이학석사 학위논문

Quantum Algorithms Using Quantum Fourier Transform

(양자 푸리에 변환을 이용한 양자 알고리즘)

2018년 6월

서울대학교 대학원

수 리 과 학 부

이 두 영

Quantum Algorithms Using Quantum Fourier Transform

(양자 푸리에 변환을 이용한 양자 알고리즘)

지도교수 이 훈 희

이 논문을 이학석사 학위논문으로 제출함

2018년 4월

서울대학교 대학원

수 리 과 학 부

이 두 영

이두영의 이학석사 학위논문을 인준함

2018년 6월

위 원 장 _____ 인

부 위 원 장 _____ 인

위 원 _____ 인

Quantum Algorithms using Quantum Fourier Transform

by

Lee Doo Young

A DISSERTATION

Submitted to the faculty of the Graduate School
in partial fulfillment of the requirements
for the degree Master of Science
in the Department of Mathematics
Seoul National University
February 2017

Abstract

In this thesis, we study quantum algorithms, especially using the quantum Fourier transform. At first, we introduce quantum Fourier transform on groups and using this, we study how to solve problems with quantum algorithms.

Keywords : qauntum algorithms, quantum Fourier transform
Student number : 2013-22910

Contents

Chapter 1

Introduction

Manin and Feynman observed that computers built from quantum components are suitable to simulating quantum mechanics. To deal with n quantum bits, a quantum computer need only n quantum bits, whereas a classical computer requires storing 2^n classical bits, exponentially many ones. Therefore, we can think of using a quantum computer is more effective.

He found through concrete examples that quantum computers are better. He discovered in 1994 that a quantum computer could efficiently factor integers and calculate discrete logarithms. These are related to cryptosystems, RSA and Diffie-Hellman key exchange protocol, respectively. The security of these cryptosystems is based on the difficulty of solving these problems classically. The result of Shor drastically reduced the runtime that had classically solved algebraic problems as well as these problems. A key point of Shor's algorithms is to use the quantum Fourier transforms.

In this thesis, we introduce the definition of the quantum Fourier transform on groups and we solve some problems with quantum algorithms using

the quantum Fourier transform. The main body of this thesis is organized as follows. In chapter 2, we give a brief introduction to the representation theory and the quantum mechanics. In chapter 3, we define the quantum Fourier transform. In chapter 4, we describe quantum algorithms for problems involving number fields. In chapter 5, we describe the hidden subgroup problem. We show how to solve the problems with the quantum Fourier transform. We introduce a quantum algorithm for the dihedral hidden subgroup problem.

Chapter 2

Preliminaries

2.1 Basic Representation Theory

Let G be a finite group. A **representation** of G is a group homomorphism π from G into the group $GL(V_\pi)$, where V_π is a vector space and $GL(V_\pi)$ denotes the group of invertible linear maps $V_\pi \to V_\pi$. The $\dim(V_\pi)$ is called the **dimension** of π, denoted by d_π. A **homomorphism** between representations π_1 and π_2 is a linear map $T : V_{\pi_1} \to V_{\pi_2}$ such that $T\pi_1(x) = \pi_2(x)T$ for all $x \in G$. The set of all such operators is denoted by $C(\pi_1, \pi_2)$. Two representations π_1 and π_2 are **equivalent** if $C(\pi_1, \pi_2)$ contains a bijective one. In particular, $C(\pi) := C(\pi, \pi)$. A closed subspace M of V_π is called an **invariant subspace** for π if $\pi(x)M \subset M$ for all $x \in G$. If M is invariant and $\neq 0$, the restriction of π to M, $\pi^M(x) = \pi(x)|M$, defines a representation of G on M, called a **subrepresenatation** of π. If π admits an invariant subspace that is nontrivial, then π is called **reducible**, otherwise π is **irreducible**. For two representations π_1 and π_2 of G, the **direct sum** of π_1 and π_2 is the representation $\pi_1 \oplus \pi_2$ of G on

$V = V_{\pi_1} \oplus V_{\pi_2}$, defined by $(\pi_1 \oplus \pi_2)(x)(v_1 \oplus v_2) = \pi_1(x)(v_1) \oplus \pi_2(x)(v_2)$ for $x \in G$ and $v_1 \in V_{\pi_1}$ and $v_2 \in V_{\pi_2}$. For two representations π_1 and π_2 of G, the **tensor product** of π_1 and π_2 is the representation $\pi_1 \otimes \pi_2$ of G on $V = V_{\pi_1} \otimes V_{\pi_2}$, defined by $(\pi_1 \otimes \pi_2)(x) = \pi_1(x) \otimes \pi_2(x)$ for $x \in G$.

Lemma 2.1.1 (Schur's Lemma)**.** *A representation π of G is irreducible if and only if $C(\pi)$ contains only scalar multiples of the identity.*

Corollary 2.1.1. *If G is abelian, then every irreducible representation of G is one-dimensional.*

We denote by $\widehat{G}$ the set of equivalence classes of irreducible representations of G.

Example 2.1.1. $\widehat{\mathbb{Z}/\mathbb{Z}_k} \simeq \mathbb{Z}/\mathbb{Z}_k$, *with the pairing* $\langle m, n\rangle = e^{2\pi imn/k}$.

Proposition 2.1.1. *If G_1, G_2 are finite groups, then*

$$(G_1 \times G_2)\widehat{\ } \simeq \widehat{G_1} \times \widehat{G_2}.$$

Theorem 2.1.1. *For a subgroup H of G,*

$$\widehat{G/H} \simeq ker H,$$

where $ker H := \{\pi \in \widehat{G} : \pi(h) = 1$ for all $h \in H\}$.

The **character** of π is the function χ_π on G taking complex values defined by

$$g \mapsto Tr(\pi(g)) = \sum_{i=1}^{d_\pi} \pi(g)_{ii}.$$

Then $\chi_\pi(1) = d_\pi$.

We denote by $\mathcal{F}(G)$ the vector space of functions on G taking values in C. The **left regular representation** L of G on $\mathcal{F}(G)$ is given by $(L(g)f)(h) =$

$f(g^{-1}h)$. For a basis $(\delta_g)_{g\in G}$ of $\mathcal{F}(G)$ defined by $\delta_g = 1$ if $g = 1$, 0 otherwise. Then the left regular representation L of G satisfies $L(G)(\delta_h) = \delta_{gh}$. Then

$$Tr(L(g)) = \begin{cases} |G|, & g = 1 \\ 0, & g \neq 1 \end{cases}.$$

Proposition 2.1.2.

$$L = \bigoplus_{\pi\in\hat{G}} d_\pi \pi.$$

Theorem 2.1.2. *By the previous proposition,*

$$\sum_{\pi\in\hat{G}} d_\pi \chi_\pi(g) = \begin{cases} |G|, & g = 1 \\ 0, & g \neq 1 \end{cases}.$$

In particular,

$$\sum_{\pi\in\hat{G}} d_\pi^2 = |G|.$$

2.2 Basic Quantum Mechanics

A classical bit can have a state of either 0 or 1. A **qubit**(quantum bit) can be in a linear combinations of states $|0\rangle$, $|1\rangle$, also known as a **superposition**. In a quantum computer, the superposition means that a quantum register exists in a superposition of all its possible configurations of 0's and 1's at the same time, unlike a classical system. we can write a quantum state in a general form

$$|\psi\rangle = \alpha|0\rangle + \beta|0\rangle,$$

where α, $\beta \in \mathbb{C}$, and $|\alpha|^2 + |\beta|^2 = 1$. We can think of $|\psi\rangle$ as a unit vector in the 2-dimensional complex plane spanned by the two basis $|0\rangle$, $|1\rangle$. A state

in the n qubit system is a superposition of 2^n basis states

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle,$$

where $a_x \in \mathbb{C}$ with $\sum_{x\in\{0,1\}^n} |a_x|^2 = 1$. Given a group G, we write $|g\rangle$ for a computational basis state corresponding to the group element $g \in G$, and $|\phi\rangle = \sum_{g\in G} b_g|g\rangle$, where $b_g \in \mathbb{C}$ with $\sum_{g\in G} |b_g|^2 = 1$. For a finite set S, the state

$$|S\rangle := \frac{1}{\sqrt{S}} \sum_{s\in S} |s\rangle.$$

A quantum state $|\psi\rangle$ is a column vector, also known as a **ket**, whereas a state $\langle\psi|$ is the row vector dual to $|\psi\rangle$, also known as **bra**. The **adjoint** of $|\psi\rangle$ is $(|\psi\rangle)^\dagger := \langle\psi|$. The **inner product** of two quantum states $|x_1\rangle$ and $|x_2\rangle$ is defined as $\langle x_1|\cdot|x_2\rangle = \langle x_1|x_2\rangle$. The **outer product** of two quantum states $|x_1\rangle$ and $|x_2\rangle$ is defined as $|x_1\rangle \times \langle x_2| = |x_1\rangle\langle x_2|$. Let $\{|\beta_i\rangle\}_{i\in I}$ be a basis for a vector space. When we **measure** a state $|\psi\rangle$, we obtain β_i as a measurement outcome, and the probability obtaining the outcome β_i is

$$p(i) = \langle\psi|\beta_i\rangle\langle\beta_i|\psi\rangle,$$

and the state after the measurement is

$$\frac{|\beta_i\rangle\langle\beta_i|\psi\rangle}{\sqrt{p(i)}}.$$

We denote the Hadamard gate by

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

To solve a decision problem, it suffices to give an algorithm with the success probability bounded above 1/2 (say, at least 2/3), since we can

repeat the computation many times and take a majority vote to reduce exponentially the probability of outputting an incorrect answer.

Let f be a function from X to Y. We know sets X and $f(X)$, but not correspondence relation of f. It is called a **black-box function**. We assume the target set Y is a subset of integers. In fact, Y need not to be a subset of integers, for example, a color set $\{red, yellow, blue, \cdots\}$. But we consider to correspond each element in Y to an integer. A classical gate defined by $x \mapsto f(x)$ is not reversible. Unlike classical, qunatum circuits have to use unitary operators. So we consider the reversible gate $(x, y) \mapsto (x, y \oplus f(x))$. In quantum setting, we use similar argument. On a quantum computer, we copy the answer into an ancilla register, and then perform the computation in reverse. The ancilla register is considered as a vector space with a basis including $\{|0\rangle, |f(x)\rangle : x \in X\}$. An operator U defined by

$$|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

is unitary. In fact,

$$\begin{aligned}
\langle\, U^\dagger U|x, y\rangle, |x', y'\rangle\,\rangle =& \langle\, U|x, y\rangle, U|x', y'\rangle\,\rangle \\
=& \langle\, |x, y \oplus f(x)\rangle, |x', y' \oplus f(x')\rangle\,\rangle \\
=& \langle x, x'\rangle\langle y \oplus f(x), y' \oplus f(x')\rangle \\
=& \delta_{x,x'}\delta_{y,y'}.
\end{aligned}$$

Chapter 3

Quantum Fourier Transform

3.1 Quantum Fourier Transform on $\mathbb{Z}/N\mathbb{Z}$

Let V be a N-dimensional vector space with basis $|0\rangle, \cdots, |N-1\rangle$. Define an operator on V by

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle.$$

We call the operator **Qunatum Fourier Transform**(shortly, **QFT**) or QFT on $\mathbb{Z}/N\mathbb{Z}$. We can write the operator as

$$QFT := \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} e^{2\pi i j k/N} |k\rangle\langle j|.$$

Theorem 3.1.1. *QFT is unitary.*

Proof. The adjoint of QFT is

$$QFT^\dagger = \frac{1}{\sqrt{N}} \sum_{j,k=0}^{N-1} e^{-2\pi i j k/N} |j\rangle\langle k|.$$

Then

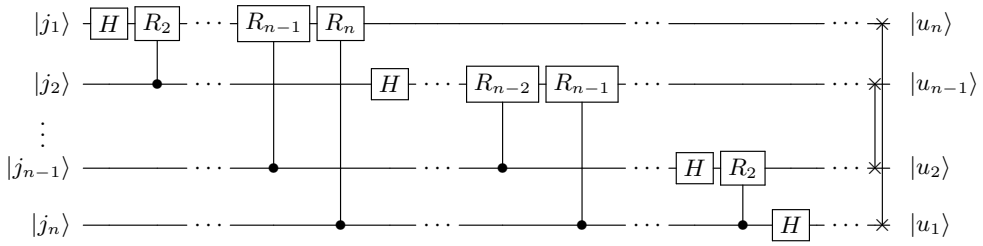
$$\begin{aligned}
QFT^\dagger QFT &= \left(\frac{1}{\sqrt{N}}\sum_{j,k=0}^{N-1} e^{-2\pi ijk/N}|j\rangle\langle k|\right)\left(\frac{1}{\sqrt{N}}\sum_{j',k'=0}^{N-1} e^{2\pi ij'k'/N}|k'\rangle\langle j'|\right) \\
&= \frac{1}{N}\sum_{j,j',k=0}^{N-1} e^{2\pi i(-jk/N+j'k/N)}|j\rangle\langle j'| \\
&= \frac{1}{N}\sum_{j,j'=0}^{N-1}\left(\sum_{k=0}^{N-1} e^{2\pi i(-j+j')k/N}\right)|j\rangle\langle j'| \\
&= \frac{1}{N}\sum_{j=0}^{N-1}\left(\sum_{k=0}^{N-1} e^{2\pi i\cdot 0\cdot k/N}\right)|j\rangle\langle j| \\
&= \sum_{j=0}^{N-1}|j\rangle\langle j| = I
\end{aligned}$$

□

The adjoint of QFT is called **Inverse QFT**. In particular, in the case where $N = 2^n$, we represent $|j\rangle = |j_1 \cdots j_n\rangle$, where $j = j_1 ... j_n = j_1 2^{n-1} + \cdots + j_n 2^0$. Apply QFT to $|j\rangle$, then

$$\begin{aligned}
|j\rangle \mapsto &\frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n}|k\rangle = \frac{1}{\sqrt{2^n}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1} e^{2\pi ij\left(\sum_{l=1}^{n} k_l 2^{-l}\right)}|k_1\cdots k_n\rangle \\
=&\frac{1}{\sqrt{2^n}}\sum_{k_1=0}^{1}\cdots\sum_{k_n=0}^{1}\bigotimes_{l=1}^{n} e^{2\pi ijk_l 2^{-l}}|k_l\rangle = \frac{1}{\sqrt{2^n}}\bigotimes_{l=1}^{n}\left(\sum_{k_l=0}^{1} e^{2\pi ijk_l 2^{-l}}|k_l\rangle\right) \\
=&\frac{1}{\sqrt{2^n}}\bigotimes_{l=1}^{n}\left(|0\rangle + e^{2\pi ij2^{-l}}|1\rangle\right) \\
=&\frac{\left(|0\rangle + e^{2\pi i0.j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i0.j_1\cdots j_n}|1\rangle\right)}{\sqrt{2^n}}.
\end{aligned}$$

In this case, the circuit for QFT is the following.



In this circuit, $|u_k\rangle := |0\rangle + e^{2\pi i 0.j_k \cdots j_n}|1\rangle$ and

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i j/2^k} \end{pmatrix}.$$

3.2 Quantum Fourier Transform on a Finite Abelian Group

Let G be a finite abelian group. Since a finite abelian group is isomorphic to the product of finite cyclic groups of the form $\mathbb{Z}/N\mathbb{Z}$, we can write QFT on a finite abelian group G.
Let $G \simeq \prod_{i=1}^{k} \mathbb{Z}/N_i\mathbb{Z}$. By using the following correspondence

$$x \in G \longleftrightarrow (x_1, \cdots, x_k) \in \prod_{i=1}^{k} \mathbb{Z}/N_i\mathbb{Z} \quad \Longrightarrow \quad |x\rangle \longleftrightarrow \bigotimes_{i=1}^{k} |x_i\rangle,$$

then

$$
\begin{aligned}
|x\rangle = \bigotimes_{i=1}^{k} |x_i\rangle \mapsto \bigotimes_{i=1}^{k} \left(\frac{1}{\sqrt{|N_i|}} \sum_{y_i=0}^{N_i-1} e^{2\pi i y_i x_i y_i / N_i} |y_i\rangle \right) \\
= \frac{1}{\sqrt{|G|}} \bigotimes_{i=1}^{k} \sum_{y_i \in \widehat{\mathbb{Z}/N_i\mathbb{Z}}} y_i(x_i)|y_i\rangle \\
= \frac{1}{\sqrt{|G|}} \sum_{y_1 \in \widehat{\mathbb{Z}/N_1\mathbb{Z}}} \cdots \sum_{y_k \in \widehat{\mathbb{Z}/N_k\mathbb{Z}}} (y_1, \cdots, y_k)(x_1, \cdots, x_k)|y_1, \cdots, y_k\rangle \\
= \frac{1}{\sqrt{|G|}} \sum_{\pi \in \widehat{G}} \pi(x)|\pi\rangle.
\end{aligned}
$$

This operator is also unitary because it is the tensor product of unitary operators.

3.3 Quantum Fourier Transform on a General Group

Let G be a group. The QFT of the state $|x\rangle$ corresponding to the group element $x \in G$ denoted by

$$|\hat{x}\rangle := \frac{1}{\sqrt{|G|}} \sum_{\pi \in \hat{G}} d_\pi |\pi\rangle|\pi(x)\rangle,$$

where d_π is the dimension of the representation π,

$$|\pi(x)\rangle := \sum_{j,k=1}^{d_\pi} \frac{\pi(x)_{j,k}}{\sqrt{d_\pi}} |j\rangle|k\rangle = (\pi(x) \otimes I_{d_\pi}) \sum_{k=1}^{d_\pi} \frac{1}{\sqrt{d_\pi}} |k,k\rangle.$$

If G is abelian, $|\pi(x)\rangle$ is a complex number with $|\pi(x)| = 1$. We can write the operator as

$$F_G := \sum_{x \in G} |\hat{x}\rangle\langle x| = \sum_{x \in G} \sum_{\pi \in \hat{G}} \sqrt{\frac{d_\pi}{|G|}} \sum_{j,k=1}^{d_\pi} \pi(x)_{j,k} |\pi, j, k\rangle\langle x|.$$

The operator F_G is also unitary.

Theorem 3.3.1. *F_G is unitary.*

Proof. At first, we need to calculate two things.

$$\begin{aligned}
\langle \pi(x)|\pi(y)\rangle &= \left(\sum_{j,k=1}^{d_\pi} \frac{\overline{\pi(x)_{j,k}}}{\sqrt{d_\pi}}\langle j,k|\right)\left(\sum_{j',k'=1}^{d_\pi} \frac{\pi(y)_{j',k'}}{\sqrt{d_\pi}}|j',k'\rangle\right)\\
&= \sum_{j,k=1}^{d_\pi}\sum_{j',k'=1}^{d_\pi} \frac{\overline{\pi(x)_{j,k}}}{\sqrt{d_\pi}}\frac{\pi(y)_{j',k'}}{\sqrt{d_\pi}}\langle j,k|j',k'\rangle\\
&= \frac{1}{d_\pi}\sum_{j,k=1}^{d_\pi} \overline{\pi(x)_{j,k}}\pi(y)_{j,k} = \frac{1}{d_\pi}\sum_{j,k=1}^{d_\pi} \pi(x^{-1})_{k,j}\pi(y)_{j,k}\\
&= \frac{1}{d_\pi}\sum_{k=1}^{d_\pi}\left(\pi(x^{-1})\pi(y)\right)_{k,k} = \frac{1}{d_\pi} Tr\left(\pi(x^{-1}y)\right).
\end{aligned}$$

$$\begin{aligned}
\langle \hat{x}|\hat{y}\rangle &= \left(\frac{1}{\sqrt{|G|}}\sum_{\pi\in\hat{G}} d_\pi\langle \pi,\pi(x)|\right)\left(\frac{1}{\sqrt{|G|}}\sum_{\pi'\in\hat{G}} d_{\pi'}|\pi',\pi'(x)\rangle\right)\\
&= \frac{1}{|G|}\sum_{\pi\in\hat{G}} d_\pi^2\langle\pi(x)|\pi(y)\rangle\\
&= \frac{1}{|G|}\sum_{\pi\in\hat{G}} d_\pi Tr\left(\pi(x^{-1}y)\right) = \delta_{x,y}.
\end{aligned}$$

Finally,

$$\begin{aligned}
F_G^\dagger F_G &= \left(\sum_{x\in G}|x\rangle\langle\hat{x}|\right)\left(\sum_{x'\in G}|\hat{x'}\rangle\langle x'|\right) = \sum_{x,x'\in G}|x\rangle\langle\hat{x}|\hat{x'}\rangle\langle x'|\\
&= \sum_{x,x'\in G}|x\rangle\delta_{x,x'}\langle x'| = \sum_{x\in G}|x\rangle\langle x| = I.
\end{aligned}$$

□

Chapter 4

Quantum Algorithms

In this chapter, we present quantum algorithms using QFT on $\mathbb{Z}/N\mathbb{Z}$ for some integer N.

4.1 Phase Estimation

Problem 4.1.1. *Suppose an unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi ix}$. Estimate x.*

Suppose estimate ϕ within error $1/2N$. If one wants to estimate n bit, set $N = 2^n$.

Algorithm 1.
1. Prepare the state

$$\frac{1}{N}\sum_{x=0}^{N-1}|x\rangle|\phi\rangle.$$

2. Apply $\sum_{x=0}^{N-1} |x\rangle\langle x| \otimes U^x$.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \phi x} |x\rangle |\phi\rangle.$$

Omit the second qubit.

3. Apply Inverse QFT.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \phi x} \left(\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i x y/N} |y\rangle \right) = \frac{1}{N} \sum_{y=0}^{N-1} \left(\sum_{x=0}^{N-1} e^{2\pi i (\phi - y/N) x} \right) |y\rangle.$$

4. Measure the state.

□

The measurement outcome is y with probability

$$\left| \frac{1}{N} \sum_{x=0}^{N-1} e^{2\pi i (\phi - y/N) x} \right|^2 = \frac{1}{N^2} \frac{\left|1 - e^{2\pi i N (\phi - y/N)}\right|^2}{\left|1 - e^{2\pi i (\phi - y/N)}\right|^2} = \frac{1}{N^2} \frac{\sin^2 \left(N\pi(\phi - y/N)\right)}{\sin^2 \left(\pi(\phi - y/N)\right)}.$$

Set

$$f(x) := \frac{\sin^2(N\pi x)}{\sin^2(\pi x)}, \quad g(x) := \frac{1}{\sin^2(\pi x)}.$$

Two functions have period 1 and symmetry by $x = 0$ and $x = 1/2$. So it's enough to consider these functions on $\left(0, \frac{1}{2}\right)$. We know that $\lim_{x \to 0} f(x) = N^2$. The function f is decreasing on $\left(0, \frac{1}{N}\right)$ from N^2 to 0. Since $\frac{1}{2N} \leq \frac{1}{N}$, $f(x) \geq f\left(\pm \frac{1}{2N}\right) = 1/\sin^2\left(\frac{\pi}{2N}\right)$ on $\left(-\frac{1}{2N}, \frac{1}{2N}\right)$. Since there is at least one integer in $\left(N\phi - \frac{1}{2}, N\phi + \frac{1}{2}\right)$, the probability obtaining the measurement result y such that y/N is the closest to ϕ is at least $\frac{1}{N^2} f\left(\frac{1}{2N}\right) = \frac{1}{N^2} g\left(\frac{1}{2N}\right)$. Since $f \leq g$ and g is decreasing on $[0, \frac{1}{2}]$, that probability is greater than the others.

Remark 4.1.1. *If ϕ is exactly k bit for $k \leq n$, there is y such that $\phi - y/2^n = 0$. Then, in step 4, the amplitude of $|y\rangle$ is* 1*. Therefore the others are zero becasue all state are unit vectors. In step 5, we obtain y with probability* 1*.*

4.2 Period Finding

Suppose a periodic function $f : \mathbb{Z}/N\mathbb{Z} \to S$ with period r, where a finite set S. Suppose N is a multiple of r.

Algorithm 2.
1. Prepare

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle.$$

Define the unitary operator U by $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$.
2. Apply U.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{N}} \sum_{c=0}^{r-1} \sum_{k=0}^{N/r-1} |c + rk\rangle|f(c)\rangle.$$

3. Measure the second qubit. Suppose the measurement result is $f(c)$. Then the post state is

$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N/r-1} |c + rk\rangle.$$

4. Apply Inverse QFT.

$$\begin{aligned}
&\frac{1}{\sqrt{N}} \sum_{k=0}^{N/r-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i(c+rk)j/N} |j\rangle \right) \\
=&\frac{1}{N} \sum_{j=0}^{N-1} e^{-2\pi ijc/N} \left(\sum_{k=0}^{N/r-1} e^{-2\pi ijrk/N} \right) |j\rangle \\
=&\frac{1}{N} \sum_{j:jr/N\in\mathbb{Z}} e^{-2\pi ijc/N} \, (N/r) \, |j\rangle \\
=&\frac{1}{r} \sum_{j=0}^{r-1} e^{-2\pi ijc/N} \left| \frac{N}{r} j \right\rangle .
\end{aligned}$$

The second equality uses the following fact that

$$\sum_{k=0}^{N/r-1} e^{-2\pi ijrk/N} = \begin{cases} 0, & \text{if } jr/N \notin \mathbb{Z} \\ N/r, & \text{if } jr/N \in \mathbb{Z} \end{cases} .$$

5. Measure the first qubit.

□

The measurement outcomes are 0, N/r, $\cdots$, $N(r-1)/r$ with uniform probability. Divide N. Suppose the result is k/r. The denominator of k/r is $r/\gcd(k,r)$. Repeat the above procedure, we suppose another denominator $r/\gcd(k',r)$. If $\gcd(k,k') = 1$, $\mathrm{lcm}(r/\gcd(k,r), r/\gcd(k',r)) = r$. The probability that two integers have p as a factor is $1/p^2$, and $\prod_{p:prime}\left(1-\frac{1}{p^2}\right) = \frac{6}{\pi^2} \approx 0.61$. This means that the algorithm success with probability at least 0.61.

4.3 Period Finding on $\mathbb{Z}$

Problem 4.3.1. *Suppose a periodic function $f : \mathbb{Z} \to S$ with period r, where a finite set S. Find r.*

Since $\mathbb{Z}$ is not finite, we cannot use QFT on $\mathbb{Z}$. To use QFT, we consider $\mathbb{Z}$ modulo N for a suitable N. Then $f : \mathbb{Z}/N\mathbb{Z} \to S$ may not be a periodic function. But f looks like a periodic function with period r, where N is not a multiple of r. Set a proper N such that $N \geq 3r^2$. In fact, we cannot choose such N since we don't know r. We start with $N = 2^1$ and repeatedly double N until $N \geq 3r^2$. The runtime incurred by this procedure is only $poly(\log r)$.

Algorithm 3.
1. Prepare

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle.$$

Define the unitary operator U by $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$.
2. Apply U.

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{N}} \sum_{c=0}^{r-1} \sum_{k=0}^{n_c-1} |c + rk\rangle|f(c)\rangle,$$

where

$$n_c = \begin{cases} \lfloor \frac{N}{r} \rfloor + 1 & \text{if } \exists\ k \in \mathbb{Z} \text{ s.t } r \lfloor \frac{N}{r} \rfloor < c + rk \leq N\} \\ \lfloor \frac{N}{r} \rfloor & otherwise \end{cases}.$$

The n_c means the number of $f(c)$ from $f(0)$ to $f(N-1)$.
3. Measure the second qubit. Suppose the measurement result is $f(c)$. Then the post state is

$$\frac{1}{\sqrt{n_c}} \sum_{k=0}^{n_c-1} |c + rk\rangle.$$

4. Apply QFT.

$$\begin{aligned}&\frac{1}{\sqrt{n_c}}\sum_{k=0}^{n_c-1}\left(\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{2\pi i(c+rk)y/N}|y\rangle\right)\\=&\frac{1}{\sqrt{n_c}}\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\left(\sum_{k=0}^{n_c-1}e^{2\pi i(c+rk)y/N}\right)|y\rangle.\end{aligned}$$

5. Measure the first qubit.

□

The measurement outcome m with probability

$$\left|\frac{1}{\sqrt{n_c}}\frac{1}{\sqrt{2^n}}\sum_{k=0}^{n_c-1}e^{2\pi i(c+rk)y/N}\right|^2=\frac{1}{n_c}\frac{1}{N}\frac{|1-e^{2\pi iryn_c/N}|^2}{|1-e^{2\pi iry/N}|^2}=\frac{1}{n_c}\frac{1}{N}\frac{\sin^2(\pi ryn_c/N)}{\sin^2(\pi ry/N)}.$$

The measurement outcome m, which has a high probability of being obtained, is the closest integer to multiples of N/r. At first, we consider the lower bound of the probability.

Lemma 4.3.1. *Let m be a measurement outcome the closest integer to multiples of N/r.*

$$p(m)\geq\frac{1}{N}\frac{1}{n_c}\frac{\sin^2(\pi rn_c/2N)}{\sin^2(\pi r/2N)}.$$

Proof. Set

$$f(x):=\frac{\sin^2(\pi rn_c/2N)}{\sin^2(\pi r/2N)}.$$

The function f has period N/r and symmetry by $x=0$ and $x=N/2r$. So it's enough to consider f on $\left(0,\frac{N}{2r}\right)$. For $k\in\mathbb{Z}$, $\lim_{x\to 0}f(x)=n_c^2$. f is decreasing on $[0,N/rn_c]$ from n_c^2 to 0. Since $1/2\leq N/rn_c$,

$$f(x)\geq f\left(\pm\frac{1}{2}\right)=\frac{\sin^2(\pi rn_c/2N)}{\sin^2(\pi r/2N)}$$

on $\left(-\frac{1}{2}, \frac{1}{2}\right)$. Since there is at least one integer in $\left(k\frac{N}{r} - \frac{1}{2}, k\frac{N}{r} + \frac{1}{2}\right)$, so we obtain the outcome m such that m is the closest to the multiples of N/r with probability at least

$$\frac{1}{N}\frac{1}{n_c}\frac{\sin^2(\pi r n_c/2N)}{\sin^2(\pi r/2N)}$$

□

Denote m_k by the closest integer to the $k\frac{N}{r}$. Set $M_k := \mathbb{Z} \cap \left(k\frac{M}{r} - \frac{N}{2r}, k\frac{M}{r} + \frac{N}{2r}\right) - \{m_k\}$. If we prove that $f(m_k) \geq f(n)$ for all $n \in M_k$ for each $k \in \mathbb{Z}$, the probability obtaining the measurement outcome m_k is higher than others.

Lemma 4.3.2. *$f(m_k) \geq f(n)$ for all $n \in M_k$ for each $k \in \mathbb{Z}$.*

Proof. Define f as in the previous proof and Set

$$g(x) := 1/\sin^2(\pi r x/N).$$

Then g also has period $\frac{N}{r}$ and symmetry by $x = 0$, and $x = \frac{N}{2r}$ and $f \leq g$ and g is decreasing on $\left(0, \frac{N}{2r}\right)$. So we can assume that $k = 0$ and consider these functions on $\left(0, \frac{N}{2r}\right)$. For any $n \in M_0$,

$$\left|m_0 - \frac{kN}{r}\right| < \frac{1}{2} \Rightarrow \quad \left|m_0 - \frac{kN}{r}\right| \leq \frac{r-1}{2r} < \frac{1}{2}, \quad \frac{r+1}{2r} \leq \left|n - \frac{kN}{r}\right| \leq \frac{N}{2r},$$
$$\left|m_0 - \frac{kN}{r}\right| = \frac{1}{2} \Rightarrow \quad \frac{3}{2} \leq \left|n - \frac{kN}{r}\right| \leq \frac{N}{2r}.$$

Then $f(m_0) \geq f(1/2)$ and $g\left((r+1)/2r\right) \geq g(n) \geq f(n)$. If we obtain $f(1/2) > g\left((r+1)/2r\right)$, the desired result follows. To prove that, the amount of decrease from $g(1/2)$ to $f(1/2)$ is less than that of decrease from $g(1/2)$ to $g(1/2 + 1/2r)$. For the latter, consider a line l passing through

$(N/2r, 1)$ and $(1/2, g(1/2))$. Since g is convex, $g \leq l$ on $[1/2, N/2r]$. It's enough to show

$$g(1/2) - f(1/2) < \frac{g(1/2) - g(N/2r)}{N/2r - 1/2} \frac{1}{2r}.$$

If $N \geq 3r^2$ and $N \geq 3r$,

$$\begin{aligned} LHS =& \frac{1 - \sin^2(\pi r n_c/2N)}{\sin^2(\pi r/2N)} \leq \frac{1 - \sin^2\left((\pi r)(\frac{N}{r} - 1)/2N\right)}{\sin^2(\pi r/2N)} \\ =& \frac{1 - \sin^2(\pi/2 - \pi r/2N)}{\sin^2(\pi r/2N)} = \frac{1 - \cos^2(\frac{\pi r}{2N})}{\sin^2(\pi r/2N)} = 1, \quad \text{and} \\ RHS =& \frac{1/\sin^2(\pi r/2N) - 1}{N - r} = \frac{1 - \sin^2(\pi r/2N)}{(N-r)\sin^2(\pi r/2N)} = \frac{1}{(N-r)} \cot^2\left(\frac{\pi r}{2N}\right) \\ \geq& \frac{1}{(N-r)} \left(\frac{\pi}{2\sqrt{3}} \frac{2N}{\pi r}\right)^2 = \frac{N^2}{(N-r)(\sqrt{3}r)^2} \geq 1. \end{aligned}$$

□

Now, we get k/r using the continued fraction of $m/2^n$. For $k = 0, \cdots, r-1$, since we choose N such that $N \geq 3r^2 \geq r^2$,

$$\left| m_k - \frac{kN}{r} \right| \leq \frac{1}{2} \quad \Rightarrow \quad \left| \frac{m_k}{N} - \frac{k}{r} \right| \leq \frac{1}{2N} \leq \frac{1}{2r^2}.$$

Definition 4.3.1. *A continued fraction is defined by a collection $a_0, \cdots, a_N$ of positive integers such that*

$$[a_0, \cdots, a_N] := a_0 + \frac{1}{a_1 + \frac{1}{\cdots + \frac{1}{a_N}}}.$$

Define the n-th convergent $(0 \leq n \leq N)$ of this continued fraction for $[a_0, \cdots, a_n]$.

Theorem 4.3.1. *Suppose s/r is a rational number such that*

$$\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2r^2}.$$

Then s/r is a convergent of the continued fraction for ϕ.

Lemma 4.3.3. *If $N > 3r^2$ and $\left|\frac{m}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}$, then k/r will be the only convergent of m/N with its denominator $\leq \sqrt{3N}$.*

Proof. Suppose a/b is a convergent of m/N satisfying $\left|\frac{m}{N} - \frac{k}{r}\right| \leq \frac{1}{2N}$ and $b \leq \sqrt{3N}$.

$$\left|\frac{a}{b} - \frac{k}{r}\right| \leq \left|\frac{a}{b} - \frac{m}{N}\right| + \left|\frac{m}{N} - \frac{k}{r}\right| \leq \frac{1}{N}.$$

Then $|ar - bk| \leq br/N < 1$. Since both ar and bk are integers, $ar = bk$. □

Now we obtain k/r with high probability. From this point forward, it is the same as the case where $r|N$.

4.4 Period Finding Using Phase Estimation

Now we solve the same problem with other way, using phase estimation. Recall the Problem 4.3.1:

Problem 4.3.1. *Suppose a periodic function $f : \mathbb{Z} \to S$ with period r, where a finite set S. Find r.*

Set N such that $N \geq 3r^2$. We need the following lemma for using the phase estimation.

Lemma 4.4.1. *For each $\ell = 0, \cdots, r-1$, define a state*

$$|f_\ell\rangle := \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i \ell x/r} |f(x)\rangle.$$

Then, for $x \in \mathbb{Z}/N\mathbb{Z}$,

$$|f(x)\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x/r} |f_\ell\rangle.$$

Proof.

$$\begin{aligned}\frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x/r} |f_\ell\rangle =& \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \ell x/r} \left(\frac{1}{\sqrt{r}} \sum_{y=0}^{r-1} e^{-2\pi i \ell x/r} |f(y)\rangle \right) \\ =& \frac{1}{r} \sum_{y=0}^{r-1} \sum_{\ell=0}^{r-1} e^{2\pi i (x-y)\ell/r} |f(y)\rangle = |f(x)\rangle.\end{aligned}$$

□

Algorithm 4.

1. Prepare

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|0\rangle.$$

Define the unitary operator U by $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$.

2. Apply U.

$$\begin{aligned}\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle|f(x)\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left(\frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{2\pi i \ell x/r} |f_\ell\rangle \right) \\ &= \frac{1}{\sqrt{rN}} \sum_{\ell=0}^{r-1} \sum_{x=0}^{N-1} e^{2\pi i \ell x/r} |x\rangle|f_\ell\rangle.\end{aligned}$$

3. Measure the second qubit. Suppose the measurement result is f_ℓ. Then the post state is

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} e^{2\pi i \ell x/r} |x\rangle.$$

After this step, it is the same as the Algorithm 1.

□

From the obtained measurement outcome, we have ℓ/r using the continued fraction, and finally we have r.

4.5 Order Finding

Problem 4.5.1. *Let x, N are positive integers such that* $\gcd(x, N) = 1$. *Find the order ord(x) of x modulo N.*

We choose a large N_0 such that $3\,(ord(x))^2$. Unlike the period finding, we know $ord(x) \leq N$. So it is sufficient to choose $N_0 \geq 3N^2$.

Algorithm 5.
1. Prepare

$$\frac{1}{\sqrt{N_0}} \sum_{x=0}^{N_0-1} |x\rangle|1\rangle.$$

Define $U : |x\rangle|y\rangle \mapsto |x\rangle|n^x y \pmod{N_0}\rangle$.
2. Apply U.

$$\frac{1}{\sqrt{N_0}} \sum_{x=0}^{N_0-1} |x\rangle|n^x (\mathrm{mod}\ N_0)\rangle.$$

After this step, it is the same as the Algorithm 3.

□

4.6 Factorization

Problem 4.6.1. *Factorize an integer N.*

The following algorithm returns an integer as a factor in N. If we get the integer x, use the algorithm from the top with N/x instead of N.

Algorithm 6.
1. If N is even, return the factor 2.
From now on, we assume N is odd integer.
2. Choose a number $a \in \{1, \cdots, N-1\}$. Compute $\gcd(a, N)$ using the Euclidean algorithm. If $\gcd(a, N) \not\equiv 1$, return $\gcd(a, N)$. If $\gcd(a, N) = 1$, go next step.
3. Determine the order r of a modulo N using the Order Finding.
4. If r is odd, the algorithm has failed. Then return to the step 1. If r is even, go next step.
5. If $a^{r/2} \equiv -1 \pmod{N}$, the algorithm fails. If $a^{r/2} \not\equiv -1 \pmod{N}$, then return a non trivial factor of $\gcd(a^{r/2} - 1, N)$ or $\gcd(a^{r/2} + 1, N)$.

□

Theorem 4.6.1. *Suppose* $1 \leq x \leq N$ *such that* $x^2 \equiv 1 \pmod{N}$ *and* $x \not\equiv \pm 1 \pmod{N}$. *Then at least one of* $\gcd(x-1, N)$ *and* $\gcd(x+1, N)$ *is a non-trivial factor of* N.

By definition of order, $a^r \equiv 1$ but $a^{r/2} \not\equiv 1$. So if $a^{r/2} \not\equiv -1$, by thm, at least one of $\gcd(a^{r/2} - 1, N)$ and $\gcd(a^{r/2} + 1, N)$ is a non-trivial factor of N. Now we show this algorithm successes with high probability.

Lemma 4.6.1. *Let* $N = p_1^{m_1} \cdots p_k^{m_k}$ *for* $k \geq 2$ *and distinct odd primes* p_i, *and* x *be uniformly at random in* $\mathbb{Z}/N\mathbb{Z}^\times$. *Then* $r := ord(x)$ *is even and* $x^{r/2} \neq \pm 1 \pmod{N}$ *with probability at least* $1 - (1/2)^{k-1}$.

Proof. By the Chinese remainder theorem, choosing x uniformly at random from $\mathbb{Z}/N\mathbb{Z}^\times$ is equivalent to choosing x_i uniformly at random $\mathbb{Z}/p_i^{m_i}\mathbb{Z}^\times$ for each i independently.

Let $r_i := ord(x_i)$. $r = \mathrm{lcm}\{r_1, \cdots, r_k\}$. Let $r_i = 2^{t_i} s_i$ and s_i are odd. If r is odd, then r_i is odd, and $t_i = 0$, and all $t_i = 0$. If r is even and $x^{r/2} = -1$

(mod N), then $x_i^{r/2} = -1 \pmod{p_i^{m_i}}$, and $r_i \nmid r/2$, and r/r_i is odd, and the number of factor 2 in r = the number of factor 2 in r_i, and all t_i are equal. This means that $p([r$:odd] or [r:even and $x^{r/2} = -1 \pmod N$])$\leq p$(all t_i is equal). To calculate RHS, we need to prove

$$p(t_i = \text{a nonnegative integer } j) \leq \frac{1}{2}. \tag{4.6.1}$$

In other words, if we choose y uniformly at random in $\mathbb{Z}/p^m\mathbb{Z}^\times$ and $ord(y) = 2^{t_y}s_y$ for s_y is odd, the number of y such that $t_y = j$ is at most $|\mathbb{Z}/p^m\mathbb{Z}^\times|/2$. Let $|\mathbb{Z}/p^m\mathbb{Z}^\times| =: 2^u v$, where v is odd. Let g be a generator of $\mathbb{Z}/p^m\mathbb{Z}^\times$. Then $g^{2^u v} \equiv 1 \pmod{p^m}$. For any $b \in \mathbb{Z}/2^u v\mathbb{Z}$, let $ord(g^b) =: 2^{u_b}v_b$. Choosing $y \in \mathbb{Z}/p^m\mathbb{Z}^\times$ is equivalent to choosing $b \in \mathbb{Z}/2^u v\mathbb{Z}$. The number of y such that $t_y = j$ is the same as the number of b such that $u_b = j$. Therefore (4.6.1) means that The number of $b \in \mathbb{Z}/2^u v\mathbb{Z}$ such that $u_b = j$ is at most $2^u v/2$. Then $u_b \leq u$ and $2^u v | b2^{u_b}v_b$. If b is odd, $u \leq u_b$. So $u_b = u$. The number of such b is at least $2^u v/2$. If b is even, $u_b \leq u - 1$. The number of b such that $u_b \leq u - 1$ is at least $2^u v/2$. Thus the size of two sets is equal with $2^u v/2$. We complete to prove (4.6.1). Finally,

$$\begin{aligned} p(\text{all } t_i \text{ is equal}) &= \sum_{j=0}^{\infty} p(\text{all } t_i = j) \\ &= \sum_{j=0}^{\infty} \prod_{i=1}^{k} p(t_i = j) \\ &\leq \left(\frac{1}{2}\right)^{k-1} \sum_{j=0}^{\infty} p(t_1 = j) = \left(\frac{1}{2}\right)^{k-1}. \end{aligned}$$

Therefore $p\left(r\text{:even and } x^{r/2} \neq -1 \pmod N\right) \geq 1 - \left(\frac{1}{2}\right)^{k-1}$. □

4.7 Discrete Logarithm

Problem 4.7.1. *Let a, N be integers such that $gcd(a, N) = 1$ and $b = a^s \pmod N$ for some integer s. Find s.*

Assume we already know the order of a is r. Define $f : \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} \to S$ by $(x, y) \mapsto b^x a^y$.

Algorithm 7.

1. Prepare

$$\frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle|0\rangle.$$

Define the unitary operator U by $|x_1\rangle|x_2\rangle|y\rangle \mapsto |x_1\rangle|x_2\rangle|y + f(x_1, x_2)\rangle$.

2. Apply U.

$$\frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle|f(x,y)\rangle = \frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle|a^{sx+y}\rangle.$$

3. Measure the third qubit. Suppose the outcome is a^c. $L_c := \{(x, y) \in \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z} : sx + y = c\}$.

$$|L_c\rangle := \frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}|x, c - sx\rangle.$$

4. Apply QFT over $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ on the first two qubits.

$$\begin{aligned}
&\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1}\left(\frac{1}{\sqrt{r}}\sum_{x'=0}^{r-1}e^{2\pi i x x'/r}|x'\rangle\right)\left(\frac{1}{\sqrt{r}}\sum_{y'=0}^{r-1}e^{2\pi i(c-sx)y'/r}|y'\rangle\right)\\
=&\frac{1}{r\sqrt{r}}\sum_{x,x',y'=0}^{r-1}e^{2\pi i(xx'+(c-sx)y')/r}|x', y'\rangle\\
=&\frac{1}{\sqrt{r}}\sum_{y'=0}^{r-1}e^{2\pi i c y'/r}|y's, y'\rangle.
\end{aligned}$$

The second equality uses the following fact that

$$\sum_{x=0}^{r-1} e^{2\pi i(x'-sy')s/r} = \begin{cases} r, & x'-sy' \equiv 0 \\ 0, & x'-sy' \neq 0 \end{cases}.$$

5. Measure the second qubit.

□

We obtain a pair $(y's, y')$ for a uniformly random $y' \in \mathbb{Z}/r\mathbb{Z}$. Repreat the above process, We obtain another pair $(z's, z')$. If $\gcd(y', z') = 1$, then $\exists\lambda_1, \lambda_2$ such that $\lambda_1 y' + \lambda_2 z' = 1$. we obtain $s = \lambda_1(sy') + \lambda_2(sz')$ with high probability.

4.8 Discrete Logarithm Using Phase Estimation

We recall the Problem 4.7.1:

Problem 4.7.1. *Let a, N be integers such that $gcd(a, N) = 1$ and $b = a^s$ (mod N) for some integer s. Find s.*

We also need the following lemma for using the phase estimation.

Lemma 4.8.1. *For each $\ell \in \mathbb{Z}/r\mathbb{Z}$, define a state*

$$|f_\ell\rangle := \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i\ell x/r} |f(0, x)\rangle.$$

Then, for $x_1, x_2 \in \mathbb{Z}/r\mathbb{Z}$,

$$|f(x_1, x_2)\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i\ell(sx_1+x_2)/r} |f_\ell\rangle.$$

Proof.

$$\begin{aligned}
&\frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1} e^{2\pi i\ell(sx_1+x_2)/r}|f_\ell\rangle \\
=&\frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1} e^{2\pi i\ell(sx_1+x_2)/r}\left(\frac{1}{\sqrt{r}}\sum_{x=0}^{r-1} e^{-2\pi i\ell x/r}|f(0,x)\rangle\right) \\
=&\frac{1}{r}\sum_{\ell=0}^{r-1}\sum_{x=0}^{r-1} e^{2\pi i\ell(sx_1+x_2-x)/r}|f(0,x)\rangle \\
=&\frac{1}{r}\sum_{x=0}^{r-1}\left(\sum_{\ell=0}^{r-1} e^{2\pi i\ell(sx_1+x_2-x)/r}\right)|f(0,x)\rangle \\
=&|f(0,sx_1+x_2)\rangle = |f(x_1,x_2)\rangle.
\end{aligned}$$

□

Algorithm 8.

1. Prepare

$$\frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle|0\rangle.$$

Define the unitary operator U by $|x_1\rangle|x_2\rangle|y\rangle \mapsto |x_1\rangle|x_2\rangle|y+f(x_1,x_2)\rangle$.

2. Apply U.

$$\begin{aligned}
&\frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle|f(x,y)\rangle \\
=&\frac{1}{r}\sum_{x=0}^{r-1}\sum_{y=0}^{r-1}|x\rangle|y\rangle\left(\frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1} e^{2\pi i\ell(sx+y)/r}|f_\ell\rangle\right) \\
=&\frac{1}{r\sqrt{r}}\sum_{\ell=0}^{r-1}\left(\sum_{x=0}^{r-1} e^{2\pi i\ell sx/r}|x\rangle\right)\left(\sum_{y=0}^{r-1} e^{2\pi i\ell y/r}|y\rangle\right)|f_\ell\rangle.
\end{aligned}$$

3. Measure the second qubit. Suppose the measurement result is f_ℓ. Then the post state is

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

After this step, it is the same as the Algorithm 1.

□

From the obtained measurement outcome, we have $(\ell s, \ell)$ using the continued fraction, and finally we have s.

Chapter 5

Hidden Subgroup Problem

For a group G, we are given a function $f : G \to S$, where S is a finite set. We say f **hides** a subgroup H if $f(x) = f(y)$ if and only if $x - y \in H$ for any $x, y \in G$. In other words, f is constant on the cosets of the subgroup H, and distinct on each coset.

Problem 5.0.1 (Hidden Subgroup Problem)**.** *Suppose $f : G \to S$ hides a subgroup H of a group G. Find H.*

We denote Hidden Subgroup Problem by HSP, shortly.

5.1 Abelian Hidden Subgroup Problem

Abelian HSP is a HSP where G is abelian. Some algorithms in the last chapter are examples of Abelian HSP.

Example 5.1.1 (Period finding)**.** *Suppose $f : \mathbb{Z} \to S$ has a period r. That is, $f(0), \cdots, f(r-1)$ are all distinct and there exists the smallest integer r such that $f(x+r) = f(x)$ for all $x \in \mathbb{Z}$. Then f hides a subgroup $H = \langle r \rangle$.*

Example 5.1.2 (Order finding)**.** *Let a, N be integers such that* $\gcd(a, N) = 1$ *and r be the order of a modulo N. Suppose $f : \mathbb{Z} \to S$ by $x \mapsto a^x \pmod N$. Then f hides a subgroup $H = \langle r \rangle$.*

Example 5.1.3 (Discrete logarithm)**.** *Let a, N be integers such that* $\gcd(a, N) = 1$ *and r be the order of a modulo N. Let $b = a^s \pmod N$ for some integer s. Suppose $f : \mathbb{Z}_r \times \mathbb{Z}_r \to S$ by $(x_1, x_2) \mapsto b^{x_1} a^{x_2} \pmod N$. f hides a subgroup $H = \{(\ell, -s\ell) : \ell \in \mathbb{Z}_r\}$. Find H.*

Proof. We need to show that for $(x_1, x_2) \in \mathbb{Z}_r \times \mathbb{Z}_r$,

$$f(x_1, x_2) = f(y_1, y_2) \Leftrightarrow (x_1, x_2) - (y_1, y_2) \in H.$$

Suppose $f(x_1, x_2) = f(y_1, y_2)$. Then $s(x_1 - y_1) + x_2 - y_2 \equiv 0 \pmod r$. Let $\ell = x_1 - y_1$. Then $x_2 - y_2 \equiv -s\ell \pmod r$. For the converse, suppose $x_2 - y_2 = -s(x_1 - y_1)$. Then $1 = a^{x_2 - y_2 + s(x_1 - y_1)} = b^{x_1 - y_1} a^{x_2 - y_2}$, and $b^{x_1} a^{x_2} = b^{y_1} a^{y_2}$. Therefore $f(x_1, x_2) = f(y_1, y_2)$. □

The following is an algorithm for solving the Abelian HSP.

Algorithm 9. Suppose G is finite.

1. Prepare

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle.$$

Define a unitary operator U by $|x\rangle|y\rangle \mapsto |x\rangle|y + f(x)\rangle$.

2. Apply U. Let $G = \cup_{i=0}^{\frac{|G|}{|H|}-1} (a_i + H)$.

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{i=0}^{\frac{|G|}{|H|}-1} \sum_{h \in H} |a_i + h\rangle |f(a_i)\rangle.$$

3. Measure the second qubit. Suppose the measurement outcome is $f(c)$. Then the post state is

$$\frac{1}{\sqrt{\frac{|H|}{|G|}}}\frac{1}{\sqrt{|G|}}\sum_{h\in H}|c+h\rangle = \frac{1}{\sqrt{|H|}}\sum_{h\in H}|c+h\rangle.$$

4. Apply QFT.

$$\begin{aligned}
&\frac{1}{\sqrt{|H|}}\sum_{h\in H}\left(\frac{1}{\sqrt{|G|}}\sum_{\pi\in\hat{G}}\pi(c+h)|\pi\rangle\right)\\
=&\frac{1}{\sqrt{|H|}}\frac{1}{\sqrt{|G|}}\sum_{\pi\in\hat{G}}\pi(c)\left(\sum_{h\in H}\pi(h)\right)|\pi\rangle\\
=&\sqrt{\frac{|H|}{|G|}}\sum_{\pi|_H=1}\pi(c)|\pi\rangle.
\end{aligned}$$

The second equality uses the following fact that

$$\sum_{h\in H}\pi(h) = \begin{cases} |H| & \text{if } H\subset ker\pi \\ 0 & \text{if } \exists\ h_0\in H \text{ s.t } \pi(h_0)\neq 1 \end{cases}.$$

For the second case, suppose $\pi(h_0)\neq 1$.

$$\sum_{h\in H}\pi(h) = \sum_{h\in H}\pi(h_0+h) = \pi(h_0)\sum_{h\in H}\pi(h).$$

Thus $\sum_{h\in H}\pi(h)=0$.

5. Measure.

□

We obtain $\pi\in\hat{G}$ such that $\pi(h)=1$ for all $h\in H$ with uniform propability $\frac{|H|}{|G|}$. Repeat the entire process t times, Then we get $\pi_1,\cdots,\pi_t$. Set

$$K_t := \bigcap_{1\le i\le t} ker\pi_i,$$

where $ker\pi := \{g \in G : \pi(g) = 1\}$. Then $H \leq K_t \leq G$. After $t+1$ process, suppose $K_t \neq H$ and π_{t+1} such that $K_t \subset ker\pi_{t+1}$. Then $K_{t+1} = K_t$. This probability is

$$\sum_{\pi: K_t \subset ker\pi} \frac{|H|}{|G|} = \frac{|H|}{|G|}\frac{|G|}{|K_t|} = \frac{|H|}{|K_t|} \leq 1/2.$$

Since $\{K_t\}$ is reduced by half (or more) with probability at least $1/2$. Define indicator random variables $X_1, \cdots, X_T$ by

$$X_i = \begin{cases} 1, & \text{if } K_i = H \text{ or } K_{i+1} \subsetneq K_i \\ 0, & \text{otherwise} \end{cases}.$$

Then we have $\mathbb{E}(X_i) = p(X_i = 1) \geq 1/2$, and $\mathbb{E}(\sum X_i) = \sum \mathbb{E}(X_i) \geq T/2$.

Lemma 5.1.1. *If $G =: K_0 \supsetneq K_1 \supsetneq \cdots \supsetneq K_s = K_r$ for all $r \geq s$, $s \leq \log_2 |G|$.*

Proof. If $s > \log |G|$, $2^s > |G|$.

$$|K_s| \leq \frac{|K_{s-1}|}{2} \leq \cdots \leq \frac{|K_1|}{2^{s-1}} \leq \frac{|G|}{2^s} < 1.$$

□

If $\sum X_i > \log_2 |G|$, this algorithm successes.

Lemma 5.1.2. *$Y_i := \mathbb{E}[\sum^T X_i | X_1, \cdots, X_i]$. Then Y_i is a martingale.*

Proof.

$$\begin{aligned} \mathbb{E}[Y_i | X_1, \cdots, X_{i-1}] &= \mathbb{E}[\mathbb{E}[\sum X_i | X_1, \cdots, X_i] | X_1, \cdots, X_{i-1}] \\ &= \mathbb{E}[\sum X_i | X_1, \cdots, X_{i-1}] = Y_{i-1} \end{aligned}$$

□

Let X'_k be an independent copy of X_k. $\sum X'_i := \sum X_i - X_k + X'_k$.

$$\begin{aligned}
\mathbb{E}(\sum X'_i | X_1, \cdots, X_k) &= \mathbb{E}(\sum X'_i | X_1, \cdots, X_{k-1}) = Y_{k-1} \\
|Y_i - Y_{i-1}| &= |\mathbb{E}(\sum X_i | X_1, \cdots, X_i) - \mathbb{E}(\sum X_i | X_1, \cdots, X_{i-1})| \\
&= |\mathbb{E}(\sum X_i | X_1, \cdots, X_i) - \mathbb{E}(\sum X'_i | X_1, \cdots, X_{i-1}, X_i)| \\
&= |\mathbb{E}(X_k - X'_k | X_1, \cdots, X_n)| \leq 1.
\end{aligned}$$

Theorem 5.1.1 (Azuma's inequality)**.** *Let $(Y_i)_{i=1}^n$ be a martingale. $|Y_i - Y_{i-1}| \leq c_i$ for all i. Then*

$$\left.\begin{array}{l} p(Y_n \geq Y_0 + \lambda) \\ p(Y_n \leq Y_0 - \lambda) \end{array}\right\} \leq \exp\left(-\frac{\lambda^2}{2\sum_{i=1}^n c_i^2}\right).$$

By Azuma's inequality,

$$p\left(\sum^T X_i \leq T/2 - \lambda\right) \leq p\left(\sum^T X_i \leq \mathbb{E}(\sum^T X_i) - \lambda\right) \leq e^{-\lambda^2/2T}.$$

If $T = a \log |G|$ and $\lambda = b \log |G|$ such that $\frac{a}{2} - b = 1$,

$$p\left(\sum X_i \leq \log |G|\right) \leq \exp\left(-\frac{b^2}{2a} \log |G|\right).$$

Therefore we get H with probability at least $1 - \exp\left(-\frac{b^2}{2a} \log |G|\right)$.

5.2 Normal Hidden Subgroup Problem

Problem 5.2.1. *Suppose $f : G \to S$ hides a normal subgroup H of G. Find H.*

Algorithm 10. *nhsp*

1. Prepare

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|0\rangle.$$

Define a unitary operator U by $|x\rangle|y\rangle \mapsto |x\rangle|y+f(x)\rangle$.

2. Apply U. Let $G=\cup_{i=0}^{\frac{|G|}{|H|}-1}(a_iH)$.

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle=\frac{1}{\sqrt{|G|}}\sum_{i=0}^{\frac{|G|}{|H|}-1}\sum_{h\in H}|a_ih\rangle|f(a_i)\rangle.$$

3. Measure the second qubit. Suppose the measurement outcome is $f(c)$. Then the post state is

$$\frac{1}{\sqrt{\frac{|H|}{|G|}}}\frac{1}{\sqrt{|G|}}\sum_{h\in H}|ch\rangle=\frac{1}{\sqrt{|H|}}\sum_{h\in H}|ch\rangle.$$

4. Apply QFT.

$$\begin{aligned}
&\frac{1}{\sqrt{|H|}}\sum_{h\in H}\left(\frac{1}{\sqrt{|G|}}\sum_{\pi\in\hat{G}}d_\pi|\pi,\pi(ch)\rangle\right)\\
=&\frac{1}{\sqrt{|G||H|}}\sum_{h\in H}\sum_{\pi\in\hat{G}}d_\pi|\pi\rangle|\pi(ch)\rangle\\
=&\frac{1}{\sqrt{|G||H|}}\sum_{\pi\in\hat{G}}d_\pi|\pi\rangle\left(|\pi(c)\sum_{h\in H}\pi(h)\rangle\right)\\
=&\sqrt{\frac{|H|}{|G|}}\sum_{\pi:H\subset ker\pi}d_\pi|\pi\rangle|\pi(c)\rangle.
\end{aligned}$$

The third equality uses the following fact that

$$\sum_{h\in H}\pi(h)=\begin{cases}|H|I & \text{if } H\subset ker\pi\\ 0 & \text{if } \exists\ h_0\in H \text{ s.t } \pi(h_0)\neq 1\end{cases}.$$

For the second case, suppose $\pi(h_0) \neq 1$ for some $h_0 \neq 1$. Then

$$\sum_{h\in H} \pi(h)\pi(x) = \sum_{h\in H} \pi(xx^{-1}hx) = \sum_{h\in H} \pi(x)\pi(x^{-1}hx) = \pi(x)\sum_{h\in H} \pi(h)$$

since H is a normal subgroup of G. The operator $\sum_{h\in H}\pi(h)$ commutes with $\pi(x)$ for all $x \in G$. By Schur's lemma, then $\sum_{h\in H}\pi(h)$ is a multiple of the identity. Therefore $\sum_{h\in H}\pi(h) = 0$ because

$$\sum_{h\in H} \pi(h) = \sum_{h\in H} \pi(h_0h) = \pi(h_0)\sum_{h\in H} \pi(h).$$

$$\sqrt{\frac{|H|}{|G|}} \sum_{H\subset ker\pi} d_\pi|\pi\rangle|\pi(c)\rangle = \sum_{H\subset ker\pi} \frac{\sqrt{d_\pi|H|}}{\sqrt{|G|}} \sum_{j,k=1}^{d_\pi} \pi(c)_{j,k}|\pi\rangle|j,k\rangle.$$

5. Measure the first qubit.

□

The probability of obtaining π when measuring the first qubit is

$$\begin{aligned}\sum_{j,k=1}^{d_\pi} \left|\frac{\sqrt{d_\pi|H|}}{\sqrt{|G|}}\pi(c)_{j,k}\right|^2 &= \sum_{j,k=1}^{d_\pi} d_\pi\frac{|H|}{|G|}\pi(c^{-1})_{k,j}\pi(c)_{j,k} \\ &= \sum_{k=1}^{d_\pi} d_\pi\frac{|H|}{|G|}\pi(c^{-1}c)_{k,k} \\ &= d_\pi^2\frac{|H|}{|G|}.\end{aligned}$$

Repeat the entire process t times, Then we get $\pi_1, \cdots, \pi_t$. Set

$$K_t := \bigcap_{1\leq i\leq t} ker\pi_i.$$

After $t+1$ process, suppose $K_t \neq H$ and we obtain a π_{t+1} such that $K_t \subset ker\pi_{t+1}$. Then $K_{t+1} = K_t$. This probability is

$$\sum_{K_t \subset ker\pi} d_\pi^2 \frac{|H|}{|G|} = \frac{|H|}{|G|} \sum_{K_t \subset ker\pi} d_\pi^2 = \frac{|H|}{|G|}\frac{|G|}{|K_t|} = \frac{|H|}{|K_t|} \leq \frac{1}{2}.$$

As the Abelian HSP, we obtain H with high probability.

5.3 Hidden Subgroup Problem on the Dihedral Group D_N

Problem 5.3.1. *Suppose $f : D_N \to S$ hides a subgroup H of D_N. Find H.*

Note that $D_N \cong \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$ with $(x,a)\cdot(y,b) = (x+(-1)^a y, a+b)$. The subgroups of D_N are either cyclic $\langle(x,0)\rangle$ or dihedral $\langle(x,0),(y,1)\rangle$.

Remark 5.3.1. *We reduce the general dihedral HSP to the dihedral HSP where the hidden subgroup is of the form $\langle(y,1)\rangle$ for some $y \in \mathbb{Z}/N\mathbb{Z}$.*

Proof. Suppose that $f : D_N \to S$ hides a subgroup $H = \langle(x,0),(y,1)\rangle$. We can check that all cosets of H are $(z,0)H$ for $z = 0, \cdots, x-1$ and $(z,1)H = (z-y,0)H$. We assume that $(z,0)H \mapsto f(z)$ for $z = 0, \cdots, x-1$. Then $f|_{\mathbb{Z}/N\mathbb{Z}}$ hides $\langle(x,0)\rangle$. Since $\mathbb{Z}/N\mathbb{Z}$ is abelian, we can find x.

Set $H' := \langle(y,1)\langle(x,0)\rangle\rangle = \{(0,0)\langle(x,0)\rangle, (y,1)\langle(x,0)\rangle\}$. Then H' is a subgroup of $D_N/\langle(x,0)\rangle$. We can also check that all cosets of H' are of the form $(z,0)H'$ and $(z,0)H' \mapsto f(z)$ for $z = 0, \cdots, x-1$. Define $f' : D_N/\langle(x,0)\rangle \to S$ induced by f. Then f' hides $\langle(y,1)\langle(x,0)\rangle\rangle$. $D_N/\langle(x,0)\rangle$ is isomorphic to a dihedral group $D_{N/\gcd(x,N)}$. So f' hides the subgroup $\langle(y,1)\rangle$ of $D_{N/\gcd(x,N)}$. □

Remark 5.3.2. *In the problem, if we can determine the last bit of y (that is, whether y is even or odd), we determine all the bits of y.*

Proof. Both subgroups $\{(2x,0),(2x,1) : x = 0,\cdots,N/2\}$ and $\{(2x,0),(2x+1,1) : x = 0,\cdots,N/2\}$ are isomorphic to $D_{N/2} \leq D_N$. If y is even, $\langle(y,1)\rangle \leq \{(2x,0),(2x,1) : x = 0,\cdots,N/2\}$. If y is odd, $\langle(y,1)\rangle \leq \{(2x,0),(2x+1,1) : x = 0,\cdots,N/2\}$. We can restrict the problem to finding $\langle(y',1)\rangle$ in $D_{N/2}$, where y' is ignored from the least bit of y. That is, $y' = y/2$ if y is even, and $y' = (y-1)/2$ if y is odd. In this situation, determining the last bit of y' means that determining the second least bit of y. Continuing the process, we can obtain all bits of y. □

We introduce an algorithm for the Dihedral HSP using QFT on $\mathbb{Z}/N\mathbb{Z}$. Following the first 3 steps in the Algorithm 10, we obtain the state

$$|(c,0)H\rangle := \frac{1}{\sqrt{2}}\left(|c,0\rangle + |y+c,1\rangle\right).$$

Apply QFT on the first qubit. Then

$$\begin{aligned}
&= \frac{1}{\sqrt{2}}\left(\left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ick/N}|k\rangle\right)|0\rangle + \left(\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi i(c+y)k/N}|k\rangle\right)|1\rangle\right) \\
&= \frac{1}{\sqrt{2N}}\left(\sum_{k=0}^{N-1} e^{2\pi ick/N}|k\rangle \otimes \left(|0\rangle + e^{2\pi iyk/N}|1\rangle\right)\right).
\end{aligned}$$

Measure the first qubit. When the measurement outcome is k, the post state is

$$|\Psi_k\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi iyk/N}|1\rangle\right).$$

Repeat this process, suppose we obtain $|\Psi_p\rangle$, $|\Psi_q\rangle$. Then

$$\begin{aligned}
|\Psi_p, \Psi_q\rangle =& \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi iyp/N}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi iyq/N}|1\rangle\right) \\
=& \frac{1}{2}\left(|0,0\rangle + e^{2\pi iy(p+q)/N}|1,1\rangle + e^{2\pi iyq/N}|0,1\rangle + e^{2\pi iyp/N}|1,0\rangle\right) \\
\overset{CNOT}{\to}& \frac{1}{2}\left(|0,0\rangle + e^{2\pi iy(p+q)/N}|1,0\rangle + e^{2\pi iyq/N}|0,1\rangle + e^{2\pi iyp/N}|1,1\rangle\right) \\
=& \frac{1}{2}\left((|0\rangle + e^{2\pi iy(p+q)/N}|1\rangle)|0\rangle + (e^{2\pi iyq/N}|0\rangle + e^{2\pi iyp/N}|1\rangle)1\rangle\right) \\
=& \frac{1}{\sqrt{2}}\left(|\Psi_{p+q}\rangle|0\rangle + e^{2\pi iyq/N}|\Psi_{p-q}\rangle|1\rangle\right).
\end{aligned}$$

If we measure the second qubit, we get $|\Psi_{p+q}\rangle$ when the outcome is 0, and $|\Psi_{p-q}\rangle$ when the outcome is 1 with uniform probability 1/2. Up to phase, the information of $|\Psi_{-k}\rangle$ and $|\Psi_k\rangle$ is the same since

$$\begin{aligned}
X|\Psi_{-k}\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle + e^{-2\pi iyk/N}|0\rangle\right) = e^{-2\pi iyk/N}\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi iyk/N}|1\rangle\right) \\
&= e^{-2\pi iyk/N}|\Psi_k\rangle.
\end{aligned}$$

Our goal is obtaining the state

$$|\Psi_{2^{n-1}}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^y|1\rangle\right).$$

And apply H.

$$\begin{aligned}
H|\Psi_{2^{n-1}}\rangle &= \frac{1}{2}\left((1+(-1)^y)|0\rangle + (1-(-1)^y)|1\rangle\right) \\
&= \begin{cases} |0\rangle, & \text{if } y \text{ is even} \\ |1\rangle, & \text{if } y \text{ is odd} \end{cases}.
\end{aligned}$$

Finally, measure the state. Then we know the parity of y.

Algorithm 11. For some integer m,
1. Make a list L_0 of copies of the state $|\Psi_k\rangle$. Pair $|\Psi_p\rangle$, $|\Psi_q\rangle$ in L_0 which share the last m bits. Apply the above process to each pair. Collect $|\Psi_{p-q}\rangle$ and make a list L_1 of state $|\Psi_k\rangle$ such that the last m bit of k is 0.
2. For each $0 \leq j < \lceil \frac{n-1}{m} \rceil - 1$, we assume a list L_j of states $|\Psi_k\rangle$ such that at least mj bits of k is 0. Pair $|\Psi_p\rangle$, $|\Psi_q\rangle$ in L_j which share the last $m(j+1)$ bits. Extract the state $|\Psi_{p-q}\rangle$ from each pair. Let the new list L_{j+1} consist of $|\Psi_{p-q}\rangle$.
3. For $j = \lceil \frac{n-1}{m} \rceil - 1$, Pair $|\Psi_p\rangle$, $|\Psi_q\rangle$ in $L_{\lceil (n-1)/m \rceil - 1}$ which share the last $(n-1) - m(\lceil \frac{n-1}{m} \rceil - 1)$ bits. Extract the state $|\Psi_{p-q}\rangle$ from each pair. The final list $L_{\lceil (n-1)/m \rceil}$ consists of $|\Psi_0\rangle$ and $|\Psi_{2^{n-1}}\rangle$.
4. Measure $H|\Psi_{2^{n-1}}\rangle$. Determine the last bit of y.

□

Now, we choose the appropriate m. Since unpaired elements are at most 2^m,

$$|L_{j+1}| \geq \frac{|L_j| - 2^m}{4}.$$

Set $|L_0| = 2^\ell$. Then $|L_{(n-1)/m}| \geq 2^{-2(n-1)/m}|L_0| = 2^{\ell - 2(n-1)/m} \geq 2^m$. Then

$$\ell \geq \frac{2(n-1)}{m} + m.$$

We consider the minimum of RHS. By the arithmetic-geometric mean inequality, $m = \sqrt{2}\sqrt{n-1}$ precisely. But for convenience of calculation, and constant does not effect to complexity of this algorithm, $m \simeq \sqrt{n-1}$, so $(n-1)/m \simeq m$ and $\ell \simeq 3m$. Set

$$m := \lceil \sqrt{n-1} \rceil.$$

Note that $m \geq \sqrt{n-1}$, and $(n-1)/m \leq (n-1)/\sqrt{n-1} = \sqrt{n-1}$, and $\lceil (n-1)/m \rceil \leq m$.

Now think of the probability for success of this algorithm. For this, we consider the number of elements of each L_i. The meaning of the success of this algorithm is existence of $|\Psi_{2^{n-1}}\rangle$ in the last set. If the last set has sufficient many elements, we can find the qubit with high probability. It is sufficient to consider $L_{\lceil (n-1)/m \rceil}$, but now we calculate the probability for L_m.

For $1 \leq i \leq T$, define an indicator random variable

$$X_i = \begin{cases} 1, & \text{with probability } 1/2 \\ 0, & \text{with probability } 1/2 \end{cases}.$$

Lemma 5.3.1 (Chernoff inequality)**.** *Let $X_1, \cdots, X_T$ be independent, unbaised Bernoulli random variables. Then*

$$p\left(\sum^{T} X_i \leq \frac{(1-b)N}{2}\right) \leq \exp\left(-\frac{Nb^2}{2}\right).$$

Set $|L_0| = C_0 2^{3m}$ for some C_0. Let P_j be a maximal set of pairs $|\Psi_p\rangle$, $|\Psi_q\rangle$ in L_j. Then

$$|P_0| \geq \frac{|L_0| - 2^m}{2} = \frac{C_0 2^{3m} - 2^m}{2} = \frac{2^{3m}\left(C_0 - 2^{-2m}\right)}{2},$$

$$\frac{|P_0|}{2}(1-b_0) \geq \frac{2^{3m}\left(C_0 - 2^{-2m}\right)}{4}(1-b_0) =: C_1 2^{3m-2},$$

where $b_0 := 2^{-8m/3}$ and $C_0 \geq 3$.

$$\begin{aligned} p\left(|L_1| \leq C_1 2^{3m-2}\right) &\leq p\left(|L_1| = \sum^{|P_0|} X_i \leq \frac{(1-b_0)|P_0|}{2}\right) \\ &\leq \exp\left(-\frac{|P_0| b_0^2}{2}\right) \leq \exp\left(-2^{m/3-1}\right). \end{aligned}$$

The second inequality uses the Chernoff inequality. The third inequality follows that

$$\begin{aligned}\frac{|P_0|b_0^2}{2} \geq & \frac{2^{3m}(C_0 - 2^{-2m})}{2}\frac{2^{-8m/3}}{2} \geq 2^{3m-2}(C_0 - 2^{-2m})2^{-8m/3} \\ \geq & 2^{m/3-2}(C_0 - 2^{-2m}) \geq 2^{m/3-2}(C_0 - 1) \geq 2^{m/3-1}.\end{aligned}$$

Thus we have

$$p\left(|L_1| \geq C_1 2^{3m-2}\right) \geq 1 - \exp\left(-2^{m/3-1}\right).$$

For $j = 0, \cdots, m-1$, set

$$C_{j+1} := \left(C_j - 2^{-2m+2j}\right)(1 - b_j), \quad C_m := 3, \quad b_j := 2^{-j-4m/3}.$$

Then $0 \leq C_{j+1} < C_j$. Then by induction, we can prove, for $j = 1, \cdots, m$,

$$p\left(|L_j| \geq C_j 2^{3m-2j} \middle| |L_i| \geq C_i 2^{3m-2i} \text{ for } i = 1, \cdots, j-1\right) \geq 1 - \exp\left(-2^{m/3-1}\right).$$

By the chian rule,

$$p\left(|L_j| \geq C_j 2^j \text{ all j}\right) \geq \left(1 - \exp\left(-2^{m/3-1}\right)\right)^m.$$

We obtain the last bit of y with probability at least $\left(1 - \exp\left(-2^{m/3-1}\right)\right)^m$.

Bibliography

[1] Andrew M. Childs and Wim van Dam: *Quantum algorithms for algebraic problems,* Reviews of Modern Physics 82, 1-52, 2010.

[2] G. Folland: *A course in Abstract Harmonic Analysis,* CRC Press, 1995.

[3] Kosmann-Schwarzbach, Yvette: *Groups and Symmetries From Finite Groups to Lie Groups,* Springer, 2010.

[4] M. Nielson and I.Chuang: *Quantum Computation and Quantum Information,* Cambridge University Press, UK, 2000.

[5] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma: *Normal Subgroup Reconstruction and Quantum Computation Using Group Representations,* In Proc. of STOC 2000, 627-635. ACM, 2000.

[6] Phillip Kaye, Raymond Laflamme, and Michele Mosca : *An Introduction to Quantum Computing,* Oxford University Press, 2007.

[7] Artur Ekert and Richard Jozsa: *Quantum computation and Shor's factoring algorithm,* Reviews of Modern Physics, Vol. 68, No. 3, 1996.

[8] Greg Kuperberg: *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem,* SIAM Journal on Computing, 2004. quant-ph/0302112v2.

[9] G. G. Hardy, Edward M. Wright: *An Introduction to the Theory of Numbers,* Post & Telecom Press, 2009.

국 문 초 록

이 논문에서 양자 알고리즘을 공부하는데 특히 양자 푸리에 변환을 이용한 알고리즘을 다룬다. 군 위에서의 양자 푸리에 변환을 소개하고 양자 알고리즘으로 문제들을 푸는 방법을 공부한다.

주요어휘 : 양자 알고리즘, 양자 푸리에 변환
학번 : 2013-22910