m$ <u>hides</u> H if $\forall x, y \in G$, $f(x) = f(y)$ iff $x - y \in H$.

equiv. f is constant on every coset and varies across cosets.

In Simon's problem, $G = \{0,1\}^n$ and $H = \{0, s\}$. and the fn f hides H.