Hidden Subgroups and Quantum Computation

Lecture 08

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

August 08, 2025

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Overview

Today we will take a look at the general QFT.

Then, I will go over some background about dihedral groups, which should make reading Kuperberg's paper easier.

If we would like to talk about the HSP for general finite groups, then we need a general QFT.

Let G be a finite group such that $|G| = n$, $f : G \to \mathbb{C}$ be a function, and $\rho : G \to \mathrm{GL}(\mathcal{V})$ be a representation.

The Fourier transform of the function f at the representation ρ is

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{n}} \sum_{g \in G} f(g)\rho(g).$$

Recall that we denote a complete set of irreducibles of G by $\widehat{G}$.

The inverse Fourier transform of $\hat{f}$ is

$$f(g) = \sqrt{\frac{1}{n}} \sum_{\rho \in \widehat{G}} \sqrt{d_\rho} \operatorname{tr}\left(\hat{f}(\rho)\rho(g^{-1})\right).$$

Check that this recovers our original function f.

Fix an ordering $G = \{g_1, \ldots, g_n\}$ of the finite group. We can then label f by its action on each element of G, writing

$$f = (f(g_1), \ldots, f(g_n)),$$

which is a vector in $\mathbb{C}^n$.

Likewise, order the set of irreducibles $\widehat{G} = \{\rho_1, \ldots, \rho_m\}$. For all $1 \leq k \leq m$, let $\mathcal{V}_k$ be a $\mathbb{C}$-linear space of dimension d_{ρ_k}.

For each k, pick a basis β_k for $\mathcal{V}_k$ such that $\hat{f}(\rho_k)$ is a $d_{\rho_k} \times d_{\rho_k}$ unitary matrix.

The reason that we can choose our bases in such a way is sketched in Lomont's review.

Add up the number of all possible matrix entries of $\hat{f}(\rho_k)$ for $1 \leq k \leq m$:

$$d_{\rho_1}^2 + d_{\rho_2}^2 + \cdots + d_{\rho_m}^2 = \sum_{\rho \in \widehat{G}} d_\rho^2.$$

From Lecture 06, we know this is just $|G| = n$.

We can thus arrange these matrix entries in a vector $\hat{f} \in \mathbb{C}^n$, starting with $\hat{f}(\rho_1)_{1,1}$ and continuing up through $\hat{f}(\rho_m)_{d_{\rho m}, d_{\rho m}}$.

That is, both f and $\hat{f}$ are realizable in $\mathbb{C}^n$, so define a (unitary) linear transformation

$$\Gamma : \mathbb{C}^n \to \mathbb{C}^n$$

by $f \mapsto \hat{f}$.

We call this Γ the general quantum Fourier transform.

Given an arbitrary finite group G of order n, a finite set S, and an H-coset separating function $f : G \to S$, there is a general path toward a solution of the HSP.

Compute

$$\frac{1}{\sqrt{n}} \sum_{g \in G} |g\rangle \otimes |f(g)\rangle .$$

Measure the second register, yielding

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle \otimes |f(ch)\rangle ,$$

where we pick the coset cH uniformly. Then, apply the general QFT.

Perform a projective measurement on the register and observe a representation ρ. We can also choose to observe indices of the resultant matrix after applying the QFT.

Use some classical information processing on the (post-measurement) classical data to find generators of $H \leq G$.

Assigned reading: §5 of Lomont's review to see an overview of progress on the HSP for nonabelian groups.

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

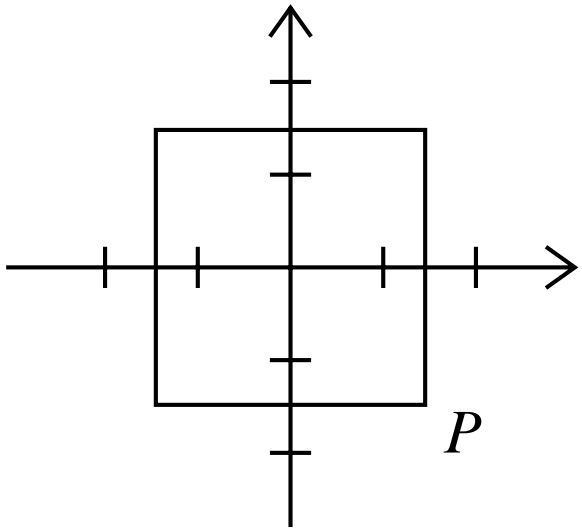
ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

In a sense, the dihedral group D_n, of order $2n$, is the quintessential nonabelian group.

The dihedral group D_n encodes information about the rigid motions of a regular n-gon.

Let $n = 4$, so that we are working with a regular 4-gon P. That is, P is a square.

Say P is embedded in the plane $\mathbb{R}^2$, with its center at the origin, so that it looks like



How many times can we rotate P counterclockwise about the origin so that it still looks the same in the plane?

Clearly, we have four possible rotations. If r is a rigid rotation of P by the angle $\pi/4$, then the four rotations are r, r^2, r^3, and r^4 puts us back where we started. That is, $r^4 = e$, the "identity" rotation.

How many lines through the origin can we reflect P over so that it looks the same in the plane?

Well we can reflect over the x-axis, over the y-axis, and over the lines $y = x$ and $y = -x$.

Let s be the reflection over the x-axis. Clearly, $s^2 = e$, the "identity" reflection.

Reflecting over the y-axis is the same as rotating the square P by $\pi/4$ (applying r) and then reflecting over the x-axis (applying s).

We write this motion as sr.

In this way, the other two reflections are precisely sr^2 and sr^3.

Thus, including the three nontrivial rotations r, r^2, r^3, the four reflections s, sr, sr^2, sr^3, and the identity $r^4 = s^2 = e$, there are eight so-called rigid motions of P.

Since we embedded $P \hookrightarrow \mathbb{R}^2$, we can realize each rigid motion as a linear transformation $\mathbb{R}^2 \to \mathbb{R}^2$. Further, these are all isomorphisms, since each rigid motion has an inverse.

Putting the rigid motions of P together, the set

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

forms a group under the operation of function composition.

Formally, the dihedral group D_n is the subgroup generated by two formal elements r and s. If e is the identity element in D_n, then we require that

(i) r is of order n.

(ii) s is of order 2.

(iii) $srsr = e$.

This characterizes a unique (up to isomorphism) group of order $2n$.

Note

To make rigorous sense of the previous characterization, we could write

$$D_n \simeq \langle r, s | r^n, s^2, srsr \rangle = \mathrm{Free}(r, s)/\,\mathrm{ncl}(r^n, s^2, srsr),$$

where $\mathrm{Free}(-) : \mathsf{Set} \to \mathsf{Grp}$ *is the free group functor and* ncl *denotes normal closure, i.e., the smallest normal subgroup of* $\mathrm{Free}(r, s)$ *containing* $\{r^n, s^2, srsr\}$*. We call such a quotient a presentation of* D_n*.*

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

The elements of the form r^k are called rotations and the elements of the form $s\,r^k$ are called reflections.

If we extended our geometric discussion of D_4 to D_n, we could have discovered the listed relations ourselves. See Keith Conrad's notes for a nice investigation of D_n.

`kconrad.math.uconn.edu/blurbs/grouptheory/dihedral.pdf`

Intuitively, the power k of a reflection sr^k is called the slope of the reflection, since $\pi k/n$ is precisely the angle between the line of reflection of sr^k and the line of reflection of s.

In the context of the HSP, we would call the task of finding a hidden subgroup $H \leq D_n$ generated by a reflection $H = \langle s r^k \rangle$ the dihedral hidden subgroup problem (DHSP).

We say that H is the hidden reflection.

Certainly, finding a hidden reflection amounts to finding its slope.
But, why does the DHSP reduce to finding reflections?

Theorem

Finding an arbitrary hidden subgroup $H \leq D_n$ amounts to finding the slope k of a hidden reflection.

Observe that there is a subgroup $\langle r \rangle \leq D_n$ which is isomorphic to $\mathbb{Z}/n$. We will write $C_n = \langle r \rangle$.

Further C_n is normal in D_n. It is easy to check that $H' = H \cap C_n$ is thus normal in H, for any subgroup $H \leq D_n$.

Proof.

Suppose $H \neq \langle s r^k \rangle$ for all $1 \leq k \leq n$. Then, either $H = \{e\}$ or $H' \neq \{e\}$, since C_n has all the rotations. Shor's algorithm allows us to factor n, so we can find the hidden subgroup $H' \leq C_n$ using the cyclic HSP. □

Proof, continued.

Again, since C_n has all the rotations, H/H' has no nontrivial rotations. Thus, we have

$$H/H' = \begin{cases} \{eH'\}, & H \text{ has only rotations} \\ \text{reflection} & H \text{ has at least one reflection.} \end{cases}$$

If $H = \{e\}$, then any algorithm to find the slope of a reflection will fail, so we indirectly find H to be trivial. □

Kuperberg proves the following.

Theorem

There is a quantum algorithm that finds a hidden reflection in D_n with time and query complexity $2^{O(\sqrt{\log n})}$.