Central European University

Masters Thesis

Sumset Estimates in Abelian Groups

Author:
Daniel Glasscock

Supervisor:
Dr. Gergely Harcos

May 30, 2011

Contents

Introduction

Let A be a finite set in an abelian group. We define

$$A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\},$$
$$A - A = \{a_1 - a_2 \mid a_1, a_2 \in A\}$$

to be the *sum set* and *difference set* of A, respectively. The cardinalities of these sets are denoted by $|A|$, $|A + A|$, and $|A - A|$.

Let $|A| = n$. It is immediate that $n \leq |A \pm A| \leq n^2$; it is not difficult to show (Lemma 1.4) that

$$n \leq |A + A| \leq n(n + 1)/2,$$
$$n \leq |A - A| \leq n(n - 1) + 1$$

and that these bounds are achieved. If n, s, and d are positive integers such that $n \leq s \leq n(n+1)/2$ and $n \leq d \leq n(n-1)+1$, then it is an easy exercise to construct sets A, A' in some abelian group with $|A| = |A'| = n$ and $|A+A| = s$, $|A' - A'| = d$. It is in general, however, impossible to construct a single set A with $|A| = n$, $|A + A| = s$, $|A - A| = d$.

In this thesis, we are concerned with understanding what triples (n, s, d) are attainable and generalizations of this problem. We explore the interplay between $|A + A|$, $|A - A|$, and the cardinalities of higher sumsets, as well as the cardinalities of sumsets involving multiple distinct sets.

Freĭman and Pigarev [25] in 1973 showed that

$$|A + A|^{3/4} \leq |A - A| \leq |A + A|^{4/3}$$

when A is a finite set of real vectors. In 1976, Imre Ruzsa [27] showed by elementary means that

$$\left(\frac{|A + A|}{|A|}\right)^{1/3} \leq \frac{|A - A|}{|A|} \leq \left(\frac{|A + A|}{|A|}\right)^{2}$$

when A is a finite set of integers. These are some of the first examples of the non-trivial relationship between $|A+A|$ and $|A-A|$. Both of these results have since been shown to hold in arbitrary abelian groups.

Much weaker connections between $|A + A|$ and $|A - A|$ existed before this, but they relied on deeper inverse theorems concerning the structure of the set A. Freĭman's famous theorem from the late 1960's, for example, gives a structural description of sets A for which $|A + A|$ is small. This information can be used to get a weak upper bound on $|A - A|$. Understanding such inverse theorems and their generalizations motivated the early study of sumset estimates.

Since the late 1970's, sumset estimates have taken on a life of their own. We briefly mention two landmarks here. In 1989, Ruzsa [28] published a simplified version of Helmut Plünnecke's graph theoretic method for handling the repeated addition of an integer basis to a set of integers. Plünnecke's method is still one of the most important tools in estimating sumsets; see Section 1.3.4. Very recently, Giorgis Petridis announced a simplified proof of Plünnecke's inequality and elementary proofs of many important corollaries to Ruzsa's results with Plünnecke's method; see Section 2.2.3.

This thesis explores many of the most important results over the last 35 years in sumset estimates. We turn now to an outline of the work and briefly recall a few of the main results.

This thesis is divided into two main chapters. Chapter 1 is devoted to the study of sumset estimates which involve only a single, finite set in an abelian group. Chapter 2 is devoted to the study of those estimates with two or more possibly distinct sets. We call the former *symmetric* sumset estimates and the latter *asymmetric* sumset estimates.

Each chapter is divided further into two sections. The first section covers estimates which involve only one addition or subtraction, while the second covers estimates involving repeated addition and subtraction. We call the former *lower* sumset estimates and the latter *higher* sumset estimates.

We mention some of the most important results here. The most important lower sumset estimates are Theorems 2.7 and 2.8.

Theorem. *For finite sets A, B, and C in an abelian group, we have*

$$|A||B-C| \leq |A-B||A-C|,$$
$$|A||B+C| \leq |A+B||A+C|.$$

These inequalities were shown by Ruzsa in 1976 and 1989, respectively. The second, however, is historically much more difficult than the first; until 2011, it depended on Plünnecke's method. We present elementary proofs of both of these inequalities in Sections 2.2.2 and 2.2.3.

The most important symmetric corollary to these theorems is Theorem 1.12. Freĭman and Pigarev's 1973 result follows easily from these inequalities, as is shown in Section 1.2.5.

Theorem. *For a finite set A in an abelian group, we have*

$$\left(\frac{|A+A|}{|A|}\right)^{1/2} \leq \frac{|A-A|}{|A|} \leq \left(\frac{|A+A|}{|A|}\right)^{2}.$$

For the higher estimates, the most important result is Plünnecke's inequality, Theorem 1.29.

Theorem. *Let A, B be finite sets in an abelian group, $i \leq k$ be integers, $|A| = n$, and $|A+iB| = \alpha n$. There exists a non-empty $X \subseteq A$ such that*

$$|X+kB| \leq \alpha^{k/i}|X|.$$

This result relies on Plünnecke's theorem which we do not prove in this thesis. A weaker version with an elementary proof is given in Section 2.3.2. The most important corollary is the Plünnecke-Ruzsa inequality and its generalizations from Section 2.3.3.

Theorem. *Let A, B_1, ..., B_k be finite sets in an abelian group, $|A| = n$, $|A+B_i| = \alpha_i n$. Then there exists a non-empty $X \subseteq A$ such that*

$$|X+B_1+\cdots+B_k| = \alpha_1 \cdots \alpha_k |X|.$$

There are finally two appendices which are referenced throughout the thesis. Appendix A is concerned with the behavior of sumsets under products and projections. Most importantly, it reduces the study of sumset estimates in torsion-free abelian groups to sumset estimates in the integers. Appendix B details two constructions of sets with many more differences than sums.

Besides the extended simplex examples of Hennecart, Robert, and Yudin in Appendix B and the formalized comments from Gowers' blog post on Petridis' new work, there are no original results presented in this thesis. The presentation and order of the material is, however, mostly new. The author strove to collect and organize results in a meaningful and enlightening way and to highlight open questions and conjectures.

Chapter 1 is intended to be especially well motivated. Many of the results are corollaries to more general theorems from Chapter 2, and in this way Chapter 1 motivates Chapter 2. In addition to serving as a reference, this thesis was written to serve as an introduction to the field. Section 1.3.3, for example, exists solely to motivate the section following it.

There are many interesting questions related to sumset estimates that are not addressed in this thesis; we briefly mention some of them here. The closest related results which are not included are those showing that Plünnecke-type results are not possible in various situations. These theorems generally concern bounds on sumsets of *all* subsets of the set in question.

There has been much work concerning sumset estimates when something is known about the structure of the set or the ambient group. The famous Cauchy-Davenport theorem, for example, is the lower bound in Lemma 2.2 in the case $G = \mathbb{F}_p$. One may consider how the existence of arithmetic progressions in, or the density of, a set of integers affects the behavior of the sumsets. For multi-dimensional sets, the dimension of the set being considered may be used to have better control over the cardinality of sumsets.

Sum/product estimates and problems involving infinte sets of integers are not considered in this thesis. We do not consider minimal range type problems (with Sidon sets, for example) or problems specifically involving sets with more sums than differences. Beyond the theorems in Section 2.2.1, there is no further mention of inverse theorems. We do not explore the relationship between sumset estimates and entropy inequalities. Finally, we do not consider sumset estimates in non-abelian groups.

The author would like to thank Dr. Gergely Harcos for his close inspection and detailed remarks on this work. A warm thanks is also extended to Dr. Imre Ruzsa who kindly and patiently introduced me to the subject and made this thesis possible.

Chapter 1: Symmetric sumset estimates

In this chapter we explore sumset estimates involving a single finite set in an abelian group. We leave the proofs of some estimates to the next chapter since they are just as easily shown in a more general setting. We distinguish between torsion-free and arbitrary abelian groups when improvements are possible.

1.1 Definitions, examples, and affine equivalence

Let A be a finite set in an abelian group. We define

$$A + A = \{a_1 + a_2 \mid a_1, a_2 \in A\},$$
$$A - A = \{a_1 - a_2 \mid a_1, a_2 \in A\}$$

to be the *sum set* and *difference set* of A, respectively. We call these the *lower sumsets* of A. We will be concerned primarily with the cardinalities of these sets, denoted by $|A|$, $|A + A|$, and $|A - A|$.

Examples 1.1

If $A = \{1, 2, \ldots, n\}$, then $A+A = \{2, 3, \ldots, 2n\}$, $A-A = \{-n+1, \ldots, n-1\}$, and so $|A+A| = |A-A| = 2n-1$. A set of the form $\{a, a+d, \ldots, a+(n-1)d\}$ with $a, d \in \mathbb{Z}$, $d \neq 0$, and $n \in \mathbb{N}$ is called an *arithmetic progression* of *length* n with *base* a and *step* d. An arithmetic progression in an abelian group G is a set of the same form with $a, d \in G$, $d \neq 0$. A straight-forward calculation gives that arithmetic progressions of length n in the integers (more generally, in torsion-free abelian groups) have $2n-1$ sums and $2n-1$ differences.

Let $A = \{2^0, 2^1, \ldots, 2^{n-1}\}$. Because the only solutions to the equations $x_1 + x_2 = x_3 + x_4$ and $x_1 - x_2 = x_3 - x_4$ in A are the trivial ones, one may check that $|A + A| = n(n+1)/2$ and $|A - A| = n(n-1) + 1$ (see Lemma 1.4). Such a set is called a *Sidon set* and is said to be in *general position*. We call a solution to $x_1 + x_2 = x_3 + x_4$ a *coincidence* among the sums of A, and similarly for the differences. Hence a Sidon set is a set in which there are no non-trivial coincidences among the sums or differences.

Let A be a finite subgroup of an abelian group G. We see that $A \subseteq A + A$ since $0 \in A$, and $A + A \subseteq A$ since A is closed under addition. The same is true for $A - A$, hence $A + A = A - A = A$. If A is a coset of a finite subgroup, then it may be quickly verified that $|A + A| = |A - A| = |A|$.

Let k be a positive integer. We denote the k-fold sum $A + \cdots + A$ by kA, and we extend this to all integers by defining $(-k)A$ to be $-(kA) = -A - \cdots - A$ and $0A = \{0\}$. For integers k, l, we write $kA - lA$ to mean $kA + (-l)A$. When $|k| + |l| > 2$, we call these the *higher sumsets* of A. Again, we will be primarily interested in the cardinality $|kA - lA|$.

When we write kA, we implicitly assume that $k \neq 0$ so that $|kA| \geq |A|$. Similarly, when we write $kA - lA$, we implicitly assume that $k, l \geq 0$ and $(k, l) \neq (0, 0)$. One must exercise a bit of caution when adding and subtracting sets. Note that $kA + lA = (k + l)A$ is true in general only when k, and l are both non-negative or non-positive, and that $A \subseteq A + A$ does not imply $A - A \subseteq A$.

Examples 1.2

If A is an arithmetic progression of length n in a torsion-free abelian group, then $kA - lA$ is an arithmetic progression of length $(k + l)(n - 1) + 1$.

We say that A is in *general position* with respect to a finite number of sumsets of A if each sumset is as large as possible; that is, if there are no non-trivial coincidences among the specified sums. Note, however, that A cannot be in general position with respect to all higher sumsets; see Example 1.3.

For a finite subgroup A of an abelian group G, $kA - lA = A$ by the same reasoning as above. If A is a coset, then $|kA - lA| = |A|$.

If $A = \{a_1, \ldots, a_n\}$ is a set of real numbers, then the translation of A by a real number t is $A + \{t\} = \{a_1 + t, \ldots, a_n + t\}$ and will be denoted by $A + t$. The dilation of A by a real number $d \neq 0$ is $\{da_1, \ldots, da_n\}$ and will be denoted by $d \cdot A$. Note that neither translation nor dilation affects the cardinality of the sumsets of A.

We say that two finite sets of integers A, B are *affinely equivalent* if there are rational numbers $q \neq 0$ and r such that $B = q \cdot A + r$. By the comment above, we see that $|B| = |A|$ and $|kB - lB| = |kA - lA|$ for all integers k, l. For example, all arithmetic progression of length n in $\mathbb{Z}$ are affinely equivalent; in particular, they are all affinely equivalent to $\{1, \ldots, n\}$.

Example 1.3 A set of three integers is affinely equivalent to $\{0, m_1, m_2\}$ for some $0 < m_1 < m_2$ with $\gcd(m_1, m_2) = 1$. Given a set of integers A, we can use this to show that there are non-trivial coincidences among the sums in kA for some k. Indeed, take a three element subset of A. Represented as $\{0, m_1, m_2\}$, we see that the m_2-fold sum $m_1 + \cdots + m_1$ is equal to the m_1-fold sum $m_2 + \cdots + m_2$ plus $m_2 - m_1$ zeros. This gives that there will be non-trivial coincidences among the sums in $m_2 A$.

If A is a finite set in an abelian group G, then we denote the translate of A by $g \in G$ by $A + g$, as above. If $G = \mathbb{Z}/m\mathbb{Z}$ is a cyclic group, then the dilation $d \cdot A$ has the properties above as long as $(m, d) = 1$. In this way, we get the same notion of affine equivalence in cyclic groups. (A bit more care is required to define dilation and affine equivalence in arbitrary abelian groups. We will not have need for it here, hence we do not develop it.)

1.2 Lower estimates

In this section, we aim to understand the relationship between $|A|$, $|A + A|$, and $|A - A|$. It is easy to see that $|A + A|$ and $|A - A|$ are individually at least $|A|$ and at most $|A|^2$; it is more difficult to see how these quantities behave together.

A non-trivial solution to the equation $x_1 + x_2 = x_3 + x_4$ in A can be seen as reducing the size of $A + A$. Such a solution may be rearranged to form a non-trivial solution to the equation $x_1 - x_2 = x_3 - x_4$, thereby reducing the size of $A - A$. Thus we expect to see that $|A + A|$ and $|A - A|$ are positively correlated. We are immediately concerned with making this intuition precise.

We begin with the trivial estimates; that is, bounding $|A + A|$ and $|A - A|$ separately in terms of $|A|$. We discuss briefly sets $|A|$ for which $|A+A| > |A-A|$, and how products and projections may be used in regards to sumset estimates. We then explore how restricting one of $|A + A|$, $|A - A|$ near its minimal and maximal values affects the other. We conclude with some miscellaneous single set sumset estimates.

1.2.1 The trivial estimates

Our first goal is to bound $|A+A|$ and $|A-A|$ individually in terms of $|A|$.

Lemma 1.4. *Let A be a finite set of integers, $|A| = n$. Then*

$$2n-1 \leq |A+A| \leq n(n+1)/2,$$
$$2n-1 \leq |A-A| \leq n(n-1)+1.$$

Proof. If $A = \{a_1 < \cdots < a_n\}$, then the sequences

$$a_1 + a_1 < a_1 + a_2 < \cdots < a_{n-1} + a_n < a_n + a_n,$$
$$a_1 - a_n < a_2 - a_n < \cdots < a_{n-1} - a_1 < a_n - a_1$$

exhibit $2n-1$ distinct elements of $A+A$ and $A-A$, respectively.

We now consider the upper bounds. There are $\binom{n+1}{2} = n(n+1)/2$ ways to choose indices $i \leq j$, and each of the corresponding sums $a_i + a_j$ may be distinct. Similarly, there are $n(n-1)$ ways to choose indices $i \neq j$, and each of the corresponding differences $a_i - a_j$ may be distinct. Combined with the only remaining difference, namely 0, there are at most $n(n-1)+1$ possible differences. □

Corollary 1.5. *The previous lemma applies to finite sets in torsion-free abelian groups.*

Proof. Let A be a finite set in a torsion-free abelian group. Corollary A.3 gives that there is a set of integers A' such that

$$|A'| = |A|, \quad |A'+A'| = |A+A|, \quad |A'-A'| = |A-A|.$$

Since the bounds in Lemma 1.4 apply to A', they apply to A. □

We now show the analogous result in arbitrary abelian groups, where the potential for torsion reduces the lower bounds.

Lemma 1.6. *Let A be a finite set in an abelian group, $|A| = n$. Then*

$$|A| \leq |A+A| \leq n(n+1)/2,$$
$$|A| \leq |A-A| \leq n(n-1)+1.$$

Proof. If $a \in A$, then $|A| = |A+a| \leq |A+A|$, and similarly for $|A-A|$. The proof of the upper bounds is the same as in Lemma 1.4. □

From Examples 1.1, we see that the lower/upper bounds in the torsion-free case are simultaneously obtained by arithmetic progressions/Sidon sets. In the general case, the lower bounds are simultaneously obtained by cosets of finite subgroups of the ambient group.

1.2.2 MSTD sets, products, and projections

Now that we have bounded $|A+A|$ and $|A-A|$ separately, we begin to explore the relationship between the two. The following is a natural first question. Do there exist finite sets A_1, A_2, A_3 (in some abelian groups) such that

1. $|A_1 + A_1| < |A_1 - A_1|$,
2. $|A_2 + A_2| = |A_2 - A_2|$,
3. $|A_3 + A_3| > |A_3 - A_3|$?

Do there exist arbitrarily large examples of such sets?

We have seen that a set with no non-trivial coincidences between its sums and differences satisfies 1. There are fewer sums than differences for such sets because $x_1 + x_2 = x_2 + x_1$ while in general $x_1 - x_2 \neq x_2 - x_1$. Arbitrarily large examples of such sets are found easily; random subsets of large abelian groups, for example, are likely to be such.

The singleton $\{0\}$ trivially satisfies 2. More generally, if A is symmetric about 0, that is $A = -A$, then $A + A = A - A$. By translating, a set which is symmetric about any element of the ambient group satisfies 2. Note, however, that not all sets satisfying 2. are symmetric; take, for example, $\{-5, -3, 1, 3, 5\}$. It is again easy to find arbitrarily large examples of such sets: take any set A and form $A_2 = A \cup -A$.

Call a set satisfying 3. a *more sums than differences* (MSTD) set. These sets have an interesting history. The first published examples are due to Marica [13] in 1969, and since then MSTD sets have been studied for their own sake. Most recently, MSTD sets have been counted [6, 14, 38] and infinite families have been constructed [7, 15, 19]; the reader is referred to [18] for a general discussion. It is enough for us at the moment to know that there are many MSTD sets.

Examples 1.7

The set $\{-7, -5, -4, -3, 0, 4, 5, 7\}$ has 26 sums and 25 differences. It has the smallest diameter and the fewest number of elements of all MSTD sets in the integers, and all 8-element MSTD sets are affinely equivalent to it; see [7].

The set of sums of $\{0, 1, 2, 4, 5, 9\} \subseteq \mathbb{Z}/12\mathbb{Z}$ is all of $\mathbb{Z}/12\mathbb{Z}$, while the class 6 is not representable as a difference. $\mathbb{Z}/12\mathbb{Z}$ is the smallest cyclic group in which an MSTD set exists.

If $A_3 = \{0, 1, 2, 4, 5, 9, 12, 13, 17, 20, 21, 22, 24, 25\}$, then $A_3 \cup (A_3 + 20)$ has 91 sums and 83 differences. This MSTD set gives us the largest known values of the quantities $\log|A + A| \big/ \log|A - A|$, $\log \frac{|A+A|}{|A|} \Big/ \log \frac{|A-A|}{|A|}$, and $\log \frac{|A+A|}{|A-A|} \Big/ \log|A|$ as A runs over finite sets of integers. For more on the importance of these functions, see Sections 1.2.3 and 1.2.5. This example is due to Hegarty [7].

Unlike in 1. and 2., it is not immediately obvious how to form large examples of MSTD sets. One natural way is to consider products, which we briefly describe here. See Appendix A for more details.

Given a finite set A in an abelian group G, we may take its cartesian product $A^2 = A \times A$ in $G \times G$. Since the group operation works component-wise, it is not hard to verify that $|A^2| = |A|^2$, $|A^2 + A^2| = |A + A|^2$, and $|A^2 - A^2| = |A - A|^2$. Thus if A_3 is an MSTD set, then A_3^2 will be a larger one. By iterating this, we

may form arbitrarily large examples of MSTD sets, albeit in different abelian groups. Arbitrarily large examples of MSTD sets in the integers may be found by projecting down examples in $\mathbb{Z}^d$ while preserving the sum and difference set sizes. This technique actually gives us more via the following theorems.

Theorem 1.8. *For finite $A \subseteq \mathbb{Z}$, let $F(A) = |A+A| - |A-A|$. Then F is unbounded in both the positive and negative directions as it ranges over all finite subsets of $\mathbb{Z}$.*

Proof. Let $A = \{0, 1, 3\}$. We see $|A+A| = 6$, $|A-A| = 7$, so that $F(A) = -1$. For $d \geq 1$ an integer, A^d in $\mathbb{Z}^d$ satisfies $|A^d + A^d| = 6^d$, $|A^d - A^d| = 7^d$. By Theorem A.1 in Appendix A, there exists a set of integers with 6^d sums and 7^d differences. Thus F attains $6^d - 7^d$ for every integer $d \geq 1$, meaning that it is unbounded in the negative direction. Similarly, we show that F is unbounded in the positive direction by considering powers of an MSTD set; the first from Examples 1.7 would do. □

In exactly the same way, we have the following theorem.

Theorem 1.9. *For finite $A \subseteq \mathbb{Z}$, let $G(A) = |A+A|/|A-A|$. Then G attains values arbitrarily close to 0 and arbitrarily large positive values as it ranges over all finite subsets of $\mathbb{Z}$.*

With a bit more care, Martin and O'Bryant [14] and Hegarty [7] showed independently that the range of F is all of $\mathbb{Z}$. In the same vein, we ask the following question.

Question 1. *Given an $r \in \mathbb{Q}_+$, does there exist a finite set of integers A such that $G(A) = r$?*

Products, projections, and theorems like the ones above are important when working with sumset estimates. The tensor power trick, outlined in Section A.3, is a good example. The two theorems above tell us that bounds of the form $|A+A| \leq |A-A| + C_1$ and $|A+A| \leq C_2|A-A|$ with C_1, C_2 constant are not possible. These techniques are commonly used without any explicit reference to them.

1.2.3 Estimates near the minimum

We now want to understand how to make the following questions precise. If $|A+A|$ is close it its minimal value, must $|A-A|$ be close? If so, how close? The intuition is that $|A+A|$ and $|A-A|$ are positively correlated, i.e. that the answer to the first question is "yes." The rest of this section is devoted to determining to which degree this is true.

We begin by restricting $|A+A|$ to be exactly its minimal value. In addition to beging able to determine the exact value of $|A-A|$, we find detailed information on the structure of A itself. The next two theorems are examples of inverse theorems and are proven in greater generality in Section 2.2.1.

Corollary 1.10. *Let A be a finite set in a torsion-free abelian group. The following are equivalent:*

1. *A is an arithmetic progression*

2. $|A + A| = 2|A| - 1$

3. $|A - A| = 2|A| - 1$

There is an analogous connection in arbitrary abelian groups.

Corollary 1.11. *Let A be a finite set in an abelian group. The following are equivalent:*

1. *A is a coset of a subgroup*

2. $|A + A| = |A|$

3. $|A - A| = |A|$

Now we want to relax this bound near the minimum; that is, understand the freedom of one of $|A + A|$, $|A - A|$ if the other is restricted to be near its minimal value. As a first example, if we stipulate that A is a set of integers with $|A - A| \leq 2|A| + 1$, then there are already three possibilities for $|A + A|$.

Saying that $|A + A| \leq \alpha|A|$ is saying that $|A + A|$ is roughly within a factor of α of its minimal value. Therefore, bounding the quantities $|A + A|/|A|$, $|A - A|/|A|$ from above is one way to formulate $|A + A|$, $|A - A|$ being near to its minimal value.

In the late 1960's, Freĭman gave a structural characterization of sets of integer A for which $|A + A|/|A|$ is small. This structure implies a weak upper bound on $|A - A|/|A|$. More specifically, if $|A + A| \leq \alpha|A|$, then Freĭman's results show $|A + A| \leq f(\alpha)|A|$ where f depends only on α. The dependence, however, is exponential, and therefore is quite weak. Nevertheless, this shows a positive correlation between $|A + A|$ and $|A - A|$ in one direction.

Much better bounds are available, however, if we do not consider the structure of A. Ruzsa [27], inspired by a question of Erdős and the weak correlation implied by Freĭman's work, showed in 1976 via elementary arguments that

$$|A + A| \leq \alpha|A| \implies |A - A| \leq \alpha^2|A|$$
$$|A - A| \leq \alpha|A| \implies |A + A| \leq \alpha^3|A|$$

for finite sets of integers A.

Taking powers of A, we see that bounds of the form $|A + A|/|A| \leq |A - A|/|A| + C$ and $|A + A|/|A| \leq C|A - A|/|A|$ with C constant are not possible. In other words, if we assume $|A + A| \leq \alpha|A|$ and we would like to have a polynomial $f(\alpha)$ such that $|A - A| \leq f(\alpha)|A|$, f must be at least quadratic.

Ruzsa was able to improve α^3 to α^2 in the second inequality above in 1989 with Plünnecke's method. Though this symmetrized the two results, the proof of the second remained difficult (dependent upon Plünnecke's theorem) until very recently.

The following theorem records these results as easy symmetric corollaries to Theorems 2.7 and 2.8 and Corollary 2.9.

Theorem 1.12. *[Ruzsa 1976, 1989] Let A be a finite set in an abelian group G. Then*

$$\left(\frac{|A + A|}{|A|}\right)^{1/2} \leq \frac{|A - A|}{|A|} \leq \left(\frac{|A + A|}{|A|}\right)^{2}.$$

Equivalently,

$$|A+A| \leq \alpha|A| \implies |A-A| \leq \alpha^2|A|$$
$$|A-A| \leq \alpha|A| \implies |A+A| \leq \alpha^2|A|$$

If G is torsion-free, then $\frac{|A+A|}{|A|} \leq \left(\frac{|A-A|}{|A|}\right)^2 - 1 + \frac{1}{|A|}$.

It is a natural next question to ask whether these bounds are sharp. Consider the quantity $\log \frac{|A+A|}{|A|} \Big/ \log \frac{|A-A|}{|A|}$ as A ranges over finite sets in abelian groups. The theorem above gives us that it is bounded between $1/2$ and 2.

Hennecart, Robert, and Yudin [8] showed in 1999 that simplices in the integer lattice have many more differences than sums. Theorem B.4 in Appendix B uses these simplices to show that there are sets A with $\log \frac{|A+A|}{|A|} \Big/ \log \frac{|A-A|}{|A|}$ arbitrarily close to $1/2$. This shows that the exponent in $\frac{|A-A|}{|A|} \leq \left(\frac{|A+A|}{|A|}\right)^2$ is sharp.

The other exponent, however, is still open.

Question 2. *Is the exponent 2 in* $\frac{|A+A|}{|A|} \leq \left(\frac{|A-A|}{|A|}\right)^2$ *sharp?*

If $A' = \{0, 1, 2, 4, 5, 9, 12, 13, 17, 20, 21, 22, 24, 25\}$, then $A = A' \cup (A' + 20)$ has 23 elements, 91 sums, and 83 differences. It is due to Hegarty [7] and gives us the largest known value of $\log \frac{|A+A|}{|A|} \Big/ \log \frac{|A-A|}{|A|}$ at just greater than 1.0846.

1.2.4 Estimates near the maximum

We follow now the analogous train of thought with the joint behavior of $|A+A|$ and $|A-A|$ near their maximal values. We seek to understand the freedom of one of $|A+A|$, $|A-A|$ if the other is near its maximum value.

Just as before, we begin by restricting one of $|A+A|$, $|A-A|$ to be exactly at its maximum. We again have exact information on the size of the other sumset, though we do not have a structural classification. The proof is exactly as in Lemma 2.6 and uses the counting from Lemma 1.4.

Lemma 1.13. *Let A be a finite set in an abelian group, $|A| = n$. The following are equivalent:*

1. *There are no non-trivial solutions to the equation $x_1 + x_2 = x_3 + x_4$ in A; i.e. if $a_1 + a_2 = a_3 + a_4$ with $a_i \in A$, then $\{a_1, a_2\} = \{a_3, a_4\}$*
2. *There are no non-trivial solutions to the equation $x_1 - x_2 = x_3 - x_4$ in A; i.e. if $a_1 - a_2 = a_3 - a_4$ with $a_i \in A$, then $\{a_1, a_4\} = \{a_2, a_3\}$*
3. $|A+A| = n(n+1)/2$
4. $|A-A| = n(n-1)+1$

A set satisfying any of the conditions above is called a *Sidon set*. We see that no non-trivial coincidences among the sums is equivalent to no non-trivial coincidences among the differences.

Just as in the previous section, we want to relax the condition of being exactly at the maximum value. If we stipulate that A is a set of integers with $|A+A| \geq n(n+1)/2 - 1$, then there are already three possibilities for $|A-A|$.

One way to formulate $|A+A|$, $|A-A|$ being close to the maximum is bounding $|A+A|/|A|^2$, $|A-A|/|A|^2$ from below. We might ask if $|A+A| \geq \alpha|A|^2$ implies that $|A-A| \geq f(\alpha)|A|^2$ for some function f depending only on α. In marked contrast to bounds near the minima, the answer to this question is negative. Ruzsa [30] in 1992 was able to show the following.

Theorem 1.14. *There exists a $c_1 > 0$ and an integer $n_1 \geq 1$ such that for all $n \geq n_1$ there is a set of integers A with $|A| = n$ and*

$$|A+A| \geq n^2/2 - n^{2-c_1}, \qquad |A-A| \leq n^{2-c_1}$$

Similarly, there exists a $c_2 > 0$ and an integer $n_2 \geq 1$ such that for all $n \geq n_2$ there is a set of integers A with $|A| = n$ and

$$|A-A| \geq n^2 - n^{2-c_2}, \qquad |A+A| \leq n^{2-c_2}$$

Theorem 1.12 gives us that neither c_1 nor c_2 may be larger than $1/2$. Ruzsa [33] improved the upper bound on c_2 in 2008 to $1/3$ via Theorem 1.19. Ruzsa did not compute explicit values for the constants c_1, c_2, and effective lower bounds for them have not been published.

Question 3. *What are effective values for the constants c_1, c_2 in Theorem 1.14?*

In this sense of "close to the maximum", then, we do not see a close connection between $|A+A|$, $|A-A|$. Formulating it in another way, we may simply quantify the difference between $|A+A|$, $|A-A|$ and their maximal values. For a finite set A in an abelian group, $|A| = n$, we define

$$\Delta_+(A) = n(n+1)/2 - |A+A|,$$
$$\Delta_-(A) = n(n-1) + 1 - |A-A|$$

to be the *sum deficit* and the *difference deficit* of A, respectively.

From the trivial estimates, we have immediately that $0 \leq \Delta_+(A) \leq n(n-3)/2 + 1$ and $0 \leq \Delta_-(A) \leq n(n-3) + 2$. Ruzsa [33] showed the following connection.

Theorem 1.15. *Let A be a finite set in an abelian group. Then*

$$\Delta_+(A) \leq \frac{1}{2}\Delta_-(A)^{3/2} + \Delta_-(A)$$
$$\Delta_-(A) \leq 2(\Delta_+(A)^2 + \Delta_+(A))$$

Moreover, there are arbitrarily large sets of integers A for which the second inequality is equality.

Ruzsa conjectures in the same paper that the correct exponent on $\Delta_-(A)$ in the first inequality is $4/3$.

Conjecture 1.16. *Let A be a finite set in an abelian group. Then $\Delta_+(A) \leq c\Delta_-(A)^{4/3}$ for some positive constant c.*

1.2.5 Other estimates

In this section, we formulate three other miscellaneous sumset estimates.

1. It is immediate from the trivial bounds that $|A \pm A| \leq |A \mp A|^2$. Naturally, we are led to ask what the best exponent is here. The following theorem was first proven by Freĭman and Pigarev in [25]. We show it as an easy corollary to Theorems 2.7 and 2.8 from the second chapter.

Theorem 1.17. *Let A be a finite set in an abelian group. Then*

$$|A + A| \leq |A - A|^{4/3}$$
$$|A - A| \leq |A + A|^{4/3}$$

Proof. Setting B, C in Theorem 2.8 to $-A$ and using the trivial bound $|A+A| \leq |A|^2$, we see

$$|A + A|^3 \leq |A|^2 |A + A|^2 \leq |A - A|^4.$$

We obtain the other inequality in the same way with B, C set to A in Theorem 2.7. □

It is still an open question to determine what the best exponents are here. The theorem gives that $\log |A+A| / \log |A-A|$ is bounded between $3/4$ and $4/3$ as A runs over finite sets in abelian groups.

Question 4. *What are the infima of values of c_1, c_2 such that $|A + A| \leq |A - A|^{c_1}$, $|A - A| \leq |A + A|^{c_2}$ hold for all finite sets A?*

The largest known value of $\log |A+A| / \log |A-A|$ is attained by the third example in Examples 1.7 at just over 1.0208, which means $c_1 \geq 1.0208$. Theorem B.2 uses simplices in the integer lattice to show that $\log |A+A| / \log |A-A|$ may be arbitrarily close to $\frac{\log 2}{\log(1+\sqrt{2})}$ from above. In other words, $c_2 \geq \frac{\log(1+\sqrt{2})}{\log 2} > 1.2715$.

2. It is easy to see that neither $|A + A|/|A - A|$ nor $|A - A|/|A + A|$ may be bounded from above by a constant. Both, however, are trivially bounded from above by $|A|$. This leads us to ask what power of $|A|$ can bound $|A+A|/|A-A|$. To my knowledge, this estimate has not been formulated elsewhere.

Corollary 1.18. *Let A be a finite set in an abelian group. Then*

$$\frac{|A + A|}{|A - A|} \leq \min\left(\frac{|A - A|}{|A|}, |A|^{1/2}\right).$$

The same inequality is true if all $+$ and $-$ signs are switched.

Proof. From Theorem 2.8, we get $|A + A|/|A - A| \leq |A - A|/|A|$. If $|A|^{1/2} \leq |A-A|/|A|$, then $|A+A|/|A-A| \leq |A+A|/|A|^{3/2} \leq |A|^{1/2}$, as desired. Switching the $+$ and $-$ signs, we may use Theorem 2.7 in the analogous way. □

Again we may ask for lower bounds on the best exponent on $|A|$.

Question 5. *What are the infima of values of c_1, c_2 such that $|A+A|/|A-A| \leq |A|^{c_1}$, $|A - A|/|A + A| \leq |A|^{c_2}$ hold for all finite sets A?*

The third MSTD set from Examples 1.7 shows that $c_1 > 0.0293$. Theorem B.5 uses simplices to show that $c_2 > 0.4$.

3. We briefly present here some recent sumset inequalities from Ruzsa in [33]. All of the proofs are elementary. The main result is as follows.

Theorem 1.19. *Let A be a finite set in an abelian group, $|A| = n$. Then*

$$|A + A| \left(\Delta_-(A)^2 + \frac{n^3}{6} \right) \geq \frac{n^5}{20}.$$

In particular, if $|A + A| < n^2/10$, then

$$|A + A| \Delta_-(A)^2 \geq \frac{n^5}{30}.$$

A positive correlation between $|A + A|$ and $|A - A|$ would mean a negative one between $|A + A|$ and $\Delta_-(A)$. The lower bound in this theorem gives us that $|A+A|$ small implies $\Delta_-(A)$ large and vice versa. In particular, this shows that $|A+A|$ is comparable with $|A|^2$ when $\Delta_-(A)$ is bounded by $|A|^{3/2}$. It also shows that the constant c_2 from Theorem 1.14 cannot be greater than $1/3$.

Ruzsa conjectures the analogous inequality holds for the product $|A-A|\Delta_+(A)^2$ in the following way.

Conjecture 1.20. *There exists a $c > 0$ such that if $|A - A| < cn^2$, then*

$$|A - A| \Delta_+(A)^2 \geq cn^5.$$

He was able to show the following weaker version.

Theorem 1.21. *If $|A - A| < n^2/2$, then for n sufficiently large, we have*

$$|A - A| \Delta_+(A)^2 \geq \frac{n^4}{9}.$$

1.3 Higher estimates

In this section, we are concerned with understanding the behavior of $|kA|$ and more generally $|kA - lA|$ in terms of k and l. One of the primary goals is to understand their behavior in terms of the cardinalities $|A|$, $|A + A|$, $|A - A|$ studied in the last section. We want to see, for example, that if $|A + A|$ is not too large compared to $|A|$, then $|kA|$ does not grow too quickly as a function of k.

We begin with the trivial estimates on $|kA|$, $|kA - lA|$. After discussing generalizations of MSTD sets, we introduce the Plünnecke-Ruzsa results by showing how $|kA - lA|$ may be controlled by $|3A|$ in an elementary way. We then give a brief description of Plünnecke's method, one of the primary tools in understanding higher sumset estimates.

Though we still focus on symmetric sumsets in this section, we will need the notation for asymmetric sumsets. The reader should refer to Section 2.1. Recall that when we write $|kA - lA|$, we implicitly assume that k, $l \geq 0$, and $(k, l) \neq (0, 0)$.

1.3.1 The trivial estimates

As with the lower sumsets, we begin by establishing the trivial estimates for $|kA|$ and $|kA - lA|$ in terms of $|A|$.

Lemma 1.22. *Let A be a finite set of integers, $|A| = n$. Then*

$$k(n-1)+1 \leq |kA| \leq \binom{n+k-1}{k}.$$

Proof. If $A = \{a_1 < \cdots < a_n\}$, then consider a sequence

$$a_1 + a_1 + \cdots + a_1 < a_2 + a_1 + \cdots + a_1 < \cdots < a_n + a_n + \cdots + a_n$$

in kA in which exactly one index is incremented by 1 at each step. Such a sequence exhibits $k(n-1)+1$ distinct elements of kA.

For the upper bound, each $a_{i_1} + a_{i_2} + \cdots + a_{i_k}$ with $i_1 \leq i_2 \leq \cdots \leq i_k$ may be distinct. There are $\binom{n+k-1}{k}$ such non-decreasing, length k sequences of indices from $\{1, 2, \ldots, n\}$. □

Corollary 1.23. *The previous lemma holds for finite sets of torsion-free abelian groups.*

Lemma 1.24. *Let A be a finite set in an abelian group, $|A| = n$. Then*

$$n \leq |kA| \leq \binom{n+k-1}{k}.$$

The proofs of Corollary 1.23, Lemma 1.24 follow exactly as the proofs of Corollary 1.5, Lemma 1.6 for the lower trivial estimates.

From Examples 1.2, we see that the lower/upper bounds in the torsion-free case are obtained by arithmetic progressions/sets in sufficiently general position. In the general case, the lower bound is obtained by cosets of finite subgroups of the ambient group.

The lower bounds on $|kA - lA|$ are similar. If A is a finite set in a torsion-free abelian group, then one can show in the same way as above that $(k+l)(|A| - 1) + 1 \leq |kA - lA|$. This bound is attained if A is an arithmetic progression. For general abelian groups, we have $|A| \leq |kA - lA|$, which is attained at cosets of finite subgroups.

Writing a closed form expression for the exact upper bound on $|kA - lA|$ in terms of $|A|$ is likely difficult. Using the asymmetric trivial estimate $|A + B| \leq |A||B|$ (Lemma 2.2), we may write $|kA - lA| \leq |kA||lA|$ and then apply the bounds in Lemma 1.22. As a polynomial in $|A|$, this gives the right order of growth, but it is not sharp. We record this in the following lemma.

Lemma 1.25. *Let A be a finite subset of an abelian group G, $|A| = n$. Then*

$$n \leq |kA - lA| \leq \binom{n+k-1}{k}\binom{n+l-1}{l}.$$

If G is torsion-free, then $(k+l)(n-1)+1 \leq |kA - lA|$.

1.3.2 Higher MSTD sets and generalizations

The first higher sumset cardinalities are $|3A| = |-3A|$ and $|2A - A| = |A - 2A|$. Following Section 1.2, we are naturally led to ask the following questions. Do there exist finite sets A_1, A_2, A_3 (in some abelian groups) such that

1. $|3A_1| < |2A_1 - A_1|$
2. $|3A_2| = |2A_2 - A_2|$
3. $|3A_3| > |2A_3 - A_3|$

Does there exist a finite set A_4 such that

4. $|3A_4| < |A_4 - A_4|$

Do there exist arbitrarily large examples of such sets?

As we show in Appendix A, powers of sets satisfying any of the conditions above will be larger examples satisfying the same conditions. The last question, then, is equivalent to the question of existence for these sets.

Sets in general position satisfy 1. and symmetric sets satisfy 2. A set satisfying 3. is a sort of higher MSTD set; see Section 1.2.2. One may come across examples by searching random sets in some interval of integers. For example, the set

$$A_3 = \{0, 4, 5, 10, 11, 17, 23, 24, 28\}$$

is such that $|3A_3| = 74$ and $|2A_3 - A_3| = 73$. I do not know whether it is the smallest or shortest of all such sets in the integers. It is interesting to note that it is not an MSTD set: $|A_3 + A_3| = 34$ while $|A_3 - A_3| = 35$. Much more is known about MSTD sets than their higher generalizations; that is, very little is known about higher MSTD sets in general.

The 7-dimensional simplex of size 11, $\Delta_{11}^7 = \{(x_1, \ldots, x_7) \in \mathbb{Z}^7 \mid 0 \leq x_i \text{ and } \sum x_i \leq 11\}$, satisfies 4. In fact,

$$|\Delta_{11}^7| = 18564, \quad |\Delta_{11}^7 - \Delta_{11}^7| = 18880961, \quad |3\Delta_{11}^7| = 18643560.$$

Just as with 3., virtually nothing is known about the density of such sets in an interval of integers or how to construct them in general.

These considerations lead us very naturally to the following question.

Question 6. *Given $k, l, k', l' \geq 0$ with $(k, l), (k', l') \neq (0, 0)$, does there exist a finite set A in an abelian group such that $|kA - lA| < |k'A - l'A|$?*

This question was asked in much greater generality and partially answered in [20]. Question 6 is still open; in fact, given a $k \geq 1$, we do not even know if there exists an A such that $|A - A| > |kA|$.

1.3.3 Controlling $|kA - lA|$ with $|3A|$

We now look to further generalize results from Section 1.2. We saw via Theorem 1.12 that $|A + A|$ is small (within a multiple of $|A|$) if $|A - A|$ is small and vice versa. We may ask if the same is true of the pair $|3A|$, $|2A - A|$. The intuition behind the corollary (that non-trivial solutions to $x_1 + x_2 = x_3 + x_4$ may be arranged to form non-trivial solutions to $x_1 - x_2 = x_3 - x_4$) generalizes to this case, leading us to expect a positive answer. We prove the following theorem in the next section.

Theorem 1.26. *Let A be a finite set in an abelian group. Then*

$$\left(\frac{|3A|}{|A|}\right)^{2/3} \leq \frac{|2A-A|}{|A|} \leq \left(\frac{|3A|}{|A|}\right)^{2},$$

from which it follows that

$$|3A|^{7/9} \leq |2A-A| \leq |3A|^{3/2}.$$

More generally, though, we seek to understand how all higher sumsets $|kA-lA|$ may be controlled by some manageable collection of lower sumsets. The ratio $|A+A|/|A|$ measures the degree to which taking sums magnifies the set A. We may wonder whether it alone may be used to understand the growth of all of the higher sumsets. To what degree does the growth of the first set of sums $|A+A|/|A|$ reflect the growth of the iterated sums $|kA|/|A|$ and $|kA-lA|/|A|$?

Plünnecke's method and the Plünnecke-Ruzsa inequalities are the standard tools for answering such questions. We will discuss them in the next section. The remainder of this section will be used as preparation and motivation for the results of the next. In particular, we show how to partially answer such questions by elementary means via the following lemma.

Lemma 1.27. *Let A be a finite set in an abelian group, $|A| = n$, and $|3A| = \alpha n$. Then*

$$|kA-lA| \leq \alpha^{k+l} n.$$

This lemma is indicative of how these results are generally stated. We understand α as reflecting the growth of $|3A|$ over $|A|$, and we understand the growth of $|kA-lA|$ over $|A|$ by bounding $|kA-lA|/|A|$ in terms of a function of α. Recall that Theorem 1.12 was stated naturally in these terms: if $|A| = n$, $|A+A| = \alpha n$, then $|A-A| \leq \alpha^2 n$ and vice versa.

We present a proof of the lemma based on Ruzsa's triangle inequality, Theorem 2.7:

$$|A||B-C| \leq |A+B||A+C|.$$

(Note that we have made the substitutions $B \to -B$ and $C \to -C$.) This inequality has an elementary proof. Lemma 1.27 was known to Ruzsa and Turjányi [35] already in 1985, years prior to Ruzsa discovering and reformulating Plünnecke's work.

Proof of Lemma 1.27. We induct on $k+l$. We have $|A| \leq |2A| \leq |3A| = \alpha n$. By Ruzsa's triangle inequality, $|A||A-A| \leq |A+A|^2 \leq \alpha^2 n^2$, so that $|A-A| \leq \alpha^2 n$. This covers the bases cases of $k+l = 1, 2$.

If $k+l \geq 3$, then since $|kA-lA| = |lA-kA|$, we may assume without loss of generality that $k \geq 2$. We see

$$\begin{aligned} |A||kA-lA| &= |A||2A-(lA-(k-2)A)| \\ &\leq |3A||(l+1)A-(k-2)A| \\ &\leq |3A|\alpha^{k+l-1} n. \end{aligned}$$

The last inequality follows from the inductive hypothesis. Dividing by $|A|$ yields the result. □

This result shows that indeed the growth of $|3A|$ over $|A|$ governs the growth of the higher sumsets. Note that there was nothing particular about our choice of $|3A|$; we could have used $|2A - A|$ or any other higher sumset. Bounding the growth of the higher sumsets by $|2A|$, however, cannot be achieved with Ruzsa's triangle inequality. This is the subject of the next section.

1.3.4 Plünnecke's method

In 1970, Plünnecke [26] published a graph theoretic method to estimate the density of sumsets of infinite sets of integers. Ruzsa [28, 29] published a simplified version of Plünnecke's results in 1989 in which he applied them to the study of higher sumsets. There are many good accounts of Ruzsa's version of Plünnecke's method; we refer the reader to [32] for a quick overview with applications and [1, 23] for a more in-depth discussion with proofs. For completeness, we briefly describe the method and state the main results here.

Given finite sets A, B, we model the higher sumsets A, $A + B$, $\ldots$, $A + kB$ with the following directed graph. If $V_i = A + iB$, the vertices are a disjoint union $V_0 \cup \cdots \cup V_k$. There is a directed edge from $x \in V_i$ to $y \in V_{i+1}$ if $y = x + b$ for some $b \in B$. This is an example of a *bridging*, *commutative* graph.

The *magnification ratio* of V_0 in V_i is then defined as

$$D_i = \min \left\{ \frac{|\mathrm{im}(X, V_i)|}{|X|} \;\middle|\; X \subseteq V_0,\ X \neq \emptyset \right\}$$

where $\mathrm{im}(X, V_i)$ is the image of X in V_i, the set of those vertices in V_i to which there is a directed path from some vertex in X. Plünnecke's main result concerns these magnification ratios; in our limited formulation, it is the following.

Theorem 1.28. *The sequence $D_i^{1/i}$ is decreasing.*

Using the trivial bound $D_i \leq |V_i|/|V_0|$ and replacing $|V_i|$ with $|A + iB|$, $|\mathrm{im}(X, V_i)|$ with $|X + iB|$ we have the following theorem.

Theorem 1.29 (Plünnecke's inequality)**.** *Let A, B be finite sets in an abelian group, $i \leq k$ be integers, $|A| = n$, and $|A + iB| = \alpha n$. There exists a non-empty $X \subseteq A$ such that*

$$|X + kB| \leq \alpha^{k/i} |X|.$$

To put it another way, there is a subset X of A for which $|X + kB|/|X|$ is bounded by a power of $|A + iB|/|A|$. This gives us a bound on the growth of the higher sumset cardinality $|X + kB|$ over $|X|$ with information on the growth of the lower sumset cardinality $|A + iB|$ over $|A|$. We will see immediately how this applies to symmetric sumset estimates. See Section 2.3.1 for a further discussion.

Until very recently, the simplest proofs of Plünnecke's theorem made use of, among other things, Menger's theorem and the tensor power trick applied to products of commutative graphs. Petridis [22, 23, 24] recently gave a simpler proof of Plünnecke's theorem and, in particular, an elementary proof of Plünnecke's inequality in the $i = 1$ case. This is discussed in Sections 2.3.1 and 2.3.2.

We are now interested in understanding what Plünnecke's method yields regarding single set sumset estimates. Setting $B = A$ or $B = -A$ in Plünnecke's inequality and using that $|X| \leq |A|$, $|kB| \leq |X + kB|$, and $|X| + |kB| - 1 \leq |X + kB|$ when the ambient group is torsion-free, we have the following corollary.

Corollary 1.30. *Let A be a finite set in an abelian group G, $i \leq k$ be positive integers, $|A| = n$, $|A + iA| = \alpha n$. We have*

$$|kA| \leq \alpha^{k/i} n.$$

If G is torsion-free, then

$$|kA| \leq (\alpha^{k/i} - 1)n + 1.$$

The same conclusions are true if we define α instead by $|A - iA| = \alpha n$.

More is possible when we combine Plünnecke's inequality with Ruzsa's triangle inequality. Setting $B = A$ in Theorem 2.17, we have the following.

Corollary 1.31. *Let A be a finite set in an abelian group, $i \leq k \leq l$ be positive integers, $|A| = n$, $|A + iA| = \alpha n$. We have*

$$|kA - lA| \leq \alpha^{(k+l)/i} n.$$

The same conclusion is true if we define α instead by $|A - iA| = \alpha n$.

When $i = 1$, we achieve our goal of establishing control on the growth of the higher sumsets with $|A + A|/|A|$ and $|A - A|/|A|$. This strengthens Lemma 1.27. When $i > 1$, we see a scaling; we may more precisely control $|kA - lA|$ with information on the higher sumsets $|A + iA|$, $|A - iA|$.

We conclude by proving Theorem 1.26, stated in the beginning of the previous section.

Proof of Theorem 1.26. If $|A| = n$ and $|2A - A| = \alpha n$, then Corollary 1.30 with $i = 2$ gives that $|3A| \leq \alpha^{3/2} n$. Using the trivial estimate $|3A| \leq n^3$, we have

$$|3A|^7 \leq n^3 |3A|^6 \leq |2A - A|^9.$$

The last inequality follows from raising $|3A| \leq \alpha^{3/2} n$ to the sixth power and rearranging. We don't have the same sort of control on $|2A - A|$ as we do on $|3A|$. Assuming $|3A| = \alpha n$ and applying Theorem 2.7, we have

$$|A||2A - A| \leq |3A||2A| \leq \alpha^2 |A|^2.$$

Hence $|2A - A| \leq \alpha^{3/2} n$. The trivial estimate $|2A - A| \leq n^3$ yields $|2A - A| \leq |3A|^{3/2}$. □

1.3.5 Growth of $|kA|$

We turn our attention now to better understanding the growth of kA in terms of k. We begin by stating a theorem of Khovanskiĭ [9, 10] which shows that the growth of $|kA|$ for a fixed A as $k \to \infty$ is governed by a polynomial. Then we compare $|kA|$ with $\frac{k}{k-1}|(k-1)A|$ and $|(k-1)A|^{\frac{k}{k-1}}$.

Theorem 1.32. *Let A be a finite set in an abelian group. There is a polynomial f and an integer k_0 such that for $k > k_0$, $|kA| = f(k)$.*

While $|kA|$ my behave irregularly for small k, it eventually stabilizes into polynomial growth. The polynomial f and threshold k_0 are in general not computable. Compare this with the exponential bound from Plünnecke's inequality: $|kA| \leq (|A+A|/|A|)^k |A|$. This result was generalized to multiple summands by Nathanson [17] and Nathanson and Ruzsa [21].

There are many known proofs of the following two results. We present them as corollaries to theorems in the second chapter, both of which have elementary proofs. These may be interpreted as showing that the sequence $|kA|$ exhibits faster than linear, but slower than exponential, growth. The main reference is [5].

Corollary 1.33. *Let A be a finite set in an abelian group. Then*

$$|kA| \geq \frac{k|(k-1)A| - 1}{k-1}.$$

Consequently, the sequence $\frac{(k+1)|kA|-1}{k}$ is increasing.

Proof. The first statement is a direct application of Theorem 2.25 with all variables set to A. To prove the second, we multiply the first inequality by $k+1$, subtract 1, and divide by k to see

$$\frac{(k+1)|kA| - 1}{k} \geq \frac{(k+1)\frac{k|(k-1)A|-1}{k-1} - 1}{k} \geq \frac{k|(k-1)A| - 1}{k-1}.$$

The last inequality follows from the fact that $|(k-1)A| \geq 1$. □

See [11] for an alternative proof in torsion-free abelian groups. We prove the following as both a corollary to Theorem 2.26 and as a corollary to Theorem 1.29 using Plünnecke's method.

Corollary 1.34. *Let A be a finite set in an abelian group. Then*

$$|kA| \leq |(k-1)A|^{\frac{k}{k-1}}.$$

Consequently, the sequence $|kA|^{1/k}$ is decreasing.

Proof. Set all of the variables to A in Theorem 2.26. Alternatively, use Theorem 1.29 above with (A, B) set to $(\{0\}, A)$. We get that $X = \{0\}$ and hence that $|kA| \leq |iA|^{k/i}$. We have the desired result with $i = k-1$. □

Chapter 2: Asymmetric sumset estimates

In this chapter we consider sumset estimates involving two or more possibly distinct sets. Most of the results from the first chapter are proven in much greater generality.

2.1 Definitions and examples

For A, B finite subsets of an abelian group, we define

$$A + B = \{a + b \mid a \in A, b \in B\},$$
$$A - B = \{a - b \mid a \in A, b \in B\}$$

to be the *sum set* and *difference set* of A and B, respectively. These are the *lower sumsets* of A and B.

In the same way as in the first chapter, for k, l positive integers, $kA + lB$ denotes the set of sums of k elements from A with l elements from B. We define $(-k)A = -(kA)$, $0A = \{0\}$, and interpret $kA - lB$ to be $kA + (-l)B$. These are examples of the *higher sumsets* of A and B. If C is a finite set in the same abelian group, we define $A + B + C$ accordingly.

As before, we are primarily interested in the relationship between the cardinalities $|A|$, $|A + B|$, $|A - B|$, $|A + 2B|$, $|A + B + C|$, and the like. Writing kA and $kA - lB$, we again implicitly assume that $k > 0$ and $k, l \geq 0$, $(k, l) \neq 0$, respectively.

Examples 2.1

If A and B are arithmetic progressions of the same step size in a torsion-free abelian group, then one can check that $A + B$ is an arithmetic progression with the same step size of length $|A| + |B| - 1$. If A and B are arithmetic progressions of different step sizes, then $A + B$ is an example of a *generalized arithmetic progression*.

The sets A and B are said to be in *general position* if there are no non-trivial solutions to the equation $x + y = x' + y'$ with $x, x' \in A$, $y, y' \in B$; that is, there are no non-trivial coincidences among the sums of A and B. It is easy to see in this case that there are no non-trivial coincidences among the differences either, hence $|A + B| = |A - B| = |A||B|$ (see Lemma 2.2).

If A is a finite subgroup of an abelian group and $B \subseteq A$, then $A + B = A$ since $A + b = A$ for each $b \in B$. If A is a coset of a finite subgroup H and B is a translate of some subset H' of H, then it is easy to verify that $|A + B| = |H + H' + g| = |H| = |A|$.

Translations, dilations, and affine equivalence extend to this more general setting, with the caveat that $|A+B|$ is not invariant under dilations of just one of the sets. If $A' = A+g$ and $B' = B+h$, then $|A'+B'| = |A+B+g+h| = |A+B|$. If $A' = d \cdot A$ and $B' = d \cdot B$, then $|A' + B'| = |d \cdot (A + B)| = |A + B|$.

2.2 Lower estimates

Let A, B be finite sets in an abelian group. By rearranging solutions to the equation $x + y = x' + y'$ with x, $x' \in A$, y, $y' \in B$, we are led to expect the same sort of positive correlation between $|A+B|$ and $|A-B|$ as we saw between

$|A+A|$ and $|A-A|$ in Chapter 1. This is indeed the case, though the correlation is not as strong.

We begin exploring asymmetric sumset estimates by establishing the trivial estimates and some basic inverse theorems. In Sections 2.2.2 and 2.2.3, we present two asymmetric inequalities of fundamental importance. We conclude with some miscellaneous asymmetric sumset estimates.

2.2.1 Trivial estimates and inverse theorems

We begin studying asymmetric sumset estimates by bounding $|A+B|$ and $|A-B|$ separately in terms of $|A|$, $|B|$.

Lemma 2.2. *Let A, B be finite sets in an abelian group G. We have*

$$\max(|A|,|B|) \leq |A+B| \leq |A||B|$$

If G is torsion-free, then $|A|+|B|-1 \leq |A+B|$. The same bounds hold with $|A-B|$ in place of $|A+B|$.

Proof. The lower bound in the general case follows from the fact that $A+b, a+B \subseteq A+B$ and $|A+b| = |A|$, $|a+B| = |B|$ for all $a \in A, b \in B$. Since there are $|A||B|$ choices for $a \in A$, $b \in B$ and each $a+b$ may be distinct, we have $|A+B| \leq |A||B|$.

By Corollary A.3 in Appendix A, it is sufficient to check that $|A|+|B|-1 \leq |A+B|$ holds when A and B are finite sets of integers. If $A = \{a_1 < \cdots < a_n\}$ and $B = \{b_1 < \cdots < b_m\}$, then the sequence

$$a_1+b_1 < a_1+b_2 < \cdots < a_{n-1}+b_m < a_n+b_m$$

exhibits $n+m-1$ distinct elements of $A+B$.

Finally, replacing B with $-B$ in the results above gives us the same bounds for $A-B$. □

Now we are interested in relating the quantities $|A+B|$, $|A-B|$. We begin by showing that $|A+B|$, $|A-B|$ achieve their minimum and maximum values simultaneously. In the case that they are at their minimums, we are able to deduce structural information on A and B in the following way.

Theorem 2.3. *Let A, B be finite sets of integers. The following are equivalent:*

1. *A, B are arithmetic progressions with the same step size*
2. *$|A+B| = |A|+|B|-1$*
3. *$|A-B| = |A|+|B|-1$*

Proof. Assuming 1., it is easy to check that $A+B$, $A-B$ are arithmetic progressions of length $|A+B| = |A-B| = |A|+|B|-1$ with step size matching that of A, B.

Let $A = \{a_1 < \cdots < a_n\}$, $B = \{b_1 < \cdots < b_m\}$. Then in $A+B$ we have sequences of the form $a_1+b_1 < \cdots < a_n+b_m$ in which exactly one of the indices is increased by 1 at each step. Such a sequence may begin with, for example,

$$a_1+b_1 < a_1+b_2 < a_2+b_2 < a_3+b_2 < \cdots < a_n+b_m.$$

Each such sequence has $|A| + |B| - 1$ elements, and so if we assume 2., then all of these sequences are the same. Thus we see that 2. is equivalent to the assertion

$$a_i + b_j = a_k + b_l \quad \Longleftrightarrow \quad i + j = k + l. \tag{$*$}$$

Similarly for $A - B$, we have sequences $a_1 - b_m < \cdots < a_n - b_1$ with $|A| + |B| - 1$ elements in which either the first index is increased by 1 or the second index is decreased by 1 at each step. We see, in the same way as above, that 3. is equivalent to the assertion

$$a_i - b_j = a_k - b_l \quad \Longleftrightarrow \quad i - j = k - l.$$

This is clearly equivalent to $(*)$, hence 2. and 3. are equivalent.

Assuming $(*)$, we have, in particular, that the distance between any two consecutive elements of A is the same as the distance between any two consecutive elements of B. This gives that A and B are arithmetic progressions of the same step size, as desired. □

Corollary 2.4. *The previous theorem holds for finite sets in torsion-free abelian groups.*

Proof. The map φ_M described in Appendix A is linear and hence preserves arithmetic progressions. It is enough, then, that the claim holds for finite sets of integers. □

We have the analogous connection in arbitrary abelian groups.

Theorem 2.5. *Let A, B be finite sets in an abelian group G. The following are equivalent:*

1. *There exists a finite subgroup H of G such that B is contained in a coset of H and A is a union of cosets of H*
2. $|A + B| = |A|$
3. $|A - B| = |A|$

Proof. Note that all of the conditions are invariant under translating B. Thus we may assume without loss of generality that $0 \in B$.

Assuming 1., we have that $B \subseteq H$, and hence $A + b = A$, $A - b = A$ for all $b \in B$. This yields $|A + B| = |A - B| = |A|$.

Since $A + b \subseteq A + B$, 2. implies that $A + b = A + B$ for all $b \in B$. This implies that $A + b = A + b'$ for all $b, b' \in B$, which is equivalent to saying that $A - b = A - b'$ for all b, b'. Since $A - B$ is a union of $A - b$ over $b \in B$, we get that $|A - B| = |A - b| = |A|$, which is 3. The same argument in reverse shows that 3. implies 2., hence they are equivalent to each other and to

$$A + b = A + b' \text{ for all } b, b' \in B. \tag{$*$}$$

Now we show that $(*)$ implies 1. Since $0 \in B$, $(*)$ gives that $A + b = A$ for all $b \in B$. Let $H = \{g \in G \mid A + g = A\}$; it is easy to verify that H is a finite subgroup. From the previous comment, $B \subseteq H$. Finally, if $a \in A$, then the coset $H + a \subseteq A$ by the definition of H. This gives that A is the union of the cosets $H + a$ for $a \in A$, as desired. □

We no longer have the structural characterizations at the upper bounds, but we are able to show that the bounds are attained simultaneously.

Lemma 2.6. *Let A, B be a finite sets in an abelian group. The following are equivalent:*

1. *There are no solutions to the equation $x + y = x' + y'$ for $x, x' \in A$, $y, y' \in B$*
2. *There are no solutions to the equation $x - y = x' - y'$ for $x, x' \in A$, $y, y' \in B$*
3. $|A + B| = |A||B|$
4. $|A - B| = |A||B|$

Proof. By rearranging the equations, 1. and 2. are clearly equivalent. There are $|A||B|$ possibilities for the sums $a + b$ with $a \in A$, $b \in B$, hence 1. and 3. are equivalent. The analogous statement for differences shows that 2. and 4. are equivalent. □

Theorems along these lines are called *inverse theorems* since we use the sumsets $A + B$ and $A - B$ to deduce information on A and B. There are many more such inverse theorems, Freĭman's theorem perhaps being the most famous; the reader is referred to [16, 36].

2.2.2 Ruzsa's triangle inequality

We now present two inequalities of fundamental importance to sumset estimates. For finite sets A, B, C in an abelian group, we will show

$$|A||B - C| \leq |A - B||A - C|,$$
$$|A||B + C| \leq |A + B||A + C|.$$

The first is sometimes called *Ruzsa's triangle inequality*, for reasons explained below. The second is a special case of the Plünnecke-Ruzsa inequality, Theorem 2.22. Both were established by Ruzsa, but by very different means. In particular, the first has an elementary proof while the second, until very recently, relied heavily on Plünnecke's method. We present one proof of the first inequality and three proofs of the second in this section and the next.

Theorem 2.7 (Ruzsa, 1976)**.** *Let A, B, C be finite sets in an abelian group. Then*

$$|A||B - C| \leq |A - B||A - C|.$$

Proof. We describe an injection φ of $A \times (B - C)$ into $(A - B) \times (A - C)$. To each $d \in B - C$ associate a $b_d \in B$, $c_d \in C$ such that $d = b_d - c_d$, and let $\varphi(a, d) = (a - b_d, a - c_d)$.

To verify that φ is injective, suppose $\varphi(a, d) = \varphi(a', d')$ for $a, a' \in A$, $d, d' \in D$. This yields

$$a - b_d = a' - b_{d'},$$
$$a - c_d = a' - c_{d'}.$$

Subtracting the first equation from the second yields $b_d - c_d = b_{d'} - c_{d'}$, or $d = d'$. This in turn gives $b_d = b_{d'}$, $c_d = c_{d'}$, whereby $a = a'$, as desired. □

There are other sumset inequalities that admit an injection argument similar to the one above. We will present a more complicated injection argument for the second inequality in the next section.

For A, B finite sets in an abelian group G, let

$$d(A,B) = \log \frac{|A-B|}{\sqrt{|A||B|}}.$$

We see that d is symmetric and non-negative by Lemma 2.2. Theorem 2.7 is then equivalent to the triangle inequality

$$d(A,B) \leq d(A,C) + d(B,C)$$

for all finite sets C in G. Note that d is not a distance function in the usual sense because $d(A,A)$ is not always zero; Corollary 1.11 characterize when $d(A,A)$ is zero. Many of the results here may be comfortably reformulated in terms of d.

2.2.3 Plünnecke-Ruzsa inequality with two summands

We now want to prove the sum version of Ruzsa's triangle inequality. It is not immediately clear why simple injective proofs like the one used above fail, but they do. Ruzsa first published the inequality in 1989 as a corollary to Theorem 2.22 which was obtained using Plünnecke's method.

In 2011, Petridis [22] gave an elementary proof of the inequality by introducing a new theorem and a new approach to proving sumset estimates. In a comment on Tim Gower's blog post [2] on Petridis' results, Christian showed how to prove Petridis' theorem with an injection argument. We present both of these arguments, in addition to Ruzsa's original one, in this section.

We begin with Ruzsa's original argument from [28] in 1989.

Theorem 2.8 (Ruzsa, 1989)**.** *Let A, B, C be finite sets in an abelian group. We have*

$$|A||B+C| \leq |A+B||A+C|.$$

Proof (Ruzsa, 1989). Using Theorem 2.22, there exists a non-empty $X \subseteq A$ such that

$$|B+C| \leq |X+B+C| \leq \frac{|A+B|}{|A|}\frac{|A+C|}{|A|}|X| \leq \frac{|A+B|}{|A|}|A+C|.$$

Multiplying by $|A|$ yields the desired inequality. □

Following the same proof but using the stronger $|X|+|B+C|-1 \leq |X+B+C|$ for torsion-free groups, we have the following easy corollary. This corollary will not follow from Petridis' arguments below.

Corollary 2.9. *Let A, B, C be finite sets in a torsion-free abelian group. We have*

$$|A||B+C| \leq |A+B||A+C| - |A|(|A|-1).$$

We now present Petridis' argument from [22]. The first step is a theorem concerning the growth of $|A+B+C|$ when A and B are such that $\frac{|A+B|}{|A|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty $Z \subseteq A$. Isolating from the beginning a set which minimizes the growth ratio $\frac{|Z+B|}{|Z|}$ is the key to Petridis' new arguments.

Theorem 2.10 (Petridis, 2011)**.** *Let A and B be finite sets in an abelian group G such that $\frac{|A+B|}{|A|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty $Z \subseteq A$. Then*

$$|A||A+B+C| \leq |A+B||A+C|$$

for all finite sets C in G.

Proof. We proceed by induction on $|C|$. When $C = \{c\}$, $|A+B+\{c\}| = |A+B|$ and $|A+\{c\}| = |A|$, and the inequality is trivially satisfied.

Suppose now that the inequality is satisfied for C and that we wish to prove it for $C' = C \cup \{x\}$ for some integer $x \notin C$. Let $Z = \{a \in A \mid \{a\} + B + \{x\} \subseteq A + B + C\}$ so that

$$A + B + C' = (A + B + C) \cup \Big((A + B + \{x\}) \Big\backslash (Z + B + \{x\})\Big).$$

Since $Z \subseteq A$, it follows that $|A + B + C'| \leq |A + B + C| + |A + B| - |Z + B|$. (Note that if $Z = \emptyset$, then $Z + B + \{x\} = \emptyset$ and $|Z + B| = 0$.) The inductive hypothesis $|A||A+B+C| \leq |A+B||A+C|$ combined with our assumption that $|A||Z + B| \geq |Z||A + B|$ gives

$$|A||A + B + C'| \leq |A + B|(|A + C| + |A| - |Z|).$$

Now it is sufficient to show that $|A + C| + |A| - |Z| \leq |A + C'|$.

Let $W = \{a \in A \mid a + x \in A + C\}$. Observe that

$$A + C' = (A + C) \cup \Big((A + \{x\}) \Big\backslash (W + \{x\})\Big)$$

is a disjoint union, whereby $|A + C'| = |A + C| + |A| - |W|$. Also, $W \subseteq Z$, so that $|W| \leq |Z|$. These together show that $|A + C'| \geq |A + C| + |A| - |Z|$, as desired. □

The condition on A and B may seem to be restrictive. Note, however, that given sets A, B, there is always a subset A' of A such that $\frac{|A'+B|}{|A'|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty $Z \subseteq A$. Using this, Theorem 2.8 follows easily.

Proof of Theorem 2.8 (Petridis, 2011). Let $A' \subseteq A$ be a subset of A such that $\frac{|A'+B|}{|A'|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty $Z \subseteq A$. Then

$$|A||B + C| \leq |A||A' + B + C| \leq |A|\frac{|A' + B|}{|A'|}|A' + C| \leq |A + B||A + C|,$$

where the first inequality is trivial, the second follows from Theorem 2.10, and the third uses the assumption on $|A'|$ above with $Z = A$ and that $A' \subseteq A$. □

We show in Section 2.3.2 how to apply Petridis' result inductively to get bounds on higher sumsets. It is of particular interest to find out if his arguments can provide elementary proofs of most or all of the results obtained by Plünnecke's method. As it stands, Plünnecke's method yields slightly stronger results; see Sections 2.3.1 and 2.3.2.

We conclude this section with a proof of Petridis' theorem with an injection argument given by Christian on Gowers' blog [2]. We begin with a lemma.

Lemma 2.11 (Christian, 2011)**.** *Let A, B be finite sets in an abelian group. A satisfies $\frac{|A+B|}{|A|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty $Z \subseteq A$ if and only if there exists a bijection $\psi : A \times (A+B) \to A \times (A+B)$ such that $\psi(a, A+B) \subseteq A \times (\{a\}+B)$ for all $a \in A$.*

Proof. If such a ψ exists, for any $Z \subseteq A$ it induces an injection $Z \times (A+B) \hookrightarrow A \times (Z+B)$, whereby $|Z||A+B| \leq |A||Z+B|$, as desired.

Conversely, define $f : A \to \mathcal{P}(A \times (A+B))$ by $f(a) = A \times (\{a\}+B)$. For each $Z \subseteq A$, we have

$$|f(Z)| = |A \times (Z+B)| = |A||Z+B| \geq |Z||A+B|.$$

Hall's marriage theorem gives us a matching in which each $a \in A$ is paired with a subset of size $|A+B|$ of $A \times (\{a\}+B)$. Defining ψ according to this matching yields the desired bijection. □

Proof of Theorem 2.10 (Christian, 2011). Fix a bijection ψ as in the lemma. We describe an injection φ of $A \times (A+B+C)$ into $(A+B) \times (A+C)$. Impose a linear ordering $\leq$ on C. For each $e \in A+B+C$, denote by c_e the smallest element $c \in C$ such that $e - c \in A+B$, and let $d_e = e - c_e$. Denote ψ^{-1} by $(\psi_1^{-1}, \psi_2^{-1})$. Finally, define $\varphi(a, e) = (\psi_2^{-1}(a, d_e), \psi_1^{-1}(a, d_e) + c_e)$.

To show that φ is injective, suppose $\varphi(a, e) = \varphi(a', e')$ for $a, a' \in A$, $e, e' \in A+B+C$. We have

$$\begin{aligned} \psi_2^{-1}(a, d_e) &= \psi_2^{-1}(a', d_{e'}), \\ \psi_1^{-1}(a, d_e) + c_e &= \psi_1^{-1}(a', d_{e'}) + c_{e'}. \end{aligned}$$

If $c_e = c_{e'}$, then the fact that ψ is a bijection gives that $a = a'$ and $d_e = d_{e'}$. Then $e = d_e + c_e = d_{e'} + c_{e'} = e'$ shows that $(a, e) = (a', e')$.

If $c_e \neq c_{e'}$, we may assume without loss of generality that $c_e < c_{e'}$ and write

$$\begin{aligned} e' = d_{e'} + c_{e'} &= d_{e'} - \psi_1^{-1}(a', d_{e'}) + \psi_1^{-1}(a', d_{e'}) + c_{e'} \\ &= d_{e'} - \psi_1^{-1}(a', d_{e'}) + \psi_1^{-1}(a, d_e) + c_e \\ &= \psi_1^{-1}(a, d_e) + (d_{e'} - \psi_1^{-1}(a', d_{e'})) + c_e. \end{aligned}$$

Note that $\psi_1^{-1}(a, d_e) \in A$ and $c_e \in C$. The equation $\psi(\psi_1^{-1}(a', d_{e'}), \psi_2^{-1}(a', d_{e'})) = (a', d_{e'})$ gives that $d_{e'} - \psi_1^{-1}(a', d_{e'}) \in B$ (using that $\psi(a, A+B) \subseteq A \times (\{a\}+B)$ for all $a \in A$). Thus we have written e' as $d + c$ with $d \in A+B$, $c \in C$ where $c = c_e < c_{e'}$, contradicting the minimality of $c_{e'}$. □

2.2.4 Other estimates

We conclude this section by outlining some miscellaneous asymmetric sumset estimates.

1. The following is a useful corollary to Ruzsa's triangle inequality and the Plünnecke-Ruzsa inequality.

Corollary 2.12. *Let A, B, C be finite sets in an abelian group. We have*

$$|A||B \pm C| \leq |A \pm B||A \pm C|$$

for any choice of the signs.

Proof. Using Theorems 2.7 and 2.8 and the substitutions $A \to -A$, $B \to -B$, $C \to -C$, we have

$$\begin{aligned}
&|A||B-C| \le |A-B||A-C|, \quad |A||B+C| \le |A+B||A+C|,\\
&|A||B-C| \le |A+B||A+C|, \quad |A||B+C| \le |A-B||A-C|,\\
&|A||B+C| \le |A+B||A-C|, \quad |A||B-C| \le |A-B||A+C|,\\
&|A||B+C| \le |A-B||A+C|, \quad |A||B-C| \le |A+B||A-C|. \qquad \square
\end{aligned}$$

2. We discussed in Section 1.2.3 that $|A+A|$ and $|A-A|$ are strongly correlated near their minimum values. More specifically, we showed that $|A+A| \le \alpha|A|$ implies that $|A-A| \le \alpha^2|A|$ and vice versa.

We are naturally led to wonder whether the corresponding statement holds for asymmetric estimates: does there exist an $f(\alpha)$ such that if $|A+B| \le \alpha|A|$, then $|A-B| \le f(\alpha)|A|$? The answer was shown to be negative by Ruzsa in [31]. He shows, roughly speaking, that there exists a $\theta > 1$ and arbitrarily large sets of integers A and B such that $|A+B| \le \alpha|A|$ and

$$|A-B| \ge f(\alpha)|A+B|^{\theta}$$

where f is a function only of α. Since $|A| \le |A+B|$ and the exponent on $|A+B|$ is greater than 1, the fact that $|A|$ can be arbitrarily large means that the left hand side cannot be bounded by only a function of $|A|$ and α. See Theorem B.6 in Appendix B.

We do have, however, by the trivial bounds that $|A-B| \le |A+B|^2$. We may improve the exponent to $3/2$ by the following.

Corollary 2.13. *Let A, B be finite sets in an abelian group. We have*

$$|A-B| \le |A+B|^{3/2}.$$

Proof. We see by the trivial bounds and a double application of Corollary 2.12 that

$$|A-B|^2 \le |A||B||A-B| \le |A||A+B||B+B| \le |A+B|^3. \qquad \square$$

This is currently the best exponent we have on this inequality.

Question 7. *What is the infimum of values of c such that $|A-B| \le |A+B|^c$ holds for all finite sets A, B in an abelian group?*

Simplices in the integer lattice show via Theorem B.2 that the best exponent cannot be lower than $\frac{\log(1+\sqrt{2})}{\log 2}$. It is particularly interesting that the best exponent comes from a symmetric example. Is there not a way to utilize the asymmetry to construct better ones?

3. For finite sets A, B in an abelian group, Ruzsa's triangle inequality and the trivial estimates yield

$$|A-B| \le |A+B|\frac{|A+A|}{|A|} \le |A+B||2A|^{1/2}.$$

Corollary 1.34 gives that the sequence $|kA|^{1/k}$ is decreasing, hence the following theorem from [3] is an improvement.

Theorem 2.14. *For finite sets A, B in an abelian group, we have*

$$|A-B| \leq |A+B||3A|^{1/3}.$$

Theorem B.3 in Appendix B shows that $|A-B| \leq |A+B||6A|^{1/6}$ fails to hold for $A = B = \Delta_k^{2k}$ when k is sufficiently large. This leads us to the following question.

Question 8. *Does the inequality $|A-B| \leq |A+B||kA|^{1/k}$ hold for $k = 4, 5$ for all finite sets A, B in an abelian group?*

Combined with information on the growth of $|A+B|$, Theorem 2.14 may be used to strengthen Corollary 2.13 when $|A+B| \leq |A|^{4/3}$ in the following way.

Corollary 2.15. *Let A, B be finite sets in an abelian group, $|A+B| = \alpha|A|$. We have*

$$|A-B| \leq \alpha^{2/3}|A+B|^{4/3}.$$

Proof. By Corollary 2.16, we have $|3B| \leq \frac{|A+B|^3}{|A|^2}$. It follows from Theorem 2.14 above that

$$|A-B| \leq |A+B||3A|^{1/3} \leq \frac{|A+B|^2}{|A|^{2/3}} = \alpha^{2/3}|A+B|^{4/3}. \qquad \square$$

2.3 Higher estimates

As in the symmetric case, our goal is to understand the growth of higher asymmetric sumsets in terms of lower ones. Plünnecke's method, introduced in Section 1.3.4, is one of the most important tools in accomplishing this task.

We forego the trivial estimates in this section. To estimate $|kA+lB|$ or $|A+B+C|$, we use a combination of the asymmetric trivial estimates in Section 2.2.1 with the single set sumset estimates of Section 1.3.1.

Recent results by Petridis gives elementary proofs of some of the corollaries to Plünnecke's inequality. Sections 2.3.1 and 2.3.2 were written in such a way as to juxtapose the results from Plünnecke's method and from Petridis. We then show how some Plünnecke-type results and the results from Section 1.3.5 may be extended to different summands.

2.3.1 Corollaries to Plünnecke's method

Here we prove a useful corollary to Plünnecke's inequality which allows us to bound $|kB-lB|$ in terms of $|A+iB|$. As shown in Section 1.3.4, an application of this to symmetric estimates gives bounds on the higher sumsets of A in terms of $|A+A|$ or $|A-A|$. For convenience, we restate the main result of Plünnecke's method due to Ruzsa in 1989.

Theorem (Plünnecke's inequality)**.** *Let A, B be finite sets in an abelian group, $i \leq k$ be positive integers, $|A| = n$, and $|A+iB| = \alpha n$. There exists a non-empty $X \subseteq A$ such that*

$$|X+kB| \leq \alpha^{k/i}|X|.$$

Passing to a subset X of A is necessary for this result. To see that X cannot always be taken to be a singleton, let $A = B$ be an arithmetic progression of integers length L. Then $|kB|$ is on the order of kL while $\alpha^{k/i}$ is on the order of $i^{k/i}$. The inequality fails to hold for large L. To see on the other hand that X cannot always be taken to be A, $A = B = \{0, 1, 3\}$ provides a small counter-example.

It is important in some applications to have control over the size of the subset X. There are results along these lines, primarily due to Ruzsa. The reader is referred to [1].

Plünnecke's inequality is often applied via the following corollary. The proof follows immediately from the previous corollary using that $|X| \leq n$, $|kB| \leq |X + kB|$, and $|X| + |kB| - 1 \leq |X + kB|$ when the ambient group is torsion-free.

Corollary 2.16. *Let A, B be finite sets in an abelian group G, $i \leq k$ be positive integers, $|A| = n$, and $|A + iB| = \alpha n$. We have*

$$|kB| \leq \alpha^{k/i} n.$$

If G is torsion-free, then $|kB| \leq (\alpha^{k/i} - 1)n + 1$.

More generally, we can use a double application of this combined with Ruzsa's triangle inequality to handle repeated addition and subtraction of a set B.

Theorem 2.17. *Let A, B be finite sets in an abelian group, $i \leq k \leq l$ be positive integers, $|A| = n$, $|A + iB| = \alpha n$. Then*

$$|kB - lB| \leq \alpha^{(k+l)/i} n.$$

Proof. By Plünnecke's inequality, there exists a non-empty $X \subseteq A$ such that

$$|X + kB| \leq \alpha^{k/i} |X|.$$

There are now two cases. If $k < l$, then apply the Plünnecke's inequality again with X in place of A to get a non-empty $X' \subseteq X$ such that

$$|X' + lB| \leq \left(\alpha^{k/i}\right)^{l/k} |X'| = \alpha^{l/i} |X'|.$$

If $k = l$, then let $X' = X$ and note that it satisfies the same inequality. In either case, we may now use Ruzsa's triangle inequality to see

$$\begin{aligned} |X'||kB - lB| &\leq |X' + kB||X' + lB| \\ &\leq |X + kB||X' + lB| \\ &\leq \alpha^{k/i} |X| \alpha^{l/i} |X'| \\ &\leq \alpha^{(k+l)/i} n |X'| \end{aligned}$$

Dividing by $|X'|$ yields the result. □

2.3.2 Corollaries to Petridis' Theorem

Slightly different versions of the corollaries to Plünnecke's theorem are available by inductively applying Petridis' theorem. The results presented in this section are simultaneously weaker and stronger: we lose the scaling feature but have more information on the subset X of A.

Theorem 2.18. *Let A, B be finite sets in an abelian group, $|A| = n$, and $|A + B| = \alpha n$. There exists a non-empty $X \subseteq A$ such that for all $k \geq 1$, we have*

$$|X + kB| \leq \alpha^k |X|.$$

This is a stronger version of Plünnecke's inequality in the $i = 1$ case because the subset X is now independent of k.

Proof. Let X be a non-empty subset of A such that $\frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty subsets Z of A.

We induct on k. Since $\frac{|X+B|}{|X|} \leq \frac{|A+B|}{|A|} = \alpha$, we have the base case $k = 1$ by

$$|X + B| = \frac{|X + B|}{|X|}|X| \leq \alpha |X|.$$

Assuming now that we have the result for k, we use Petridis' theorem and the inductive hypothesis to see

$$\begin{aligned} |X||X + B + kB| &\leq |X + B||X + kB| \\ &\leq |X + B|\alpha^k |X| \\ &\leq |X + B|\alpha^k n. \end{aligned}$$

Dividing by $|X|$ and using again that $\frac{|X+B|}{|X|} \leq \alpha$ yields the inductive step. □

Note that we may easily strengthen the inductive hypothesis in the proof above to be $|X + kB| \leq \left(\frac{|X+B|}{|X|}\right)^k |X|$. Using this, we strengthen the result to the following corollary.

Corollary 2.19. *Let A, B be finite sets in an abelian group and X be a non-empty subset of A such that $\frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty subsets Z of A. Then for all $k \geq 1$,*

$$|X + kB| \leq \left(\frac{|X + B|}{|X|}\right)^k |X|.$$

The following result is the analogue to Theorem 2.17 in the $i = 1$ case. It follows easily from Theorem 2.18 or 2.19.

Theorem 2.20. *Let A, B be finite sets in an abelian group, $|A| = n$, $|A+B| = \alpha n$. Then*

$$|kB - lB| \leq \alpha^{k+l} n.$$

Proof. Let X be a non-empty subset of A such that $\frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty subsets Z of A. By Ruzsa's triangle inequality and the previous theorem, we have

$$\begin{aligned} |X||kB - lB| &\leq |X + kB||X + lB| \\ &\leq \alpha^{k+l}|X|^2 \\ &\leq \alpha^{k+l} n|X|. \end{aligned}$$

Dividing by $|X|$ yields the desired inequality. □

Note again the we lose the scaling feature but that the subset X is the same for all k, l. Just as before, using a stronger inductive hypothesis, we've actually shown the following slightly stronger result.

Corollary 2.21. *Let A, B be finite sets in an abelian group and X be a non-empty subset of A such that $\frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$ for all non-empty subsets Z of A. Then for all $k, l \geq 1$,*

$$|kB - lB| \leq \left(\frac{|X + B|}{|X|}\right)^{k+l} |X|.$$

It is possible that similar elementary arguments may yield the scaling results as in Plünnecke's inequality. The reader is referred to the comments on Gowers' blog post [2] regarding these results.

2.3.3 Plünnecke-Ruzsa inequality

We turn our attention now to higher sumset estimates involving multiple, possibly distinct summands. We begin with a useful generalization of Plünnecke's inequality to handle multiple sets.

Theorem 2.22. *Let A, B_1, ..., B_k be finite sets in an abelian group, $|A| = n$, $|A + B_i| = \alpha_i n$. Then there exists a non-empty $X \subseteq A$ such that*

$$|X + B_1 + \cdots + B_k| = \alpha_1 \cdots \alpha_k |X|.$$

This is generally known as the Plünnecke-Ruzsa inequality. The proof is a clever application of Plünnecke's inequality and the tensor power trick; the reader is referred to Ruzsa's original proof in [28] from 1989.

This theorem is often applied via the following corollary. As before, the proof follows easily from the fact that $|X| \leq |A|$, $|B_1 + \cdots + B_k| \leq |X + B_1 + \cdots + B_k|$, and $|X| + |B_1 + \cdots + B_k| - 1 \leq |X + B_1 + \cdots + B_k|$ if the ambient group is torsion-free.

Corollary 2.23. *Let A, B_1, ..., B_k be finite sets in an abelian group G, $|A| = n$, $|A + B_i| = \alpha_i n$. We have*

$$|B_1 + \cdots + B_k| \leq \alpha_1 \cdots \alpha_k n.$$

If G is torsion-free, then we have $|B_1 + \cdots + B_k| \leq (\alpha_1 \cdots \alpha_k - 1)n + 1$.

Note that when $B_i = B$ in the Plünnecke-Ruzsa inequality, we recover the $i = 1$ case of Plünnecke's inequality. Gyarmati, Matolcsi, and Ruzsa [4] showed in 2008 that the Plünnecke-Ruzsa inequality may be generalized to exhibit the same scaling as in Plünnecke's inequality.

Theorem 2.24. *Let $i \leq k$ be positive integers and A, B_1, ..., B_k be finite sets in an abelian group. Let $K = \{1, \ldots, k\}$, and for $J \subseteq K$, let B_J denote $\sum_{j \in J} B_j$. Let $|A| = n$, $|A + B_J| = \alpha_J n$, and*

$$\beta = \left(\prod_{I \subseteq K, |I| = i} \alpha_I \right)^{1/\binom{k-1}{i-1}}.$$

There exists a non-empty $X \subseteq A$ such that

$$|X + B_K| \leq \beta |X|.$$

Note that when $i = 1$, we recover the Plünnecke-Ruzsa inequality, and that when $B_i = B$, we recover Plünnecke's inequality.

2.3.4 Superadditivity and submultiplicativity

Applying the trivial estimates twice to a sumset of the form $A + B + C$ in a torsion-free abelian group yields

$$|A| + |B| + |C| - 2 \leq |A + B + C| \leq |A||B||C|.$$

We showed a strengthening on the Plünnecke-Ruzsa inequality in the previous section by making use of more general subsums of $A + B_1 + \cdots + B_k$. Following the same idea, we might ask whether or not $|A+B+C|$ may be more effectively bounded by $|A + B|$, $|A + C|$, and $|B + C|$.

The answer is affirmative in much greater generality. We present the two main theorems of [5], both of which have elementary proofs. The following result is a subadditivity property for sumsets.

Theorem 2.25. *Let A_1, ..., A_k be finite sets in a torsion-free abelian group. We have*

$$|A_1 + \cdots + A_k| \geq \frac{1}{k-1} \left(\sum_{i=1}^{k} |A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| - 1 \right).$$

The following result is a supermultiplicativity property for sumsets.

Theorem 2.26. *Let A_1, ..., A_k be finite sets in an abelian group. We have*

$$|A_1 + \cdots + A_k| \leq \left(\prod_{i=1}^{k} |A_1 + \cdots + A_{i-1} + A_{i+1} + \cdots + A_k| \right)^{\frac{1}{k-1}}.$$

The proof of Theorem 2.26 in [5] relies on a lemma which is well known as an entropy inequality. There are many exciting connections between sumset estimates and entropy inequalities; the reader is referred to [34]. The following recent theorem of Madiman, Marcus, and Tetali [12] answers a question posed in [5] utilizing this connection.

Theorem 2.27. *Let A, B_1, $\ldots$, B_k be finite subsets of an abelian group. If $\mathcal{I}$ is a collection of r-elements subsets of $\{1,\ldots,k\}$, then for any $C \subseteq B_1 + \cdots + B_k$, we have*

$$|A + C|^{|\mathcal{I}|} \leq |C|^{|\mathcal{I}|-r} \prod_{I \in \mathcal{I}} \Big|A + \sum_{i \in I} B_i\Big|.$$

Appendix A: Products and projections

One of the most natural ways to create large families of additive sets is to form products. We begin by showing that cardinalities of sumsets behave well under taking products. We then describe how to project sets in $\mathbb{Z}^d$ to $\mathbb{Z}$ while preserving the cardinalities of a specified set of sumsets.

Using products and projections, we show that finite sets in the integer lattice $\mathbb{Z}^d$, and hence in torsion-free abelian groups, provide no new information with regards to sumset cardinalities. We conclude by outlining two tricks common to the field: the digit trick and the tensor power trick.

A.1 Products

Let A_1, A_2 be finite subsets of the abelian groups G_1, G_2, respectively. We form the product $A = A_1 \times A_2$ as a finite subset of the abelian group $G = G_1 \times G_2$.

As sums and differences are computed coordinate-wise, it is easy to verify that

$$\begin{aligned} |A| &= |A_1||A_2|, \\ |A + A| &= |A_1 + A_1||A_2 + A_2|, \\ |A - A| &= |A_1 - A_1||A_2 - A_2|. \end{aligned}$$

More generally, for integers k, l we have

$$|kA - lA| = |kA_1 - lA_1||kA_2 - lA_2|.$$

This easily generalizes to different summands. Indeed, let $A_{1,i}$, $A_{2,i}$ be finite collections of sets in G_1, G_2, respectively. Then

$$\Big|\sum_i (A_{1,i} \times A_{2,i})\Big| = \Big|\sum_i A_{1,i}\Big|\Big|\sum_i A_{2,i}\Big|.$$

This fact underlies the multiplicative nature of many of the results in the field.

It is common to take the product of a set with itself in order to find a larger set with similar properties. For example, suppose that we wish to find a set A with $|A+A|-|A-A| \geq c$ for some integer $c \geq 1$. It is sufficient to find $A' \subseteq G'$ such that $|A' + A'| - |A' - A'| \geq 1$ and then set A to be $A'^{m_c} \subseteq G'^{m_c}$ for a sufficiently large integer m_c.

Note, however, that A in the previous example is situated in a group which depends on m_c. If we wish to find such a set in a fixed group G, then we might look for a way to transform an example in G'^{m_c} to an example in G while maintaining some of its additive structure. This is explained for $G = \mathbb{Z}$ in the next section.

A.2 Projections

Let A be a finite set in $\mathbb{Z}^d$. We wish to find a set A' in $\mathbb{Z}$ such that

$$|A'| = |A|, \quad |A' + A'| = |A + A|, \quad |A' - A'| = |A - A|.$$

In other words, we wish to find a set of integers which has the same "low-level" additive structure as our original set.

To this end, it is sufficient to describe a map $\varphi : A \longrightarrow \mathbb{Z}$ with the property that

$$a_1 + a_2 = a_3 + a_4 \iff \varphi(a_1) + \varphi(a_2) = \varphi(a_3) + \varphi(a_4)$$

for all $a_i \in A$. The map $\varphi : A \longrightarrow \varphi(A)$ is called a *Freĭman isomorphism* of *order* 2. If we set $A' = \varphi(A)$, then it is any easy exercise to verify that the desired equations above hold. (See [36] for more on Freĭman homomorphisms.)

For $M \in \mathbb{Z}^d$, define $\varphi_M : \mathbb{Z}^d \longrightarrow \mathbb{Z}$ by $\varphi_M(x) = x \cdot M$. In order for φ_M to be a Freĭman isomorphism of order 2 from A to $\varphi_M(A)$, we need only to check that

$$a_1 + a_2 - a_3 - a_4 = 0 \iff (a_1 + a_2 - a_3 - a_4) \cdot M = 0$$

for all $a_i \in A$. The "only if" implication is trivial. The "if" implication requires that M be the normal vector to a hyperplane which avoids the set finite $(A + A - A - A) \backslash \{0\}$ in $\mathbb{Z}^d$. Such a vector M exists, and φ_M is the desired projection. We have just shown the following theorem.

Theorem A.1. *Let A be a finite set in $\mathbb{Z}^d$. There exists a set of integers A' such that $|A'| = |A|$, $|A' + A'| = |A + A|$, and $|A' - A'| = |A - A|$.*

This can be easily generalized to higher sumsets by employing higher order Freĭman isomorphisms. Using φ_M as above, we need only that the hyperplane defined by M avoids a larger, but still finite, set. We have the following corollary.

Corollary A.2. *Let A be a finite set in $\mathbb{Z}^d$ and $p \geq 1$ be an integer. There exists a set of integers A', depending on p, such that $|A'| = |A|$ and $|kA' - lA'| = |kA - lA|$ for integers k, l where $|k| + |l| \leq p$.*

If A is a finite subset of a torsion-free abelian group G, then we may speak about the subgroup $\langle A \rangle$ generated by the elements of A. It is a finitely generated, torsion-free abelian group, hence it is isomorphic $\mathbb{Z}^d$ for some d. Because the set A and all of its sumsets lie in $\langle A \rangle$, we have the following corollary.

Corollary A.3. *The previous corollary holds when A is a finite subset of a torsion-free abelian group.*

While the structure of sets is sometimes better understood in $\mathbb{Z}^d$, this result gives that cardinality questions about single set sumsets in the integers are equivalent to cardinality questions about single set sumsets in arbitrary torsion-free abelian groups. This is utilized often as it is usually helpful to have the ordering of a set of integers.

This generalizes nicely to the case of different summands. Suppose, for example, we are given finite sets A, B in $\mathbb{Z}^d$ and wish to find finite sets of integers A', B' such that

$$|A'| = |A|, \quad |B'| = |B|, \quad |A' + B'| = |A + B|, \quad |A' - B'| = |A - B|.$$

The same $\varphi_M : A \cup B \longrightarrow \mathbb{Z}$ defined above with an appropriately chosen M will work. Note that the comments above on higher order Freĭman isomorphisms and torsion-free abelian groups hold more generally in this setting.

Indeed, given a finite number of finite sets in an abelian group and a finite collection of sumsets of those sets, we may find sets of integers which have the same additive structure with respect to the collection of sumsets. We record this in as a corollary, the proof of which is a combination of the comments in this paragraph and the results above.

Corollary A.4. *Let $A_1, \dots A_m$ be finite sets in a torsion-free abelian group, and let $S_1, \dots, S_r$ be sumsets involving $A_1, \dots, A_m$. (For example, $S_1 = A_1 + A_2 - A_m$.) There exist finite sets of integers $A_1', \dots, A_m'$ such that $|S_i| = |S_i'|$ for all i, where S_i' is S_i with all instances of A_i replaced by A_i'.*

A.3 The digit and tensor power tricks

Given a finite set of integers A, it is often useful to combine the process of taking products and projecting back to the integers. If we define φ_M as above and let $M = (1, m, \dots, m^{d-1})$, then we realize A^d in the integers with the set

$$A' = \left\{ \sum_{i=1}^{d} a_i m^{i-1} \;\middle|\; (a_1, \dots, a_d) \in A^d \right\}.$$

The set A' then has the desired sumset cardinalities as long as m is sufficiently large. This is sometimes referred to as the *digit trick* or the *base expansion method*. See Appendix B, Section B.2 for an explicit example.

We now describe the *tensor power trick* as it usually arises when dealing with sumsets. Suppose that $X(A)$ and $Y(A)$ are products of sumsets of A. Suppose that we want to show that $X(A) \leq Y(A)$ holds for all finite sets A in any abelian group, but that we are only able to show the weaker inequality $X(A) \leq CY(A)$ for some constant $C \geq 1$.

Because the weaker inequality holds also for A^d and $X(A^d) = X(A)^d$, $Y(A^d) = Y(A)^d$ from the comments in the first section, we have $X(A)^d \leq CY(A)^d$ holds for all A, $d \geq 1$. Taking d-th roots and letting $d \to \infty$, we see that $X(A) \leq Y(A)$ holds for all sets A, as we wanted to show.

This trick works for sets of integers as well by the corollaries from the previous section. More specifically, if we are able to show that $X(A) \leq CY(A)$ holds when A is a finite set of integers, then $X(A) \leq Y(A)$ holds for all finite sets of integers as well since we are able to realize products of sets of integers as sets of integers.

Given that we have multiplicativity with distinct summands as well, the tensor power trick holds in much greater generality than just described. As a concrete example, Ruzsa shows in [31] that the inequality

$$|A + 2B| \leq 3|A + B|\sqrt{|B + B|}$$

holds for all finite sets A, B. The constant 3 is removed by applying the inequality to A^d and B^d and letting $d \to \infty$ as described above.

See [37] for a more in-depth discussion of the tensor power trick with many more examples.

Appendix B: Sets with many more differences than sums

Here we are concerned with constructing sets which have many more differences than sums. As described in Appendix A, such sets are easily attained as products; here we describe two different constructions. We begin by elaborating on the simplex example of Hennecart, Robert, and Yudin in [8]. We then discuss a construction of Ruzsa from [31] which shows, roughly speaking, that $|A-B|$ may be much larger than $|A+B|$.

B.1 Simplices in $\mathbb{Z}^d$

Simplices in the integer lattice exhibit many more differences than sums. This was published by Hennecart, Robert, and Yudin [8] who attribute the idea to Freĭman and Pigarev [25]. Here we use these sets to show lower bounds for the exponents in Theorems 1.12 and 1.17 and Corollary 1.18 as well as answer a question related to Question 8.

Let $\Delta_l^d = \{(x_1,\dots,x_d) \in \mathbb{Z}^d \mid 0 \le x_i \text{ for all } i \text{ and } \sum_i x_i \le l\}$ be the d-dimensional simplex of size l. The following lemma will allow us to compare the number of sums and differences of Δ_l^d.

Lemma B.1.

$$\begin{aligned}
|\Delta_l^d| &= \binom{d+l}{d} \\
|\Delta_{l_1}^d + \Delta_{l_2}^d| &= \binom{d+l_1+l_2}{d} \\
|\Delta_{l_1}^d - \Delta_{l_2}^d| &= \sum_{i=0}^{\min(d,l_2)} \binom{d}{i}\binom{l_2}{i}\binom{d-i+l_1}{d-i} \\
&= \sum_{i=0}^{\min(d,l)} \binom{d}{i}^2 \binom{d-i+l}{d} \quad \text{if } l_1 = l_2 = l
\end{aligned}$$

Proof. For $|\Delta_l^d|$, we have l balls to put into d boxes. To count the number of sums, note that $\Delta_{l_1}^d + \Delta_{l_2}^d = \Delta_{l_1+l_2}^d$ and use the first remark.

To count the number of differences, we define two helper functions. Let $\mathcal{P} : \mathbb{Z}^d \to \mathbb{Z}$ take a lattice point to the sum of its positive-valued coordinates, and let $\mathcal{N} : \mathbb{Z}^d \to \mathbb{Z}$ take a lattice point to the sum of its negative-valued coordinates. Let

$$D_{l_1,l_2}^d = \{x \in \mathbb{Z}^d \mid \mathcal{P}(x) \le l_1 \text{ and } \mathcal{N}(x) \ge -l_2\}.$$

First we show that $\Delta_{l_1}^d - \Delta_{l_2}^d = D_{l_1,l_2}^d$. If $x = x_1 - x_2$ where $x_1 \in \Delta_{l_1}^d$, $x_2 \in \Delta_{l_2}^d$, then clearly $\mathcal{P}(x) \le \mathcal{P}(x_1) \le l_1$. Similarly, $\mathcal{N}(x) \ge \mathcal{N}(-x_2) \ge -l_2$. Hence $\Delta_{l_1}^d - \Delta_{l_2}^d \subseteq D_{l_1,l_2}^d$.

Conversely, let x be such that $\mathcal{P}(x) \le l_1$ and $\mathcal{N}(x) \ge -l_2$. Define x_1 to be x with its negative-valued coordinates replaced by 0. Define x_2 to be $-x$ with its negative-valued coordinates replaced by 0. Then $x_1 \in \Delta_{l_1}^d$, $x_2 \in \Delta_{l_2}^d$, such that $x = x_1 - x_2$, and so $\Delta_{l_1}^d - \Delta_{l_2}^d \supseteq D_{l_1,l_2}^d$.

We wish to count $D^d_{l_1,l_2}$. We may partition it according to the coordinates at which its elements are negative. Fix $N \subseteq \{1,\dots,d\}$, and let

$$D^d_{l_1,l_2,N} = \{x \in \mathbb{Z}^d \mid x_i < 0 \text{ if and only if } i \in N,\ \mathcal{P}(x) \le l_1, \text{ and } \mathcal{N}(x) \ge -l_2\}.$$

Then we have the disjoint union

$$D^d_{l_1,l_2} = \bigcup_{N\subseteq\{1,\dots,d\}} D^d_{l_1,l_2,N}.$$

Now we count $D^d_{l_1,l_2,N}$. Note that we have two conditions on $x \in D^d_{l_1,l_2,N}$: $\mathcal{N}(x) \ge -l_2$ on the $|N|$ negative-valued coordinates, and $\mathcal{P}(x) \le l_1$ on the $|\overline{N}|$ non-negative-valued coordinates. We have therefore a copy of $\Delta^{|N|}_{l_2-|N|}$ in the negative-valued coordinates and a copy of $\Delta^{|\overline{N}|}_{l_1}$ in the non-negative-valued coordinates. Because the two conditions are independent, we have

$$|D^d_{l_1,l_2,N}| = |\Delta^{|N|}_{l_2-|N|}||\Delta^{|\overline{N}|}_{l_1}| = \binom{l_2}{|N|}\binom{|\overline{N}|+l_1}{|\overline{N}|}$$

Note also that $N \in \{1,\dots,d\}$ can be only as large as $\min(d,l_2)$ since $x_i \le -1$ for $i \in N$. We have finally that

$$|D^d_{l_1,l_2}| = \sum_{i=0}^{\min(d,l_2)} \binom{d}{i}\binom{l_2}{i}\binom{d-i+l_1}{d-i}.$$

If $l_1 = l_2 = l$, then we may use the identity $\binom{l}{i}\binom{d-i+l}{d-i} = \binom{d}{i}\binom{d-i+l}{d}$ to simplify the sum. □

We now give a lower bound for the exponent in Theorem 1.17. The following theorem first appeared as part of the main theorem in [8].

Theorem B.2. *If $c \in \mathbb{R}$ is such that $|A-A| \le |A+A|^c$ holds for all finite $A \subseteq \mathbb{Z}$, then $c \ge \frac{\log(1+\sqrt{2})}{\log 2} > 1.2715$.*

Proof. By Appendix A, it is sufficient to show a sequence of finite sets $A_k \subseteq \mathbb{Z}^{d_k}$ such that $\log|A_k - A_k|/\log|A_k + A_k|$ tends to $\frac{\log(1+\sqrt{2})}{\log 2}$ as k tends to infinity. We will show that $A_k = \Delta^{2k}_k$ works with the help of Lemma B.1.

In order to estimate the difference set $|\Delta^{2k}_k - \Delta^{2k}_k|$, let

$$M_k = \max_{0\le i\le k} \binom{2k}{i}^2\binom{3k-i}{2k}.$$

Using Stirling's formula, we see

$$\log\binom{2k}{i}^2\binom{3k-i}{2k} \sim \log\left(\frac{(2k)^2(3k-i)^3}{(2k-i)^4(k-i)}\right)^k\left(\frac{(2k-i)^2(k-i)}{i^2(3k-i)}\right)^i$$

as $k, i \to \infty$. The right hand side is maximized at $i = (2-\sqrt{2})d$ at which it attains $4k\log(1+\sqrt{2})$. Hence $\log M_k \sim 4k\log(1+\sqrt{2})$ as $k \to \infty$. We see from Lemma B.1 that $M_k \le |\Delta^{2k}_k - \Delta^{2k}_k| \le (k+1)M_k$, from which it follows that

$$\log|\Delta^{2k}_k - \Delta^{2k}_k| \sim \log M_k \sim 4k\log(1+\sqrt{2}) \qquad k \to \infty.$$

We also have that

$$\log|\Delta_k^{2k}+\Delta_k^{2k}| = \log\binom{4k}{2k} \sim 4k\log 2 \qquad k\to\infty.$$

Combining these two estimates, we have

$$\frac{\log|\Delta_k^{2k}-\Delta_k^{2k}|}{\log|\Delta_k^{2k}+\Delta_k^{2k}|} \sim \frac{\log(1+\sqrt{2})}{\log 2} \qquad k\to\infty. \qquad \square$$

Using the same Δ_k^{2k}, we may show that the inequality $|A-B| \le |A+B||6A|^{1/6}$ from Question 8 fails to hold even in the case that $A=B$.

Theorem B.3. *There exists a finite set of integers A such that*

$$|A-A| > |A+A||6A|^{1/6}.$$

Proof. Using the estimates from the previous proof and that $6\Delta_k^{2k} = \Delta_{6k}^{2k}$, we have

$$\begin{aligned}\log|6\Delta_k^{2k}| &\sim k\log(2^{16}/3^6),\\ \log|\Delta_k^{2k}+\Delta_k^{2k}| &\sim 4k\log 2,\\ \log|\Delta_k^{2k}-\Delta_k^{2k}| &\sim 4k\log(1+\sqrt{2}).\end{aligned}$$

Since

$$4\log(1+\sqrt{2}) > 4\log 2 + \frac{1}{6}\log\frac{2^{16}}{3^6},$$

we have that

$$|\Delta_k^{2k}-\Delta_k^{2k}| > |\Delta_k^{2k}+\Delta_k^{2k}||6\Delta_k^{2k}|^{1/6}$$

when k is sufficiently large. We may construct a set of integers with the same sumset sizes by the work in Appendix A. $\square$

In the same vein, we have the following theorem. This shows, in particular, that the exponent in Theorem 1.12 is the best possible.

Theorem B.4. *If $c\in\mathbb{R}$ is such that $\frac{|A-A|}{|A|} \le \left(\frac{|A+A|}{|A|}\right)^c$ holds for all finite $A\subseteq\mathbb{Z}$, then $c\ge 2$.*

Proof. We follow closely the steps in Theorem B.2 with $\Delta_{k^2}^k$. In order to control $|\Delta_{k^2}^k - \Delta_{k^2}^k|/|\Delta_{k^2}^k|$, we define

$$M_k = \max_{0\le i\le k}\binom{k}{i}^2\binom{k+k^2-i}{k}.$$

We check that $\log\left(\binom{k}{i}^2\binom{k+k^2-i}{k}\Big/\binom{k+k^2}{k}\right)$ is asymptotic to

$$\log\left(\frac{k(k+k^2-i)}{(k+1)(k-i)^2}\right)^k\left(\frac{k(k+k^2-i)}{(k+1)(k^2-i)}\right)^{k^2}\left(\frac{(k-i)^2(k^2-i)}{i^2(k+k^2-i)}\right)^i$$

as $k, i \to \infty$. This is maximized at $i = \frac{1}{2}(1+2k-\sqrt{1+4k^2})k$ at which it attains

$$\log\left(\frac{2k+\sqrt{1+4k^2}}{k+1}\right)^k \left(\frac{2k^2+1+\sqrt{1+4k^2}}{2k(k+1)}\right)^{k^2}.$$

This is asymptotic to $2k\log 2$ as $k \to \infty$, hence $\log \frac{M_k}{|\Delta^k_{k^2}|} \sim 2k\log 2$. From $M_k \le |\Delta^k_{k^2} - \Delta^k_{k^2}| \le (k+1)M_k$, we deduce that

$$\log \frac{|\Delta^k_{k^2} - \Delta^k_{k^2}|}{|\Delta^k_{k^2}|} \sim \log \frac{M_k}{|\Delta^k_{k^2}|} \sim 2k\log 2 \qquad k \to \infty.$$

We also have as $k \to \infty$ that

$$\log \frac{|\Delta^k_{k^2} + \Delta^k_{k^2}|}{|\Delta^k_{k^2}|} \sim k\log\left(1+\frac{k}{k+1}\right)\left(1+\frac{1}{4k^2+4k}\right)^k \sim k\log 2.$$

Combining these two estimates, we have

$$\log \frac{|\Delta^k_{k^2} - \Delta^k_{k^2}|}{|\Delta^k_{k^2}|} \Big/ \log \frac{|\Delta^k_{k^2} + \Delta^k_{k^2}|}{|\Delta^k_{k^2}|} \sim 2 \qquad k \to \infty. \qquad \square$$

We conclude with a lower bound on one of the exponents in Corollary 1.18.

Theorem B.5. *If $c \in \mathbb{R}$ is such that $\frac{|A-A|}{|A+A|} \le |A|^c$ holds for all finite $A \subseteq \mathbb{Z}$, then $c \ge \log\left(\frac{3842+1066\sqrt{13}}{3125}\right)\Big/\log\left(\frac{256}{27}\right) > 0.4$.*

Proof. Following the same steps with Δ^{3d}_d, we let $M_k = \max_{0\le i\le k} \binom{3k}{i}^2 \binom{4k-i}{3k}$ and find that $\log\left(\binom{3k}{i}^2\binom{4k-i}{3k}\Big/\binom{5k}{3k}\right)$ is asymptotic to

$$\log\left(\frac{108(3k)^3(4k-i)^4}{3125(3k-i)^6(k-i)}\right)^k \left(\frac{(3k-i)^2(k-i)}{i^2(4k-i)}\right)^i \qquad k, i \to \infty.$$

This is maximized at $i = \left(\frac{5-\sqrt{13}}{2}\right)k$ at which it attains $k\log\frac{3842+1066\sqrt{13}}{3125}$, and so $\log\frac{M_k}{|\Delta^{3k}_k+\Delta^{3k}_k|} \sim k\log\frac{3842+1066\sqrt{13}}{3125}$ as $k \to \infty$. From $M_k \le |\Delta^{3k}_k - \Delta^{3k}_k| \le (k+1)M_k$, we deduce that

$$\log \frac{|\Delta^{3k}_k - \Delta^{3k}_k|}{|\Delta^{3k}_k + \Delta^{3k}_k|} \sim \log \frac{M_k}{|\Delta^{3k}_k + \Delta^{3k}_k|} \sim k\log\frac{3842+1066\sqrt{13}}{3125} \qquad k \to \infty.$$

We also have as $k \to \infty$ that

$$\log|\Delta^{3k}_k| \sim k\log(256/27).$$

Combining these estimates, we see as $k \to \infty$ that

$$\log \frac{|\Delta^{3k}_k - \Delta^{3k}_k|}{|\Delta^{3k}_k + \Delta^{3k}_k|} \Big/ \log|\Delta^{3k}_k| \sim \log\left(\frac{3842+1066\sqrt{13}}{3125}\right)\Big/\log\left(\frac{256}{27}\right). \qquad \square$$

B.2 An asymmetric construction of Ruzsa

We now describe a construction of Ruzsa which yields two sets A, B of integers such that $|A-B|$ is much larger than $|A+B|$. This was first published in [31]; we take the presentation almost verbatim from [3]. We will prove the following theorem.

Theorem B.6. *Let $\alpha > 1$ be a real number. Let U be a set of non-negative integers containing 0, and set $s = |U+U|$, $d = |U-U|$, and $q = 2\max U + 1$. If $d < q$, then there exists pairs (A, B) of finite, non-empty sets of integers with $|B| \le |A|$, $|B|$ arbitrarily large such that $|A+B| \le \alpha|A|$ and*

$$|A-B| \ge \left(\frac{2(\alpha-1)}{3\alpha}\right)^{5/4} |A+B|^{1+\log(d/s)/\log q}.$$

The idea is to take a set of integers U which has many more differences than sums and magnify the difference by making use of asymmetric sumsets. We do this first by magnifying U via the digit trick, then adding and subtracting this new set with multiple copies of itself and an interval.

The set $U = \{0, 1, 3, 6, 13, 17, 21\}$ gives $s = 26$, $d = 39$, and $q = 43$. This will yield the exponent

$$1 + \log(d/s)/\log q = 1 + \log(39/26)/\log 43 > 1.1078.$$

This theorem shows that the asymmetric analogue of Theorem 1.12 is not possible. See Section 2.2.4.

Proof. Fix k to be an arbitrarily large integer. Set

$$B = \left\{ \sum_{i=0}^{k-1} u_i q^i \;\middle|\; (u_0, \dots, u_{k-1}) \in U^d \right\}.$$

This is a magnified copy of U via the digit trick as described in Appendix A. Since q is large enough, we have $|B+B| = s^k$ and $|B-B| = d^k$.

Next, set

$$A = \{1, \dots, L\} \cup \bigcup_{i=1}^{m} (a_i + B)$$

where m, L are positive integers to be specified later and the a_i's are positive integers larger than $L + q^k$ and such that $a_i - a_j \notin (B-B) \cup (B+B)$ when $i \ne j$. (It is not difficult to find such a_i's by choosing them consecutively, one sufficiently larger than the previous.)

Since $\max B < q^k$ and $m \ge 1$, the lower bound on the a_i's gives that $|A| \ge L + |B|$; in other words, there is no overlap between the interval and the at least one translate of B.

Consider $A+B$ and $A-B$. The condition on the a_i's guarantees that B plus the translated copies of B in A do not overlap. If we let $t = |\{1, \dots, L\} + B| = |\{1, \dots, L\} - B|$, then we see that

$$|A+B| = ms^k + t, \qquad |A-B| = md^k + t.$$

Since $\max U < q/2$, we have that $\max B < q^k/2$. This gives that $B \subseteq \{0, \dots, q^k/2\}$, and hence $L \le t \le L + q^k/2$.

We choose

$$L = \left\lfloor \frac{3q^k}{2(\alpha-1)} \right\rfloor, \qquad m = \left\lfloor \left(\frac{q}{s}\right)^k \right\rfloor.$$

We need to show the upper bound on $|A+B|$ and the lower bound on $|A-B|$. Note that $m \geq 1$ since $q \geq s$, and so $|A| \geq |B|$.

By the choice of L and m, we have

$$|A+B| \leq q^k + t \leq \frac{3}{2}q^k + L \leq \frac{3\alpha q^k}{2(\alpha-1)} \leq \alpha(L+1) \leq \alpha|A|.$$

If k is so large that $d^k \leq t$ (recall $d < q$), then we have

$$|A-B| \geq \left(\left(\frac{q}{s}\right)^k - 1\right) d^k + t \geq \left(\frac{qd}{s}\right)^k \geq \left(\frac{2(\alpha-1)|A+B|}{3\alpha}\right)^{1+\log(d/s)/\log q}.$$

The last inequality follows from $|A+B| \leq \frac{3\alpha q^k}{2(\alpha-1)}$ by taking the logarithm of both sides.

By Theorem 1.17 and our assumption that $d < q$, we have $d \leq \min(q, s^{4/3})$, and so $d^4 \leq qs^4$. This gives that

$$1 + \frac{\log d - \log s}{\log q} \leq \frac{5}{4},$$

which, combined with $\frac{2(\alpha-1)}{3\alpha} < 1$, yields

$$|A-B| \geq \left(\frac{2(\alpha-1)}{3\alpha}\right)^{5/4} |A+B|^{1+\log(d/s)/\log q}. \qquad \square$$

References

[1] Alfred Geroldinger and Imre Z. Ruzsa, *Combinatorial number theory and additive group theory*, Advanced Courses in Mathematics. CRM Barcelona, Birkhäuser Verlag, Basel, 2009, Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008. MR 2547479 (2010f:11005)

[2] William T. Gowers, *A new way of proving sumset estimates*, `http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/`, February 2011.

[3] Katalin Gyarmati, François Hennecart, and Imre Z. Ruzsa, *Sums and differences of finite sets*, Funct. Approx. Comment. Math. **37** (2007), no. part 1, 175–186. MR 2357317 (2008i:11013)

[4] Katalin Gyarmati, Máté Matolcsi, and Imre Z. Ruzsa, *Plünnecke's inequality for different summands*, Building bridges, Bolyai Soc. Math. Stud., vol. 19, Springer, Berlin, 2008, pp. 309–320. MR 2484645 (2010a:11018)

[5] ———, *A superadditivity and submultiplicativity property for cardinalities of sumsets*, Combinatorica **30** (2010), no. 2, 163–174. MR 2676833 (2011d:11013)

[6] Peter Hegarty and Steven J. Miller, *When almost all sets are difference dominated*, Random Structures Algorithms **35** (2009), no. 1, 118–136. MR 2532877 (2010f:11016)

[7] Peter V. Hegarty, *Some explicit constructions of sets with more sums than differences*, Acta Arith. **130** (2007), no. 1, 61–77. MR 2354149 (2008m:11048)

[8] François Hennecart, Gilles Robert, and Alexander Yudin, *On the number of sums and differences*, Astérisque (1999), no. 258, xiii, 173–178, Structure theory of set addition. MR 1701195 (2000f:11024)

[9] Askold G. Khovanskiĭ, *The Newton polytope, the Hilbert polynomial and sums of finite sets*, Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57–63, 96. MR 1209944 (94e:14068)

[10] ———, *Sums of finite sets, orbits of commutative semigroups and Hilbert functions*, Funktsional. Anal. i Prilozhen. **29** (1995), no. 2, 36–50, 95. MR 1340302 (96e:20091)

[11] Vsevolod F. Lev, *Structure theorem for multiple addition and the Frobenius problem*, J. Number Theory **58** (1996), no. 1, 79–88. MR 1387726 (97d:11056)

[12] Mokshay M. Madiman, Adam Marcus, and Prasad Tetali, *Entropy and set cardinality inequalities for partition-determined functions, with applications to sumsets*, CoRR **abs/0901.0055** (2009).

[13] John Marica, *On a conjecture of Conway*, Canad. Math. Bull. **12** (1969), 233–234. MR 0249390 (40 #2635)

[14] Greg Martin and Kevin O'Bryant, *Many sets have more sums than differences*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 287–305. MR 2359479 (2008i:11038)

[15] Steven J. Miller, Brooke Orosz, and Daniel Scheinerman, *Explicit constructions of infinite families of MSTD sets*, J. Number Theory **130** (2010), no. 5, 1221–1233. MR 2607310 (2011c:11010)

[16] Melvyn B. Nathanson, *Additive number theory*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996, Inverse problems and the geometry of sumsets. MR 1477155 (98f:11011)

[17] ———, *Growth of sumsets in abelian semigroups*, Semigroup Forum **61** (2000), no. 1, 149–153. MR 1839220 (2002c:11129)

[18] ———, *Problems in additive number theory. I*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 263–270. MR 2359476 (2009c:11020)

[19] ———, *Sets with more sums than differences*, Integers **7** (2007), A5, 24. MR 2282188 (2008d:11008)

[20] Melvyn B. Nathanson, Kevin O'Bryant, Brooke Orosz, Imre Ruzsa, and Manuel Silva, *Binary linear forms over finite sets of integers*, Acta Arith. **129** (2007), no. 4, 341–361. MR 2346109 (2009a:11057)

[21] Melvyn B. Nathanson and Imre Z. Ruzsa, *Polynomial growth of sumsets in abelian semigroups*, J. Théor. Nombres Bordeaux **14** (2002), no. 2, 553–560. MR 2040693 (2004k:11024)

[22] Giorgis Petridis, *New Proofs of Plünnecke-type Estimates for Product Sets in Non-Abelian Groups*, ArXiv e-prints (2011).

[23] ———, *Plünnecke's Inequality*, ArXiv e-prints (2011).

[24] ———, *Upper Bounds on the Cardinality of Higher Sumsets*, ArXiv e-prints (2011).

[25] V. P. Pigarev and Gregory A. Freĭman, *The relation between the invariants R and T*, Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian), Kalinin. Gos. Univ., Moscow, 1973, pp. 172–174. MR 0434995 (55 #7957)

[26] Helmut Plünnecke, *Eine zahlentheoretische Anwendung der Graphentheorie*, J. Reine Angew. Math. **243** (1970), 171–183. MR 0266892 (42 #1794)

[27] Imre Z. Ruzsa, *On the cardinality of $A + A$ and $A - A$*, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam, 1978, pp. 933–938. MR 519317 (80c:05016)

[28] ———, *An application of graph theory to additive number theory*, Sci. Ser. A Math. Sci. (N.S.) **3** (1989), 97–109. MR 2314377

[29] ———, *Addendum to: An application of graph theory to additive number theory*, Sci. Ser. A Math. Sci. (N.S.) **4** (1990/1991), 93–94.

[30] ———, *On the number of sums and differences*, Acta Math. Hungar. **59** (1992), no. 3-4, 439–447. MR 1171750 (93h:11025)

[31] ———, *Sums of finite sets*, Number theory (New York, 1991–1995), Springer, New York, 1996, pp. 281–293. MR 1420216 (97i:11019)

[32] ———, *Cardinality questions about sumsets*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 195–205. MR 2359472 (2008k:11028)

[33] ———, *Many differences, few sums*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **51** (2008), 27–38 (2009). MR 2567492 (2011d:11014)

[34] ———, *Sumsets and entropy*, Random Structures Algorithms **34** (2009), no. 1, 1–10. MR 2478535 (2009j:05030)

[35] Imre Z. Ruzsa and Sándor Turjányi, *A note on additive bases of integers*, Publ. Math. Debrecen **32** (1985), no. 1-2, 101–104. MR 810596 (87a:11014)

[36] Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006. MR 2289012 (2008a:11002)

[37] Tricki, *The tensor power trick*, `http://www.tricki.org/article/The_tensor_power_trick`, August 2009.

[38] Yufei Zhao, *Counting MSTD sets in finite abelian groups*, J. Number Theory **130** (2010), no. 10, 2308–2322. MR 2660895