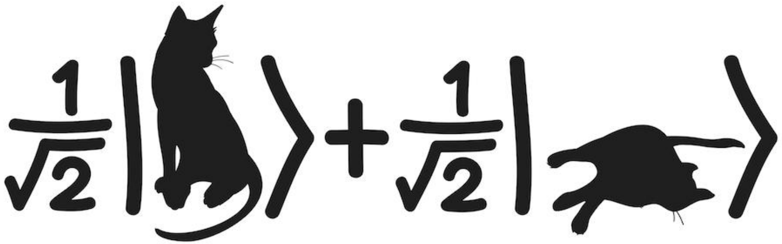
Quantum Mechanics & Quantum Computation



Umesh V. Vazirani
University of California, Berkeley

Lecture 12: Early Quantum Algorithms

Simon's Algorithm

Simon's algorithm

We are given a 2-1 function $f : \{0,1\}^n \to \{0,1\}^n$ such that:
there is a secret string $s \in \{0,1\}^n$ such that : $f(x) = f(x \oplus s)$
Challenge: find s.

$$\begin{array}{r} 000 \\ \underline{101} \\ 101 \end{array}$$

$x = 011$
$s = 101$
$x \oplus s = 110$

Example)

$n = 3$
$s = 101$

x	f(x)
000	000
001	010
010	001
011	100
100	010
101	000
110	100
111	001

$2^n = N$

Classical Algorithm?

Collision

$\sqrt{N} = \boxed{2^{n/2}}$

exponential time.

Simon's algorithm

- Set up random superposition $\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$ $\quad r$ random n bit string
- Fourier sample to get a random $y: \quad y \cdot s = 0(\text{mod} 2)$
- Repeat steps n–1 times to generate n–1 linear equations in s.

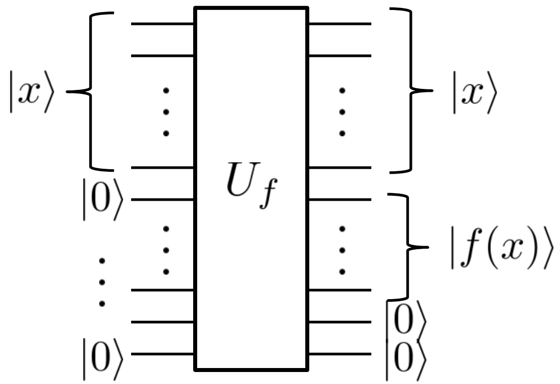
  Solve for s.

$$y = y_1 \cdots y_n$$
$$s = s_1 \cdots s_n$$

$$y_1^{(1)} s_1 + \cdots + y_n^{(1)} s_n = 0 \pmod 2$$
$$\vdots \qquad\qquad \vdots$$
$$y_1^{(n-1)} s_1 + \cdots + y_n^{(n-1)} s_n = 0 \pmod 2$$

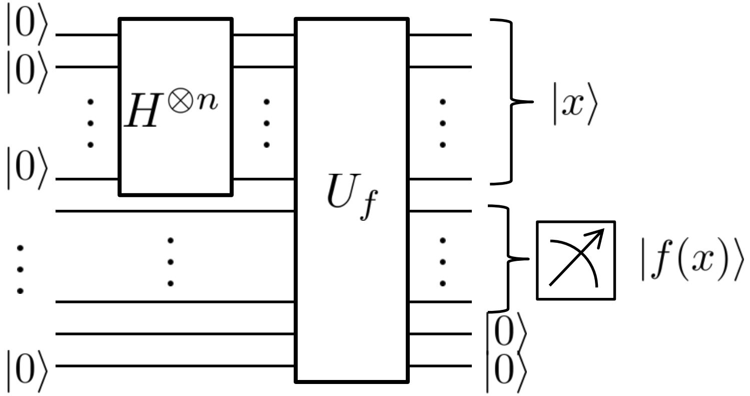
Settin up random superposition

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)



Setting up random superposition

We are given a function $f : \{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)



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

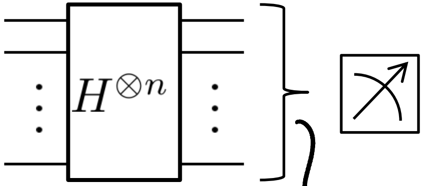
measure

see $f(r)$

1^{st} register $= \frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$

Fourier Sampling

$$\frac{1}{\sqrt{2}}|r\rangle + \frac{1}{\sqrt{2}}|r \oplus s\rangle$$



$$\sum_y \beta_y |y\rangle$$

$$\beta_y = \frac{(-1)^{r\cdot y}}{2^{\frac{n+1}{2}}} + \frac{(-1)^{(r\oplus s)\cdot y}}{2^{n+1/2}} = \frac{(-1)^{r\cdot y}}{2^{\frac{n+1}{2}}}\left[1 + (-1)^{s\cdot y}\right]$$

<u>Case 1</u> $\quad s\cdot y \equiv 1 \pmod 2 \qquad \beta_y = 0$

<u>Case 2</u> : $\quad s\cdot y \equiv 0 \pmod 2 \qquad \beta_y = \dfrac{(-1)^{r\cdot y}}{2^{\frac{n-1}{2}}} \qquad (\beta_y)^2 = \dfrac{1}{2^{n-1}}$

Reconstructing s:

$$y \cdot s \equiv 0 \pmod 2$$

$$n-1 \begin{cases} y_1 s_1 + \cdots + y_n s_n \equiv 0 \pmod 2 \\ \vdots \end{cases}$$

$$y^{(1)}, y^{(2)}, \ldots, y^{(n-1)}$$

$$\frac{1}{2^n} + \frac{1}{2^{n-1}} + \frac{1}{2^{n-2}} + \cdots + \frac{1}{4} \leq \frac{1}{2}$$

$\therefore$ independent with prob $\geq \frac{1}{2}$.

$$f(x) \qquad f(x \oplus s)$$

Simon's algorithm

We are given a function $f:\{0,1\}^n \to \{0,1\}^n$ as a black box.
We know that f is a 2-1 function. (There is a secret string $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$)