Walk through Combinatorics: Sumset inequalities*

(Version 2d: revised 3 December 2018)

The aim of additive combinatorics If A and B are two non-empty sets of numbers, their *sumset* is the set $A+B \stackrel{\text{def}}{=} \{a+b : a \in A,\ b \in B\}$. The additive combinatorics can be crudely described as being concerned with describing structure of sets A for which $A+A$ is small. The reason a whole branch of mathematics is devoted to this problem is the ubiquity of convolutions in mathematics. Recall that a convolution of two discrete-valued functions f, g is the function $f * g$ defined by $f * g(x) = \sum_{y+z=x} f(y)g(z)$. If f, g are non-negative, then the support of $f * g$ is a sumset: $\operatorname{supp} f * g \subseteq \operatorname{supp} f + \operatorname{supp} g$. This hints at links between additive combinatorics and understanding convolutions. Some of these links require generalizations of the notion of sumsets, which we will not pursue here.

Structure of sets of with small doubling Suppose A is a set of n integers. The sumset $A+A$ can be as large as $\binom{n+1}{2}$, and if A is a random sets it will be this large. We thus think of sets A with large $A+A$ as *additively unstructured*. On the other hand, the sets with small $A+A$ are very structured. Let us examine the examples.

First, if A is $\{1, 2, \dots, n\}$ or any other arithmetic progression of n elements, then $|A+A| = 2n-1$. It is not overly difficult to show by induction on n that the converse is true: for every n-element set we have $|A+A| \geq 2n-1$, with equality only for arithmetic progressions.

Second, if A is a large subset of an arithmetic progression, then $A+A$ is small, being a subset of a corresponding arithmetic progression. It can be shown that if $A+A$ is not too large, $|A+A| \leq 3n-2$, then A is a large subset of an arithmetic progression.

However, there is one more example of a set with a small sumset. Set $A' = [n]^2 \subset \mathbb{Z}^2$ satisfies $|A'+A'| \leq 4|A'|$, and if we choose any linear map $\phi\colon \mathbb{Z}^2 \to \mathbb{Z}$ that is injective on A', the set $A = \phi(A')$ also satisfies $|A+A| \leq 4|A|$. Such a set A is an arithmetic progression of arithmetic progressions, such as one drawn below.

This example can be combined with the previous example. We take a dense subset of $[n]^2$, and project it to $\mathbb{Z}$. These examples naturally generalize to rectangles other than

*These notes are available from the course webpage, and directly from `http://www.borisbukh.org/DiscreteMath14/notes_additive_inequalities.pdf`

squares, and to higher dimensions. A famous result in additive combinatorics, Freiman's theorem asserts that the converse is true: any set A with $|A+A| \leq K|A|$ is a dense subset of a projection of a low-dimensional parallelepiped. However, the known bounds in Freiman's theorem make it useless for majority of applications, and much of additive combinatorics is devoted to bypassing the need for Freiman's theorem.

Triangle inequalities In applications often one has a set A with small sumset, and one wishes to show that A enjoys some of the properties that the arithmetic progression enjoys. For example, one might want to conclude that the difference set $A-A$ is also small. The following inequalities serve that and other purposes

Theorem 1 (Ruzsa's difference triangle inequality)**.** *Suppose A, B, C are non-empty sets in some abelian group. Then*

$$|A-B| \leq \frac{|A-C||C-B|}{|C|}.$$

Theorem 2 (Ruzsa's sum triangle inequality)**.** *Suppose A, B, C are non-empty sets in some abelian group. Then*

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

Corollary 3 (Ruzsa's triangle inequalities)**.** *Suppose A, B, C are non-empty sets in some abelian group. Then*

$$|A \pm B| \leq \frac{|A \pm C||C \pm B|}{|C|}$$

hold for all eight possible choices of the signs.

The Corollary follows from the Theorems by replacing sets B and C by $-B$ and $-C$ as appropriate.

If we take $A = B = C$, then as a special case we obtain that

$$|A+A| \leq K|A| \quad \Longrightarrow \quad |A-A| \leq K^2|A+A|, \tag{1}$$

$$|A-A| \leq K|A| \quad \Longrightarrow \quad |A+A| \leq K^2|A-A|. \tag{2}$$

We shall prove (1) and Theorem 1, which implies (2). We shall also prove Theorem 2.

The two theorems not only resemble the triangle inequality, by allowing to control $A+B$ via $A+C$ and $B+C$, but can also be rewritten as the usual triangle inequality. Consider, for example, Theorem 1, and define $d(A,B) \stackrel{\text{def}}{=} \log\bigl[|A-B|/(|A||B|)^{1/2}\bigr]$. We can then rewrite Theorem 1 as

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

Of course, Theorem 2 be rewritten similarly.

Despite their similarities the two theorems are very different. Theorem 1 is much easier to prove, with a proof that admits a generalization to non-abelian groups.

Proof of Theorem 1. We shall prove that $|A-B||C| \le |A-C||C-B|$ by exhibiting an injection $\phi\colon (A-B)\times C \to (A-C)\times(C-B)$. For each $x \in A-B$ choose $a(x) \in A$ and $b(x) \in B$ such that $a(x)-b(x)=x$. Then put $\phi(x,c) = \big(a(x)-c, c-b(x)\big)$. The map is injective since from $\big(a(x)-c, c-b(x)\big)$ one can recover x as $x = (a(x)-c)+(c-b(x))$ and c as $c = (c-b(x))+b(x)$. □

Plünnecke–Ruzsa–Petridis inequalities The proof of (1) rests on the following lemma.

Lemma 4 (Plünnecke–Ruzsa–Petridis)**.** *If A, B are non-empty subsets of some abelian group, and*

$$|A+B| \le K|A|,$$

then there exists a non-empty set $X \subseteq A$ such that

$$|X+B+C| \le K|X+C| \tag{3}$$

for every set C.

Proof. The following proof, due to Petridis, is a great simplification of Ruzsa's proof, which in turn is a great simplification of arguments implicit in the work of Plünnecke. The proof below is highly unusual for extremal combinatorics, being a direct proof by induction.

Let X be a non-empty subset of A that minimizes the ratio $|X+B|/|X|$. Let

$$K' = \frac{|X+B|}{|X|}. \tag{4}$$

It is clear that $K' \le K$. We will show, by induction on $|C|$, that

$$|X+B+C| \le K'|X+C| \qquad \text{for all } C.$$

The base $|C|=1$ follows from (4). Suppose $|C| \ge 2$. By translating C if necessary, we may assume that $0 \in C$. Let $C' = C \setminus \{0\}$, and define

$$Y = \{x \in X : x+B \subset X+B+C'\}.$$

Then

$$\begin{aligned}(X+B+C' \cup \{0\}) \setminus (X+B+C') &= (X+B+\{0\}) \setminus (X+B+C') \\ &= (X+B) \setminus (X+B+C') \\ &\subseteq (X+B) \setminus (Y+B).\end{aligned}$$

Hence,

$$\begin{aligned}|(X+B+C' \cup \{0\}) \setminus (X+B+C')| &\le |X+B| - |Y+B| \\ &= K'|X| - |Y+B| \\ &\le K'|X| - K'|Y| \qquad \text{by minimality of } X \\ &= K'|X \setminus Y|.\end{aligned}$$

To establish (3), since $|X + C' \cup \{0\}| - |X + C'| = |X \setminus (X + C')|$, it remains to show that $|X \setminus Y| \leq |X \setminus (X + C')|$, or equivalently

$$|(X + C') \cap X| \leq |Y|.$$

However, $(X + C') \cap X \subset Y$. □

From Lemma 4 it is easy to deduce bounds on $A + A + \cdots + A$ in terms of $A + A$. Let sA denote the sumset $A + A + \cdots + A$ with s summands.

Theorem 5. *If s, t are positive integers, and $|A + A| \leq K|A|$ then*

$$|sA - tA| \leq K^{s+t}|A|.$$

In particular (1) *holds.*

Proof. Let $B = A$, and X be as in Lemma 4, then

$$|X + A + C| \leq K|X + C|$$

for every C. From that it follows that $|X + sA| \leq K|X + (s-1)A|$ and so, by induction on s, that

$$|X + sA| \leq K^{s-1}|X + A|.$$

As the inequality $|U - V| \leq |U + W||V + W|/|W|$ follows from the difference triangle inequality, which we have already proved, we deduce that

$$|sA - tA| \leq \frac{|X + sA||X + tA|}{|X|} \leq K^{s-1}\frac{|X + A||X + tA|}{|X|} \leq K^s|X + tA| \leq K^sK^t|A|. \quad \square$$

Similarly we can prove the sum triangle inequality.

Proof of Theorem 2. We shall show that $|B + C| \leq \frac{|A+B||A+C|}{|A|}$.

Let X be a subset of A minimizing the ratio $|X + B|/|X|$. Let K be this ratio. Then by Lemma 4 we have

$$|X + B + C| \leq K|X + C|.$$

Since $K \leq |A + B|/|A|$ we obtain

$$|A||B + C| \leq |A||X + B + C| \leq K|A||X + C| \leq |A + B||X + C| \leq |A + B||A + C|. \quad \square$$

Ruzsa's covering lemma The second main ingredient for proving inequalities between sumsets is the Ruzsa's covering lemma.

Theorem 6 (Ruzsa's covering lemma)**.** *For every non-empty sets A, B in some abelian group, there exists a set $X \subseteq B$ such that*

$$B \subset A - A + X$$

with $|X| \leq |A + B|/|A|$.

Proof. Let X be a maximal subset of B such that the translates $\{A + x : x \in X\}$ are disjoint. Let $b \in B$ be arbitrary. Since $A + b$ intersects $A + X$, it follows that $b \in (A+X) - A = A - A + X$. As b is arbitrary, $B \subset A - A + X$. The bound on the size of X follows since the translates are disjoint and their union is of size $|A+X| \leq |A+B|$. □

Corollary 7. *If a set A satisfies $|A + A| \leq K|A|$, then there is a X of size $|X| \leq K^4$ such that $2A - A \subset A - A + X$*

Proof. Let $B = 2A - A$. From Theorem 5 it follows that $|B - A| = |2A - 2A| \leq K^4|A|$. The rest follows from the covering lemma. □

Freiman's theorem in a group with bounded torsion As an application, we prove a version of Freiman's theorem in the case where the ambient group is of bounded torsion. Namely, we say that an abelian group G is of *torsion* r if each $x \in G$ satisfies $rx = 0$. Note that this implies, in particular, that $(r-1)x = -x$, and so $\langle A \rangle = \bigcup_{k \geq 0} kA$, where $\langle A \rangle$ is the subgroup of G generated by A.

Theorem 8 (Freiman's theorem in bounded torsion groups)**.** *Let $r \in \mathbb{N}$ be fixed. Suppose G is a group of torsion r, and $A \subset G$ is a subset satisfying $|A + A| \leq K|A|$. Then A is contained in a subgroup of G of size at most $f(r, K)|A|$ for some function f of r and K only.*

Proof. By Corollary 7 there is $X \subset A$ such that $2A - A \subset A - A + X$ and $|X| \leq K^4$. Thus, $3A - A = A + (2A - A) \subseteq A + (A - A + X) = 2A - A + X \subseteq A - A + 2X$. Similarly, we deduce that $kA - A \subseteq A - A + (k-1)X$ for every $k \in \mathbb{N}$. Let $\langle X \rangle$ denote the subgroup of G generated by X. We thus have $kA - A \subseteq A - A + \langle X \rangle$ for every k. Since every element of $\langle A \rangle$ is in $kA - A$ for some k, we deduce that

$$\langle A \rangle \subseteq A - A + \langle X \rangle$$

Thus, $|\langle A \rangle| \leq |A - A||\langle X \rangle| \leq K^2 r^{|X|}|A| \leq K^2 r^{K^4}|A|$. □

A word about non-abelian groups The naive analogue of Plünnecke's inequality is false in non-commutative groups. As an example, let F_2 be the free group on generators x and y and consider $A = \{y^t : 0 \leq t \leq n\} \cup \{x\}$. Then $AA = \{y^t : 0 \leq t \leq 2n\} \cup \{xy^t : 0 \leq t \leq n\} \cup \{y^t x : 0 \leq t \leq n\} \cup \{x^2\}$. The set A has $n + 2$ elements, and AA has $(2n + 1) + 2(n + 1) + 1 = 4n + 4$ elements. So, $|AA|/|A| \leq 4$. However AAA contains a subset $\{y^s x y^t : 0 \leq s, t \leq n\}$ of size n^2.

It is true however that if $|AAA|/|A|$ is small, then $|A^t|/|A|$ is small for every t.