Quantum Algorithms
Lecture 23
Quantum algorithms for Abelian groups II

Zhejiang University

Reduction of factoring to period finding

Factoring in parts

Let us assume that we know how to find the period. It is clear that we can factor the number y by running $O(logy)$ times a subprogram which, for any composite number, finds a nontrivial divisor with probability at least 1/2.

y has at most $O(logy)$ divisors (because $2^{logn} \sim n$). The program for each divisor can be launched for constant number of times to find a divisor with high probability.

Procedure for finding a nontrivial divisor

Input. An integer y ($y > 1$).

Step 1. Check y for parity. If y is even, then give the answer "2"; otherwise proceed to Step 2.

Step 2. Check whether y is the k-th power of an integer for $k = 2, \dots, \log_2 y$. If $y = m^k$, then give the answer "m"; otherwise proceed to Step 3.

Step 3. Choose an integer a randomly and uniformly between 1 and $y - 1$. Compute $b = \gcd(a, \boldsymbol{y})$ (say, by Euclid's algorithm). If $b > 1$, then give the answer "b"; otherwise proceed to Step 4.

Procedure for finding a nontrivial divisor

Step 4. Compute $r = per_y(a)$ (using the period finding algorithm that we assume we have). If r is odd, then the answer is “y is prime” (which means that we give up finding a nontrivial divisor). Otherwise proceed to Step 5.

Step 5. Compute $d = \gcd(a^{r/2} - 1, y)$. If $d > 1$, then the answer is “d”; otherwise the answer is “y is prime”.

For example, if $y = 21$ and $a = 2$, algorithm will find $d = 7$, but for $a = 5$ will fail to find $d > 1$.

Remark about Step 2

Step 2. Check whether y is the k-th power of an integer for $k = 2, \dots, \log_2 y$. If $y = m^k$, then give the answer "m"; otherwise proceed to Step 3.

$\log_2 y$ is linear in length of y and there are at most $\log_2 y$ different powers k to check for each case. Therefore, at most $(\log_2 y)^2$ classical checks are needed. $O(n^2)$ time complexity for input of size n.

We can consider this as addition to Step 1 to find simple solutions fast if such exist.

Analysis of the divisor finding procedure

Period finding result

If the above procedure yields a number, it is a nontrivial divisor of y. The procedure fails and gives the answer "y is prime" in two cases: 1) when $r = per_y(a)$ is odd, or 2) when r is even but $\gcd(a^{r/2} - 1, y) = 1$, i.e., $a^{r/2} - 1$ is invertible modulo y. However, $(a^{r/2} + 1)(a^{r/2} - 1) \equiv a^r - 1 \equiv 0\ (mod y)$, hence $a^{r/2} + 1 \equiv 0\ (mod y)$ in this case. The converse is also true: if r is even and $a^{r/2} + 1 \equiv 0\ (mod y)$, then the answer is "$y$ is prime".

Success probability

Let us prove that our procedure succeeds with probability at least $1 - 1/2^{k-1}$, where k is the number of distinct prime divisors of y. (Note that this probability vanishes for prime y, so that the procedure also works as a primality test.) In the proof we will need the Chinese Remainder Theorem and the fact that the multiplicative group of residues modulo p^α, p prime, is cyclic.

Denotations

Let $y = \prod_{j=1}^{k} p_j^{\alpha_j}$ be the decomposition of y into prime factors. We introduce the notation $a_j \equiv a(mod p_j^{\alpha_j})$, $r_j = per_{(p_j^{\alpha_j})} a_j = 2^{s_j} r'_j$, where r'_j is odd.

By the Chinese Remainder Theorem, r is the least common multiple of all the r_j. Hence $r = 2^s r'$, where $s = \max\{s_1, \ldots, s_k\}$ and r' is odd.

$r = per_y(a)$, i.e., $a^r \equiv 1(mod\ y)$.

y is prime - condition

We now prove that the procedure yields the answer "y is prime" if and only if $s1 = s2 = \cdots = sk$. Indeed, if $s1 = \cdots = sk = 0$, then r is odd. If $s1 = \cdots = sk \geq 1$, then r is even, but $a_j^{r_j/2} \equiv -1(mod p_j^{\alpha_j})$ (using the cyclicity of the group $(Z/p_j^{\alpha_j}Z)^*$), hence $a^{r/2} \equiv -1(mod\ y)$ (using the Chinese Remainder Theorem).

y is prime - condition

Thus the procedure yields the answer "y is prime" in both cases. Conversely, if not all the s_j are equal, then r is even and $s_m < s$ for some m, so that $a_m^{r/2} \equiv 1 (mod p_m^{\alpha_m})$. Hence $a^{r/2} \not\equiv -1 (mod\ y)$, i.e., the procedure yields a nontrivial divisor.

Assessing probability

To give a lower bound of the success probability, we may assume that the procedure has reached Step 4. Thus a is chosen according to the uniform distribution over the group $(Z/yZ)^*$. By the Chinese Remainder Theorem, the uniform random choice of a is the same as the independent uniform random choice of $a_j \in (Z/p_j^{\alpha_j}Z)^*$ for each j.

Assessing probability

Let us fix j, choose some $s \geq 0$ and estimate the probability of the event $s_j = s$ for the uniform distribution of a_j. Let g_j be a generator of the cyclic group $(Z/p_j^{\alpha_j}Z)^*$. The order of this group (number of elements) may be represented as $p_j^{\alpha_j} - p_j^{\alpha_j - 1} = 2^{t_j} q_j$, where q_j is odd. Then

$$\left|\{a_j : s_j = s\}\right| = \left|\{g_j^l : l = 2^{t_j - s} m,\ \text{where } m \text{ is odd}\}\right|$$

$$= \begin{cases} q_j & \text{if } s = 0, \\ (2^s - 2^{s-1}) q_j & \text{if } s = 1, \ldots, t_j. \end{cases}$$

Assessing probability

For any given s, the probability of the event $s_j = s$ does not exceed 1/2. Now let $s = s_1$ be a random number (depending on a_1); then $\mathrm{Pr}[sj = s] \leq 1/2$ for $j = 2, \ldots, k$. It follows that

$$\mathrm{Pr}[s1 = s2 = \cdots = sk] \leq (1/2)^{k-1}$$

This yields the desired estimate of the success probability for the entire procedure: with probability at least $1 - 1/2^{k-1}$ the procedure finds a nontrivial divisor of y.

Case y=p*q

In such case $k = 2$

With probability at least $1 - \frac{1}{2^{k-1}} = 1/2$ the procedure finds a nontrivial divisor of y - p or q.

Quantum algorithm for finding the period: the basic idea

Period finding definition

The problem is this: given the numbers q and a, construct a polynomial size quantum circuit that computes $per_q(a)$ with error probability $\epsilon \leq 1/3$. The circuit will operate on a single n-qubit register, as well as on many other qubits, some of which may be considered classical. The n-qubit register is meant to represent residues modulo q (recall that $q < 2^n$).

Modular multiplication operator

Let us examine the operator that multiplies the residues by a, acting by the rule

$$U_a\colon |x\rangle \to |ax\ mod\ q\rangle$$

(A more accurate notation would be $U_{q,a}$, indicating the dependence on q. However, q is fixed throughout the computation, so we suppress it from the subscript. We keep a because we will also use the operators U_b for arbitrary b.)

Modular multiplication operator

$$U_a\colon\ |x\rangle \to |ax\ mod\ q\rangle$$

This operator permutes the basis vectors for $0 \le x < q$ (recall that $\gcd(a, q) = 1$). However, we represent $|x\rangle$ by n qubits, so x may take any value between 0 and $2^n - 1$. We will assume that the operator U_a acts trivially on such basis vectors, i.e.,

$U_a\colon |x\rangle = |x\rangle$ for $q \le x < 2^n$.

Modular multiplication operator

$$U_a \colon |x\rangle \to |ax \; mod \; q\rangle$$

Since for the multiplication of the residues there is a Boolean circuit of polynomial $O(n^2)$ size, there is a quantum circuit (with ancillas) of about the same size.

Modular multiplication operator

The permutation given by the operator U_a can be decomposed into cycles. The cycle containing 1 is $(1, a, a^2, \ldots, a^{per_q(a)-1})$; it has length $per_q(a)$. The algorithm we are discussing begins at the state $|1\rangle$, to which the operator U_a gets applied many times. But such transformations do not take us beyond the orbit of 1 (the set of elements which constitute the cycle described above). Therefore, we consider the restriction of the operator U_a to the subspace generated by the orbit of 1.

Modular multiplication operator

v is an eigenvector for matrix A with eigenvalue λ if Av=λv.

When U is a unitary operator, then all of its eigenvalues have length 1 and can be expressed in the form $e^{2\pi i\phi}$ where ϕ is between 0 and 1.

$$\text{Eigenvalues of } U_a: \quad \lambda_k = e^{2\pi i \cdot k/t}, \text{ where } t \text{ is the period}$$

$$\text{Eigenvectors of } U_a: \quad |\xi_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i \cdot km/t} |a^m\rangle.$$

$$U_a\colon |x\rangle \rightarrow |ax \bmod q\rangle$$

Modular multiplication operator

It is easy to verify that the vectors $|\xi_k\rangle$ are indeed eigenvectors. It suffices to note that the multiplication by a leads to a shift of the indices in the sum. If we change the variable of summation in order to remove this shift, we get the factor $e^{2\pi i \cdot k/t}$.

$$\text{Eigenvalues of } U_a : \quad \lambda_k = e^{2\pi i \cdot k/t}, \text{ where } t \text{ is the period}$$

$$\text{Eigenvectors of } U_a : \quad |\xi_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i \cdot km/t} |a^m\rangle.$$

$$U_a\!: |x\rangle \rightarrow |ax \; mod \; q\rangle$$

Measuring eigenvalues

If we are able to measure the eigenvalues of the operator U_a, then we can obtain the numbers k/t. First let us analyze how this will help us in determining the period.

$$\text{Eigenvalues of } U_a: \quad \lambda_k = e^{2\pi i \cdot k/t}, \text{ where } t \text{ is the period}$$

$$\text{Eigenvectors of } U_a: \quad |\xi_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i \cdot km/t} |a^m\rangle.$$

Measuring eigenvalues

Suppose we have a machine which in each run gives us the number k/t, where t is the sought-for period and k is a random number uniformly distributed over the set $\{0, \ldots, t-1\}$. We suppose that k/t is represented as an irreducible fraction k'/t' (if the machine were able to give the number in the form k/t, there would be no problem at all).

Lemma

Having obtained several fractions of the form k_1'/t_1', k_2'/t_2', …, k_l'/t_l' we can, with high probability, find the number t by reducing these fractions to a common denominator.

If $l \geq 2$ fractions are obtained, then the probability that their least common denominator is different from t is less than $3 \cdot 2^{-l}$.

Lemma - proof

The fractions k_1'/t_1', k_2'/t_2', …, k_l'/t_l' can be obtained as reductions of fractions $k_1/t, \ldots, k_l/t$ (i.e., k_j'/t_j'=k_j/t), where $k_1, ..., k_l$ are independently distributed random numbers. The least common multiple of $t_1', ..., t_l'$ equals t if and only if the greatest common divisor of $k_1, ..., k_l$ and t is equal to 1.

Lemma - proof

The probability that $k_1, \ldots, k_l$ have a common prime divisor p does not exceed $1/p^l$. Therefore, the probability of not getting t after reducing to a common denominator does not exceed $\sum_{k=2}^{\infty} \frac{1}{k^l} < 3 \cdot 2^{-l}$ (the range of the index k in this sum obviously includes all prime divisors of t).

Generating the number k/t

Now we construct the machine M that generates the number k/t (in the form of an irreducible fraction) for random uniformly distributed k. This will be a quantum circuit which realizes the measuring operator $W = \sum_{k=0}^{t-1} V_k \otimes \Pi_{L_k}$, where $L_k = C(|\xi_k\rangle)$, the subspace generated by $|\xi_k\rangle$. The operators V_k are the form $|0\rangle \rightarrow \sum_{y,z} |y, z\rangle$, where y is an irreducible fraction and z is garbage.

Generating the number k/t

The conditional probabilities should satisfy the inequality

$$\mathbf{P}\left(\boxed{\begin{matrix} k \\ \hline t \end{matrix}} \middle| k\right) \stackrel{\text{def}}{=} \sum_z \left| \left\langle \boxed{\begin{matrix} k \\ \hline t \end{matrix}}, z \middle| V_k \middle| 0 \right\rangle \right|^2 \geq 1 - \varepsilon$$

where $\left[\frac{k}{t}\right]$ denotes the irreducible fraction equal to the rational number k/t.

Generating the number k/t

The construction of such a measuring circuit is rather complex, so we first explain how it is used to generate the outcome y with the desired probability $w_v = \sum_{k \in M_y} \frac{1}{t}$. Let us take the state $|1\rangle$ as the initial state. A direct computation (task for students - to carry it through) shows that

$$|1\rangle = \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\xi_k\rangle$$

Generating the number k/t

$$|1\rangle = \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\xi_k\rangle$$

If we perform the measurement on this state, then by the formula for total probability we obtain

$$\mathbf{Pr}[\text{outcome} = y] = \mathbf{P}\big(W(|0\rangle \otimes |1\rangle), y\big) = \sum_k \mathbf{P}(y|k)\,\mathbf{P}(|1\rangle, \mathcal{L}_k)$$

Generating the number k/t

The probabilities of all $|\xi_k\rangle$ are equal: $P(|1\rangle, L_k) = |\langle\xi_k|1\rangle|^2 = 1/t$, which corresponds to the uniform distribution of k. The property

$$\mathbf{P}\left(\boxed{\begin{matrix}k\\ \hline t\end{matrix}}\,\middle|\,k\right) \stackrel{\text{def}}{=} \sum_z \left|\left\langle \boxed{\begin{matrix}k\\ \hline t\end{matrix}}, z \,\middle|\, V_k \,\middle|\, 0\right\rangle\right|^2 \geq 1 - \varepsilon$$

guarantees that we obtain the outcome $\left[\frac{k}{t}\right]$ with probability $\geq 1 - \varepsilon$.

Generating the number k/t

To be completely pedantic, we need to derive an inequality

$$\sum_y \left| \mathbf{Pr}[\text{outcome} = y] - w_y \right| \leq 2\epsilon$$

Schematically, the machine M functions as follows:

$$|1\rangle \longrightarrow \boxed{\begin{array}{c}\text{random choice of } k\\ \text{(God playing dice)}\end{array}} \xrightarrow{|\xi_k\rangle} \boxed{\text{measuring of } W} \begin{array}{l} \nearrow\ y \neq \boxed{\begin{array}{c}k\\ \hline t\end{array}} \ \begin{array}{c}\text{with probability}\\ \leq \varepsilon,\end{array} \\ \searrow\ y = \boxed{\begin{array}{c}k\\ \hline t\end{array}} \ \begin{array}{c}\text{with probability}\\ \geq 1-\varepsilon.\end{array}\end{array}$$

Generating the number k/t

The random choice of k happens automatically, without applying any operator whatsoever. Indeed, the formula of total probability is arranged in such a way as if: before the measurement begins, a random k was generated, which then remains constant. (Of course, the formula is only true when the operator W is measuring with respect to the given subspaces L_k.)

Additional remarks

Period finding

We reformulate our period finding problem into a phase estimation problem. To find the period of a with respect to q (the smallest nonnegative number t such that $a^t \equiv 1 (mod\, q)$), we find the eigenvalues of U_a:

$$U_a\colon |x\rangle \rightarrow |ax\; mod\; q\rangle$$

Period finding

Since U has r (r - period) eigenvectors, the phase ϕ in the phase estimation equals s/r, where s is an integer in the range $0, \dots, r-1$. Each eigenvector corresponds to a different value of s.

$$U|y\rangle = |xy \mod N\rangle \qquad \exp\left[\frac{2\pi i s}{r}\right] \qquad \frac{s}{r} = \text{phase}$$

$$U|\psi_s\rangle = \underbrace{e^{2\pi i\phi}}_{\text{eigenvalue}}|\psi_s\rangle$$

Period finding

To solve the eigenvalue, we need to know the eigenvector. But we don't know the period r and therefore we don't know the eigenvectors. Fortunately, we don't need to. We know the superposition of all eigenvectors. Let's create a superposition with all the eigenvectors.

$$\frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}|v_t\rangle = \frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi ikt}{r}\right]|x^k \bmod N\rangle$$

which, using $\sum_{t=0}^{r-1}\exp\left[\frac{-2\pi ikt}{r}\right] = r\delta_{k,0}$ becomes,

$$\frac{1}{\sqrt{r}}\sum_{t=0}^{r-1}|v_t\rangle = |1\rangle$$

Eigenvectors of modular op.

$$U_x\colon\ |y\rangle \rightarrow |xy\ mod\ N\rangle$$

eigenvalues

eigenvectors

$$U|u_s\rangle = \exp\left[\frac{2\pi i s}{r}\right]|u_s\rangle \qquad \text{with} \qquad |u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i s k}{r}\right]|x^k \mod N\rangle$$

$$\underline{U|u_s\rangle} = \underbrace{U\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i k t}{r}\right]|x^k \bmod N\rangle}_{|u_s\rangle} = \underbrace{\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i k t}{r}\right]|x^{k+1} \bmod N\rangle}_{\text{apply } U|y\rangle = |xy \mod N\rangle}$$

$$= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\exp\left[\frac{-2\pi i (k-1) t}{r}\right]|x^k \bmod N\rangle = \underline{\exp\left[\frac{-2\pi i t}{r}\right]|u_s\rangle}$$

if r is the period, $x^0 = x^r$. We can shift $k \rightarrow k - 1$

$|u_s\rangle$ is eigenvector of U

Thank you for your attention!