CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, March 19 - Lecture 10.1

Today's scribe: Linkai Ma [Note: note proofread by Eric]

Reading: Chapter 5.3 & Appendix 4 of Nielsen and Chuang, Chapter 13 & Appendix A of Kitaev, Shen and Vyalyi

Agenda:

1. Simon's algorithm

1 Simon's Problem

Simon's problem is an important predecessor of Shor's algorithm, which generalizes to Bernstein-Vazirani and Deutsch-Jozsa. It can be futher generalized to the hidden subgroup problem. It gives an oracle separation of BQP and BPP.

Input: (Quantum) oracle access to a funciton $F = F_s$

$$F : \{0,1\}^n = (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow \{0,1\}^n$$
$$\text{such that } F(x) = F(y) \text{ if and only if } x = y \oplus s$$

Note that $\oplus$ is the group operation on $(\mathbb{Z}/2\mathbb{Z})^n$, which is bitwise addition mod 2.

Output: s

Remark. 1. *In the problem statement, the group structure on the domain of F is important. However, group structure on the codomain is not important.*

2.
$$< s >= \{0, s\} \cong \begin{cases} \{0\} \text{ if } s = 0 \\ \mathbb{Z}/2\mathbb{Z} \text{ if } s \neq 0 \end{cases}$$

So, we can interpret F as a function on $(\mathbb{Z}/2\mathbb{Z})^n$ that is "hiding" the subgroup $< s > \subsetneq (\mathbb{Z}/2\mathbb{Z})^n$.

3. *Another interpretation: F is a periodic function on $(\mathbb{Z}/2\mathbb{Z})^n$ with "periodicity" given by s.*

In the quantum version of the problem, we will assume as usual that we have quantum oracle access to F via unitary dilation.

$$U_F : (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n} \longrightarrow (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes n}$$
$$|x, y\rangle \longmapsto |x, F(x) \oplus y\rangle$$

Example: $n = 3, s = 101$

x	$F_s(x)$
000	000
001	001
010	010
011	011
100	001
101	000
110	011
111	010

Proposition 1. *For any classical probabilistic algorithm making no more than $2^{\frac{n}{2}}$ many queries to the oracle, there exists an $s \in \{0,1\}^n$ and a Simon oracle F_s for that s for which the algorithm fails to return the correct s with probability $\geq \frac{1}{3}$.*

Thus, any classical probabilistic algorithm requires time at least $2^{\frac{n}{2}}$ to find s (with good confidence). In fact $\Theta(2^{\frac{n}{2}})$ orcale access is enough to confidently identify s classically.

Naively, one might expect to need 2^n, but the birthday paradox gets us down to $2^{\frac{n}{2}}$.

Idea for classical algorithm:

Randomly pick two bit string $x, y \in \{0,1\}^n$ and hope for a collision, i.e., hope that $F(x) = F(y)$. If this happens and $x \neq y$,then $s = x \oplus y$. We can use the birthday paradox to show this can be made to work with high confidence as long as we make at least $2^{\frac{n}{2}}$ queries.

Issue:

How do we know that being "unlucky" a lot (finding no collisions) can not be used to deduce something helpful about s.

Idea of proof:

Need to fix a classical probabilistic algorithm first.

Then it suffices to find a single s and F_s such that the algorithm fails on that F_s with probability $\geq \frac{1}{3}$.

Pick s "cleverly" and consider a randomly chosen oracle for that s(there are exponentially many). Now argue that the probability that the algorithm fails for a random oracle $\geq \frac{1}{3}$.

Deduce that there must exist at least one "actual" orcale F_s for which the algorithm fails with probability $\geq \frac{1}{3}$.

Simon's algorithm solves Simon's problem (quantum version) using $O(n)$ calls to the oracle with time $O(n^3)$.

Given $s \in \{0,1\}^n = (\mathbb{Z}/2\mathbb{Z})^n$, define $< s >^{\perp} = \{x \in (\mathbb{Z}/2\mathbb{Z})^n : x \cdot s = 0 \text{ mod } 2\}$.

Note: $< s >^{\perp}$ determines s.

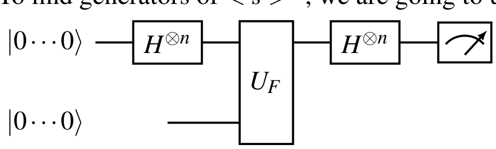
Given $g_1, \cdots, g_l$ such that $< g_1, \cdots g_l > = < s >^{\perp}$, then the linear system

$$\begin{aligned} g_1 \cdot z &= 0 \text{ mod } 2 \\ g_2 \cdot z &= 0 \text{ mod } 2 \\ &\cdots \\ g_l \cdot z &= 0 \text{ mod } 2 \end{aligned}$$

has a unique solution given by $z = s$.

This linear system can be solved in time $O(l^3)$. Thus to find s, it suffices to find $g_1, \cdots, g_l$ that generates $< s >^{\perp}$, where $l = O(\text{poly}(n))$.

To find generators of $< s >^{\perp}$, we are going to use U_F and a similar procedure to previous algorithms.



Lemma 2. *The output y of the first register in above circuit is uniformly randomly chosen element of $< s >^{\perp}$.*

Intuition: quantum oracle access to F_s allows us to uniformly randomly sample from $< s >^{\perp}$. Using this and the following lemma, we can find $g_1, \cdots, g_l$ such that $< g_1, \cdots g_l > = < s >^{\perp}$ without too much work and with high probability.

Lemma 3. *Let G be a finite abelian group and let $g_1, \cdots, g_l$ be uniformly randomly independent chosen elements of G, then:*

$$\mathbb{P}(< g_1, \cdots, g_l > = G) \geq 1 - \frac{|G|}{2^l}$$

Remark. *If G is not abelian, replace $|G|$ with the number of maximal subgroups of G.*

2 Simon's Algorithm

1. Choose l so that $1 - \frac{2^n}{2^l} \geq \frac{1}{3}$. Clearly $l = O(n)$ suffices.
2. Use l calls to U_F (can do this in parallel) to get $g_1, \cdots, g_l$, which are uniformly randomly sampled elements of $< s >^{\perp}$.
3. Classically solve the linear system $\{g_i \cdot z = 0 \text{ mod } 2 | i = 1, \cdots, l\}$

Proof of lemma ??:

Let's compute the state we get before measuring:

$$\begin{aligned}
&(H^{\otimes n} \otimes Id) \circ U_F \circ (H^{\otimes n} \otimes Id) \left(|0 \cdots 0\rangle \otimes |0 \cdots 0\rangle \right) \\
&= (H^{\otimes n} \otimes Id) \circ U_F \left(\sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} 2^{-\frac{n}{2}} |x\rangle \otimes |0 \cdots 0\rangle \right) \\
&= (H^{\otimes n} \otimes Id) \left(2^{-\frac{n}{2}} \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} |x\rangle \otimes |F(x)\rangle \right) \\
&= 2^{-n} \sum_{x,y \in (\mathbb{Z}/2\mathbb{Z})^n} (-1)^{x \cdot y} |y\rangle |F(x)\rangle
\end{aligned}$$

if $s \neq 0$, then for each $x \in (\mathbb{Z}/2\mathbb{Z})^n$, $\#F^{-1}(F(x)) = 2$. So, if $z \in Range(F)$, then $F^{-1}(z) = \{x_{z,1}, x_{z,2}\} = \{x_{z,1}, x_{z,1} \oplus s\}$

Using this for each $y \in \{0,1\}^n$, the probability of measuring y is

$$\begin{aligned}
\mathbb{P}(y) &= || \sum_{x \in (\mathbb{Z}/2\mathbb{Z})^n} 2^{-n} (-1)^{x \cdot y} |F(x)\rangle ||^2 \\
&= || \sum_{z \in Rnage(F)} \sum_{x \in F^{-1}(z)} 2^{-n} (-1)^{x \cdot y} |z\rangle ||^2 \\
&= 2^{-2n} \sum_{z \in Rnage(F)} ||(-1)^{x_{z,1} \cdot y} |z\rangle + (-1)^{x_{z,2} \cdot y} |z\rangle ||^2 \\
&= 2^{-2n} \sum_{z \in Rnage(F)} |1 + (-1)^{s \cdot y}|^2 \\
&= \begin{cases} 0 & \text{if } s \cdot y = 1 \text{ mod } 2 \\ \frac{1}{|<s^{\perp}>|} & \text{if } s \cdot y = 0 \text{ mod } 2 \end{cases}
\end{aligned}$$