2013

The Gordon game

Anthony Frenk
Eastern Washington University

THE GORDON GAME

A Thesis

Presented To

Eastern Washington University

Cheney, Washington

In Partial Fulfillment of the Requirements

for the Degree

Master of Science

By

Anthony Frenk

Summer 2013

THESIS OF ANTHONY FRENK APPROVED BY

_____ DATE:_____

W. DALE GARRAWAY, GRADUATE STUDY COMMITTEE

_____ DATE:_____

RONALD GENTLE, GRADUATE STUDY COMMITTEE

Abstract

In 1992, about 30 years after Gordon introduced group sequencings to construct row-complete Latin squares, John Isbell introduced the idea of competitive sequencing, the Gordon Game. Isbell investigated the Gordon Game and found solutions for groups of small order. The purpose of this thesis is to analyze the Gordon Game and develop a brute force method of determining solutions to the game for all groups of order 12 (up to isomorphism) as well as for abelian groups of order less than 20. The method used will be a depth first search program written in MATLAB. Consequently, group representation using matrices will be studied within the thesis.

Acknowledgements

I would like to thank Dr. Ron Gentle of the Mathematics Department at Eastern Washington University for introducing me to advanced mathematics and advising me on my thesis. I would also like to thank Dr. Dale Garraway for introducing me to group symmetries, from which I discovered my area of research. I would like to thank my friends and family, especially my mother Susan for encouraging me to struggle through to completion. Most of all I would like to thank my wife Lacey and my children Destiny, Sydney, Samuel, and Cameron. Your love and support throughout my college career has given me the strength I needed to succeed.

Contents

Chapter 1

Introduction

In 1962, Basil Gordon introduced the idea of group sequencing in an effort to construct row-complete Latin squares. Basically, a group sequencing is an ordering $\{g_1, g_2, \ldots, g_n\}$ of a finite group G such that the sequence $\{g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n\}$ has distinct elements, hence is an ordering of G as well. The classification of sequenceable groups has continued throughout the past 50 years, with major contributions by Anderson ([2],[3],[4]), Keedwell [20], Baily [7], and Isbell [18]. Chapter 4, which can be considered the main body of the thesis, investigates a small portion of their collective work. Specifically, the classification of abelian groups and dihedral groups is discussed as well as the connection between sequenceable groups, Latin squares, and Hamiltonian paths.

Chapter 2 is a review of group theoretic results and definitions that later aide in the analysis of the Gordon Game. The graduate level mathematician may skip this chapter, whereas a computer science enthusiast may wish to review their elementary group theory.

Chapter 3 is written for the graduate level mathematician. An intro-

duction to Group Action followed by proofs and examples of the The Sylow Theorems. At the end of the chapter matrix representations for those finite groups needed to investigate the Gordon Game are derived.

Chapter 5 gives an analysis of the Gordon Game from a time complexity viewpoint. The depth-first algorithm used to find solutions to the Gordon Game is developed in this chapter as well. The end of chapter 5 gives solutions for the Gordon Game for all groups (up to isomorphism) up to order 13 as well as abelian groups of size 15,17,18,19,and 20.

Chapter 2

Group Theory Review

This chapter is mostly a review of elementary group theory the reader should be familiar with. Many of the proofs in this chapter can be found in most undergraduate Abstract Algebra texts and are omitted here. The idea of this chapter is not to give a complete review of undergrad group theory, but to give definitions, notations, and results that will be used later in the thesis. Near the end of the chapter we provide a few examples of groups that will be useful later as we investigate group sequencing and the Gordon Game.

2.1 Groups, Subgroups, and Cyclic Groups

Definition 2.1. (1) A **binary operation** $*$ on a set G is a function mapping $G \times G \to G$. For each $(a, b) \in G \times G$ we denote the element $*((a, b))$ of G by $(a*b)$, or simply ab if the context of the binary operation is understood.

(2) A binary operation $\star$ is **associative** if for all $a, b, c \in G,\ a(bc) = (ab)c$.

(3) If $\star$ is a binary operation on a set G we say elements a and b of G **commute** if $ab = ba$. We say $\star$(or G) is *commutative* if for all $a, b \in G,\ ab = ba$.

Definition 2.2. A **binary algebraic structure** $\langle G, * \rangle$ is a set G together with a binary operation * on G.

Definition 2.3. A **group** is a set $\langle G, \cdot \rangle$ where G is a set and $\cdot$ is a binary operation on G such that the following axioms are satisfied:

(1) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in G$.

(2) There exists an element e in G such that for all $a \in G$,

$$e \cdot a = a \cdot e = a$$

e is called the *identity* of G.

(3) For each $a \in G$, there is an element a^{-1} in G such that

$$a \cdot a^{-1} = e = a^{-1} \cdot a$$

a^{-1} is called the *inverse* of a.

If additionally we have that all elements within $\langle G, \cdot \rangle$ commute with each other we say that G is **abelain**. We will henceforth become less formal and simply say G is a group under $\cdot$ if $\langle G, \cdot \rangle$ is a group or just G is a group when the binary operation is understood from context. Traditionally, group operations have been split into two types: multiplication and addition, with "addition" being reserved for when the group operation is abelian. We will stick with tradition and suppress the dot($\cdot$) notation for non-abelian groups and simply use concatenation of the elements so that $a \cdot b = ab$. For operations within abelian groups we will use the addition symbol (+) and write $a+b$. One final point on operation notation: we will use the powers' notation to represent repeated use of the group operation(even when the group is abelian). So that we have the following

$$\underbrace{x \cdot x \cdot \cdots \cdot x}_{\text{n times}} = x^n$$

Definition 2.4. Let G, G' be groups. A **homomorphism** is any map

$$\phi : G \longrightarrow G'$$

satisfying the rule

$$\phi(ab) = \phi(a)\phi(b),$$

for all $a, b \in G$. If additionally ϕ is a bijection, then ϕ is called an **isomorphism** of G and G'.

Definition 2.5. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = e$. The **group table** of G is the $n \times n$ matrix whose i, j (intersection of the ith row and jth column) entry is the group element $g_i g_j$ (here order of computation is important).

Definition 2.6. If G is a group, then the **order** $|G|$ of G is the number of elements in G. If $x \in G$ then we define the *order* of x to be the smallest positive integer n such that $x^n = e$ and denote this integer by the same notation, $|x|$.

Definition 2.7. Let G be a group. If a subset H of G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup** of G. We shall denote that H is a subgroup of G by $H \leq G$ and that H is a proper subgroup of G by $H < G$(i.e. $H \leq G$ but $H \neq G$).

Definition 2.8. Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G, called the **cyclic subgroup of G** generated by a, denoted by $\langle a \rangle$, and is the smallest subgroup of G that contains a, that is, every subgroup containing a contains H.

Definition 2.9. An element a of a group G **generates** G and is a **generator for** G if $G = \langle x \rangle$. A group G is a **cyclic group** if there is some element $a \in G$ that generates G.

Example 2.10. Let G be a group and let a be a fixed element of G. Examine the set

$$H_a = \{x \in G \mid xa = ax\}$$

Since $e \cdot a = a \cdot e = a$, $e \in H_a$. Also, if $x, y \in H_a$ then $x = axa^{-1}$ and $y = aya^{-1}$ and we have the following

$$\begin{aligned} (xy)a &= [(axa^{-1})(aya^{-1})]a \quad \text{(sub } x \text{ and } y \text{ from above)} \\ &= (axa^{-1}aya^{-1})a \\ &= axy \end{aligned}$$

Thus if $x, y \in H_a$ then $xy \in H_a$. Finally, if $x \in H_a$ then

$$\begin{aligned} xa &= ax \\ \Rightarrow a &= x^{-1}ax \\ \Rightarrow ax^{-1} &= x^{-1}a \end{aligned}$$

Which implies that $x^{-1} \in H_a$. Thus $H_a \leq G$.

Generalizing the previous example, let S be a subset of a group G. Then the previous argument applies to the set

$$H_S = \{x \in G \mid xs = sx \text{ for all } s \in S\}$$

implying $H_S \leq G$. When $S = G$, the subgroup H_S is called the **centre of** G, denoted $Z(G)$, and defined by

$$Z(G) = \{x \in G \mid xa = ax \text{ for all } a \in G\}$$

It is the subgroup of G that commutes with every element of G. If $Z(G)$ commutes with G, then it commutes within itself, hence $Z(G)$ is always an abelian subgroup of G.

Theorem 2.11. [11]

(1.) Every cyclic group is abelian.

(2.) A subgroup of a cyclic group G is cyclic.

Theorem 2.12. [11] If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m$$

Definition 2.13. Let r and s be two positive integers. The positive generator d of the cyclic group

$$H = \{nr + ms \mid n, m \in \mathbb{Z}\}$$

under addition is the **greatest common divisor**(abbreviated gcd) of r and s. We write $d = \gcd(r, s)$.

Theorem 2.14. [11] Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is isomorphic to the group of integers modulo n, denoted $\langle \mathbb{Z}_n, +_n \rangle$.

Theorem 2.15. [10] Any two cyclic groups of the same order are isomorphic.

2.2 Permutation Groups, Cosets, and Direct Products

Definition 2.16. A **permutation of a set** A is a function $\phi : A \to A$ that is both one to one and onto.

We would like to standardize our notation when dealing with permutation and show that function composition $\circ$ is a binary operation on the collection of all permutation of a set A. We call this operation *permutation multiplication*. We have the following example.

Note: the order of composition for $\sigma \circ \tau$ must be read in right-to-left order: first apply τ and then σ.

Example 2.17. Let

$$A = \{1, 2, 3, 4, 5\}$$

and that τ is the permutation given by the following array

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

so that $\sigma(1) = 3,\ \sigma(2) = 1$, and so on. Likewise, let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

and for example, right-to-left multiplication yields

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(3) = 2.$$

.

Theorem 2.18. [11] Let A be a nonempty set, and define S_A to be the collection of all permutations of A. Then S_A is a group under permutation multiplication called the **Symmetric Group on A**.

Definition 2.19. Let A be the finite set $\{1, 2, \ldots, n\}$, then the symmetric group on A is denoted S_n and called the **symmetric group on n letters**.

As a note, S_n has $n!$ elements. We will primarily be interested in using the symmetric groups alongside Cayley's Theorem (proved later) to create permutation matrices that represent group elements. For the sake of completeness we give the definition of a field and that of a matrix group as well as an example.

Definition 2.20. A **field** is a triple $(F, +, \cdot)$ such that $(F, +)$ is an abelian group (call its identity 0) and $(F - \{0\}, \cdot)$ is also abelian group, and the following *distributive* law holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{for all } a, b, c \in F$$

Also, for any field F define $F^\times = F - \{0\}$.

Example 2.21. Examples of fields include $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. When p is a prime, then $\mathbb{Z}_p$ is an example of a finite field.

An example of a group that is familiar to us from Linear Algebra is the general linear group of degree n.

Definition 2.22. For each $n \in \mathbb{Z}^+$, the *general linear group of degree n*, denoted $GL_n(\mathbb{F})$ is the set of all $n \times n$ matrices whose entries come from $\mathbb{F}$ and whose determinant is nonzero.

The group axioms are satisfied since matrix multiplication is associative and the $n \times n$ identity matrix is the identity of the group. Existence of inverses is guaranteed by the condition that each $A \in GL_n(\mathbb{F})$ must have non-zero determinant, which is equivalent to having a matrix inverse.

Example 2.23. Let $n = 2$ and $\mathbb{F} = \mathbb{Z}_2 = (\{0, 1\}, +)$. There are then 16 possible matrices for the set of 2×2 matrices with entries from $\mathbb{Z}_2$. Call this set $M_2(\mathbb{Z}_2)$. We list them in the following table and throw out any that don't satisfy the equation $\det(A) = ad - bc \neq 0$ for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $a, b, c, d \in \mathbb{Z}_2$. There are six matrices in the table that satisfy the equation $ad - bc \neq 0$. These

Figure 2.1: $M_2(\mathbb{Z}_2)$

$\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 0 \\ 1 & 1 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$
$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$	$\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$

matrices form $GL_2(\mathbb{Z}_2)$,

$$\left\{ \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \quad \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$$

Definition 2.24. Given a permutation π of n elements,

$$\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$$

given in two line form by

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$$

its **permutation matrix** is the $n \times n$ matrix P_π whose entries are all 0 except that in column i, the entry $\pi(i)$ equals 1. We may write

$$P_\pi = \begin{bmatrix} \mathbf{e}_{\pi(1)} & \mathbf{e}_{\pi(2)} & \vdots & \mathbf{e}_{\pi(n)} \end{bmatrix}$$

where $\mathbf{e}_{\pi(j)}$ denotes a column vector of length n with 1 in the jth position and 0 in every other position.

Listed below are properties of permutation matrices:

(1) *Permutation matrices are orthogonal (i.e. $P_\pi P_\pi^T = I$), hence the inverse exists and is the transpose of the original permutation matrix*

(2) Given two permutations π and σ of n elements and the corresponding permutation matrices P_π and P_σ we have

$$P_\pi P_\sigma = P_{\pi\circ\sigma}$$

These properties give that the map $\pi \mapsto P_\pi$ is a group monomorphism (meaning it is an injective homomorphism) from $S_n \to Gl_n(\mathbb{F})$. Additionally, this map holds for any field, $\mathbb{F}$.

Definition 2.25. Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ of G is the **left coset** of H containing a, while the subset $Ha = \{ha \mid h \in H\}$ is the **right coset** of H.

Theorem 2.26. [10] (**Theorem of LaGrange**) Let H be a subgroup of a finite group G. Then the left (resp. right) cosets of H are all of size $|H|$ and partition G. Hence, the order of H is a divisor of the order of G.

Corollary 2.2.0.1. [11] Every group of prime order is cyclic.

With this corollary and Thm. 2.14 we see immediately that if the order of a group G is a prime, p, then $G \cong \mathbb{Z}_p$.

Definition 2.27. Let H be a subgroup of a group G. The number of left cosets of H in G is the **index of H in G** and is denoted $(G : H)$. If G is a finite group then by Theorem 2.26 we have the following equation

$$|G| = (G : H)|H|$$

Definition 2.28. The **Cartesisn product of sets** $S_1, S_2, \ldots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \ldots, n$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \cdots \times S_n$$

or by

$$\prod_{i=1}^{n} S_i$$

Theorem 2.29. [11] Let $G_1, G_2, \ldots, G_n$ be groups. For $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ in $\prod_{i=1}^{n} G_i$, define $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)$ to be the element $(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$. Then $\prod_{i=1}^{n} G_i$ is a group, called the **direct product** of the groups G_i.

The multiplication defined above is known as component wise multiplication.

Theorem 2.30. [11] The group $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n}$ if and only if the numbers m_i for $i = 1, \ldots, n$ are such that the gcd of any two of them is 1.

2.3 Homomorphisms and Factor Groups

Definition 2.31. Let ϕ be a mapping of a set X into a set Y, and let $A \subseteq X$ and $B \subseteq Y$. The **image of A in Y under ϕ** is defined as $\phi[A] = \{\phi(a) \mid a \in A\}$. The set $\phi[X]$ is the **range of ϕ**. The **inverse image of B in X** is defined as $\phi^{-1}[B] = \{x \in X \mid \phi(x) \in B\}$.

The following theorem loosely states that if ϕ is a homomorphism of a group G into a group G', then ϕ preserves the identity element, inverses, and subgroups.

Theorem 2.32. [11] Let ϕ be a homomorphism of a group G into a group G'. Then the following hold:

(1.) If e is the identity element of G, then $\phi(e)$ is the identity element e' in G'.

(2.) If $a \in G$, then $\phi(a^{-1}) = \phi(a)^{-1}$

(3.) If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.

(4.) If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Definition 2.33. Let $\phi : G \to G'$ be a homomorphism of groups. The subgroup $\phi^{-1}[e'] = \{x \in G \mid \phi(x) = e'\}$ is called the **kernel of** ϕ, denoted $\text{Ker}(\phi)$.

Theorem 2.34. Let $\phi : G \to G'$ be a group homomorphism, and let $H = \text{Ker}(\phi)$. Let $a \in G$. Then the set

$$\phi^{-1}[\phi(a)] = \{x \in G \mid \phi(x) = \phi(a)\}$$

is the left coset aH of H, and is also the right coset Ha of H. Consequently, the two partitions of G into left cosets and into right cosets of H are the same.

Proof: Let $D = \{x \in G \mid \phi(x) = \phi(a)\}$ Then $x \in D$ if and only if

$$\begin{aligned}
& \phi(x) = \phi(a) \\
\Leftrightarrow \quad & \phi(a)^{-1}\phi(x) = e' \\
\Leftrightarrow \quad & \phi(a^{-1}x) = e' \\
\Leftrightarrow \quad & a^{-1}x \in \text{Ker}(\phi) = H \\
\Leftrightarrow \quad & a^{-1}x = h, \text{ some } h \in H \\
\Leftrightarrow \quad & x = ah \\
\Leftrightarrow \quad & x \in aH
\end{aligned}$$

Which shows that $D = aH$. It is a similar argument to show that $Ha = D$ by multiplying the first equation by $\phi(x)^{-1}$ on the right in place of $\phi(a)^{-1}$ on the left. Thus the two partitions of G into left cosets and right cosets of H are the same. □

Corollary 2.3.0.2. [11] Let $\phi : G \to G'$ be a group homomorphism. Then ϕ is one-to-one if and only if $\text{Ker}(\phi) = \{e\}$.

The following are three equivalent conditions for a subgroup H of a group G to be a *normal* subgroup of G.

Definition 2.35. A subgroup H of a group G is **normal** in G if H satisfies any of the following:

(1.) $gH = Hg$ for all $g \in G$.

(2.) $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.

(3.) $gHg^{-1} = H$ for all $g \in G$.

Notationally, we will denote normal subgroups by $H \trianglelefteq G$ whenever H is a normal subgroup of G.

Theorem 2.36. [11] Let H be a subgroup of a group G. Then left coset multiplication is well defined by the equation

$$(aH)(bH) = (ab)H$$

if and only if H is a normal subgroup of G.

Corollary 2.3.0.3. [11] Let H be a normal subgroup of G. Then the cosets of H form a group G/H (read G *mod* H) under the binary operation $(aH)(bH) = (ab)H$.

Definition 2.37. The group G/H in the preceding corollary is called the **factor group** of G by H. This group is also sometimes called the **quotient group**.

Theorem 2.38. [11] Let H be a normal subgroup of G. Then $\pi : G \to G/H$ defined by $\pi(x) = xH$ is a homomorphism with kernel H.

Theorem 2.39. [11] (**The Fundamental Homomorphism Theorem**) Let $\phi : G \to G'$ be a group homomorphism with kernel H. Then the map $\mu : G/H \to \phi[G]$ defined by $\mu(gH) = \phi(g)$ is an isomorphism. Also, if $\pi : G \to G/H$ is the homomorphism defined by $\pi(x) = xH$, then $\phi(g) = \mu\pi(g)$ for each $g \in G$.

Before proceeding further, we would like to give a lemma that will be useful later and involves factor groups.

Lemma 2.3.1. If $N \leq Z(G)$, and G is cyclic, then G is abelian.

Proof: Since N is a subgroup of $Z(G)$, it must commute with all elements of G and is thus a normal subgroup of G and we can form the factor group G/N. Working with G/N is cyclic, let $\overline{x}$ (the coset containg x in G/N) generate G/N. Then we can write G/N as the set $\{N, xN, x^2N, \ldots, x^{n-1}N\}$ with $(G : N) = n$. If we consider $g_1, g_2 \in G \setminus N$, then using the map from Theorem 2.38 we can send $g_i \mapsto \overline{g_i}$ for $i \in \{1, 2\}$. Then we see that $g_1 \in x^kN$ and $g_2 \in x^lN$ for some $0 \leq k, l \leq n$. Thus we may rewrite $g_1 = x^kh_1$ and

$g_2 = x_2^h$ for $h_1, h_2 \in N$. Finally, examining $g_1 g_2$ we see that

$$\begin{aligned} g_1 g_2 &= (x^k h_1)(x^l h_2) \\ &= x^k (h_1 x^l) h_2 \\ &= x^k (x^l h_1) h_2 \quad (h_1, h_2 \in N \subseteq Z(G) \\ &= x^{k+l} (h_1 h_2) \\ &= x^{l+k} (h_2 h_1) \\ &= x^l (x^k h_2) h_1 \\ &= (x^l h_2)(x^k h_1) \\ &= g_2 g_1 \end{aligned}$$

And since g_1, g_2 were chosen arbitrarily, G is abelian.

□

Definition 2.40. An isomorphism $\phi : G \to G$ of a group G onto itself is called an **automorphism** of G. The set of automorphisms of a group G form a group under the operation of function composition. This group, denoted Aut(G), is called the automorphism group on G.

Additionally, it should be noted an automorphism is a special type of permutation of the group elements. Throughout this paper we will have need to investigate a few different types of automorphisms(starting in the next chapter with group action), one of which we introduce here.

Theorem 2.41. Let G be a group and let $g \in G$. Then the map

$$i_g : G \to G$$

defined by $i_g(x) = gxg^{-1}$ for all $x \in G$ is an automorphism of G called **conjugation of x by g.**

Proof: Fix $g \in G$ and let $x, y \in G$. Then

$$\begin{aligned} i_g(xy) &= g(xy)g^{-1} \quad \text{defn of } i_g \\ &= g(xey)g^{-1} \quad \text{group prop.} \\ &= g(xg^{-1}gy)g^{-1} \quad e = g^{-1}g \\ &= (gxg^{-1})(gyg^{-1}) \quad \text{group prop.} \\ &= i_g(x)i_g(y) \quad \text{defn of } i_g \end{aligned}$$

Hence, the map is a homomorphism. To show that conjugation is an isomorphism, keep g fixed and examine the following composition

$$\begin{aligned} i_{g^{-1}} \circ (i_g)(x) &= i_{g^{-1}}(i_g(x)) && \text{(def. of composition)} \\ &= i_{g^{-1}}(gxg^{-1}) && \text{(def. of } i_g\text{)} \\ &= g^{-1}(gxg^{-1})(g^{-1})^{-1} && \text{(def. of } i_g\text{)} \\ &= (g^{-1}g)x(g^{-1}g) && \text{(inverse and group prop.)} \\ &= x && \text{(group prop.)} \end{aligned}$$

Thus, $i_{g^{-1}}$ acts as a left inverse of i_g under composition. In a similar fashion, $i_{g^{-1}}$ is a right inverse of i_g and hence i_g is a bijection. Therefore, conjugation is an isomorphism and thus an automorphism. □

Definition 2.42. Let G be a group and let $g \in G$. Then the map i_g, is called the **inner automorphism of G by g.**

We can extend conjugation to subsets of G as follows: let $H \subset G$. Then define $i_g[H] = gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. The preceding results imply a subgroup H is normal if and only if it is invariant under all inner automorphisms.

The next result, which characterizes product groups, will be useful later in the construction of groups of small order. We start with a definition.

Definition 2.43. Let A and B be subsets of a group G. Then we denote the set of products of elements of A and B by

$$AB = \{x \in G \mid x = ab \text{ for some } a \in A \text{ and } b \in B\}$$

Note that we do not claim that the product set AB is contained in either A or B. Also, this definition can be extended to include an arbitrary number of subsets of G.

Theorem 2.44. Let H and K be subgroups of a group G.

(1.) If $H \cap K = \{e\}$, the product map

$$p : H \times K \to G$$

defined by $p(h, k) = hk$ is injective. Its image is the subset HK.

(2.) If either H or K is a normal subgroup of G, then the product sets HK and KH are equal, and HK is a subgroup of G.

(3.) If H and K are normal, $H \cap K = \{e\}$, then $hk = kh$ for all $k \in K$ and $h \in H$. If also $HK = G$, then G is isomorphic to the direct product $H \times K$,

Proof: (1) Let (h_1, k_1), (h_2, k_2) be elements of $H \times K$ such that $h_1k_1 = h_2k_2$. If we multiply both sides on the left by h_1^{-1} and on the right by k_2^{-1} we find that $k_1k_2^{-1} = h_1^{-1}h_2$. Now, the left side is in K and the right side is in H. Since $H \cap K = \{e\}$, this forces $k_1k_2^{-1} = h_1^{-1}h_2 = e$, hence $h_1 = h_2$ and $k_1 = k_2$. Therefore p is injective. That the image is a subset of HK is true by definition.

(2) Suppose that H is a normal subgroup of G. and let $h \in H$ and $k \in K$. First we write $kh = (khk^{-1})k$ and note that since H is normal,

$khk^{-1} \in H$. Therefore $kh \in HK \Rightarrow KH \subset HK$. By similar reasoning, using that $hk = k(k^{-1}hk)$ we see that $KH \subset HK \Rightarrow HK = KH$. To show that HK we need closure under multiplication and inverses as well as $e \in HK$. For closure under multiplication examine the product $(hk)(h'k') = h(kh')k'$ with the middle term $kh' \in KH = HK$, so we can write it as $kh = h''k''$. Then the product becomes $hkh'k' = (hh'')(k''k') \in HK$. Closure under inverses is similar: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. And of course $e \in HK$ since both H and K are subgroups and $e = e \cdot e$. With a relabeling of H and K we have the proof in the case that K is normal.

(3) Now assume that both subgroups are normal and that $H \cap K = \{e\}$. First, it should be noted that Consider first the product $(hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$. Since K is normal, the left side is in K. Similarly, the right side is in H. Thus the above product is in the intersection, hence $hkh^{-1}k^{-1} = e$. Therefore $hk = kh$. Now observe that in $H \times K$ the product rule is $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$, which the map p sends to $h_1h_2k_1k_2$ in G . However, in G the products h_1k_1 and h_2k_2 multiply as $h_1k_1h_2k_2$. Since $hk = kh$, these two products are equal. Part (1) shows that p was injective and since we have $HK = G$, p must also be onto, hence an isomorphism.

We have the following generalization.

Corollary 2.3.0.4. If $H_1, H_2, \ldots, H_n$ are normal subgroups of G with

$$H_1H_2 \cdots H_n = G$$

and $\gcd\big(|H_i|, |H_j|\big) = 1$ for all $1 \leq i, j \leq n,\ i \neq j$, then G is isomorphic to the direct product $H_1 \times H_2 \times \cdots \times H_n$

Proof: Consider the map

$$\rho : H_1 \times H_2 \times \cdots \times H_n \longrightarrow G$$

defined by

$$\rho(h_1, h_2, \ldots, h_n) = h_1 h_2 \cdots h_n.$$

The assumption $\gcd\big(|H_i|, |H_j|\big) = 1$ for all $1 \leq i, j \leq n,\ i \neq j$ implies that $H_i \cap H_j = \{e\}$, which by part (3) implies $hh' = h'h$ for $h \in H_i$ and $h' \in H_j$ for all $1 \leq i, j \leq n$. Additionally, since the orders of H_i are pairwise relatively prime then

$$|G| = |H_1 \cdots H_n| = |H_1||H_2| \cdots |H_n| = |H_1 \times \cdots \times H_n|$$

and thus the domain and co-domain of ρ have the same size. Now, ρ is a homomorphism since

$$\begin{aligned}
\rho\Big((h_1, h_2, \ldots, h_n)(g_1, g_2, \ldots, g_n)\Big) &= \rho\big(h_1 g_1, h_2 g_2, \ldots, h_n g_n\big) \\
&= h_1 g_1 h_2 g_2 \cdots h_n g_n \text{ (defn. of } \rho) \\
&= h_1 h_2 \cdots h_n g_1 g_2 \cdots g_n \text{ (the } H_i \text{ commute)} \\
&= \rho(h_1, \ldots, h_n)\rho(g_1, \ldots, g_n) \text{ (defn. of } \rho)
\end{aligned}$$

To show ρ is surjective let $g \in G$. Then $H_1 H_2 \cdots H_n = G$ implies there exist $h_i \in H_i$ for $1 \leq i \leq n$ such that $h_1 h_2 \cdots h_n = g$. Thus $\rho(h_1, h_2, \ldots, h_n) = g$. With ρ being onto and having its domain and co-domain the same size implies ρ is a bijection, hence an isomorphism. □

We would like to end this chapter by giving a list of groups of small order. We will work with these groups as examples throughout the thesis.

Figure 2.2: Groups of Small Order

Order	*Distinct Groups*	*Order*	*Distinct Groups*
1	$\langle e \rangle$	5	$\mathbb{Z}_5$
2	$\mathbb{Z}_2$	6	$\mathbb{Z}_6$, D_3
3	$\mathbb{Z}_3$	7	$\mathbb{Z}_7$
4	$\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4$		

D_n is the group of symmetries of the regular n-gon.

Chapter 3

Group Action and Sylow Theorems

3.1 Group Action

Definition 3.1. A **group action** of a group G on a set X is a map $G \times X \to X$(written as $g \cdot x$) such that for all $x \in X$ and $g_1, g_2 \in G$:

1. $e \cdot x = x$

2. $(g_1 g_2) \cdot (x) = g_1 \cdot (g_2 \cdot x)$

Examples of group actions follow. The first will be regular group multiplication.

Example 3.2. Let G be a group and let $X = G$. Then G acts on itself by left multiplication: $g \cdot x = gx$ (where gx is in fact carried out in G here). Conditions 1 and 2 are satisfied by the group axioms of identity and associativity.

The next example will be that of a subgroup H of G acting on G as the set!

Example 3.3. Let H be a subgroup of a group G. Then H acts on G by conjugation where $h \cdot g = hgh^{-1}$ for $g \in G$ and $h \in H$. Condition 1 is satisfied by $e \cdot g = ege^{-1} = g$ and Condition 2 is satisfied since for $h_1, h_2 \in H$ and $g \in G$ we have

$$\begin{aligned} h_1 \cdot (h_2 \cdot g) &= h_1 \cdot (h_2 g h_2^{-1}) \quad \text{defn. of action} \\ &= h_1 h_2 g h_2^{-1} h_1^{-1} \quad \text{defn. of action} \\ &= (h_1 h_2) \cdot g \quad \text{defn. of action} \end{aligned}$$

When $H = G$, we have the example of conjugation from Theorem 2.41. The next example explores the action of the symmetric group on its set of elements.

Example 3.4. Let X be any set and let $G = S_X$, the symmetric group on X. Then S_X acts on X by permutation of X: $\sigma \cdot x = \sigma(x)$ for all $x \in X$.
Condition 1 is satisfied since the identity permutation, σ_e is the identity element of S_X. Condition 2 is satisfied as a consequence of the associativity of function composition.

The next result shows that the actions of subgroups of S_X on X describe all possible group actions on X.

Theorem 3.5. Let G be a group acting on a set X. For each $g \in G$, the map $\sigma_g : X \to X$ defined by $\sigma_g(x) = g \cdot x$ for $x \in X$ is a permutation of X. Also, the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

Proof: To establish that σ_g is a permutation of X we show that as a

set map, σ_g has a 2-sided inverse, $\sigma_{g^{-1}}$. For all $x \in X$ we have

$$\begin{aligned}
(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \quad \text{(definition of function composition)} \\
&= g^{-1} \cdot (g \cdot a) \quad \text{(definition of } \sigma_g\text{)} \\
&= (g^{-1}g) \cdot a \quad \text{(Condition (2) of an action)} \\
&= e \cdot a = a \quad \text{(Condition (1) of an action)}
\end{aligned}$$

This shows $(\sigma_{g^{-1}} \circ \sigma_g)$ is the identity map on X. Since g was arbitrary, we may interchanges the roles of g and g^{-1} and see $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map on X. Thus σ_g has a 2-sided inverse and is therefore a permutation of X.

To show that $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism, we check the homomorphism condition is satisfied. For all $x \in X$ we have

$$\begin{aligned}
\varphi(g_1g_2)(a) &= \sigma_{g_1g_2}(a) \quad \text{(definition of } \phi\text{)} \\
&= (g_1g_2) \cdot a \quad \text{(definition of } \sigma_{g_1g_2}\text{)} \\
&= g_1 \cdot (g_2 \cdot a) \quad \text{(Condition (2)of an action)} \\
&= \sigma_{g_1}(\sigma_{g_2}(a)) \quad \text{(definition of } \sigma_g \\
&= (\phi(g_1) \cdot \phi(g_2))(a) \quad \text{(definition of } \phi\text{)}
\end{aligned}$$

Thus ϕ is a homomorphism. The property that $\phi(g)(x) = gx$ follows by definition of ϕ. □

We shall become less formal now and write the action of G on X, $g \cdot x$, simply as gx when there is no danger of confusing the group action with the actual group operation(even though as we saw, sometimes they are indeed the same). The only time we will not do this is with conjugation, which could become terribly confusing indeed if gx were meant to represent gxg^{-1}.

Let G be a group acting on a set X. For each $x_1, x_2 \in X$ and $g \in G$ it will be important to know when $gx_1 = x_2$ and when $gx_1 = x_1$. Thus, we want

to know for each action, which $g \in G$ take x_1 into x_2 and which leave x_1 fixed. We establish the following results:

Theorem 3.6. Let G be a group acting on a set X. For $x_1, x_2 \in X$, $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $gx_1 = x_2$. The relation $\sim$ defined above is an equivalence relation on X.

Proof: For each $x \in X$, $ex = x$ so $x \sim x$ and $\sim$ is reflexsive. If $x_1 \sim x_2$ then $gx_1 = x_2$ which implies $x_1 = g^{-1}x_2$, hence $x_2 \sim x_1$ and $\sim$ is symmetric(heavy usage of group action axioms there). If $x_1 \sim x_2$ and $x_2 \sim x_3$ then $gx_1 = x_2$ and $g_2x_2 = x_3$ from some $g, g_2 \in G$. Then
$(g_2g_1)x_1 = g_2(g_1x_1) = g_2x_2 = x_3$, so $x_1 \sim x_3$ and $\sim$ is transitive. □

Definition 3.7. Let G be a group acting on a set X. Each cell in the partition of the equivalence relation described in Theorem 3.6 is an **orbit in X under G**. If $x \in X$, the cell containing x is the **orbit of x**. We denote this set by $O_x = \{gx \mid g \in G\}$.

So, given an element $x \in X$, the orbit, O_x, gives us the 'addresses' of all the different places x visits under the specific group action by G. The next result tells us that for each $x \in X$, the elements of G that leave x fixed form a subgroup of G.

Theorem 3.8. Let G be a group acting on a set X. Then for each $x \in X$, the set

$$G_x = \{g \in G \mid gx = x\}$$

is a subgroup of G.

Proof: Let $x \in X$ and let $g_1, g_2 \in G_x$. Then $g_1x = x$ and $g_2x = x$. Then $(g_1g_2)x = g_1(g_2x) = g_1x = x$, so $g_1g_2 \in G_x$, and G_x is closed under

products. The group identity, e, is in G_x by definition of a group action. If $g \in G_x$ then
$ex = x \Rightarrow (g^{-1}g)x = g^{-1}(gx) = g^{-1}x = x \Rightarrow g^{-1} \in G_x$(heavy usage of group action axioms again). Thus G_x is closed under inverses and hence is a subgroup of G.

Definition 3.9. Let G be a group acting on a set X and let $x \in X$. The subgroup $G_x = \{g \in G \mid gx = x\}$ described in the above theorem is called the **stabilizer of x in G.**

If we let $X = G$ and take the group action to be conjugation described in Example 3.3, then we can extend the concept of stabilizer of an element to that of a subgroup K.

Example 3.10. If a group acts G on itself by conjugation, then the orbit $\{gxg^{-1} \mid g \in G\}$ of $x \in G$ is called the **conjugacy class of x.** If a subgroup H acts on G by conjugation the stabilizer subgroup

$$H_x = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\}$$

is called the **centralizer of x in H** and is denoted $C_H(x)$. If $H = G$, the G is suppressed and $C(x)$ is called the **centralizer of x.** If H acts by conjugation on the set S of all subgroups of G, then the subgroup of H fixing $K \in S$, namely $\{h \in H \mid hKh^{-1} = K\}$ (this set was shown to be a group in example 2.10), is called the **normalizer of K in H** and denoted $N_H[K]$. When $H = G$ we suppress the H, write $N[K]$ and call the subgroup the **normalizer of K**.

Lemma 3.1.1. Let G be a group. Then $x \in Z(G)$ if and only if $C(x) = G$.

Proof: This follows directly from the definition of centralizer, observe

$$\begin{aligned} & x \in Z(G) \\ \Leftrightarrow & xg = gx \text{ for all } g \in G \\ \Leftrightarrow & x = gxg^{-1} \text{ for all } g \in G \\ \Leftrightarrow & g \in C(x) \text{ for all } g \in G \\ \Leftrightarrow & C(x) = G \end{aligned}$$

The next result shows the relationship between the orbits in a set X and the structure of the group G acting on X. Recall the notation for the index of a subgroup H in G is $(G : H)$.

Theorem 3.11. Let G be a group acting on a set X and let $x \in X$. Then $|O_x| = (G : G_x)$. If $|G|$ is finite, then $|O_x|$ is a divisor of $|G|$.

Proof: To show equality of sets we define a map ψ from the orbit of x to the set of left cosets of G_x in G. Let $x_1 \in O_x$. Then there exist $g_1 \in G$ such that $g_1 x = x$. Define $\psi(x_1) = g_1 G_x$ of G. If this map is well defined and a bijection, our job is finished. To show well defined, suppose also that $g_2 x = x_1$. Then $g_1 x = g_2 x$, so $g_1^{-1}(g_1 x) = g_1^{-1}(g_2 x)$, which implies $x = (g_1^{-1} g_2)x$. Therefore $g_1^{-1} g_2 \in G_x$, so we have $g_2 \in g_1 G_x$, and $g_1 G_x = g_2 G_x$. Thus ψ is well defined.

To show ψ is injective, assume $x_1, x_2 \in O_x$, and $\psi(x_1) = \psi(x_2)$. Then there exist $g_1, g_2 \in G$ such that $g_1 x = x_1$ and $g_2 x = x_2$, implying from the above reasoning that $g_2 \in g_1 G_x$. Thus $g_2 = g_1 g$ for some $g \in G_x$, which implies $x_2 = g_2 x = (g_1 g)x) = g_1(gx) = g_1 x = x_1$. Therefore ψ is injective.

It should be relatively clear that ψ is surjective. Take any left coset

g_1G_x of G_x. Then $g_1x = x_1$ for some $x_1 \in X$. Thus, map $x_1 \mapsto g_1G_x$ and ψ is onto. Hence, ψ is a bijection from O_x to the left cosets of G_x in G.

If $|G|$ is finite, then LaGrange's Theorem says that $|G| = |G_x|(G : G_x)$. Since $|O_x| = (G : G_x)$, the preceding equation yields

$$|G| = |G_x||O_x.|$$

This result is sometimes referred to as the orbit-stabilizer theorem. □

Example 3.12. Let G be a group and let G act on the set S of its subgroups by conjugation. For a fixed subgroup $H \in S$, its orbit consists of all of its conjugates, and its stabilizer is $N[H]$. Hence, by Theorem 3.11, the number of conjugates of H, which is the size of the orbit of H under the action, is equal to $|(G : N[H])|$.

For any action of G on X, if for each $x \in X$ the stabilizer of x only contains the identity $\{e\}$ of G, then we say that the action of G on X is faithful, or that G **acts faithfully** on X. Basically, this means that for a set X, each non-identity element of G 'agrees' to take each $x \in X$ 'somewhere'.

A group G is **transitive** on a set X if for any pair $x_1, x_2 \in X$ there exist $g \in G$ such that $gx_1 = x_2$. This basically says for a group to be transitive on X, each $x \in X$ must be able to 'go anywhere' else in the set X with G's help.

3.2 Sylow Theorems

In this section we establish a partial converse to the theorem of LaGrange. Namely, if the order of a group G has a prime power divisor, then G has a subgroup of that order. We start with the concept of a p-group and work our way up to the proofs of the Sylow Theorems.

Let G be a group acting on a set X and let $x \in X$. Recall the orbit of x in X under G is $O_x = \{gx \mid g \in G\}$. Suppose that there are r orbits in X under G, and let $\{x_1, x_2, \ldots, x_r\}$ contain one element from each orbit in X. Now every element of X is in precisely one orbit, so

$$|X| = \sum_{i=1}^{r} |O_{x_i}|$$

There may be one-element orbits in X. Let X_G denote this set of one element orbits. So $X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}$. If we assume that $|X_G| = s$ (i.e. there are s elements left fixed by G), with appropriate reordering of the x_i, we may rewrite the previous equation as

$$|X| = |X_G| + \sum_{i=s+1}^{r} |O_{x_i}| \tag{3.1}$$

Equation 3.1 is known as the general class equation and will be used to establish most of the results in this section.

Theorem 3.13. Let G be a group acting on a set X. Assume that $|G| = p^n$, for some prime p. Then $|X| \equiv |X_G|$ (mod p).

Proof: From Theorem 3.11 we know that for each i, $|O_{x_i}|$ divides $|G|$. Thus if $|O_{x_i}| > 1$(which it is for $s + 1 \leq i \leq r$), then p divides $|O_{x_i}|$ for $s + 1 \leq i \leq r$. Thus Equation 3.1 implies that $|X| - |X_G|$ is divisible by p, so $|X| \equiv |X_G|$ (mod p). □

Definition 3.14. Let p be a prime. A group G is a **p-group** if every element in G has order a power of p. A subgroup of a group G is a **p-subgroup of G** if the subgroup is itself a p-group.

A nice result, which we will use later that follows directly from Theorem 3.13 is the following.

Corollary 3.2.0.5. Let G be a p-group. Then $|Z(G)| \neq 1$.

Proof: If we let G act on itself by conjugation, then the set $|X_G|$ in Equation 3.1 is easily seen to be $Z(G)$ and Theorem 3.13 gives that $|G| \equiv |Z(G)| \pmod{p}$, which implies $|Z(G)| \equiv 0 \pmod{p}$. □

Theorem 3.15. (**Cauchy's Theorem**) Let p be a prime. Let G be a finite group and let p divide $|G|$. Then G has an element of order p and, consequently, a subgroup of order p.

Proof: Form the set X of all p-tuples $(g_1, g_2, \ldots, g_p)$ of elements (not necessarily distinct) of G having the property that $g_1 g_2 \cdots g_p = e$. That is,

$$X = \{(g_1, g_2, \ldots, g_p) \mid g_1 \in G \text{ and } g_1 g_2 \cdots g_p = e\}$$

In forming this p-tuple we may let $(g_1, g_2, \ldots, g_{p-1})$ be any sequence of length $p-1$ of elements of G, and g_p is then uniquely determined as $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. Thus $|X| = |G|^{p-1}$. By assumption p divides $|G|$, thus p divides $|X|$.

Let σ be the permutation in S_P defined by $(1, 2, 3, \ldots, p)$. Let σ act on X by

$$\sigma(g_1, g_2, \ldots, g_p) = (g_{\sigma(1)}, g_{\sigma(2)}, \ldots, g_{\sigma(p)}) = (g_2, g_3, \ldots, g_p, g_1).$$

Note that if $g_1 g_2 \cdots g_p = e$ then $g_1^{-1}(g_1 g_2 \cdots g_p) g_1 = g_1^{-1} e g_1 = e$. Thus $(g_2, g_3, \ldots, g_p, g_1) \in X$. Therefore, we may consider the subgroup $\langle \sigma \rangle$ of S_p to act on X by iteration in the normal way.

Now $|\langle \sigma \rangle| = p$, which implies by Theorem 3.13 that $|X| \equiv |X_{\langle \sigma \rangle}| \pmod{p}$. Since p divides $|X|$, p must also divide $|X_{\langle \sigma \rangle}|$ and since there is at least one element $(e, e, \ldots, e) \in X_{\langle \sigma \rangle}$, there must be at least p elements in $X_{\langle \sigma \rangle}$. Hence there exists some element $a \in G$, $a \neq e$, such that $(a, a, \ldots, a) \in X_{\langle \sigma \rangle}$ and $a^p = e$. so a has order p and $\langle a \rangle \leq G$ by definition. □

Corollary 3.2.0.6. Let G be a finite group. Then G is a p-group if and only if $|G|$ is a power of p.

Proof: If G is a p-group and q a prime which divides $|G|$, then G contains an element of order q by Cauchy's Theorem. Since every element of G has order a power of p, $q = p$. Hence $|G|$ is a power of p. The reverse direction is a consequence of LaGrange's Theorem. □

The following theorem classifies all groups of order p^2. Note that while this result is fairly simple, classification of groups of order p^n for $n \geq 3$ is not trivial.

Theorem 3.16. Every group of order p^2 is abelian and is one of the folowing:

(1.) Isomorphic to $\mathbb{Z}_{p^2}$.

(2.) Isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof: Let $|G| = p^2$ and let $x \in G$. We first show G is abelian. If $x \in Z(G)$, then G is abelian and we are done. Assume $x \notin Z(G)$. $|C(x)| > |Z(G)|$ since $Z(G) \subseteq C(x)$ and $x \in C(x)$ by definition. Now the orders of both $C(x)$ and $Z(G)$ divide G and by Corollary 3.2.0.5, $|Z(G)|$ is at least p. Thus the only possibility is $|C(x)| = p^2$ and $C(x) = G$ which contradicts $x \notin Z(G)$ by Lemma 3.1.1. This shows G is abelian.

Now, since the order of x divides G, if x has order p^2, then G is cyclic and therefore isomorphic to $\mathbb{Z}_p^2$. Otherwise, every non-identity element of G has order p. Let x be a non-identity element of G and set $\langle x \rangle = H$. Select $y \in G$ with $y \notin H$ and let $K = \langle y \rangle$. Since $y \notin H$, $|H \cap K| < |H|$ and must divide p. Hence $H \cap K = \{e\}$. Also, since G is abelian, H and K are normal. $G \cong H \times K$ now follows from Theorem 2.44. Note, HK is a subgroup and will be strictly larger than H, hence $HK = G$. □

Before proving the Sylow Theorems, we need just a few more results from applying Theorem 3.13 to p-subgroups of a finite group G. Recall the normalizer of a subgroup H is denoted $N[H]$.

Lemma 3.2.1. Let H be a p-subgroup of a finite group G. Then

$$\big(N[H] : H]\big) \equiv (G : H) (\text{mod } p)$$

Proof: Let $\mathscr{L}$ be the set of left cosets of H in G, and let H act on $\mathscr{L}$ by regular left multiplication, so that $h(xH) = (hx)H$. This was seen to be an action previously for elements, but this action is well defined: if $yH = xH$, then $y = xh$ for some $h \in H$, and

$$g(yH) = (gy)H = (gxh)H = (gx)(hH) = (gx)H = g(xH)$$

. Thus H acts on the set $\mathscr{L}$ as described above and $|\mathscr{L}| = (G : H)$ by definition.

Looking at $\mathscr{L}_H$, which are the left cosets of H in G that are fixed under action by all elements of H. Now $xH = h(xH)$ if and only if $H = x^{-1}hxH$, equivalently if and only if $x^{-1}hx \in H$. Thus $xH = h(xH)$ for all $h \in H$ if and only if $x^{-1}hx = x^{-1}h(x^{-1})^{-1} \in H$ for all $h \in H$, or if $x \in N[H]$. Thus the left cosets in $\mathscr{L}_H$ are those contained in $N[H]$. The number of such cosets is $(N[H] : H)$, so $|\mathscr{L}_H| = (N[H] : H)$.

Since H is a p-group, it has order a power of p by Corollary 3.2.0.6. Theorem 3.13 then implies that $|\mathscr{L}| = |\mathscr{L}_H| \pmod p$, which gives the desired result $\big(N[H] : H]\big) \equiv (G : H) \pmod p$. □

Corollary 3.2.0.7. Let H be a proper p-subgroup of a finite group G. If $p \mid (G : H)$, then $N[H] \neq H$.

Proof: It follows from Lemma 3.2.1 that if $p \mid (G : H)$, then $p \mid (N[H] : H)$, which must therefore be different from 1. Hence, $N[H] \neq H$. □

Essentially, what this says is that if you have a p-subgroup of a finite group G and p divides the index of this group in G, then the group that normalizes H is in some sense "bigger" than H itself. At this point, we state and prove the first Sylow Theorem, which asserts the existence of prime-power subgroups of G for any prime power dividing $|G|$.

Theorem 3.17. (**First Sylow Theorem**)
Let G be a finite group and let $|G| = p^n m$ where $n \geq 1$ and where p does not divide m. Then

1. G contains a subgroup of order p^i for each i where $1 \leq i \leq n$.

2. Every subgroup H of G or order p^i is a normal subgroup of a subgroup of order p^{i+1} for $1 \leq i \leq n$.

Proof: We know G contains a subgroup of order p by Cauchy's theorem. We proceed inductively to show the existence of a subgroup of order p^i for $i < n$ implies the existence of a subgroup of order p^{i+1}. Let H be a subgroup of order p^i. Since $i < n$, we see p divides $(G : H)$. By Lemma 3.2.1, we then know p divides $(N[H] : H])$. Since H is a normal subgroup of $N[H]$(surely a group is normal in the group that *normalizes* it), we can form $N[H]/H$, and we see that p divides $|N[H]/H|$. By Cauchy's theorem again, the factor group $N[H]/H$ has a subgroup K which is of order p. If we let $\gamma : N[H] \longrightarrow N[H]/H$ be the natural, or *canonical* homomorphism, then

$\gamma^{-1}[K] = \{x \in N[H] \mid \gamma(x) \in K\}$ is a subgroup of $N[H]$ and hence of G. This subgroup contains H and is of order p^{i+1}. If we repeat the above construction and note that $H < \gamma^{-1}[K] \leq N[H]$ where $|\gamma^{-1}[K]| = p^{i+1}$, then since H is normal in $N[H]$ it is surely normal in the possibly smaller group $\gamma^{-1}[K]$. $\square$

Definition 3.18. A **Sylow p-subgroup** P of a group G with $|G| = p^n m$ is a p-subgroup of G of order p^n.

Now, we know that if H is a subgroup of G, then every conjugate gHg^{-1} is also a subgroup. The second Sylow Theorem states that if you start with a Sylow p-subgroup P, then the conjugates of P are all of the Sylow p-subgroups.

Theorem 3.19. (**Second Sylow Theorem**)
Let P_1 and P_2 be Sylow p-subgroups of a finite group G . Then P_1 and P_2 are conjugate subgroups of G.

Proof: Here we proceed along the same lines as in the proof of Lemma 3.2.1 and let $\mathscr{L}$ be the set of left cosets of say P_1 and let P_2 act on this set by regular translation(left multiplication). Thus, P_2 acts on $\mathscr{L}$ by
$y(xP_1) = (yx)P_1$ for $y \in P_2$ and $x \in G$. Then by Theorem 3.13
$|\mathscr{L}_{P_2}| \equiv |\mathscr{L}| (\text{mod } p)$, and $|\mathscr{L}| = (G : P_1)$ is not divisible by p, so $|\mathscr{L}_{P_2}| \neq 0$. Let $xP_1 \in \mathscr{L}_{P_2}$ for some $x \in G$. Then $y(xP_1) = xP_1$ for all $y \in P_2$, hence $x^{-1}yxP_1 = P_1$ for all $y \in P_2$. Thus, $x^{-1}yx \in P_1$ for all $y \in P_2$ implies
$x^{-1}P_2x \leq P_1$. Since both groups have the same order, we must have
$P_1 = x^{-1}P_2x$, and so P_1 and P_2 are conjugate subgroups. $\square$

The final Sylow theorem gives information about the number of Sylow p-subgroups. The proof will use both Theorem 3.13 as before and the second Sylow theorem.

Theorem 3.20. (**Third Sylow Theorem**)
If G is a finite group and p divides $|G|$, then the number of Sylow p-subgroups is equal to $(G : N[P])$, is congruent to 1 modulo p, and divides $|G|$.

Proof: Let P be a Sylow p-subgroup of G. This time let $\mathscr{L}$ be the set of all Sylow p-subgroups and let P act on $\mathscr{L}$ by conjugation, so that $x \in P$ carries $T \in \mathscr{L}$ into xTx^{-1}. By Theorem 3.13 $|\mathscr{L}_P| \equiv |\mathscr{L}| \pmod{p}$. Let us find $\mathscr{L}_P$. If $T \in \mathscr{L}_P$, then $xTx^{-1} = T$ for all $x \in P$. Thus $P \leq N[T]$. We also have that $T \leq N[T]$ always. Since P and T are Sylow p-subgroups in G, they are Sylow p-subgroups in $N[T]$. But then by the second Sylow Theorem, P and T are conjugate subgroups in $N[T]$. Since T is a normal subgroup of $N[T]$, it is the only conjugate in $N[T]$(Definition 2.35). Thus $T = P$. Then $\mathscr{L}_P = \{P\}$. Since $1 = |\mathscr{L}_P| \equiv |\mathscr{L}| \pmod{p}$, we see the number of Sylow p-subgroups is congruent to 1 modulo p.

Now if we let G act on $\mathscr{L}$ by conjugation, then Example 3.12 shows that the number of Sylow p-subgroups is equal to $|(G : N[P])|$ and thus divides $|G|$. □

The Sylow Theorems, in conjunction with the idea of semi-direct products (see [10]), are powerful for classifying non-abelian groups given only their order. They have their uses in determining abelian groups of small order as well. Of course, the main result on abelian groups is The Fundamental Theorem for Finitely Generated Abelian groups which can be found in most undergraduate and graduate Algebra texts (see [10]). However, we do not need such a strong result for our purposes and so the Sylow Theorems will suffice. The rest of this chapter will be devoted to specific applications of the Sylow Theorems to abelian groups of order pq and p^2q (for $|G| = 12$ we will find all groups up to isomorphism).

3.3 Applications of Sylow Theory

3.3.1 Groups of order pq

Earlier we classified groups of order p and p^2. The classification of groups of order p^n is quite a bit more involved then for the cases when $n = 1, 2$. In this section we consider groups of order pq with p and q distinct primes.

Throughout this section and the next let n_p and n_q represent the number of Sylow p and q subgroups,respectively, of a group G. Additionally, let P(resp. Q) be a p-subgroup (resp. q) of G.

Theorem 3.21. If $|G| = pq$ for primes p and q with $p > q$ then G is isomorphic to either $\mathbb{Z}_{pq}$ or to a non-abelian group K with presentation

$$K = \{\langle x, y\rangle : x^p = e = y^q \text{ and } yx = x^s y\}$$

where $s^q \equiv 1$ (mod p).

Proof: By the second and third Sylow Theorems we have $n_p \equiv 1 \bmod p$, $n_q \equiv 1 \bmod q$, $n_p \mid q$ and $n_q \mid p$. These conditions together force $n_p = 1$ and $n_q = 1$ or p. Hence, $P \trianglelefteq G$. If also $n_q = 1$ then $Q \trianglelefteq G$. Furthermore, by LaGrange's Theorem $P \cap Q = \{e\}$ and $PQ = G$. Thus, by Theorem 2.44 $G \cong P \times Q$. Since $|P| = p$, $P \cong \mathbb{Z}_p$. Likewise $Q \cong \mathbb{Z}_q$ and so $G \cong \mathbb{Z}_{pq}$.

Assume then that $n_q = p$. Let $x \in P$ and $a \neq e$. Then $\langle a\rangle = P$. Choose $y \in G \setminus \{P\}$. Then since P is normal it must contain all elements of order p, hence by Lagrange Theorem and that G isn't cyclic, y has order q. Therefore, $\langle y\rangle = Q$ is a Sylow q-subgroup. Examine the cosets of P in G. There are $(G : P) = q$ such cosets and they can be listed as $\{P, Py, Py^2, \ldots, Py^{q-1}\}$. The reason for this is

$Py^i = Py^j,\ 0 \leq i, j < q \Leftrightarrow Py^{i-j} = P \Leftrightarrow y^{i-j} \in P \cap Q = \{e\} \Leftrightarrow i = j$. Thus a presentation for the elements of G is given by $G = \{\langle x, y\rangle : x^p = e = y^q\}$. Now to determine the multiplication of xy we let Q act on P by conjugation. This induces an automorphism of P since P is normal. Thus $yxy^{-1} = x^s$, for some s, $1 < s < p$ ($s \neq 1$ as this would imply G was abelian). Proceeding inductively, we find that $y^i x y^{-i} = x^{s^i}$. setting $i = q$ yields

$$\begin{aligned} x &= x^{s^q} \\ \Rightarrow e &= x^{s^q - 1} \\ \Rightarrow p &\mid (s^q - 1) \\ \Rightarrow s^q &\equiv 1 mod p \end{aligned}$$

Thus s has order q in the multiplicative group $(\mathbb{Z}_p \setminus \{e\}, *)$. □

As a special case, let $q = 2$ and we see the conditions on s above imply $s \equiv -1$ (mod p). Hence G is isomorphic to either the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p with presentation

$$D_p = \{\langle x, y\rangle : x^p = e = y^2 \text{ and } yx = x^{-1}y\}$$

.

Example 3.22. Let $|G| = 15 = 5 \cdot 3$. Then $5 > 3$, $5 \not\equiv 1$ (mod 3), hence $n_p = 1,\ n_q = 1$ and $G \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$. This gives that there is, up to isomorphism, one group of order 15.

Example 3.23. Let $|G| = 14 = 7 \cdot 2$. Then by our note above, G is either $\mathbb{Z}_{14}$ or the dihedral group D_7.

3.3.2 Groups of order p^2q

Classifying the groups of order p^2q is a non-trivial matter which uses the concept of semi-direct products and finite field theory extensively. For a full

treatment, see [21] for a variety of approaches. Our purpose will be to find only the abelian groups of order p^2q.

Theorem 3.24. Let G be a group of order p^2q. If G is abelian, then G is isomorphic to either $\mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$.

Proof: If G is abelian, then every subgroup of G is normal and by the Third Sylow Theorem, $n_p = 1$ for all p dividing G. Thus P is normal, Q is normal and the result follows by Theorems 2.44 and 3.16.

Example 3.25. Let G be abelian and $|G| = 18 = 3^2 * 2$. Then we can see from the above result that $G \cong \mathbb{Z}_9 \times \mathbb{Z}_2$ or $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2$.

Proceeding in a fashion similar to the previous example, we can state that there are two abelian groups of order 20, namely

$$\mathbb{Z}_5 \times \mathbb{Z}_4, \text{ and } \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

The next result classifies all group of order 12.

Theorem 3.26. There are five isomorphism classes of groups of order 12. They are represented by:

(i) the product of cyclic groups $\mathbb{Z}_3 \times \mathbb{Z}_4$;

(ii) the product of cyclic groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$;

(iii) the alternating group A_4;

(iv) the dihedral group D_6;

(v) the group generated by $\langle x, y \rangle$, with relations $x^4 = e$, $y^3 = e$, $xy = y^2x$.

Note: $\mathbb{Z}_3 \times \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_{12}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$.

Proof: let G be a group of order 12. Let H be a Sylow 2-subgroup, which has order 4, and let K be a Sylow 3-subgroup,of order 3. It follows from Theorem 3.20 that the number of Sylow 2-subgroups is either 1 or 3, and that the number of Sylow 3-subgroups is 1 or 4. Also, H is a group of order 4 and is isomorphic to either the cyclic group $\mathbb{Z}_4$ or the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. We prove the following lemma first:

Lemma 3.3.1. At least one of the two subgroups H,K is normal.

Proof: Suppose that K is not normal. Then K has four conjugate subgroups $K = K_1, \ldots, K_4$. Since $|K_i| = 3$, the intersection of any two of these groups must be the identity(since each non identity element generates the group). This gives 8 non identity elements which leaves only three elements of G which are not in any of the groups of K_i. Any Sylow 2-subgroup H has order 4, and $H \cap K_i = \{e\}$. Therefore it consists of these three elements and e. This describes H for us and shows that there is only one Sylow 2-subgroup. Thus H is normal. □

Since $H \cap K = \{e\}$, every element of HK has a unique expression as a product hk (Theorem 2.44), and since $|G| = 12$, $HK = G$. If H is normal, then G operates on K by conjugation, and will show that this operation, together with the structure of H and K, determines the structure of G. Similarly, if K is normal then H operates on K, and this operation determines G.

Case 1: H and K are both normal. Then by Theorem 2.44, G is isomorphic to the product group $H \times K$. There are two possibilities:

(1.) $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$.

(2.) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$.

These are the abelian groups of order 12.

Case 2: H is normal but K is not. So there are four conjugate Sylow 3-subgroups $\{K_1, \ldots, K_4\}$, and G operates by conjugation on this set S of four subgroups. This operation determines a permutation representation

$$\varphi : G \longrightarrow S_4.$$

The stabilizer of K_i is the normalizer $N[K_i]$, which contains K_i. Lemma 3.2.1 gives $(N[K_i] : K_i) \equiv (G : K_i) \pmod 3$. $(G : K_i) \equiv 1 \pmod 3$, and since we assumed K was not normal, $(N[K_i] : K_i) \neq 4$, which implies $(N(K_i) : K_1) = 1$. Thus, $N[K_i] = K_i$. Since the only element common to the subgroups K_i is the identity element, the intersection of the normalizers is only the identity. Thus φ is injective and G is isomorphic to its image under φ.

Since G has four subgroups of order 3, it contains eight elements of order 3, and these elements certainly generate the group. If x has order 3, then $\varphi(x)$ is a permutation of order 3 in S_4. If $\sigma \in S_4$ is a permutation of order 3, say $\sigma = (a, b, c)$, then σ can be decomposed into the following $\sigma = (a, c)(a, b)$. Hence any 3-cycle is even. Therefore im$\varphi \subset A_4$ (the group of even permutations). Since $|G| = |A_4|$ and φ is injective, the two groups are equal.

Case 3: K is normal, but H is not. In this case H operates on K by conjugation, and conjugation by an element of H is an automorphism of K. We let y be a generator for the cyclic group K : $y^3 = e$. There are only two

automorphisms of K—the identity and the automorphism which interchanges y and y^2.

Suppose that H is cyclic of order 4, and let x generate H : $x^4 = e$. Then since G is not abelian, $xy \neq yx$, and so conjugation by x is not the trivial automorphism of K. Hence $xyx^{-1} = y^2$, and the following generators and relations define a non-abelian group of order 12:

$$x^4 = e,\ y^3 = e,\ xy = y^2x.$$

The last possibility is that H is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then the elements of H are $\{e, v, w, vw\}$, and the relations $v^2 = w^2 = e$, and $vw = wv$ hold in H. Since there are only two automorphisms of K, there is an element $w \neq e$ in H which operates trivially: $wyw^{-1} = y$. Since G is not abelian, there is also an element v which operates non-trivially: $vyv^{-1} = y^2$. Since $w^2 = e$ and $y^3 = e$ it must hold that $x = wy$ has order 6. Then we have

$$\begin{aligned} vxv^{-1} &= vwyv^{-1} \\ &= wvyv^{-1} \\ &= wy^2 \\ &= y^2w \\ &= (wy)^{-1} \\ &= x^{-1} \end{aligned}$$

The relations $x^6 = e,\ v^2 = e,\ vxv^{-1} = x^{-1}$ define the group D_6, so G is the group of symmetries of the regular hexagon in this case.

In the next chapter we will give matrix representations for the groups classified in this section.

3.4 Representations for our Groups

In the last section we dealt with finding abelian groups of small order. Later we will be using these groups to play the Gordon game. In order to do this, we will employ the help of a computer search program. This program will be written in MATLAB, and as such we will need to be able to represent our group elements as matrices. Cayley's Theorem would allow us to do this by associating group or order n with a subgroup of S_n, and then using the corresponding permutation matrices as our group elements. Wjile this is a feasible strategy, the resulting matrices are $n \times n$ and thus can become cumbersome to work with. Thus, if possible, we would like a simpler representation for our group elements. Fortunately, we will not need representations for all of the groups we wish to play with; we will be able to input the integers mod n as a row vector of length n where the components of the vector will be the integers $[0, n-1]$. However, we will need representations for the group elements of the other abelian groups we wish to investigate. With that in mind, we have the following definition for a matrix representation.

Definition 3.27. [6] An n-dimensional *matrix representation* of a group G is a homomorphism

$$R : G \longrightarrow GL_n(\mathbb{F})$$

Although we didn't give this as a definition earlier, we have previously seen an example of this type of map. The map

$$\pi : S_n \longrightarrow GL_n(\mathbb{F})$$

in which a permutation gets sent to its permutation matrix, $\sigma \mapsto P_\sigma$ is an example of a matrix representation. So, given that our goal is to extend

Isbell's work to include abelian groups of size less than 20 and to include the groups of order 12, we need representations for the following:

1. $\mathbb{Z}_{10} \times \mathbb{Z}_2$
2. $\mathbb{Z}_6 \times \mathbb{Z}_3$
3. *All groups of order 12*

To find representations for these groups as matrices, recall from linear algebra that when we raise a diagonal matrix to power n, the result is that we raise each of the diagonal entries to the power n.

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^n = \begin{pmatrix} x^n & 0 \\ 0 & y^n \end{pmatrix}$$

We can use this result to our advantage since the summands of the direct products themselves are cyclic as well.

3.4.1 Using roots of unity

We shall start by finding representations for the abelian groups with cyclic components. The idea will be to replace each of the generators with a 2×2 diagonal matrix with one of the entries equal to 1 and the other equal to an n^{th} root of unity that will be picked according to the order of the component. Recall, an n^{th} root of unity is a complex number that is a solution to $x^n - 1 = 0$. Such roots of unity can be found using Euler's formula,

$$e^{i\theta} = \cos\theta + i\sin\theta$$

For example, the 6 roots of unity divide the unit circle into 6 equal parts, thus each cuts out an angle of $\frac{2\pi}{6}$ or $\frac{\pi}{3}$. Therefore, in the above equation if we let

$\theta = \frac{\pi}{3}$, we get

$$\begin{aligned} e^{i\frac{\pi}{3}} &= \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} \\ &= \frac{1}{2} + i\frac{\sqrt{3}}{2} \end{aligned}$$

From the equation $x^n - 1 = 0$ and the property of diagonal matrices mentioned above, if we pick $\alpha \in \mathbb{C}$ such that α is a primitive root of unity then the matrix $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ will have order n and thus be isomorphic to $\mathbb{Z}_n$ by Theorem 2.15.

Our first group will be $\mathbb{Z}_6 \times \mathbb{Z}_3$. We need β a primitive $6th$ root of unity, which we calculated above to be $\alpha = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Now, α generates a group of order 6, which means that $\beta = \alpha^2$ will generate a group of order 3. Fortunate for us, that's exactly what we need. If we take the set $\{(1,0),(0,1)\}$ as a generating set for $\mathbb{Z}_6 \times \mathbb{Z}_3$, then mapping $(1,0) \mapsto \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $(0,1) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & \beta \end{smallmatrix}\right)$ we have the map

$$\phi((x,y)) = \begin{pmatrix} \alpha^x & 0 \\ 0 & \alpha^{2y} \end{pmatrix}$$

is a homomorphism $\mathbb{Z}_6 \times \mathbb{Z}_3 \longrightarrow GL_2(\mathbb{C})$.

For the next group $\mathbb{Z}_{10} \times \mathbb{Z}_2$, we let γ be a primitive 10^{th} root of unity and note that if $\gamma^{10} = 1$, then $\delta = \gamma^5$ has order 2, i.e. $\delta^2 = (\gamma^5)^2 = 1$. But this must mean that $\gamma^5 = \pm 1$ and since we assumed γ was a primitive 10^{th} root of unity, we must have $\gamma^5 = -1$. Therefore, we have the map $(1,0) \mapsto \left(\begin{smallmatrix} \gamma & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $(0,1) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ giving

$$\phi((x,y)) = \begin{pmatrix} \beta^x & 0 \\ 0 & (-1)^y \end{pmatrix}$$

is a homomorphism $\mathbb{Z}_{10} \times \mathbb{Z}_2 \longrightarrow GL_2(\mathbb{C})$.

Our last abelian group for which we need a matrix representation is the group $\mathbb{Z}_6 \times \mathbb{Z}_2$. The legwork for this group has been done for us since we know

$\alpha^6 = 1$ and that the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ has order 2. Thus the map $(1,0) \mapsto \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $(0,1) \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

This completes the list of abelian groups for which we need matrices that represent their elements. The next section gives another approach to finding representations.

3.4.2 Using Rigid Motions

In this section we take the groups that represent symmetries of geometric shapes and treat their generators as linear transformations, thus inducing a matrix representation. The idea, taken from linear algebra, is to take a basis $\{v_1, v_2\}$ for a vector space, say $\mathbb{R}^2$. Then, for a given linear transformation $\phi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, the matrix

$$\Big[\phi(v_1),\ \phi(v_2)\Big]$$

where $\phi(v_i)$ is written as a column vector, is a matrix representation for ϕ.

Consider first the group $D_6 = \{\langle x, y\rangle : x^6 = y^2 = e \text{ and } xy = yx^{-1}\}$. This group represents the rigid motions of the regular hexagon, and if we position the hexagon in the plane with it's center at the origin, as in Fig.3.1, we can take as a basis $\{v_1, v_2\}$ where each v_i passes through a vertex separated by $120\,^\circ$.

Figure 3.1: Basis for Symmetries of the Hexagon

.

Let x denote counterclockwise rotation by 60° and y denote reflection across the axis through v_1. Applying these transformations to $\{v_1, v_2\}$ in Fig. 3.1 we see that

$$x(v_1) = v_1 + v_2$$
$$x(v_2) = -v_1$$
$$y(v_1) = v_1$$
$$y(v_2) = -v_1 - v_2$$

Using the output of the transformation as columns of R_x and R_y respectively, we have the following matrix representations for x and y

$$R_x = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad R_y = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

To verify the relations on x and y hold, observe

$$\begin{aligned} R_x R_y &= \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} R_y R_x^{-1} &= \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \\ &= R_y R_x^{-1} \end{aligned}$$

Also, it can be checked that

$$R_x^6 = R_y^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, the relations on the generators x and y hold for R_x and R_y and therefore $\{R_x, R_Y\}$ generate a group of matrices isomorphic to D_6

We would like to mention, without proof, that for any n, the dihedral group $D_n = \{\langle x, y\rangle : x^n = y^2 = e \text{ and } xy = yx^{-1}\}$ can be represented by the following map

$$x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$
$$y \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

with the entries and calculations taken mod n.

Our next group shall be A_4. Recall from group theory that A_4 is isomorphic to T, the group of symmetries on the 3-dimensional tetrahedron and thus the group elements may be considered as linear transformations of $\mathbb{R}^3$. If we position the tetrahedron with center at the origin, one choice of basis will have the coordinate axes passing through three of the vertices. Label the vertices $\{1, 2, 3, 4\}$ and corresponding basis vectors $\{v_1, v_2, v_3\}$ as shown in Figure 3.2.

Figure 3.2: Basis for Symmetries of the Tetrahedron

.

Abstractly, T has presentation

$$\langle x, y : x^3 = y^2 = (xy)^3 = e \rangle$$

. Let x denote 120° counter-clockwise rotation about the axis of symmetry through v_2 and let y denote rotation by 180° about the axis of symmetry which passes through the midpoints of edges $(1, 2)$ and $(3, 4)$. Applying x to the basis yields

$$x(v_1) = v_3$$

$$x(v_2) = v_2$$

$$x(v_3) = -v_1 - v_2 - v_3$$

The matrix representation of this transformation is thus

$$R_x = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & -1 \\ 1 & 0 & -1 \end{pmatrix}$$

Similarly, applying y to the basis yields

$$y(v_1) = v_3$$

$$y(v_2) = -v_1 - v_2 - v_3$$

$$y(v_3) = v_1$$

with corresponding matrix representation

$$R_y = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$$

As a check of the relations, we have

$$R_x^3 = R_y^2 = (R_x R_y)^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

. Therefore the matrices $\{R_x, R_y\}$ generate a group isomorphic to A_4.

For the last group, recall the relations on the generators in Theorem 3.26: $\langle x, y : x^4 = e, y^3 = 1, xy = y^2x\rangle$ This group is the semi-direct product $\mathbb{Z}_3 \ltimes \mathbb{Z}_4$. We choose not to investigate semi-direct products since we are primarily interested in working with abelian groups. The previous two groups were clearly not abelian and since we wanted to include all groups of order 12, we needed to include this one as well. The literature will refer to this group as the dicyclic group of order 12 [6]. Listed below is the group table for $\mathbb{Z}_3 \ltimes \mathbb{Z}_4$.

Figure 3.3: $\mathbb{Z}_3 \ltimes \mathbb{Z}_4$

$*$	e	x	x^2	x^3	y	y^2	xy	x^2y	x^3y	xy^2	x^2y^2	x^3y^2
e	e	x	x^2	x^3	y	y^2	xy	x^2y	x^3y	xy^2	x^2y^2	x^3y^2
x	x	x^2	x^3	e	xy	xy^2	x^2y	x^3y	y	x^2y^2	x^3y^2	y^2
x^2	x^2	x^3	e	x	x^2y	x^2y^2	x^3y	y	xy	x^3y^2	y^2	xy^2
x^3	x^3	e	x	x^2	x^3y	x^3y^2	y	xy	x^2y	y^2	xy^2	x^2y^2
y	y	xy^2	x^2y	x^3y^2	y^2	e	x	x^2y^2	x^3	xy	x^2	x^3y
y^2	y^2	xy	x^2y^2	x^3y	e	y	xy^2	x^2	x^3y^2	x	x^2y	x^3
xy	xy	x^2y^2	x^3y	y^2	xy^2	x	x^2	x^3y^2	e	x^2y	x^3	y
x^2y	x^2y	x^3y^2	y	xy^2	x^2y^2	x^2	x^3	y^2	x	x^3y	e	xy
x^3y	x^3y	y^2	xy	x^2y^2	x^3y^2	x^3	e	xy^2	x^2	y	x	x^2y
xy^2	xy^2	x^2y	x^3y^2	y	x	xy	x^2y^2	x^3	y^2	x^2	x^3y	e
x^2y^2	x^2y^2	x^3y	y^2	xy	x^2	x^2y	x^3y^2	e	xy^2	x^3	y	x^2
x^3y^2	x^3y^2	y	xy^2	x^2y	x^3	x^3y	y^2	x	x^2y^2	e	xy	x^2

A representation for the x and y is given below.

$$R_x = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$R_y = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

The above matrices satisfy the relations for $\mathbb{Z}_3 \ltimes \mathbb{Z}_4$. Observe,

$$R_x^4 = R_y^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{aligned} R_x R_y &= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} i & -i \\ 0 & -i \end{pmatrix} \end{aligned}$$

while

$$\begin{aligned} R_y^2 R_x &= \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\ &= \begin{pmatrix} i & -i \\ 0 & -i \end{pmatrix} \\ &= R_x R_y \end{aligned}$$

Our work up to this point has been to classify abelian groups of size less than 20 and construct matrix representations for those that we cannot represent in other ways for the purposes of MATLAB programming. The next chapter can

be regarded as the main body of work for this thesis. The first topic discussed is that of group sequencing. We will classify some sequenceable groups and give examples of group sequencings. In addition, we discuss topics related to group sequencing including Terraces, Latin squares, Hamiltonian paths, and the Gordon game.

Chapter 4

Group Sequencing

In 1961, Basil Gordon (1931-2012), a mathematician working at UCLA, was investigating the connection between specific types of Latin squares and the arrangement of group elements. An example of a Latin square is given below. Basically, to form a Latin square one starts with a symbol set X of order n. Each element of X must appear in each row and each column exactly once in the $n \times n$ array containing the symbols. The connection to arrangements of group elements is immediate since the Cayley table for a finite group G of order n is a Latin square of order n. In fact, we say a Latin square is based on a group G if the Cayley table for G corresponds ot the Latin square.

Figure 4.1: A Latin square

a	b	c
b	c	a
c	a	b

The connection Gordon was trying to determine was to a specific type of Latin square called complete Latin squares. We will investigate this connection more formally later in the chapter, but the idea behind a complete Latin square

is that for any pair of distinct symbols $(a, b) \in X$, one can locate the pair as consecutive entries in some row and some column of the square. This condition is much more stringent than just having each element represented, but the reward is also greater. For example, in agricultural experiments a symbol may represent a treatment to be given to a plot of land (to test effectiveness of promoting crop growth). If there are n treatments to test and there is a reasonable possibility that neighboring tests may affect one another, then a complete Latin square is a good design.

During the investigation of possible methods to construct complete Latin squares based on groups the following problem arose: can the elements of a finite group G be ordered in a sequence $\{a_1, a_2, \ldots, a_n\}$ in such a way that the sequence of partial products $\{b_1, b_2, \ldots, b_n\}$, where $b_i = a_1 a_2 \cdots a_i$, are all distinct? The solution to this problem would effectively give a method for constructing complete Latin squares based on a group G. Gordon investigated this problem and solved it for the case where G was an abelian group. The first section details the method of constructing what Gordon termed group sequencings.

4.1 Sequencing Abelian Groups

We start with Gordon's definition for a sequenceable group.

Definition 4.1. A non-trivial finite group G of order n is said to be **sequenceable** if its elements can be arranged in a sequence

$$\mathbf{a} = \big(a_1, a_2, \ldots, a_n\big)$$

such that the partial products

$$\mathbf{b} = \big(b_1, b_2, \ldots, b_n\big)$$

where $b_i = a_1 a_2 \cdots a_i$, are distinct. **a** is called a *sequencing* for G.

First, note that if G is sequenceable, then we must have $a_1 = b_1 = e$, where e is the identity for G. If $a_i = e$ for some $i \neq 1$, then

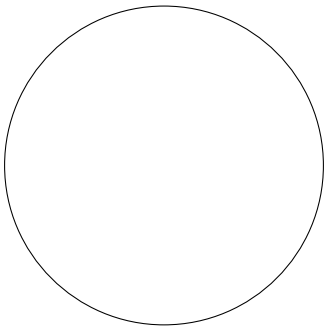
$$b_i = b_{i-1} a_i = b_{i-1} e = b_{i-1}$$

and thus the elements of **b** are not distinct.

As was mentioned in the introduction, Gordon solved the problem of determining which abelian groups were sequenceable. In order to gain insight into his proof, we will start by trying to sequence the most basic of abelian groups, $\mathbb{Z}_n$.

Example 4.2. Start by choosing your favorite group of integers mod n, say $\mathbb{Z}_{12}$. My choice here is not entirely arbitrary, as I can envision $\mathbb{Z}_{12}$ as being the numbers on a standard clock as pictured below.

Figure 4.2: Integers mod 12



Now, since both of our sequences **a** and **b** must be distinct and since **b** represents the partial products, a_i must therefore represent the element added to b_{i-1} to equal b_i. Thus, we can think of each a_i as representing a "movement" around the clock. Start by choosing $a_1 = 0$, and move clockwise one unit to 1. Then move two units counterclockwise to 11, three units clockwise to

2, followed by four units counterclockwise to 10, etc. We should end with eleven units clockwise from 7 to 6. If we let clockwise steps be positive and couterclockwise steps be negative we see that

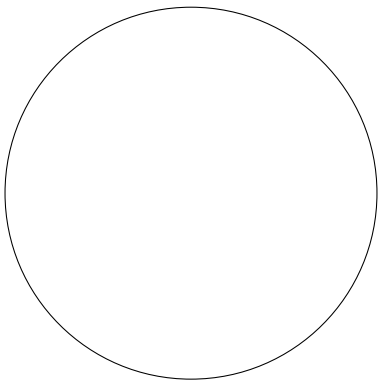
$$\begin{aligned}\mathbf{a} &= \{0, 1, -2, 3, -4, 5, -6, 7, -8, 9, -10, 11\} \\ &= \{0, 1, 10, 3, 8, 5, 6, 7, 4, 9, 2, 11\}\end{aligned}$$

and the corresponding sequence of partial products is given by where we traveled to after each step. Specifically,

$$\mathbf{b} = \{0, 1, 11, 2, 10, 3, 9, 4, 8, 5, 7, 6\}$$

Well, this procedure worked well in the case $\mathbb{Z}_{12}$. Does it hold for $\mathbb{Z}_n$ when n is odd? Let's try to sequence $\mathbb{Z}_{15}$ using the same greedy algorithm as before. Using the fifteen hour clock below as a guide, follow the same process for choosing each b_i as before.

Figure 4.3: Integers mod 15



Pick 0, then 1, then 14, then 2, etc. to get

$$\mathbf{b} = \{0, 1, 14, 2, 13, 3, 12, 4, 11, 5, 10, 6, 9, 7, 8\}$$

To compute the a_i we use that if $b_i = a_1 \cdots a_i$ and $b_{i-1} = a_1 \cdots a_{i-1}$, then $a_i = b_{i-1}^{-1} b_i$. Thus our sequencing looks like

$$\mathbf{a} = \{0, 1, 13, 3, 11, 5, 9, 7, 7, 9, 5, 11, 3, 13, 1\}$$

This doesn't look good. We only used the odd steps. While this sequence definitely looks interesting (we will visit this exact form later in the chapter), it fails to have distinct elements, and thus will not be a sequencing for $\mathbb{Z}_{15}$. Should we consider a different strategy for picking the b_i's? The answer is no. In fact, we cannot for a sequencing for $\mathbb{Z}_n$ with n odd since the partial products of such a sequencing will necessarily have to be distinct and the sum of all the group elements, b_n, written in any order, will be the identity 0 since the elements commute and cancel in pairs. This contradicts that $b_1 = 0$.

Okay, so $\mathbb{Z}_n$ is not sequenceable if n is odd. We can use the same argument above to say that for n even, $\mathbb{Z}_n$ is sequenceable. The reasoning is that there is an element of order 2 in $\mathbb{Z}_n$ when n is even that doesn't cancel with any other elements in the partial products and so the sum of all the elements of G, written in any order, is this order 2 element. The ordering of the rest of the initial list was to ensure we didn't cancel anything too early, which would have created a duplicate element. Is this the case for any group that is abelian and has order 2 elements? Let's do another example, this time taking the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. This is the other abelian group of order 12 that we found previously.

Example 4.3. Let G be the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. This group has as elements

$$\Big\{(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,1,1),(0,1,2),$$
$$(1,0,0),(1,0,1),(1,0,2),(1,1,0),(1,1,1),(1,1,2),\Big\}$$

Notice there are 3 elements of order 2, they are $\{(0,1,0),(1,0,0),(1,1,0)\}$. They correspond to the non-identity elements of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, of which there is an isomorphic copy within G. These elements create a subgroup of order 4. Now, if this group were to have a sequence of distinct partial products, assume it was the following $(b_1, b_2, \ldots, b_{12})$, where each $b_i = a_1 \cdots a_i$. Then we have that if $a_i = (1,1,0) = (1,0,0) + (0,1,0)$, then the elements $(1,0,0)$ and $(0,1,0)$ occur twice in the expansion. That's not good, because each time they occur they will cancel, thus eliminating all the order 2 elements, and we will be back to the situation where the sum of the elements is the identity, $b_n = 0$.

We have an example where a group containing a single element of order 2 was sequenceable. Also, we saw that if G contained zero or more than one element of order 2, then the G was not sequenceable. Before proving a necessary condition for a group G to be sequenceable, we establish the following lemma, which generalizes the above example concerning the number of order 2 elements within a group G.

Lemma 4.1.1. If G is an abelian group then the set

$$H = \{a \in G \mid 2a = a + a = 0\}$$

forms a subgroup which can be regarded as a vector space over the field with 2 elements.

Proof: Assume H has order k, with $k > 1$. Let $x, y \in H$. Then using additive notation, $2x = 0 = 2y$ and their product $x + y$ also has order 2 since $x+y+x+y = 2x+2y = 0$. Thus H is closed under inverses and products and is hence a subgroup of G. By Definition 3.14, H is a p-group and by Corollary 3.2.0.6 the order of H is a power of 2, so $|H| = 2^m$ for $m > 1$. If we choose the scalar field to be $\mathbb{F}_2$, the field with two elements, then $\mathbb{F}_2$ acts on H by

left multiplication. The terminology in abstract terms is that H is a left R-module, with $\mathbb{F}_2$ acting as R. Modules can be thought of as the generalization of group action to rings. Essentially, if groups act on sets, then rings 'act' on modules. Due to the more complex nature of a ring, the structure on which it acts must have more structure. H possess this extra structure by being abelian and when the ring acting on the module happens to be a field ($\mathbb{F}_2$ in our case), the axioms for a module are the same as those for a vector space over $\mathbb{F}$ [10]. Hence, in the finite case, H can be regarded as a vector space of dimension m. □

We now state and prove a necessary condition for G to be sequenceable.

Theorem 4.4. If a finite abelian group G is sequenceable, then G has a single element of order 2.

Proof: Suppose that $\{a_1, a_2, \ldots, a_n\}$ is a sequencing of G with associated partial product sequence $\{b_1, b_2, \ldots, b_n\}$. Assume G has no elements of order 2. Then for each $a \in G \setminus 0$, we have that $a \neq -a$, and thus all of non-identity elements of G will cancel in pairs (we saw this in the example using $\mathbb{Z}_{15}$), leaving $b_n = 0$. This contradicts $b_1 = 0$. Thus G must have at least one element of order 2. Assume G has k elements of order 2. By lemma 4.1.1, the subgroup H generated by these elements can be regarded as a vector space over $\mathbb{Z}_2$ with dimension m and order $k + 1 = 2^m$, for $m > 1$. Additionally, H has a basis $\{v_1, v_2, \ldots, v_m\}$ and each $h \in H$ can be written uniquely as $\lambda_1 v_1 + \cdots + \lambda_m v_m$ with $\lambda_i \in \mathbb{Z}_2$. In this form, there are 2^{m-1} elements of H that have the basis element v_i in their expansion for each i. Since each v_i occurs an even number of times in the sum of all the elements and $2v_i = 0$, we again must have $b_n = 0$, a contradiction. Thus G cannot have more than one element of order 2. □

So, we have a necessary condition for a group to be sequenceable. The next question is whether we can turn this into a sufficient condition. We start with a definition.

Definition 4.5. A group G is a **binary group** if G has exactly one element of order 2.

So the condition we seek to prove is that if G is a finite binary abelian group, then G is sequenceable. It will be helpful to know the form of all finite binary abelian groups, and for this purpose we will need The Fundamental Theorem of Finitely Generated Abelian Groups. This theorem gives complete structural information about all finite abelian groups. The proof is frequently given as a specific case of a more general theorem pertaining to finitely generated R-Modules.

Theorem 4.6. [10] (**Fundamental Theorem of Finitely Generated Abelian Groups**) Let G be a finitely generated abelian group. Then

(1.)

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

for some integers $r, n_1, n_2, \ldots, n_s$ satisfying the following conditions:

(a.) $r \geq 0$ and $n_j \geq 2$ for all j, and

(b.) $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$

(2.) the expression in (1) is unique.

In the statement of the theorem, the expression $\mathbb{Z}^r$ is known as the *free abelian group of rank r*. For more information about free groups in general, [16] is a good source. In the case where G is finite, then $r = 0$ above and we

have that G is isomorphic to a direct product of cyclic groups $\mathbb{Z}_{n_i}$ with the added condition that the order of each summand divides the one before it. Using the above theorem and the fact that if d divides the order of a cyclic group A, then A contains a unique subgroup of order d, we can classify finite binary abelian groups as follows

Lemma 4.1.2. Let G be a finite binary abelian group. Then G is isomorphic to $\mathbb{Z}_{2^k} \times B$, where $k \geq 1$ and B is an abelian group of odd order.

Proof: By Theorem 4.6 $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ and since G is a binary group we can take that $n_1 = 2^k$ for some $k \geq 1$. If $2 \mid n_i$ for $1 < i \leq s$, then there would exist a second subgroup of order 2 contained in one of the other summands of G. This contradicts that G is a binary group by lemma 4.1.1. Thus all n_i for $1 < i \leq s$ are odd and hence $|\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}|$ has odd order and this completes the proof. □

We need just one final piece before stating Gordon's result about sequenceable abelian groups.

Lemma 4.1.3. If $(j, \sigma_1, \sigma_2, \ldots, \sigma_m)$ are positive integers then there exist unique integers $j_0, j_1, \ldots, j_m$ such that

$$\begin{aligned} j &\equiv j_0 (\text{mod } \sigma_1\sigma_2\cdots\sigma_m) \\ j_0 &= j_1 + j_2\sigma_1 + j_3\sigma_1\sigma_2 + \cdots + j_m\sigma_1\cdots\sigma_{m-1} \\ \text{and } 0 &\leq j_i < \sigma_i \quad \text{for } 1 \leq i \leq m \end{aligned}$$

Proof: j_0 is unique by the properties of equivalence classes mod n. The case where $m = 1$ is clear. If $m = 2$, then we can use the division algorithm to find unique integers j_1, j_2 such that

$$j_0 = j_1 + j_2 v_1 \quad \text{and } 0 \leq j_i < v_1$$

Since $j_0 < v_1 v_2$, we must also have $j_2 < v_2$. The result now follows by induction on m. We are now ready to state Gordon's result about sequenceable groups.

Theorem 4.7. [13] A finite abelian group G is sequenceable if and only if G is the direct product of two groups A and B, where A is cyclic of order 2^k $(k > 0)$ and B is of odd order (or empty).

The direction $(\Rightarrow)$ has already been done using Theorem 4.4 and Lemma 4.1.2. The reverse direction is constructive and before giving the details, I think it is important to gain some insight into how the construction works. We shall define the sequence of partial products **b** and show they are distinct. Then, using $a_i = b_{i-1}^{-1} b_i$, we show the **a** has distinct elements. We walk through the construction using $G = \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ as a guide.

Example 4.8. *Let $G = \mathbb{Z}_{12}$. We know this group is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$. Using the Chinese Remainder correspondence, we have $\mathbb{Z}_{12} \to \mathbb{Z}_4 \times \mathbb{Z}_3$ by the map $1 \mapsto (1,1)$. So, we have the group elements of $\mathbb{Z}_4 \times \mathbb{Z}_3$, listed in order $0 - 11$ are*

$$\big\{(0,0),(1,1),(2,2),(3,0),(0,1),(1,2),(2,0),(3,1),(0,2),(1,0),(2,1),(3,2,)\big\}$$

G has order $n = 12$. Recall from Ex.4.2 the sequence of partial products of $\boldsymbol{b}$ is given by

$$\boldsymbol{b} = \{0,1,11,2,10,3,9,4,8,5,7,6\}$$

which corresponds to the sequence in $\mathbb{Z}_4 \times \mathbb{Z}_3$

$$\boldsymbol{b} = \Big((0,0),(1,1),(3,2),(2,2),(2,1),(3,0),(1,0),(0,1),(0,2),(1,2),(3,1),(2,0)\Big)$$

A generating set of G is $\{(1,0),(0,1)\}$. Set $c_0 = (1,0)$ and $c_1 = (0,1)$. It should be noted that in general if A is the direct product of cyclic groups then

the set

$$\{e_i \in A \mid e_i \text{ has a 1 in the } i^{th} \text{ component and 0's elsewhere}\}$$

can be used as a generating set for A. The order of c_0 *is 4 and the order of* c_1 *is 3. Set* $\sigma_0 = 4$ *and* $\sigma_1 = 3$. *For* $0 \leq j < \frac{n}{2}$, *use Lemma 4.1.3 to find the unique integers* j_0, j_1 *such that*

$$j \equiv j_0 \ (mod\ \sigma_1)$$

$$j_0 = j_1$$

$$0 \leq j_1 < \sigma_1$$

They are

$$j = 0 \equiv 0 = j_0 = j_1$$

$$j = 1 \equiv 1 = j_0 = j_1$$

$$j = 2 \equiv 2 = j_0 = j_1$$

$$j = 3 \equiv 0 = j_0 = j_1$$

$$j = 4 \equiv 1 = j_0 = j_1$$

$$j = 5 \equiv 2 = j_0 = j_1$$

Now, using the notation $(1,0)^k$ *to mean* $(1,0)$ *added to itself* k *times, let* $i = 2j + 1$ *for* $0 \leq j < 6$ *and examine the elements of* b_i *in the sequence of partial products. We have*

$$j = 1,\ b_3 = (3,2) = (1,0)^{-1} + (0,1)^{-1}$$

$$j = 2,\ b_5 = (2,1) = (1,0)^{-2} + (0,1)^{-2}$$

$$j = 3,\ b_7 = (1,0) = (1,0)^{-3} + (0,1)^{0}$$

$$j = 4,\ b_9 = (0,2) = (1,0)^{-4} + (0,1)^{-1}$$

$$j = 5,\ b_{11} = (3,1) = (1,0)^{-5} + (0,1)^{-2}$$

And note that each b_i has the form $c_0^{-j}+c_1^{-j_1}$. Next, let $i = 2j+2$ for $0 \leq j < 6$ and examine the even b_i's. They are

$$j = 0,\ b_2 = (1,1) = (1,0)^1 + (0,1)^1$$

$$j = 1,\ b_4 = (2,2) = (1,0)^2 + (0,1)^2$$

$$j = 2,\ b_6 = (3,0) = (1,0)^3 + (0,1)^3$$

$$j = 3,\ b_8 = (0,1) = (1,0)^4 + (0,1)^1$$

$$j = 4,\ b_{10} = (1,2) = (1,0)^5 + (0,1)^2$$

$$j = 5,\ b_{12} = (2,0) = (1,0)^6 + (0,1)^3$$

And note that each b_i has the form $c_0^{j+1} + c_1^{j_1+1}$.

The patterns found above will be the ones we use in the construction of the sequence of partial products for the proof of Theorem 4.7. Assume G is finite of order n and that $G = A \times B$ with A a cyclic group of order 2^k and B a group of odd order. From our previous discussion we know G has a generating set, call it $\{v_0, v_1, \ldots, v_m\}$, where v_0 has order 2^k and for $1 \leq i \leq m$, v_i has order σ_i. Also, σ_i must be odd for all i. Then for $0 \leq j < \frac{n}{2}$ find the unique integers $j_0, j_1, \ldots, j_m$ described in Lemma 4.1.3 such that

$$j \equiv j_0 (\text{mod } \sigma_1\sigma_2\cdots\sigma_m)$$

$$j_0 = j_1 + j_2\sigma_1 + j_3\sigma_1\sigma_2 + \cdots + j_m\sigma_1\cdots\sigma_{m-1}$$

$$\text{and } 0 \leq j_i < \sigma_i \quad \text{for } 1 \leq i \leq m$$

If i is of the form $i = 2j + 1$ for $0 \leq j < \frac{n}{2}$, define b_i to be

$$b_i = c_0^{-j} c_1^{-j_1} c_2^{-j_2} \cdots c_m^{-j_m}$$

where $j_1, j_2, \ldots, j_m$ are the integers we calculated at the beginning of the proof. If i is even, $i = 2j + 2$ for $0 \leq j < \frac{n}{2}$, then define b_i as follows

$$b_i = c_0^{j+1} c_1^{j_1+1} c_2^{j_2+1} \cdots c_m^{j_m+1}.$$

To show the elements $b_1, b_2, \ldots, b_n$ are all distinct assume for some α, β that $b_\alpha = b_\beta$. First, assume α and β are odd. So $\alpha = 2s + 1, \beta = 2t + 1$, and b_α, b_β are component wise equal. This leads to the equations

$$\begin{aligned} s &\equiv t \pmod{2^k} \\ s_1 &\equiv t_1 \pmod{\sigma_1} \\ &\vdots \\ s_m &\equiv t_m \pmod{\sigma_m} \end{aligned}$$

From the inequality $0 \leq s_i, t_i \leq \sigma_i$ we can conclude that for $1 \leq i \leq m$, $s_i = t_i$. Thus $s_0 = t_0$, which implies $s \equiv t \pmod{\sigma_1\sigma_2 \cdots \sigma_m}$. Combining this with the first equation directly above we can say that $s \equiv t \pmod{n}$, thus implying $s = t$ since both must be less than n. The argument to show that for even α, β is similar so we may state also that $b_{2s+2} = b_{2t+2}$ implies $s = t$. Now, consider the case where $b_{2s+1} = b_{st+2}$ for some s, t. Again comparing components (specifically their exponents) we have the following equations (note we have moved all variables to one side, explicitly $-s \equiv t + 1 \bmod 2^k$)

$$\begin{aligned} s + t + 1 &\equiv 0 \bmod 2^k \\ s_1 + t_1 + 1 &\equiv 0 \bmod \sigma_1 \\ &\vdots \\ s_m + t_m + 1 &\equiv 0 \bmod \sigma_m \end{aligned}$$

Now, s_i and t_i are integers and since both are strictly less than σ_i we can say that $s_i + t_i \leq 2(\sigma_i - 1)$. Thus we have the inequality

$$s_i + t_i + 1 \leq 2(\sigma_i - 1) + 1 < 2\sigma_i$$

. This implies that $s_i + t_i + 1 = \sigma_i$ for $1 \leq i \leq m$. So we have a system of equations

$$\begin{aligned} s_1 + t_1 + 1 &= \sigma_1 \\ s_2 + t_2 + 1 &= \sigma_2 \\ &\vdots \\ s_m + t_m + 1 &= \sigma_m \end{aligned}$$

We can eliminate most of the variables by multiplying each equation by a portion of the product $\sigma_1\sigma_2\cdots\sigma_m$. Specifically, multiply the $(i+1)'$st equation by $\sigma_1\sigma_2\cdots\sigma_i$ starting with $i = 1$ and ending with $i = m - 1$. The result is

$$\begin{aligned} s_1 + t_1 + 1 &= \sigma_1 \\ \sigma_1(s_2 + t_2 + 1) &= \sigma_1\sigma_2 \\ \sigma_1\sigma_2(s_3 + t_3 + 1) &= \sigma_1\sigma_2\sigma_3 \\ &\vdots \\ \sigma_1\sigma_2\cdots\sigma_{m-1}(s_m + t_m + 1) &= \sigma_1\sigma_2\cdots\sigma_m \end{aligned}$$

If we add all the equations up and combine like terms then we have

$$s_0 + t_0 + 1 = \sigma_1\sigma_2\cdots\sigma_m$$

which implies $s + t + 1 \equiv 0 \pmod{\sigma_1\sigma_2\cdots\sigma_m}$. When we combine this with $s + t + 1 \equiv 0 \pmod{2^k}$ from above, we get that $s + t + 1 \equiv 0 \pmod{n}$. But this

cannot be since s, t are both less than $\frac{n}{2}$ which means that $s+v+1 \leq n-1 < n$. Thus the even terms are distinct from the odd terms and so the b_i are all distinct.

Finally, we must show that the sequence a $= (a_1, a_2, \ldots, a_n)$ are all distinct. The process is the same as for the sequence **b**: compare the coefficients and work mod the σ_i. The case where an odd indexed a_s may equal an even indexed a_t can be handled by noting that for $i = 2j + 2$ with $0 \leq j < \frac{n}{2}$, a_i has exponent $2j + 1$ in the exponent of c_0 while for $i = 2j + 1$ with same bounds on j, a_i has $-2j$ as the exponent of c_0. Clearly, they cannot be equal even if all other components are equal (which is possible). We have created the sequence $(b_1, b_2, \ldots, b_n)$ and corresponding $(a_1, a_2, \ldots, a_n)$ and shown that both have distinct elements. Thus we conclude that G is sequenceable. □

As an example, we sequence just one more group with our new formula.

Example 4.9. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. Use the generating set

$$\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$$

with $c_0 = (1, 0, 0), c_1 = (0, 1, 0), c_2 = (0, 0, 1)$, which have orders 2,3,3 respectively. Note that for $0 \leq j < 9$, $j = j_0$, so the triple of integers (j_0, j_1, j_2) we

need for the exponents on (c_0, c_1, c_2) are given by

$$\begin{aligned} j_0 &= j_1 + j_2(\sigma_1) \\ 0 &= 0 + 0(3) \\ 1 &= 1 + 0(3) \\ 2 &= 2 + 0(3) \\ 3 &= 0 + 1(3) \\ 4 &= 1 + 1(3) \\ 5 &= 2 + 1(3) \\ 6 &= 0 + 2(3) \\ 7 &= 1 + 2(3) \\ 8 &= 2 + 2(3) \end{aligned}$$

Form the sequence **b** first by using

$$b_i = \begin{cases} c_0^{-j} + c_1^{-j_1} + c_2^{-j_2} & \text{if } i = 2j+1 \\ c_0^{j+1} + c_1^{j_1+1} + c_2^{j_2+1} & \text{if } i = 2j+2 \end{cases}$$

For example, if $j = 4$ then $(j_0, j_1, j_2) = (4, 1, 1)$ and for $i = 9 = 2j+1$ we have

$$\begin{aligned} b_9 &= c_0^{-j} + c_1^{-j_1} + c_2^{-j_2} \\ &= (1,0,0)^{-4} + (0,1,0)^{-1} + (0,0,1)^{-1} \\ &= (4,0,0)^{-1} + (0,2,0) + (0,0,2) \\ &= (0,0,0) + (0,2,0) + (0,0,2) \\ &= (0,2,2) \end{aligned}$$

The rest of the sequence **b** is calculated similarly and is given below

$$\mathbf{b} = \Big\{(0,0,0),(1,1,1),(1,2,0),(0,2,1),(0,1,0),(1,0,1),$$
$$(1,0,2),(0,1,2),(0,2,2),(1,2,2),(1,1,2),(0,0,2),$$
$$(0,0,1),(1,1,0),(1,2,1),(0,2,0),(0,1,1),(1,0,0)\Big\}$$

and the corresponding sequence **a** can be calculated using $a_i = b_{i-1}^{-1} b_i$

$$\mathbf{a} = \Big\{(0,0,0),(1,1,1),(0,1,2),(1,0,1),(0,2,2),(1,2,1),$$
$$(0,0,1),(1,1,0),(0,1,0),(1,0,0),(0,2,0),(1,2,0),$$
$$(0,0,2),(1,1,2),(0,1,1),(1,0,2),(0,2,1),(1,2,2),\Big\}$$

Let's take just a moment to look at the sequencing **a** we have just created. If we list the elements of **a** as

$$\mathbf{a} = \{e, a_2, \ldots, a_n, \ldots, a_{2n}\}$$

notice that the unique order 2 element, $(1,0,0)$ is equal to a_9 and that for $1 \leq i \leq 8$, we have $a_{n+1+i} = (a_{n+1-i})^{-1}$, which is to say that each element is positioned symmetrically from its inverse with the order 2 element in the middle. This type of sequencing will be important later in the classification of sequenceable groups, so we give it a name.

Definition 4.10. *[2]* Suppose G is a group of order $2n$ with unique element g^* of order 2. A sequencing $(e, a_2, \ldots, a_n, \ldots, a_{2n})$ will be called a **symmetric sequencing** if and only if $a_n = g^*$ and for all $1 \leq i \leq n-1$,
$a_{n+1+i} = (a_{n+1-i})^{-1}$.

Although Gordon was not able to determine which odd ordered groups were sequenceable (the first non-abelian group of odd order sequenced by

Mendelsohn [22] in 1966), he did find that if a finite group G of odd order were sequenceable, then the group $G \times \mathbb{Z}_2$ had a symmetric sequencing. Much of the work on sequencing odd ordered groups and the concept of 2-sequencings can be seen as generalizations of the following result.

Theorem 4.11. *[2]* If G is a sequenceable group of odd order n then $G \times \mathbb{Z}_2$ has a symmetric sequencing.

Proof: The proof can be found in [2], p.23 Theorem 4.

Recall that Gordon was working with certain types of Latin squares when this problem first arose. The following subsection establishes this connection between sequenceable groups and Latin squares.

4.1.1 Latin Squares

Consider the following Latin square:

Figure 4.4: Latin Square of size 4

1	2	3	4
2	4	1	3
3	1	4	2
4	3	2	1

Now, if we take any ordered pair (x, y) with $x \neq y$, then (x, y) occurs as a pair of consecutive entries (in either orders) in some row of this square. Likewise, note that the pair (x, y) occurs as a pair of consecutive entries in some column of the square as well.

Definition 4.12. A **latin square** [23] or order n is an $n \times n$ array defined on a set X with n elements such that every element of X appears once in each

row and once in each column. The notation $L = (l_{ij})$ represents a Latin square L with l_{ij} in the ith row and jth column.

A Latin square will be called **row complete** if it satisfies the property listed above, namely that any ordered pair of distinct elements occur as a pair of consecutive horizontal entries $l_{ij},\ l_{i+1,j}$ exactly once in some row of the square. A Latin square is **column complete** if any ordered pair of elements (x, y), $x \neq y$ occurs exactly once in each order in consecutive vertical entries can find the same occurrence in some column of the square. A Latin square that is both row and column complete is called a complete Latin square.

As mentioned earlier, Latin squares are useful in the design of experiments in which it is desired to investigate the interaction of nearest neighbors. The idea being that you test all possible interactions without duplicates. Gordon proved the following theorem which provides a method for constructing complete Latin squares from sequenceable grous.

Theorem 4.13. *[13]* Let G be a sequenceable group and let $(a_1, a_2, \ldots, a_n)$ be a sequencing with corresponding distinct partial products $(b_1, b_2, \ldots, b_n)$. Then $L = (l_{ij})$, where $l_{ij} = b_i^{-1} b_j$ for $1 \leq i, j \leq n$, is a complete Latin square.

Proof: Suppose $l_{ij} = l_{ik}$ for some $1 \leq i, j, k \leq n$. Then

$$b_i^{-1} b_j = b_i^{-1} b_k$$

, giving $a_j = a_k$. Therefore $j = k$ and L has no repeated entries in any row. Similarly, L has no repeated entries in any column. Therefore L is a Latin square.

To show that L is vertically complete suppose

$$l_{xy} = l_{uv}, \text{ and,}$$

$$l_{x+1,y} = l_{u+1,v}$$

We must show that $x = u$ and $y = v$. From the definition of l_{ij} we have

$$b_x^{-1} b_y = b_u^{-1} b_v, \text{ and,}$$
$$b_{x+1}^{-1} b_y = b_{u+1}^{-1} b_v$$

Invert both sides of the first equation to get $b_y^{-1} b_x = b_v^{-1} b_u$. Multiplying this on the right of the the second equation yields

$$(b_{x+1}^{-1} b_y)(b_y^{-1} b_x) \;=\; (b_{u+1}^{-1} b_v)(b_v^{-1} b_u)$$

which simplifies to $b_{x+1}^{-1} b_x = b_{u+1}^{-1} b_u$. Now, by the definition of b_i the above simplifies to $a_{x+1} = a_{u+1}$, thus $x = u$. Substituting this into the first equation gives that $b_y = b_v$, thus $y = v$. To show row complete start with the same setup except increment y and v instead of x and u and after inverting the first equation multiply it on the left of the second. □

So, Gordon's proof gives a method of constructing complete Latin squares of order n for any even n. Before moving on, here are a few examples from the groups we have sequenced. We already have the Latin square of order 4, but the one based on a group sequencing would look something like this

Example 4.14. Let $G = \mathbb{Z}_4$. Then $\mathbf{a} = (0, 3, 2, 1)$ is a sequencing of G with partial products $(0, 3, 1, 2)$. The corresponding complete Latin square L is given in the following figure.

$$\begin{array}{cccc} 0 & 3 & 1 & 2 \\ 1 & 0 & 2 & 3 \\ 3 & 2 & 0 & 1 \\ 2 & 1 & 3 & 0 \end{array}$$

Example 4.15. Let $G = \mathbb{Z}_{12}$ Then the sequence $\mathbf{a}$ of G with corresponding partial products $\mathbf{b}$ and also the sequence $\mathbf{b}^{-1}$ where the elements in $\mathbf{b}^{-1}$ are

the inverses of those in $\mathbf{b}$.

$$\mathbf{a} = (0, 1, 10, 3, 8, 5, 6, 7, 4, 9, 2, 11)$$

$$\mathbf{b} = (0, 1, 11, 2, 10, 3, 9, 4, 8, 5, 7, 6)$$

$$\mathbf{b}^{-1} = (0, 11, 1, 10, 2, 9, 3, 8, 4, 7, 5, 6)$$

The corresponding complete Latin square given by $l_{ij} = b_i^{-1} b_j$ is given the following figure.

Figure 4.5: Latin square of size 12

0	1	11	2	10	3	9	4	8	5	7	6
11	0	10	1	9	2	8	3	7	4	6	5
1	2	0	3	11	4	10	5	9	6	8	7
10	11	9	0	8	1	7	2	6	3	5	4
2	3	1	4	0	5	11	6	10	7	9	8
9	10	8	11	7	0	6	1	5	2	4	3
3	4	2	5	1	6	0	7	11	8	10	9
8	9	7	10	6	11	5	0	4	1	3	2
4	5	3	6	2	7	1	8	0	9	11	10
7	8	6	9	5	10	4	11	3	0	2	1
5	6	4	7	3	8	2	9	1	10	0	11
6	7	5	8	4	9	3	10	2	11	1	0

There is also a connection between sequenceable groups and graph theory. This connection is made through complete Latin squares. In graph theory, a *graph* is a set (V, E) where V is a representation of a set of objects, usually denoted as *vertices*, and E is a set of links between the vertices, usually called *edges*. A complete graph is one in which every pair of distinct vertices

is connected by a unique edge. A complete directed graph is a complete graph with the added condition that the edges are directed (usually represented by arrows instead of straight lines), and this denotes that a path is not able to be traveled in both directions. The complete directed graph on n vertices is usually denoted K_n.

Mendelsohn [22] showed that if there is a row-complete Latin square of order N then the complete directed graph on n vertices can be decomposed into n disjoint Hamiltonian paths. A **Hamiltonian path** is a path which visits each vertex exactly once. Two paths are said to be *disjoint* if they have no edges in common.

The method for creating the n disjoint paths is to start by associating each symbol in the set X of the Latin square with a vertex of the graph. Then take each row of the row complete Latin square and associate each consecutive pair of entries in the square with a directed edge that connects them in the graph. Since we choose elements of our path from a Latin square the paths are Hamiltonian (we visit each vertex exactly once in a path). Since the Latin square is row complete each ordered pair (x, y) is of vertices occurs exactly once in horizontal cells, thus no edge is repeated and the paths are disjoint. A complete Latin square of order 4 is given in Example 4.14. Fig.5.5 gives the complete directed graph, K_4 and Fig.5.6 gives the decomposition of K_4 into disjoint Hamiltonian paths.

Figure 4.6: K_4

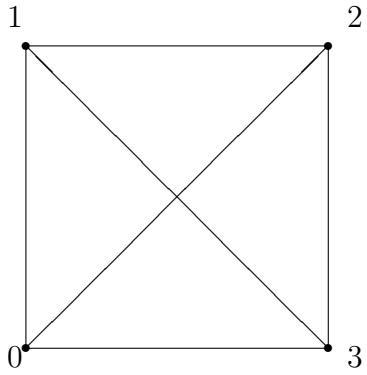
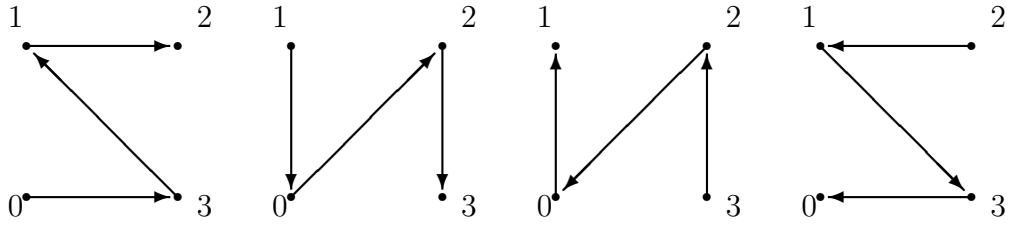


Figure 4.7: Decomposition of K_4 into Hamiltonian Paths



We have seen the practical applications for investigating which groups are sequenceable. Gordon determined which abelian groups admitted sequencings, and this provided a method for constructing complete Latin squares of order $2n$. But the question still remains, are the only groups sequenceable binary abelian groups? Gordon devoted some time to this question and by mapping G onto the Abelian group G/C, where C is commutator subgroup (the normal subgroup generated by all elements of the form $x^{-1}y^{-1}xy$ for $x, y \in G$), was able to find a sequencing for the non-abelian group of order 10 (D_5) as well as show that D_3 and D_4 and the quaternions, Q, were not sequenceable. However, further results on the subject would remain unknown for the next few years. in 1968 Mendelsohn [22] sequenced the first non-abelian group of odd order, 21, and this would set in motion the classification of sequenceable groups. As our knowledge of the classification of groups is somewhat limited,

we will seek to find the answers to just two questions at present: (1) Other than D_5, what, if any, dihedral groups are sequenceable? (2) If we relax the condition that the sequence of group elements be all distinct while keeping the distinct partial products condition, what results can be obtained? The first questioon is the subject of the next section. We will return to the second question at the end of the chapter.

4.2 Sequencing Dihedral Groups

Mentioned in the last section was the idea that we can gain insight into whether or not a group is sequenceable by examining the factor group G/C where C is the commutator subgroup of G. To see how this process works, we have the following definition.

Definition 4.16. Let G be a group. Then an element $aba^{-1}b^{-1} \in G$ for $a, b \in G$ is called a **commutator of the group**.

Theorem 4.17. Let G be a group. The set of all commutators of G generate a subgroup C, called the **commutator subgroup** and denoted $[G, G]$. Furthermore, C is a normal subgroup of G and in general if $N \trianglelefteq \mathrm{G}$, then G/N is abelian if and only if $C \leq N$.

Proof: There are a few parts to this theorem. First, that the set of $[a, b]$ for $a, b \in$ generates a subgroup of G is clear. Of course, the product of two commutators need not be a commutator, but it will be contained in the subgroup generated by them. To show C is normal, let $g \in G$ and $x \in C$. Then under the action of conjugation by g, we must have $gxg^{-1} \in C$. Since we know the form of all elements in C are products of commutator, it will suffice

to show that $g(aba^{-1}b^{-1})g^{-1} \in C$ for all $g, a, b \in G$. Observe,

$$\begin{aligned} g^{-1}[a,b]g &= g^{-1}(aba^{-1}b^{-1})g \\ &= (g^{-1}aba^{-1})(gb^{-1}bg^{-1})(b^{-1}g) \\ &= \big((g^{-1}a)b(a^{-1}g)b^{-1}\big)(bg^{-1}b^{-1}g) \\ &= \big[(g^{-1}a)b(g^{-1}a)^{-1}b^{-1}\big](bg^{-1}b^{-1}g) \\ &= [g^{-1}ag, g^{-1}bg] \end{aligned}$$

Thus $g(aba^{-1}b^{-1})g^{-1} \in C$ and C is normal in G.

Now, form the factor group G/C and let $\overline{a}, \overline{b} \in G/C$. Then

$$\begin{aligned} (aC)(bC) &= (ab)C \\ &= ab(b^{-1}a^{-1}ba)C \quad \text{since } b^{-1}a^{-1}ba \mapsto e \; in G/C \\ &= (ba)C \end{aligned}$$

Thus G/C is abelian. Finally, if G/N is abelian for $N \trianglelefteq G$, then

$$\begin{aligned} a^{-1}Nb^{-1}N &= b^{-1}Na^{-1}N \\ \Rightarrow N &= aba^{-1}b^{-1}N \\ \Rightarrow C &\leq N \end{aligned}$$

On the other hand if $C \leq N$, then

$$\begin{aligned} aNbN &= (ab)N \\ &= ab(b^{-1}a^{-1}ba)N \\ &= (ba)N \end{aligned}$$

and G/N is abelian. □

The commutator subgroup C has another name, the **derived group**, denoted G'. The derived group is a good measure of how 'abelian' G is since if G is abelian $G' = \{e\}$. Seen in this light, it makes sense that G/C is abelian.

Lemma 4.2.1. Suppose G is a sequenceable with sequencing $(a_1, \ldots, a_n)$ and distinct partial products $(b_1, \ldots, b_n)$. Let H be a normal subgroup of G and let

$$\phi : G \longrightarrow G/H$$

be the natural homomorphism defined by $\phi(g) = \overline{g} = gH$. Write $G/H = \{x_1, \ldots, x_r\}$, where $r = \frac{n}{h}$ ($|H| = h$). Then each x_i, for $1 \leq i \leq r$, must occur h times in both of the sequences $(\overline{a_1}, \ldots, \overline{a_n})$ and $(\overline{b_1}, \ldots, \overline{b_n})$.

Proof: Each $a_i \in G$ gets mapped to a specific $x_i \in G/H$. Thus is $\phi(a_i) = \overline{a_i} = x_j$ for $1 \leq i \leq n$ and $1 \leq j \leq r$, then $\overline{a_i}$ is replaced by x_j in the sequence $(\overline{a_1}, \ldots, \overline{a_n})$. The same reasoning applies to the sequence of mapped partial products. Since there are h elements in G represented by each x_j, and each x_j is distinct, there must be $n = rh$ replacements, h of which are x_j for $1 \leq j \leq r$. □

Essentially what is happening is that if we take a sequencing of G and project it down onto a specific factor group then we can simplify the original sequencing. The newly created sequences are called a quotient sequencing.

Definition 4.18. Let G be a group of order n and let $H \trianglelefteq G$. Let $G/H = \{x_i, \ldots, x_r\}$ with $r = \frac{n}{h}$. A sequence α of length n conisting of elements of G/H is called a **quotient sequencing** of G/H if each x_i, for $1 \leq i \leq r$, occurs h times in both α and $P(\alpha)$, where $P(\alpha)$ denotes the sequence of partial products of α.

With this definition we can restate the previous lemma as the image under ϕ of a sequencing of G is a quotient sequencing of G/H. This is a nice result; it allows us to work within the factor group G/H and create quotient sequencings that have the potential to be projected back to sequencings of G.

The benefit is two-fold since if we cannot find a quotient sequencing of G/H, then G cannot posses a sequencing. Secondly, if we can find a suitable quotient sequencing it is easy to check whether it projects back or not. An example of both follows.

Example 4.19. Let $G = S_3$. S_3 has elements

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Take $H = \{e, (123), (132)\}$. Then $H \trianglelefteq G$. Form the factor group

$$S_3/H \cong \{0, x\},$$

with $0 = \{e, (123), (132)\}$ and $x = \{(12), (13), (23)\}$. A quotient sequencing of S_3/H must have three $0's$ and three $x's$ in each of its sequence and partial product sequence. Additionally, if S_3 is to have a sequencing, we must have a 0 as the first element of both sequences. The task is then to find all possible sequences of $0's$ and $x's$ that could satisfy these conditions. We may use automorphisms of S_3 as well as examining the configuration of possible sequences to eliminate those possible quotient sequences that cannot project back. For example, the sequence $000xxx$ cannot be a sequence of S_3 since the first three $0's$ would produce the identity as the the third element of the partial products. Using similar arguments Friedlander [12] determined there are four distinct possibilities for quotient sequencings of S_3/H. They are

$$0, 0, x, 0, x, x; \quad 0, 0, x, x, x, 0; \quad 0, x, 0, x, 0, x; \quad 0, x, x, 0, x, 0$$

We must therefore take each of these sequences and project them back to S_3. Lets show how this would work for the first quotient sequencing in the list. We must pick the first 0 to be the identity e. We may pick either (123) or (132) since an automorphism on S_3 can take $(123) \mapsto (132)$. Project the second 0

back to (123). For similar reasons, we can pick the first x to be (12). So, we have the sequence $\{e, (123), (12), \}$ thus far. The fourth term must be (132), and up to this point the partial products in S_3 will be $\{e, (123), (23), (13)\}$. Now, when we add the fifth term, whether it be (13) or (23) we repeat a partial product element (either e or (123)). Thus this particular quotient sequence cannot project back to a sequencing of S_3. A similar argument for the remaining three quotient sequencings demonstrates that, according to our previous lemma, S_3 is not sequenceable.

This technique of quotient mapping and then projecting back to the group is useful when the factor group is small. Specifically, if we let $G = D_n$, for odd n, then we can use the commutator subgroup described above and the resulting factor group will be isomorphic to $\mathbb{Z}_2$, as small as we can get (non-trivially). The next example shows this relationship.

Example 4.20. Let $G = D_n$ and use the presentation

$$D_n = \{a^2 = b^n = e \text{ and } ba = ab^{-1}\}$$

When n is odd, the commutator subgroup is the group of rotations, $\langle b \rangle$. To see this, take any $[a, b] \in D_n$. Then, using that $b^i a^j = a^j b^{i \cdot (-1^j)}$ for $j \in 0, 1$ and $0 \leq i < n$, we have

$$\begin{aligned} a^j b^i a^{-j} b^{-i} &= a^j (b^i a^{-j}) b^{-i} \\ &= a^j (a^{-j} b^{i \cdot (-1)^{-j}}) b^{-i} \\ &= (a^j a^{-j}) b^{i \cdot (-1)^j} b^{-i} \\ &= b^{i \cdot (-1^j)} b^{-1} \end{aligned}$$

Now, if $j = 0$, then we get that $a^j b^i a^{-1} b^{-i} = e$. If $j = 1$, we get$[a, b] = b^{-2i}$. Thus we have that $[G, G] \subseteq \langle b^2 \rangle$. Forming the factor group $D_n / \langle b^2 \rangle$, we see

that $a^2 = 1$ and also $b^2 = 1$. Coupling this with $b^n = 1$ forces $\langle b^2 \rangle = \langle b \rangle$ which forces the factor group to be isomorphic to $\mathbb{Z}_2$. Additionally, when n is odd, the above computations imply $\langle b^2 \rangle \subseteq [G, G]$. Thus $\langle b \rangle = [G, G]$.

In the case where n is even, we don't quite get all of the rotations and the factor group $D_n/[G, G]$ is isomorphic to the Klien 4 group. This can be seen since we have still $a^2 = 1$, $b^2 = 1$, but $b^n = 1$ doesn't force $\langle b^2 \rangle = \langle b \rangle$, because n is even. This is the main reason why for even n we don't use the commutator subgroup to form our quotient mapping; you get 4 different elements in the quotient sequencing instead of just 2. Thus, we can analyze quotient mappings for D_n by first separating them into two classes based on whether n is odd or even. We treat the case where n is odd here, and the case where n is even can be found in [18]. If we let $n = 2k + 1$, then we can form the factor group

$$D_n/D'_n = \{0, x\}.$$

where reflections are sent to x and all rotations sent to 0. An example using D_5 follows.

Example 4.21. Let $G = D_5$. The factor group $D_5/\langle b \rangle$ was hand checked by Friedlander [12] to have 36 different quotient sequencings with 0 as a first element. Of these, nine were reported to project back to sequencings of D_5 and seven of those projected back to two different sequences, i.e inequivalent under automorphism. Hence there are a total of 16 sequencings of D_5. One of quotient sequences that were found to project back to a sequencing of D_5 was of the form

$$\{0, 0, 0, x, x, x, x, x, 0, 0\}$$

This quotient sequence, which splits essentially drops the reflections in the middle of the rotations has been seen to generalize to D_n for $n = 4k + 1$

[12]. The resulting quotient sequence in this case is

$$\underbrace{0,0,\ldots,0}_{k+1},\underbrace{x,x,\ldots,x}_{2k+1},\underbrace{0,0,\ldots,0}_{k} \tag{4.1}$$

with the sequence of partial products being

$$\underbrace{0,0,\ldots,0}_{k+1},\underbrace{x,0,x,0\ldots,x}_{2k+1},\underbrace{x,x,\ldots,x}_{k} \tag{4.2}$$

If we examine the quotient sequence in Eq. 4.1 we see it has the form in D_n, after projection,

$$\left\{b^{\alpha_1},b^{\alpha_2},\ldots,b^{\alpha_{k+1}},ab^{\beta_1},ab^{\beta_2},\ldots,ab^{\beta_{2k+1}},b^{\gamma_1},\ldots,b^{\gamma_k}\right\} \tag{4.3}$$

with the sequence of partial products being

$$\begin{aligned}\Big\{b^{\alpha_1},b^{\alpha_1+\alpha_2},\ldots,b^{\alpha_{S_\alpha}},ab^{\beta_1-S_\alpha},ab^{\beta_2-\beta_1+S_\alpha},ab^{\beta_3-\beta_2+\beta_1-S_\alpha},\\ ab^{\beta_4-\beta_3+\beta_2-\beta_1+S_\alpha}\ldots,ab^{S_\beta-S_\alpha},b^{S_\beta-S_\alpha+\gamma_1},\ldots,b^{S_\beta-S_\alpha+S_\gamma}\Big\}\end{aligned} \tag{4.4}$$

where the α,β,γ are all integers taken mod n and $S_\alpha=\alpha_1+\alpha_2+\cdots+\alpha_{k+1}$, S_β is the sum of the β_i with alternating signs starting with β_1 positive, and S_γ is as S_α. If we examine this sequence closely then the following conditions must hold

1. The α_i and γ_j for $1\leq i\leq k+1$ and $1\leq j\leq k$ must all be distinct mod n.

2. The β_i for $1\leq i\leq 2k+1$ must be distinct mod n.

3. Since the product of a rotation and a reflection is a reflection and the product of two reflections is a rotation we know the elements in the product sequence 'swap' back and forth in the middle starting with $ab^{\beta_2-\beta_1+S_\alpha}$, a rotation. Thus we must have $\alpha_1,\alpha_1+\alpha_2,\ldots,S_\alpha,\beta_2-\beta_1+S_\alpha,\beta_4-\beta_3+\beta_2-\beta_1+S_\alpha,\ldots,\beta_{2k}-\beta_{21-1}+\ldots+\beta_2-\beta_1+S_\alpha$ must all be distinct mod n.

4. For entirely analogous reasons the powers on the rotations must be different mod n. These are $\beta_1 - S_\alpha, \beta_3 - \beta_2 + \beta_1 - S_\alpha, \ldots, S_\beta - S_\alpha, S_\beta - S_\alpha + \gamma_1, \ldots, S_\beta - S_\alpha + S_\gamma$.

To simplify the notation somewhat we can create an indexing set for the different partial sums of β_i. Let $\delta = \{\delta_1, \ldots, \delta_k\}$ and $\epsilon = \{\epsilon_0, \ldots, \epsilon_k\}$, each of length k and $k+1$, respectively, and define δ_i, ϵ_i as follows

$$\begin{cases} \delta_i = \beta_{2i} - \beta_{2i-1} & 1 \leq i \leq k \\ \epsilon_0 = \beta_1 - S_\alpha & \\ \epsilon_i = \beta_{2i+1} - \beta_{2i} & 1 \leq i \leq k \end{cases} \tag{4.5}$$

Using the sets δ and ϵ we can account for the fact that in condition (3) above, the partial sums of β can be broken up into pairs and likewise for ϵ in condition (4).

Now, if we let (α, δ) denote the sequence

$$\{\alpha_1, \ldots, \alpha_{k+1}, \delta_1, \ldots, \delta_k\}$$

then condition (3) can be restated as $P(\alpha, \delta)$, the partial sums of (α, δ) are distinct mod n. Likewise we can restate condition (4) as $P(\epsilon, \gamma)$ are distinct mod n. We can use back substitution to solve for the β_i in terms of δ and ϵ. If we let $(\epsilon \wedge \delta)$ denote the sequence $\{\epsilon, \delta_1, \epsilon_1, \ldots, \delta_k, \epsilon_k\}$, then condition (2) is restated as $P(\epsilon \wedge \delta)$ must be distinct mod n.

These four conditions provide sufficient conditions for D_n, $n = 2k+1$ to be sequenceable. We state this as a theorem.

Theorem 4.22. [12] Let G be the dihedral group of order $2n$, with $n = 2k+1$. If there exists sequences of integers $\alpha, \gamma, \delta, \epsilon$ of lengths $k+1, k, k, k+1$ respectively satisfying the (modified) conditions above then G is sequenceable.

So, from here the search is on for odd n such that we can create these sets of integers satisfying the above conditions. In 1976, Anderson [2] showed that D_p was sequenceable if p was an odd prime with a primitive root r such that $3r \equiv -1 \mod p$. Recall a primitive root of p is a generator of the cyclic group $\mathbb{Z}_p \setminus 0$ under multiplication. In that same year, Friedlander [12] proved that if p was a prime congruent to 1 mod 4, then D_p was sequenceable. Although the details of the proof are beyond the scope of this thesis, we can state the result and give a outline of the proof.

Theorem 4.23. [12] If G is the dihedral group of order $2p$, where p is a prime congruent to 1 mod 4, $p \equiv 1 \pmod 4$, then G is sequenceable.

Proof: (**Outline**) The idea of the proof is to choose arithmetic progressions for the sequences $\alpha, \gamma, \delta, \epsilon$. Then it can be shown that one obtains quadratic progressions for the sequence of partial products. Using this one proceeds to use quadratic residues to show no two terms in the sequences can be equal. Before giving the sets chosen we need just a bit of background number theory.

Definition 4.24. Let p be an odd prime. An integer $a > 0$ is a **quadratic residue** of p if it is congruent to a perfect square mod p and is a quadratic non-residue mod p otherwise.

As an example we note that for $p = 5$, 4 is a quadratic residue and for the prime $p = 13$, 3 is a quadratic residue ($3 \equiv 16 \pmod{13}$). Another definition from number theory is that of the Legendre symbol.

Definition 4.25. Let p be a prime and a be any integer. Then the Legendre

symbol is a function of a and p defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue and } a \not\equiv 0 \text{ (mod p)} \\ -1 & \text{if } a \text{ is quadratic non-residue} \\ 0 & \text{if } a \equiv 0 \bmod p \end{cases}$$

The Legendre symbol has many interesting properties in number theory and the reader is encouraged to see [26] for a well delivered thesis on quadratic and cubic reciprocity. One of the results from that paper is Euler's Theorem, which state that for a prime p and $a > 0$ and $(a, p) = 1$ that $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$. This gives a quick check for finding quadratic residues and non-residues. Now we may get back to the proof outline. The sets chosen for $\alpha, \gamma, \delta, \epsilon$ are

$$\alpha = \{0, 2, 4, \ldots, 2k\}$$

$$\gamma = \{1, 3, 5, \ldots, 2k-1\}$$

$$\delta = \{-a, -3a, -5a, \ldots, -(2k-1)a\}$$

$$\epsilon = \{0, 2a, 4a, \ldots, 2ka\}$$

where the Legendre symbol $\left(\frac{a}{n}\right) = -1$. Condition (1) is verified since the integers run through $[0, 2k]$ without repeats. The verification of the other conditions are made using results about the congruence of p mod 4 and the Legendre symbol. The proof is elegant and establishes a method by which future sequencers would find infinitely many other sequenceable D_n. Anderson [3] would later use a computer search program to find all sequenceable D_n for $5 \leq n \leq 50$. Using these results, Isbell [18] proved that D_n was sequenceable for $n \not\equiv 0$ (mod 4), except D_3. Isbell's proofs are constructive and care should be taken to do a few examples before examining the general case. In 1997 Li [27] completed the classification of sequenceable dihedral groups by sequencing

D_n where $\equiv 0 \pmod 4$, $n \neq 4$. As examples, we give sequencings for D_n for $n = 5, 13$ using Friedlander's method and D_{34} using Isbell's formulas.

Example 4.26. Let $G = D_5$. G has representation

$$G = \{\langle a, b\rangle : \ a^2 = e = b^5, \ ab = b^{-1}a\}$$

. We take $p = 5$, and $k = 2$. Using Euler's formulas we find

$$\left(\frac{2}{5}\right) = 2^{(5-1)/2} \equiv -1 \mod 5$$

So we may take $a = 2$. Then forming our integer sets we set

$$\alpha = \{0, 2, 4\}$$

$$\gamma = \{1, 3, \}$$

$$\delta = \{3, 4\}$$

$$\epsilon = \{0, 4, 3\}$$

Remember to reduce mod 5 each time. Next, we use the ϵ_i, δ_j to determine the $\beta' s$. Working forwards we see that

$$\epsilon_0 = \beta_1 - S_\alpha$$

$$0 = \beta_1 - 6 \Rightarrow \beta_1 = 6 \equiv 1$$

$$\delta_1 = \beta_2 - \beta_1$$

$$3 = \beta_2 - 1 \Rightarrow \beta_2 = 4$$

$$\epsilon_1 = \beta_3 - \beta_2$$

$$4 = \beta_3 - 4 \Rightarrow \beta_3 = 8 \equiv 3$$

$$\delta_2 = \beta_4 - \beta_3$$

$$4 = \beta_4 - 3 \Rightarrow \beta_4 = 7 \equiv 2$$

$$\epsilon_2 = \beta_5 - \beta_4$$

$$3 = \beta_5 - 2 \Rightarrow \beta_5 = 5 \equiv 0$$

Hence we have the following sets that will be the exponents on a, b

$$\alpha = \{0, 2, 4\}$$

$$\beta = \{1, 4, 3, 2, 0\}$$

$$\gamma = \{1, 3, \}$$

And thus a sequence for D_5 will be

$$\left\{e, b^2, b^4, ab, ab^4, ab^3, ab^2, a, b, b^3\right\}$$

with corresponding partial products

$$\left\{e, b^2, b, ab, b^4, ab^4, b^3, ab^2, ab^3, ab\right\}$$

Our next example will be D_{13}. The process to determine the specific $\beta's$ is the same and will therefore be skipped.

Example 4.27. Let $G = D_{13}$. G has presentation

$$G = \{\langle a, b\rangle : \ a^2 = e = b^{13}, \ ab = b^{-1}a\}.$$

We take $p = 13$, $k = 6$ and

$$\left(\frac{2}{13}\right) = 2^{(13-1)/2} \equiv -1 \mod 13.$$

Thus we may use $a = 2$ as before. Working mod 13 we use Theorem 4.23 to form the following sets

$$\alpha = \{0, 2, 4, 6, 8, 10, 12\}$$

$$\gamma = \{1, 3, 5, 7, 9, 11\}$$

$$\delta = \{11, 7, 3, 12, 8, 4\}$$

$$\epsilon = \{0, 4, 8, 12, 3, 7, 11\}$$

Next we use Eq.4.5 to solve for β_i, for $1 \leq i \leq 13$. Each β_i is determined recursively.

$$\beta = \{3, 1, 5, 12, 7, 10, 9, 8, 11, 6, 0, 4, 2\}$$

Now, with the α, β, γ defined we can give a sequencing of D_{13} as

$$\big\{e, b^2, b^4, b^6, b^8, b^{10}, b^{12}, ab^3, ab, ab^5, ab^{12}, ab^7, ab^{10},$$
$$ab^9, ab^8, ab^{11}, ab^6, a, ab^4, ab^2, b, b^3, b^5, b^7, b^9, b^{11}\big\}$$

with the corresponding partial products being

$$\big\{e, b^2, b^6, b^{12}, b^7, b^4, b^3, a, b, ab^4, b^8, ab^{12}, b^{11},$$
$$ab^{11}, b^{10}, ab, b^5, ab^8, b^9, ab^6, ab^7, ab^{10}, ab^2, ab^9, ab^5, ab^3\big\}$$

Now, before giving the formulas for Isbell's sequencing of D_n, it must be noted that Isbell used a different representation for the dihedral groups than the one we are familiar with. A short treatment of this type of presentation is given next.

Recall the a presentation for the dihedral group of order $2n$ is given by $D_n = \{\langle x, y\rangle : x^n = y^2 = e \text{ and } xy = yx^{-1}\}$. This definition works well in most cases, but Isbell chose to consider D_n as the set $\mathbb{Z}_n \times \mathbb{Z}_2$ with $(x, 0) \in \mathbb{Z}_n$, $(0, \delta) \in \mathbb{Z}_2$ and multiplication defined by

$$(x, 0)(y, \delta) = (x + y, \delta)$$
$$(x, 1)(y, \delta) = (x - y, 1 + \delta)$$

This definition is consistent with the development of the dihedral groups as the semi-direct product $\mathbb{Z}_n \ltimes \mathbb{Z}_2$ and multiplication given by

$$(x_1, \delta_1)(x_2, \delta_2) = (h_1\delta_1 \cdot x_2, \delta_1\delta_2)$$

where $\delta_1 \cdot x_2$ is the group action of $\mathbb{Z}_2$ on $\mathbb{Z}_n$ within the overall group. Since the only non-trivial action $\mathbb{Z}_2$ is capable of performing is inversion, we get that $\delta_1 \cdot x_2 = x_2^{-1}$. Now, this action is trivial when $\delta = 0$, hence the second multiplication formula in the above equation. The elements $(x, 0)$ represent the rotations, which commute with each other and the elements $(x, 1)$ are the inversions. The difference in choice for which presentation to use is yours; I wanted to give both so the reader would be familiar.

The method Isbell uses is very similar to that of Friedlander, and he splits the constuction of his sequences into five cases. They are $n = 4k + 1$, $n = 8k+7$, $n = 8k+3$,$(k \neq 1, 2, 4)$, and the case $n = 4k+2$ split into whether k is even or odd. As mentioned, the overall structure of the sequencings follow the method of putting all reflections in the middle and separating the rotations to either side in varying intricate ways for D_n, n odd. In the last two cases, the construction changes slightly. In these cases we form the sequence $(e, \beta, \alpha, \delta, \gamma)$ where here e is the identity, β handles the reflections $(x, 1)$, α and γ partition the rotations $(x, 0)$ as before and δ is $(4k + 1, 1)$, which is the reflection of order 2 that mirrors the single rotation of order 2. What should be noted is the order of the sequencings are different than in the method studied above.

We proceed by giving the sequence for β, which nearly mimics that of Friedlander's.

$$\begin{aligned}\beta \quad &= (0,1),(1,1),(2,1),\ldots,(2k-1,1),(4k,1),(2k,1),(2k+1,1),\ldots,\\ &\quad (4k-1,1)\end{aligned}$$

If we were to write this in the notation we are familiar with it would be

$$\beta \;=\; a, ab, ab^2, \ldots, ab^{2k-1}, ab^{4k}, ab^{2k}, ab^{2k+1}, \ldots, ab^{4k-1}$$

Next, we have the construction for the α and γ parts. Note that σ_1 has the

same type of feel that we used to define γ before, excepting the alternating positive negative signs. Likewise with σ_2. What is also different is that we switch the odds to go with γ and the evens to go with α. So, for the following two sequences in $\mathbb{Z}_{4k+2}$

$$\begin{aligned}\sigma_1 &= -3, 5, -7, 9, \ldots, 2k-3, 1-2k, 2k-2, -(2k-3), 2k-5 \ldots, \\ &\quad -5, 3 \\ \sigma_2 &= -2, 4, -6, 8, \ldots, 2k-4, -(2k-2), 1, 2k-1, -1, -(2k-4), \\ &\quad 2k-6, \ldots, -4, 2\end{aligned}$$

set α to be $(2k+2, 0)$ followed by the sequence with σ_1 in the first co-ordinates and 0's in the second, followed by $2k, 0), (2k+1, 0)$. So, we have

$$\begin{aligned}\alpha &= \big\{(2k+2, 0), (-3, 0), (5, 0), (-7, 0), (9, 0), \ldots, (2k-3, 0), (1-2k, 0), \\ &\quad (2k-2, 0), (-(2k-3), 0), (2k-5, 0), \ldots, (-5, 0), (3, 0), \\ &\quad (2k, 0), (2k+1, 0)\big\}\end{aligned}$$

Now, define γ to be the sequence with σ_2 in the first co-ordinates and 0's in the second. Thus we have

$$\begin{aligned}\gamma &= \big\{(-2, 0), (4, 0), (-6, 0), (8, 0), \ldots, (2k-4, 0), (-(1-2k), 0), (1, 0), \\ &\quad (2k-1, 0), (-1, 0), (-(2k-4), 0), (2k-6, 0), \ldots, (-4, 0), (2, 0)\big\}\end{aligned}$$

The case where $n = 4k+2$ and k is odd is handled similarly with only a slight change in the middle of both the σ seqeunces. The reader is encouraged to view these constructions and the proofs of their validity in [18]. To get a good feel for the entire length of the sequence we do an example where $k = 8$ and thus $n = 34$.

Example 4.28. Let $G = D_{34}$. In this example we will use the formulas from above to sequence G. We start with the sequences for β, α, γ . They are

$$\begin{aligned}\beta \quad &= \big\{(0,1),(1,1),(2,1),(3,1),(4,1),(5,1),(6,1),(7,1),(8,1),(9,1),\\ &\quad (10,1),(11,1),(12,1),(13,1),(14,1),(15,1),(32,1),(16,1),\\ &\quad (18,1),(19,1),(20,1),(21,1),(22,1),(23,1),(24,1),(25,1),\\ &\quad (26,1),(27,1),(28,1),(29,1),(30,1),(31,1)\big\}\end{aligned}$$

The sequence for σ_i are given below, note they must be taken mod 34.

$$\begin{aligned}\sigma_1 \quad &= \big\{-3,5,-7,9,-11,13,-15,14,-13,11,-9,7,-5,3\big\}\\ \sigma_2 \quad &= \big\{-2,4,-6,8,-10,12,-14,1,15,-1,-12,10,-8,6,-4,2\big\}\end{aligned}$$

Now we can list the sequences for α and γ. Don't forget the added elements to α.

$$\begin{aligned}\alpha \quad &= \big\{(18,0),(31,0),(5,0),(27,0),(9,0),(22,0),(13,0),(19,0),\\ &\quad (14,0),(21,0),(11,0),(25,0),(7,0),(29,0),(3,0),(16,0),(17,0)\big\}\end{aligned}$$

Finally, we have the sequence for γ is

$$\begin{aligned}\gamma \quad &= \big\{(32,0),(4,0),(28,0),(8,0),(24,0),(10,0),(12,0),(20,0),\\ &\quad (1,0),(15,0),(33,0),(22,0),(10,0),(26,0),(6,0),(30,0),(2,0)\big\}\end{aligned}$$

4.3 Terraces and 2-Sequencings

Recall the second topic we wanted to investigate concerning sequencings: if we keep the condition that partial products must be different while relaxing the condition that the elements that form the sequence need not be distinct, are there meaningful results that can be obtained? To see an example of this, we

bring back the attempt to sequence $\mathbb{Z}_{15}$ from section 4.1. The sequence with associated partial products are

$$\mathbf{a} = \{0, 1, 13, 3, 11, 5, 9, 7, 7, 9, 5, 11, 3, 13, 1\}$$
$$\mathbf{b} = \{0, 1, 14, 2, 13, 3, 12, 4, 11, 5, 10, 6, 9, 7, 8\}$$

Now, the partial products are distinct and the sequence **a** does have some interesting properties. First, it is a sequence of increasing odd integers interlaced with a sequence of decreasing odd integers. Second, if we disregard the identity, we see that **a** is also a palindrome. Lastly, each non-identity element appears twice and no two elements are inverses of each other in the group. Let's compare this with a sequencing of $\mathbb{Z}_{12}$ given below

$$\mathbf{a} = \{0, 1, 11, 2, 10, 3, 9, 4, 8, 5, 7, 6, \}$$
$$\mathbf{b} = \{0, 1, 10, 3, 8, 5, 6, 7, 4, 9, 2, 11\}$$

Okay, comparing this sequence in a the above light we see that we have again an increasing sequence of odd integers this time interlaced with a decreasing sequence of even integers. Also, the sequence certainly isn't a palindrome. However, each element and it's inverse appears exactly once and the only elements of order 2 appear exactly once as well. The last condition is clearly due to **a** being a sequencing of $\mathbb{Z}_{12}$, but it is worth noting because if we want to form 'lesser' types of sequencings in the future, we want our original sequencings to satisfy the relaxed conditions as well. Before making any new definitions, let's try a few more odd ordered $\mathbb{Z}_n$.

Example 4.29. Using the greedy algorithm of taking from the right and then left, etc. examine the following list of attempted sequences of $\mathbb{Z}_n$ for $n = 3, 5, 7, 9, 11, 13$. Note that we list the partial products first, followed by

the sequence of translations using negatives to represent moving left along the 'clock' and then the corresponding congruences last.

$$\begin{aligned}
\mathbf{b}_3 &= \{0,1,2\} \\
\mathbf{a}_3 &= \{0,1,1\} \\
&= \{0,1,1\} \\
\mathbf{b}_5 &= \{0,1,4,2,3\} \\
\mathbf{a}_5 &= \{0,1,-2,3,-4\} \\
&= \{0,1,3,3,1\} \\
\mathbf{b}_7 &= \{0,1,6,2,5,3,4\} \\
\mathbf{a}_7 &= \{0,1,-2,3,-4,5,-6\} \\
&= \{0,1,5,3,3,5,1\} \\
\mathbf{b}_9 &= \{0,1,8,2,7,3,6,4,5\} \\
\mathbf{a}_9 &= \{0,1,-2,3,-4,5,-6,7,-8,\} \\
&= \{0,1,7,3,5,5,3,5,7,1\} \\
\mathbf{b}_{11} &= \{0,1,10,2,9,3,8,4,7,5,6\} \\
\mathbf{a}_{11} &= \{0,1,-2,3,-4,5,-6,7,-8,9,-10\} \\
&= \{0,1,9,3,7,5,5,7,3,9,1\} \\
\mathbf{b}_{13} &= \{0,1,12,2,11,3,10,4,9,5,8,6,7\} \\
\mathbf{a}_{13} &= \{0,1,-2,3,-4,5,-6,7,-8,9,-10,11,-12\} \\
&= \{0,1,11,3,9,5,7,7,5,9,3,11,1\}
\end{aligned}$$

Okay, we can definitely see a pattern start to develop and as before in the **a** sequence we get two occurrences of an element and none of its inverse. We turn this property into a definition.

Definition 4.30. [7] Let G be a finite group of order n. Then a **2-sequencing** of G is an ordering $\mathbf{a} = \{a_1, a_2, a_3, \ldots, a_n\}$, not necessarily distinct, such that the partial products $b_i = a_1 \cdots a_i$ are all distinct and $\mathbf{a}$ consists of

(1.) one occurrence of each element $x \in G$ which satisfies $x^2 = e$.

(2.) for every other element $x \in G$, either two occurrences of x and none of x^{-1}, or one of x and one of x^{-1}, or none of x and two of x^{-1}.

The sequence $\mathbf{b}$ of partial products is called a **terrace** of G. If the elements of $\mathbf{a}$ are distinct, then $\mathbf{b}$ is called a *directed terrace*.

Note that in the definition, a directed terrace is simply a sequencing for G. So, by relaxing the conditions on $\mathbf{a}$ to allow an element and it's inverse to occur in pairs (in a sense), we have the concept of a 2-sequencing. We will say a group is **terraced** if it has a terrace. Clearly, sequenceable groups are terraced. Additionally, from our work above we can see that $\mathbb{Z}_n$ is terraced with the following terrace and corresponding 2-sequencing

$$\mathbf{a}_j = \begin{cases} j & \text{if } j \text{ is odd} \\ n - j & \text{if } j \text{ is even} \end{cases}$$

with $0 \leq j \leq n-1$, and

$$\mathbf{b}_{2k-1} = k$$

$$\mathbf{b}_{2k} = n - k$$

with $0 \leq k \leq \dfrac{n-1}{2}$. When n is even, we get back the sequencing for $\mathbb{Z}_n$ we developed earlier. So, $\mathbb{Z}_n$ can be terraced. This leads to the question of which other finite abelian groups also posses a terrace? For example, can we take a

terrace for $\mathbb{Z}_3$ and somehow combine it with a terrace for $\mathbb{Z}_5$ in such a way that we terrace $\mathbb{Z}_3 \times \mathbb{Z}_5$? Let's start small and try to terrace $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Start with a terrace of $\mathbb{Z}_3$ given by $\{0, 1, 2\}$ with corresponding 2-sequencing $\{0, 1, 1\}$. A terrace of $\mathbb{Z}_3 \times \mathbb{Z}_3$ will then be an arrangement of ordered pairs $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ such that the path through them encounters each pair exactly once (in this sense it will be a Hamiltonian path). Additionally, the 'hops' (or edges in the graph theory setting) to get from one pair to the next must occur in pairs according to the definition. Start by drawing an array of points from $\mathbb{Z}_3 \times \mathbb{Z}_3$ as in Fig.4.7

Figure 4.8: Elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$

$$(0,2) \qquad (1,2) \qquad (2,2)$$

$$(0,1) \qquad (1,1) \qquad (2,1)$$

$$(0,0) \qquad (1,0) \qquad (2,0)$$

The process here is to start at the bottom by terracing $\mathbb{Z}_3$ in the first co-ordinate and leaving the second co-ordinates all 0's. Then as we proceed to the next row, repeat the terracing for $\mathbb{Z}_3$ in the first co-ordinate and continue the process of terracing $\mathbb{Z}_3$ in the second co-ordinate. In this way we guarantee distinct points.

So, now we have our set of points. Note that within a given row, there is only a change in the x position and this change corresponds to the values in the 2-sequencing for $\mathbb{Z}_3$. The same can be said for changes within each

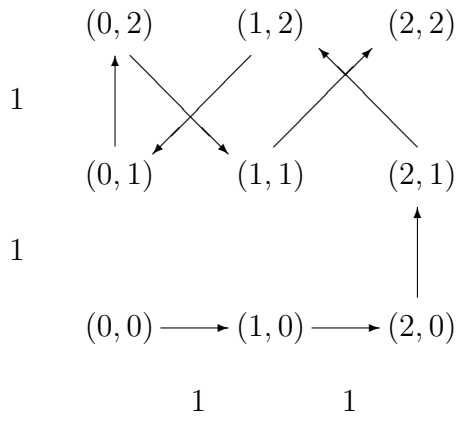
column; they correspond to the 2-sequencing of $\mathbb{Z}_3$ in the second co-ordinate. Label the changes between row elements along the bottom row between each column and label the changes between columns along the side between rows as in the figure below. Now, a path through the bottom row horizontally will

Figure 4.9: Elements of $\mathbb{Z}_3 \times \mathbb{Z}_3$

$$
\begin{array}{ccccc}
 & (0,2) & & (1,2) & & (2,2) \\
1 & & & & & \\
 & (0,1) & & (1,1) & & (2,1) \\
1 & & & & & \\
 & (0,0) & & (1,0) & & (2,0) \\
 & & 1 & & 1 &
\end{array}
$$

essentially be terracing $\mathbb{Z}_3$, which will satisfy our requirements for a terrace in the product group. When we get to the end of the row, turn up to $(2,1)$, which starts the sequencing of $\mathbb{Z}_3$ in the second co-ordinate. Then proceed as in the figure below to move vertically up and horizontally left, then vertically down and horizontally left, making a zig-zag pattern until you come to the end of the row. Notice you will be using element from the second and third row here at the same time. At the end of the row, move up (and this is key) to the third row. Notice that this movement is the next step in the sequencing of $\mathbb{Z}_3$ in the second co-ordinate. Throughout the zig-zag process we made changes in both co-ordinates, so none of these can correspond to the terracing of $\mathbb{Z}_3$ in either co-ordinate. Now we must make changes that represent the inverses of those made during the first pass through. The changes can be read directly from the labels on the bottom and side of the array of points. For example,

Figure 4.10: Terracing of $\mathbb{Z}_3 \times \mathbb{Z}_3$



the step from $(2,1) \to (1,2)$ can be seen as a $(-1,1)$ change since we move left 1 unit and up 1 unit according to the labels on the bottom. Thus, we must counter this with the inverse step $(1,-1)$ which looking at the array and considering the scheme we are using can only happen during the step from $(0,2) \to (1,1)$. This suggests we should work our way back through the by first heading vertically down and horizontally right, then vertically up and horizontally right completing a crossing pattern. Notice that we will always have the same number of arrows whether moving right to left or vice versa. Also, for each step going to the left, there is a corresponding inverse step coming back through the right. The end result is the following terrace for $\mathbb{Z}_3 \times \mathbb{Z}_3$

$$\{(0,0),(1,0),(2,0),(2,1),(1,2),(0,1),(0,2),(1,1),(2,2)\}$$

with corresponding 2-sequencing

$$\{(0,0),(1,0),(1,0),(0,1),(-1,1),(-1,-1),(0,1),(1,-1),(1,1)\}$$

In the next example we use the same technique to find a terrace for $\mathbb{Z}_5 \times \mathbb{Z}_5$.

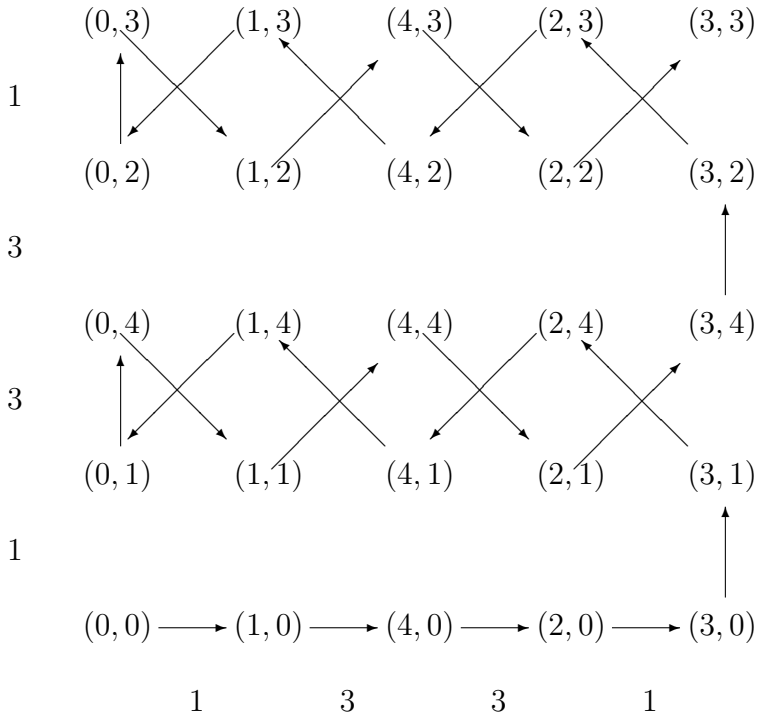
Example 4.31. Let $G = \mathbb{Z}_5$. Start with a terrace of $\mathbb{Z}_5$

$$\mathbf{b} = \{0, 1, 4, 2, 3\}$$

$$\mathbf{a} = \{0, 1, 3, 3, 1\}$$

Extend this to an array of points for $\mathbb{Z}_5 \times \mathbb{Z}_5$ according to the procedure listed above with the appropriate elements of the 2-sequencings listed between columns and rows. Follow the same pattern of criss-crossing each pair of levels starting with 2 and 3, then moving up to 4 and 5 as shown in the figure.

Figure 4.11: Terracing of $\mathbb{Z}_5 \times \mathbb{Z}_5$



Now, we have a pretty clear method for sequencing $\mathbb{Z}_m \times \mathbb{Z}_n$ for m, n odd. Recall if either m or n is a power of 2, then we can sequence the resulting group according to Theorem 4.7. The next question would be to go about

terracing a third product. If we can terrace $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \mathbb{Z}_{n_3}$ for n_i odd, then we can proceed by induction using Theorem 4.6 to show that any abelian group of odd order can be terraced.

Again, lets start small and create a terrace for $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. This will give us insight as to the type of occurrences we can expect to find in the terracing of the more general setting.

Example 4.32. Start with a terrace for $\mathbb{Z}_3 \times \mathbb{Z}_3$ given by

$$\{(0,0),(1,0),(2,0),(2,1),(1,2),(0,1),(0,2),(1,1),(2,2)\}$$

with corresponding 2-sequencing

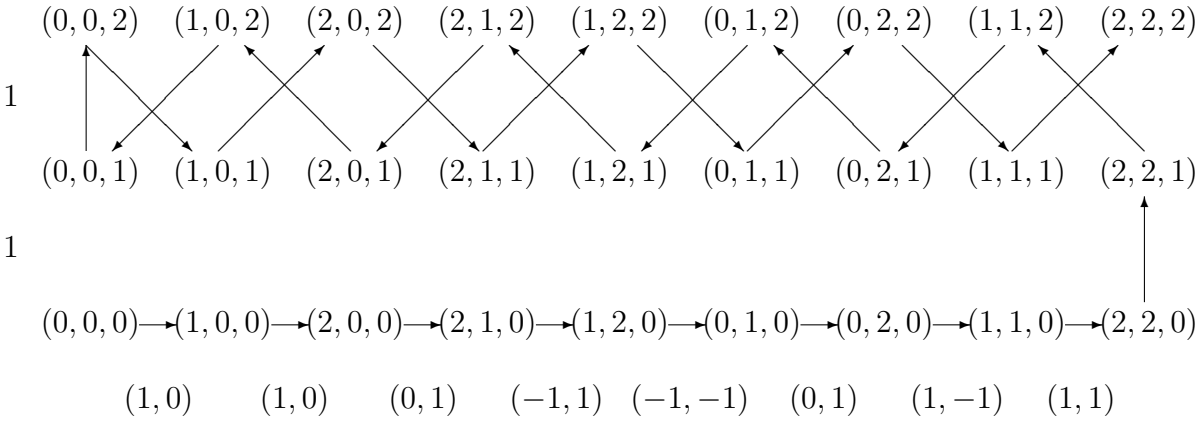
$$\{(0,0),(1,0),(1,0),(0,1),(-1,1),(-1,-1),(0,1),(1,-1),(1,1)\}.$$

Proceed as before to use the terrace for $\mathbb{Z}_3 \times \mathbb{Z}_3$ as the first co-ordinate and place 0's in the second co-ordinate. Thus the first row will be

$$\{(0,0,0),(1,0,0),(2,0,0),(2,1,0),(1,2,0),(0,1,0),(0,2,0),(1,1,0),(2,2,0)\}$$

Next form the remaining two rows by cycling through the terrace for $\mathbb{Z}_3$ in the second co-ordinate as you move up the rows while keeping the first co-ordinate (in this case the first two co-ordinates) constant. We have the following array

Figure 4.12: Terracing of $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$



The next step is to account for the differences in each step. They are listed below

$$\big\{(0,0,0),(1,0,0),(1,0,0),(0,1,0),(-1,1,0),(-1,-1,0),$$
$$(0,1,0),(1,-1,0),(1,1,0),(0,0,1),(-1,-1,1),$$
$$(-1,1,-1),(0,-1,1),(1,1,-1),(1,-1,1),(0,-1,-1),$$
$$(-1,0,1),(-1,0,-1),(0,0,1),(1,0,-1),(1,0,1),(0,1,-1),$$
$$(-1,1,1),(-1,-1,-1),(0,1,1),(1,-1,-1),(1,1,1)\big\}$$

We draw attention to $(-1,-1,1)$ and it's inverse $(1,1,-1)$ both occurring within the same pass through the array. This is a difference from the first few products we terraced, where an elements' inverse only occurred during the pass through the array in the opposite direction. However, this example along with the previous terraces cover all of the cases we can expect to find when terracing odd ordered abelian groups. We can claim by induction and the Fundamental Theorem of Finitely Generated Abelian groups that all odd ordered abelian groups are terraced.

Before tackling the product of two even ordered abelian groups, say $\mathbb{Z}_4 \times \mathbb{Z}_4$ we take a look at terracing $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and compare this with the sequencing we created in Ex. **??**. The result is rather surprising.

Example 4.33. In order to terrace $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, start with a terrace of $\mathbb{Z}_2$, $\mathbf{b} = \{0,1\}$ and form the 3×2 array needed to terrace $\mathbb{Z}_2 \times \mathbb{Z}_3$. Next, notice that if we terrace this array in the manner consistent with previous groups will get the following terrace and corresponding 2-sequencing

$$\mathbf{b} = \{(0,0),(1,0),(1,1),(0,2),(0,1),(1,2)\}$$
$$\mathbf{a} = \{(0,0),(1,0),(0,1),(1,1),(0,2),(1,1)\}$$

Figure 4.13: Elements of $\mathbb{Z}_2 \times \mathbb{Z}_3$

$$(0,2) \qquad (1,2)$$

$$1$$

$$(0,1) \qquad (1,1)$$

$$1$$

$$(0,0) \qquad (1,0)$$

$$1$$

which corresponds to the following in the isomorphic group $\mathbb{Z}_6$

$$\mathbf{b} = \{0, 3, 1, 2, 4, 5\}$$
$$\mathbf{a} = \{0, 3, 4, 1, 2, 1\}$$

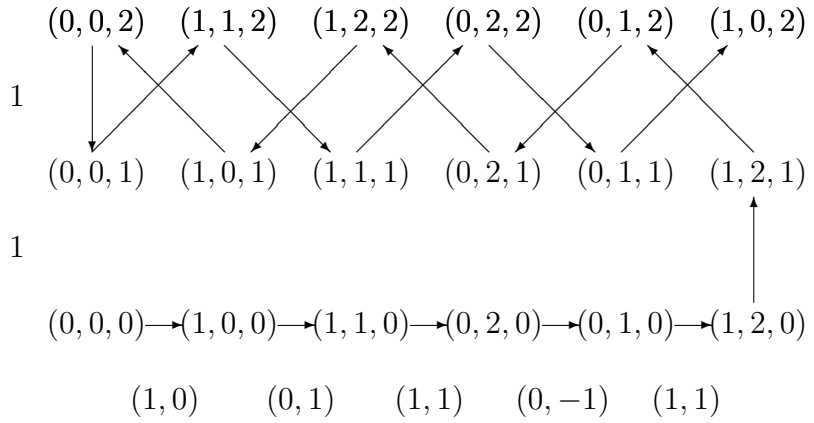
What should be noted is that while **b** is a terrace (and a fine one at that with inverses and order 2 elements present), it is **not** the terrace we would normally use for $\mathbb{Z}_6$, i.e. $\{0, 1, 5, 2, 4, 3\}$, which gives a sequencing of $\mathbb{Z}_6$. Writing the normal terrace in $\mathbb{Z}_2 \times \mathbb{Z}_3$ would be

$$\mathbf{b} = \{(0,0), (1,1), (1,2), (0,2), (0,1), (1,0)\}$$
$$\mathbf{a} = \{(0,0), (1,1), (0,1), (1,0), (0,2), (1,2)\}$$

Trace the path that produces this terrace and notice how it is different from our previous paths. Furthermore, look back at the sequencing of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ given in Ex.**??** provided by Theorem 4.7. Can we hope to realize this sequencing when we terrace $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ according to the methods developed in this section? There is only one way to find out. We will stick with the terrace for $\mathbb{Z}_2 \times \mathbb{Z}_3$ formed by our normal method.

Start by forming the array of points for $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ with the first row being the terrace of $\mathbb{Z}_2 \times \mathbb{Z}_3$ followed vertically by cycling through the terrace for $\mathbb{Z}_3$ in the third component. List the differences along the bottom and sides as before. Finally, plot the paths taken through the array that terraces $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. The final product is shown in Fig.4.13

Figure 4.14: Terracing of $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$



Now, the terrace is certainly not the same as the sequencing we arrived at in Ex.**??**. The corresponding 2-sequencing will also differ. This should serve notice that our method for terracing does give a sequencing for $\mathbb{Z}_n$ when n is even, but fails to do the same in the general setting where G is an abelian binary group.

4.4 Symmetric Sequencing and 2-Sequences

The subject of this chapter will be to bring together concepts and results from the previous three sections into a main result on sequencing. The result we prove at the end of the section will allow us to give a slightly more elegant proof of the sufficiency part of Theorem 4.7. Additionally, this result is regarded as

a main result on which most of the work on 2-sequencings is based [23].

Our first section on sequencings dealt with the general problem of which abelian groups where sequenceable and introduced the idea of a symmetric sequencing. We introduced the concept of quotient mapping in the next section and used this idea to help sequence certain dihedral groups. The last section introduced the concept of 2-sequencings and their corresponding terraces and we showed that abelian groups of odd order could be terraced using a criss-crossing path through the array of points that represented the group elements. The main result of this section ties these concepts together in the following theorem.

Theorem 4.34. [4] Let G be a binary group of order $2n$ and let $\Lambda(G)$ be the unique subgroup of G of order 2. Then G has a symmetric sequencing if and only if $G/\Lambda(G)$ has a 2-sequencing.

Before we can prove this result, we will need a preliminary result about binary groups.

Lemma 4.4.1. Let G be a binary group of order $2n$ and let z be the unique element of order 2. Then $\langle z \rangle$ is a normal subgroup of G and $z \in Z(G)$, z is contained in the center of G.

Proof: Since conjugation is a group automorphism the order of gzg^{-1} is a again 2 and therefore by assumption must equal z. This proves both that $z \in Z(G)$ and that $\langle z \rangle \trianglelefteq G$. □

We are now in a position to prove the ($\Rightarrow$) of Theorem 4.34. Assume G has a symmetric sequencing given by

$$\mathbf{a} = \{a_1, a_2, \ldots, a_{n-1}, a_n, z, a_n^{-1}, a_{n-1}^{-1}, \ldots, a_2^{-1}, a_1^{-1}\},$$

where z is the unique element of order 2. Let $\pi : G \longrightarrow G/\Lambda(G)$ be the natural projection of G onto $G/\Lambda(G)$. Thus for $a_i \in G$ with $1 \leq i \leq n$ we have that $a_i \mapsto \{a_i, a_i z\}$, the coset containing a_i. We need to check that the resulting sequence

$$\{\pi(a_1), \pi(a_2), \ldots, \pi(a_n)\}$$

is a 2-sequencing for $G/\Lambda(G)$. Since $\mathbf{a}$ is a symmetric sequencing of G it follows that the cosets have the form $\{b_k, b_k z\}$, hence every coset appears once int he partial products of the $\pi(\mathbf{a})$ sequence and thus these partial products are distinct. The first condition for a 2-sequencing is that if $x^2 = e$ for $x \in G/\Lambda(G)$, then x occurs exactly once in $\{\pi(a_1), \pi(a_2), \ldots, \pi(a_n)\}$. Assume there exists $y \in G/\Lambda(G)$ such that $y^2 = e$. Since $y = \{x, xz\}$ for some $x \in G$ and since z is the unique order 2 element, $y^2 = e \in G/\Lambda(G)$ implies $x^2 = z \in G$, which implies $x^{-1} = xz$. Now y occurs at least once either as the coset represented by x or xz. Therefore assume y occurs twice in the quotient mapping, which means we have $\overline{a_i} = \overline{a_j}$ for some $i \neq j$. This implies either $a_i = a_j$ or $a_i = a_j z$ for $1 < i, j \leq n$. The first result contradicts that $\mathbf{a}$ is a sequencing. Taking $a_i = a_j z$ and multiplying by a_i on the left and z on the right and using $a_i^2 = z$ gives that $z = a_j z a_i = a_j a_i z$ since $z \in Z(G)$. But this implies $a_i = a_j^{-1}$, which contradicts that $\mathbf{a}$ was a symmetric sequencing. Thus y exactly once in the quotient mapping.

Next, let $y \in G/\Lambda(G)$ and assume $y^2 \neq e$. Now, $y = \{x, xz\}$ for some $x \in G$, and if y appears twice in the quotient mapping, then x and xz appear in some order in $\mathbf{a}$ before the middle term z. Thus x^{-1} and $x^{-1}z = (xz)^{-1}$, which together form the coset $y^{-1} \in G/\Lambda(G)$, cannot appear as elements in $\mathbf{a}$ to the left of z. Thus, y^{-1} doesn't appear in the quotient map. A similar argument holds if y^{-1} appears twice. If y appears exactly once, then x or xz

(but not both) appears in $\mathbf{a}$ before z. If $a_i = x$ and x^{-1} doesn't appear as some a_j, for $1 < i, j \leq n$, then xz and $x^{-1}z$ both appear to the right of z in $\mathbf{a}$. This contradicts that $\mathbf{a}$ was symmetric. Thus, if y appears once then so must y^{-1}. Clearly, we cannot have y appearing more than once, since there are only 2 elements in the coset. A third appearance would mean that in the original sequence $\mathbf{a}$ we would have had some element appearing twice.

The proof of the other direction is constructive and therefore we should provide examples to see how it works before giving the technical details. There examples are somewhat artificial, but they get the idea across.

Example 4.35. Let $G = \mathbb{Z}_8$. Then a 2-sequencing of the factor group $G/\langle 4 \rangle$ is given by

$$\big\{\{0,4\},\{1,5\},\{2,6\},\{3,7\}\big\}$$

with corresponding terrace

$$\big\{\{0,4\},\{1,5\},\{3,7\},\{2,6\}\big\}$$

The idea is to select along with 0 one element at a time from each coset such that not only are the resulting 3 non-trivial elements all distinct, but also that the inverses form a disjoint set of elements. This last condition is so that we don't have $a_i = a_j^{-1}$ for $1 < i, j \leq 4$. Thus we can select 0 then 1 then 2 and finally 3. Here we can't choose 7 because then in G $1 = 7^{-1}$. We continue the sequence $0, 1, 2, 3$, with 4 in the middle and then go downhill by selecting the inverses accordingly, finishing with

$$\mathbf{a} = \{0,1,2,3,4,5,6,7\}$$

and directed terrace

$$\mathbf{b} = \{0,1,3,6,2,7,5,4\}$$

.

The previous example gives the procedures to follow when y and y^{-1} both occur once in the 2-sequencing. Also, we saw what to do with y if $y^2 = e$ in the 2-sequencing. The next example demonstrates the procedure if y occurs twice and y^{-1} doesn't occur in the 2-sequencing.

Example 4.36. Let $G = \mathbb{Z}_{18}$. Then a 2-sequencing of the factor group (isomorphic to $\mathbb{Z}_9$) with corresponding terrace is given by

$$\mathbf{a} = \big\{\{0,9\},\{1,10\},\{7,16\},\{3,12\},\{5,14\},\{5,14\},\{3,12\},\{7,16\},\{1,10\}\big\}$$
$$\mathbf{b} = \big\{\{0,9\},\{1,10\},\{8,17\},\{2,11\},\{7,16\},\{3,12\},\{6,15\},\{4,13\},\{5,14\}\big\}$$

Now, starting with the 2-sequencing **a** we select 0, then 1, then 7, then 3, then 5. We can select either of the elements in the cosets up to this point without worry because none of the cosets are inverses of each other. However, when we get to the second $\{5,14\}$, we must select 14 so as not to have 5 repeated in the sequence for G. Likewise for the remaining cosets. Thus we have $\{0,1,7,3,5,14,12,16,10\}$ as the start of our symmetric sequence. Proceed by choosing 9 next, followed by taking the inverse of the element that is equal distance from 9 as the next element. Thus we have

$$\mathbf{a} = \{0,1,7,3,5,14,12,16,10,9,8,2,6,4,13,15,11,17\}$$

with partial products sequence

$$\mathbf{b} = \{0,1,8,11,16,12,6,4,14,5,13,15,3,7,2,17,10,9\}.$$

So, the procedure we use when y or y^{-1} occurs twice in the 2-sequencing is to select either coset element the first occurrence and then choose the opposite element on the second occurrence. Combining these three rules into a nice package we have

(1) : if $y \in G/\Lambda(G)$, $y \neq y^{-1}$ and y(equivalently y^{-1}) occurs twice in our 2-sequencing, the two occurrences of $y = \{x, xz\}$ can be projected back to x and xz (in either order).

(2) : if $y \in G/\Lambda(G)$, $y \neq y^{-1}$ and both y and y^{-1} occur once in our 2-sequencing, say $y = \{x, xz\}$ and $y^{-1} = \{x^{-1}, x^{-1}z\}$, we can either project y to x and y^{-1} to $x^{-1}z$ or y to xz and y^{-1} to x^{-1}.

(3) : if $y \in G/\Lambda(G)$, $y = y^{-1}$ and$y \neq e, z$ then y must occur once in our 2-sequencing. Now $y = \{x, x^{-1}\}$ and y may be projected back to either x or x^{-1}.

(4) : If $y = \{e, z\} \in G/\Lambda(G)$ then y must be projected to e.

This process gives a sequence of the form $(e, a_2, \ldots, a_n)$ in G where $a_i \neq a_j$ and $a_i^{-1} \neq a_j$ for $1 < i, j \leq n$, with $i \neq j$. Extend this to a sequence of all elements of G,

$$\mathbf{a} = \left\{e, a_2, \ldots, a_n, z, a_n^{-1}, \ldots, a_2^{-1}\right\}.$$

We claim that the sequence $\mathbf{a}$ is a symmetric sequencing of G. Observe the partial products are

$$\mathbf{b} = \left\{e, b_2, \ldots, b_n, b_n z, b_{n-1} z, \ldots, b_2 z\right)$$

and we know that the sequence $\{e, b_2, \ldots, b_n\}$ are all distinct since they form the terrace for the factor group and the other side of $\mathbf{b}$ was formed by taking inverses. The sequence is symmetric, so the claim is verified and the proof is complete.

Now, to finish the section we offer a different route to proving that if G is an abelian group of the form $\mathbb{Z}_{2^k} \times \mathbb{Z}_m$ where $\mathbb{Z}_m$ is of odd order then G is sequenceable.

Start with $\mathbb{Z}_{2^k} \times \mathbb{Z}_m$ and using the unique order 2 element form the factor group isomorphic to $\mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_m$. Continue in this process until on the n^{th} iteration you arrive at a group isomorphic to $\mathbb{Z}_m$. Then by results in the previous section, this group has a 2-sequencing, hence the group $\mathbb{Z}_2 \times \mathbb{Z}_m$ has a symmetric sequencing. Continue working backwards until you reach the original group, which will thus have a symmetric sequencing. Note that in both proofs you are given a method of constructing the sequencings.

4.5 The Gordon Game

In 1992, Isbell [17] introduced the idea of 'competitive' sequencing of G by two players moving alternately. The Gordon Game $\Gamma(G)$ for a given finite group G is played as follows. A counter is placed on the identity element, e, of G. White and Black then take turns (White moves first) to move the counter around the group subject to condition that the $(n+1)^{\text{st}}$ move (to x_{n+1}) must satisfy

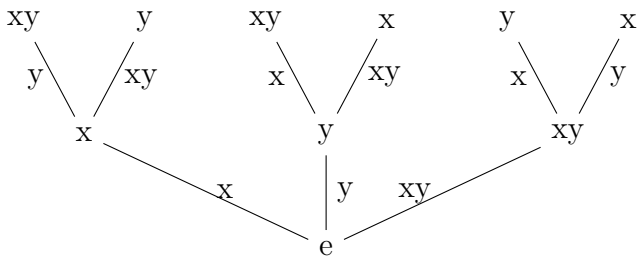
$$(1)\ x_{n+1} \notin \{e, x_1, \ldots, x_n\}, \text{ and} \tag{4.6}$$

$$(2)\ x_n^{-1} x_{n+1} \notin \left\{x_1, x_1^{-1} x_2, \ldots, x_{n-1}^{-1} x_n\right\}. \tag{4.7}$$

The first player unable to move loses. The first condition ensures that a player cannot move the counter to a group element previously visited (moved to). The second condition is better explained by example.

Example 4.37. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ with group elements $\{e, x, y, xy\}$ and relations $x^2 = y^2 = (xy)^2 = e$. Then $\Gamma(G)$ has the following game tree

Figure 4.15: $\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2)$



In the tree above, the nodes represent where the counter can be moved to and the edges are labeled with the required movements. We see immediately that Black has a forced win by simply playing any available move (there are no moves left after the second level). A typical game may start with the following sequence of moves ($\mathbf{M}$) with corresponding positions ($\mathbf{P}$) :

$$\mathbf{M} = (e, y, x)$$
$$\mathbf{P} = (e, y, xy)$$

Now, $\mathbf{P}$ is the list we must consult to satisfy condition (1) of Equation 4.6 and $\mathbf{M}$ must satisfy condition (2). So, it is White's turn, and he can only move to position x. However, this would require a movement of y since $(xy)y = xyy = x$. Since y has already been used as a movement, White is stuck and thus forced to concede victory.

What is interesting about the sequences is this: they are backwards from what we have thought of as normal sequencing for groups! Recall that for a finite group G, a sequencing is a list $(e, g_1, \ldots, g_n)$ such that the sequence of partial products $(e, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n)$ are distinct. Thus $\mathbf{M}$ represents the sequence and $\mathbf{P}$ is the sequence of partial products. This is backwards because we are picking where we want to go as the elements of $\mathbf{P}$, but in

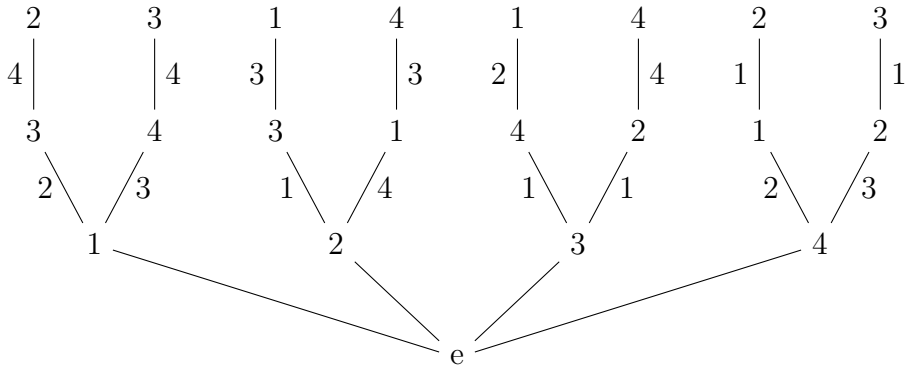
reality they become the partial products of how we plan to get there (the actual movements).

It should be noted that if each player tried to drag the game out as long as possible and exhaust the entire set of available movements, then the resulting set $\mathbf{M}$ would be a sequencing of the group G with corresponding basic directed terrace $\mathbf{P}$. Of course, from Theorem 4.7, we know that is not possible for $\mathbb{Z}_2 \times \mathbb{Z}_2$ since all of the non-identity elements are order 2.

Let's play another game, this time using the group $G = \mathbb{Z}_5$. Maybe Whites luck will change.

Example 4.38. Let $G = \mathbb{Z}_5 = \{e, 1, 2, 3, 4\}$. Then $\Gamma(G)$ has the following game tree (initial movements from the identity have been omitted for aesthetics).

Figure 4.16: Game tree for$\Gamma(\mathbb{Z}_5)$



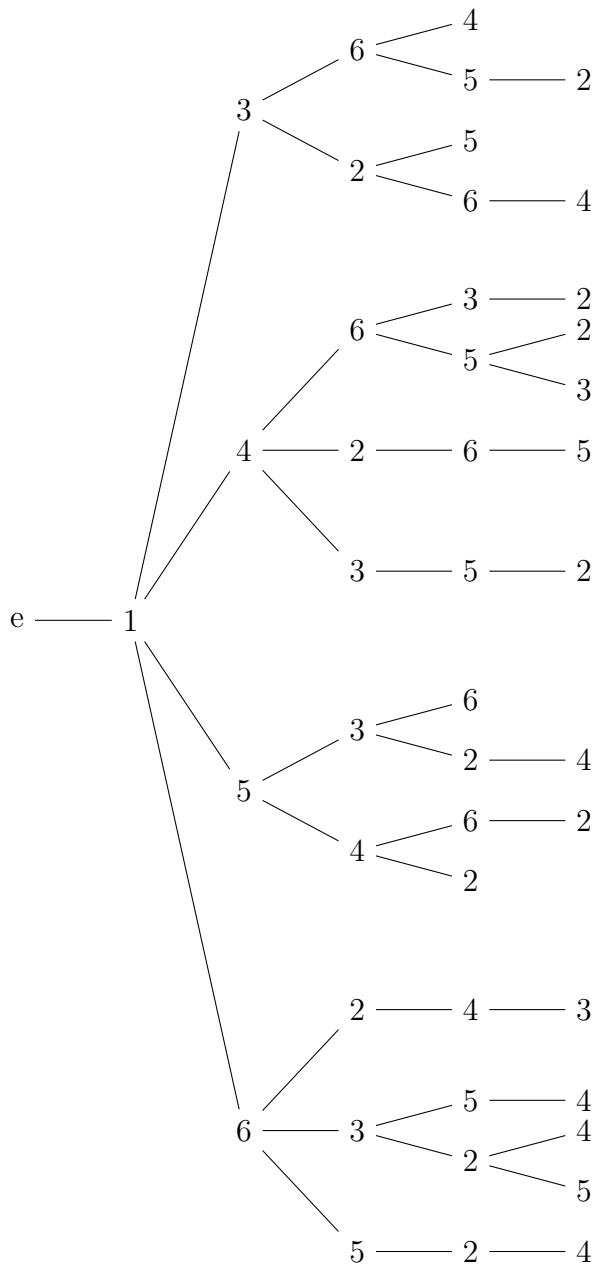
We see the reversal of the last example in that for $\Gamma(\mathbb{Z}_5)$ White has a forced win from every starting position. It seems rather cruel to play a game with someone where one player literally has no chance whatsoever. Before moving to another example where both players seem to have a fighting chance, let's look at this tree for just a minute. Notice the structure of the branches

extending up from each of the four first moves. That they are all the same structurally is not a coincidence. In fact, we can transfer from one set of games played with a starting move of $x_1 = 1, 2, 3, 4$ to any other set of games with a different starting move by using the fact that the automorphisms on $\mathbb{Z}_p$ are transitive on non-identity elements. Recall that left multiplication by a group G on itself is a group action, and hence induces a permutation of the group. Left multiplication by a generator of a cyclic group is an automorphism, and the generators of $\mathbb{Z}_p$ are exactly the non-identity elements (a generator, a, of $\mathbb{Z}_n$ is any element such that $gcd(a, n) = 1$). The multiplication is carried out mod p, so to go from the games starting with, say, placement $x_1 = 2$ to the games starting with $x_1 = 3$, we simply multiply all of the nodes and edges by 4, since $2 * 4 = 8 \equiv 3 \pmod 5$. Thus to study $\Gamma(\mathbb{Z}_p)$ we need only concern ourselves with examining the set of games starting with $x_1 = 1$ (we could choose any non-identity element of $\mathbb{Z}_p$).

Let's play a few games using $\mathbb{Z}_7$. These games last a bit longer and we shall see there are plenty of opportunities for both White and Black to win (but only one has a best play winning strategy). There are exactly 108 possible games that can be played using $\mathbb{Z}_7$, but we are only concerned with those starting with first move $x_1 = 1$; of which there are 18. Aren't automorphisms great!

Example 4.39. Let $G = \mathbb{Z}_7$. Then the following figure gives the game tree for $\Gamma(\mathbb{Z}_7)$. We have omitted labeling the edges to avoid clutter. One can see from the diagram that although there are 14 games in which White wins, the 4 times Black wins are all best play moves and so Black has a forced win for $\Gamma(\mathbb{Z}_7)$.

Figure 4.17: Game tree for $\Gamma(\mathbb{Z}_7)$



We give one final example using non-abelian group, D_3. The group of symmetries on the equilateral triangle is the smallest non-abelian group and will serve our purpose well here. We opt to stay with the notation used by Isbell and let D_3 be the set of ordered pairs $(x, a) \in \mathbb{Z}_3 \times \mathbb{Z}_2$ with multiplication defined by:

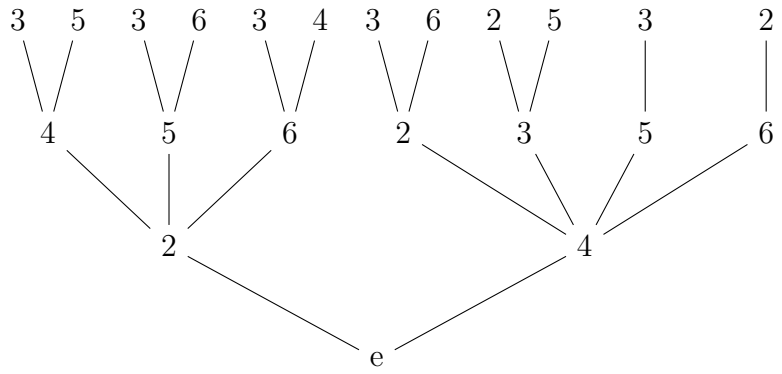
$$\begin{aligned} (x,0)(y,a) &= (x+y,a) \\ (x,1)(y,a) &= (x-y,1+a) \end{aligned}$$

Additionally, we would like to index this set to avoid listing ordered pairs as nodes. We will use the commonly accepted practice [18] of indexing the group by associating $(i, 0)$ with $i+1$ and $(i, 1)$ with $n+1+i$. This lists the identity, followed by the rotations, and then the reflections in order from 1 to $2n$. So, we have the following group elements and their indices listed below

$$\begin{pmatrix} (0,0) & (1,0) & (2,0) & (0,1) & (1,1) & (2,1) \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Using a similar argument from the last example, if White has a forced win in games starting with $x_1 = (1, 0)$, then he will still have a forced win in the games starting with $(2, 0)$ (conjugation by an element of order 2, which was seen to be an automorphism will send $(1, 0) \mapsto (2, 0)$). Likewise for any of the games with reflections as first moves; a forced win in one will transfer to a forced win in the other branches. Therefore, we submit the game tree for $\Gamma(D_3)$ with starting moves of $(1, 0)$ and $(0, 1)$. We see that White has a forced win in 3 moves.

Figure 4.18: Game tree for $\Gamma(D_3)$



We define the **remoteness** [8] of $\Gamma(G)$ as the number of moves (half-moves) the game takes if the theoretical winner aims (rationally, i.e. using best play) to win as soon as possible while the loser aims to survive as long as possible. We can see from the examples above that $\Gamma(\mathbb{Z}_5)$ and $\Gamma(D_3)$ both have remoteness 3 and that $\Gamma(\mathbb{Z}_2 \times \mathbb{Z}_2)$ has remoteness 2. The parity tells you the winner, White if odd, Black if even. Isbell [17] investigated the Gordon game for groups of small order, finding the following results. In the table W and B denote forced wins for White and Black, respectively.

$\mathbb{Z}_2$:	W	$\mathbb{Z}_3$:	W	$\mathbb{Z}_4$:	W
$\mathbb{Z}_2 \times \mathbb{Z}_2$:	B	$\mathbb{Z}_5$:	W	$\mathbb{Z}_6$:	B
D_3:	W	$\mathbb{Z}_7$:	B	$\mathbb{Z}_8$:	B
$\mathbb{Z}_2 \times \mathbb{Z}_4$:	W	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$:	B	D_4:	B
Q_8:	W	$\mathbb{Z}_9$:	B	$\mathbb{Z}_3 \times \mathbb{Z}_3$:	B
$\mathbb{Z}_{10}$:	W	$\mathbb{Z}_{11}$:	B	$\mathbb{Z}_{13}$:	B

Additionally, Isbell made the following tentative conjecture

Conjecture 1. Black(player 2) wins $\Gamma(\mathbb{Z}_p)$ for primes $p > 5$.

Isbell offers the following reasoning for this conjecture; Although White has $p-1$ choices for first move in the game $\Gamma(\mathbb{Z}_p)$, the automorphisms of $\Gamma(\mathbb{Z}_p)$ are transitive on nonzero elements and so all opening moves for White are equivalent. Such an automorphism of $\mathbb{Z}_p$ is unique and the argument for Black winning is that 'in the unique game which Black faces after White's first move in $\Gamma(\mathbb{Z}_p)$ the $p-3$ possible moves are all different (inequivalent by automorphism). For large p, it is very unlikely that all are losing moves'.

This reasoning seems plausible and while we would like to be able to prove or disprove such a conjecture, the purpose of this paper is to extend the results of Isbell by finding theoretical winners for the groups of order 12 missing in the table and extend the table to include most abelian groups of order less than 20.

Chapter 5

Analysis of the Gordon Game

5.1 Introduction

We have seen how the Gordon game is played in a few cases for very small n. At this point, we need to get a bit technical so we can analyze the different complexities of our game later. We have the following definition.

Definition 5.1. [8] Define a game to be one in which the following hold:

1. There are just two players, we will call them White and Black.
2. There are finitely many positions and a particular starting position.
3. There are clearly defined rules that specify the moves that either player can make from a given position to its options.
4. White and Black move alternately.
5. Both players know what is going on, so there is complete information.
6. There are no chance moves such as rolling dice or shuffling cards.
7. In the normal play convention a player unable to move loses.

8. The rules are such that play will always come to an end because some player will be unable to move.

It should be clear from our examples of play in the previous chapter that the Gordon Game satisfies our definition of a game. However, determining an optimal strategy for playing the game changes based on the choice for G. The problem becomes computationally difficult. Computational complexity theory [1] is a branch of computer science and mathematics that focuses on classifying computational problems according to their inherent difficulty. Within this field, there are several methods for measuring game complexity, which estimates the computational difficulty of finding optimal strategies for combinatorial games. There are several ways of measuring game complexity. We will use the game-tree complexity method, which we describe below. We start with the formal definition of a game tree.

Definition 5.2. [1] In game theory, a **game tree** is a directed graph whose nodes are positions in a game and whose edges are moves. The complete game tree for a game is the game tree starting at the initial position and containing all possible moves from each position.

We gave game trees for different groups in the last chapter. Note that the game tree for $\Gamma(\mathbb{Z}_7)$ is not a complete game tree. The first task in analyzing the difficulty in determining optimal strategies is the game tree size.

Definition 5.3. The **game tree size** is the total number of possible games that can be played.

The game tree size for different groups will obviously vary, but we can achieve an upper bound by considering the flow of game play. For a group of size n, White has $n-1$ opening moves. Suppose this move is to place

the counter on g_1. Then Black cannot leave the counter alone (a move of e), he cannot move it to the identity (a move of g_1^{-1}), and he cannot move it to g_1^2. Thus he has $n-3$ moves. Let the second move be g_2, so we have the sequences $M = \{e, g_1, g_2\}$ and $P - \{e, g_1, g_1g_2\}$. Then White cannot use $\{e, g_1, g_2, g_2^{-1}, (g_1g_2)^{-1}\}$, which leaves $n-5$ choices. Continuing in this process, if the next move is g_3, then this leaves

$$\{e, g_1, g_2, g_3, g_3^{-1}, (g_2g_3)^{-1}, (g_1g_2g_3)^{-1}\}$$

as the list of moves not allowed, which is $n-7$. Now, it is certainly possible that some of the elements in the above list are duplicates. In this case, you would get one more move available. This is the case when a player chooses an order 2 element as a movement. It is inevitable that at some point the number of moves available stops decreasing by 2, and also that there may be consecutive turns where a player has the same number of moves as before. However, for the most part, we can assume that the number of moves decreases by 2 each time and so we may take an upper bound for the game tree size to be the product $(n-1)\cdot(n-3)\cdots(1)$. Although this is not quite as bad as $n!$, it is still larger by comparison to 2^n for small values of n. As a quick example, $2^{12} = 4096$ while $11 * 9 * 7 * 5 * 3 = 10395$. This is not a good sign.

It will be worth noting that for all of the games Isbell investigated, the remoteness was always less than or equal to $n-3$. This means that on average, assuming best play, there was still at worst 3 unplayed moves. This doesn't improve our upper bound for the game tree size, but every little bit will help.

The game-tree complexity measure uses the idea of a decision tree.

Definition 5.4. A **decision tree** is a subtree of the game tree with each position labeled with "White", "Black", or "draw" (note that draw cannot be

a possibility for our game), if that position can be proved to have that value (assuming best play) by examining only other positions in the graph.

Here is the process for creating a decision from a subtree of a game tree.

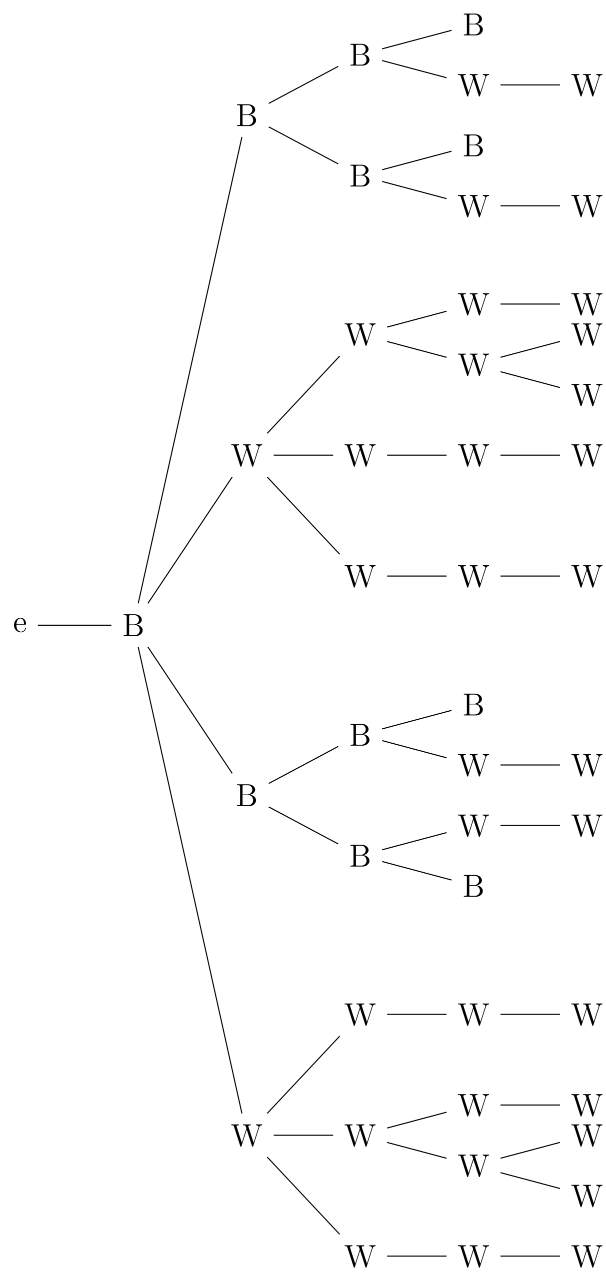
1. *All terminal positions can be labeled directly.*

2. *A position with White to move can be labeled "W" if any successor position is a win for White, or labeled "Black" if all successor positions are wins for Black.*

3. *A position with Black to move can be labeled "B" if any successor position is a win for Black, or labeled "W" if all successor positions are wins for White.*

Example 5.5. Examine the game tree for $\Gamma(\mathbb{Z}_7)$ with a starting move of 1 as shown in Figure 4.17. Start with the top branch where the partial product are $\{0, 1, 3, 6, 4\}$. This sequence has length 5 so it must be White's turn. Thus, the terminal point can be labeled "B" to indicate a win for Black. Thus the term preceding this one can also be labeled "B" since it would be Black's turn. Looking at the sequence $\{0, 1, 3, 2, 5\}$ we see that the 5 can be labeled "B" as well and therefore the preceding term can be labeled for Black also. Since we have both successors labeled Black and from the position 3 it is White's turn, we must label the 3 with a "B". This automatically allows us to label the first vertex 1 with a "B", since it would be Black's turn and there is at least one "B" in a successor position. From the root node e, this forces a win for Black. The remaining branches of the decision tree are given in the following figure.

Figure 5.1: $\Gamma(\mathbb{Z}_7)$ Decision Tree



Now we can define the game tree complexity, according to Allis.

Definition 5.6. [1] The **game tree complexity** of a game is the number of leaf nodes (total number of games played from a position) in the smallest decision tree that establishes the value of the initial position.

Thus the game tree complexity is an estimate of the number of positions that would need to be evaluated in a minimax search to determine the value of the initial position. A minimax search algorithm can be thought of as exploring the nodes of a game tree. The effective branching factor of the tree is the average number of children of each node (i.e., the average number of legal moves in a position). It is nearly impossible to determine the actual game tree complexity without seeing the entire game tree (and then what is the point), but for some games a reasonable lower bound can be given by raising the game's average branching factor to the power of the number of levels in an average game, or

$$GTC \geq b^d$$

where b is the average branching factor and d the number of levels in an average game.

Example 5.7. In this example we compare lower bounds for the GTC for $\Gamma(\mathbb{Z}_7)$ and $\Gamma\mathbb{Z}_{11}$. For $\mathbb{Z}_7$, the average branching factor is $(6+4+3+2+1)/5 \approx 3.2$ and the number of levels is 5, and so a lower bound for GTC is $3.2^5 \approx 335$. We don't have the full game tree for $\Gamma(\mathbb{Z}_{11})$, but we can use a upper bound for the branching factor, and we know that the remoteness according to Isbell is equal to 8 (this was verified by my program as well). We can take one more than the remoteness level (notice we used 5 for $\mathbb{Z}_7$). The reasoning behind taking one more level is that on average the search program will have to look

at *every* sequence from a given position until it finds a best play forced win. So, take $d = 9$. Now, we certainly cannot have 9 turns if at each level the number of moves decreases by 2. So, for now we shall turn to the output of our search program and use the values for an average game. We have $b = (10 * 8 * 7 * 4 * 4 * 2 * 2 * 2)/8 = 8960$. Thus $GTC \geq 3.72 \times 10^{35}$. So, we didn't even double the size of the group, and yet the GTC is at least 32 orders of magnitude larger. Clearly the difficulty in finding an optimal strategy for the Gordon game for larger order groups is immense.

We shall now turn to another type of measure used to analyze computer programs. In computer science, the **time complexity** [9] of an algorithm is the amount of time an algorithm takes to run as a function of the length input. The time complexity of an algorithm is commonly expressed using big O notation, which excludes coefficients and lower order terms. These are excluded because the time complexity is described as the length of the inputs tends towards infinity. For example, if the time required by an algorithm on all inputs of size n is at most $f(n) = 5n^3 + 3n$, then the time complexity of $f(n)$ is considered being $O(n^3)$.

Time complexity is commonly estimated by counting the number of elementary operations performed by the algorithm, where an elementary operation takes a fixed amount of time to perform. Thus the amount of time taken and the number of elementary operations performed by the algorithm differ by at most a constant factor. Since an algorithm's performance time may vary with different inputs of the same size, one commonly uses the worst-case time complexity of an algorithm, denoted as T(n), which is defined as the maximum amount of time taken on any input of size n. Time complexities are classified by the nature of the function T(n). For example, an algorithm

with $T(n)$ being $O(n)$ is called a linear time algorithm, and an algorithm with $T(n)$ being $O(2^n)$ is said to be an exponential time algorithm. An example will help.

Example 5.8. Suppose you compare two algorithms used to complete a specific computational task. Assume the first program takes $f_1(n) = n^2$ steps to complete, while the other takes $f_2(n) = 2n + 20$ steps. At first glance, it may appear that f_1 is a better program. Certainly, for $n \leq 5$ it is true that $n^2 \leq 2n+10$. However, n^2 scales much faster than $2n+10$ as n gets arbitrarily large. This is easiest to see by looking at the ratio,

$$\frac{f_1(n)}{f_2(n)} = \frac{2n + 20}{n^2}$$

This is a decreasing sequence that has it's maximum value at $n = 1$. Thus we can say that $f_1(n) \leq 22 f_2(n)$ and for large inputs, f_2 is a better choice.

It should be noted that if we were to consider a third program, say $f_3(n) = n + 1$, then we would have that both f_1 and f_3 are considered equally efficient on large inputs because as the size of the input get arbitrarily large, the coefficients and constant factors become inconsequential.

5.2 Search Program

In this section we walk through the necessary logic for a search program designed to find solutions to the Gordon game. The search program will be a depth first, as opposed to breadth first. A breadth first search would be useful if we were dealing with different distances between vertices, but the concept of distance has little meaning in this context. The elements of a group are not given different weights, so examining the path from g_1 to g_2 has the same importance as the path from g_2 to g_3.

Let G be a finite group of order n. Define the following terms:

Notation:

M A subset of G whose elements can potentially be used as movements in the current sub-game.

A The sequence of movements for the current sub-game

B A sequence of partial products of the list **A**

Using the above notations, we have the following preconditions for the program:

- $M = G - \{e\}$
- $A = B = \{e\}$, the identity of G.

We populate the set A and B with the identity since the game must start at the identity. Call the program and pass as inputs the sets A, B, M.

The program operates recursively. Pick the first element in M and call it x(locally). Find the last element in B and call it b. Compute the product $y = bx$. Run a search through B to determine if y is equal to any element in B. If $y \in B$, choose the next element in M and repeat. If $y \notin B$, append y to the end of B. Next remove the element x from M and append it to the end of A. Make copies of the adjusted sets A, B, M and make another call to the program with the new copies as inputs.

If, after trying all possible $x \in M$(or if M is empty), the program cannot find an x such that $bx \notin B$, then the program terminates and returns 1 if the length of B is even or returns 2 if the length of B is odd.

Assume at the i^{th} level the program receives output from a call to itself at level $i+1$. If it is Player 1's turn and the output is a win for Player 1, the program has found a force win for Player 1 and so it will **NOT** try to select any additional elements from M at the current level. It will return this value (1 in this case) to the previous call to the program, level $i-1$.

There can be other record keeping information sent to the program. For instance we may want to create a global variable called `gamecnt` that counts the total number of games played. If you eliminated the output of the program so that it only tries to search the game tree throughly, you would get an idea of the total number of games possible. Additionally, you could print out the sequences A and B at the terminal end of a path. By only recording those sequences that had length equal to the order of G, you would effectively have all possible sequencings of G.

Some notes about the program: First, it visits each vertex in the game tree at most once (and exactly once if you remove the force win flag). Second, it moves along each edge only to a neighbor one level down or up (so no hops or jumps through the game tree), and does so either zero times or exactly twice as to whether the force win flag is in place. Thirdly, it performs a finite set of operations while at a vertex (record where you are, how you got there, etc.). These record keeping steps can be done in linear time, so they can reasonably be ignored. Combining these notes we can say the time complexity as a function of the input will be at worst $O(|V| + |E|)$ where V will be the set of vertices in the game tree listed with repetition and E the set of edges(likewise listed with repetition). Now, $|V| \leq n!$ since at each level $i+1$ their is at worst 1 choice less for each vertex than at level i. The exception is towards the end-game where it is possible that you have the last few levels

and at each level there is the same small number of moves. This should not take away from the situation when you go from $n-1$ possible moves on the first level to $n-3$ moves on the second. In most cases $n-2$ will be larger than 2. Another exception is when your opponent picks an order 2 element.

Given the reasoning above, we conclude that the program runs in better than $O(n!)$, but not by enough to be considered to run in exponential time. It should also be noted that using automorphisms to eliminate parts of the game tree that the program has to search is helpful; it took nearly 2 days to find a solution for $\mathbb{Z}_{18}$, while the program returned a solution within a few hours for $\mathbb{Z}_{19}$.

In the next section we list the results of running the program on all the groups of order 12 as well as the abelian groups we created matrices for in the previous sections.

5.3 Results

In this section we finally get to test out our algorithm and record some results. Before we sent the groups of order 12 into the machine created in the previous sections, we wanted to make sure it gave results consistent with the literature. We tested our algorithm on $G = \mathbb{Z}_n$ for $n \leq 13$ and for $G = D_n$ for $n = 3, 4$. As expected, our results reconfirmed Isbell's. As discussed previously, when using the algorithm to process $\mathbb{Z}_n$, a traditional matrix representation is not required. For this reason, we were able to determine force wins for $\mathbb{Z}_n$ for $n \leq 20$. Fig. 5.3 gives the updated table of forced wins for $\Gamma(G)$.

Observe that players split $\Gamma(G)$ for $|G| = 12$ with Black winning $\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$, and D_{12}, while White picks up the win for $\mathbb{Z}_{12}$ and A_4. Also, observe that Isbell's conjecture holds for primes $5 < p \leq 19$.

Mentioned earlier was the idea of including additional output to the program, mainly that of movement/placement histories and total sequences played. For the development of strategy, this information could prove very useful. It seems worth noting two curiosities from analyzing these outputs. (1) In $\Gamma(\mathbb{Z}_{2n})$, with $4 \leq n \leq 10$, White has a forced win, but the *only* opening move that guarantees a best play win is $a_1 = n$. A quick look at the table shows that White doesn't have forced wins in $\Gamma(\mathbb{Z}_n)$ for *odd* n. That's right! White only wins $\Gamma(\mathbb{Z}_n)$ for even n, $10 \leq n \leq 20$ (excepting $n = 6, 8$). The curious thing about the above strategy is this: by selecting $x_1 = \frac{n}{2}$, White gives Black the largest possible set of opening moves $(n - 2)$. Also, as we have seen from our work on sequencing abelian binary groups, selecting the unique order 2 element is the quickest way to ensure the game cannot go the length of G. From this point of view, the strategy seems clear: Pick the order 2 element and then play a version of what Conway calls the TweedleDee TweedleDum Strategy [8]. By this I mean White should try to alternate turns by not playing inverses of previously taken moves until there are only a few moves left and then he should have the last move. This is obviously just a superficial connection and I cannot provide an exact play book based on position, but the results cannot be denied: White wins in those groups with a binary element by playing that element first.

Figure 5.2: Winners of $\Gamma(G)$

$\mathbb{Z}_2$:	W	$\mathbb{Z}_3$:	W	$\mathbb{Z}_4$:	W
$\mathbb{Z}_2 \times \mathbb{Z}_2$:	B	$\mathbb{Z}_5$:	W	$\mathbb{Z}_6$:	B
D_3:	W	$\mathbb{Z}_7$:	B	$\mathbb{Z}_8$:	B
$\mathbb{Z}_2 \times \mathbb{Z}_4$:	W	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$:	B	D_4:	B
Q_8:	W	$\mathbb{Z}_9$:	B	$\mathbb{Z}_3 \times \mathbb{Z}_3$:	B
$\mathbb{Z}_{10}$:	W	$\mathbb{Z}_{11}$:	B	$\mathbb{Z}_{12}$:	W
$\mathbb{Z}_2 \times \mathbb{Z}_6$:	B	$\mathbb{Z}_3 \rtimes \mathbb{Z}_4$:	B	D_6:	B
A_4:	W	$\mathbb{Z}_{13}$:	B	$\mathbb{Z}_{14}$:	W
$\mathbb{Z}_{15}$:	B	$\mathbb{Z}_{16}$:	W	$\mathbb{Z}_{17}$:	B
$\mathbb{Z}_{18}$:	W	$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$:	B	$\mathbb{Z}_{19}$:	B
$\mathbb{Z}_{20}$:	W	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$:	W		

Appendix

Here I would like to present the source code I used in finding the solutions I have presented in this paper. The first source code defines the parameters and displays output based on the output of the main program, which is presented second. The programming environment is MATLAB. Comments are provided (using %) to help clarify steps.

```
%SET UP IN MATLAB TO RUN THE PROGRAM.
%HERE WE DEFINE OUR GROUPS AND DISPLAY WHAT WE ARE WORKING WITH.


global seq_count;
seq_count = 0;
global p1win;
p1win = 0;
global p2win;
p2win = 0;
modulus = 12;
% Here we define the matrices <x1,x2,...xn> needed
% to describe the group.
a = [0 i; i 0];
b = [0 -1; 1 -1];


M = {a a^2 a^3 b b^2 a*b a^2*b a^3*b a*b^2 a^2*b^2 a^3*b^2} ;
P = M;


% HP starts with the identity matrix
HP = {eye(2)};
```

```
% index sets for M, HM, P, and IHP (HP doesn't need index set)
% a single vector ranging from 1 to (modulus-1)
IM = 1:modulus-1 ;
IHM = [] ;
IP = 1:modulus-1 ;
IHP = [0] ;

% Instructions for record keeping
disp('Output of Gordon Game using G = Z3 sX Z4
                        generators <a,b> as follows:')
a, b
disp('')
disp('Use the following list for M as a guide to the index set')
disp('M = {a a^2 a^3 b b^2 ab a^2b a^3b ab^2 a^2b^2 a^3b^2}')

% tic/toc used to time the sequence
tic
force_win = GenSeqMat(M,P,HP,IM,IHM,IP,IHP,1,0) ;
toc
if force_win==1
    disp('Player White has a force win!')
else
    disp('Player Black has a force win!')
end;
```

```
%THIS IS THE PROGRAM CODE TO ACTUALLY RUN THE SEARCH.

function force_win = GenSeqMat(M,P,HP,IM,IHM,IP,IHP,printall,
player)
%
% Inputs:
%  M = current Move choices in matrix form
%  P = current Position choices in Matrix form
%  HP = History of Placements used in matrix form
%  IM = index set of the M set
%  IHM = index set of history of Movements used
%  IP = index set of the P set
%  IHP = index set of history of Placements used
%  printall = nonzero to print complete history at end
%  player = current player turn 1-p1, 0-p2

global seq_count ;
global p1win  ;
global p2win  ;

% (locally) found no legal moves yet
found = 0 ;
% (locally) player value comes in at 0
player = ~player;
% (locally) found a force win (p1 = 1, p2 = 2)
force_win = 0;
```

```
% if M is empty we're done with this sequence
% otherwise try all avail moves
if ~isempty(M)
   % for each possible move in M
   for n=1:length(M)
            if force_win == 0 || force_win == 1 && player == 0
            || force_win == 2 && player == 1

                mytry = HP{end}*M{n} ;

               % see if that is a legal position to take
               index = 0 ;
               for j=1:length(P)
                        if mytry==P{j}
                                 index = j;
                        end;
               end;


               if index ~=0  % then found a legal move
            % record that we found a legal move
            found = found+1 ;

            % concatenate this move to the histories
            HMM = [HM IM(n)] ;
```

```
            IHPP = [IHP IP(index)] ;
                    HPP = {HP{1:end} P{index}};

            % remove entry i from M and it's index set
            MM = {M{1:n-1} M{n+1:end}};
                    IMM = [IM(1:n-1) IM(n+1:end)] ;
            % remove the current position from P and it's index set
            PP = {P{1:index-1} P{index+1:end}};
                    IPP = [IP(1:index-1) IP(index+1:end)] ;

            % now continue with the set of next moves
            force_win = GenSeqMat(MM,PP,HPP,IMM,IHMM,IPP,IHPP,printall,
            player) ;
        end ;
           end;

    end ;
end ;

% if no legal moves found we're done with this branch
if found==0
    seq_count = seq_count+1 ;
    disp(['sequence ', num2str(seq_count), ':']) ;

   % if number of moves is even, player 2 wins
    if mod(length(IHM),2) == 0
```

```
        disp 'player 2 won' ;
        p2win = p2win + 1;
            force_win = 2;
    else
        disp 'player 1 won' ;
        p1win = p1win + 1;
            force_win = 1;
    end ;

    % print the histories if directed to do so
    if printall ~= 0
        disp(['Move History: ', num2str(IHM), '
        Moves Avail: ', num2str(IM)]) ;
        disp(['Posn History: ', num2str(IHP), '
        Posns Avail: ', num2str(IP)]) ;
    end ;
end ;
```

Bibliography

[1] L. Allis Searching for Solutions in Games and Artificial Intelligence (Ph. D. thesis) University of Limburg, Maastricht, The Netherlands (1994).

[2] B.A. Anderson, *Sequencings and Starters*, Pacific J. Math. **64** (1976)

[3] B.A. Anderson,A fast method for sequencing low order non-abelian groups, *Ann. Discrete Math.* **34**

[4] B.A. Anderson,Sequencings of dicyclic groups, *Ars Combin.* **23**(1987)

[5] D.S. Archdeacon, J.H. Dinitz, D.R. Stinson and T.W. Tillson, Some new row complete latin squares, *J. Combin. Theory Ser. A***29**(1980)

[6] M. Artin, Algebra, Prentice Hall, New Jersey, 1991.

[7] R.A. Bailey, Quasi-complete latin squares: construction and randomization, J.R. *Stat. Soc. Ser. B Stat. Methodol.***46**(1984)

[8] E.R. Berlekamp, J.H. Conway, and R.K. Guy, *Winning Ways*, vol. **2**, Academic Press, 2003.

[9] S.Dasgupta, C. Papadimitriou, U. Vazirani, Algorithms, McGraw Hill, New York, 2008.

[10] D.S. Dummit and R.M. Foote, Abstract Algebra, Prentice Hall, New Jersey, 1991.

[11] John B. Fraleigh, A First Course In Abstract Algebra Seventh Edition, Pearson Education, Inc., 2003.

[12] R. Friedlander, Sequences in groups with distinct partial products, *Aequationes Math.* **14** (1976) 59-66.

[13] B. Gordon, *Sequences in groups with distinct partial products*, Pacific J. Math **11** (1961)

[14] J. Higham, A product theorem for row-complete latin squares, *J. Combin. Des.***5**(1997)

[15] J. Higham, Row-complete latin squares of every composite order exist, *J. Combin. Des.***6**(1998)

[16] Thomas W. Hungerford, Algebra, Springer-Verlag, New York, 1974.

[17] J. Isbell, *The Gordon game of a finite group*, Amer. Math. Monthly **99** (1991)

[18] J. Isbell, Sequencing certain dihedral groups, *Discrete Math.***85**(1990)

[19] D. Joyner, *Adventures in group theory: Rubik's Cube, Merlin's machine, and other mathematical toys*, Baltimore, Md.: Johns Hopkins University Press, 2002.

[20] A.D. Keedwell, Sequenceable groups: a survery, L.M.S. *Lecture Notes* **49**

[21] Melissa E. McDirmid, Classifying finite groups,Eastern Washington University (2003)

[22] N.S. Mendelsohn, Hamiltonian decompositions of the complete directed n-graph,*Proc. Colloq. Tihany* Academic Press, (1968),

[23] M. A. Ollis, *Sequencible groups and related topics*, Electron. J. Combin., Dynamic Survey(10):34pp, 2002.

[24] E.J. Williams, Experimental designs balanced for the estimation of residual effects of treatments, *Aust J. Sci. Res. A***2**(1949)

[25] `http://en.wikipedia.org/wiki/Permutation_matrix`

[26] Suzanne Rousseau, Quadratic and cubic reciprocity,Eastern Washington University (2012)

[27] P. Li, Sequencing the dihedral groups D_{4k}, Discrete Math. **175** (1997) 271-276

Anthony Frenk was born in Milton, FL, on August 16, 1982, to Susan L. Mason and Arthur G. Frenk Jr. After completing his degree at Milton High School in June 2000, he attended the University of West Florida for two years until 2002. He later attended Eastern Washington University in Cheney, WA, and received his Bachelor of Arts Degree in Mathematics in December 2011. After completing his B.A. he attended Graduate School at Eastern Washington University and received his Masters of Science in Applied Mathematics in August 2013. Anthony lives with his wife and three children in the Spokane, WA area.