CS506: Introduction to Quantum Computing
University of Illinois Chicago
Class Notes
October 27, 2025

Professor: Bhaskar DasGupta
Student: Leonardo Ferreira (lferr10) - UIN: 652276741

1 Recap:

Let

$$N = 2^n, \qquad n = \log_2 N, \qquad R = (\text{unknown period}), \qquad m = \left\lfloor \frac{N}{R} \right\rfloor$$

The QFT-based state before measurement is

$$|\psi\rangle = \text{QFT}_{2^n}|\Phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \left(\sum_{z=0}^{m-1} e^{2\pi i(x_0+zR)y/2^n} \right) |y\rangle$$

When measuring $|\psi\rangle$, we obtain a value y_0 with probability

$$P_R[y_0] = \frac{1}{2^n m} \left| \sum_{z=0}^{m-1} e^{2\pi i z R y_0/2^n} \right|^2$$

2 Case 1: $mR = 2^n$

When $mR = 2^n$, we have $m = \frac{2^n}{R}$ integer. Then $Ry_0/2^n = y_0/m$ is an integer if and only if $y_0 = km$ for some k.

In that case, the sum over z simplifies to m, giving

$$P_R[y_0 = km] = \frac{1}{R},$$

and $P_R[y_0 \neq km] = 0$.

Hence, the possible measurement results are $\{0, m, 2m, \ldots, (R-1)m\}$, all equally likely.

3 Case 2: $mR \neq 2^n$

Now $Ry_0/2^n$ is not necessarily integer. Let $a = e^{2\pi i R y_0/2^n}$. Then the geometric sum yields

$$\sum_{z=0}^{m-1} a^z = \frac{a^m - 1}{a - 1} = \frac{e^{2\pi i R y_0 m/2^n} - 1}{e^{2\pi i R y_0/2^n} - 1}$$

The numerator vanishes only when $Ry_0/2^n$ is integer; otherwise, we get a nonzero amplitude that produces a probability distribution peaked around integer multiples of $\frac{2^n}{R}$.

4 Recovering the Period R

We measure y_0, and ideally $y_0 \approx \lambda \frac{2^n}{R}$. To estimate R, we compute $\frac{y_0}{2^n} \approx \frac{\lambda}{R}$.

The value λ/R can be approximated by a rational number using the *continued fraction expansion* of $\frac{y_0}{2^n}$.

Example: Continued Fraction

For instance, suppose $y_0/2^n = 189/263 \approx 0.7186$. Using the Euclidean algorithm:

$$263 = 1 \times 189 + 74, \quad 189 = 2 \times 74 + 41, \quad 74 = 1 \times 41 + 33, \quad 41 = 1 \times 33 + 8, \quad 33 = 4 \times 8 + 1$$

This corresponds to the continued fraction expansion

$$\frac{189}{263} = [0; 1, 2, 1, 1, 4].$$

The convergents of this continued fraction yield rational approximations that allow us to recover $\frac{\lambda}{R}$.

5 Computing the GCD

To combine multiple measurements, we compute gcd of several observed frequencies.

Given t observed values

$$\frac{\lambda_1 2^n}{R}, \frac{\lambda_2 2^n}{R}, \ldots, \frac{\lambda_t 2^n}{R},$$

we can extract the λ_i and compute $\gcd(\lambda_1, \lambda_2, \ldots, \lambda_t)$.

This is done efficiently using Euclid's algorithm:

$$\mathrm{GCD}(x, y) = \mathrm{GCD}(y, x \bmod y),$$

which runs in $O(\log x \times \log y)$ time.

6 Probability of Success

Let $\lambda_1, \lambda_2, \ldots, \lambda_t$ be uniformly random integers from $\{0, 1, \ldots, R-1\}$. We want $\gcd(\lambda_1, \ldots, \lambda_t) = 1$ so that the true R can be recovered.

$$P[\gcd(\lambda_1, \ldots, \lambda_t) = 1] = 1 - P[\gcd(\lambda_1, \ldots, \lambda_t) > 1] = 1 - \sum_{\lambda \geq 2} P_R[\gcd(\lambda_1, \ldots, \lambda_t) = \lambda]$$

Approximating, we get:

$$P[\gcd(\lambda_1, \ldots, \lambda_t) = 1] \geq 1 - \frac{R}{R^4 - 1} \approx 1 - \frac{1}{R^3}.$$

Hence, with $t = O(\log \log R)$ samples, the probability of success approaches 1.

7 Method 2 (LCM Approach)

Alternatively, we can use the least common multiple:

$$R = \mathrm{LCM}(R_1, R_2),$$

where $R_i = \frac{R}{\gcd(R, \lambda_i)}$

With probability at least $6/\pi^2 > 2/3$, this recovers the true R after a few repetitions.