Quantum Algorithms
Lecture 24
Quantum algorithms for Abelian groups III

Zhejiang University

The phase estimation procedure

Measuring eigenvalues

Now we will construct the operator that measures the eigenvalues of U_a: $|x\rangle \rightarrow |ax \; mod \; q\rangle$. The eigenvalues have the form $\lambda_k = e^{2\pi i \phi_k}$, where $\phi_k = \frac{k}{t} \; mod \; 1$

The phase ϕ_k is a real number modulo 1, i.e., $\phi_k \in R/Z$. (The set R/Z can be conveniently represented as a circle of unit length.) The procedure for determining ϕ_k is called phase estimation.

Measuring eigenvalues

As we already mentioned, we can limit ourselves to the study of the action of the operator U_a on the input vector $|\xi_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i \cdot km/t} |a^m\rangle$. The construction is divided into four stages.

This time authors did a nice job to first describe general idea of the construction, stages are described by subchapters.

Construction – stage 1

We construct a measuring operator such that the conditional probabilities depend on the value of $\phi = \phi_k$. Thus a single use of this operator will give us some information about ϕ (like flipping a biased coin tells something about the bias, though inconclusively).

In case of coin flipping we gather some statistics to evaluate the probability. Here a bit different approach will be used.

Construction – stage 2

We localize the value of ϕ with modest precision. It is the moment to emphasize that, in all the arguments, there are two parameters: the probability of error ε and the precision δ. As the result of a measurement, we obtain some number y, for which the condition $|y - \phi|_{mod1} < \delta$ must hold with probability at least $1 - \varepsilon$. (Here $|\cdot|_{mod1}$ denotes the distance on the unit length circle, e.g., $|0.1 - 0.9|_{mod1} = 0.2$.) For the time being, a modest precision will do, say $\delta = 1/16$.

Construction – stage 3

Now we must increase the precision. Specifically, we determine ϕ with precision $1/2^{2n+2}$.

Modular exponentiation here will be very useful as it will allow to do such operation very efficiently.

Construction – stage 4

We need to pass from the approximate value of ϕ to the exact one, represented in the form of an irreducible fraction. It is essential to be able to distinguish between numbers of the form $\phi = k/t$, where $0 \leq k < t < 2^n$. Notice that if $k1/t1 \neq k2/t2$, then $|k1/t1 - k2/t2|_{mod1} \geq 1/(t1 \cdot t2) > 1/2^{2n}$. Therefore, knowing $\phi = k/t$ with precision $1/2^{2n+1}$, one can, in principle, determine its exact value. Moreover, this can be done efficiently by the use of continued fractions.

Construction - remarks

At stage 3, we will use the operator U_b for arbitrary b (not just for $b = a$, the number for which we seek the period). To this end, we introduce an operator U that sends $|b, x\rangle$ to $|b, bx \, mod q\rangle$ whenever $\gcd(b, q) = 1$. How the operator U acts in the remaining cases is not important; this action can be defined in an arbitrary computationally trivial way, so that U be represented by a quantum circuit of size $O(n^2)$. In fact, all the earlier arguments about the simulation of Boolean circuits by quantum circuits hold true for the simulation of circuits that compute partially defined functions.

Problem 13.2 – realizing op.

We construct a classical operator $V_b \in L(B \otimes B^{\otimes n})$ (the basis vectors in $B^{\otimes n}$ are numbered from 0 to $2^n - 1$) such that

$$V_b|0,0\rangle = |0,1\rangle,\ V_b|1,0\rangle = |1,b\rangle.$$

Then the circuit $V_b^{-1}[0,B]U[B,A]V_b[0,B]$ realizes the operator $\Lambda(U_b)[0,A]$, where B denotes a set of n ancillas.

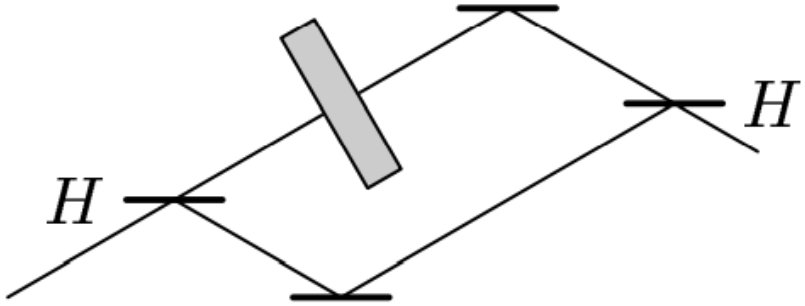
$$U\colon\ |b,x\rangle\ \rightarrow\ |b,bx\ mod q\rangle$$
$$U_b\colon\ |x\rangle \rightarrow |bx\ mod\ q\rangle$$

Stage 1.
How to get some information about the phase.

Operator for measuring eigenvalues

$$\Xi(U) = (H \otimes I)\Lambda(U)(H \otimes I)\colon B^{\otimes N} \to B^{\otimes N}$$

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



If the initial vector has the form $|\psi\rangle = |\eta\rangle \otimes |\xi\rangle$ ($|\xi\rangle \in L_j$), then $\Xi(U)|\psi\rangle = |\eta'\rangle \otimes |\xi\rangle$, where

$$|\eta'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \lambda_j \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}|\eta\rangle = \frac{1}{2}\begin{pmatrix} 1+\lambda_j & 1-\lambda_j \\ 1-\lambda_j & 1+\lambda_j \end{pmatrix}|\eta\rangle$$

Operator for measuring eigenvalues

We have $\lambda_k = e^{2\pi i \phi_k}$, so we have:

$$\Xi(U_a) = \sum_k V_k \otimes \Pi_{\mathcal{L}_k}, \quad V_k = \frac{1}{2}\begin{pmatrix} 1+e^{2\pi i\varphi_k} & 1-e^{2\pi i\varphi_k} \\ 1-e^{2\pi i\varphi_k} & 1+e^{2\pi i\varphi_k} \end{pmatrix}$$

and its action in the form

$$|0\rangle \otimes |\xi_k\rangle \xmapsto{\Xi(U_a)} \left(\frac{1+e^{2\pi i\varphi_k}}{2}|0\rangle + \frac{1-e^{2\pi i\varphi_k}}{2}|1\rangle\right) \otimes |\xi_k\rangle$$

Operator for measuring eigenvalues

$$|0\rangle \otimes |\xi_k\rangle \xrightarrow{\Xi(U_a)} \left(\frac{1 + e^{2\pi i \varphi_k}}{2} |0\rangle + \frac{1 - e^{2\pi i \varphi_k}}{2} |1\rangle \right) \otimes |\xi_k\rangle$$

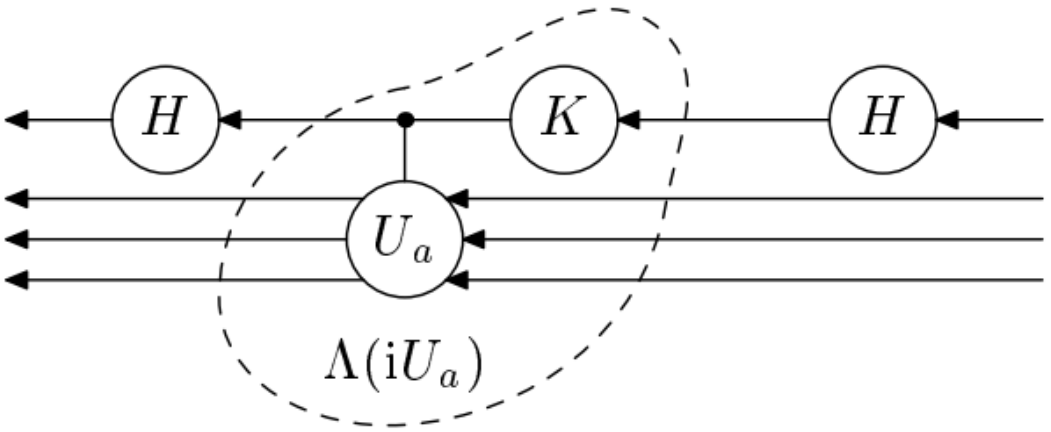
We get conditional probabilities for the first qubit:

$$\mathbf{P}(0|k) = \left| \frac{1 + e^{2\pi i \varphi_k}}{2} \right|^2 = \frac{1 + \cos(2\pi\varphi_k)}{2}, \qquad \mathbf{P}(1|k) = \frac{1 - \cos(2\pi\varphi_k)}{2}$$

Although the conditional probabilities depend on ϕ_k, they do not allow one to distinguish between $\phi_k = \phi$ and $\phi_k = -\phi$ (like in case of global phase). That is why another type of measurement is needed.

Another operator - improvement

We will use the operator $\Xi(iU_a)$. $K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ is from the standard basis.



The encircled part of the diagram realizes the operator $\Lambda(iU_a)$. Indeed, K multiplies only $|1\rangle$ by i, but this is just the case where the operator U_a is applied (by the definition of $\Lambda(U_a)$).

Another operator - analysis

For the operator $\Xi(iU_a)$ the conditional probabilities are

$$\mathbf{P}(0|k) = \frac{1 - \sin(2\pi\varphi_k)}{2}, \qquad \mathbf{P}(1|k) = \frac{1 + \sin(2\pi\varphi_k)}{2}$$

The complexity of the realization of the operators $\Xi(U_a)$ and $\Xi(iU_a)$ depends on the complexity of the operator $\Lambda(U_a)$, which is not much higher than the complexity of the operator U. Thus, $\Xi(U_a)$ and $\Xi(iU_a)$ can be realized by quantum circuits of size $O(n^2)$ in the standard basis.

Stage 2.
Determining the phase with constant precision.

Our next task

We want to localize the value of $\phi = \phi_k$, i.e., to infer the inequality $|\phi - y|_{mod1} < \delta$ for some (initially unknown) y and a given precision δ. To get such an estimate, we apply the operators $\Xi(U_a)$ and $\Xi(iU_a)$ to the same "object of measurement" but different "instruments" (auxiliary qubits). The reasoning is the same for both operators, so we limit ourselves to the case $\Xi(U_a)$.

Considering eigenvectors

We have the quantum register A that contains $|\xi_k\rangle$. Actually, this register initially contains $|1\rangle = \frac{1}{\sqrt{t}}\sum_{k=0}^{t-1}|\xi_k\rangle$, but we consider each $|\xi_k\rangle$ separately. (We can do this because we apply only operators that are measuring with respect to the orthogonal decomposition $\oplus_k C(|\xi_k\rangle)$, so that different eigenvectors do not mix.) Let us introduce a large number s of auxiliary qubits. Each of them will be used in applying the operator $\Xi(U_a)$.

Estimating probabilities

Experiment is repeated s times, outcomes are stored in separate qubits, then frequency of outcome 1 is estimated classically. Probability to fail to estimate with enough precision is estimated by Chernoff 's bound:

$$\mathbf{Pr}\left[\left|s^{-1}\sum_{r=1}^{s} v_r - p_*\right| \geq \delta\right] \leq 2e^{-2\delta^2 s}$$

For a fixed δ we can find a suitable constant $c = c(\delta)$ such that the error is smaller than ε when $s = clog(1/\varepsilon) = \Theta(\log(1/\varepsilon))$ trials are made.

Estimating probabilities

So, we have learned how to find $\cos(2\pi\phi)$ and $\sin(2\pi\phi)$ with any given precision δ. Now we choose δ so that the value ϕ can be determined from the values of the sine and the cosine with precision $1/16$. This still takes $\Theta(\log(1/\varepsilon))$ trials. The second stage is completed.

Stage 3.
Determining the phase with exponential precision.

More operators

To increase the precision, we will use, along with $\Lambda(U_a)$, the operators $\Lambda((U_a)^{2^j})$ for all $j \leq 2n-1$. We can quickly raise numbers to a power, but, in general, computing a power of an operator is difficult. However, the operation U_a of $(mod\ q)$-multiplication by a possesses the following remarkable property:

$$(U_a)^p = U_{a^p} = U_{(a^p mod\ q)}$$

More operators

Consequently, $\Lambda((U_a)^{2^j}) = \Lambda(U_b)$, where $b \equiv a^{2^j}(mod q)$. The required values for the parameter b can be calculated using a circuit of polynomial size; then we can build an according controlled operation.

Eigenvalues and angle precision

We found the eigenvalue $\lambda_k = \lambda = e^{2\pi i\phi}$ for some eigenvector $|\xi_k\rangle$. This same vector is an eigenvector for any power of the operator U_a, the eigenvalue will have corresponding power: for $(U_a)^{2^j} = U_{a^{2^j}}$ it equals $\lambda^{2^j} = e^{2\pi i \cdot 2^j \phi}$.

It is like for each j we can estimate the next bit of ϕ after the decimal point.

Eigenvalues and angle precision

In other words, we can determine with precision $1/16$ the values of $\phi, 2\phi, \ldots, 2^{2n-1}\phi$ modulo 1. But this allows us to determine ϕ with precision $1/2^{2n+2}$ efficiently (in linear time with constant memory).

Then we do classical postprocessing so that compute more precisely (by sharpening – described in a book in details) the value of ϕ. Algorithm is quite efficient since we use constant number of operations for each bit. It follows that the computation can be represented by a Boolean circuit of size $O(m)$ and depth $O(logm)$, where m is the number of bits.

Stage 4.
Determining the exact value of the phase.

Finding a fraction

We have found a number y satisfying $|y - k/t| < 1/2^{2n+1}$. We represent it as a continued fraction and try all convergents of y until we find a fraction k'/t' such that $|y - k'/t'| < 1/2^{2n+1}$. The second part of Theorem A.13 guarantees that the number k/t is contained among the convergents, and therefore will be found unless the algorithm stops earlier. The running time of this algorithm is $O(n^3)$.

Theorem A.13, part 2: If $|z - p/q| < 1/(q(2q-1))$, then p/q is a convergent of z.

Continued fractions - example

Find the continued fraction for $3.245 = \frac{649}{200}$

Step	Real Number	Integer part	Fractional part	Simplified	Reciprocal of f
1	$r = \frac{649}{200}$	$i = 3$	$f = \frac{649}{200} - 3$	$= \frac{49}{200}$	$\frac{1}{f} = \frac{200}{49}$
2	$r = \frac{200}{49}$	$i = 4$	$f = \frac{200}{49} - 4$	$= \frac{4}{49}$	$\frac{1}{f} = \frac{49}{4}$
3	$r = \frac{49}{4}$	$i = 12$	$f = \frac{49}{4} - 12$	$= \frac{1}{4}$	$\frac{1}{f} = \frac{4}{1}$
4	$r = 4$	$i = 4$	$f = 4 - 4$	$= 0$	**STOP**

Continued fraction form for $3.245 = \frac{649}{200} = [3; 4, 12, 4]$

$$= 3 + \cfrac{1}{4 + \cfrac{1}{12 + \frac{1}{4}}}$$

Convergents - example

$$2 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}}$$

Continued fraction expression [2,3,1,2]

The convergents are $c_1 = 2, c_2 = 2 + \frac{1}{3} = \frac{7}{3}, c_3 = 2 + \cfrac{1}{3 + \frac{1}{1}} = \frac{9}{4}, c_4 = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{2}}} = \frac{25}{11}$

Observations

It is essential that the vector $|\xi_k\rangle$ does not deteriorate during the computation. So the state should not be destroyed, quality should not drop. This is one of the reasons why Shor's algorithm is challenging for current real quantum computers.

Observations

The entire period finding procedure depends on the parameters l and s; they should be adjusted so that the error probability be small enough. The error can occur in determining the period t as the least common denominator or in estimating the cosine and the sine of ϕ_k with constant precision δ. The total probability of error does not exceed $3 \cdot 2^{-l} + nle^{-\Omega(s)}$. If it is required to get the result with probability of error $\leq 1/3$, then we must set $l = 4$, $s = \Theta(\log n)$. In this way we get a quantum circuit of size $O(n^3 \log n)$.

Summary

In this diagram on page 128: q is our number that is given (for factoring task); a is our randomly picked number for which we need to find period; n is number of bits (length) of q; s is number of trials in stage 2, where we perform experiments to estimate probabilities; l is precision from Lemma 13.2 – how many fractions needed to find t with high probability.

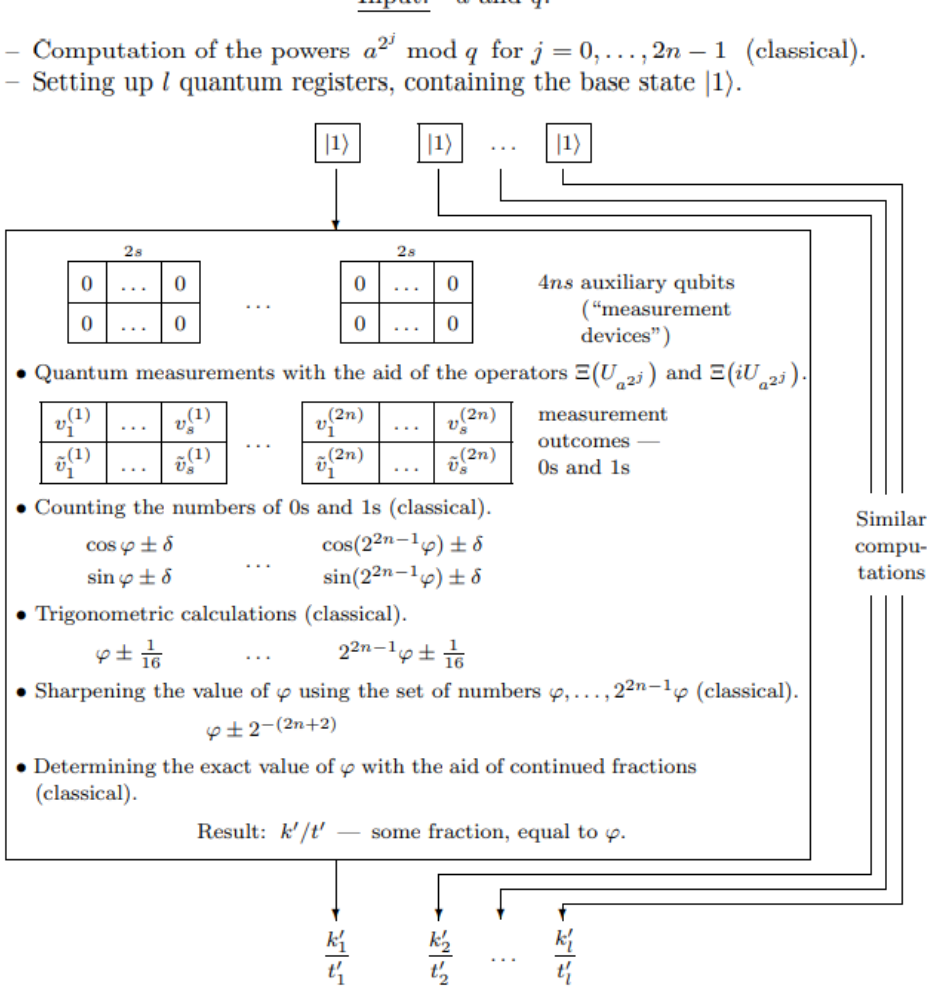


Table 13.1. General scheme of the period finding algorithm. Shown in a box is the phase estimation part.

Discussion of the algorithm

Which eigenvalues

Which eigenvalues do we find? We find a randomly chosen eigenvalue. The distribution over the set of all eigenvalues can be controlled by appropriately choosing the initial state. In our period finding algorithm, it was $|1\rangle = \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\xi_k\rangle$, which corresponded to the uniform distribution on the set of eigenvalues associated with the orbit of 1.

Other operators

Is it possible to find eigenvalues of other operators in the same way as in the algorithm for determining the period?

The answer to the question is “yes” — it is only necessary to implement $\Lambda(U)$, which is usually easy. However, in general, the attainable precision is not great and depends polynomially on the number of times the operator $\Lambda(U)$ is used. If one can efficiently compute the powers of U, then the precision can be made exponential.

Small remark

As we have learned, the Quantum phase estimation algorithm, is a quantum algorithm to estimate the phase (or eigenvalue) of an eigenvector of a unitary operator.

Phase estimation is frequently used as a subroutine in other quantum algorithms. You can consider this as main technique that was learned from Shor's algorithm. Please become confident with this algorithm, it is very useful.

Small remark

In Shor's algorithm we learned how to reduce factoring problem to period finding and how to solve period finding with the help of Phase estimation algorithm.

In lecture 26 I consider to show you another summary and implementation of Shor's algorithm, which is widely used in current implementations. You can consider this as revision lecture for Shor's algorithm.

Thank you for your attention!