College of Creative Studies

University of California, Santa Barbara
College of Creative Studies

Senior Thesis

The Existence of Perfect s-bases of size m for Finite Abelian Groups

Author:

Nicholas Geis

Supervised by:

Karel Casteels

July 13, 2018

Contents

Abstract

Given a finite abelian group G and a subset A of G, we call A an *s-basis* if every element of G can be generated by the sum of at most s elements of A, including repetition. A natural question to ask is,"What is the smallest s-basis for a given s and a group G?" This question and its variations are studied extensively in additive combinatorics. In particular, we consider *perfect* s-bases. An s-basis, A with cardinality m, is considered *perfect* if every element of G can be written as a "unique" sum of at most s elements of A. It is conjectured that there are no perfect s-bases of size m for any abelian group G unless either $s = 1$ or $m = 1$. The conjecture has been shown to hold when $s = 2$ and $s = 3$. We generalize that proof technique in order to prove the conjecture for $s \leq 20$ while providing intuition behind the combinatorial limitations of the structure of finite abelian groups implied by this result.

1 Introduction

Let G be a finite abelian group. Given an $s \in \mathbb{N}$, a classical problem in additive combinatorics is determining the smallest s-basis for G. Formally, finding an m such that

$$m = \min\{|A| : \ A \subseteq G \text{ such that } [0, s]A = G\}.$$

At a New York Number Theory Seminar in 2003, Bela Bajnok gave a talk titled *The Spanning Number and the Independence Number of a Subset of an Abelian Group* [2]. Although his focus was on general spanning sets and s-bases for abelian groups, he introduced the concept of a perfect s-basis of size m. Intuitively, these perfect s-bases are the smallest possible value of m where

$$[0, s]A \leq \binom{m+s}{s} = |G|.$$

He notes that he "could not find perfect spanning sets for $s \geq 2$ and $m \geq 3$." Then in his 2017 book titled *Additive Combinatorics: A Menu of Research Problems* [1], he poses the following conjecture:

Conjecture 1.1. *There are no perfect s-bases of size m for G, unless $s = 1$ or $m = 1$.*

Additionally in [1], Bajnok proves that Conjecture 1.1 holds when $s = 2, 3$.

Theorem 1.2. *Conjecture 1.1 holds when $s = 2, 3$.*

The main focus of this thesis will be attempting to prove Conjecture 1.1. In particular, we show that Conjecture 1.1 can only hold if $s < m$. Then, we generalize the proof technique for Theorem 1.2 in order to prove more supporting results for the validity of Conjecture 1.1.

2 Background

Recall from linear algebra the definition of a spanning set.

Definition 2.1. Let V be an $\mathbb{C}$-space and $A \subseteq V$. We say that A is a *spanning set* if every element of V can be written as a linear combination of elements from A with weights from $\mathbb{C}$.

Let G denote a finite abelian group with order n and $\mathbb{N}$ be the natural numbers including 0. We are interested in finding spanning sets for G.

We first clarify the concept of a linear combination of elements in G without having a field to pull the scalars from. To address this problem, we introduce a scalar multiplication for G by looking at G as a $\mathbb{Z}$-module. In other words, we have the map $\cdot : \mathbb{Z} \times G \to G$ with

$$n \cdot g = ng := \begin{cases} \underbrace{g + g + \ldots + g}_{n-\text{times}}, & \text{when } n \geq 0 \\ -(-n)g, & \text{when } n < 0. \end{cases}$$

Definition 2.2. Let G be an abelian group. Let $A = \{a_i\}_{i=1}^m \subseteq G$. For any $s \in \mathbb{N}$, we define

$$[0, s]A := \left\{ \lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_m a_m \;\middle|\; \lambda_i \in \mathbb{N},\ \sum_{i=1}^{m} \lambda_i \leq s \right\}.$$

Definition 2.2 simply restricts the number of elements in A we can add together. To better see this, consider the following examples:

Example 2.3. Let $G = (\mathbb{Z}/10\mathbb{Z}, +)$ and take $A = \{0, 2, 4\}$. Let $s = 2$. Then

$$[0, 2]A = \{0, 2, 4, 6, 8\}$$

as

$$0 = 0, \quad 2 = 2, \quad 4 = 4, \quad 2 + 4 = 6, \quad 4 + 4 = 8.$$

Example 2.4. Let $G = (\mathbb{Z}/8\mathbb{Z}, +)$ and take $A = \{1\}$. Then

$$[0, 7]A = G$$

as every nonzero element $g \in G$ can be expressed as $g = \lambda \cdot 1$ with $1 \leq \lambda \leq 7$ and $0 = 0 \cdot 1$.

Notice that in Example 2.4, we have that $[0,7]A = G$. Here, A is an example of a spanning set for G.

Definition 2.5. We say that A *spans* G, or A is a *spanning set* for G, if there exists an $s \in \mathbb{N}$ such that

$$[0,s]A = G.$$

Remark 2.6. Notice that even though G is finite, not every subset of G needs to span G. For example, consider $G = (\mathbb{Z}/8\mathbb{Z}, +)$ and $A = \{2\}$. For every $s \in \mathbb{N}$, $[0,s]A$ only contains even elements of $\mathbb{Z}/8\mathbb{Z}$. Hence, A does not span G.

In particular, we are interested in finding spanning sets given an $s \in \mathbb{N}$. This introduces the main focus of this thesis.

Definition 2.7. Let $(G, *)$ be a finite abelian group and $A \subseteq G$. We call A an *s-basis* for G if $[0,s]A = G$.

Example 2.8. Let $G = (\mathbb{Z}/8\mathbb{Z}, +)$ and $A = \{1,3,5,7\}$. We have that A is a 2-basis for G because

$$[0,2]A = \{0,1,2,3,4,5,6,7\} = G.$$

Thus, A is an s-basis for G as every element of G can be obtained by the addition of at most two elements from A.

Notice that the subset defined in Example 2.4 is a 7-basis for $\mathbb{Z}/8\mathbb{Z}$. Thus for the same group, there exist s-bases for different values of s. In fact, notice that the subset from Example 2.8 is also a 7-basis for $\mathbb{Z}/8\mathbb{Z}$. So the existence of an s-basis is not too interesting. In fact, finding an s-basis for a given s can lead to a few degenerate cases. One such example is taking $A = G\backslash\{0\}$ then A is an s-basis for G for every $s \geq 1$. Another example is taking $A = G$.

We will focus on the question of finding an s-basis for G with least cardinality.

Many papers[1] have presented results that provide lower bounds on m given a fixed s and a group G in terms of the order of the group n. However, this thesis will take a different

[1]Refer to Chapter B in [1] to find a survey of the majority of the results in this area.

approach. In particular, we will look for spanning sets of size m that are "maximal." To clarify this, we need to introduce a few more definitions.

For a given $s, m \in \mathbb{N}$ consider the set

$$\Lambda^m([0,s]) := \left\{ (\lambda_1, \ldots, \lambda_m) \in \mathbb{N}^m \;\middle|\; \sum_{i=1}^{m} \lambda_i \leq s \right\}.$$

Notice that if $|A| = m$, then we can rewrite Definition 2.2 using $\Lambda^m([0,s])$ as

$$[0,s]A = \{\lambda_1 a_1 + \ldots + \lambda_m a_m \mid (\lambda_1, \ldots, \lambda_m) \in \Lambda^m([0,s]),\ a_i \in A\}.$$

Thus, if A is an s-basis of size m for G then $|\Lambda^m([0,s])| \geq |G|$ as $\Lambda^m([0,s])$ contains all the possible combinations of elements in A. Through a counting argument, we have that

Proposition 2.9. *For $m, s \in \mathbb{N}$ we have that*

$$|\Lambda^m([0,s])| = \binom{m+s}{s}.$$

Proof. This proof technique is the same as the proof technique for determining the dimension of the vector space of polynomials in n variables with degree at most D from [4].

We are going to reduce this to a simple counting problem by turning each element of $\Lambda^m([0,s])$ into a string of $\star$'s and |'s. Take some $(\lambda_1, \lambda_2, \ldots, \lambda_m) \in \Lambda^m([0,s])$. Begin the string by adding λ_1 many $\star$'s and then adding a |. Continue this process for each λ_i for $1 \leq i \leq m$. Then after adding the final |, add $s - \sum_{i=1}^{m} \lambda_i$ many $\star$'s to the end of the string. We will have s many $\star$'s and m many |'s in our string. Notice that this process creates a bijection between strings of length $m+s$ of s many $\star$'s and m many |'s and $\Lambda^m([0,s])$. Additionally, note that the number of such strings is $\binom{m+s}{s}$ as we simply need to choose the s spots to place our $\star$'s. Hence, Proposition 2.9 holds.

□

Hence,

Corollary 2.10. *If A is an s-basis of size m for G and $|G| = n$, then*

$$n \leq \binom{m+s}{s}.$$

Now, we can look at what it means for a spanning set to be "maximal". In particular, we will look at the extreme case for an s-basis A for a group G when $n = |\Lambda^m([0, s])|$.

Definition 2.11. Let $A \subseteq G$ be an s-basis for G. Let $|G| = n$ and $|A| = m$. We call A a *perfect s-basis of size m* if

$$n = \binom{m+s}{s}.$$

For convenience, we introduce the notation for the generator map.

Definition 2.12. Let G be a finite abelian group and $A = \{a_i\}_{i=1}^m$ be a subset of G. We call the map $F : \Lambda^m([0, s]) \to G$ defined as

$$F((\lambda_1, \ldots, \lambda_m)) = \sum_{i=1}^{m} \lambda_i a_i$$

the *generator map of A*.

Notice that if $A = \{a_i\}_{i=1}^m$ is a perfect s-basis of size m for G, the generator map of A is a surjection. Since surjections between finite sets of equal cardinality are injective, F is injective. Therefore, we have the following result.

Proposition 2.13. *Let G be a finite abelian group and $A \subseteq G$ with $A = \{a_i\}_{i=1}^m$. Then A is a perfect s-basis of size m for G if and only if for every $g \in G$ we have a unique $(\lambda_1, \ldots, \lambda_m) \in \Lambda^m([0, s])$ such that*

$$\lambda_1 a_1 + \ldots + \lambda_m a_m = g.$$

Now, we can pose the simple question: does every group contain a perfect s-basis of size m for some s and m? The short answer is yes.

Example 2.14. For example, consider $A = \{1\}$ and $G = \mathbb{Z}/8\mathbb{Z}$ from Example 2.4. A is a perfect 7-basis of size 1 for G as A spans G and

$$|\mathbb{Z}/8\mathbb{Z}| = 8 = \binom{7+1}{1}.$$

Remark 2.15. Notice that for any s we can find a G and A such that A is a perfect s-basis of size 1 for G. Since A consists of a single element that generates G, G must be cyclic. And by Definition 1.5, we have that $|G| = \binom{s+1}{1} = s + 1$. Recall that there exists only one cyclic group of order n, namely $\mathbb{Z}/n\mathbb{Z}$, up to isomorphism [3]. Hence, $G \cong \mathbb{Z}/(s+1)\mathbb{Z}$.

Now consider the following example:

Example 2.16. Take any abelian group G of order n. Notice that $A = G\backslash\{0\}$ is a perfect 1-basis of size $n-1$. This is trivial as every nonzero element of G is in A and then we form 0 by taking $\lambda_1 = \ldots = \lambda_m = 0$. Since $s = 1$, every element of G is a unique linear combination of elements in A. Hence, by Proposition 2, A is a perfect 1-basis of size $n-1$.

The arguments for both Example 1.2.2 and Example 1.5.1 classify perfect s-bases of size m for abelian groups when $s = 1$ or $m = 1$. In particular, the arguments above can be formalized to prove the following theorem.

Theorem 2.17 ([1])**.** *Let G be a finite abelian group, $A \subseteq G$ and $a \in A$. We have the following:*

1. *$A \subseteq G$ is a perfect 1-basis for G if and only if $A = G\backslash\{0\}$.*
2. *$\{a\} \subseteq G$ is a perfect s-basis for G if and only if $G \cong \mathbb{Z}/(s+1)\mathbb{Z}$ and $\gcd(a, s+1) = 1$.*

Now, what happens when s and m are both not equal to 1? Can we classify all the abelian groups that have perfect s-bases of size m for $s, m > 1$? Currently, there are partial results.

Theorem 2.18 ([1])**.** *For any abelian group G, there are no perfect s-bases of size m for G when $s = 2, 3$ and $m > 1$.*

Theorem 2.18 led to the following conjecture.

Conjecture 2.19 ([1])**.** *For any abelian group G, there are no perfect s-bases of size m for G, unless $s = 1$ or $m = 1$.*

The main focus of this thesis will be proving Conjecture 2.19. In particular, we show that Conjecture 2.19 can only hold if $s < m$. Then, we generalize the proof technique for Theorem 2.18 in order to prove Conjecture 2.19 for larger values of s.

3 Results

3.1 Proof Idea

The proof for Theorem 2.18 can be found in [1]. However, for the sake of self-containment, we will summarize the proof technique here.

First, we fix s. For Theorem 2.18, $s = 2$ or $s = 3$. Then we assume the existence of an abelian group G that contains a perfect s-basis of size m for some $m > 1$. Call this basis A.

Second, we construct a family of disjoint sets based on A. Call this family $\mathcal{F}$. Since all sets of $\mathcal{F}$ are disjoint,

$$\sum_{F \in \mathcal{F}} |F| \leq |G| = \binom{s+m}{m}.$$

By the construction of the sets, the inequality will provide an upper bound to m. In the proof of Theorem 2.18, for both $s = 2$ and $s = 3$, they found $m \leq 3$.

And third, we test each value of $m > 1$. To do so, we rely on the Fundamental Theorem of Finite Abelian Groups.

Theorem 3.1 (The Fundamental Theorem of Finite Abelian Groups [3])**.** *Let G be an abelian group of order $n > 1$ and let the unique factorization of n into distinct prime powers be*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then there exists groups $H_1, H_2, \ldots, H_k$ such that $|H_i| = p_i^{\alpha_i}$ and

$$G \cong A_1 \times A_2 \times \cdots \times A_k.$$

Additionally, for each $H \in \{H_1, H_2, \ldots, H_k\}$ with $|H| = p^{\alpha}$,

$$H \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$, where t and $\beta_1, \ldots, \beta_t$ depend on i.

Example 3.2. When $s = 2$, then $m \leq 3$. So either $|G| = 6$ or $|G| = 10$. By Theorem 3.1, that implies that either $G \cong \mathbb{Z}/6\mathbb{Z}$ or $G \cong \mathbb{Z}/10\mathbb{Z}$.

Example 3.3. When $s = 3$, then $m \leq 3$. So either $|G| = 10$ or $|G| = 20$. By Theorem 3.1, there are 3 possibilities: $G \cong \mathbb{Z}/10\mathbb{Z}$, $G \cong \mathbb{Z}/20\mathbb{Z}$ or $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

Various arguments are used to reach a contradiction once the structure of the group was determined. For example, the latter cases in Example 3.3 where computed and checked explicitly using [5] and [6].

A major issue with this proof technique is that the last step is computationally difficult if the groups are large with highly composite cardinalities. The next sections are devoted to proving a numerical approach to the problem in order to bypass that final step.

3.2 Proof that shows $s < m$

Before beginning this section, I would like to thank Ben Spitz and Cole Hugelmeyer whose algebraic curiosities of the subject led to the formalizations of the techniques below.

Let G be a finite abelian group and $A \subseteq G$ be a perfect s-basis of size m for G. This section concerns itself with proving the following Theorem.

Theorem 3.4. *Let $s, m > 1$ and let G be a finite abelian group. Suppose that $A \subseteq G$ is a perfect s-basis of size m for G. Then $s < m$.*

In order to proof Theorem 3.4, we will develop several algebraic tools.

Definition 3.5. Let G be a finite abelian group and $A = \{a_i\}_{i=1}^m$ be a subset of G. We call the map $\phi : \mathbb{Z}^m \to G$ defined as

$$\phi((\lambda_1, \ldots, \lambda_m)) = \sum_{i=1}^{m} \lambda_i a_i$$

the *full generator map of A*.

Remark 3.6. Notice that $\phi|_{\Lambda^m([0,s])} = F$, where F is the generator map of A from Definition 2.12. Hence, the name *full* generator map of A. Additionally, note that ϕ is a group homomorphism between $\mathbb{Z}^m$ and G as the linearity follows from both $\mathbb{Z}^m$ and G being abelian.

By working with the full generator map, we can utilize the additional group structure of its domain.

Lemma 3.7. *Let G be a finite abelian group and $A \subseteq G$ be a perfect s-basis of size m. Let ϕ be the full generator map of A. Let $x, y \in \ker \phi$. If $x \neq y$, then $(x + \Lambda^m([0,s])) \cap (y + \Lambda^m([0,s])) = \emptyset$.*

Proof. Let $x \neq y \in \ker \phi$ and suppose that $v \in (x + \Lambda^m([0,s])) \cap (y + \Lambda^m([0,s]))$. That implies that there exist $w_1, w_2 \in \Lambda^m([0,s])$ such that

$$v = x + w_1 \quad \text{and} \quad v = y + w_2.$$

However, notice that

$$\phi(v) = \phi(x + w_1) = \phi(x) + \phi(w_1) = \phi(w_1).$$

Similarly, $\phi(v) = \phi(w_2)$. However, since ϕ is injective on $\Lambda^m([0,s])$, we have that $w_1 = w_2$. But this implies that $x = y$ and so Lemma 3.7 holds.

□

Lemma 3.8. *Let G be a finite abelian group and $A \subseteq G$ be a perfect s-basis of size m. Let ϕ be the full generator map of A. For any $x \in \mathbb{Z}^m$, there exists a $y \in \ker \phi$ such that $x \in y + \Lambda^m([0,s])$.*

Proof. Take any $x \in \mathbb{Z}^m$. Consider $y = x - F^{-1}(\phi(x))$, where $F = \phi|_{\Lambda^m([0,s])}$ is the generator map of A. Notice that

$$\phi(y) = \phi(x) - \phi(F^{-1}(\phi(x))) = \phi(x) - \phi(x) = 0.$$

So $y \in \ker \phi$. Additionally, by construction, $F^{-1}(\phi(x)) \in \Lambda^m([0,s])$. Hence, x is of the desired form.

□

Notice that for any $x \in \mathbb{Z}^m$, there exists a $y \in \ker \phi$ such that $x \in y + \Lambda^m([0,s])$ by Lemma 3.8. Additionally, by Lemma 3.7, that y is unique.

Definition 3.9. For any $x \in \mathbb{Z}^m$, let $\mathfrak{s}(x)$ denote the unique element of $\ker \phi$ such that $x \in \mathfrak{s}(x) + \Lambda^m([0,s])$.

Corollary 3.10. *Let G be a finite abelian group and $A \subseteq G$ be a perfect s-basis of size m. Let ϕ be the full generator map of A. Then $\mathbb{Z}^m = \bigsqcup_{y \in \ker \phi} y + \Lambda^m([0,s])$, where $\sqcup$ is the disjoint union.*

Now, we begin the proof of Theorem 3.4.

Proof. Let $s, m > 1$ and let G be a finite abelian group with $A \subseteq G$ a perfect s-basis of size m. Assume that $m \leq s$. Consider the elements

$$d_1 = (s - m + 2, 1, 1, \ldots, 1) \quad \text{and} \quad d_2 = (1, s - m + 2, 1, \ldots, 1).$$

Notice that $d_1, d_2 \notin \Lambda^m([0,s])$. However, for any e_i, where e_i is a standard basis vector for $\mathbb{Z}^m$, we have that $d_1 - e_i, d_2 - e_i \in \Lambda^m([0,s])$.

Now, I claim that $\mathfrak{s}(d_1) = d_1$.

Suppose that $\mathfrak{s}(d_1) \neq d_1$. Since $d_1 \notin \Lambda^m([0,s])$, $\mathfrak{s}(d_1) \neq 0$ by Lemma 3.7. Therefore, there exists a nonzero $y \in \Lambda^m([0,s])$ with $d_1 = \mathfrak{s}(d_1) + y$. Since y is nonzero, there is a $j \in \{1, 2, \ldots, m\}$ such that $y - e_j \in \Lambda^m([0,s])$. Hence, $d_1 - e_j \in \mathfrak{s}(d_1) + \Lambda^m([0,s])$. However, $d_1 - e_j \in \Lambda^m([0,s])$ by construction. So by Lemma 3.7, $\mathfrak{s}(d_1) = 0$ which is a contradiction. Thus, $\mathfrak{s}(d_1) = d_1$.

Similarly, $\mathfrak{s}(d_2) = d_2$. However, notice that

$$(s - m + 2, s - m + 2, 1, \ldots, 1)$$

is in both $\mathfrak{s}(d_1) + \Lambda^m([0,s])$ and $\mathfrak{s}(d_2) + \Lambda^m([0,s])$ which also contradicts Lemma 3.7.

Therefore, Lemma 3.8 does not hold and so we must have that $s < m$.

□

3.3 Counting Argument

For the remainder of this chapter, let $s, m > 1$.

To begin, we introduce notation to describe sum partitions.

Definition 3.11. For a natural number $n > 0$, we say that $P = (p_1, p_2, \ldots, p_k)$, with nonzero $p_i \in \mathbb{N}$, is a *sum partition of* n if

$$n = p_1 + p_2 + \ldots + p_k.$$

Let $\mathbf{P}(n)$ denote the set of *unordered partitions of* n.

Example 3.12. Consider $n = 5$. We have that

$$1+1+1+1+1$$

is a partition of 5. Additionally, we can show that

$$\mathbf{P}(5) = \{(5),\ (1,4),\ (2,3),\ (1,1,3),\ (1,2,2),\ (1,1,1,2),\ (1,1,1,1,4),\ (1,1,1,1,1)\}.$$

Now, let G be a finite abelian group and A be a subset of G. We will define the following sets based on A.

Definition 3.13. Let $|A| \geq n+1$. We define the set $P * A - A$ for a given $P \in \mathbf{P}(n)$ as

$$P*A-A = \{p_1a_1+p_2a_2+\ldots+p_ka_k-a \mid P=(p_1,\ldots,p_k),\ a_i,a \in A \text{ and each unique}\} \subseteq G.$$

Example 3.14. Let $G = (\mathbb{Z}/8\mathbb{Z}, +)$ and $A = \{1,2,5,7\}$. Let $P = (1,1,1)$ and $Q = (1,2)$. Then

$$P * A - A = \{1,3,5\} \quad \text{and} \quad Q * A - A = G.$$

Remark 3.15. Notice that for $n > 0$ and partition $P \in \mathbf{P}(n)$ with $P = (p_1, p_2, \ldots, p_k)$, we have that $k \leq n$ as $(1,1,\ldots,1)$ is the partition with the largest k. Therefore, in Definition 3.13, $|A| \geq n+1$ ensures that we have enough unique elements of A to properly define $P * A - A$.

Now, we can connect the tools above to perfect s-bases for finite abelian groups.

Theorem 3.16. *Let G be a finite abelian group and let A be a perfect s-basis of size m for G. Let $P, Q \in \mathbf{P}(s-1)$ be distinct sum partitions of $s-1$ with $P = (p_1, p_2, \ldots, p_k)$ and $Q = (q_1, q_2, \ldots, q_l)$. Then*

$$(P * A - A) \cap (Q * A - A) = \emptyset.$$

Proof. Let G be a finite abelian group and let A be a perfect s-basis of size m for G with $s, m > 1$. By Theorem 3.4, we have that $s < m$. Take $P, Q \in \mathbf{P}(s-1)$ with $P \neq Q$ and $P = (p_1, p_2, \ldots, p_k)$ and $Q = (q_1, q_2, \ldots, q_l)$. Since $k \leq s < m$ and $l \leq s < m$, both $P * A - A$ and $Q * A - A$ are well-defined.

Assume for the sake of contradiction that there exists an $x \in G$ such that

$$x \in (P * A - A) \cap (Q * A - A).$$

Since x is in the intersection we have that

$$x = p_1 a_1 + p_2 a_2 + \ldots + p_k a_k - a \tag{1}$$

and

$$x = q_1 a_1' + q_2 a_2' + \ldots + q_l a_l' - a' \tag{2}$$

where a_i and a are all unique and a_j' and a' are all unique. Equations (1) and (2) imply that

$$p_1 a_1 + p_2 a_2 + \ldots + p_k a_k + a' = q_1 a_1' + q_2 a_2' + \ldots + q_l a_l' + a. \tag{3}$$

Since A is a perfect s-basis for G and $\sum_{i=1}^{k} p_i + 1 \leq s$, we have that $a \in \{a_1, a_2, \ldots, a_k, a'\}$. By construction, $a \neq a_i$ for all i so $a = a'$.

We reduce (3) to

$$p_1 a_1 + p_2 a_2 + \ldots + p_k a_k = q_1 a_1' + q_2 a_2' + \ldots + q_l a_l' = g. \tag{4}$$

Order the elements of A as $\{\alpha_i\}_{i=1}^{m}$. Next, we convert P and Q into elements of $\Lambda^m([0, s])$. For $P = (p_1, p_2, \ldots, p_k)$, consider the tuple $(p_1', p_2', \ldots, p_m')$ defined as

$$p_i' = \begin{cases} p_j, & \text{if } \alpha_i = a_j \text{ for some } j \text{ in (3)} \\ 0, & \text{else.} \end{cases}$$

Similarly, we form $(q_1', q_2', \ldots, q_m')$. By construction, $\sum_{i=1}^{m} p_i' = \sum_{j=1}^{k} p_j = s - 1$. So

$$(p_1', p_2', \ldots, p_m'), (q_1', q_2', \ldots, q_m') \in \Lambda^m([0, s]).$$

Then by Proposition 2.13, we have that $(p_1', p_2', \ldots, p_m') = (q_1', q_2', \ldots, q_m')$ or equivalently $P = Q$. Therefore, the result holds and our sets are disjoint.

□

Notice that for any natural numbers $1 \leq N \leq M \leq s - 1$, the result from Theorem 3.16 holds for any $P \in \mathbf{P}(N)$ and for any $Q \in \mathbf{P}(M)$. So we have the following corollary.

Corollary 3.17. *Let G be a finite abelian group and let A be a perfect s-basis of size m for G. Let $N, M \in \mathbb{N}$ and $N \leq M \leq s-1$. Let $P \in \mathbf{P}(N)$ and $Q \in \mathbf{P}(M)$ be distinct sum partitions of N and M respectively with $P = (p_1, p_2, \ldots, p_k)$ and $Q = (q_1, q_2, \ldots, q_l)$. Then*

$$(P * A - A) \cap (Q * A - A) = \emptyset.$$

Since the sets described in Corollary 3.17 are all disjoint subsets of G, we have that

$$\sum_{l=2}^{s-1} \sum_{P \in \mathbf{P}(l)} |P * A - A| \leq |G|. \tag{5}$$

In particular, we can count $|P * A - A|$ for a given $P \in \mathbf{P}(k)$.

Proposition 3.18. *Let $N \leq s-1$ be a natural number and $P \in \mathbf{P}(N)$ with $P = (p_1, \ldots, p_{k_P})$. Then*

$$|P \cdot A - A| = \frac{m(m-1) \cdot \ldots \cdot (m - (k_P + 1))}{\prod_{i=1}^{s-1} \sigma_P(i)!}$$

where $\sigma_P(i)$ is the number of times that i appears in P.

Proof. This will be done through a simple counting argument. All elements of $P \cdot A - A$ are of the form

$$p_1 a_1 + p_2 a_2 + \ldots + p_{k_P} a_{k_P} - a$$

where each a_i and a are different. Thus there are simply

$$m(m-1) \cdot \ldots \cdot (m - (k_P + 1))$$

many possible combinations including repeated combinations. Since G is abelian, a repeated combination occurs when there exist $i, j \in \{1, \ldots, k_P\}$ such that $i \neq j$ but $p_i = p_j$. For each $i \in \{1, \ldots, s-1\}$, there are $\sigma_P(i)!$ many repeated combinations. Thus to avoid repetition, we simply divide and get the desired result. □

Corollary 3.19. *Let G be a finite abelian group with a perfect s-basis of size m. Let $N \leq s-1$ be a natural number and $P \in \mathbf{P}(N)$ with $P = (p_1, p_2, \ldots, p_{k_P})$. Then*

$$\sum_{l=2}^{s-1} \sum_{P \in \mathbf{P}(l)} \frac{m(m-1) \cdot \ldots \cdot (m - k_P)}{\prod_{i=1}^{s-1} \sigma_P(i)!} \leq \binom{m+s}{s}.$$

Proof. Notice that from (5), Proposition 3.18 and Definition 2.11, we get that

$$\sum_{l=2}^{s-1} \sum_{P \in \mathbf{P}(l)} \frac{m(m-1)\cdot \ldots \cdot (m-k_P)}{\prod_{i=1}^{s-1} \sigma_P(i)!} = \left| \bigcup_{l \in \{2,3,\ldots,s-1\}} (P \cdot A - A) \right| \leq |G| = \binom{m+s}{s}$$

□

For simplicity, we provide names for the functions in Corollary 3.19. Let

$$p_s(m) := \binom{m+s}{s} \tag{6}$$

and

$$q_s(m) := \sum_{l=2}^{s-1} \sum_{P \in \mathbf{P}(l)} \frac{m(m-1)\cdot \ldots \cdot (m-k_P)}{\prod_{i=1}^{s-1} \sigma_P(i)}. \tag{7}$$

Notice both $p_s(m)$ and $q_s(m)$ are polynomials. Next, we outline a few properties of both polynomials. Let $\deg(f)$ be the degree of a polynomial f and $\text{coeff}(f)$ be the leading coefficient.

Proposition 3.20. For $p_s(m)$ defined at (6), $\deg(p_s) = s$ and $\text{coeff}(p_s) = \frac{1}{s!}$.

Proof. This is immediate by expanding the binomial coefficient in the definition of p_s in (6). □

Proposition 3.21. For $q_s(m)$ defined at (7), $\deg(q_s) = s$ and $\text{coeff}(q_s) = \frac{1}{(s-1)!}$.

Proof. Let $\mathbf{P} = \bigcup_{l \in \{2,3,\ldots,s-1\}} \mathbf{P}(l)$. Notice that

$$\deg(q_s) = \max_{P \in \mathbf{P}} \{k_P \mid P = (p_1, p_2, \ldots, p_{k_P})\} + 1$$

by the construction of q_s. Additionally, k_P is maximized by the all 1's partition of $s-1$ so $k_P = s-1$. Hence, $\deg(q_s) = s$. It is immediate that $\text{coeff}(q_s) = \frac{1}{(s-1)!}$ as the all 1's partition of $s-1$ is the only partition that has a degree s monomial. □

By Corollary 3.19, we are interested in finding integer values of $m \geq 0$ such that

$$p_s(m) - q_s(m) \geq 0.$$

First, notice that $p_s(0) - q_s(0) = 1$ for $s \geq 3$. So there exists a region where both m and $p_s(m) - q_s(m)$ are strictly positive. And second, note that coeff$(p_s - q_s) < 0$ by Propositions 3.20 and 3.21. Since $p_s - q_s$ is a polynomial with a negative leading coefficient,

$$\lim_{m \to \infty} p_s(m) - q_s(m) = -\infty.$$

As a result,

$$\sup_{m \in \mathbb{N}} \{m \mid p_s(m) - q_s(m) > 0\} < \infty.$$

Hence, we have the following theorem.

Theorem 3.22. *Conjecture 2.19 is true for $m, s > 1$ if*

$$\max\{\alpha \mid \textit{where } \alpha \textit{ is a real root of } p_s(m) - q_s(m)\} \leq s.$$

Proof. Suppose that the conjecture does not hold. Then there exists an abelian group G with a perfect s-basis of size size m for some values of $s, m > 1$. From the argument above, we have that

$$\sup_{m \in \mathbb{N}} \{m \mid p_s(m) - q_s(m) > 0\} < \infty.$$

Since $p_s(m) - q_s(m)$ is a polynomial, it is continuous. Therefore, the largest natural number, say M, such that $p_s(m) - q_s(m) > 0$ will have a real root between M and $M + 1$. Thus,

$$\max\{\alpha \mid \text{where } \alpha \text{ is a real root of } p_s(m) - q_s(m)\} < \infty.$$

Additionally, since $s < m$ from Theorem 3.4, we must have that

$$\Big\lfloor \max\{\alpha \mid \text{where } \alpha \text{ is a real root of } p_s(m) - q_s(m)\} \Big\rfloor \geq m > s.$$

Hence, we have shown the contrapositive of Theorem 3.22.

□

Theorem 3.22 is very useful as it simplifies the original proof technique from [1]. Instead of finding an upper bound on m and checking every possible group using the Fundamental Theorem of Finite Abelian Groups, we only need to compute the polynomial $p_s(m) - q_s(m)$ and compare the maximum real root to s. For small cases like $s \leq 20$, we computed the polynomials and their maximum real roots using code in Mathematica. The next pages contain a table of the polynomials and their maximum real root for $s \in \{3, 4, \ldots, 20\}$.

Table 1: $p_s(m) - q_s(m)$ **Polynomials and Maximum Roots**

s	$p_s(m) - q_s(m)$	approximate max real root
4	$-\frac{x^4}{8} - \frac{x^3}{12} + \frac{17x^2}{8} + \frac{25x}{12} + 1$	4.29537
5	$-\frac{x^5}{30} - \frac{x^4}{8} + \frac{x^3}{4} + \frac{21x^2}{8} + \frac{137x}{60} + 1$	4.04907
6	$-\frac{x^6}{144} - \frac{13x^5}{240} - \frac{7x^4}{144} + \frac{29x^3}{48} + \frac{55x^2}{18} + \frac{49x}{20} + 1$	4.02851
7	$-\frac{x^7}{840} - \frac{11x^6}{720} - \frac{13x^5}{240} + \frac{11x^4}{144} + \frac{77x^3}{80} + \frac{619x^2}{180} + \frac{363x}{140} + 1$	4.09048
8	$-\frac{x^8}{5760} - \frac{11x^7}{3360} - \frac{61x^6}{2880} - \frac{x^5}{30} + \frac{1351x^4}{5760} + \frac{211x^3}{160} + \frac{5453x^2}{1440} + \frac{761x}{280} + 1$	4.18896
9	$-\frac{x^9}{45360} - \frac{23x^8}{40320} - \frac{169x^7}{30240} - \frac{13x^6}{576} + \frac{7x^5}{1080} + \frac{2399x^4}{5760} + \frac{151517x^3}{90720} + \frac{8279x^2}{2016} + \frac{7129x}{2520} + 1$	4.30459
10	$-\frac{x^{10}}{403200} - \frac{61x^9}{725760} - \frac{23x^8}{20160} - \frac{907x^7}{120960} - \frac{353x^6}{19200} + \frac{2183x^5}{34560} + \frac{24841x^4}{40320} + \frac{365683x^3}{181440} + \frac{221933x^2}{50400} + \frac{7381x}{2520} + 1$	4.428
11	$-\frac{x^{11}}{3991680} - \frac{13x^{10}}{1209600} - \frac{139x^9}{725760} - \frac{x^8}{560} - \frac{19x^7}{2240} - \frac{469x^6}{57600} + \frac{97801x^5}{725760} + \frac{100291x^4}{120960} + \frac{427117x^3}{181440} + \frac{235913x^2}{50400} + \frac{83711x}{27720} + 1$	4.55428
12	$-\frac{x^{12}}{43545600} - \frac{97x^{11}}{79833600} - \frac{1193x^{10}}{43545600} - \frac{491x^9}{1451520} - \frac{34661x^8}{14515200} - \frac{19687x^7}{2419200} + \frac{362461x^6}{43545600} + \frac{63731x^5}{290304} + \frac{11458271x^4}{10886400} + \frac{4872997x^3}{1814400} + \frac{186791x^2}{37800} + \frac{86021x}{27720} + 1$	4.68077

13	$-\frac{x^{13}}{518918400}-\frac{59x^{12}}{479001600}-\frac{13x^{11}}{3801600}-\frac{2333x^{10}}{43545600}-\frac{3697x^9}{7257600}-\frac{5867x^8}{2073600}-\frac{44729x^7}{7257600}+\frac{1349641x^6}{43545600}+\frac{109211x^5}{345600}+\frac{13978619x^4}{10886400}+\frac{60085523x^3}{19958400}+\frac{154079x^2}{29700}+\frac{1145993x}{360360}+1$	4.80601
14	$-\frac{x^{14}}{6706022400}-\frac{47x^{13}}{4151347200}-\frac{11x^{12}}{29030400}-\frac{467x^{11}}{63866880}-\frac{221x^{10}}{2488320}-\frac{19867x^9}{29030400}-\frac{1828333x^8}{609638400}-\frac{2711x^7}{1161216}+\frac{24089x^6}{403200}+\frac{1534597x^5}{3628800}+\frac{13018031x^4}{8553600}+\frac{13286587x^3}{3991680}+\frac{2869009x^2}{529200}+\frac{1171733x}{360360}+1$	4.92923
15	$-\frac{x^{15}}{93405312000}-\frac{83x^{14}}{87178291200}-\frac{1411x^{13}}{37362124800}-\frac{841x^{12}}{958003200}-\frac{27029x^{11}}{2052864000}-\frac{47x^{10}}{358400}-\frac{219271x^9}{261273600}-\frac{1704671x^8}{609638400}+\frac{4584763x^7}{1306368000}+\frac{2055239x^6}{21772800}+\frac{13833709x^5}{25660800}+\frac{8805947x^4}{4989600}+\frac{4722176903x^3}{1297296000}+\frac{15818087x^2}{2802800}+\frac{1195757x}{360360}+1$	5.05003
16	$-\frac{x^{16}}{1394852659200}-\frac{193x^{15}}{2615348736000}-\frac{1193x^{14}}{348713164800}-\frac{3517x^{13}}{37362124800}-\frac{23x^{12}}{13516800}-\frac{75557x^{11}}{3592512000}-\frac{432349x^{10}}{2438553600}-\frac{1734799x^9}{1828915200}-\frac{20790671x^8}{9754214400}+\frac{30005921x^7}{2612736000}+\frac{12292769x^6}{91238400}+\frac{476845429x^5}{718502400}+\frac{58460417317x^4}{29059430400}+\frac{71651300797x^3}{18162144000}+\frac{1181714719x^2}{201801600}+\frac{2436559x}{720720}+1$	5.16825
17	$-\frac{x^{17}}{22230464256000}-\frac{37x^{16}}{6974263296000}-\frac{743x^{15}}{2615348736000}-\frac{3181x^{14}}{348713164800}-\frac{1139x^{13}}{5837832000}-\frac{37199x^{12}}{12773376000}-\frac{1029827x^{11}}{33530112000}-\frac{543857x^{10}}{2438553600}-\frac{9019033x^9}{9144576000}-\frac{45187067x^8}{48771072000}+\frac{622771451x^7}{28740096000}+\frac{4611983x^6}{25546752}+\frac{260150480027x^5}{326918592000}+\frac{328627862089x^4}{145297152000}+\frac{77080688557x^3}{18162144000}+\frac{407562373x^2}{67267200}+\frac{42142223x}{12252240}+1$	5.28386

18	$-\frac{x^{18}}{376610217984000}-\frac{23x^{17}}{64670441472000}-\frac{1367x^{16}}{62768369664000}-\frac{59x^{15}}{73156608000}-\frac{114767x^{14}}{5706215424000}-\frac{151751x^{13}}{426995712000}-\frac{46733x^{12}}{10287648000}-\frac{11206141x^{11}}{268240896000}-\frac{231123517x^{10}}{877879296000}-\frac{271194739x^{9}}{292626432000}+\frac{4280782903x^{8}}{4828336128000}+\frac{178264117x^{7}}{5225472000}+\frac{1362625803629x^{6}}{5884534656000}+\frac{222226979809x^{5}}{237758976000}+\frac{298886881199x^{4}}{118879488000}+\frac{3169345127x^{3}}{698544000}+\frac{1032537721x^{2}}{165110400}+\frac{14274301x}{4084080}+1$	5.39689
19	$-\frac{x^{19}}{6758061133824000}-\frac{x^{18}}{44771844096000}-\frac{1103x^{17}}{711374856192000}-\frac{823x^{16}}{12553673932800}-\frac{821x^{15}}{435891456000}-\frac{2435203x^{14}}{62768369664000}-\frac{12301049x^{13}}{20922789888000}-\frac{4772557x^{12}}{724250419200}-\frac{86202353x^{11}}{1609445376000}-\frac{256723123x^{10}}{877879296000}-\frac{799511393x^{9}}{1072963584000}+\frac{11821513x^{8}}{3511517184}+\frac{10220840479x^{7}}{209227898880}+\frac{260361136219x^{6}}{905313024000}+\frac{2823932984849x^{5}}{2615348736000}+\frac{724059040457x^{4}}{261534873600}+\frac{186197716633x^{3}}{38594556000}+\frac{198865123867x^{2}}{30875644800}+\frac{275295799x}{77597520}+1$	5.50742
20	$-\frac{x^{20}}{128047474114560000}-\frac{107x^{19}}{81096733605888000}-\frac{29x^{18}}{281423020032000}-\frac{2339x^{17}}{474249904128000}-\frac{67621x^{16}}{418455797760000}-\frac{22909x^{15}}{5977939968000}-\frac{51011447x^{14}}{753220435968000}-\frac{113266403x^{13}}{125536739328000}-\frac{106542329x^{12}}{11824496640000}-\frac{419755723x^{11}}{6437781504000}-\frac{435623887x^{10}}{1430618112000}-\frac{384117823x^{9}}{919683072000}+\frac{3089843515537x^{8}}{470762772480000}+\frac{2067893334883x^{7}}{31384184832000}+\frac{360474244787x^{6}}{1034643456000}+\frac{6436090552531x^{5}}{5230697472000}+\frac{336146145411577x^{4}}{111152321280000}+\frac{90093517097x^{3}}{17643225600}+\frac{40886468201x^{2}}{6175128960}+\frac{55835135x}{15519504}+1$	5.61556

Notice that Table 1 implies the following theorem.

Theorem 3.23. *For $3 \leq s \leq 20$, Conjecture 2.19 holds.*

Proof. This is an application of Theorem 3.22 for $s \in \{3, 4, \ldots, 20\}$ using the values computed from Table 1. □

4 Future Work

As an extension to Theorem 3.23, Conjecture 2.19 was verified using the same Mathematica code up to s = 50. Additionally, the slow growth rate of the maximum zeros strongly implies the validity of Conjecture 2.19. The immediate next step would be to show the following conjecture.

Conjecture 4.1. *Let*

$$p_s(m) := \binom{m+s}{s}$$

and

$$q_s(m) := \sum_{l=2}^{s-1} \sum_{P \in \mathbf{P}(l)} \frac{m(m-1)\cdot \ldots \cdot (m-k_P)}{\prod_{i=1}^{s-1} \sigma_P(i)}.$$

For every $s \in \mathbb{N}$,

$$\max\{\alpha \mid \textit{where } \alpha \textit{ is a real root of } p_s(m) - q_s(m)\} \leq s.$$

A proof of Conjecture 4.1 immediately proves Conjecture 2.19 by Theorem 3.22.

This combinatorial approach shows that a perfect s-basis of size m for $s, m > 1$ cannot happen for a finite abelian group because it encodes "too much" information about each element. The group elements are forced to overlap in terms of their combinations of basis elements. Using more algebraic methods like the techniques in Section 3.2 may yield intuition behind those overlaps and other underlaying algebraic limitations to the perfect s-basis structures.

Finally, we can make an adjustment to the definition of perfect s-bases for abelian groups by substituting the set

$$Z^m([0,s]) := \left\{ (\zeta_1, \ldots, \zeta_m) \in \mathbb{Z}^m \;\middle|\; \sum_{i=1}^{m} |\zeta_i| \leq s \right\}$$

in the place of $\Lambda^m([0,s])$. We will call a subset of this type a Z-perfect s-basis. Consider the following example.

Example 4.2. Let $G = \mathbb{Z}/25\mathbb{Z}$ and $A = \{3, 4\}$. We can verify that A is a Z-perfect 3-basis for G.

The idea of a Z-perfect s-basis is mentioned briefly in [2], but is not present in the later paper [1]. Since examples of Z-perfect s-bases exist for $s, m > 1$, investigating the following statement is fruitful.

Statement 1. *Classify all examples of Z-perfect s-bases for $s, m > 1$.*

5 Acknowledgements

First and foremost, I would like to thank Karel Casteels for both being my advisor and allowing me to participate in his research group during the 2017 UCSB REU. Additionally, I would like to thank the Santa Barbara Math REU for providing a wonderful and motivating research environment, the NSF and UCSB RTG for funding the initial stages of my research, and Bill Jacob and Maribel Bueno Cachadina for overseeing the Senior Thesis course at UCSB. Finally, I would like to thank my peers for their words of encouragement and their aid in the research process. In particular, I want to specifically say my thanks to Diljit Singh, Ben Spitz, and Cole Hugelmeyer.

References

[1] Bela Bajnok, *Additive Combinatorics: A Menu of Research Problems*. `https://arxiv.org/pdf/1705.07444.pdf`, 2017, 129-132.

[2] D. and G. Chudnovsky and M. Nathanson, *Number Theory: New York Seminar 2003*. Springer-Verlag New York, Inc., New York, 2004.

[3] D. David and R. Foote, *Abstract Analysis (3rd Edition)*, 2004.

[4] Larry Guth, *Polynomial Methods in Combinatorics*. 2016.

[5] Samir Lalvani, *samSets*, `http://www.cs.gettysburg.edu/ lalvsa01/`.

[6] Samir Lalvani, *irSets*, `http://www.cs.gettysburg.edu/ lalvsa01/`.