CS6846 – Quantum Algorithms and Cryptography

Simon's and Bernstein-Vazirani Algorithms

Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Simon's Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

- f is two-to-one
- $\forall x, y : f(x) = f(y) \iff y = x \oplus s$ for some fixed $s \neq 0^n$

find the value of s.

Simon's Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

- f is two-to-one
- $\forall x, y : f(x) = f(y) \iff y = x \oplus s$ for some fixed $s \neq 0^n$

find the value of s.

Classical Randomized: $\Theta(2^{n/2})$.

Simon's Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

- f is two-to-one
- $\forall x, y : f(x) = f(y) \iff y = x \oplus s$ for some fixed $s \neq 0^n$

find the value of s.

Classical Randomized: $\Theta(2^{n/2})$.

Quantum: $O(n)$ queries: exponential speedup!

Simon's Algorithm

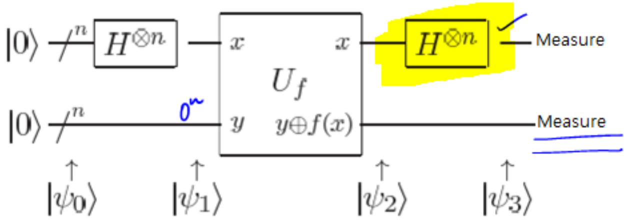
Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that:

- f is two-to-one
- $\forall x, y : f(x) = f(y) \iff y = x \oplus s$ for some fixed $s \neq 0^n$

find the value of s.

Classical Randomized: $\Theta(2^{n/2})$.

Quantum: $O(n)$ queries: exponential speedup!



Simon's Algorithm

Given a function $f : \{0,1\}^n \to \{0,1\}^n$ such that (i) f is two-to-one, (ii) $\forall x, y : f(x) = f(y) \iff y = x \oplus s$ for some fixed $s \neq 0^n$, find the value of s.

Algorithm:

- Prepare a superposition $H^{\otimes n}(|0^n\rangle) = \frac{1}{2^{n/2}} \sum_x |x\rangle$.
- Apply the unitary function U_f to this, with ancillary $\underline{0^n}$ qubits.
- Measure the last n registers in the computational basis. Discard.
- Apply the quantum fourier transform $H^{\otimes n}$ to first n registers.
- Measure this state. ——— 1 output.
- Repeat above steps "many" times.

Simon's Algorithm: Analysis

1). First Hadamard gives

$$|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_x |x\rangle \quad |0\rangle^n.$$

$\hookrightarrow$ untouched.

$y = f(x_1) = f(x_2)$ iff $x_1 = x_2 \oplus s$.

2). Apply f.

$$|\psi_2\rangle = 2^{-n/2} \sum_x |x, f(x)\rangle.$$

Ignore normalizations.

3). Measure last n bits. Say I get y.

$$|\psi_3\rangle = \left(\frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}}\right)|y\rangle.$$

Simon's Algorithm: Analysis

4) Apply $H^{\otimes n}$ on $\dfrac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}}$

$$= \sum_z 2^{-n/2 - \frac{1}{2}} (-1)^{\langle x; z \rangle} |z\rangle + \sum_z 2^{-n/2 - \frac{1}{2}} (-1)^{\langle x \oplus s; z \rangle} |z\rangle$$

$$= 2^{-n/2 - \frac{1}{2}} \sum_z (-1)^{\langle x; z \rangle} \left(1 + (-1)^{\langle s; z \rangle}\right) |z\rangle$$

$$= 2^{-n/2 - \frac{1}{2}} \sum_{z \perp s} (-1)^{\langle x; z \rangle} (1+1) |z\rangle$$

$$\cancel{+ \;\text{''} \sum_{z \not\perp s} (-1)^{\langle x; z \rangle} (1-1) |z\rangle}.$$

5) Measure to get $z \perp s$. Do "enough" times to get n Linearly Indpt z.

Simon's Algorithm: Analysis

How many times do I need to repeat?

Claim: $O(n)$ repetitions give constant probability

$$\Pr(z_1 \ldots z_{k+1} \text{ are linearly independent}) = 1 - \underbrace{\frac{2^k}{2^{n-1}}}_{}$$

Prob. z_{k+1} is in span of $z_1 \ldots z_k$.

Pr of selecting appropriate z_i in each iteration is:

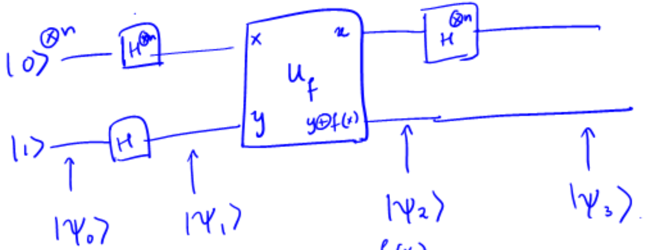
$$\prod_{i=1}^{n-1} \left(1 - \frac{1}{2^i}\right) \geq \frac{1}{4}.$$

Exercise

Given oracle access to $f : \{0,1\}^n \to \{0,1\}$ where $f(x) = \langle x, s \rangle \pmod 2$ for all $x \in \{0,1\}^n$. What is s?

Classically: n queries

Quantumly: 1 query.



$$|\psi_2\rangle = \sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)} \, |x\rangle \, |-\rangle}{2^{n/2}}.$$

Scratch Pad

- Applying Hadamard on top n bits:

$$|\psi_3\rangle = \sum_x \sum_z \frac{(-1)^{f(x)+\langle x;\, z\rangle} |z\rangle |-\rangle}{2^n}.$$

- Measure top n qubits.

Consider amplitude on $z = s$.

$$\frac{1}{2^n} \sum_x (-1)^{\underbrace{\langle x;\, s+s\rangle} \rightarrow \, ?\; 0}$$

$$= 1.$$

Scratch Pad

Interesting term.

$$(-1)^{\langle x; s\rangle + \langle x; z\rangle} = (-1)^{\langle x;\, s+z\rangle}$$

What happens when $z \neq s$?

Amplitude $= 0$. Why?

$\langle x; s\rangle \bmod 2$. Is this balanced?

$s = 1 * * * *$.

$x_0 = 0\,x'$

$x_1 = 1\,x'$

Fix $s + z = 1 * * \cdots *$

$x_0 = 0\,x'$, $x_1 = 1\,x'$

$$\underbrace{(-1)^{\langle x_0;\, z+s\rangle}} \quad \text{vs} \quad (-1)^{\langle x_1;\, z+s\rangle}$$

Consider inner product

$$0 \cdot 1 + \underbrace{\langle x'; * \cdots * \rangle}_{\Delta} \qquad\qquad 1 \cdot 1 + \Delta$$