COL7160 : Quantum Computing

Lecture 9: Simon's Algorithm

Instructor: Rajendra Kumar

Scribe: A. Sai Srinivas

1 Summary of Query Complexity

Before diving into Simon's problem, we review the progression of quantum query complexity. These early problems were designed to "sell" the utility of quantum computing by demonstrating resource separation between classical and quantum regimes.

#	Problem	Classical Det.	Classical Rand.	Quantum
1	Deutsch (1985)	2 queries	2 queries	1 query
2	Deutsch-Jozsa (1982)	$2^{n-1}+1$	constant (for small error)	1 query
3	Bernstein-Vazirani (1993)	n	n	1 query

Table 1: Comparison of query complexities for fundamental algorithms.

Remark 1. While Bernstein-Vazirani showed a separation, the advantage over randomized algorithms was relatively small. It wasn't until 1994, with the introduction of **Simon's Problem** and subsequently **Shor's Algorithm**, that the field gained massive attention due to the exponential speedup over randomized classical models.

Let's see how Simon's Problem gives a definite advantage of Quantum Computation over classical Deterministic and Randomized solutions. We will understand not only the algorithm itself, but the idea behind it which was introduced and see the "superiority" of Quantum Computers.

2 Simon's Problem

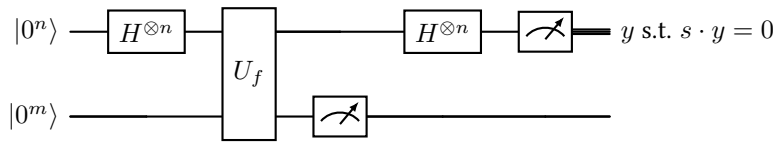
Simon's problem is the first to provide an exponential gap between quantum and randomized classical complexity. It is essentially a "hidden period-finding" problem over bitstrings.

Definition 2. Let $f : \{0,1\}^n \to \{0,1\}^m$ be a function. We are promised that there exists a hidden string $s \in \{0,1\}^n$ such that $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus s$. The goal is to find s.

To solve this problem, lets see how s changes the nature of f.

- If $s = 0^n$, the function is one-to-one.
- If $s \neq 0^n$, the function is two-to-one.

2.1 The Quantum Circuit and Interference



The quantum state evolves as follows:

1. Start in $|0^n\rangle |0^m\rangle$ and create superposition: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^m\rangle$.
2. Apply the Oracle U_f: $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$.

   Assume that f is two-one and so $s \neq 0$.

3. Measuring the second register yields some $f(x)$, collapsing the first register to:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|x\rangle + |x \oplus s\rangle\right)$$

4. Apply $H^{\otimes n}$ to the first register:

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{y\in\{0,1\}^n} \left[(-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y}\right]|y\rangle$$

Using the property $(x \oplus s) \cdot y = (x \cdot y) \oplus (s \cdot y)$, we can factor out the term $(-1)^{x\cdot y}$ and factoring the expression, we get[1]:

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

This leads to the following **Interference Conditions**:

- **Destructive Interference:** If $s \cdot y = 1 \pmod 2$, then $(-1)^{s\cdot y} = -1$. The amplitude becomes $1 + (-1) = 0$, meaning the state $|y\rangle$ will never be observed.
- **Constructive Interference:** If $s \cdot y = 0 \pmod 2$, then $(-1)^{s\cdot y} = 1$. The amplitude becomes $1 + 1 = 2$, meaning we only measure strings y that are orthogonal to the hidden string s.

Proposition 3. *The amplitude of $|y\rangle$ is non-zero if and only if $s \cdot y = 0 \pmod 2$.*

Hence all the values of $|y\rangle$ that we observe satisfy $s.y = 0$. We can repeat this experiment many number of times and sample some distinct values of y, we obtain a system of linear equations over $\mathbb{F}_2$ that allows us to solve for s. This could be done using a classical computer.
By sampling y approximately $n + 10$ times, with very high probability ($\approx 99\%$), we can solve for s.

3 Homework and Challenges

HW 1: Single Measurement Challenge
Prove that it is possible to solve Simon's Problem by applying measurement only once at the very end of the circuit. Does measuring the second register in the middle actually change the output distribution of y?

4 Next class

We will see the case of $s = 0$ and how it will be decided. (Hint: when the same circuit is used and some non-zero s is calculated, what would $f(0) \neq f(s)$ imply?)
We will see how the single measurement is possible.

[1]

$$\begin{aligned}\text{Amplitude} &= (-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y} \\ &= (-1)^{x\cdot y} + (-1)^{(x\cdot y)\oplus(s\cdot y)} \\ &= (-1)^{x\cdot y} + (-1)^{x\cdot y}\cdot(-1)^{s\cdot y} \\ &= (-1)^{x\cdot y}\left(1 + (-1)^{s\cdot y}\right)\end{aligned} \tag{1}$$