Lecture 8

Oct 22, 2024

Recap:

$\mathrm{BQTIME}(t(n))$ = "the class of all <u>decision</u> problems solvable in time $t(n)$"

$$\mathrm{BQP} = \bigcup_{c \in \mathbb{N}} \mathrm{BQTIME}(n^c)$$

= "all problems efficiently solvable on a q. computer"

We started showing that 3-SAT can be solved in $\mathrm{BQTIME}\left[O(m\sqrt{2^n})\right]$ where m = # of clauses

n = # of bits in formula φ.

We actually showed q. algorithm for finding the solution (search problem).

Key ideas:

① $$\mathcal{O}\,|x, \underbrace{0^m}_{\text{ancilla}}\rangle = (-1)^{\varphi(x)}\,|x, 0^m\rangle$$

Built using classical reversible circuit for $\varphi(x)$.

② $F = \mathbb{1} - 2|+\rangle^{\otimes n}\langle +|^{\otimes n}$

O and F are reflections, with

- $-O$ reflecting about $|x\rangle$
- $-F$ reflecting about $|+\rangle^{\otimes n}$.

$F \cdot O = (-F)\cdot(-O)$ = rotation by 2γ

where $\sin\gamma = \langle x| \cdot (|+\rangle^{\otimes n}) = \frac{1}{\sqrt{2^n}}$.

within the plane defined by $|x\rangle, |+\rangle^{\otimes n}$.

Starting angle is γ since state is $|+\rangle^{\otimes n}$.

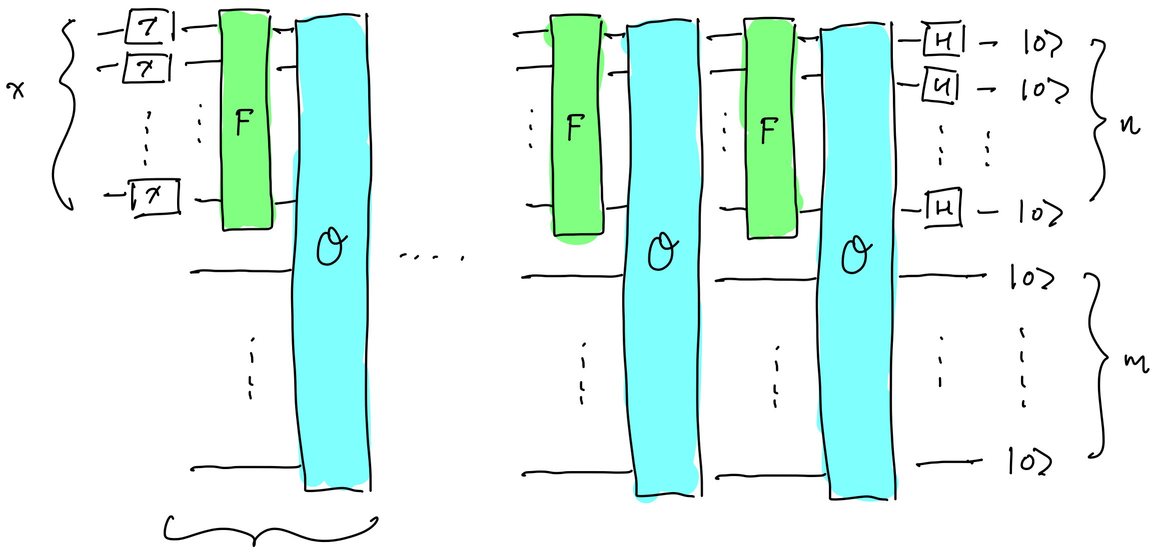
$$(F \cdot O)^t |+\rangle^{\otimes n} = |\gamma(2t+1)\rangle$$

Pick T s.t. $\gamma(2T+1) \approx \frac{\pi}{2}$

$$T = \frac{\pi}{4} \cdot \frac{1}{\gamma} = \frac{\pi}{4}\sqrt{2^n}.$$

Resulting state has good overlap with $|x\rangle$.

Measuring in standard basis outputs "x".



"Grover operator"

The full circuit requires decomposing F and $\mathcal{O}$ into individual gates. Yields $O(m\sqrt{2^n})$ gates and $\tilde{O}(\sqrt{2^n})$ time.

What happens if we run it on a φ s.t. $\varphi(x) = 0$ everywhere?

$\mathcal{O} = \mathbb{1}$ then so $(F\mathcal{O})^t |+\rangle^{\otimes n} = F^t |+\rangle^{\otimes n} = |+\rangle^{\otimes n}$.

Measuring gives a random output.

Note: This solves the search problem. To solve decision problem, check if output passes φ.

Aside: On your homework, you prove that if φ has K solutions, there is an algorithm running in time $O(\sqrt{2^n/K})$.

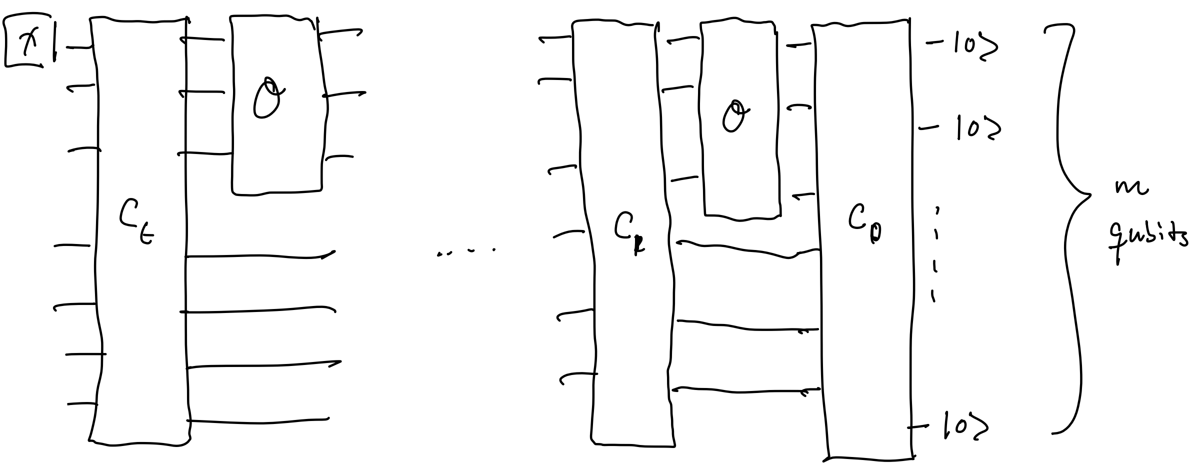
Today, we show that Grover's search is optimal in some sense.

If we are only allowed to query $\mathcal{O}$ and not φ, how many queries does it take to decide if

$$\mathcal{O} = \mathcal{O}_x := \mathbb{1} - 2|x\rangle\langle x| \text{ for some } x \in \{0,1\}^n \text{ or}$$

if $\mathcal{O} = \mathbb{1}$?

Notion of "unconstrained search" as we assume no additional knowledge of the structure of $\mathcal{O}$.



A picture of a generic decision q. algorithm making T queries to $\mathcal{O}$.

Assume a T query algorithm exists for deciding if $\mathcal{O} = \mathcal{O}_x$ or $\mathbb{1}$.

If $\mathcal{O} = \mathbb{1}$, state right before measurement is

$$|\Psi_{\mathbb{1}}\rangle = C_t C_{t-1} \cdots C_0 |0^m\rangle.$$

Otherwise define $|\Psi_x\rangle = C_t \mathcal{O}_x C_{t-1} \mathcal{O}_x \cdots C_1 \mathcal{O}_x C_0 |0^m\rangle$

notice if accepting $\mathcal{O}_x$ with $pr = 1-\epsilon$,

$$|\Psi_x\rangle = \sqrt{1-\epsilon}\, |1\rangle |\Psi_x^1\rangle + \sqrt{\epsilon}\, |0\rangle |\Psi_x^0\rangle$$

and rejecting $\mathbb{1}$,

$$|\Psi_{\mathbb{1}}\rangle = \sqrt{1-\epsilon}\, |0\rangle |\Psi_{\mathbb{1}}^0\rangle + \sqrt{\epsilon}\, |1\rangle |\Psi_x^1\rangle$$

The difference in behavior of O_x and $\mathbb{1}$:

For a random vector, $O_x|\varphi\rangle \approx \mathbb{1}|\varphi\rangle$

But for a specific vector, $O_x|x\rangle = -|x\rangle$

$\mathbb{1}|x\rangle = |x\rangle$.

Querying O_x only helps when state being queried has a lot of support on x.

Pf of lower bound: Bennett, Bernstein, Brassard, Vazirani

Fix an x (for now). $|h_T\rangle = |\Psi_{\mathbb{1}}\rangle$

$$|h_T\rangle = C_T \mathbb{1} C_{T-1} \mathbb{1} C_{T-2} \cdots C_1 \mathbb{1} C_0 |0^m\rangle$$

$$|h_{T-1}\rangle = C_T O_x C_{T-1} \mathbb{1} C_{T-2} \cdots C_1 \mathbb{1} C_0 |0^m\rangle$$

What is $\| |h_T\rangle - |h_{T-1}\rangle \|$?

$$\| |h_T\rangle - |h_{T-1}\rangle \| = \| C_T(\mathbb{1} - O_x) C_{T-1} \mathbb{1} C_{T-2} \cdots C_1 \mathbb{1} C_0 |0^m\rangle \|$$

$$2 \| \langle x| C_{T-1} \mathbb{1} C_{T-2} \cdots C_1 \mathbb{1} C_0 |0^m\rangle \|$$

because C_T is unitary (distance preserving) and

$$\mathbb{1} - O_x = \mathbb{1} - (\mathbb{1} - 2|x\rangle\langle x|) = 2|x\rangle\langle x|.$$

Let $|\varphi_T\rangle = C_{T-1}\,\mathbb{1}\,C_{T-2} \cdots C_1\,\mathbb{1}\,C_0|0^m\rangle$ } independent of x.

= state before T^{th} query

Then $\| |h_T\rangle - |h_{T-1}\rangle \| = 2\| \langle x|\varphi_T\rangle \| =: 2\sqrt{p_{x,T}}$

$\uparrow$ prob. measuring x on $|\varphi_T\rangle$

Next,

$$|h_{T-1}\rangle = C_T O_x C_{T-1}\,\mathbb{1}\,C_{T-2} \cdots C_1\,\mathbb{1}\,C_0|0^m\rangle$$

$$|h_{T-2}\rangle = C_T O_x C_{T-1} O_x \underbrace{C_{T-2} \cdots C_1\,\mathbb{1}\,C_0|0^m\rangle}_{|\varphi_{T-1}\rangle}$$

$$\| |h_{T-1}\rangle - |h_{T-2}\rangle \| = \| C_T O_x C_{T-1} (\mathbb{1} - O_x) |\varphi_{T-1}\rangle \|$$

$$= 2\| \langle x|\varphi_{T-1}\rangle \| = 2\sqrt{p_{x,T-1}}$$

I think we see the pattern,...

Keeping the pattern going...

$$|h_0\rangle = C_T O_x C_{T-1} O_x C_{T-2} \cdots \quad C_1 O_x C_0 |0^m\rangle = |\Psi_x\rangle.$$

Triangle Inequality,

$$\| |\Psi_{\mathbb{1}}\rangle - |\Psi_x\rangle \| = \| |h_T\rangle - |h_0\rangle \|$$

$$\leq \sum_{t=1}^{T} \| |h_t\rangle - |h_{t-1}\rangle \|$$

$$= 2 \sum_{t=1}^{T} \sqrt{p_{x,t}} \ .$$

Assume accept O_x w. pr. $\geq 2/3$ and accept $\mathbb{1}$ w pr. $1/3$.

So, there exists a distinguishing measurement w $\Delta \geq \frac{1}{3}$ between

$|\Psi_{\mathbb{1}}\rangle$ and $|\Psi_x\rangle$. So $\| |\Psi_{\mathbb{1}}\rangle - |\Psi_x\rangle \| \geq \frac{1}{3}$.

$$\Rightarrow \quad \frac{1}{6} \leq \sum_{t=1}^{T} \sqrt{p_{x,t}} \ .$$

Notice this calculation was done for some fixed x.

Using that it holds for all $x \in \{0,1\}^n$.

$$\frac{2^n}{6} \leq \sum_{x \in \{0,1\}^n} \sum_{t=1}^{T} \sqrt{p_{x,t}}$$

$$= \sum_{t=1}^{T} \|\sqrt{p_t}\|_1 \leftarrow \ell_1 \text{ norm of the vector } \left(\sqrt{p_{0^n,t}}, \ldots, \sqrt{p_{1^n,t}}\right)$$

$$\leq \sum_{t=1}^{T} \sqrt{2^n} \cdot \underbrace{\|\sqrt{p_t}\|_2}_{1 \text{ since prob. dist.}}$$

$$= T\sqrt{2^n}.$$

$$\Rightarrow T \geq \frac{1}{6}\sqrt{2^n}.$$

Intuition: Only queries with "mass" on x are aided by a query.
But since x is unknown, we can't have mass on all x.

Grover's algorithm starts with uniform mass and then incrementally increases the mass until $p_{x,T} = 1$.

Implications for $BQP \supseteq NP$.

1. This proves that BQP cannot have an exponential speedup for unconstrained search – only quadratic.

2. Proves that q. computers cannot efficiently solve 3-SAT in a black-box manner. If there was to be a q. algorithm for solving 3-SAT, it would have to look "under the hood" of the 3-SAT formula to get the speedup.

   i.e. "no lower bound known for structured search"

In general, q. speedups come from interference patterns. While we are running O in superposition, we aren't reducing the amplitude on "incorrect" y very quickly while increasing the amplitude on "correct" x.

Future lectures, will show structured speedups exploiting this advantage.

Lastly, we proved lower bounds for queries to

$$\mathcal{O} = \mathbb{1} - 2|x\rangle\langle x| .$$

Or in general for any function $f: \{0,1\}^n \to \{0,1\}$

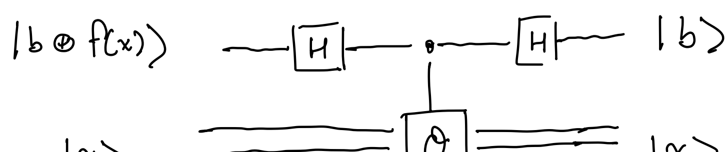
$$\mathcal{O} = \sum_x (-1)^{f(x)} |x\rangle\langle x| .$$

Wouldn't a more reasonable model be access to

$$\mathcal{O}' : |x\rangle|b\rangle \mapsto |x\rangle|b \oplus f(x)\rangle ?$$

Any query to $\mathcal{O}'$ can be simulated with a query to $C\text{-}\mathcal{O}$.
So, query lower bounds for $\mathcal{O}$ yield query lower bounds for $\mathcal{O}'$.

Pf. Claim:



State before $C\text{-}\mathcal{O}$ gate:

$$\frac{|0\rangle + (-1)^b |1\rangle}{\sqrt{2}} \otimes |x\rangle$$

After C-O gate:

$$\frac{|0\rangle + (-1)^{b \oplus f(x)} |1\rangle}{\sqrt{2}} \otimes |x\rangle$$

"phase kickback"

Final state:

$$|b \oplus f(x)\rangle \otimes |x\rangle.$$

So using "phase" form of the oracle for query lower bounds is sufficient.