CS6846 – Quantum Algorithms and Cryptography

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

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

Period Finding Problem :

Given $f : \mathbb{Z}_N \to$ "Colors"

↳ unstructured set

where for some $s \in \mathbb{Z}_N \setminus \{0\}$

it holds that $f(x) = f(x+s)$.

Otherwise f values are distinct

ie if x & y do not differ by a multiple of s, $f(x) \neq f(y)$.

Goal : find s.

ALGORITHM:

1). Prepare superposition state of inputs

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x\rangle.$$

2). Attach $|0^m\rangle \Rightarrow \frac{1}{\sqrt{N}} \sum_x |x\rangle |0^m\rangle$

3). Apply function oracle

$$\frac{1}{\sqrt{N}} \sum_x \underline{\underline{|x\rangle}} \, |f(x)\rangle$$

collapse to a given colour

4) Apply QFT to the input registers.

5). Do some classical computation.

Notation: For each color c, $f_c : \mathbb{Z}_N \to \{0,1\}$

$$f_c(x) = 1 \text{ if } f(x) = c$$
$$= 0 \text{ otherwise.}$$

Now $\frac{1}{\sqrt{N}} \sum_x |x\rangle |f(x)\rangle$ can be rewritten

as $\sum_c \frac{1}{\sqrt{N}} \sum_x f_c(x) |x\rangle |f(x)\rangle$

6 colors.

Probability of measuring a fixed color c is $\sum_x \left(\frac{1}{\sqrt{N}} f_c(x)\right)^2 = \frac{1}{N}\sum_x f_c(x)$

$$= \mathop{E}_x \left[f_c(x)\right] = \Pr\left(f(x) = c\right) = \frac{1}{s}.$$

Now we have our resulting state as

$$\sqrt{\frac{s}{N}} \left(\sum_x f_c(x)\,|x\rangle\right)|c\rangle$$

We consider i/p registers:

$$\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} \sqrt{s}\, f_c(x)\ |x\rangle.$$

Apply QFT.

- let $g = \sqrt{s}\, f_c$,
- let $1_U : \mathbb{Z}_N \to \{0,1\}$ s.t.

$$1_U(x) = 1 \text{ if } x \in U$$
$$= 0 \text{ o.w.}$$

Claim: Let $g : \mathbb{Z}_N \to \mathbb{C}$, & $t \in \mathbb{Z}_N$.
Let $g^{+t}(x) = g(x+t)$ then g and g^{+t} have "essentially" the same Fourier coefficients

Proof: $\hat{g}^{+t}(\gamma) = \underset{x}{E}\left[g^{+t}(x)\, \chi_\gamma(x)^*\right]$

$$= \underset{x}{E}\left[g(x+t)\, \chi_\gamma(x)^*\right]$$

Change vars

$x+t = y$

$$= \underset{y}{E}\left[g(y)\, \chi_\gamma(y-t)^*\right]$$

$$= \underset{y}{E}\left[g(y)\, \chi_\gamma(y)^*\, \chi_\gamma(t)\right]$$

$$= \chi_\gamma(t)\, \underset{y}{E}\left[g(y)\, \chi_\gamma(y)^*\right]$$

$$= \omega^{\gamma t}\, \hat{g}(\gamma)$$

This implies:

$$|\widehat{g^{+t}}(\gamma)|^2 = |\omega^{\gamma t}\,\hat{g}(\gamma)|^2$$
$$= |\hat{g}(\gamma)|^2.$$

Proposition: Let $H = \{0, s, 2s, \dots\} \subseteq \mathbb{Z}_N$

& let $h = 1_H$.

$$\hat{h}(\gamma) = \frac{1}{s} \text{ if } \gamma \in \{0, \tfrac{N}{s}, 2\tfrac{N}{s} \dots\}$$
$$= 0 \text{ otherwise}$$

Consider our state

$$\frac{1}{\sqrt{N}} \sum_x \sqrt{s}\, f_c(x)\,|x\rangle \Rightarrow \frac{1}{\sqrt{N}} \sum_x \sqrt{s}\, h(x)\,|x\rangle$$

Applying QFT, we get

$$\sum_{\gamma} \sqrt{s}\, \hat{h}(\gamma) |\gamma\rangle$$

Measure we get γ with prob $s \cdot |\hat{h}(\gamma)|^2$.

Since $\hat{h}(\gamma) = \frac{1}{s}$ iff $\gamma \in H$, we

get $\gamma \in H$ with prob $s \cdot \left(\frac{1}{s}\right)^2 = \frac{1}{s}$.

Proof of Proposition: $h(x)$ is nonzero only when $x \in H$.

$$\hat{h}(\gamma) = \underset{x \in \mathbb{Z}_N}{E}\left(h(x) \cdot \chi_\gamma(x)^* \right) = \frac{1}{s} \underset{x \in H}{E}\left(\chi_\gamma(x)^* \right)$$

When $\gamma \in \{0, \frac{N}{s}, 2N/s \ldots\}$, $\chi_\gamma(x)^* = \omega^{-\gamma x}$

Since x was sampled from H and $\gamma \in \{0, \frac{N}{s} \cdots\}$, $x \cdot \gamma$ is a multiple of N, so $\chi_\gamma(x)^* = 1$.

$$\hat{h}(\gamma) = \frac{1}{s} \mathop{E}_{x \in H}[\chi_\gamma(x)^*] = \frac{1}{s}.$$

The set $\{0, \frac{N}{s}, \frac{2N}{s} \cdots\}$ has cardinality s. (exercise).

Prob of sampling γ in this set is $\left(\sqrt{s}\, \hat{h}(\gamma)\right)^2 = s \cdot \left(\frac{1}{s}\right)^2 = \frac{1}{s}$.

Total Prob of this set is 1.

Claim: If a & b are sampled from $\{0, 1 \ldots s-1\}$, iid & uniform,

$$\Pr\left(\gcd(a,b)=1\right) \geq \Omega(1).$$

As long as gcd of samples gives us $\frac{N}{s}$, we can recover s (N is known).