Periodicity

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.

Period Finding Algorithm 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.

Discussion of Algorithm

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

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

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,

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

Proof. See Preskill, section 6.9.

Discussion (cont'd)

With probability $\geq 4/\pi^2$, we have

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

or

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

Recalling the assumption that $M \leq \sqrt{N}$, this becomes

$$-\frac{1}{2M^2} \leq \frac{y}{N} - \frac{k}{r} \leq \frac{1}{2M^2}.$$

We also have the assumption that $r < M$.

Now any two distinct rationals k_1/r_1, k_2/r_2 with $r_1 < M$, $r_2 < M$, are at least $1/M^2$ apart.

So, there can be at most one rational number k/r with $r < M$ that satisfies the inequality above. The best rational apporximation p/q to y/N with $q < M$ can be found in $O(n^3)$ steps using the continued fraction algorithm.

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:

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

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

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

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

Properties of Continued Fractions

- 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

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

Discussion of algorithm (cont'd)

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.