3.3 Periodicity

This section follows Preskill section 6.9 very closely.

Consider an oracle that computes a function

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

that has an unknown period r

$$1 \ll r \ll 2^n;$$

thus,

$$f(x) = f(x + mr)$$

for any x and m such that

$$0 \leq x \leq 2^n - 1, \;\; 0 \leq x + mr \leq 2^n - 1.$$

We wish to find r. Classically this problem is hard, requiring $O(\sqrt{r})$ oracle calls on average. There exists a quantum poly(n) algorithm that we describe next.

3.3.1 An algorithm for period finding

Let $N = 2^n$. Assume the period is known to satisfy $r < M$ where $M \leq \sqrt{N}$.

1. Prepare the state

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0^m\rangle$$

2. Call the oracle

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

3. Measure the output register

$$\to \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle|f(x_0)\rangle$$

where

$$0 \leq x_0 < r,$$

and A is the integer such that

$$N - r \leq x_0 + (A-1)r < N,$$

or

$$A - 1 < \frac{N}{r} < A + 1.$$

4. Apply QFT to the input register

$$\to \frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{2\pi i x_0 y/N} \sum_{j=0}^{A-1} e^{2\pi i j r y/N} |y\rangle$$

5. Measure the input register

$$\to |y\rangle$$

6. Find a rational approximation $p/q \approx y/N$ such that $q \leq M$.

7. Check if $q = r$. Otherwise, repeat the algorithm.

3.3.2 Discussion of the algorithm

In step 5, the probability of observing $|y\rangle$ is

$$P(y) = \frac{A}{N}\left|\frac{1}{A}\sum_{j=0}^{A-1} e^{2\pi ijry/N}\right|^2 .$$

This favors integers y close to integer multiples of N/r. E.g., if N/r is an integer (hence equals A),

$$P(y) = \begin{cases} 1/r & y = A\cdot(\text{integer}) \\ 0 & \text{otherwise.} \end{cases}$$

In general,

$$\sum_{k=0}^{r-1} P\left\{\left|y - k\frac{N}{r}\right| \leq \frac{1}{2}\right\} \geq \frac{4}{\pi^2}$$

Proof. Let

$$\theta_y = (2\pi/N)(yr \pmod N),$$

to write

$$\begin{aligned} P(y) &= \frac{1}{AN}\left|\frac{e^{iA\theta_y}-1}{e^{i\theta_y}-1}\right|^2 \\ &= \frac{1}{AN}\left|\frac{\sin(A\theta_y/2)}{\sin(\theta_y/2}\right|^2 \end{aligned}$$

There are r values of y in $\{0,\ldots,N-1\}$ such that

$$-\frac{r}{2} \leq yr \pmod N \leq \frac{r}{2}. \tag{3.1}$$

For each such y,

$$-\pi\frac{r}{N} \leq \theta_y \leq \pi\frac{r}{N}.$$

So,

$$|A\theta_y/2| \leq \frac{\pi}{2}\frac{Ar}{N} \approx \frac{\pi}{2},$$

where we used the assumption $r \ll N$ and the fact $A \approx N/r$ derived earlier. Now, the sine function satisfies

$$|x| \geq |\sin(x)| \geq (2/\pi)|x|, \quad \text{for } |x| \leq \pi/2,$$

which can be seen by drawing the function. Using these, for each y satisfying (3.1), we have

$$P(y) \geq \frac{4A}{N\pi^2} \geq \frac{4}{\pi^2 r}$$

This completes the proof.

Suppose y satisfies

$$\left|y - k\frac{N}{r}\right| \leq \frac{1}{2}$$

or

$$\left|\frac{y}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}.$$

Then, k/r is an approximation to y/N with an error bound $1/(2N)$. Under the assumption $r < M \leq \sqrt{N}$, k/r turns out to be the only rational number p/q with $q \leq M$ that approximates y/N with error bound $1/(2N)$. This is because

$$|k/r - p/q| = \frac{|qk - rp|}{rq} > 1/M^2 \geq 1/N$$

and thus two distinct fractions both with denominators less than M cannot both be within distance $1/(2N)$ of y/N. The approximation k/r can be found by continued fractions algorithm that is discussed below.

With probability better than $4/\pi^2$ we determine a value k/r where k is selected roughly equiprobably from $\{0, 1, \ldots, r-1\}$. If k and r are relatively prime, $\mathrm{GCD}(k, r) = 1$, then r will be determined. If $\mathrm{GCD}(k, r) \neq 1$, we only determine a factor of r. In this case the check $f(x) = f(x + r)$ fails and we repeat the algorithm.

The probability that a number k chosen uniformly from $\{0, \ldots, r-1\}$ is relatively prime to r is

$$\phi(r)/r \geq c/\log\log(r)$$

where $\phi(r)$ is the Euler's ϕ function and c is a constant independent of r. So, in $O(\log\log(r))$ repetitions of the algorithm we have $O(1)$ probability of determining r.

This completes the discussion of the period-finding algorithm.

3.3.3 The continued fractions algorithm

In step 6, we find an approximation p/q to y/N by continued fractions algorithm.

Example. Approximate 105/23.

$$\begin{aligned}
105/23 &= 4 + 13/23 = 4 + \frac{1}{23/13} \\
&= 4 + \frac{1}{1 + 10/13} = 4 + \frac{1}{1 + \frac{1}{13/10}} \\
&= 4 + \frac{1}{1 + \frac{1}{1+3/10}} = 4 + \frac{1}{1 + \frac{1}{1+\frac{1}{10/3}}} \\
&= 4 + \frac{1}{1 + \frac{1}{1+\frac{1}{3+1/3}}}
\end{aligned}$$

The fraction is written also as

$$\frac{105}{23} = [4, 1, 1, 3, 3].$$

The convergents are:

$$[4, 1] = 4 + \frac{1}{1} = 5$$

$$[4, 1, 1] = 4 + \frac{1}{1 + \frac{1}{1}} = 9/2$$

$$[4, 1, 1, 3] = 4 + \frac{1}{1 + \frac{1}{1+\frac{1}{3}}} = 32/7$$

$$[4,1,1,3,3] = 4 + \cfrac{1}{1 + \frac{1}{1+\frac{1}{3+\frac{1}{3}}}} = 105/23$$

We cite the following properties of the continued fractions algorithm without proof.

- The expansion of a rational p/q with p and q L-bit integers is obtained in $O(L)$ 'split-and-invert' operations.

- Khintchine (1935). Let α be a real number and suppose we seek a rational number p/q closest to α such that $q \leq Q$.

  Let $\alpha = [a_0, a_1, \ldots]$ and let $p_k/q_k = [a_0, \ldots, a_k]$ be the kth convergent. Let n be the index such that $q_n \leq Q < q_{n+1}$. Let $j \geq 0$ be the largest integer such that $q_n + jq_{n+1} \leq Q$. Then, the best approximation p/q with $q \leq Q$ is either p_n/q_n or

$$\frac{p_{n-1} + jp_n}{q_{n-1} + jq_n}.$$