Combinatorial Approaches to Minimal Zero Sequences of Finite Abelian Groups, and a Surprising Connection

Zachary J. Turner
University of Houston, Department of Mathematics

Bryson W. Finklea, St. Johns University

ɘɹooM ɨɹɹɘT
University of Washington, Department of Mathematics

August 1, 2003

Abstract

This paper presents a fresh new combinatorial approach to the study of minimal zero sequences of a finite abelian group. We begin by presenting some general algebraic theory aimed at reducing the search space of potential minimal zero sequences for a certain class of groups, as well as describe the optimal algorithm for generating all minimal zero sequences of such a group. We continue by giving a closed form solution for the number of atoms in an infinite family of groups. Then, by introducing the concept of the *dimension class* of an atom in the block monoid of a group, we are able to give a partial description of another infinite family of groups.

Finally, we conclude by making a strong connection between the study of minimal zero sequences and the polynomials of a group which are invariant under a certain class of cyclic variable substitutions.

1 Introduction

1.1 General Introduction

Before we can do anything, we need to get some terminology out of the way.

Definition 1. *Let G be a finite abelian group. A* zero-sequence of G *is a non-empty sequence S of elements of G which sums to zero. If there is no proper subsequence of S which is also a zero-sequence, S is said to be a* minimal zero sequence.

In general, when one wants to sum up two numbers a and b, they would naturally be inclined to write $a + b$. However, in our case, we will usually be summing up many items at once, and it becomes tedious to write the + symbol so many times. For this reason, it will occasionally serve us to write the sequence multiplicatively. In other words, let $S = g_1, g_2, ..., g_k$. For shorthand, we will simply write this as $g_1 g_2 \dots g_k$. Note that it is quite possible an element repeats in the sequence. In this case, in keeping with the multiplicative notation, we will write the *multiplicity* of the element as an exponent. So, for example, the sequence $S = g_1 g_1 g_2 g_2 g_2 g_3$ is written ${g_1}^2 {g_2}^3 g_3$. The reader is warned not to think that we are multiplying things, as what we are really doing is *adding* elements. We just use the multiplicative notation as a shorthand. Care has been taken to make sure that it is always clear from context whether we are using additive or multiplicative notation.

Actually, what we've said about always adding elements is still not quite true. A group has an arbitrary operation, and what we are *really* interested in is sequences which, when "combined" under the operation of the group, result in the *identity* of the group. However, because of the following well-known result from algebra, we can say without loss of generality that any group we're dealing with uses the operation addition, and the identity is in fact 0 as we are familiar with it.

Fundamental Theorem of Finite Abelian Groups[Foo99]. *Let G be a finite abelian group. Then, $\exists n_1, n_2, \dots, n_k \in \mathbb{N}\backslash\{1\}$ with $n_j | n_{j+1}$ such that $G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_k}$.*

When dealing with large collections of objects, it is helpful to give them give them a standard algebraic structure, in order that we can use the entire theory of algebra to deduce results about the items in the collection. As it happens, the set of all zero- sequences of a finite abelian group form a *monoid*.

Definition 2. *A* monoid *is a set G along with a binary operation $\circ$ such that*

1. $\forall a, b \in G, a \circ b \in G$
2. $\exists e \in G$ *such that* $\forall a \in G, a \circ e = e \circ a = a$.

In other words, a monoid can be thought of as an algebraic structure which resembles a group, except for the fact that every element need not have an inverse.

We will denote by $\mathcal{B}(G)$ the set

$$\mathcal{B}(G) \equiv \left\{ g_1, g_2, \ldots, g_t \in G \,\middle|\, \sum_{i=1}^{t} g_i = 0 \right\},$$

and we will call $\mathcal{B}(G)$ the *block monoid of* G. If we consider $\mathcal{B}(G)$ under the operation of sequence union, then $\mathcal{B}(G)$ forms a monoid. It is left as an exercise to the reader to verify this.

The algebraist will notice that the *atoms* or *irreducibles* of $\mathcal{B}(G)$ are exactly the minimal zero sequences of G, and we will use these three terms interchangeably.

1.2 Exploring the Davenport Constant

In what follows, we pursue two main paths in the atomic theory of block monoids, and as a bonus we present a surprising and remarkable connection with invariant theory of finite abelian groups. In Section 2, we further explore the long-studied *Davenport constant*, or the length of the longest atom of $\mathcal{B}(G)$. We determine the Davenport constant for ${\mathbb{Z}_2}^k \oplus \mathbb{Z}_6$ for $k = 4, 5, 6, 7$, ${\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10}$, and ${\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6$. Additionally, we strengthen existing upper bounds on $D(G)$ for the general group G, and we provide better upper bounds for D on a certain family of groups, strengthening those given by [Maz92].

Much of the work which will be presented was made possible by the use of a computer program designed for computing minimal zero sequences of finite abelian groups, and its algorithm is presented in this section. We also give some ideas on how to improve the speed of the algorithm by orders of magnitude.

In Section 2, we attack the question of the structure and number of atoms of all lengths in $\mathbb{Z}_k$, ${\mathbb{Z}_2}^n$, and ${\mathbb{Z}_3}^n$. We provide a complete description of $\mathbb{Z}_k$ and partial descriptions of ${\mathbb{Z}_2}^n$ and ${\mathbb{Z}_3}^n$.

The surprising connection to invariant theory is discussed in closing in Section 3. Strom[Str48] calculated the number of invariant polynomials of $\mathbb{Z}_n$ up to $n = 10$, and we extend this by leaps and bounds, presenting the table all the way up to $n = 64$. We then show how counting minimal invariant polynomials of a group is equivalent to counting minimal zero sequences, and we finish by extending Strom's work to the general case of $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ and making the same connection to minimal zero sequences. We also give a similar table for the general case, up to $\mathbb{Z}_7 \oplus \mathbb{Z}_7$.

1.3 Atom Counting 101

While research in block monoids is fairly active, one area that is still relatively uncharted territory involves *counting* the number of atoms in the block monoid of a group. Section 3 provides foundation for such study.

We start by pointing out that the existence of atoms of every length less than the Davenport constant $D(G)$ is clear. An atom of length $D - 1$ is constructed by combining any two elements in a Davenport sequence, and one of length

$D-2$ by combining any two additional elements. Proceeding in this fashion, it is clear we can construct atoms of length $D-3, D-4, ..., 1$. This fact not only gives some familiarity with the non-Davenport atoms but will also be assumed in the final formulas given in section 3.

Secondly, it is well known that the number of Davenport sequences for cyclic groups of order n is equal to $\phi(n)$, the Euler Phi function [Wri80] (Do not confuse this with the Davenport constant itself. $\phi(n)$ is the *number* of sequences which have length equal to the Davenport constant). For example, in Z_6, the Davenport sequences are $1^6, 5^6$ (2^6 is not a Davenport sequence since it is not even minimal). It is interesting to note that when n is prime, then the number of Davenport sequences is $n-1$ since $\phi(n)$=$n-1$ when n is prime.

It is natural to ask (but difficult to answer) about non-Davenport atoms, and about non-cyclic groups. In Section 3 we tackle this very question, and solve the problem of counting the number of atoms in $\mathcal{B}({\mathbb{Z}_2}^n)$ and the atoms of certain types in $\mathcal{B}(\mathbb{Z}_n)$ and $\mathcal{B}({\mathbb{Z}_3}^n)$.

Notice that by partitioning atoms into classes where two atoms are in the same class whenever they have the same length, we obtain an equivalence relation[Foo99]. We will make use of this fact, and we will refer to the equivalence classes as *length classes*. Most of the atom counting in Section3 partitions the atoms by length class and counts the number of atoms in some or all of these classes. We are able to solve $\mathcal{B}({\mathbb{Z}_2}^n)$ completely, and in $\mathcal{B}(\mathbb{Z}_n)$ and $\mathcal{B}({\mathbb{Z}_3}^n)$ we count some of the length classes and give ideas on how to count the others.

The reason for partitioning the atoms into such classes is that it actually turns out to be easier to count them when they are organized by length. Indeed, we state a conjecture that this has to do with the varying behavior of different isomorphism classes (we formally state this conjecture later). The reason that this partition is sufficient to count all atoms in the case of $\mathcal{B}({\mathbb{Z}_2}^n)$ is because each element of this group is its own inverse and this fact leads to a significant simplification in the counting process. In other groups, however, this is not true, and even in $\mathcal{B}(\mathbb{Z}_n)$ and $\mathcal{B}({\mathbb{Z}_3}^n)$, partitioning the atoms into length classes alone is insufficient. More precisely, a length class alone is not specific enough to define an isomorphism class, so we further partition atoms by their *multiplicity classes*.

Multiplicity classes describe the multiplicity of the elements in addition to the overall length and are defined by the construction that follows: order the elements from highest to lowest multiplicity. For each distinct element in this ordering, pick the next lowest symbol of your choosing (we will use the Roman alphabet exclusively). Write this letter as raised to the k'th power, where k is the multiplicity of the distinct sequence element you are currently looking at. Repeat this process for the remaining elements in the sequence, and you are left with a string representing the multiplicity class. For example, the atom $1 \cdot 1 \cdot 1 \cdot 2 \cdot 3 \cdot 3$ in $\mathcal{B}(Z_{10})$ is rearranged $1 \cdot 1 \cdot 1 \cdot 3 \cdot 3 \cdot 2$ and represented a^3b^2c. The particular atom is then a member of this multiplicity class. Multiplicity classes are more specific than length classes since we get many more partitions this way, and hence proofs relying on multiplicity classes tend to be easier than those relying on length classes. It is interesting to note that all atoms in $\mathcal{B}({\mathbb{Z}_2}^n)$

are composed of all distinct elements. So in a sense, we are also counting by multiplicity classes in ${\mathbb{Z}_2}^n$, it is just that they do not further partition the length classes as they do in other $\mathcal{B}(G)$.

Section 3.1 gives proofs for the number of atoms in $\mathcal{B}(\mathbb{Z}_n)$ for some multiplicity classes, and this is as far as we partition $\mathcal{A}(\mathcal{B}(\mathbb{Z}_n))$. However, for $\mathcal{B}({\mathbb{Z}_3}^n)$, we are able to introduce the concept of a *dimension classes* and partition the atoms into even finer partitions. Since the term dimension class is specific to section 3.3, it's exact definition will not be presented until we reach that section. A general equation is given for the number of atoms in $\mathcal{B}({\mathbb{Z}_3}^n)$ that is reminiscent of the formula for the number of atoms in $\mathcal{B}({\mathbb{Z}_2}^n)$, but it is significantly more complicated, and we only determine its values for certain dimension classes. In addition, this knowledge gives us explicit formula for atoms of lengths $1, 2, ..., 6$.

To this work on counting atoms is appended Section (reference), which gives select theorems restricting the available multiplicity classes for larger families of groups, including $\mathcal{B}({\mathbb{Z}_p}^n)$, p prime. These are in the same spirit as the first three subsections which use the ideas of structure in their counting, and this connection is indicated in detail in the conclusion of the paper.

2 Bounded By The Davenport Constant

2.1 Structure of Davenport Sequences

In this section we aim to determine the structure of Davenport sequences in groups where $D(G) \neq M(G)$. We do this in two ways. First we restrict the multiplicities of certain elements appearing in Davenport sequences, and secondly we fix by group automorphisms many elements appearing in the sequence. At the end of the section we use these results along with a computer program (described in section 2.5) to determine the Davenport constant of several groups for which it was previously unknown.

We will use the following two definitions extensively througout this section. We define a method of considering irreducibles in one group as irreducibles in a smaller group for which more may be known about the structure of Davenport sequences. We also define a means for calling irreducibles equivalent in structure, thus if we are only interested in the length of the longest irreducible we need not consider irreducibles which are equivalent.

Definition 1. *Let $G = \mathbb{Z}_n \oplus G'$. Then a* reduction *from $\mathcal{B}(G)$ into $\mathcal{B}(G')$ is an epimorphism $\phi : \mathcal{B}(G) \to \mathcal{B}(G')$ where $\phi(B)$ is the block $B' \in \mathcal{B}(G')$ obtained by dropping the first coordinate from every element of B. $\phi(B)$ will be called the* reduction of B into $\mathcal{B}(G')$.

Definition 2. *Let $g_1, g_2 \in G$. We will call g_1 and g_2* equivalent *if $\exists \phi : G \to G$ a group automorphism such that $\phi(g_1) = g_2$. We will say that two blocks $B_1, B_2 \in \mathcal{B}(G)$ are equivalent if $\exists \phi' : G \to G$ a group automorphism such that $\phi(B_1) = B_2$.*

Let $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ and let $B \in \mathcal{B}(G)$. Suppose $G \simeq \mathbb{Z}_n \oplus G'$ for some n and G. We will examine B', the reduction of B into G'. Since B is a zero-sequence, the sum of the elements of B is zero in each coordinate and therefore B' is also a zero-sequence. In many cases, even when B is an irreducible, B' may factor. In fact, since $D(G) \geq D(G') + n - 1$ [vEB69], B is a Davenport sequence implies that B' must necessarily factor. On the other hand, if B' is irreducible, B must be irreducible since a factorization of B would induce a factorization of B' under the reduction. If we know how B' factors in G' we can infer structure about B in G. Theorem 2.1 makes use of this to examine blocks containing elements with maximal multiplicity (multiplicity one less than the element's order). The Corollary to Theorem 2.1 uses this theorem to make restrictions on the multiplicity of elements in Davenport sequences of groups where $D(G) \neq M(G)$.

Theorem 2.1. *Let $G = \mathbb{Z}_n \oplus G'$ and $q = (1, 0, \ldots, 0)$. Consider $B \in \mathcal{A}(\mathcal{B}(G))$ such that B is equivalent to $q^{n-1}B'$ for some sequence B'. Then the reduction of B' into G' must be irreducible.*

Proof. Suppose to the contrary that the reduction of B' factors in G'. Then this factorization partitions B' into non-empty parts each of which sum to an element of the form $(x, 0, \ldots, 0) \in G$. Now, if $x = 0$ for any part, then this is a zero-subsequence of B, a contradiction since $B \in \mathcal{A}(G)$. So therefore $x \geq 1$, and a part which sums to $(x, 0, \ldots, 0)$ along with q^{n-x} sums to $(0, 0, \ldots, 0) \in G$ producing another contradiction. □

Corollary. *Let $G = \mathbb{Z}_n \oplus G'$ and $q = (1, 0, \ldots, 0)$. If $D(G) > D(G') + n - 1$, then no Davenport sequence contains an element equivalent to q with multiplicity $n - 1$.*

Theorem 2.2. *Let $G \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \mathbb{Z}_p \oplus \mathbb{Z}_{pm} \simeq {\mathbb{Z}_p}^{k+1} \oplus \mathbb{Z}_m$ where p is prime. Then every maximal length irreducible is equivalent to one containing the elements*
${e_1}^* = (1, 0, \ldots, 0, x_1), {e_2}^* = (0, 1, 0, \ldots, 0, x_2), \ldots, {e_{k+1}}^* = (0, 0, \ldots, 1, x_{k+1})$ where $x_i \in [0, m-1]$ for each i.

Proof. Consider a Davenport sequence $B \in \mathcal{B}(G)$ and consider a largest set of elements in B that are linearly independent in the first $k+1$ coordinates. By a change of basis in ${\mathbb{Z}_p}^{k+1}$ these elements are equivalent to ${e_1}^*, {e_2}^*, \ldots, {e_i}^*$ where the last coordinate of each of the e's lie in $[0, m-1]$ for some $1 \leq i \leq k+1$. Suppose to the contrary that $i < k+1$. Then after the above change of basis none of the elements of B may have a non-zero entry in the $i+1$-st coordinate since this element could have been added to the set of elements considered and still be linearly independent in the first $k+1$ coordinates, contradicting that the set was maximal. But then a longer atom of $\mathcal{B}(G)$ can be found by adding $(0, 0, \ldots, 0, 1, 0, \ldots, 0, 0)$ to B and modifying one element of B to have $i+1$-st coordinate $p-1$ instead of 0. This contradicts that B was a Davenport sequence. □

2.2 Calculating the Davenport Constant

We use a computer program (described in section 2.5) to determine the Davenport constant of several groups by searching over all possible zero-sequences. For large groups G the number of zero-sequences of length m becomes quite large, approximately $|G|^m$, many of which are not irreducible. Thus, without reducing the search space, it quickly becomes unreasonable to search all zero-sequences to determine the longest irreducible. Theorem 2.1 reduces the search space by restricting the multiplicity of certain elements. Theorem 2.2 reduces the search space to searching particular cases where many elements of the sequence are fixed. These reductions alone are enough to examine groups much larger than before and have been used to determine $D(G)$ for ${\mathbb{Z}_2}^k \oplus \mathbb{Z}_6$ for $k = 4, 5, 6, 7$, ${\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10}$, and ${\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6$ by searching the following cases:

${\mathbb{Z}_2}^n \oplus \mathbb{Z}_6$:
It has been shown that $D(H \oplus K) \geq D(H) + D(K) - 1$ for groups H and K [vEB69]. Thus, we know $D({\mathbb{Z}_2}^n \oplus \mathbb{Z}_6) \geq D(|{Z_2}^{n-1} \oplus \mathbb{Z}_6) + 1$, so the question remains as to when the inequality is strict. For $n = 1, 2$, and 3 there is equality. It was shown in 1969 by P.C. Baayen that $D(\mathbb{Z}_2^4 \oplus \mathbb{Z}_6) > M(G)$ and this is the group with smallest order such that $D(G) \neq M(G)$. We will consider now n for which $D(\mathbb{Z}_2^n \oplus \mathbb{Z}_6) > D(\mathbb{Z}_2^{n-1} \oplus \mathbb{Z}_6) + 1$. Then by Corollary 2.1 no element of order 2 occurs in a Davenport sequence (since all elements of order 2 are equivalent). Write $G \simeq \mathbb{Z}_2^{n+1} \oplus \mathbb{Z}_3$ and then by Theorem 2.2 a Davenport sequence will contain the elements $(1, 0, 0, \ldots, 0, x_1)$, $(0, 1, 0, \ldots, 0, x_2)$, $\ldots$, $(0, 0, \ldots, 1, x_{n+1})$ where each $x_i \in \{1, 2\}$ (since there are no elements of order 2, $x_i \neq 0$.) By a change of basis in the $\mathbb{Z}_2^n$ coordinates, it does not matter which $x_i = 1$ only the number of x_i, so all Davenport sequences are equivalent to one with the first m x_i equal to one and the remaining equal to two. By a further automorphism which sends the last coordinate to its inverse, all Davenport sequences are equivalent to one containing the elements $(1, 0, \ldots, 0, x_1), (0, 1, 0, \ldots, 0, x_2), \ldots, (0, 0, \ldots, 0, 1, x_{n+1})$ where $x_1 = x_2 = \cdots = x_m = 1$ and $x_{m+1} = x_{m+2} = \cdots = x_{n+1} = 2$ for some $\lceil \frac{n+1}{2} \rceil \leq m \leq n + 1$. There are $\lfloor \frac{n+1}{2} \rfloor + 1$ cases to consider, one for each i. For each case, $n + 1$ of the elements in the sequence are known. Thus, it remains to use the computer program to search for the remaining elements to determine the longest such zero-sequence containing these elements. This search can further be reduced by restricting the multiplicity of elements. By Corollary 2.1, elements of order three can have multiplicity at most one and elements of order six can have multiplicity at most four. Using the program and these restrictions we find $D({\mathbb{Z}_2}^4 \oplus \mathbb{Z}_6) = 11, D({\mathbb{Z}_2}^5 \oplus \mathbb{Z}_6) = 12, D({\mathbb{Z}_2}^6 \oplus \mathbb{Z}_6) = 13$, and $D({\mathbb{Z}_2}^7 \oplus \mathbb{Z}_6) = 15$.

${\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10}$:
If $D({\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10}) > M({\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10})$ then by Corollary 2.1 there will be no elements of order two in a Davenport sequence, all elements of order five will have multiplicity at most three, and all elements of order ten have multiplicity at most eight in a Davenport sequence. Since ${\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10} \simeq {\mathbb{Z}_2}^5 \oplus \mathbb{Z}_5$, by Theorem

2.2 every Davenport sequence is equivalent to a Davenport sequence containing the elements $(1,0,0,0,0,x_1)$, $(0,1,0,0,0,x_2)$, $(0,0,1,0,0,x_3)$, $(0,0,0,1,0,x_4)$, and $(0,0,0,0,1,x_5)$ where $x_i \in \{1,2,3,4\}$. So there are 4^5 cases to consider. Consider two sets of values for the five elements, $\{x_1,x_2,x_3,x_4,x_5\}$ and $\{x_1',x_2',x_3',x_4',x_5'\}$. If there is an automorphism of $\mathbb{Z}_5$ which maps the elements of one set to the elements of the other, then by a change of basis in ${\mathbb{Z}_2}^4$ it can be shown that the blocks are equivalent. Thus it is only necessary to consider sets of x_i's which are not automorphic to other sets. Thus there are only 14 cases to consider. The computer program is then used to search these cases for the longest irreducibles containing these elements. We find $D({\mathbb{Z}_2}^4 \oplus \mathbb{Z}_{10}) = 15$.

${\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6$:
If $D({\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6) > M({\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6)$ then by Corollary 2.1 the element of order two does not appear in a Davenport sequence, all elements of order three have multiplicity at most one, and all elements of order six have multiplicity at most four. Since ${\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6 \simeq {\mathbb{Z}_3}^4 \oplus \mathbb{Z}_3$, by Theorem 2.2 all Davenport sequences are equivalent to a Davenport sequence containing the elements $(1,0,0,0,x_1),(0,1,0,0,x_2),(0,0,1,0,x_3)$, and $(0,0,0,1,x_4)$ where $x_i \in \{0,1\}$. Again it does not matter which x are one and which are zero, only the number of ones and zeros. Thus there are five cases to consider. Using the computer program, we searched these five cases to find the longest irreducibles. We find $D({\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6) = 13 > M({\mathbb{Z}_3}^3 \oplus \mathbb{Z}_6) = 12$.

2.3 Upper Bound for the Davenport Constant

Let us turn our attention now to bounding the Davenport constant for arbitrary groups. Currently the best upper bounds are

$$D(G) \leq |H| + |K| - 1 \tag{1}$$

where $G = H \oplus K$ and $|H| \mid |K|$ [Ols69],

$$D(G) \leq n_i(1 + \ln |G'|) \tag{2}$$

where $G \simeq \mathbb{Z}_{n_i} \oplus G'$ [Kru69], and

$$D(G_{n,k}) \leq 2 \cdot k(1 + (n-1)\ln 2) + M(G_{n,k}) \tag{3}$$

where $G_{n,k} = {\mathbb{Z}_2}^n \oplus \mathbb{Z}_k$ with k odd [Maz92].

In Theorem 2.3 we demonstrate an upper bound for $D(G)$ which, although it seems quite large, beats these previous bounds in many cases.

Theorem 2.3. *Let $G \simeq H \oplus K$. Then $D(G) \leq D(H)D(K)$.*

Proof. For every $g \in G, g = (g_1, g_2)$ where $g_1 \in H$ and $g_2 \in K$. Consider a Davenport Sequence B of length D and let $B = B_1 \cup B_2 \cup \cdots \cup B_k$ where the sequence of first coordinates of the elements of B_i form an irreducible of $\mathcal{B}(H)$ for each i. Then $|B_i| \leq D(H)$ for each i. Let $b_i \in K$ be the second coordinate of the

sum of the elements of B_i (the first coordinates sum to zero). Then the sequence of b_i's form a zero-sequence in $\mathcal{B}(K)$. If this sequence factors, then the partition of the corresponding B_i's would be a zero-subsequence of B contradicting that B is irreducible. Therefore this sequence is irreducible in K. Therefore $k \leq D(K)$. Then $D = |B| = |B_1| + |B_2| + \cdots + |B_k| \leq D(H) \cdot k \leq D(H)D(K)$. □

Corollary. $D({\mathbb{Z}_2}^n \oplus \mathbb{Z}_6) = D({\mathbb{Z}_2}^{n+1} \oplus \mathbb{Z}_3) \leq 3n + 6$.

Proof. Let $G = {\mathbb{Z}_2}^n \oplus \mathbb{Z}_6 \simeq {\mathbb{Z}_2}^{n+1} \oplus \mathbb{Z}_3$. Let $H = {\mathbb{Z}_2}^{n+1}$ and $K = \mathbb{Z}_3$, then by Theorem 2.3, $D(G) \leq D({\mathbb{Z}_2}^{n+1})D(\mathbb{Z}_3) = 3(n + 2)$. □

Consider $G = {\mathbb{Z}_2}^n \oplus \mathbb{Z}_6$ along with the previous three bounds. For the first bound, we may write $G \simeq ({\mathbb{Z}_2}^m) \oplus ({\mathbb{Z}_2}^{n+1-m} \oplus \mathbb{Z}_3)$ where $0 \leq m \leq n + 1 - m$. Then we know $D(G) \leq 2^m + 3 \cdot 2^{n+1-m} - 1$. However, $2^m + 3 \cdot 2^{n+1-m} - 1 \geq 3 \cdot 2^{n+1-\frac{n+1}{2}} \geq 3 \cdot 2^{\frac{n+1}{2}}$. This bound grows exponentially, and for $n \geq 5$ is larger than $3(n + 2)$. For the second bound, $n_i = 6$ and so $D(G) \leq 6(1 + \ln 2^n) = 6(1 + n \cdot \ln 2) \approx 6 + 4n$ which is strictly greater than our bound. And finally, with the final bound, $k = 3$ so $D(G) \leq 2 \cdot 3(1 + (n - 1) \ln 2) + n + 6 = (6 \cdot \ln 2 + 1)n + (12 - 6 \cdot \ln 2) \approx 5n + 7$ which is also strictly greater than our bound.

Corollary. $D({\mathbb{Z}_3}^n \oplus \mathbb{Z}_6) \leq 2(2n + 3)$.

Proof. Write $G \simeq {\mathbb{Z}_3}^{n+1} \oplus \mathbb{Z}_2$ and let $H = {\mathbb{Z}_3}^{n+1}$ and $K = \mathbb{Z}_2$, then $D(G) \leq 2(2(n + 1) + 1) = 4n + 6$. □

Again this bound beats the previous three bound. The first gives rise to $D(G) \leq 3^m + 2 \cdot 3^{n+1-m} - 1$ and since $3^m + 2 \cdot 3^{n+1-m} - 1 \geq 2 \cdot 3^{\frac{n+1}{2}} - 1$ which is exponential and greater than $4n + 6$ for $n \geq 5$. The second bound gives rise to $D(G) \leq 6(1 + \ln 3^n) = 6(1 + n \cdot \ln 3) \approx 6.5n + 6$. And the third bound does not apply to this case.

Corollary. *Let $G = {\mathbb{Z}_2}^n \oplus \mathbb{Z}_{2k}$ where k is odd. Then $D(G) \leq k(n + 2)$.*

This compares to $k \cdot 2^{\frac{n+1}{2}} - 1$ of the first bound which is always greater than $k(n + 2)$ for $n \geq 5$, $2k(1 + \ln 2^n) \approx 1.38kn + 2k$ from the second bound, and $2k(1 + (n - 1) \ln 2) + n + 2k \approx (1.38k + 1)n + 2.6k$ which is strictly greater than our bound.

Corollary. *Let $G = {\mathbb{Z}_3}^n \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Then $D(G) \leq 3(2n + 1)$.*

This first gives rise to the bound $D(G) \leq 3^m + 4 \cdot 3^{n-m} - 1$ which is at least as large as $4 \cdot 3^{n-m} \geq 4 \cdot 3^{\frac{n}{2}}$ which is larger than $6n + 3$ for $n \geq 2$. The second yields the bound $D(G) \leq 6(1 + \ln(2 \cdot 3^{n-1}) = 6(1 + \ln 2 + n - 1 \ln 3) \approx 6.59n + 3.56$ which is larger than our bound of $6n + 3$. And the third bound does not apply.

2.4 A lower bound on $D(G) - M(G)$

Definition 3. *Let $G = {\mathbb{Z}_2}^n \oplus \mathbb{Z}_6$ and define $d_n = D(G) - M(G)$.*

Since $D({\mathbb{Z}_2}^n \oplus \mathbb{Z}_6) \geq D({\mathbb{Z}_2}^{n-1} \oplus \mathbb{Z}_6) + 1$ and $M({\mathbb{Z}_2}^n \oplus \mathbb{Z}_6) = M({\mathbb{Z}_2}^{n-1} \oplus \mathbb{Z}_6) + 1$, then $d_n \geq d_{n-1}$. We previously showed that $d_n \geq 1$ when $n \geq 4$ and $d_n \geq 2$ when $n \geq 7$. In this section we will construct explicit zero-sequences to demonstrate $d_n \geq 3$ for $n \geq 35$, $d_n \geq 4$ for $n \geq 56$, and $d_n \geq 6$ for $n \geq 165$. If we use the previously known lower bound for d_n of $\log_2 n - 6$ [Maz92] we would need an n of 512 to achieve $d_n \geq 3$, $n = 2^10$ for $d_n \geq 4$, and $n = 2^12$ for $d_n \geq 6$.

Definition 4. *Let $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ and consider $x = (x_1, x_2, \ldots, x_k) \in G$. Define the* value of x, *$v(x) = \sum_{i=1}^{k} x_i \in \mathbb{Z}$.*

Let $G = \mathbb{Z}_2^n \oplus \mathbb{Z}_6 \simeq \mathbb{Z}_2^{n+1} \oplus \mathbb{Z}_3$. Let ${e_i}^*$ denote the element of ${\mathbb{Z}_2}^{n+1} \oplus \mathbb{Z}_3$ with a 1 in the i'th coordinate, a 1 in the last coordinate, and 0's everywhere else. Consider a zero-sequence $B = {e_1}^* {e_2}^* \ldots {e_{n+1}}^* q_1 q_2 \ldots q_m$, where $q_1, q_2, \ldots, q_m \in G$. Since no subsequence of the ${e_i}^*$'s is a zero- sequence, a zero-subsequence of B must contain some subset of the q_i's.

Claim 2.1. *Consider a subsequence Q of the q_i's and let*

$$q = (x_1, x_2, \ldots, x_{n+1}, y) = \sum_{q_j \in Q} q_j \in G.$$

Then there is a zero-subsum of B containing Q and elements of ${e_j}^*$, $j = 1, 2, \ldots, n+1$ if and only if $v(q) \equiv 0 \mod 3$.

Proof. Suppose $v(q) \equiv 0 \mod 3$. Consider the subsequence containing the elements of Q and ${e_i}^*$ for every i such that $x_i = 1$. Then the sum of this sequence is zero in the first $n+1$ coordinates. The last coordinate of the sum is y plus 1 for each ${e_i}^*$ in the subsequence, modulo 3, which is, y plus the number of nonzero x_i modulo 3 and this is $v(q) \mod 3 = 0$, and so the sequence is a zero-subsum of B.

Conversely, suppose there is a zero-subsum containing the elements of Q and some elements of the ${e_i}^*$'s. ${e_i}^*$ is an element of the zero-subsum if and only if $x_i = 1$ since no other ${e_j}^*$ has a nonzero entry in the i-th coordinate. Each ${e_i}^*$ adds a 1 to the last coordinate of the sum. The last coordinate is y plus the number of ${e_i}^*$'s which is y plus the number of nonzero x_i's which is $v(q)$ and therefore $v(q) \mod 3 = 0$. □

We will use the following construction to create irreducibles for certain n. Construct a table with m rows and $\binom{m}{k}$ columns. Fill in the table so that each column has k 1's and the remaining entries 0 and so each column is distinct. Let the q_i have first and last coordinate 1 and remaining coordinates corresponding to the i-th row for $1 \leq i \leq m$.

Claim 2.2. *Let Q be a subset of the q_i's containing r elements. Then*

$$v(q) = (r \pmod 2) + (r \pmod 3) + \sum_{j=1}^{\alpha} \binom{r}{2j+1} \binom{m-r}{k-(2j+1)}$$

where $\alpha = \min\{k, \lfloor \frac{r-1}{2} \rfloor\}$.

Proof. Let $q = (x_1, x_2, \ldots, x_{n+1}, y) = \sum_{q_i \in Q} q_i \in G$. Each of the r elements adds a 1 to x_1 and y, so $x_1 = (r \mod 2)$ and $(y = r \mod 3)$. $x_i = 1$ whenever an odd number of the k choosen elements in the i-th row fall within the r elements of the subset. That is to say, for every way of choosing an odd number at most k from the r elements and the remaining elements to make k from the $m - r$ elements not in the set, a 1 is added to $v(q)$. Therefore $v(q)$ is as claimed. □

We will use the general construction above to demonstrate several choices for m and k so that $v(q) \not\equiv 0 \mod 3$ for all subsets of r elements, $1 \leq r < m$.

Claim 2.3. *$D(\mathbb{Z}_2{}^{35} \oplus \mathbb{Z}_6) \geq 44$ and so $d_n \geq 3$ for $n \geq 35$.*

2.5 The Algorithm

We will close this section by presenting the algorithm which was used to calculate the minimal zero sequences. In essence, what this algorithm actually does is construct *zero-free sequences*. In other words, it constructs sequences which are guaranteed to have no zero-subsum. It is a recursive algorithm which, at each step, appends an element to the end of the sequence, and then updates the subsums and determines which elements are no longer available. It then recurses again, and the algorithm repeats like this. In pseudocode:

```
GenerateZeroFreeSequences(curSequence, Forbidden)
{
    MZS=curSequence
    MZS.AddToBack(Inverse(SequenceSum(MZS)))
    SaveSequence(MZS)
    Avail = EntireGroup\Forbidden
    while(Avail≠ ∅)
    {
        k=min{Avail}
        Avail = Avail\{k}
        Subsums = {k} ∪ ({k} + Subsums)[1] ∪ Subsums
        Forbidden = Inverses(Subsums)
        curSequence.AddToBack(k)
        GenerateZeroFreeSequences(curSequence, Forbidden)
        curSequence.RemoveLastItem()
    }
}
```

[1]This is the traditional definition of set addition. In other words, $A + B = \{\, a + b \mid a \in A,\ b \in B \,\}$

3 Counting Atoms in Block Monoids

The most time in this section has been spent on the frontier that is the atoms of $\mathcal{B}({\mathbb{Z}_3}^n)$, presented in Section 3.3. Section 3.2 is a good introduction to the style of argument used in Section 3.3.

Keep in mind that we're counting atoms of the block monoid (and hence minimal zero sequences of a group) when you begin reading Section 4. As we will show in that section, counting minimal zero sequences of a group is identical to answering questions about invariant theory, so while the question of counting atoms is interesting in it's own right, it is interesting for other reasons as well. See Table 1 for a list of formulas.

3.1 Counting Atoms in $\mathcal{B}(\mathbb{Z}_n)$

Let us start at the beginning. The zero element is the one atom of length 1 in $\mathcal{B}(\mathbb{Z}_n)$, and this is analogously true for any $\mathcal{B}(G)$. The number of atoms of length two in $\mathcal{B}(\mathbb{Z}_n)$ is shown in the following theorem.

Theorem 3.1. *There are $\lceil \frac{n-1}{2} \rceil$ atoms of length two for cyclic groups.*

Proof. Atoms of length two consist of elements and their inverses. For n even, $\frac{n}{2}$ is its own inverse. Otherwise, elements have inverses distinct from themselves. □

This theorem is extended in Theorem 3.7. With an equally simple proof, the formula is given for the number of atoms in the block monoid over *any* finite abelian group.

As stated in the introduction Section 1.3, the number of Davenport sequences in $\mathcal{B}(\mathbb{Z}_n)$ is known to be $\phi(n)$. The following theorem uses the idea of repeatedly combining pairs of elements in the Davenport sequence to determine multiplicity classes that have the same number of atoms as the number of Davenports, that is, the number of atoms in the multiplicity class a^n.

Theorem 3.2. *In $B(Z_n)$, there are the same number of Davenport sequences a^n as there are minimal sequences in each of the multiplicity classes*

$$a^{n-x}b, \text{ where } n \geq 2(x+1), x \geq 2$$

Proof. Every such $a^{n-x}b$ has a corresponding Davenport sequence a^n where a is some fixed element of maximal order, and $b = a^x$. Therefore, there are at least as many; we must show there are only this many. If so, there must be a fixed a_1 with ${a_1}^{n-x}b$ an atom but ${a_1}^n$ not an atom. Such a_1 has order $s \leq \frac{n}{2}$ because it must have order that divides n. Then, $n - x \leq s - 2$, else we would have either a zero-subsum ${a_1}^s$ or the atom would be of that form. This implies $n - x \leq \frac{n}{2} - 2 \Rightarrow n \leq 2(x-2)$, which contradicts our assumption. □

The reader is encouraged to check the conclusion of this paper for ideas and conjectures in this area. As in $\mathcal{B}({\mathbb{Z}_3}^n)$, atom counting in $\mathcal{B}(\mathbb{Z}_n)$ is now fertile ground, even for a reader with limited background in algebra.

3.2 Counting All Atoms in $\mathcal{B}(\mathbb{Z}_2{}^n)$

$\mathcal{B}(\mathbb{Z}_2{}^n)$ is complete and short. Furthermore, we have a place in our hearts for $\mathcal{B}(\mathbb{Z}_2{}^n)$ since it was the block monoid that first captured us into atom counting and away from our previous endeavor which had been to characterize monoids through various graph models. Although the graphs do *not* appear in this paper, their fruits are scattered throughout.

Theorem 3.3 plays the role of preparing the reader's mind for the web to come in Section 3.3. $\mathcal{B}(\mathbb{Z}_2{}^n)$ is the most accessible, but also the least interesting because it provides no further study.

The method of choosing the elements in the following theorem is reminiscent of the computer algorithm presented in section 2.5. One difference is that the algorithm had a built-in ordering of the elements to guard against counting repetitions. This theorem methodically counts all permutations and then divides out by the number of them at the end.

Theorem 3.3. *The number of atoms of length m, $m \geq 2$, in $\mathcal{A}(\mathcal{B}(\mathbb{Z}_2{}^n))$ is* $\frac{\prod_{i=0}^{m-2} 2^n - 2^i}{m!}$.

Proof. Consider an atom $a_1a_2...a_m$ of length m in $\mathcal{B}(\mathbb{Z}_2{}^n)$. The number of these atoms is found by determining the number of choices, or number of available elements, for each of the first $m-1$ a_i. There will be one choice for the final element a_m, the inverse of the sum of all the other elements and never a part of a proper zero subsum. There are 2^n-1 available choices for a_1, all the elements in the group but the zero element, herein denoted 0. There are 2^n-2 choices for a_2, all but 0 and a_1, and 2^n-4 choices for a_3, all but 0, a_1, a_2, and $x = (a_1a_2)$.

In general, elements are unavailable for a choice if they would produce a zero subsum with a subset of the elements that have come before. In the present case $\mathbb{Z}_2{}^n$, elements are their own inverses and any element equal to a sum of elements before it produces a zero subsum with those elements. In any group, 0 produces its own zero subsum. Therefore, the number of elements unavailable for the i^{th} choice is $\sum_{j=0}^{i-1} \binom{i-1}{j} = 2^{i-1}$, and the number available $(2^n - 2^{i-1})$. The number of ways to choose an atom is the product of the choices for the individual element: $\prod_{i=1}^{m-1} 2^n - 2^{i-1} = \prod_{i=0}^{m-2} 2^n - 2^i$. Since there are all possible repetitions by permutation of the m elements in this count, the expression is divided by $m!$, $\frac{\prod_{i=0}^{m-2} 2^n - 2^i}{m!}$.

□

Corollary. *A simple summation of lengths $m \geq 2$ added to 1 to account for the zero element atom of length $m = 1$ gives the total number of atoms in $\mathcal{B}(\mathbb{Z}_2{}^n)$*

as

$$\sum_{j=2}^{n+1} \frac{\prod_{i=0}^{j-2} 2^n - 2^i}{j!} + 1.$$

It is noted only here and in passing that when $m = 3$, the expression reduces itself to the Gaussian binomial coefficient[2] $\begin{bmatrix} n \\ 2 \end{bmatrix}_2$ [Ros00].

3.3 Counting Atoms in $\mathcal{B}({\mathbb{Z}_3}^n)$

The case of the atoms of $\mathcal{B}({\mathbb{Z}_3}^n)$ is the most interesting because it provides a gateway to the counting and classifying of atoms in the block monoids over more complicated finite abelian groups. For instance, $\mathcal{B}(\mathbb{Z}_p^n)$ for prime p and $\mathcal{B}(\mathbb{Z}_l^n)$ for integer l are close in structure to $\mathcal{B}({\mathbb{Z}_3}^n)$. For beginning work in $\mathcal{B}(\mathbb{Z}_p^n)$, see Section 3.4.

As in the above count of atoms of $\mathcal{B}({\mathbb{Z}_2}^n)$, we count the number of atoms of a length m of $\mathcal{B}({\mathbb{Z}_3}^n)$ by considering the number of choices in the sequence element-by-element, ensuring that no elements produce zero subsums. Since in $\mathcal{B}({\mathbb{Z}_2}^n)$ each element is its own inverse, no element in an atom could repeat or be linearly dependent on previous ones, which is not the case in the atoms of $\mathcal{B}({\mathbb{Z}_3}^n)$.

In place of the atom $a_1a_2...a_m$, we consider a sequence of the same length with elements I, N, and $\mathbb{I}$ called a *dimension class* and defined as follows. Choosing an element a_i can either increase the dimension of the subspace by one or not increase it at all, denoted I or N, respectively. In other words, if a_i cannot be written as a linear combination of the previous elements, we write I, and if it can be written as such a linear combination, we write N. If an element has multiplicity two, let it be chosen before the others and be denoted $\mathbb{I}$, one symbol counting for two elements. Thus, the number of permutations in the count is $(m - 2|\mathbb{I}|)!|\mathbb{I}|!$, the first term for the number of elements of multiplicity 1 and the second term for the number of elements of multiplicity 2. We divide out by this number of permutations at the end of the process. Unlike the length and multiplicity classes, this current definition of dimension class is specific to $\mathcal{B}({\mathbb{Z}_3}^n)$. For instance, in $\mathcal{B}({\mathbb{Z}_7}^n)$, we might have a multiplicity class of a^4b^4c that we were required to partition into dimension classes. However, our definition of multiplicity classes would not be able to handle most cases of elements of multiplicities ≥ 3. Furthermore, let X_i represent either I or N, and let $|\mathbb{I}|$ and $|X|$ be the number of $\mathbb{I}$'s and X's, respectively.

This recently-developed notation will be convenient to abstract from the details of $\mathcal{B}({\mathbb{Z}_3}^n)$. However, most of the intuition for this section developed elsewhere from study of what we called tree diagrams of $\mathcal{B}({\mathbb{Z}_3}^n)$. The tree diagrams are *not* included in this paper, because they became cumbersome as early as lengths 5 and 6, and nearly impossible for lengths 8 and greater. Though the outdated tree diagrams were intuitively accessible for small lengths, once

[2]also called the q-binomial coefficient, and written $\begin{bmatrix} a \\ b \end{bmatrix}_q$

the difficulty of understanding the current notation is overcome, the greater abstraction provided by the dimension classes proves able to handle arbitrary lengths.

Theorem 3.4. A Dimension Class Structure Theorem
The dimension sequence is of the form $\mathbb{I}_1, \mathbb{I}_2, ..., \mathbb{I}_{|\mathbb{I}|}, X_1, X_2, ..., X_{|X|}, N$, *where* $2|\mathbb{I}| + |X| + 1 = m$; *and if* $|X| \geq 1$, *then* $X_1 = I$; *and if* $|\mathbb{I}| = 0$ *and* $|X| \geq 3$, *then* $X_2 = I$.

Equivalently:
a) If no $\mathbb{I}$ *is in the sequence, i.e. if no* $a_i = a_j$, *and the number of elements in the sequence is greater than or equal to 3, then the first two elements are* I.
b) Every $\mathbb{I}$ *increases the subspace dimension by* 1.
c) In case $|\mathbb{I}| \geq 1$, *the element following the last* $\mathbb{I}$ *is an* I *if there is more than one element of multiplicity 1.*
d) The last element in the sequence is always N.

Proof. a) The first element a_1 increases the subspace from 0 to 1 and so is denoted I. If the second element a_2 did not increase the subspace dimension, then it would be a multiple of the first element equal to $0, a_1$, or $(a_1)^2 = (a_1)^{-1}$. These are all unavailable because they either repeat the first element or produce a zero subsum. If a_2 is the last choice, then the number of elements in the sequence is 2, contrary to assumption. Therefore, the choice of a_2, if not the last, must also increases the subspace dimension and be denoted I in the dimension sequence.
b) The first $\mathbb{I}$, $\mathbb{I}_1$, denotes that in the sequence $a_1 = a_2$. The choice of a_1 increases the dimension for the same reasons as in a). As is the case for all $\mathbb{I}$, the repetition of the element again does not increase the subspace.

Since the $\mathbb{I}$'s are chosen first and are located at the beginning of the sequence, an element a_{2k-1}, the first element of the pair $\mathbb{I}_k$, $k \geq 2$ is preceded only by other $\mathbb{I}$'s. Assume that some $\mathbb{I}_k$ does not increase the dimension. Then its first element a_{2k-1} must be a linear combination of the previous $2k-2$ elements. This is shown in the following equation where only the first element a_{2i-1} of the pair $\mathbb{I}_i$ is shown and where accordingly $s_i \in \{0, 1, 2\}$: $a_{2k-1} = s_1a_1 + s_2a_3 + ... + s_{k-1}a_{2k-3}$. But any such a_{2k-1} will produce a zero subsum. Let $r_i = (3 - s_i) \mod 3$. Then $a_{2k-1} + r_1a_1 + r_2a_3 + ... + r_{k-1}a_{2k-3} = 0$.
c) If the element following the last $\mathbb{I}$ is not an I, it is an N. But such an N would be a linear combination of the first element a of the pairs of $\mathbb{I}$'s preceding it. As in b), such an N would produce a zero subsum. This is only possible in an atom if this element were the last element, and the subsequence were the entire sequence. But it is required that there be more than one element of multiplicity 1.
d) The last element is determined to be the inverse of those that come before it. □

Theorem 3.4 restricts the form of the possible dimension classes. Another clear restriction but one yet to be proved, is an upper bound ratio of $|N| : |I|$ counting the previous elements from any element. For instance, we cannot

have the dimension class $IIINNNN$, or even $IINN$. There simply are not enough elements linearly dependant on two elements to prevent repeats and zero subsums. In general, ideas such as this for furthering the research are found in the conclusion of the paper, Section 5.

Theorem 3.5 that follows gives the general formula of the number of atoms in $\mathcal{B}({\mathbb{Z}_3}^n)$ of length m. It contains a function f that gives the number of choices available for the choice of any N, which is only determined small $|N|$, and thus the only lengths completely determined are small m. After this theorem, the formula is then determined for classes of x's where $N \leq 2$. Finally, the explicit formulas for m=1,2,...,6 will be presented at the end of this section.

Theorem 3.5. *Let x be a dimension class of length m, and E_m be the set of all x's for an m; let $u(x) = |I| + |\mathbb{I}|$; let the indexing of N be $1, 2, .., j$, and let $v(x)$ be the number of N's in x. Let $f(N(x, j))$ denote the number of choices for $N(x, j)$.*

Then, the formula for the number of atoms of a particular length m is

$$\frac{\sum\limits_{x \in E_m} \Big(\prod\limits_{i=0}^{u(x)-1} (3^n - 3^i) \prod\limits_{j=1}^{v(x)} f(N(x,j)) \Big)}{(m - 2|\mathbb{I}|)!|\mathbb{I}|!}$$

.

The proof will follow Theorem 3.6

Theorem 3.6. *There are $\prod\limits_{i=0}^{u(x)-1} 3^n - 3^i$ choices for the $u(x)$ elements labelled I or $\mathbb{I}$ in the sequence x.*

Proof. The only restriction on the choice of the i^{th} I or $\mathbb{I}$ is that it must not be an element that is in the subspace of the elements chosen before it. Such elements total 3^{i-1}. Because there are 3^n group elements, there are $3^n - 3^{i-1}$ choices for the i^{th} I or $\mathbb{I}$. Therefore, the number of choices for the $u(x)$ I or $\mathbb{I}$'s of sequence x is $\prod\limits_{i=1}^{u(x)} 3^n - 3^{i-1} = \prod\limits_{i=0}^{u(x)-1} 3^n - 3^i$. □

We now prove Theorem 3.5.

Proof. $\sum\limits_{x \in E_m}$ sums over the possible dimension classes of atoms of length m, and the denomenator divides out by $(m-2|\mathbb{I}|)!$ for the permutations of the elements of multiplicity 1, and $|\mathbb{I}|!$ for the permutations of the elements of multiplicity 2. The first product in the sum is the product for the I's and $\mathbb{I}$'s (theorem 3.6). The second product $\prod\limits_{j=1}^{v(x)} f(N(x, j))$ is by definition the number of choices of each N. And the number of choices for any dimension class is the number of elements available of each of the I's, N's, and $\mathbb{I}$'s. □

Let $w(x,j)$ be the number of I's and $\mathbb{I}$'s before $N(x,j)$ in x, and let $W(x,j)$ be the set of the coordinate place of the previous N's for $N(x,j)$ in x. Then $tj = (w + |W|) \in 1, 2, ...3, m$, and it seems that $f(x, N(x,j)) = f\big(w(x,j), W(x,j)\big)$ denote the number of choices for $N(x,j)$.

In other words, it seems that w, W, t are the important properties of a $N(x,j)$, and that t is a function of w and W, so we can let f be a function of these latter two only. This is stated generally now without proof.

The last $N(x,j)$, $N(x,v)$, is a special case for which there is only one choice; notated $f(N(x,v)) = f(w(x,v), W(x,v)) = 1$.

The penultimate N is also a special case because, in addition to not producing a zero subsum and not repeating an previous element, the elements chosen for the penultimate also cannot be such that it forces the final element to repeat a previous element or to produce a zero subsum. In particular, the final element cannot repeat the penultimate element. Where $u(N(x,j))$ is the set of unavailable elements for $N(x,j)$, $f(N(x,j)) = (3^{w_j} - |u(N_j)|)$. Let $u_r(N(x,j))$ be the set of elements unavailable because they would repeat a previous element, and $u_z(N(x,j))$ be the set of elements unavailable because they would cause a zero subsum. For all $N(x,j)$, $t_j \notin \{m-1, m\}$, $u(N(x,j)) = u_r(N(x,j)) \cup u_z(N(x,j))$. Let $u_f(N(x,j))$ be the elements unavailable for the penultimate choice because they would determine the final element unavailable (an example of computing $u_f(N(x,j))$ is given for $v = 2$ below). Then for N_{v-1} and $t_j = m-1$, $u(N(x,j)) = u_z(N(x,j)) \cup u_r(N(x,j)) \cup u_f(N(x,j))$. For all other $N(x,j)$, $t(x,j) \leq m-2$, $u(N(x,j)) = u_z(N(x,j)) \cup u_r(N(x,j))$.

The inner part of the formula, the two products, is determined for particular x's in the following applications of the formula, all of which except the first require their own proofs.

Application 1. *For sequence x, $v(x) = 1$, that is, of the form $I, I, ..., I, N$, there are $\prod_{i=0}^{m-2} (3^n - 3^i)$ choices.*

Lemma 3.6.1. *There is an automorphism from each subspace defined by a subsequence of an atom under which all the I's and $\mathbb{I}$'s are mapped to the standard bases elements of that subspace.*

Proof. Since each choice I or $\mathbb{I}$ increases the dimension of the subspace by 1, they form an independent basis for the subspace. Therefore, they can be mapped to $\{(1,0,0,...,0), (0,1,0,...,0), (0,0,1,...,0), ..., (0,0,0,...,1)\}$. The elements labelled N are mapped accordingly. □

Application 2. *For sequence x, $v(x) = 2$, $t(x)_1 = m-1$, that is, of the form $I_1, I_2, ..., I_{m-2}, N, N$, there are $\left(\prod_{i=0}^{m-3} (3^n - 3^i)\right)\left(3^{m-2} - 2^{m-2} - 2m + 3\right)$ choices.*

Proof. Assume the automorphism of the lemma. Since the subsums of the first $m-2$ elements unioned with the zero element has a 0 or 1 in each coordinate, $u_z(N_1) = \{\alpha_1, \alpha_2, ..., \alpha_{m-2} | \alpha_i \in \{0, 2\}\}$. The elements N_1 cannot repeat are clearly $u_r(N_1) = \{(1,0,0,...,0), (0,1,0,...,0), ..., (0,0,0,...,1)\}$. Since N_1 is

Length	Formula
3	$\frac{(3^n-1)(3^n+3)}{3!}$
4	$\frac{(3^n-1)(3^n+3)(3^n-3)}{4!}$
5	$\frac{(3^n-1)(3^n+3)(3^n-3)(3^n-4)}{5!}$
6	$\frac{(3^n-1)(3^n-3)(3^n-9)\left(3^{2n}-3^{n+1}+12\right)}{6!}$

Table 1: Formulas for atoms of length m in ${\mathbb{Z}_3}^n$

the penultimate choice, we also compute the elements unavailable because they would make the final choice unavailable. $u_f(N_1) = \{u_z(d)\} \cup \{\alpha_1, \alpha_2, ..., \alpha_{m-2} | \alpha_i$ all 2 but one $1\} \cup (1, 1, ..., 1)$. The first set contains the elements that chosen as the penultimate element would force the final element to be unavailable, and the second set is the elements that chosen as the penultimate would make the final a repeat of a previous element. The final element $(1, 1, ..., 1)$ would make the penultimate equal to the final element. (Repeats are bad because we have assumed all repeats to be moved to the beginning of the sequence and represented $\mathbb{I}$.) $u(N_1) = u_z(N_1) \cup u_r(N_1) \cup u_f(N_1)$ or $u(N_1) = \{\alpha_1, \alpha_2, ..., \alpha_{m-2} | \alpha_i \in \{0, 2\}\} \cup \{(1, 0, 0, ..., 0), (0, 1, 0, ..., 0), ..., (0, 0, 0, ..., 1)\} \cup \{\alpha_1, \alpha_2, ..., \alpha_{m-2} | \alpha_i$ all 2 but one $1\} \cup \{1, 1, 1, ..., 1\}$.

These number

$$\Big[\prod_{i=0}^{m-3}(3^n - 3^i)\Big]\Big[\prod_{j=1}^{2} f(N(x, j))\Big]$$

$$= \Big[\prod_{i=0}^{m-3}(3^n - 3^i)\Big]\Big[3^{m-2} - (2^{m-2} + 2(m-2) + 1)\Big]$$

$$= \left(\prod_{i=0}^{m-3}(3^n - 3^i)\right)\left(3^{m-2} - 2^{m-2} - 2m + 3\right)$$

□

Table 1 gives the number of atoms of lengths $3, 4, 5, 6$ in $\mathcal{B}({\mathbb{Z}_3}^n)$.

3.4 Additional Theorems

This section gives a few theorems that do not fit into the above categories. As promised in Theorem 3.1, the first theorem in this section gives the number of atoms of length 2 in arbitrary G.

Theorem 3.7. *In any finite abelian group $G \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \mathbb{Z}_{n_k}$ where $1 < n_1 | n_2 | \cdots | n_k$, let x be the number of n_i such that 2 divides n_i. Then the number of atoms of length 2 is*

$$\frac{|G| - 2^x}{2} + 2^x - 1$$

.

Proof. There are exactly $2^x - 1$ elements of order 2, and $\frac{|G|-2^x}{2}$ elements of order ≥ 3. Each of the former is its own inverse, so forms a length 2 atom. Pairs of the later form length 2 atoms. □

The next two proofs are multiplicity class restriction theorems on $(\mathbb{Z}_p)^n$.

Theorem 3.8. *In $(\mathbb{Z}_p)^n$, there is no atom of the form ${a_1}^x {a_2}^x ... {a_y}^x$, where $x \geq 2$.*

Proof. Assume to the contrary there is such an atom. Then $a_1 a_2 ... a_y = a \neq 0 \Rightarrow {a_1}^x {a_2}^x ... {a_y}^x = a^x \Rightarrow a^x = 0 \Rightarrow x = p \Rightarrow (a_i)^x = 0$, a zero subsum of the supposed atom. □

Theorem 3.9. *In $(\mathbb{Z}_p)^n$, there is no atom of the form ${a_1}^{p-x_1} {a_2}^{p-x_2} ... {a_y}^{p-x_y}$, where $p \geq x_i \geq \frac{p}{2}$.*

Proof. ${a_1}^{x_1} {a_2}^{x_2} ... {a_y}^{x_y}$ is a zero subsum if $x_i \leq p - x_i$ (by theorem 3.8 they are not all equal), that is, if $x_i \geq \frac{p}{2}$. □

4 Minimal Zero Sequences and Invariant Theory of Finite Abelian Groups

4.1 Preliminary Results

We will conclude by presenting a remarkable and unexpected connection between the invariant theory of cyclic groups, which is generally studied from the perspective of algebra, and the study of minimal zero sequences of a cyclic group, which can be thought of as more combinatorial in nature. Previous research has aimed to, given a cyclic group order n, count the number of n-variable polynomials of the group which are invariant under a cyclic substitution of the variables[Str48]. Since then, no major advancements have been made with respect to the number of these invariant polynomials of a cyclic group, and currently it is only known for cyclic groups of equal order and degree up to degree 10 (which were calculated by Strom). Using the results which will be presented in this paper, the number of invariant polynomials of cyclic groups of equal order and degree have been calculated up to degree 60, and we will conclude with a table listing these values, as well as another table listing these values for the groups $\mathbb{Z}_m \oplus \mathbb{Z}_n$.

First we shall prove a lemma, and mention a few other facts which will be used consistently through the paper.

From this point on, it is assumed that s_n denotes the cyclic permutation of n variables defined by

$$s_n = (x_{n-1} x_{n-2} \dots x_1 x_0)$$

and

$$\varepsilon_n = e^{\frac{2\pi i}{n}},\ n \in \mathbb{Z}$$

Fact 1. *[Nee00]*

$$\varepsilon_n{}^{kn} \equiv 1,\ k \in \mathbb{Z} \tag{9}$$

Fact 2. *[Gra94]*

$$\sum_{k=0}^{n} r^k = \begin{cases} \frac{1-r^{n+1}}{1-r}, & \text{for } r \neq 1; \\ n+1, & \text{for } r = 1. \end{cases} \tag{10}$$

The following lemma will be useful in simplifying many of the arguments that follow, so we will present it here. If the reader is eager to get directly to the main results, she may skip this for the time being, and come back to it later.

Lemma 4.0.1. *Let $m, n \in \mathbb{N},\ 0 \leq j \leq m \leq n$, and suppose that $p^k = 1 \Leftrightarrow k \equiv 0 \pmod{n}$. Then,*

$$\sum_{k=0}^{n-1} (p^{m-j})^k = \begin{cases} n, & \text{if } m = j; \\ 0, & \text{if } m \neq j. \end{cases}$$

Proof. Clearly if $m = j$, then the sum reduces to

$$\sum_{k=0}^{n-1} 1^k$$

and we can apply (10). So suppose $m \neq j$. Then, $p^{m-j} \neq 1$. So, again by (10),

$$\sum_{k=0}^{n-1} (p^{m-j})^k = \frac{1 - p^{n(m-j)}}{1 - p^{m-j}}$$

But by hypothesis, $p^{n(m-j)} = 1$, and $p^{m-j} \neq 1$ □

We would like to point out in passing that if p and q are polynomials in the variables $x_1, x_2, \ldots, x_k$, then the cyclic permutation of variables S_k respects both addition and multiplication of polynomials. In other words, $S_k(p+q) = S_k(p) + S_k(q)$ and $S_k(pq) = S_k(p)S_k(q)$. This is fairly easy to see if you just think of S_k as replacing one variable with another variable, and so forth.

4.2 Zero Sequences and Invariant Polynomials of $\mathbb{Z}_n$

At this point for the reader's convenience we will reproduce Strom's original argument[Str48] providing necessary and sufficient conditions for a polynomial of a cyclic group to be invariant. We will fill in some of the details left out of the original argument, but nonetheless the reader is referred to [Str48] for the original argument.

Consider the polynomial in the n variables $x_0, x_1, \ldots, x_{n-1}$:

$y_j = \sum_{k=0}^{n-1} \varepsilon_n{}^{jk} x_k,\ j = 0, 1, \ldots, n-1.$

Theorem 4.1. *For all $j,\ 0 \leq j \leq n-1,\ x_j$ can be written as a linear combination of y's. Specifically, $nx_j = \sum_{k=0}^{n-1} \varepsilon_n{}^{k(n-j)} y_k$*

Proof. Replacing y_k in the sum, we obtain the following double sum:

$$\sum_{k=0}^{n-1} {\varepsilon_n}^{k(n-j)} \sum_{m=0}^{n-1} {\varepsilon_n}^{km} x_m$$

Notice that by (9) ${\varepsilon_n}^{k(n-j)} = {\varepsilon_n}^{-kj}$. Therefore, making the simplification and rearranging the double sum yields

$$\sum_{m=0}^{n-1} x_m \sum_{k=0}^{n-1} ({\varepsilon_n}^{m-j})^k$$

And now, by Lemma 4.0.1, the inner sum is 0 whenever $m \neq j$, and the inner sum is n when $m = j$. □

The proofs that follow will use the previous theorem in order to switch polynomials in x_j to polynomials in y_j and vice versa, where convenient.

The astute reader may be wondering about the relationship between our strange definition for ε_m and the fact that we are in essence "rotating" the variables while keeping the constants fixed. The next theorem presents a striking result which makes this relationship precise.

Theorem 4.2. *Let $H_j(\mathbf{y}) = y_j$. The cyclic permutation s_n applied to H_j can be written in terms of elementary multiplication as*

$$s_n \circ H_j = {\varepsilon_n}^j H_j$$

Proof.

$$s_n \circ H_j = \sum_{k=0}^{n-1} {\varepsilon_n}^{j(k+1)} x_k = {\varepsilon_n}^j \sum_{k=0}^{n-1} {\varepsilon_n}^{jk} x_k = {\varepsilon_n}^j y_j = {\varepsilon_n}^j H_j$$

□

We are nearly done at this point, because the problem of finding polynomials which are invariant under this strange permutation has reduced itself to polynomials which are invariant when multiplied by a simple constant. Using this fact, we can easily find necessary and conditions that a polynomial be invariant.

Theorem 4.3. *The polynomial*

$$Q(y_0, y_1, \ldots, y_{n-1}) = \sum_{\alpha_0,\ldots,\alpha_{n-1}} c_{\alpha_0,\ldots,\alpha_{n-1}} {y_0}^{\alpha_0} {y_1}^{\alpha_1} \cdots {y_{n-1}}^{\alpha_{n-1}}$$

is invariant under s_n if and only if, for every term of the polynomial

$$\alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1} \equiv 0 \pmod{n} \tag{11}$$

Proof. Notice that

$$s_n \circ {y_k}^{\alpha_k} = ({\varepsilon_n}^k y_k)^{\alpha_k} = {\varepsilon_n}^{k\alpha_k} {y_k}^{\alpha_k}$$

Thus, by Theorem 4.2,

$$s_n \circ Q(y_0, y_1, \ldots, y_{n-1}) = \sum_{\alpha_0, \cdots, \alpha_{n-1}} c_{\alpha_0, \cdots, \alpha_{n-1}} {\varepsilon_n}^{\alpha_1 + \cdots + (n-1)\alpha_{n-1}} {y_0}^{\alpha_0} \ldots {y_{n-1}}^{\alpha_{n-1}}$$

and when

$${\varepsilon_n}^{\alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1}} = 1$$

the individual terms of the polynomial are invariant under s_n. □

Now, we know what *all* invariant polynomials look like, but it suffices to consider only *minimal* invariant polynomials (i.e. those which do not contain a sub-polynomial which is also invariant) since the set of all invariant polynomials is completely determined by the set of all minimal invariant polynomials, as we can just form linear combinations of them[Str48].

We will now state a few basic definitions about minimal zero sequences, and proceed to make the connection with (11)

Note the appearance of the integers $1, 2, \ldots, n-1$ in (11). In words what (11) says is that some number of 1's + some number of 2's + $\cdots$ + some number of n-1's $\equiv 0 \pmod{n}$. But this is exactly what a zero-sum sequence is. The connection is of course extended to minimal zero sequences since we are counting only those invariant polynomials which are minimal.

Theorem 4.4. *Let $G = \mathbb{Z}_k$. Denote by $MZS(k)$ the number of minimal zero sequences of G, and denote by $Inv(k)$ the number of invariant polynomials of G. Then, $MZS(k) \equiv Inv(k)$.*

In fact, this follows as a corollary of the previous results, but we state it as a theorem due to it's extreme importance.

Proof. Let P be a minimal invariant polynomial of G. Then, combining (11) with the fact that minimal invariant polynomials contain exactly one term, we know this polynomial corresponds to exactly one minimal zero sequence. Conversely, let K be a minimal zero sequence of G. We can therefore write $\sum K$ in the form $\alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1}$, and since $\sum K \equiv 0 \pmod{n}$, we see that it corresponds to the invariant polynomial

$$P = c_{\alpha_0, \cdots, \alpha_{n-1}} {y_0}^{\alpha_0} \ldots {y_{n-1}}^{\alpha_{n-1}}$$

□

4.3 The Next Simplest Case: Zero Sequences and Invariant Polynomials of $\mathbb{Z}_m \oplus \mathbb{Z}_n$

Now that we have established the basic connection between the counting of minimal zero sequences of a cyclic group and the counting of invariant polynomials of a cyclic group, and in fact shown that they are equivalent, we will proceed to extend Strom's original work by first establishing the same connection between the number of invariant polynomials of the group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ and the minimal zero sequences of $\mathbb{Z}_m \oplus \mathbb{Z}_n$. This will give the reader some insight into how to proceed towards the general case. Finally, we will establish the connection with the general case of $G = \bigoplus_{i=1}^{k} \mathbb{Z}_{n_i}$.

In what follows, we will simply present the generalization of the previous theorems along with their proofs. The reader is encouraged to compare each theorem with its more specific counterpart which precedes.

Consider the polynomial in the mn variables $x_{ab},\ (a,b) \in G = \mathbb{Z}_m \oplus \mathbb{Z}_n$, defined by $y_{jk} = \sum_{a=0}^{m-1}\sum_{b=0}^{n-1} {\varepsilon_m}^{ja}{\varepsilon_n}^{kb}x_{ab}\ \forall (j,k) \in G$

Theorem 4.5. *For all $j,k \in G,\ x_{jk}$ can be written as a linear combination of y's. Specifically, $|G|x_{jk} = \sum_{a=0}^{m-1}\sum_{b=0}^{n-1} {\varepsilon_m}^{a(m-j)}{\varepsilon_n}^{b(n-k)}y_{ab}$*

Proof. Replacing y_{ab} in the sum, we obtain the following double sum:

$$\sum_{a=0}^{m-1}\sum_{b=0}^{n-1} {\varepsilon_m}^{a(m-j)}{\varepsilon_n}^{b(n-k)} \sum_{c=0}^{m-1}\sum_{d=0}^{n-1} {\varepsilon_m}^{ac}{\varepsilon_n}^{bd}x_{cd}$$

$$= \sum_{c=0}^{m-1}\sum_{d=0}^{n-1} x_{cd}\left(\sum_{a=0}^{m-1}\left({\varepsilon_m}^{c-j}\right)^a \sum_{b=0}^{n-1}\left({\varepsilon_n}^{d-k}\right)^b\right)$$

Now, by Lemma 4.0.1,

$$\sum_{b=0}^{n-1}\left({\varepsilon_n}^{d-k}\right)^b = \begin{cases} 0, & \text{if } d \neq k; \\ n, & \text{if } d = k. \end{cases}$$

Similarly,

$$\sum_{a=0}^{m-1}\left({\varepsilon_m}^{c-j}\right)^a = \begin{cases} 0, & \text{if } c \neq j; \\ m, & \text{if } c = j. \end{cases}$$

Thus, the only contribution to the outer two sums is when $c = j \wedge d = k$. □

Corollary. *Any polynomial P in the mn variables $x_{jk}, (j,k) \in G$ can be written uniquely as a polynomial Q in terms of the mn variables $y_{jk}, (j,k) \in G$.*

Let s_{ij} denote the cyclic permutation on mn variables defined by

$$s_{\alpha\beta}\ :\ x_{ij} \rightarrow x_{(i+\alpha)\bmod m,(j+\beta)\bmod n}$$

Notice that any polynomial in the variables $x_{jk}, (j,k) \in G$ is invariant under cyclic permutation of the variables if and only if it is invariant under s_{10} and s_{01}.

Theorem 4.6. *Let $Q_{jk}(\mathbf{y}) = y_{jk}$. Then, $s_{10} \circ Q_{jk} = {\varepsilon_m}^j Q_{jk}$. Likewise, $s_{01} \circ Q_{jk} = {\varepsilon_n}^k Q_{jk}$*

Proof.

$$s_{10} \circ Q_{jk} = s_{10}\left(\sum_{a=0}^{m-1}\sum_{b=0}^{n-1} {\varepsilon_m}^{ja}{\varepsilon_n}^{kb}x_{ab}\right) = \sum_{a=0}^{m-1}\sum_{b=0}^{n-1} {\varepsilon_m}^{ja}{\varepsilon_n}^{kb}x_{(a+1)\bmod m,b}$$
$$= \sum_{b=0}^{n-1}{\varepsilon_n}^{kb}\left({\varepsilon_m}^{j(m+1)}x_{0b} + \sum_{a=1}^{m-1}{\varepsilon_m}^{j(a+1)}x_{ab}\right) = \sum_{b=0}^{n-1}{\varepsilon_n}^{kb}\sum_{a=0}^{m-1}{\varepsilon_m}^{j(a+1)}x_{ab}$$
$$= {\varepsilon_m}^j\sum_{b=0}^{n-1}\sum_{a=0}^{m-1}{\varepsilon_n}^{kb}{\varepsilon_m}^{ja}x_{ab} = {\varepsilon_m}^j Q_{jk}$$

And similarly for $s_{01} \circ Q_{jk} = {\varepsilon_n}^k Q_{jk}$. □

Theorem 4.7. *The polynomial*

$$Q(\mathbf{y}) = \sum_{\substack{\alpha_{rs} \\ (r,s)\in\mathbb{Z}_n\oplus\mathbb{Z}_m}} C^* \prod_{j=0}^{m-1}\prod_{k=0}^{n-1} {y_{jk}}^{\alpha_{jk}}$$

is invariant under s_{10} whenever each term of Q satisfies

$$\sum_{j=0}^{m-1} j \sum_{k=0}^{n-1}\alpha_{jk} \equiv 0 \pmod{m} \tag{12}$$

Likewise, Q is invariant under s_{01} whenever each term of Q satisfies

$$\sum_{k=0}^{n-1} k \sum_{j=0}^{m-1}\alpha_{jk} \equiv 0 \pmod{n} \tag{13}$$

Proof. Notice that

$${y_{jk}}^{\alpha_{jk}} = \left({\varepsilon_m}^j y_{jk}\right)^{\alpha_{jk}} = {\varepsilon_m}^{j\alpha_{jk}}{y_{jk}}^{\alpha_{jk}}$$

Now, let $\Gamma_j = \sum_{k=0}^{n-1}\alpha_{jk}$. Then, by Theorem 4.6,

$$s_{10} \circ Q_k = \sum_{\alpha_0,\cdots,\,\alpha_{n-1}} C^* {\varepsilon_m}^{\Gamma_1+2\Gamma_2+\cdots+(m-1)\Gamma_{m-1}} \prod_{j=0}^{m-1}\prod_{k=0}^{n-1}{y_{jk}}^{\alpha_{jk}}$$

and when

$$\sum_{j=0}^{m-1} j\Gamma_j = \sum_{j=0}^{m-1} j \sum_{k=0}^{n-1} \alpha_{jk} \equiv 0 \pmod{m}$$

the individual terms of the polynomial are invariant under s_{10}.

The proof of the other case follows similarly. □

Notice that what 12 really says is that if you consider the set $S_k = \{(k, p) \in \mathbb{Z}_m \oplus \mathbb{Z}_n\}$, then some number of elements of S_1 plus some number of elements of S_2 plus $\cdots$ plus some number of elements of S_{m-1} add up to an element in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ whose first coordinate is 0. Likewise, 12 ensures that the second coordinates sum to 0.

Theorem 4.8. *Let $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Denote by $MZS(G)$ the number of minimal zero sequences of G, and denote by $Inv(G)$ the number of invariant polynomials of G. Then, $MZS(G) \equiv Inv(G)$.*

This probably comes as no surprise to the reader, but we shall prove it nonetheless.

Proof. Let P be a minimal invariant polynomial of G. Then, combining (12) and (13) with the fact that minimal invariant polynomials contain exactly one term, we know this polynomial corresponds to exactly one minimal zero sequence. Conversely, let K be a minimal zero sequence of G. We can therefore break $\sum K$ into two separate equations corresponding to the sum of the first coordinate and the sum of the second coordinate. It is easy to see that these correspond exactly to (12) and (13), respectively, and thus to exactly one minimal invariant polynomial. □

4.4 The Whole Shebang: Zero Sequences and Invariant Polynomials of $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$

At this point the reader is probably has a pretty good idea of how to extend the previous argument to the general case of $\bigoplus_{i=1}^{k} \mathbb{Z}_{n_i}$. For the sake of completeness, however, we will present the argument here. Now that the hard work is out of the way, the only real difficulty is in getting past the notation. As in the previous section, we shall only present the generalized versions of the theorems along with their proofs.

Let us set the following notation in advance, in order to simplify matters:

1. $G = \bigoplus_{i=0}^{k} \mathbb{Z}_{n_i}$.

2. If $\alpha \in G$, then $\pi_i(\alpha)$ denotes the i'th coordinate of α.

Consider the polynomial in the $|G|$ variables $x_\alpha,\ \alpha \in G$, defined by

$$y_\alpha = \sum_{\beta \in G} \left(\prod_{p=1}^{k} \varepsilon_{n_p}{}^{\pi_p(\alpha)\pi_p(\beta)} \right) x_\beta$$

Theorem 4.9. *For all $\alpha \in G$, x_α can be written as a linear combination of y's. Specifically,*

$$|G| x_\alpha = \sum_{\beta \in G} \left(\prod_{q=1}^{k} \varepsilon_{n_q}{}^{\pi_q(\beta)(n_q - \pi_q(\alpha))} \right) y_\beta$$

Proof. Replacing y_β in the sum, we obtain the following:

$$\sum_{\beta \in G} \left(\prod_{q=1}^{k} \varepsilon_{n_q}{}^{\pi_q(\beta)(n_q - \pi_q(\alpha))} \right) \sum_{\gamma \in G} \left(\prod_{p=1}^{k} \varepsilon_{n_p}{}^{\pi_p(\beta)\pi_p(\gamma)} \right) x_\gamma$$

$$= \sum_{\gamma \in G} x_\gamma \sum_{\beta \in G} \prod_{q=1}^{k} \left(\varepsilon_{n_q}{}^{\pi_q(\gamma) - \pi_q(\alpha)} \right)^{\pi_q(\beta)}$$

Now, $\pi_q(\gamma) - \pi_q(\alpha) = 0$ means that the q'th coordinate of γ and the q'th coordinate of α are the same. Note that this only happens for *every* value of q when $\gamma = \alpha$. Thus, the only contribution to the inner sum comes when $\gamma = \alpha$, in which case the inner sum is equal to n_q. Thus, for each value of q, we get one contribution to the sum, namely, a factor of n_q.

Since, $|G| = \prod_{q=1}^{k} n_q$ we are done. □

Corollary. *Any polynomial P in the $|G|$ variables $x_\alpha,\ \alpha \in G$ can be written uniquely as a polynomial Q in terms of the $|G|$ variables $y_\alpha,\ \alpha \in G$.*

Let s_α denote the cyclic permutation on $|G|$ variables defined by

$$s_\alpha \ : \ \pi_j(x_\beta) \rightarrow [\pi_j(x_\beta + \alpha)] \bmod n_j, \quad \alpha \in G$$

From now on, we will write $\mathbf{e}_j$ to denote the j'th basis vector. In other words, $\mathbf{e}_j$ is the vector with 1's in the j'th coordinate, and 0s everywhere else.

Theorem 4.10. *Let $Q_\alpha(\mathbf{y}) = y_\alpha$. Then, $s_{\mathbf{e}_j} \circ Q_\alpha = \varepsilon_{n_j}{}^{\pi_j(\alpha)} Q_\alpha$.*

Proof.

$$s_{\mathbf{e}_j} \circ Q_\alpha = s_{\mathbf{e}_j} \left(\sum_{\beta \in G} \left(\prod_{p=1}^{k} \varepsilon_{n_p}{}^{\pi_p(\alpha)\pi_p(\beta)} \right) x_\beta \right)$$

Now, notice that this operation only affects the j'th coordinate of x_β, and leaves the other ones alone. Thus, we can pull out the term in the product where $p = j$,

and rewrite the product.

$$= \sum_{\beta \in G} \left[\left({\varepsilon_{n_j}}^{\pi_j(\alpha)(\pi_j(\beta)+1)} \right) \left(\prod_{\substack{1 \le p \le k \\ p \ne j}} {\varepsilon_{n_p}}^{\pi_p(\alpha)\pi_p(\beta)} x_\beta \right) \right]$$

$$= {\varepsilon_{n_j}}^{\pi_j(\alpha)} \sum_{\beta \in G} \left(\prod_{p=1}^{k} {\varepsilon_{n_p}}^{\pi_p(\alpha)\pi_p(\beta)} x_\beta \right)$$

$$= {\varepsilon_{n_j}}^{\pi_j(\alpha)} Q_\alpha$$

□

Theorem 4.11. *The polynomial*

$$Q(\mathbf{y}) = \sum_{\substack{\alpha_\beta \\ \beta \in G}} C_{\alpha_\beta} \prod_{\gamma \in G}^{n-1} {y_\gamma}^{\alpha_\gamma}$$

is invariant under $s_{\mathbf{e}_j}$ whenever each term of Q satisfies

$$\sum_{i=0}^{n_i - 1} i \left(\sum_{\substack{\gamma \in G \\ \pi_j(\gamma) = i}} \alpha_\gamma \right) \equiv 0 \pmod{n_j} \tag{14}$$

Proof. Notice that

$$s_{\mathbf{e}_j} \circ {y_\gamma}^{\alpha_\gamma} = \left({\varepsilon_{n_j}}^{\pi_j(\gamma)} y_\gamma \right)^{\alpha_\gamma} = {\varepsilon_{n_j}}^{\alpha_\gamma \pi_j(\gamma)} y_\gamma^{\alpha_\gamma}$$

We should make a few comments here. If we apply $s_{\mathbf{e}_j}$ to ${y_\gamma}^{\alpha_\gamma}$ for every $\gamma \in G$, what we will get is a product of ε terms like that which you see above. When combined, the exponent will be a sum that looks like

$$\alpha_{\gamma_1}\pi_j(\gamma_1) + \alpha_{\gamma_2}\pi_j(\gamma_2) + \alpha_{\gamma_3}\pi_j(\gamma_3) + \cdots + \alpha_{\gamma_{|G|}}\pi_j(\gamma_{|G|})$$

However, fixing any j, many different elements of G clearly will have the same j'th coordinate, meaning that, for example, if we choose γ_1 and γ_2 appropriately, $\gamma_1\pi_j(\gamma_1) + \gamma_2\pi_j(\gamma_2) = \pi_j(\gamma_1)(\gamma_1 + \gamma_2)$. Thus, the sum inside the parentheses is the sum of all elements of G which have the same j'th coordinate. Since the j'th coordinate ranges from 0 to $n_j - 1$, we can use this to write the sum in a more compact form.

Let

$$\Gamma_{ab} = \sum_{\substack{\gamma \in G \\ \pi_b(\gamma) = a}} \alpha_\gamma$$

. Then, by Theorem 4.6,

$$s_{\mathbf{e}_j} \circ Q_\gamma = \sum_{\substack{\alpha_\beta \\ \beta \in G}} C_{\alpha_\beta} \varepsilon^{\Gamma_{1j}+2\Gamma_{2j}+\cdots+(n_j-1)\Gamma_{n_j-1,j}} \prod_{\gamma \in G}^{n-1} {y_\gamma}^{\alpha_\gamma}$$

and when

$$\sum_{i=0}^{n_j-1} i\Gamma_{ij} = \sum_{i=0}^{n_j-1} i \sum_{\substack{\gamma \in G \\ \pi_j(\gamma)=i}} \alpha_\gamma \equiv 0 \pmod{n_j}$$

the individual terms of the polynomial are invariant under $s_{\mathbf{e}_j}$. □

Theorem 4.12. *Let $G = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$. Then $MZS(G) \equiv Inv(G)$.*

Proof. Let K be a minimal zero sequence of G. Then, $\sum K = 0$, and this can be broken into k diophantine equations, or the following compressed diophantine equation:

$$\sum_{i=0}^{n_i-1} i \left(\sum_{\substack{\gamma \in G \\ \pi_j(\gamma)=i}} \alpha_\gamma \right) \equiv 0 \pmod{n_j}$$

In other words, the sum of some number of elements which have j'th coordinate $1 + \cdots +$ the sum of some number of elements which have j'th coordinate $n_j - 1$ equal to 0 modulo n_j. Thus this corresponds to a minimal invariant polynomial. Conversely, if P is a minimal invariant polynomial, then P contains exactly one term and the exponents of its variables satisfy the diophantine equation

$$\sum_{i=0}^{n_i-1} i \left(\sum_{\substack{\gamma \in G \\ \pi_j(\gamma)=i}} \alpha_\gamma \right) \equiv 0 \pmod{n_j}$$

Thus, this corresponds to a minimal zero sequence. □

4.5 Computational Results

We conclude this section with a table listing the number of minimal zero sequences (and hence the number of invariant polynomials) of the cyclic groups Z_n, broken down into the number of minimal zero sequences of each length. The last column is the total number of minimal zero sequences of the group.

Table 2: Minimal Zero Sequences of $\mathbb{Z}_n$

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16		Total
$\mathbb{Z}_1$		1																	1
$\mathbb{Z}_2$		1	1																2
$\mathbb{Z}_3$		1	1	2															4
$\mathbb{Z}_4$		1	2	2	2														7
$\mathbb{Z}_5$		1	2	4	4	4													15
$\mathbb{Z}_6$		1	3	6	6	2	2												20
$\mathbb{Z}_7$		1	3	8	12	12	6	6											48
$\mathbb{Z}_8$		1	4	10	18	16	8	4	4										65
$\mathbb{Z}_9$		1	4	14	26	32	18	12	6	6									119
$\mathbb{Z}_{10}$		1	5	16	36	48	32	12	8	4	4								166
$\mathbb{Z}_{11}$		1	5	20	50	82	70	50	30	20	10	10							348
$\mathbb{Z}_{12}$		1	6	24	64	104	84	36	20	12	8	4	4						367
$\mathbb{Z}_{13}$		1	6	28	84	168	180	132	84	60	36	24	12	12					827
$\mathbb{Z}_{14}$		1	7	32	104	216	242	162	96	42	30	18	12	6	6				974
$\mathbb{Z}_{15}$		1	7	38	130	306	388	264	120	88	56	40	24	16	8	8			1494
$\mathbb{Z}_{16}$		1	8	42	158	388	532	386	236	144	88	56	40	24	16	8	8		2135
$\mathbb{Z}_{17}$		1	8	48	192	528	832	736	496	352	240	176	112			...			3913
$\mathbb{Z}_{18}$		1	9	54	226	642	1044	822	514	282	174	90	66			...			4038
$\mathbb{Z}_{19}$		1	9	60	270	846	1566	1566	1098	774	540	396	270			...			7936
$\mathbb{Z}_{20}$		1	10	66	314	1020	1972	1912	1120	608	416	272	176			...			8247
$\mathbb{Z}_{21}$		1	10	74	366	1284	2718	2952	1986	1224				...					12967
$\mathbb{Z}_{22}$		1	11	80	420	1532	3422	3900	2810	1830				...					17476
$\mathbb{Z}_{23}$		1	11	88	484	1892	4598	5940	4620	3234				...					29162
$\mathbb{Z}_{24}$		1	12	96	548	2208	5560	6996	4772	2848				...					28065
$\mathbb{Z}_{25}$		1	12	104	624	2684	7324					...							49609
$\mathbb{Z}_{26}$		1	13	112	700	3108	8828					...							59358
$\mathbb{Z}_{27}$		1	13	122	788	3692	11160					...							83420
$\mathbb{Z}_{28}$		1	14	130	878	4244	13364					...							97243
$\mathbb{Z}_{29}$		1	14	140	980	4984	16660					...							164967
$\mathbb{Z}_{30}$		1	15	150	1082	5658	19538					...							152548
$\mathbb{Z}_{31}$		1	15	160						...									283082
$\mathbb{Z}_{32}$		1	16	170						...									295291
$\mathbb{Z}_{33}$		1	16	182						...									405919
$\mathbb{Z}_{34}$		1	17	192						...									508162
$\mathbb{Z}_{35}$		1	17	204						...									674630
$\mathbb{Z}_{36}$		1	18	216						...									708819
$\mathbb{Z}_{37}$									...										1230258
$\mathbb{Z}_{38}$									...										1325732
$\mathbb{Z}_{39}$									...										1709229
$\mathbb{Z}_{40}$									...										1868565
$\mathbb{Z}_{41}$									...										3045109
$\mathbb{Z}_{42}$									...										2804473
$\mathbb{Z}_{43}$									...										4694718
$\mathbb{Z}_{44}$									...										4695997
$\mathbb{Z}_{45}$									...										5902561
$\mathbb{Z}_{46}$									...										7581158
$\mathbb{Z}_{47}$									...										10761816
$\mathbb{Z}_{48}$									...										9772607
$\mathbb{Z}_{49}$									...										15214301
$\mathbb{Z}_{50}$									...										15826998
$\mathbb{Z}_{51}$									...										20930012
$\mathbb{Z}_{52}$									...										23378075
$\mathbb{Z}_{53}$									...										34502651
$\mathbb{Z}_{54}$									...										32192586
$\mathbb{Z}_{55}$									...										44961550
$\mathbb{Z}_{56}$									...										47162627
$\mathbb{Z}_{57}$									...										63662925
$\mathbb{Z}_{58}$									...										74515122
$\mathbb{Z}_{59}$									...										102060484
$\mathbb{Z}_{60}$									...										85954379

Table 3: Minimal Zero Sequences of $\mathbb{Z}_m \oplus \mathbb{Z}_n$

	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4$	$\mathbb{Z}_5$	$\mathbb{Z}_6$	$\mathbb{Z}_7$
$\mathbb{Z}_2$	5	20	39	166	253	974
$\mathbb{Z}_3$	20	69	367	1494	2642	12967
$\mathbb{Z}_4$	39	367	1107	8247	19463	97243
$\mathbb{Z}_5$	166	1494	8247	31029	164967	508162
$\mathbb{Z}_6$	253	2642	19463	164967	390861	4694718
$\mathbb{Z}_7$	974	12967	97243	508162	4694718	9540473

5 Conclusion

In closing, we present further ideas for areas of research, mostly furthering those of section 3. Some similar notes are contained within the main body of the paper.

Some of the ideas presented here are well-considered and known to be difficult, such as the F-T conjecture. However, most of the ideas are fresh and untouched except by the glance that deemed them interesting, accessible, and probably true.

Within section 3, Section 3.3 is the most interesting and most promising for future work, but also the most difficult. Section 3.1 on cyclic groups is also open for further work, and is probably more easily attainable. $\mathcal{B}({\mathbb{Z}_2}^n)$ is a special case; and its potential ends with itself . However, $\mathcal{B}(\mathbb{Z}_n)$, and especially $\mathcal{B}({\mathbb{Z}_3}^n)$, will provide the foundation for future work in groups not so nice. (The nature of research is shown by the fact that by now ago we thought counting the atoms in $\mathcal{B}({\mathbb{Z}_m}^n)$ would have been a solved problem now.)

An example of some ideas that will lead to an understanding and general formula for $\mathcal{B}(\mathbb{Z}_n)$ is the following conjecture: The number of atoms in the following classes is a "nice" multiple of the number of Davenport atoms:

$$a^{n-x}{b_1}^{\beta_1}{b_2}^{\beta_2}...{b_y}^{\beta_y}, \text{ where } n \geq 2(x-1), x \geq 4,$$

$$\text{and } \beta_1 + \beta_2 + ... + \beta_y = x, \beta_i \geq 2.$$

This should give the idea of what is involved in counting by the method of working-down from the Davenport sequences. Furthermore, one should be able to prove the uniqueness of length $n-1$ atoms in $\mathcal{B}(\mathbb{Z}_n)$ to be of the multiplicity class $a^{n-2}b$, and be able to union the multiplicity classes of the above conjecture into the number in length classes. Clearly, it is only a step further to start considering the atoms of all the various orders in the group in a similar manner individually and then summing up all the various results from these explorations of classes of elements of different order.

Note that *order classes* will play a role that they are only trivially playing in ${Z_m}^n$, where every element is of the same order. Order classes need to be defined in a similar manner to our other classes, and there may be more than one way of doing it.

We were lead to the idea of counting atoms by considering isomorphism classes. These were simply multiplicity classes in $\mathcal{B}({\mathbb{Z}_2}^n)$. It seems that with our classes we are really trying to find the classes that uniquely determine the automorphism or isomorphism classes for different groups. The interplay of the various classes, sometimes being equivalent and sometimes partitioning differently is very interesting. Multiplicity classes clearly partition length classes, and dimension classes partition multiplicity classes, so that there is a hierarchy among them. However, the order class seems to be of a different beast, but necessary to consider for groups with various orders. Of the three groups we looked at, $\mathcal{B}(\mathbb{Z}_n)$ had order class different from multiplicity class, but $\mathcal{B}({\mathbb{Z}_2}^n)$

and $\mathcal{B}({\mathbb{Z}_3}^n)$, and in general $B({\mathbb{Z}_n}^n)$, are not partitioned at all by order class, since every element is of the same order.

Order classes and multiplicity classes are found by the same computer program that found minimal zero sequences.

For $\mathcal{B}({\mathbb{Z}_3}^n)$, it is natural to ask about bounding the ratio $|N| : (|I| + |\mathbb{I}|)$, as mentioned in Section 3.3. In addition, it would be nice and easy to produce an overall bound for the function itself. Furthermore, the applications given at the end of that section have been furthered on paper using the help of a Maple program to produce the number of available choices for particular N's when $|N| = 3$. These additional applications were based on an intuitive tree diagram model of the atoms and will probably look nice in the rather new notation of dimension classes.

The explored question of Davenport sequences is, given the block monoid over a finite abelian group, what is the length of the longest atoms? A similar and complimentary question is: given a length, what portion of block monoids over a family of finite abelian groups have atoms that length? If one answer is known for a family of groups, so is the other. Currently the former is better explored than the latter, into which little effort seems to have been put. It is easy to prove the theorem which gives a formula for which n of $(Z_3)^n$ have atoms of a given length m. However, if much progress is made in the direction of section 3, then the informing could flow in the opposite direction, and we could learn more about the Davenport theory from the structure theory that accompanies the counting of atoms. Similarly, in the realm of computation, we could have further multiplicity *inclusion* theorems, which would be more powerful in searches for Davenport sequences than their older brothers, the multiplicity *exclusion* theorems.

Similarly, within the ideas presented in section 3, the more structural theories can feed off the combinatorial proofs and vice versa.

Can a connection be made from counting atoms in $\mathcal{B}({\mathbb{Z}_2}^n)$ to Gaussian coefficients similar and as close as the connection of minimal zero sequences to invariant theory?

Further conjectures include the F-T conjecture: Let G, H be finite abelian groups of the same order, with rank$(G) \leq$ rank (B), then $|\mathcal{A}(\mathcal{B}(G))| \geq |\mathcal{A}(\mathcal{B}(H))|$. This checks out for orders up to about 40 (we have the data, usually just some statistics about the atoms instead of every single atom, stored for groups such fairly small order).

A further conjecture concerns the difference in the number of atoms of two consecutive cyclic groups $\mathcal{B}(\mathbb{Z}_n)$ and $\mathcal{B}(\mathbb{Z}_{n+1})$. Not only is it true that $|\mathcal{A}(\mathcal{B}(\mathbb{Z}_{n+1}))| - |\mathcal{A}(\mathcal{B}(\mathbb{Z}_n))|$ has no upper bound, but it is here conjectured that it has no lower bound either. A lower bound seems to be pushed when $n + 1$ is a composite with many distinct factors and n is a prime.

References

[Foo99] David S. Dummit—Richard M. Foote, *Abstract algebra*, 2nd ed., John Wiley & Sons, 1999.

[Gra94] Graham—Patashnik—Knuth, *Concrete mathematics: A foundation for computer science*, Addison Wesley, 1994.

[Hun97] Thomas Hungerford, *Algebra*, Springer Verlag, 1997.

[Kru69] P. Van Emde Boas — D. Kruyswijk, *A combinatorial problem on finite abelian groups iii*, Mathematical Centre Amsterdam (1969).

[Maz92] Marcin Mazur, *A note on the growth of davenport's constant*, Manuscripta Mathematica (1992).

[Mon91] Ivan Niven—H. S. Zuckerman—H. L. Montgomery, *An introduction to the theory of numbers*, John Wiley & Sons, 1991.

[Nat99] Melvyn B. Nathanson, *Elementary methods in number theory*, Springer Verlag, 1999.

[Nee00] Tristan Needham, *Visual complex analysis*, Clarendon Press, 2000.

[Ols69] J. E. Olson, *A combinatorial problem on finite abelian groups.*, Journal of Number Theory (1969).

[Ros91] Kenneth Ireland—Michael Rosen, *A classical introduction to modern number theory*, Springer Verlag, 1991.

[Ros00] Kenneth H. Rosen, *Handbook of discrete and combinatorial mathematics*, CRC Press, 2000.

[Str48] Carl W. Strom, *Invariants of cyclic groups of equal order and degree*, Proceedings of the Iowa Society of Mathematics (1948).

[vEB69] P. van Emde Boas, *A combinatorial problem on finite abelian groups ii*, Mathematisch Centrum (1969).

[Wri80] G. H. Hardy—E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1980.