Notes on Group Theory:

Rubik's Cube and the Permutation Group

Coding Club

September 11, 2024

Mohammed Alshamsi
2021004826
mo.alshamsi@aurak.ac.ae

Department of Computer Science and Engineering
American University of Ras Al Khaimah
2023–24

Contents

1 Introduction

Welcome to the third set of "lecture notes" for the AURAK Coding Club. The idea is to introduce a useful topic that lends itself easily to coding applications. These topics tend to be mathematical in nature, but most (if not all) of it will be intuitive material that doesn't require much background knowledge.

1.1 How to Read this Document

This is essentially just a short monologue about group theory and related concepts. We'll go over the elementary definitions and results, and give some examples. This is by no means meant to give you a comprehensive introduction; it's just a quick tour to get you started. Check the bibliography if you want to learn more about the topic.

I'll be sure to bring up coding aplications whenever it makes sense. Any code I write at those points will be in the C language. If you've taken (or are taking) CSCI 112, you'll be able to follow along without much trouble. Furthermore, there will be coding exercises. You're free to solve them in any language.

If you don't know any coding, check this link for a quick intro to C.

1.2 Basics

Briefly, a *group* is a set that has some additional structure. This section will review sets and introduce a few related concepts which will be helpful later.

Sets. Here we introduce sets, subsets, unions, intersections, and partitions.

Relations and functions. Cartesian product, relations, and functions. Binary operations are literally just functions but with nicer notation.

2 What is a Group?

Here we define what a group is, and provide some examples.

2.1 Cayley Tables

These are a nice way to represent smaller groups. We list a few properties of them that indicate things about the group (e.g. symmetric means it's abelian).

2.2 Subgroups

A subgroup is just a subset that is also a group under the same operation. Ha.

2.3 Generators and Cyclic Groups

We define generators and cyclic groups, as well as generating sets of not-necessarily-cyclic groups. We note that their ability to "generate" the group relies heavily on the operation in question.

2.4 Groups of Permutations

Yeah these are pretty cool. We'll define groups of permutations, show the two slick notations, and maybe the algorithm(s?) from TAOCP S1.3.3. (The scope creep has already begun, but it won't be as bad as the whole string search algorithm from last time... hopefully.)

3 Cosets and Quotient Groups

As usual, definitions and examples, but we *might* want to break this down a little with additional examples to make sure it really sticks.

3.1 Lagrange's Theorem

This is so cool.

4 The Rubik's Cube Group

We'll introduce the notations for moves and how the moves are actually generators for the whole set. I think we might want to talk about group actions before this point but I'm not yet sure.

4.1 Coset Spaces

I don't know what these are yet.

4.2 Thistlethwaite's Algorithm

But this algorithm uses coset spaces, so we need to talk about those before we introduce it.