QIC 890/891 Selected Advanced Topics in Quantum Information

Module 1: *Quantum Algorithms for Number Theory Problems*

Lecture 2

Lecturer: Fang Song, University of Waterloo *May 6, 2015*

► **Recap**. Last time we discussed quantum algorithms for HSP on finite abelian groups. We saw quantum circuits to implement QFT efficiently. We also introduced an important tool called phase estimation.

► **Today**. We will extend our discussion to HSP on infinite groups $\mathbb{Z}$ (a.k.a. period finding over $\mathbb{Z}$). As an important applications, we will see that factoring can be reduced to HSP on $\mathbb{Z}$. We will introduce a little of basic Fourier analysis to get some insight on the quantum HSP algorithms.

⟦I wanted to draw the quantum circuits for a few algorithms we saw. Let me do it now. ⟧

PhE ckt

QFT on $\mathbb{Z}_N$

1 Period finding over $\mathbb{Z}$

The problem of finite abelian HSP can be extended naturally to the infinite group of integers $\mathbb{Z}$.

Definition 1 (HSP on $\mathbb{Z}$)**.** *Given a black-box function $f : \mathbb{Z} \to S$, where S is a set. f satisfies the promise that:*

$$f(x) = f(y) \quad \text{if and only if} \quad x + y \in r\mathbb{Z}$$

for some unknown $r \in \mathbb{Z}$. The goal is to find r using queries to f.

The hidden group here is $H := r\mathbb{Z}$. This problem is also known as period finding over $\mathbb{Z}$.

1.1 Reducing factoring to HSP on $\mathbb{Z}$

In 1994, Peter Shor ingeniously found that QFT can be used to solve the problem of order finding in group $\mathbb{Z}_L$ for an integer L [**?**]. (In the same seminal paper, Shor also gave a quantum algorithm for discrete logarithm, which we discussed in Lecture 1.) Namely for $a \in \mathbb{Z}_L$ the lease positive integer r such that $a^r = 1 \bmod L$ can be found efficiently on a quantum computer. This implies an efficient quantum algorithm for *factoring* immediately by a known observation (due to Miller in the 70s) that factoring reduces to order finding.

We explain the reduction briefly here. First note that if z is a non-trivial square root of 1 mod L i.e. $z^2 = 1 \mod L$ and $x \neq \pm 1 \bmod L$, then $L|(z^2 - 1)$ and hence $GCD(z-1, L)$ (or $GCD(z+1, N)$) is a non-trivial factor of L. The fact below tells us that if we can compute the order of a random $a \in \mathbb{Z}_L$, then we get a non-trivial square-root of 1 mod N.

Fact: [?, Theorem 5.2] Let $L = p_1^{\alpha_1} \cdot p_m^{\alpha_m}$ be the prime factorization of an odd composite integer. If we pick a random $a \in_R \mathbb{Z}_L$ with $a \neq 1 \& GCD(a, L) = 1$, then the order r of a is even and $a^{r/2} \neq -1 \bmod N$ except with probability $O(1/2^m)$.

Note that if we define $f : \mathbb{Z} \to \mathbb{Z}_L$ by $f(x) = a^x \bmod L$. Then clearly f is periodic over $\mathbb{Z}$ with period r and is injective within each period. Therefore order finding reduces to HSP on $\mathbb{Z}$ and actually Shor's quantum algorithm for order finding can also solve HSP on $\mathbb{Z}$ in general. We stress that because in general we do not known a multiple N of r, so we do not get an instance of HSP on $\mathbb{Z}_N$, with hidden subgroup $H := \langle r \rangle$.

1.2 Quantum algorithm for HSP on $\mathbb{Z}$

Since we are given a function $f : \mathbb{Z} \to S$, we can not hope to represent every integer on a computer of finite memory. We have to truncate the function somehow. For example, we will only consider f on $\{0, 1, \ldots, N-1\}$ for some integer N. Of course, N cannot be too small (e.g., less than period r), because otherwise we lose the periodic information. We assume that we know an upper bound of r and we show that by picking N sufficiently larger than r, there is an efficient quantum algorithm to solve the problem. If we do not know such a bound, we can just start with $N = 2$ and repeatedly double N till we find r. This only incurs $poly(\log r)$ overhead.

▶ **The algorithm**. The algorithm follows the usual structure.

1. Prepare $\frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} |x, f(x)\rangle$ and measure the 2nd register. Since f is periodic with period r we get superposition of points separated by r

$$\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |x_0 + jr\rangle .$$

   Here n depends on where the first point x_0 appears,which is nearly uniformly random (occurring with prob. n/N). Specifically $n = \lfloor N/r \rfloor + 1$ if $x_0 < N - r\lfloor N/r \rfloor$ and $n = \lfloor N/r \rfloor$ otherwise. (We will not worry about this technical detail.)

2. Apply Fourier transform over $\mathbb{Z}_N$, we get

$$\frac{1}{\sqrt{nN}} \sum_{j=0}^{n-1} \sum_{k \in \mathbb{Z}_N} \omega_N^{k(x_0+jr)} |k\rangle = \frac{1}{\sqrt{nN}} \sum_{k \in \mathbb{Z}_N} \omega_N^{kx_0} \sum_{j=0}^{n-1} \omega_N^{jkr} |k\rangle$$

3. Measure and get k. Use *continued fraction* algorithm to recover r from k/N.

QCkt for period finding on $\mathbb{Z}$

▶ **Analysis**. We need to identify which k's we get in step 3. The probability of getting $k \in \mathbb{Z}_N$ is given by

$$\Pr(k) = \left| \frac{1}{\sqrt{nN}} \sum_{j=0}^{n-1} \omega_N^{jkr} \right|^2$$

If by luck $r|N$, i.e., $N = nr$, then $\sum_{j=0}^{n-1} \omega_N^{jkr}$ becomes n if $k = \ell\frac{N}{r}$ and 0 otherwise. Namely we get exactly each of the r multiples $\ell\frac{N}{r}$ at random with probability $|\frac{n}{\sqrt{nN}}|^2 = 1/r$. However, in general N is not a multiple of r and in this case,

$$\sum_{j=0}^{n-1} \omega_N^{jkr} = \frac{1-\omega_N^{krn}}{1-\omega_N^{kr}} = \omega_N^{(n-1)kr/2} \frac{\sin(n \cdot \frac{\pi kr}{N})}{\sin(\frac{\pi kr}{N})}$$

Hence

$$\Pr(k) = \frac{\sin^2(n\frac{\pi kr}{N})}{nN\sin^2(\frac{\pi kr}{N})}$$

We expect that this distribution looks similar to the case where $r|N$. Namely it is peaked around k which is close to some integer multiple of N/r. We show this is indeed the case. Let $k = \lfloor \ell N/r \rceil = \ell N/r + \epsilon_\ell$ for some $j \in [r]$ with $|\epsilon_\ell| \leq 1/2$. Then

$$\Pr(k = \lfloor \ell N/r \rceil) = \frac{\sin^2(n\frac{\pi(\ell N/r+\epsilon_\ell)r}{N})}{nN\sin^2(\frac{\pi(\ell N/r+\epsilon_\ell)r}{N})} = \frac{\sin^2(n\theta_\ell)}{nN\sin^2(\theta_\ell)}$$

with $\theta_\ell = \frac{\pi\epsilon_\ell r}{N}$. Since $|\epsilon_\ell| \leq 1/2$ and $nr \leq N$, $n\theta_\ell \in [-\pi/2, \pi/2]$. By the inequality $\frac{4x^2}{\pi^2} \leq \sin^2 x \leq x^2$, we have

$$\Pr(b = \lfloor \ell N/r \rceil) \geq \frac{4n^2\theta_\ell^2/\pi^2}{nN\theta_\ell^2} \geq \frac{4}{r\pi^2}$$

⟦$\Pr(\cup A_i) = 1 - \Pr(\cap \bar{A}_i) \geq 1 - \Pi \Pr(\bar{A}_i) \geq 1 - (1 - \frac{4}{r\pi^2})^r = \Omega(1)$⟧

This implies that with constant probability we measure a value k that is $1/2$ away from one of the r integer multiple of N/r. Specifically we have $|k - \ell N/r| \leq 1/2$ for some $j \in [r]$. That is $|k/N - \ell/r| \leq 1/2N \leq 1/2r^2$ if we pick $N \geq r^2$. Continued fraction expansion (discussed next) will find r efficiently then.

► **Continued Fraction**.

$$CF(\alpha) = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

Truncating at a finite number gives a *convergent* of the expansion. The important property we need is stated below.

Fact: [**?**, Theorem 5.1] Suppose $|p/q - \phi| \leq \frac{1}{2q^2}$, then p/q is a convergent of the CF of ϕ.

2 A bite on Fourier analysis

⟦I promised last time to give some explanation why quantum HSP algorithm works. Let me give it a shot.⟧

What happened in HSP algorithm? Why does it work?

There is a general theory of Fourier analysis on *locally compact abelian* (LCA) groups, which cover all the groups we are concerned with. There is an associated group of homomorphisms called the dual group $\hat{G} := \mathrm{Hom}(G, \mathbb{R}/\mathbb{Z})$. Every LCA group is equipped with the so called Haar measure μ. Let $\mathrm{L}^2(G)$ and $\mathrm{L}^2(\hat{G})$ be the (Hilbert) spaces of square-integrable (w.r.t. μ) functions on G and $\hat{G}$ respectively. Then Fourier transform $\mathcal{F}_G$ is a unitary map from $\mathrm{L}^2(G)$ and $\mathrm{L}^2(\hat{G})$.

$\{|x\rangle : x \in G\}$ and $\{|y\rangle : y \in \hat{G}\}$ are orthonormal bases for $\mathrm{L}^2(G)$ and $\mathrm{L}^2(\hat{G})$ respectively. We call them the standard bases. For an arbitrary function $|f\rangle \in \mathrm{L}^2(G)$ (i.e. $f : G \to S$ and squre-integrable), we can decompose it as

$$|f\rangle = \sum_{x \in G} f(x)|x\rangle$$

(for discrete G). Similarly we can write $\hat{f} = \mathcal{F}_G f$ as

$$|\hat{f}\rangle = \sum_{y \in \hat{G}} \hat{f}(y)|y\rangle\,.$$

Let $|\zeta_y\rangle \in \mathrm{L}^2(G)$ such that

$$\mathcal{F}_G|\zeta_y\rangle = |y\rangle \in \mathrm{L}^2(\hat{G})\,.$$

$\{|\zeta_y\rangle, y \in \mathrm{L}^2(\hat{G})\}$ forms another basis for $\mathrm{L}^2(G)$ and is called the *Fourier basis*.

Fact: Fourier transforming f followed by measuring under standard basis of $\mathrm{L}^2(\hat{G})$ ($\{|y\rangle, y \in \hat{G}\}$), which is usually referred to as *Fourier Sampling*, is equivalent to measuring f under Fourier basis of $\mathrm{L}^2(G)$ ($\{|\zeta_y\rangle, y \in \hat{G}\}$).

Fact: Let $H \leq G$, then $\hat{H} := \{y \in \hat{G} : \forall x \in H, y(x) = 1\}$ is a subgroup of $\hat{G}$. It is usually called the dual or reciprocal subgroup of H.

Fact: If f is periodic on $H \leq G$, then $|\hat{f}\rangle$ has nontrivial only on $|y\rangle, y \in \hat{H}$.

Remarks. To make this a precise mathematical statement, we need to generalize the definition of Fourier transform to other space of functions. As computer scientists, we are fine being sloppy sometimes.

► **Example: cyclic group $\mathbb{Z}_N$.**

- $\hat{\mathbb{Z}}_N \cong \mathbb{Z}_N$, and hence it is usually identified with $\mathbb{Z}_N$.
- $\{|x\rangle, x \in \mathbb{Z}_N\}$ is the standard basis for $\mathrm{L}^2(\mathbb{Z}_N)$ and $\{|\chi_y\rangle : y \in \mathbb{Z}_N\}$ is the standard basis of $\mathrm{L}^2(\hat{\mathbb{Z}}_N)$.
- Let
$$|\zeta_y\rangle := \mathcal{F}^{-1}_{\mathbb{Z}_N}|\chi_y\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} \omega_N^{-xy}|x\rangle\,.$$
$\{|\zeta_y\rangle, y \in \mathbb{Z}_N\}$ is the Fourier basis of $\mathrm{L}^2(\mathbb{Z}_N)$.
- Let $H \leq G$. $\hat{H} = \{\chi_y : \forall x \in H, \chi_y(x) = 1\}$.

- Consider an HSP instance $\mathrm{HSP}(f, \mathbb{Z}_N)$. The quantum algorithm produces random samples from $\hat{H}$ and recovers H from there.

Let $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$ be the unit complex circle. It is identified with the quotient group $\mathbb{R}/\mathbb{Z}$ in our discussion. We review the Fourier transforms on groups that we are concerned with this this course.

G	$\hat{G}$	$\hat{f} := \mathcal{F}_G f$
$\mathbb{Z}_N$	$\mathbb{Z}_N$	$\hat{f}(\chi_y) = \frac{1}{\sqrt{\lvert G\rvert}} \sum_{x\in G} \chi_y(x) f(x), y \in G (i.e., \chi_y \in \hat{G})$
$\mathbb{Z}$	$\mathbb{T}$	$\hat{f}(y) = \sum_{x\in\mathbb{Z}} \omega^{xy} f(x), y \in \mathbb{T}$
$\mathbb{T}$	$\mathbb{Z}$	$\hat{f}(y) = \int_{\mathbb{T}} \omega^{xy} f(x) dx, y \in \mathbb{Z}$
$\mathbb{R}$	$\mathbb{R}$	$\hat{f}(y) = \int_{\mathbb{R}} \omega^{xy} f(x) dx, y \in \mathbb{R}$

Note that These objects extend naturally to high dimensions. $\mathcal{F}_{\mathbb{Z}_N}$ is often referred to as *discrete Fourier transform* (DFT) and $\mathcal{F}_{\mathbb{Z}}$ is known as *discrete-time Fourier transform* (DTFT) in the field of signal processing.

▶ **Convolution**. The convolution of two functions on $\mathbb{R}$ is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(x-t) g(t) dt \,.$$

There is a nice duality between convolution and multiplication.

$$\mathcal{F}(f * g) = (\mathcal{F}f)(\mathcal{F}g), \quad \mathcal{F}(fg) = (\mathcal{F}f) * (\mathcal{F}g) \,.$$

Similar definitions and properties hold for other abelian groups we consider as well.

2.1 Intuitive explanation for period finding on $\mathbb{Z}$

Given an instance f of HSP on $\mathbb{Z}$ with period r. The quantum algorithm for $\mathrm{HSP}(f, \mathbb{Z})$ can be understood understood following the mental process summarized in the table below.

Paradise	f	$\overset{\mathcal{F}_{\mathbb{Z}}}{\mapsto}$	$\hat{f}$
[Truncation]	$\downarrow W_N$		
Mid-land	$W_N f$	$\overset{\mathcal{F}_{\mathbb{Z}}}{\mapsto}$	$\hat{f} * \hat{W}_N$
Reality (Q-Alg.)		$\overset{\mathcal{F}_{\mathbb{Z}_N}}{\mapsto}$	$k/N \approx \ell/r$

1. If we apply $\mathcal{F}_{\mathbb{Z}}$ on f, Fourier analysis tells us that $\hat{f}$ will be peaked perfectly on the dual of $r\mathbb{Z}$, which contains all $\{y \in \mathbb{T}, ry \in \mathbb{Z}\}$ (because then $\omega^{xy} = 1$ for any $x \in r\mathbb{Z}$). We call this the paradise.

2. But we need to truncate the function on a computer. This amounts to multiplying f with the window function $W_N : \mathbb{Z} \to \mathbb{Z}_2$, where $W_N(x) = 1$ iff. $x \in \mathbb{Z}_N$. By the

convolution/multiplication duality, $\mathcal{F}_{\mathbb{Z}}(W_N f) = \hat{f} * \hat{W}_N$ (convolution taken over $\mathbb{T}$). For any $y \in \mathbb{T}$

$$\hat{W}_N(y) = \sum_{x=0}^{N-1} \omega^{xy} = \omega^{(N-1)y/2} \frac{\sin(\pi N y)}{\sin(\pi y)} .$$

Which is peaked at the origin and the first 0 occurs at $1/N$. Basically $\hat{f} * \hat{W}_N$ will be concentrated within a small neighbourhood around each $\frac{1}{r}\mathbb{Z}$. If we sample from here, we get approximation (of precision $\approx 1/2N$) of ℓ/r for some $\ell \in [r]$ with high probability. Then Continued Fraction works if $1/N2 \leq 1/2r^2$ and hence picking $N = \Omega(r^2)$ suffices. This *mid-land* contains noise but is still very nice.

3. Implement $\mathcal{F}_{\mathbb{Z}}$ is infeasible unfortunately. The actual quantum algorithm we saw, applies $\mathcal{F}_{\mathbb{Z}_N}$ instead and the measurement produces samples from $\mathcal{F}_{\mathbb{Z}_N}(W_N f)$. This can be thought of as sampling the $\mathcal{F}_{\mathbb{Z}} f$ with space $1/N$ due to the following fact.

   Fact: Let f be a function on $\mathbb{Z}$ but only nontrivial on $\mathbb{Z}_N$. Let $\hat{f} := \mathcal{F}_{\mathbb{Z}} f$ and $\hat{f}' := \mathcal{F}_{\mathbb{Z}_N} f$. Then

$$\forall y \in \mathbb{T}, \hat{f}(y) = \sum_{x \in \mathbb{Z}} \omega^{xy} ,$$

$$\forall k \in \mathbb{Z}_N, \hat{f}'(k) = \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_N} \omega_N^{xk} \frac{1}{\sqrt{N}} \hat{f}(k/N) .$$

   Therefore

   - if $r|N$, then sampling $\mathcal{F}_{\mathbb{Z}_N}(W_N f)$ gets exactly the integer multiples of N/r
   - otherwise, we get $\lfloor \ell N/r \rceil$ that approximates $\ell N/r$. Our (tedious) calculation showed that the quantum algorithm hits these points with high probability.

This explains intuitively what the quantum HSP algorithm does. We see that Reality is the most nasty one. It takes us a lot of effort to make sure useful information can be extracted. This is still manageable in low dimensions, but will become harder and harder to analyze, especially when we move on to $\mathbb{R}$ and $\mathbb{R}^n$.

Paradise is too far to reach. As a compromise, you may be wondering by now, can we somehow realize the *mid-land*, i.e., can we sample the continuous spectrum $\mathcal{F}_{\mathbb{Z}}(W_N f)$? Implementing $\mathcal{F}_{\mathbb{Z}}$ is infeasible, but can we perform Fourier sampling on $\mathbb{Z}$ by other means, at least in some approximate sense?

The answer is YES, as we will see next time.