CS-506: Quantum Computing

Scribe: Chinmay Kawle
UIN: 650199704
Date: 3rd November 2025

Period Finding and Continued Fractions

We are given an unknown period r satisfying $1 < r < 2^{n_0}$, and define

$$m = \frac{2^n}{r},$$

which need not be an integer. Let $N_f = 2^{n+1}$ and $N \geq 2^n$. We consider the state obtained after measurement in the period-finding algorithm:

$$x = \left\lfloor \frac{k2^n}{r} \right\rfloor + \delta_k, \quad 0 \leq |\delta_k| \leq \frac{1}{2},$$

with probability at least $\frac{4}{\pi^2} > 0.4$.

Unknown parameters: k, r, δ_k, x
Known: $2^n = N$
Goal: find r

From the measurement, we have

$$\frac{x}{2^n} = \frac{k}{r} + \frac{\delta_k}{2^n}.$$

Since $|\delta_k| \leq \frac{1}{2}$, we get

$$\left| \frac{x}{2^n} - \frac{k}{r} \right| = \left| \frac{\delta_k}{2^n} \right| \leq \frac{1}{2^{n+1}} = \frac{1}{2N} \leq \frac{1}{4r^2}.$$

Hence, $\frac{x}{2^n}$ is a rational number that can be expressed as a continued fraction expansion using Euclid's GCD algorithm:

$$\frac{x}{2^n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}, \quad a_0, a_1, \ldots, a_t \geq 0.$$

The time complexity of computing the continued fraction is $O(\log_2^2 N)$.

—

Hardy & Wright Result

From number theory (Hardy & Wright, Chapter on Continued Fractions):

For any rational number b satisfying

$$\left| b - \frac{k}{r} \right| < \frac{1}{2r^2},$$

the value $\frac{k}{r}$ will be a *convergent* of the continued fraction expansion of b.

Thus, each possible convergent can be checked to find r.

The convergent is unique and denoted as

$$[a_0, a_1, \ldots, a_j] = \frac{A}{B},$$

where $B < N$ and j is the largest index satisfying this condition.

—

Proof of Uniqueness

Suppose not. Assume we have two convergents

$$[a_0, \ldots, a_j] = \frac{k'}{r'}, \qquad [a_0, \ldots, a_j, \ldots, a_z] = \frac{k''}{r''},$$

with both $r', r'' < N$, satisfying

$$\left| b - \frac{k'}{r'} \right| < \frac{1}{2r^2}, \qquad \left| b - \frac{k''}{r''} \right| < \frac{1}{2r^2}.$$

Also,

$$[a_0, a_1, \ldots, a_{j+1}] = \frac{k'''}{r'''},$$

with $r''' < N$, since j+1 is between j and z

$$\left| b - \frac{k'''}{r'''} \right| < \frac{1}{2r^2},$$

Then

$$\left| \frac{k'}{r'} - \frac{k'''}{r'''} \right| < \left| \frac{k'}{r'} - b \right| + \left| b - \frac{k'''}{r'''} \right| < \frac{1}{r^2}.$$

But from the property of distinct rational numbers with denominators $r', r''' < r$,

$$\left| \frac{k'}{r'} - \frac{k'''}{r'''} \right| \geq \frac{1}{r'r'''} \geq \frac{1}{r^2},$$

which gives a contradiction. Therefore, such a rational number cannot exist, and the convergent is unique.

—

Summary

We have obtained a rational number $\frac{c_1}{r_1}$ whose value is equal to $\frac{k_1}{r}$ for some $k_1 \in \{1, 2, \ldots, r-1\}$ with probability at least $\frac{4}{\pi^2} > 0.4$.

Repeating the computation yields another estimate $\frac{c_2}{r_2}$ whose value is equal to $\frac{k_2}{r}$, and the true period is given by

$$r = \text{LCM}(r_1, r_2),$$

with success probability greater than equal to $\frac{6}{\pi^2} > \frac{2}{3}$.

—

Factoring Using Non-trivial Square Roots of Unity

Given a positive integer N, the goal is to find a non-trivial factor p such that

$$N = p \cdot q, \quad 1 < p < N.$$

The naive algorithm checks all p from 2 to $N-1$ and is $O(N)$ time, which is not polynomial in the input size $O(\log_2 N)$.

Modular Arithmetic

We define a non-trivial square root of unity modulo N as a number x satisfying

$$x^2 \equiv 1 \pmod{N}, \quad x \not\equiv \pm 1 \pmod{N}.$$

Note: The symbol $\equiv$ denotes congruence modulo N, meaning $x^2 \equiv 1 \pmod{N}$ if N divides $(x^2 - 1)$, i.e., x^2 and 1 have the same remainder when divided by N.

If such an x exists, then

$$(x+1)(x-1) \equiv 0 \pmod{N},$$

but N divides neither $x+1$ nor $x-1$.

Hence, computing

$$\gcd(N, x+1), \quad \gcd(N, x-1)$$

yields two non-trivial factors of N.

Example

Let $N = 15$ and $x = 4$.

$$x^2 = 16 \equiv 1 \pmod{15}.$$

Then,

$$\gcd(15, 4+1) = \gcd(15, 5) = 5, \quad \gcd(15, 4-1) = \gcd(15, 3) = 3.$$

Thus, the non-trivial factors of N are 3 and 5.