Hidden Subgroups and Quantum Computation

Lecture 01

Dheeran E. Wiggins

Summer 2025
Illinois Mathematics and Science Academy

June 18, 2025

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Overview

Today we will cover some preliminaries which should mostly be review. Exercises will cover the basics of sets and groups.

Many of the quintessential quantum algorithms can be reinterpreted as instances of the hidden subgroup problem (HSP).

To develop the language of the HSP, we must first be comfortable with the rudimentary properties of an algebraic structure known as a group.

In mathematics, we like collecting things. For all relevant purposes, we call a collection of *any* mathematical objects a set.

We say the objects in a set are its elements. If S is a set, then we write $x \in S$ to say that x is an element of S.

(i) To combine sets, we use the union: $S \cup T$ is all of S and all of T in a single set.

(ii) To restrict sets, we use the intersection: $S \cap T$ is the smallest subset contained in both S and T.

(iii) To subtract sets, we use the set difference: $S \setminus T$ is the subset of S containing only those elements which are not in T.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Some standard sets include

(i) $\mathbb{N} = \{0, 1, 2, \dots\}$.

(ii) $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2 \dots\} = -\mathbb{N} \cup \mathbb{N}$.

(iii) $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z} \text{ and } q \neq 0\}$.

(iv) $\mathbb{R}, \mathbb{C}, \mathbb{M}_n(\mathbb{C}), \dots$

A function $f : S \to T$ from S to T is a rule which assigns uniquely to each $s \in S$ an element $f(s) \in T$.

If $f : S \to T$ is both injective and surjective, it is called a bijection (or, isomorphism of sets). We write $S \simeq T$.

The (Cartesian) product of two sets $S \times T$ is the set

$$\{(s,t) : s \in S \text{ and } t \in T\}.$$

If $S = T$, we will often write $S \times S = S^2$, and likewise for

$$\underbrace{S \times \cdots \times S}_{n \text{ times}} = S^n.$$

Collections of objects are useful in their own right, but often we need a way to systematically combine the objects.

A group is a pair $(G, \cdot)$, where G is a set and $(-) \cdot (-) : G^2 \to G$ is a binary operation, satisfying associativity, the existence of an identity, and the existence of inverses.

Some standard groups are

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ with addition.

(ii) $\mathbb{Z}/n = \{0, \ldots, n-1\}$ with addition modulo n.

(iii) the invertible $n \times n$ complex matrices $\mathrm{GL}_n(\mathbb{C}) \subseteq \mathbb{M}_n(\mathbb{C})$ with multiplication.

(iv) the dihedral group D_n.

(v) the (direct) product of groups $G \times H$ with componentwise operations.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Since every group $(G, \cdot)$ has, in particular, an *underlying* set G, we can talk about functions $\varphi : G \to H$ between groups.

However, we want the image $\varphi(G) \subseteq H$ to be a group as well. A (group) homomorphism is a function $\varphi : G \to H$ between groups such that for all $g_1, g_2 \in G$, we have

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2).$$

A bijective homomorphism is called an isomorphism of groups, in which case we write $G \simeq H$.

Oftentimes, we will care about whether a subgroup $H \leq G$ is invariant under conjugation. This warrants some jargon.

A subgroup $H \leq G$ is called normal if for all $g \in G$, the set gHg^{-1} is contained in H. We write $H \lhd G$.

In fact, normal subgroups actually give us a way to build new groups from old. If $H \lhd G$ is a normal subgroup, then define the quotient G/H by

$$G/H = \{gH : g \in G\}$$

with operation

$$(g_1H) \cdot (g_2H) = g_1g_2H.$$

The most useful (for our purposes) example of a quotient group will be $\mathbb{Z}/n\mathbb{Z}$. Check that $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. Then, the quotient is exactly

$$\{k + n\mathbb{Z} : k \in \mathbb{Z}\}.$$

Further, the quotient operation tells us that

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = k + \ell + n\mathbb{Z},$$

so we can identify $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ with $k \pmod{n}$ in $\mathbb{Z}/n$.

We have seen some examples of groups, how to define structure-preserving functions between them, and how to form quotients.

We now focus in on the class of groups which are *finitely generated* and *abelian*.

A group G is called abelian if for all $g_1, g_2 \in G$, we have

$$g_1 g_2 = g_2 g_1.$$

That is, an abelian group is one in which the operation is commutative.

If $S \subseteq G$ is a subset of group elements, we write $\langle S \rangle$ for the smallest subgroup of G which contains all the elements in S.

If $H \leq G$ is given by $\langle S \rangle$, where S is a finite set $\{g_1, \ldots, g_n\} \subseteq G$, then we say H is finitely generated.

Unlike with the general theory of groups, groups which are both finitely generated and abelian have a clean classification.

Theorem

Every finitely generated abelian group G is isomorphic to

$$\mathbb{Z}^r \times \mathbb{Z}/p_1 \times \cdots \times \mathbb{Z}/p_n,$$

where $r \geq 0$ is called the rank, and each of the p_k, for $1 \leq k \leq n$, is a power of a prime.

Next time we will introduce some additional structure:

(i) (finite-dimensional) $\mathbb{C}$-linear spaces $\mathcal{V}$.

(ii) Dirac notation for linear algebra.

(iii) inner products $\langle -|- \rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{C}$.

Once we have built up groups and $\mathbb{C}$-linear spaces, we can talk about group representations $\rho : G \to \mathrm{Aut}(\mathcal{V})$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN