CSCE 785
10/17/2023

Simon's Problem circuit analysis

Shor's algorithm background; Modular arith.

Recall: $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ (some m)

such that there exists an $s \in \{0,1\}^n$ such that

$\forall x \neq y$ $(x, y \in \{0,1\}^n)$, $f(x) = f(y)$ iff $x \oplus y = s$

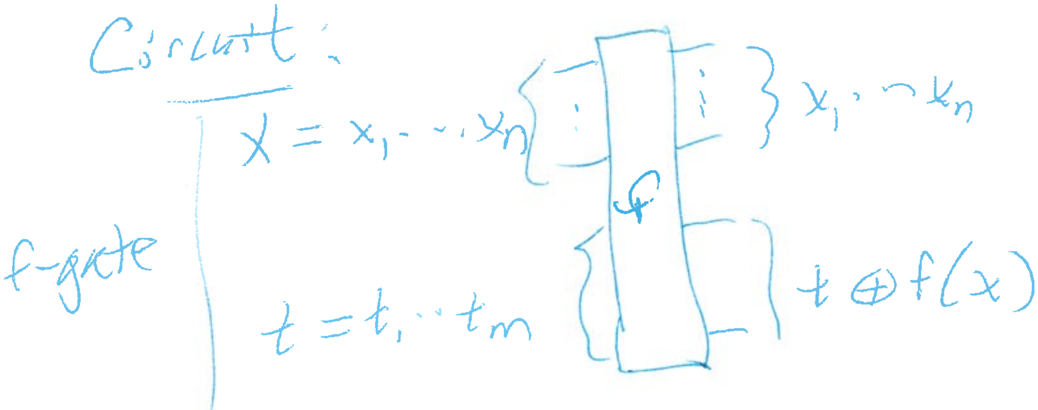
[equiv: $y = x \oplus s$, etc.]

$s \neq 0$: $f(x) = f(x \oplus s)$

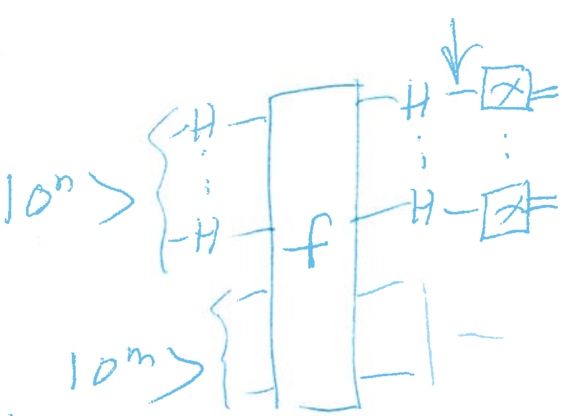
only collision involving x, $x \oplus s$

$\therefore f$ is 2-to-1

Circuit:



Its own inverse!



Step thru:

$$|0^n, 0^m\rangle \xmapsto[= H \otimes \cdots \otimes H]{H_1 \cdots H_n} \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, 0^m\rangle \xmapsto{\text{f-gate}} \frac{1}{2^{n/2}} \sum_{x} |x, f(x)\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{2^{n/2}} \sum_x H^{\otimes n} |x, f(x)\rangle = \frac{1}{2^n} \sum_x \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y, f(x)\rangle$$

$$= |\psi_{out}\rangle = \frac{1}{2}\left(|\psi_{out}\rangle + |\psi_{out}\rangle \right)$$

$$\cancel{= \frac{1}{2^{n+1}} \left(\sum_{x,y} (-1)^{x \cdot y} |y, f(x)\rangle + \sum (-1) \quad |y, f(x)\rangle \right)}$$

$$= \frac{1}{2^{n+1}} \Bigg(\sum_y \Big(\sum_x (-1)^{x \cdot y} |y, f(x)\rangle \Big)$$

$$+ \underbrace{\sum_y \Big(\sum_x (-1)^{(x \oplus s) \cdot y} |y, \overset{f(x \oplus s)}{\overset{\shortparallel}{f(x)}}\rangle \Big)}\Bigg)$$

$$= \sum_y \Big(\sum_x (-1)^{\overset{z = x \oplus s}{\underline{(x \oplus s)}} \cdot y} |y, f(\overset{z}{x \oplus s})\rangle \Big)$$

{As x runs through all strings of n bits, $x \oplus s$ also runs through all strings of n bits
$\therefore$ same sum}

Then use $f(x \oplus s) = f(x)$

$$|\psi_{out}\rangle = \frac{1}{2^{n+1}} \left(\sum_y \left(\sum_x \Big((-1)^{x \cdot y} + \underbrace{(-1)^{(x \oplus s) \cdot y}}_{(-1)^{x \cdot y} (-1)^{s \cdot y}} \Big) |y, f(x)\rangle \right) \right)$$

Note: $(-1)^{(x \oplus s)\cdot y} = (-1)^{(x+s)\cdot y} = (-1)^{x\cdot y + s\cdot y}$

$= (-1)^{x\cdot y}(-1)^{s\cdot y}$

$$|\psi_{out}\rangle = \frac{1}{2^{n+1}} \sum_y \left((1+(-1)^{s\cdot y}) \sum_x (-1)^{x\cdot y} |y, f(x)\rangle \right)$$

$$= \frac{1}{2^{n+1}} \sum_x \left((-1)^{x\cdot y} \sum_y (1+(-1)^{s\cdot y}) |y\rangle \right) \otimes |f(x)\rangle$$

$$= \frac{1}{2^{n+1}} \sum_x \left(\sum_y (-1)^{x\cdot y} (1+(-1)^{s\cdot y}) |y\rangle \right) \otimes |f(x)\rangle$$

$$= \frac{1}{2^{n+1}} \sum_y |y\rangle \otimes \left(\sum_x (-1)^{x\cdot y} (1+(-1)^{s\cdot y}) |f(x)\rangle \right)$$

$s\cdot y = 1$: $\sum_x (-1)^{x\cdot y} \underbrace{(1+(-1)^{s\cdot y})}_{1-1=0} |f(x)\rangle = 0$

$s\cdot y = 0$: $\sum_x (-1)^{x\cdot y} \underbrace{(1+(-1)^{s\cdot y})}_{1+1=2} |f(x)\rangle$

$$\therefore |\psi_{out}\rangle = \frac{1}{2^n} \sum_{y: s\cdot y=0} \left(\sum_x (-1)^{x\cdot y} |y, f(x)\rangle \right)$$

$$= \frac{1}{2^n} \sum_{y: s\cdot y=0} |y\rangle \otimes \left(\overbrace{\sum_x (-1)^{x\cdot y} |f(x)\rangle}^{\text{norm indep of } y} \right)$$

Measure y in state $|\psi_{out}\rangle$

Review: $|\psi\rangle = \sum_{z \in \{0,1\}^n} \alpha_z |z\rangle$

measure the first k qubits, say.

For each outcome $p \in \{0,1\}^k$, get p with probability $\sum_{z : z = p \cdots} |\alpha_z|^2$

So get a uniformly random y such that $s \cdot y \overset{\text{mod } 2}{=} 0$.

Run the circuit k times, get indep random $y_1, \ldots, y_k$ such that $y_i \cdot s \underset{\text{mod } 2}{=} 0$ for $1 \le i \le k$.

I matrix form:

$$\begin{bmatrix} - & y_1 & - \\ - & y_2 & - \\ & \vdots & \\ - & y_k & - \end{bmatrix} \begin{bmatrix} s \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix}$$

(all arithmetic is in $\mathbb{Z}_2$)

Assume that $s \neq 0^n$. Then get $y_1, y_2, \ldots$ until the matrix above has rank $n-1$.

Then kernel of the matrix above is 1-dimensional subspace of $\mathbb{Z}_2^n$, and it contains $s \neq 0$, so kernel is $\{0^n, s\}$ so s found by standard lin. algebra techniques.

Q: ~~How lit~~ How many ~~times~~ y_i needed to get rank $n-1$ with high probability?

Claim: If rank is $< n-1$ and a new row is added, it increases the rank by 1 with prob $\geq \frac{1}{2}$.

$S = \{y : s \cdot y = 0\}$ has dimension $n-1$

so $|S| = 2^{n-1}$

Chosen $y_1, \dots, y_k$ such that $\text{rank}\begin{bmatrix} - & y_1 & - \\ & \vdots & \\ - & y_k & - \end{bmatrix} < n-1$.

Then rows span a space S_k of dim $\leq n-2$.

Choose a random $y_{k+1} \in S$. $|S_k| \leq 2^{n-2} = \frac{1}{2}|S|$

$\therefore \text{Prob}\{y_{k+1} \notin S_k\} \geq \frac{1}{2}$, and if so, then $\underbrace{\dim(S_{k+1})}_{\text{new rank}} > \underbrace{\dim(S_k)}_{\text{old rank}}$

Modular arithmetic

Pick $n \geq 2$ (the modulus)

$a, b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ means $a-b$ is a multiple of n.

equiv. relation $a \equiv_n b$ (shorthand)

$a \equiv_n b \Rightarrow a+c \equiv_n b+c$
& $ac \equiv_n bc$

Def: $\mathbb{Z}_n$ (sometimes $\mathbb{Z}/n\mathbb{Z}$)

$\mathbb{Z}_n : \{0, \ldots, n-1\}$

For every $a \in \mathbb{Z}$ there is a unique $r \in \mathbb{Z}_n$ such that $a \equiv_n r$ (r = remainder when a is divided by n)

so $a \equiv_n b$ means they have the same remainder.

Modular arith (mod n) happens entirely inside $\mathbb{Z}_n$.
$+, \cdot, -, /$ gives elements of $\mathbb{Z}_n$:
Use normally then take the remainder by div by n.