COL7160 : Quantum Computing

Lecture 14: Shor's Algorithm (Order Finding)

Instructor: Rajendra Kumar **Scribe:** Eeshan Yadav

1 Introduction

These notes cover the number-theoretic success probability calculation used in Shor's reduction (why a random choice of a succeeds with constant probability) and the phase-estimation based order-finding routine.

2 Order and Chinese Remainder Structure

Definition 1. Let $a \in \mathbb{Z}_N^*$. The *order* of a modulo N, denoted by $\mathrm{ord}_N(a)$, is defined to be the smallest positive integer r such that

$$a^r \equiv 1 \pmod{N}.$$

Recall the algorithm covered in previous lecture. We need to analyze the probability

$$\Pr\left[r \text{ is even and } a^{r/2} \not\equiv -1 \pmod{N}\right]$$

for a uniformly random choice of $a \in \mathbb{Z}_N^*$.
In class we will only cover the special case when $N = p_1 p_2$ (distinct odd primes). This proof idea can be easily extended for any N. By Chinese Remainder Theorem,

$$\mathbb{Z}_N^* \cong \mathbb{Z}_{p_1}^* \times \mathbb{Z}_{p_2}^*,$$

so a uniformly random $a \bmod N$ corresponds to independent uniform residues modulo p_1 and p_2. Write

$$a \bmod p_1 = g_1^{x_1}, \qquad a \bmod p_2 = g_2^{x_2},$$

for fixed generators g_1, g_2 of $\mathbb{Z}_{p_1}^*, \mathbb{Z}_{p_2}^*$. Define

$$r_1 = \mathrm{ord}_{p_1}(g_1^{x_1}), \qquad r_2 = \mathrm{ord}_{p_2}(g_2^{x_2}).$$

Then

$$r = \mathrm{ord}_N(a) = \mathrm{lcm}(r_1, r_2).$$

3 Parity and 2-adic valuation

Let $v_2(k)$ denote the exponent of the highest power of 2 dividing the integer k.
The two cases that lead to failure/success can be expressed in terms of v_2:

- r odd $\iff v_2(r_1) = v_2(r_2) = 0$.
- r even and $a^{r/2} \equiv -1 \pmod{N}$ corresponds to $v_2(r_1) = v_2(r_2) = t$ for some $t \geq 1$.

Why $a^{r/2} \equiv -1 \pmod{N}$ implies $v_2(r_1) = v_2(r_2)$?
Assume r is even and

$$a^{r/2} \equiv -1 \pmod{N}.$$

Write the local orders as

$$r_1 = 2^{v_1} s_1, \qquad r_2 = 2^{v_2} s_2,$$

where s_1, s_2 are odd and $v_1 = v_2(r_1),\ v_2 = v_2(r_2)$.

Since $a^{r/2} \equiv -1 \pmod{N}$, we have for each $i \in \{1, 2\}$

$$a^{r/2} \equiv -1 \pmod{p_i},$$

in particular $a^{r/2} \not\equiv 1 \pmod{p_i}$. Therefore $r_i \nmid \frac{r}{2}$ for $i = 1, 2$.
Let $v = \max(v_1, v_2)$. Because $r = \operatorname{lcm}(r_1, r_2)$, the 2-adic valuation of r is $v_2(r) = v$, so we can write

$$r = 2^v \ell$$

for some odd $\ell = \operatorname{lcm}(s_1, s_2)$. Hence

$$\frac{r}{2} = 2^{v-1}\ell.$$

Now suppose for contradiction that $v_1 < v_2$. Then $v = v_2$ and $v - 1 \geq v_1$. Because $s_1 \mid \ell$, we have

$$r_1 = 2^{v_1} s_1 \text{ divides } 2^{v-1}\ell = \frac{r}{2},$$

so $r_1 \mid \frac{r}{2}$. That would imply $a^{r/2} \equiv 1 \pmod{p_1}$, contradicting $a^{r/2} \equiv -1 \pmod{p_1}$. Thus $v_1 < v_2$ is impossible. By the same symmetric argument (swap indices) $v_2 < v_1$ is impossible as well. Therefore neither strict inequality can hold, and we must have

$$v_1 = v_2.$$

In other words, $v_2(r_1) = v_2(r_2)$, as required.
So both failure cases (the order is odd, or the order is even but $a^{r/2} \equiv -1$) are captured by the event

$$E : \ v_2(r_1) = v_2(r_2).$$

Hence the probability we need to bound is

$$\Pr(E) = \Pr\left[v_2(r_1) = v_2(r_2)\right].$$

Because residues modulo p_1 and p_2 are independent for a uniformly random a, the random variables r_1, r_2 are independent. Therefore

$$\Pr\left[v_2(r_1) = v_2(r_2)\right] = \sum_{t \geq 0} \Pr\left[v_2(r_1) = t \wedge v_2(r_2) = t\right] = \sum_{t \geq 0} \Pr\left[v_2(r_1) = t\right] \Pr\left[v_2(r_2) = t\right].$$

Final summation bound

If we can show that for every $t \geq 0$,

$$\Pr\left[v_2(r_1) = t\right] \leq \tfrac{1}{2},$$

then

$$\Pr\left[v_2(r_1) = v_2(r_2)\right] = \sum_t \Pr[v_2(r_1) = t] \Pr[v_2(r_2) = t] \leq \sum_t \tfrac{1}{2} \Pr[v_2(r_2) = t] = \tfrac{1}{2}.$$

Thus $\Pr(E) \leq 1/2$, i.e. the probability of the union of the two failure cases is at most $1/2$, and the complementary event (success: r even and $a^{r/2} \not\equiv -1$) has probability at least $1/2$.

Remark 2. The key counting step is to show $\Pr[v_2(r_i) = t] \leq 1/2$ for each t. A standard route is to write $p_i - 1 = 2^T \cdot s$ with s odd and count the number of residues whose order has 2-adic valuation exactly t; this uses that the set of elements of a given order is a union of $\varphi(\cdot)$-sized cyclic subgroups. Leave this counting as an exercise (or see the textbook argument): it yields the desired $1/2$ bound for every t.

4 Order Finding via Phase Estimation

Input. Integer N and $a < N$ with $\gcd(a, N) = 1$.

Goal. Output the smallest $r > 0$ such that $a^r \equiv 1 \pmod{N}$.

Complexities.

- Best known classical requires at least $N^{1/3}$ time.
- Quantum (Shor): poly$(\log N)$; in simple cost-models the dominant cost is roughly $(\log N)^3$.

Modular-multiplication unitary M_a

Define M_a on computational basis states by

$$M_a |x\rangle = |ax \bmod N\rangle, \qquad x \in \{0, 1, \ldots, 2^n - 1\},$$

where $2^n \geq N$. To extend M_a to the whole 2^n-space it is convenient to define

$$M_a |x\rangle = |x\rangle \qquad \text{for } x \notin \{0, \ldots, N-1\},$$

so M_a acts as a permutation on the first N basis states and identity on the rest. Hence M_a is unitary (a permutation matrix on the computational basis).

Lemma 3. *The operator M_a is unitary.*

Proof. It suffices to show that M_a maps computational basis states to distinct computational basis states.
Let $|x\rangle$ and $|y\rangle$ be two basis states with $x, y \in \{0, \ldots, N-1\}$. Suppose

$$M_a |x\rangle = M_a |y\rangle .$$

Then

$$|ax \bmod N\rangle = |ay \bmod N\rangle$$

which implies

$$ax \equiv ay \pmod{N}.$$

Since $\gcd(a, N) = 1$, the element a has a multiplicative inverse modulo N. Multiplying both sides by a^{-1} gives

$$x \equiv y \pmod{N}.$$

But $x, y \in \{0, \ldots, N-1\}$, hence $x = y$. Therefore the mapping $x \mapsto ax \bmod N$ is injective, and since the domain is finite it is a permutation of the set $\{0, \ldots, N-1\}$.
Thus M_a permutes computational basis states and is therefore a unitary operator. □

Eigenvectors and eigenvalues

Let $r = \mathrm{ord}_N(a)$. For $j = 0, 1, \ldots, r-1$ define

$$|\psi_j\rangle = \frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} \omega_r^{-jt} |a^t\rangle$$

Notice that

$$\omega_r = e^{2\pi i/r}.$$

It is easy to verify that $|\psi_j\rangle$ is an eignevector, i.e.

$$M_a |\psi_j\rangle = \omega_r^j |\psi_j\rangle ,$$

If we are M_a, and ψ_j, then maybe we can find r by doing the phase estimation.

Issues / obstacles.

1. **Eigenvectors:** the natural eigenvectors of the modular-multiplication operator involve the unknown period r itself (so we cannot classically prepare them without already knowing r).
2. **Controlled powers:** We need to create unitary matrices of the form $M_a^{2^k}$ so that we can apply the Order Finding Algorithm. Note: this one is actually easy to resolve as $M_a^{2^k} = M_{a^{2^k}}$
3. **Precision:** We have to decide how much precision in phase estimation we need to get the value of r.

To resolve the first obstacle, notice that

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle .$$

Thus $|1\rangle$ is an equal superposition of eigenstates of M_a.

Phase estimation on $|1\rangle$

Run standard phase estimation with m ancilla qubits and controlled-$M_a^{2^k}$ gates. Expanding $|1\rangle$ in the eigenbasis,

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle .$$

After phase-estimation (and the inverse QFT on the ancilla) the joint state becomes (up to the usual approximation)

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} |\psi_j\rangle \, |\varphi_j\rangle ,$$

where the phase-register state $|\varphi_j\rangle$ has the explicit Fourier-like form (derived from the QFT analysis)

$$|\varphi_j\rangle = \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{2\pi i x \left(\frac{j}{r} - \frac{y}{2^m}\right)} |y\rangle .$$

The inner sum over x is a geometric series / Dirichlet kernel and concentrates amplitude on those y for which

$$\left| \frac{j}{r} - \frac{y}{2^m} \right|$$

is small.

Measurement guarantee. Phase estimation implies that with high probability a measured ancilla value y satisfies

$$\left| \frac{y}{2^m} - \frac{j}{r} \right| < \frac{1}{2^{m+1}}.$$

So the measurement yields a rational approximation $y/2^m \approx j/r$.

5 Recovering the order

If 2^m is large enough (choose m so that $2^{m+1} > N^2$ suffices), then from the measured rational $y/2^m$ we can recover the reduced fraction j/r uniquely via the continued-fraction algorithm. Concretely:

$$\left| \frac{y}{2^m} - \frac{j}{r} \right| < \frac{1}{2^{m+1}} \quad \text{and} \quad \left| \frac{j}{r} - \frac{j-1}{r-1} \right| > \frac{1}{r^2} > \frac{1}{N^2},$$

so choosing $1/2^{m+1} < 1/N^2$ separates distinct possible fractions and yields j/r uniquely (Can be done by Continued Fraction).

Exercises

- Prove that $\Pr[v_2(r_i) = 1] \leq 1/2$ for a uniformly random $x \in \mathbb{Z}_{p_i}^*$.
- Write the full phase-estimation circuit for M_a and show that the circuit size is $\mathcal{O}(poly(n))$ where $n = \lceil \log_2 N \rceil$.
- Read about the continued fraction [dW23][Chapter 5.4].

References

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023.