# LECTURE - 5

* Fourier transform over $\mathbb{F}_2^n$

* Deutsch - Jozsa continued

* Simon's Algorithm

**Last time:**

$$|x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$$

"Phase kickback" For boolean $f: \{0,1\}^n \to \{0,1\}$.

$$|x\rangle|-\rangle \xrightarrow{U_f} (-1)^{f(x)}|x\rangle|-\rangle$$

$$\sum \alpha_x |x\rangle|-\rangle \xrightarrow{U_f} \sum (-1)^{f(x)} \alpha_x |x\rangle|-\rangle.$$

**Deutsch-Jozsa**

Superposition access to $f$ meaning $\sum \alpha_x |x\rangle|-\rangle \xmapsto{U_f} \sum (-1)^{f(x)} \alpha_x |x\rangle|-\rangle$

- Promise. $f$ is either constant or balanced

  Decide which is the case.

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

← ignore going fwd, still there

2) $U_f \left( \sum_x |x\rangle |-\rangle \right) \longrightarrow$

$$\sum_x (-1)^{f(x)} |x\rangle |-\rangle$$

measure and discard

3) $H^{\otimes n} \left( \quad \right)$

$$= \sum_x (-1)^{f(x)} H^{\otimes n} (|x\rangle)$$

4) Measure in computational basis

5) $f$ is constant $\Longleftrightarrow$ measurement result is $0^n$.

"$\Rightarrow$"

When $f$ is constant, $(-1)^{f(x)} = (-1)^0 \ \forall x$

or $= (-1)^1 \ \forall x$

then $\pm \sum_{x \in \{0,1\}^n} H^{\otimes n} (|x\rangle) = \pm |0^n\rangle$

"$\Leftarrow$"

msmt outcome is $0^n \Rightarrow f$ is constant

$\equiv$ $f$ is balanced $\Rightarrow$ msmt outcome is NOT $0^n$

$$H^{\otimes n}\left(\sum_x \frac{(-1)^{f(x)}|x\rangle}{2^{n/2}}\right)$$

dropping this for ease

$$= \sum_x (-1)^{f(x)} H^{\otimes n}(|x\rangle)$$

---

$H^{\otimes n}(|x\rangle)$ for any $x = x_1 \ldots x_n$

$$= \bigotimes_{i\in[n]} H(|x_i\rangle)$$

$$= \bigotimes_{i\in[n]} \left(|0\rangle + (-1)^{x_i}|1\rangle\right)$$

$$= \sum_{y\in\{0,1\}^n} (-1)^{\langle x,y\rangle}|y\rangle$$

operations over $\mathbb{F}_2^n$

Example $x = 011$ ($x_1 x_2 x_3$)

$H^{\otimes 3}|x\rangle$ ($x_1 = 0$ so "+", $x_2 = 1$ so "−", $x_3 = 1$ so "−")

$$= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= +|000\rangle - |001\rangle - |010\rangle$$

$$= \sum_y (-1)^{\langle x, y\rangle \bmod 2} |y\rangle$$

$+$ or $-$? $|\underline{y_1}\, y_2 y_3\rangle$ ($y_1$ is the 1st)

are the number of 1s in $|y_1 y_2 y_3\rangle$ at indices $i$ where $x_i = 1$, even or odd?

**Claim.** $H^{\otimes n}(|x\rangle) = \sum_{y \in \{0,1\}^n} (-1)^{\langle x,y \rangle} |y\rangle$.

[We saw the proof].

To prove correctness of DJ, we wanted to show that:

If $\sum_x (-1)^{f(x)} H^{\otimes n}(|x\rangle) = \sum_{y \in \{0,1\}^n} \alpha_y |y\rangle$ and $f$ is balanced

then $\alpha_{0^n} = 0$.

We obtained.

$$\sum_x (-1)^{f(x)} \left( H^{\otimes n}(|x\rangle) \right)$$

$$= \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left( \sum_{y \in \{0,1\}^n} (-1)^{\langle x,y \rangle} |y\rangle \right)$$

$$= \sum_{x,y \in \{0,1\}^n \times \{0,1\}^n} (-1)^{f(x)+\langle x,y \rangle} |y\rangle$$

$$= \sum \alpha_y |y\rangle$$

## Amplitude on $|0^n\rangle$ (i.e. Calculating $\alpha_{0^n}$)

is $\sum_x (-1)^{f(x) + \langle x, 0^n \rangle}$

$= \sum_x (-1)^{f(x)}$

$= 0.$

for balanced $f$

# 0s in $f(x)$ = # 1s in $f(x)$

$\Rightarrow \#(-1)^0 = \#(-1)^1$

$\Rightarrow$ #1s = #(-1)s

## Fourier transform (over $\mathbb{F}_2^n$)

$\sigma, x \in \mathbb{F}_2^n$

$\sigma \cdot x = \langle \sigma, x \rangle = \bigoplus_{i : \sigma_i = 1} x_i$

← parity of $x$ restricted to positions where $\sigma_i = 1$

$(-1)^{\sigma \cdot x} = \prod_{i : \sigma_i = 1} (-1)^{x_i}$

$\chi_\sigma(x)$

Lets zoom into $\chi_\sigma(x)$

when $\sigma = 0^n$,

$\chi_{0^n}(x)$. $\forall x$, $\chi_{0^n}(x) = (-1)^0 = 1$.

$$\chi_\sigma = \begin{bmatrix} \chi_\sigma(0^n) \\ \chi_\sigma(0^{n-1}1) \\ \vdots \\ \chi_\sigma(1^n) \end{bmatrix}_{2^n \times 1} \qquad \chi_{0^n} = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix}$$

The set

$$\chi_{0^n}, \chi_{0^{n-1}1}, \chi_{0^{n-2}10} \ldots\ldots\ldots \chi_{1^n}$$

$$= \{\chi_\sigma\}_{\sigma \in \{0,1\}^n}$$

is a basis for $\mathbb{C}^{2^n}$.

Why?

We will show that $\forall\, \sigma \neq \gamma$,

$\chi_\sigma$ and $\chi_\gamma$ are orthogonal.

$\langle \chi_\sigma, \chi_\gamma \rangle = 0$ when $\sigma \neq \gamma$

$= 1$ when $\sigma = \gamma$.

$$\langle \chi_\sigma, \chi_\gamma \rangle = \sum_x \chi_\sigma(x)\,\chi_\gamma(x)$$

Let's first look at $\sum_x \chi_\sigma(x)$

When $\sigma = 0^n$, $\chi_\sigma(x) = 1 \quad \forall\, x$

$$\therefore \sum_x \chi_\sigma(x) = 2^n$$

when $\sigma \neq 0^n$, $\chi_\gamma(x) = \prod_{i:\sigma_i=1} (-1)^{x_i}$

$$\sum_x \prod_{i:\sigma_i=1} (-1)^{x_i}$$

$$= \prod_{i:\sigma_i=1} \sum_{x_i \in \{0,1\}} (-1)^{x_i}$$

$$= \prod_{i:\sigma_i=1} \left( (-1)^1 + (-1)^0 \right)$$

$$= \prod_{i:\sigma_i=1} (-1+1) = 0.$$

$$\mathop{\mathbb{E}}_{x \leftarrow \{0,1\}^n} \chi_\sigma(x) = \begin{cases} 1 & \text{if } \sigma = 0^n \\ 0 & \text{otherwise} \end{cases}$$

$$\sum_x \chi_\sigma(x)\,\chi_\tau(x)$$

$$= \sum_x \left[ \prod_{i:\sigma_i=1} (-1)^{x_i} \prod_{i:\tau_i=1} (-1)^{x_i} \right]$$

$$= \sum_x \left[ \prod_{i:(\sigma_i \oplus \tau_i)=1} (-1)^{x_i} \right]$$

$$= \begin{cases} 2^n & \text{when } \sigma \oplus \tau = 0^n \\ 0 & \text{when } \sigma \oplus \tau \neq 0^n. \end{cases}$$

$$\mathbb{E} = \begin{cases} 1 & \text{when } \sigma \oplus \tau = 0^n \\ 0 & \text{otherwise.} \end{cases}$$

This proves $\{\chi_\sigma\}_{\sigma \in \{0,1\}^n}$ is a basis. "Fourier basis".

# Simons algorithm.

## Problem.

Given $f : \{0,1\}^n \to \{0,1\}^n$

s.t. (1) $f$ is two-to-one.

(2) $f(x) = f(x \oplus s)$ for some $s \neq 0^n$ and $\forall x$.

Goal : find $s$.

---

1) First prepare $\frac{1}{2^{n/2}} \sum_x |x\rangle$

$\left( = H^{\otimes n}(|0^n\rangle) \right)$.

2) $\sum_x |x\rangle|0\rangle$

$\downarrow U_f$

$\sum_x |x\rangle|f(x)\rangle$.

3) Measure last $n$ registers (in computational basis)

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

where $f(x') = y$

Goal: find $s$.

4) Apply Fourier transform to first $n$ regs.

$$H^{\otimes n}\left(|x\rangle + |x \oplus s\rangle\right)$$

$$= H^{\otimes n}|x\rangle + H^{\otimes n}|x \oplus s\rangle$$

$$= \sum_{r \in \{0,1\}^n} (-1)^{x \cdot r}|r\rangle + \sum_{r \in \{0,1\}^n} (-1)^{(x \oplus s) \cdot r}|r\rangle$$

$$= \sum_{r \in \{0,1\}^n} \left((-1)^{x \cdot r} + (-1)^{(x \oplus s) \cdot r}\right)|r\rangle.$$

$$= \sum_{\gamma} (-1)^{x \cdot \gamma} \left[1 + (-1)^{s \cdot \gamma}\right] |\gamma\rangle$$

when $s \cdot \gamma = 0$, then this term is 1

when $s \cdot \gamma = 1$, then this term is $-1$.

$\Rightarrow$ Amplitude on $|\gamma\rangle$ is 0 when $s \cdot \gamma = 1$.

$$= \sum_{\gamma \text{ s.t. } s \cdot \gamma = 0} (-1)^{x \cdot \gamma} |\gamma\rangle$$

If we measure this state we will get some $\gamma$ s.t. $\gamma \cdot s = 0$.

$\gamma_1, \gamma_2 \ldots \gamma_n$ s.t. $\forall i$, $\gamma_i \cdot s = 0$

$n$ equations in $n$ variables (if linearly independent), solve to find $s$.

$\gamma_1, \gamma_2 \ldots \gamma_k$. $\gamma_{k+1}$ uniformly

$O(n)$ $\gamma$'s are bitstrings.