CS6846 – Quantum Algorithms and Cryptography

Simon's Algorithm over $\mathbb{Z}_N$

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

Review of QFT over $\mathbb{Z}_2^n$:

Basis of "Parity" functions

$$\chi_\gamma(x) = (-1)^{\gamma \cdot x}$$

$\gamma \cdot x$: inner product mod 2

↳ "characters" on $\mathbb{Z}_2^n$

$$g = \sum_{\gamma \in \mathbb{Z}_2^n} \hat{g}(\gamma) |\chi_\gamma\rangle$$

Definition: Let $\mathbb{C}^*$ denote nonzero complex numbers & G be a group with operation $*$.

A character on G is a function

$$\chi: G \to \mathbb{C}^*$$ satisfying

$$\chi(g * h) = \chi(g) \cdot \chi(h).$$

Properties:

1). $\chi_0 = 1$

2) $\mathop{E}_{x \leftarrow \{0,1\}^n}[\chi_\gamma(x)] = 0$ where $\gamma \neq 0$

3. $\chi_\alpha(x) = \chi_x(\alpha)$

4. $\hat{g}(\gamma) = \underset{x}{E}\left[\chi_\gamma(x)\, g(x)\right]$

$= \langle \chi_\gamma \mid g \rangle$

5. $\chi_{\gamma+\sigma}(x) = \chi_\gamma(x)\, \chi_\sigma(x)$.

F.T is the unitary transformation that takes any g to its representation w.r.t χ_γ

$$\frac{1}{\sqrt{N}} \sum_x g(x)|x\rangle = \sum_\gamma \hat{g}(\gamma)|\gamma\rangle.$$

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{r \in \mathbb{Z}_2^n} (-1)^{r \cdot x} |x_r\rangle$$

If $g_x(y) = \sqrt{N}$ when $y = x$

$= 0$ o.w.

$$g_x = \frac{1}{\sqrt{N}} \sum_y g_x(y) |y\rangle = |x\rangle.$$

$\mathbb{Z}_N$:

- $\chi(x) = \chi(x+0) = \chi(x)\chi(0)$

$\Rightarrow \chi(0) = 1.$

- $\chi(\underbrace{x + x + \cdots + x}_{k \text{ times}}) = \chi(x)^k.$

If $k = N$,

$$\chi(x)^N = 1.$$

$\chi(x)$ is an N^{th} root of unity.

$\chi(k) = \chi(1)^k$, χ is completely determined by its value on 1.

We can write

$$\chi(1) = \omega^r \text{ where}$$

$e^{\frac{2\pi i}{N}} = \omega$ is primitive N^{th} root of 1

$r \in \mathbb{Z}_N$.

$$\therefore \chi(x) = \chi(1)^x = (\omega^r)^x$$

$$= \omega^{r \cdot x}.$$

Let's define

$$\chi_\gamma : \mathbb{Z}_N \to \mathbb{C} \quad \text{as}$$

$$\chi_\gamma(x) = \omega^{\gamma \cdot x}$$

Then $\chi_\gamma(x+y) = \chi_\gamma(x)\,\chi_\gamma(y)$.

The set $\{\chi_\gamma\}_{\gamma \in \mathbb{Z}_N}$ forms an orthonormal basis.

- $\chi_0 = 1$.
- $\mathop{E}_{x \leftarrow \mathbb{Z}_N}[\chi_\gamma(x)] = 0$ for $\gamma \neq 0$.

$$\underset{x}{E}\left[\chi_\gamma(x)\right] = \frac{1}{N}\sum_{x=0}^{N-1} \omega^{\gamma x}$$

$$= \frac{1}{N}\left(\frac{\omega^{\gamma N} - 1}{\omega^{\gamma} - 1}\right) = 0.$$

- $\chi_\alpha(x) = \chi_x(\alpha)$.

- $\chi_\sigma(x)\,\chi_\gamma(x) = \chi_{\sigma+\gamma}(x)$.

- $\chi_\gamma(x)^* = \chi_{-\gamma}(x) = \chi_\gamma(-x)$

  ↳ $(\omega^{\gamma x})^* = \omega^{-\gamma x}$

Claim: $\{\chi_\gamma\}_{\gamma \in \mathbb{Z}_N}$ form an orthonormal basis.

$$\langle \chi_\sigma \mid \chi_\gamma \rangle = \underset{x}{E} \left[\chi_\sigma(x)^* \, \chi_\gamma(x) \right]$$

$$= \underset{x}{E} \left[\chi_{-\sigma}(x) \, \chi_\gamma(x) \right]$$

$$= \underset{x}{E} \left[\chi_{\underbrace{\gamma - \sigma}_{=0}}(x) \right]$$

$$= 1 \quad \text{if} \quad \gamma - \sigma = 0$$

$$= 0 \quad \text{otherwise.}$$

$$\hat{g}(\gamma) = \langle \chi_\gamma | g \rangle$$

$$= \mathop{E}_{x} \left[\chi_\gamma^*(x) \; g(x) \right]$$

The unitary transformation that takes a function to its Fourier representation is the Fourier transform

$$\frac{1}{\sqrt{N}} \sum_{x \in Z_N} g(x) |x\rangle \longrightarrow \sum_{\gamma \in Z_N} \hat{g}(\gamma) |\gamma\rangle .$$

Example : $g_x(y) = \sqrt{N}$ when $y = x$

$= 0$ o.w.

The vector representation of g_x is $|x\rangle$

i.e. $\hat{g}_x(r) = \underset{y}{E}\left[\chi_r^*(y)\, g_x(y)\right] = \chi_r(x)^*$.

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{r \in \mathbb{Z}_N} \chi_r(x)^* |r\rangle$$

Implementing Fourier Transform over $\mathbb{Z}_N$

$$|x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}_N} \chi_y(x)^* |y\rangle$$

where $\chi_y(x)^* = \omega^{-yx}$.

Consider $n = 4$, $N = 2^4 = 16$.

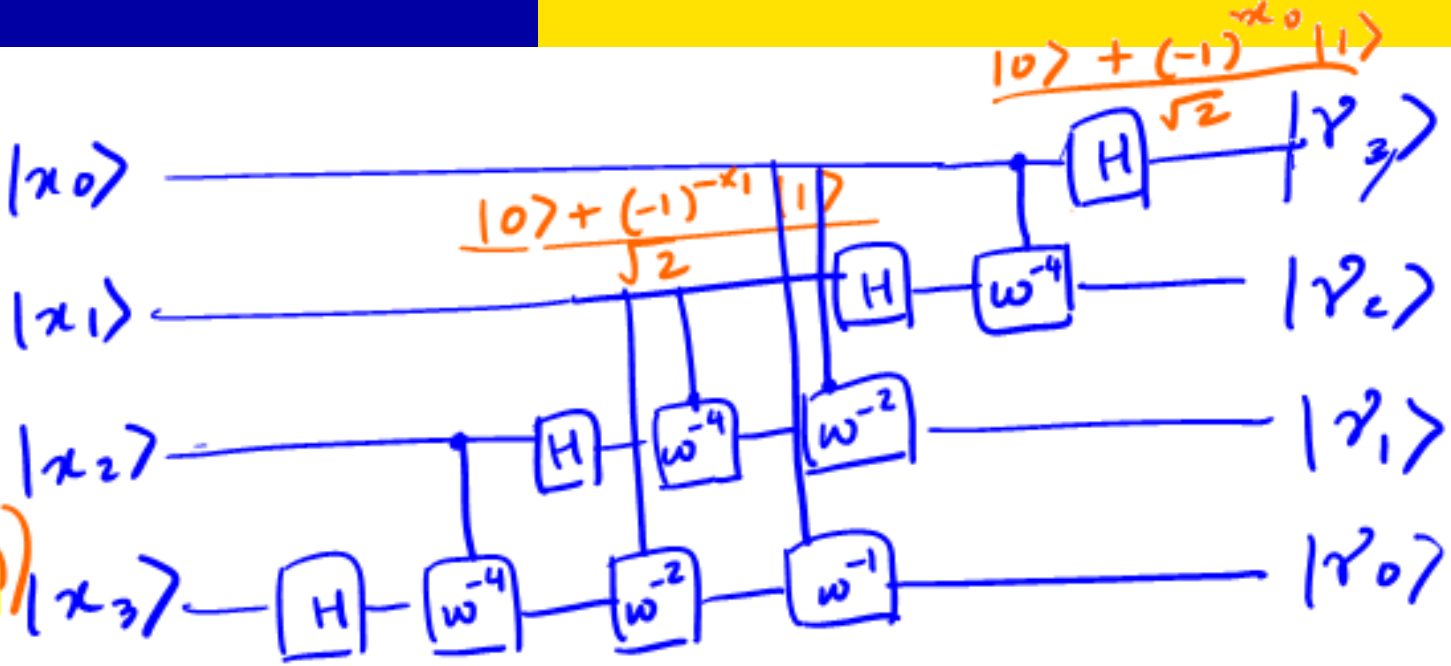
$$|x\rangle \rightarrow \frac{1}{4}\Big(1 \cdot |0000\rangle + \omega^{-x}|0001\rangle + \omega^{-2x}|0010\rangle + \omega^{-3x}|0011\rangle + \cdots \omega^{-15x}|1111\rangle \Big)$$

Key observation is that the previous state is unentangled. That is, $\exists$ $|\psi_0\rangle\,|\psi_1\rangle\,|\psi_2\rangle\,|\psi_3\rangle$ s.t. the above state is tensor of these.

$$\left(\frac{|0\rangle + \omega^{-8x}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + \omega^{-4x}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + \omega^{-2x}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + \omega^{-x}|1\rangle}{\sqrt{2}}\right)$$

$\omega^{-4x_0 - 8x_1} = (-1)^{-x_1}\,\omega^{-4x_0}$

Q: ω^{-8x} ? $x = \sum_{i=0}^{n-1} 2^i x_i$



$O(n^2)$

$= O(\text{poly}(\log N))$

Classically

$O(N \log N)$.

$N = 2^n$

$\omega^{-8x} = \omega^{-8\left(\sum_{i=0}^{3} 2^i x_i\right)} = \omega^{-8x_0}$

$= (-1)^{x_0}$

$\omega = e^{\frac{2\pi i}{16}}$

$\omega^8 = e^{\pi i} = -1.$

$\omega^{-8x_0} = (\omega^8)^{-x_0} = (-1)^{-x_0}$

$$|x_1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{-x_1}\omega^{-4x_0}|1\rangle\right)$$

$$|x_2\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{-x_2}\omega^{-4x_1-2x_0}|1\rangle\right)$$

$$|x_3\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{-x_3}\omega^{-4x_2-2x_1-x_0}|1\rangle\right)$$

Use Controlled Phase shift gates for ω^{blah}.