Period Finding

Jiman Hwang

Disclaimer: This document is for self-study only and may contain false information. Mainly referenced from [NC00], [GHH08]

1 Problem

Given $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ such that

$$\begin{aligned} &\forall x\ f(x) = f(x+r) \qquad \text{for some } r \in \mathbb{N} \\ &\forall x, y \in \{0, \cdots, r-1\}\ x \neq y \to f(x) \neq f(y) \end{aligned}$$

find r.

2 Solution

2.1 The circuit

Build a quantum gate of $(m+n)$ qubits, $U : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ such that

$$2r^2 \leq N \leq M \tag{1}$$

where

$$M \stackrel{\text{def}}{=} 2^m, N \stackrel{\text{def}}{=} 2^n, \oplus \text{ is XOR.}$$

Using the above quantum gate, Hadamard gates H, and Quantum Fourier Transform gate QFT [Ros03], build the following circuit.

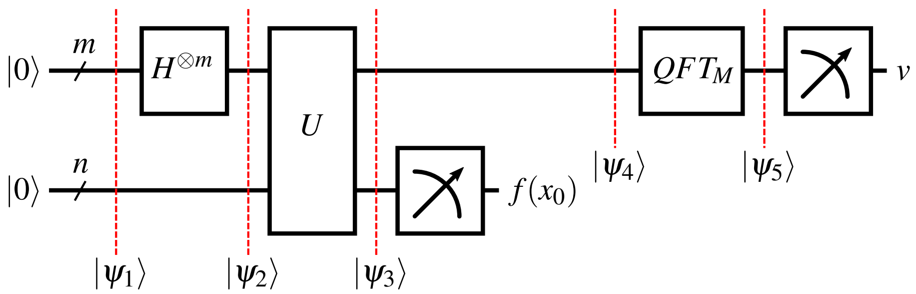

Figure 1: Circuit for period finding

Let's take a look at each state $|\psi\rangle$ one by one. The first initial state is

$$|\psi_1\rangle = |0\rangle|0\rangle$$

Generating a superposition on the first register,

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle |0\rangle$$

Next, U produces

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle |f(x)\rangle$$

We measure the second register, which results $f(x_0)$. From now, we consider only the state of first register. The first register is composed of states that produce $f(x_0)$. Assuming the number of states of that kind is *mu*.

$$|\psi_4\rangle = \frac{1}{\sqrt{\mu}} \sum_{y=0}^{\mu-1} |x_0 + yr\rangle$$

where

$$\mu = \lfloor M/r \rfloor \text{ or } \lfloor M/r \rfloor + 1 \tag{2}$$

according to x_0, r, M. To elicit r, do the phase analysis on it by applying QFT.

$$\begin{aligned}
|\psi_5\rangle =& \frac{1}{\sqrt{\mu}} \sum_{y=0}^{\mu-1} QFT_M |x_0 + yr\rangle \\
=& \frac{1}{\sqrt{\mu}} \sum_{y=0}^{\mu-1} \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{i2\pi x(x_0+yr)/M} |x\rangle \\
=& \frac{1}{\sqrt{M\mu}} \sum_{x=0}^{M-1} e^{i2\pi x x_0/M} \sum_{y=0}^{\mu-1} e^{i2\pi xyr/M} |x\rangle
\end{aligned}$$

where $i = \sqrt{-1}$. Let $p(v)$ be the probability of getting v after measuring the first register. Then,

$$p(v) = \frac{1}{M\mu} |c(v)|^2$$

where

$$c(v) = \sum_{y=0}^{\mu-1} e^{i2\pi vyr/M}$$

2.2 Characteristic of outcome

Let $E(v)$ be the distance between v and the nearest $\frac{M}{r}k$ where $k \in \mathbb{Z}$. Then,

$$\exists k \in \mathbb{Z} \quad E(v) = \left| v - \frac{M}{r}k \right| < 1 \tag{3}$$

with high probability.

Proof. We consider two cases, $r|M$ and $r \nmid M$.

i) $r|M$

The number of states that produces specific result $f(x_0)$ is a constant.

$$\mu = \frac{M}{r}$$

Again, considering two cases of $\frac{M}{r}\big|v$ and $\frac{M}{r} \nmid v$. If $\frac{M}{r}\big|v$,

$$e^{i2\pi vr/M} = 1 \quad \Rightarrow \quad c(v) = \frac{M}{r} \quad \Rightarrow \quad p(v) = \frac{1}{r}$$

If $\frac{M}{r} \nmid v$,

$$e^{i2\pi vr/M} \neq 1 \quad \Rightarrow \quad c(v) = \sum_{y=0}^{M/r-1} \left(e^{i2\pi vr/M}\right)^y = \frac{1-e^{i2\pi v}}{1-e^{i2\pi vr/M}} = 0 \quad \Rightarrow \quad p(v) = 0$$

$\therefore$ (3) is held.

ii) $r \nmid M$

We prove (3) by showing that $\forall v_0\ E(v_0) \leq 1,\ \forall v'\ E(v') > 1$,

$$\frac{p(v_0)}{p(v')} \geq 9 \tag{4}$$

To prove it, we obtain a lower bound of $p(v_0)$ and an upper bound of $p(v')$.

Lower bound first. If $v = 0$, $E(v) = 0$. Getting $p(v)$,

$$p(0) = \frac{1}{M\mu}\mu^2 = \frac{\mu}{M} \tag{5}$$

Keeping it for later, now assume $v \neq 0$. Since $r \nmid M$, or $r \nmid 2^m$, r has at least one prime factor other than 2. Hence,

$$M \nmid vr \quad \Rightarrow \quad e^{i2\pi vr/M} \neq 1$$

This follows

$$c(v) = \sum_{y=0}^{\mu-1} \left(e^{i2\pi vr/M}\right)^y = \frac{1-e^{i2\pi v\mu r/M}}{1-e^{i2\pi vr/M}}$$

Let $\alpha \stackrel{\text{def}}{=} 2\pi vr/M$. Then,

$$\begin{aligned} |c(v)|^2 &= \left|\frac{1-e^{i\alpha\mu}}{1-e^{i\alpha}}\right|^2 = \left|\frac{1-\cos\alpha\mu - i\sin\alpha\mu}{1-\cos\alpha - i\sin\alpha}\right|^2 \\ &= \frac{(1-\cos\alpha\mu)^2+\sin^2\alpha\mu}{(1-\cos\alpha)^2+\sin^2\alpha} = \frac{2-2\cos\alpha\mu}{2-2\cos\alpha} = \frac{\sin^2\frac{\alpha\mu}{2}}{\sin^2\frac{\alpha}{2}} \end{aligned}$$

Replacing α back,

$$|c(v)|^2 = \frac{\sin^2(\pi v\mu r/M)}{\sin^2(\pi vr/M)} \tag{6}$$

Let

$$\delta \overset{\text{def}}{=} v - \frac{M}{r}k \quad \text{for some } k \in \mathbb{Z} \tag{7}$$

Then,

$$\pi v \frac{r}{M} = \pi \left(\frac{M}{r}k + \delta \right) \frac{r}{M} = \pi k + \pi \delta \frac{r}{M}$$

Applying it to (6),

$$|c(v)|^2 = \frac{\sin^2(\pi \delta \mu r/M)}{\sin^2(\pi \delta r/M)} \overset{\text{def}}{=} h(\delta) \tag{8}$$

Given k, if $-\frac{1}{2} \leq \delta < \frac{1}{2}$, then there is exactly one v that satisfies (7). So

$$v_0 \overset{\text{def}}{=} \frac{M}{r}k + \delta \quad \left(\frac{1}{2} \leq \delta < \frac{1}{2} \right)$$

Note that

$$|\sin x| \geq \left| \frac{x}{\pi/2} \right| \quad \text{for } x \in \left[-\frac{\pi}{2}, \frac{\pi}{2} \right]$$

This follows

$$\sin^2 x \geq \frac{4x^2}{\pi^2} \tag{9}$$

Also, since $\pi \delta r/M \ll 1$ by (1),

$$\sin \frac{\pi \delta r}{M} \approx \frac{\pi \delta r}{M} \tag{10}$$

Using (9) and (10),

$$h(\delta) \geq \frac{\frac{4}{\pi^2} (\pi \delta \mu r/M)^2}{(\pi \delta r/M)^2} = \frac{4\mu^2}{\pi^2}$$

$$\therefore p(v_0) = \frac{1}{M\mu} |c(v_0)|^2 = \frac{1}{M\mu} h(\delta) \geq \frac{4\mu}{\pi^2 M} \tag{11}$$

This bound is persistent even if we remember (5). Note that this lower bound covers $\forall v_0 \; E(v_0) \leq 1$ because $p(v) \geq 0$ and $-\frac{1}{2} \leq \delta < \frac{1}{2}$ implies $|\delta| \leq 1$ and $E(v_0) \leq 1$.

Now look at the case of $1 < |\delta| \leq \frac{M}{2r}$. We'll get an upper bound of $f(\delta)$. To begin with,

$$g(x) \overset{\text{def}}{=} \frac{\sin x\mu\beta}{\sin x\beta} \quad \text{for } 1 \leq x \leq \frac{M}{2r}$$

where $\beta = \pi r/M$. We'll obtain the maximum value of $g(x)$ and utilize it to get an upper bound of the case $\forall v' \; E(v') > 1$. To achieve it, get the values at critical points and compare them with $g(1)$ and $g\left(\frac{M}{2r}\right)$. Differentiating $g(x)$,

$$g'(x) = \frac{\mu\beta \cos x\mu\beta \cdot \sin x\beta - \sin x\mu\beta \cdot \beta \cos x\beta}{\sin^2 x\beta}$$

Let $x_0 \in \left(1, \frac{M}{2r}\right)$ such that $g'(x_0) = 0$. Then,

$$\begin{aligned} &\mu \cos x_0 \mu \beta \cdot \sin x_0 \beta = \sin x_0 \mu \beta \cdot \cos x_0 \beta \\ \Rightarrow\ &\mu \tan x_0 \beta = \tan x_0 \mu \beta \end{aligned}$$

Putting back β,

$$\mu \tan \frac{\pi x_0 r}{M} = \tan \frac{\pi x_0 \mu r}{M} \tag{12}$$

Meanwhile, from (2),

$$\mu \leq \frac{M}{r} \leq \mu + 2$$

Giving a boundary of $r\mu/M$,

$$1 - \frac{2r}{M} < \frac{r\mu}{M} \leq 1 \tag{13}$$

From (1) and (13),

$$\mu r/M \approx 1 \tag{14}$$

From (12) and (14),

$$\mu \tan \frac{\pi x_0 r}{M} > \pi x_0$$

This states that the left hand side of (12) is large enough to approximate its solution as

$$\frac{\pi x_0 \pi r}{M} \approx \frac{\pi}{2} + \pi n \tag{15}$$

where $n \in \mathbb{N} \because x_0 > 1$ and (14). Now enumerating major values,

$$\begin{aligned} g(1) =& \frac{\sin(\pi\mu r/M)}{\sin(\pi r/M)} = \frac{\sin(\pi - \pi\mu r/M)}{\sin(\pi r/M)} \approx \frac{\pi - \pi\mu r/M}{\pi r/M} \\ =& \frac{M}{r} - \mu \leq \frac{M}{r} - \left\lfloor \frac{M}{r} \right\rfloor < 1 \end{aligned}$$

$$g\left(\frac{M}{2r}\right) = \sin \frac{\pi}{2}\mu \leq 1$$

$$g(x_0) = \frac{1}{\sin\left[\frac{\pi}{\mu}\left(\frac{1}{2} + n\right)\right]} \leq \frac{1}{\sin\left[\frac{\pi}{\mu}\left(\frac{1}{2} + 1\right)\right]} = \frac{1}{\sin \frac{3\pi}{2\mu}} \approx \frac{2\mu}{3\pi}$$

Among the values, $\frac{2\mu}{3\pi}$ is the largest one. Hence,

$$f(\delta) \leq \{g(\delta)\}^2 \leq \frac{4\mu^2}{9\pi^2} \quad \text{for } 1 < |\delta| \leq \frac{M}{2r}$$

If $v' = \frac{M}{r}k + \delta$ such that $1 < |\delta| \leq \frac{M}{2r}$, then

$$p(v') = \frac{1}{M\mu}\left|c(v')\right|^2 = \frac{f(\delta)}{M\mu} \leq \frac{4\mu}{9\pi^2 M} \tag{16}$$

Combining two bounds, (11) and (16),

$$\frac{p(v_0)}{p(v')} \geq \frac{4\mu}{\pi^2 M} \frac{9\pi^2 M}{4\mu} = 9$$

Thus, when we measure $|\psi_5\rangle$, the integer v is at lease 9 times likely to satisfy $E(v) \leq 1$ than $E(v) > 1$.

□

Here is a sample case.

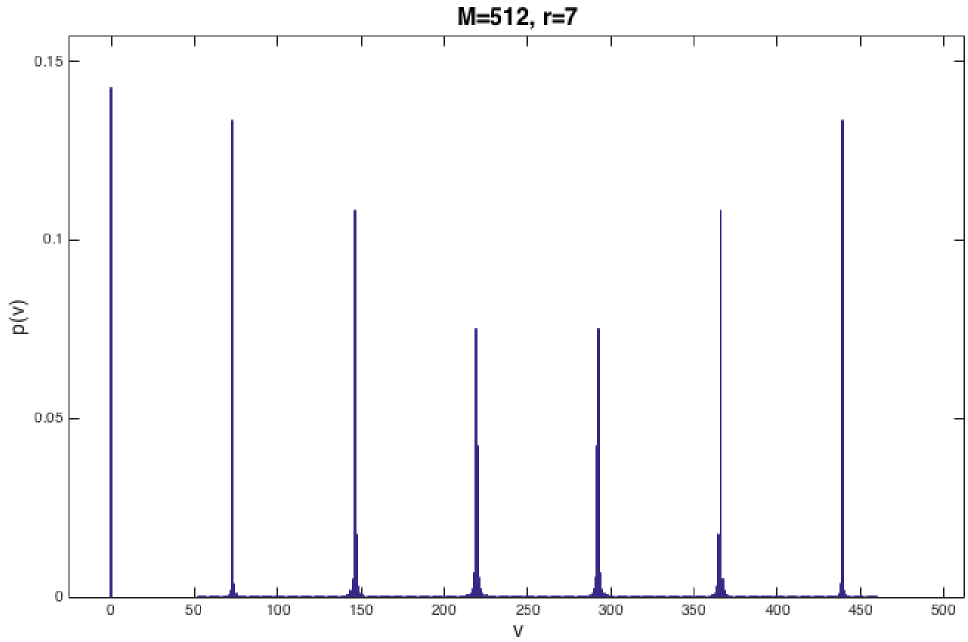

Figure 2: Sample distribution of $p(v)$

2.3 Drawing out the period

Since it is highly probable $E(v) \leq 1$, from now, we assume that v an integer such that $E(v) \leq 1$. It follows

$$\left| v - \frac{M}{r} k \right| \leq 1 \quad \Rightarrow \quad \left| \frac{v}{M} - \frac{k}{r} \right| \leq \frac{1}{M} \leq \frac{1}{2r^2}$$

Using continued fractions technique, Theorem A4.16 at [NC00], $\frac{k}{r}$ appears among convergents of $\frac{v}{M}$, giving r unless $gcd\{k,r\} \neq 1$. A couple of ways are introduced to overcome the case $gcd\{k,r\} \neq 1$ in p.229 at [NC00]. Among them, one simple way is to repeat this procedure until k is a prime so that $gcd\{k,r\} = 1$.

Problem 4.1 on p.638 at [NC00] states that there are at least $\frac{r/2}{\lg r}$ primes in $\{1, \cdots, r\}$. Therefore, considering that k's are uniformly distributed over $\{1, \cdots, r\}$, the probability that k is a prime is at least $\frac{1}{2\lg r}$. Furthermore, we know

$$\frac{1}{2\lg r} > \frac{1}{2\lg N}$$

Let $p \stackrel{\text{def}}{=} \frac{1}{2\lg N}$ and assume p is sufficiently small(this happens frequently since this algorithm is usually applied when N is large). The probability of obtaining a prime k within s tries is

$$1-(1-p)^s \approx 1-(1-sp) = sp$$

Hence, $s = 2\lg N$ tries pretty ensure that we earn prime k and r.

2.4 Summary

In sum,

1. Run the circuit.
2. Obtain an approximation of $\frac{M}{r}k$.
3. Elicit k' and r' using continued fractions technique.
4. Check if $r' = r$ by checking $f(0) = f(r')$.
5. If $r' = r$, done. Otherwise, go to 1.

The repetition will end within $2\lg N$ with high probability.

References

[GHH08] Andrew Wiles G. H. Hardy, Edward M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.

[NC00] Michael A Nielson and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[Ros03] Burton Rosenberg. Quantum fourier transforms. 2003.