Hidden Subgroups and Quantum Computation

Lecture 05

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

July 18, 2025

Overview

Today we will define the quantum Fourier transform (QFT) on $\mathbb{Z}/n$.
Then, we will talk about the cyclic case of the HSP.

If a quantum processor has n qubits $Q = \{q_1, \ldots, q_n\}$, then a register is a subset $R \subseteq Q$.

Say Q is a register of size n. Let S and T be subregisters so that $S \cup T = Q$. Then, we write $|\eta\zeta\rangle = |\eta\rangle \otimes |\zeta\rangle$ to mean that S is in the state $|\eta\rangle$ and T is in the state $|\zeta\rangle$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Recall that we use the notation $|0\rangle, \ldots, |N-1\rangle$ for the "computational" basis vectors of a space $\mathcal{H} \simeq \mathbb{C}^N$.

Let $N > 1$ be an integer. Let R be a qubit register of size $n \geq \log N$. Then, the cyclic quantum fourier transform is

$$F_N = \frac{1}{\sqrt{N}} \sum_{\ell=0}^{N-1} \sum_{k=0}^{N-1} e^{\frac{2\pi i \ell k}{N}} |\ell\rangle\langle k| .$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The factor of $N^{-1/2}$ ensures that F_N is unitary on the state space, and thus fits in our circuit model.

Let S be a finite set. Let G denote the group $\mathbb{Z}/n$. Suppose $f : G \to S$ is a function such that there exists a subgroup $H \leq G$ such that f separates H-cosets.

Our goal, per the statement of the HSP, is to find a set X such that $\langle X \rangle = H$, assuming we have full capability to compute

$$f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |f(x) \oplus y\rangle .$$

Note that we *do not* have access to the values $|H|$, h, or H itself.

Write $\Phi : G \to \mathcal{H}$ for the map taking each $g \in G = \mathbb{Z}/n$ to the computational basis vector $|g\rangle \in \mathcal{H}$.

Since H is a (cyclic) subgroup, we can write $H = \langle h \rangle$ for some $h \in H$. Then,

$$\Phi(H) = \{|0\rangle, |h\rangle, |2h\rangle, \ldots, |(|H|-1)h\rangle\} \subseteq \mathcal{H}.$$

Beginning with the computational 0 state $|0\rangle \otimes |0\rangle$, we apply F_N on the first register to yield

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

Then, apply the black box function f:

$$\frac{1}{\sqrt{N}}\sum_{\ell=0}^{N-1}|\ell\rangle\otimes|f(\ell)\rangle\,.$$

Apply projective measurement (in the sense of the fourth postulate) to the second register, collapsing to some value $f(\ell_m)$. Then, all that remains in the first register is the coset $H + \ell_m$:

$$\frac{1}{\sqrt{|H|}} \sum_{\varphi \in \Phi(H)} |\ell_m + \varphi\rangle = \frac{1}{\sqrt{|H|}} \sum_{s=0}^{|H|-1} |\ell_m + sh\rangle ,$$

where the second expression comes from the fact that $H = \langle h \rangle$.

Applying F_N again yields

$$\frac{1}{\sqrt{|H|}} \sum_{s=0}^{|H|-1} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i(\ell_m+sh)k}{N}} |k\rangle .$$

Simplifying gives

$$\frac{1}{\sqrt{|H|N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i \ell_m k}{N}} |k\rangle \sum_{s=0}^{|H|-1} e^{\frac{2\pi i shk}{N}} .$$

Observe that $h/N = |H|$. Then,

$$\sum_{s=0}^{|H|-1} e^{\frac{2\pi i s h k}{N}} = \begin{cases} 0, & |H| \nmid k \\ |H|, & |H| \mid k. \end{cases}$$

Thus, we get

$$\left|\psi_f\right\rangle = \frac{1}{\sqrt{h}} \sum_{t=0}^{h-1} e^{\frac{2\pi i \ell_m t |H|}{N}} \left| t|H| \right\rangle .$$

If $\mathfrak{U} = \{\mathcal{U}_i\}_{i \in I}$ is a set of quantum circuits which compute the QFT over a set of groups $\{G_i : |G_i| < \infty \text{ for all } i\}_{i \in I}$, then we call $\mathfrak{U}$ efficient if for all $i \in I$, the size of $\mathcal{U}_i$ is polynomial in $\log |G_i|$.

Assigned reading: §3.4 of Lomont's review to understand the efficient computation of F_N on $\mathbb{Z}/N$.

https://arxiv.org/pdf/quant-ph/0411037.

Measuring $\left|\psi_f\right\rangle$ returns a scaling $\lambda|H|$ for $\lambda \in \{0, \ldots, h-1\}$, where there value of λ is uniformly distributed.

Applying the measurement several times gives a collection of scalings $\mathcal{C} = \{\lambda_\alpha |H|\}_\alpha$. Taking the GCD of $\mathcal{C}$ yields $|H|$ with high probability.

The computation of $\gcd(\mathcal{C})$ can be done via the Euclidean algorithm with complexity $O(\log^2(N))$, where $\log(N)$ is the number of digits in N.

Suppose we measured $\left|\psi_f\right\rangle$ k times, yielding a collection

$$\mathcal{C} = \{\lambda_1|H|, \ldots, \lambda_k|H|\}.$$

Lemma

Suppose we have $k \geq 2$ uniformly random samples $\lambda_1, \ldots, \lambda_k$ from the set $\{0, 1, \ldots, h-1\}$, where $h \geq 2$. Then,

$$\mathbb{P}(\gcd(\lambda_1, \ldots, \lambda_k) = 1) \geq 1 - 2^{-k/2}.$$

Theorem

Let G be a cyclic group generated by g with $|G| = n$. Then,

(i) *for all $H \leq G$, $H = \langle h \rangle$ for some h.*

(ii) *for all $H \leq G$, $|H| \mid n$.*

(iii) *for all (positive) divisors $d \mid n$, there is precisely one subgroup $H \leq G$ such that $|H| = d$. Further, $H = \langle g^{N/d} \rangle$.*

If we can ascertain $|H|$ with high probability from our procedure, then we can easily recover H, and thus, a generating set $X = \{g^{N/d}\}$ of H.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Therefore, running the described process a reasonable enough k-times determines H with high probability, no matter the choices of N and h.

Next time we will discuss

(i) character theory of finite abelian groups.

(ii) the general, finite abelian HSP.

(iii) Simon's and Shor's algorithms.

After this, we will be prepared to delve into a bit more representation theory and progress on the nonabelian HSP.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN