CHAPTER 2

Sumsets

We now come to some of the key definitions in additive combinatorics.

DEFINITION 2.1 (Sumsets and difference sets). Suppose that A and B are two sets in some abelian group. Then we write $A+B := \{a+b|a \in A, b \in B\}$ and $A-B := \{a-b|a \in A, b \in B\}$. Similarly if C is a further set we define $A+B+C := \{a+b+c|a \in A, b \in B, c \in C\}$, and so on. If A is a set and k, l are non-negative integers, not both zero, then $kA - lA$ denotes the set of sums $a_1 + \cdots + a_k - a'_1 - \cdots - a'_l$ with $a_1, \ldots, a_k, a'_1, \ldots, a'_l \in A$.

DEFINITION 2.2 (Doubling constant). Suppose that A is a finite set in some abelian group. Then we define the doubling constant $\sigma[A] := |A+A|/|A|$. More generally if A, B are two potentially different sets we define $\sigma[A,B] := |A+B|/|A|^{1/2}|B|^{1/2}$.

In this section we shall develop some basic inequalities for sumsets and difference sets.

2.1. Basic sumset estimates and Ruzsa calculus

The following result, though its proof is extremely simple, has proved to be absolutely fundamental in the subject.

THEOREM 2.1 (Ruzsa triangle inequality). *Suppose that U, V and W are three finite sets in some ambient abelian group. Then $|U||V-W| \leqslant |U-V||U-W|$.*

Proof. We define a map $\phi : U \times (V-W) \to (U-V) \times (U-W)$ as follows. For each $d \in V-W$, choose $v(d)$ and $w(d)$ such that $v(d)-w(d) = d$, and set $\phi(u,d) = (u-v(d), u-w(d))$. This map is well-defined and, furthermore, injective. Indeed if $\phi(u,d) = \phi(u',d')$ then $d = v(d)-w(d) = v(d')-w(d') = d'$, and hence $v(d) = v(d')$, $w(d) = w(d')$. Therefore $u = u'$. □

Remark. This inequality may be rewritten in the form

$$\log \frac{|V-W|}{|V|^{1/2}|W|^{1/2}} \leqslant \log \frac{|U-V|}{|U|^{1/2}|V|^{1/2}} + \log \frac{|U-W|}{|U|^{1/2}|W|^{1/2}},$$

at which point it becomes extremely natural to define the *Ruzsa distance* $d(U,V) := \log \frac{|U-V|}{|U|^{1/2}|V|^{1/2}}$ between pairs of sets U, V. Ruzsa's inequality may then be interpreted as the triangle inequality for this "distance"; note, however that d is not a

bona fide metric as the distance between unequal sets may vanish (when U and V are different cosets of the same subgroup) and more importantly $d(U,U)$ is rarely zero (in fact this happens only when U is a coset of a subgroup, as you may care to check).

The triangle inequality is often supplemented with the following estimate.

THEOREM 2.2 (Second Ruzsa inequality). *Suppose that U and V are two finite sets in some ambient abelian group. Then $d(U,-V) \leqslant 3d(U,V)$.*

Remark. By swapping the roles of V and $-V$ one may, of course, obtain the complimentary inequality $d(U,V) \leqslant 3d(U,-V)$.

Proof. Write $s(x)$ for the number of pairs (u,v) with $u+v=x$ and $r(x)$ for the number with $u-v=x$. Then $\sum r(x)^2 = \sum s(x)^2$, both quantities being equal to the number of quadruples (u_1,v_1,u_2,v_2) with $u_1+v_1=u_2+v_2$ and $u_1,u_2 \in U$, $v_1,v_2 \in V$. By double counting we have

$$\sum_x s(x) = \sum_x r(x) = |U||V|$$

and furthermore, by the Cauchy-Schwarz inequality,

$$\sum_x s(x)^2 = \sum_x r(x)^2 \geqslant \frac{|U|^2|V|^2}{|U-V|}.$$

It follows immediately that there is some x for which $r(x) \geqslant |U|^{1/2}|V|^{1/2}/|U-V|$. We now apply an idea of Lev, rather reminiscent of the one used in the proof of the Ruzsa triangle inequality. Let $S \subseteq U \times V$ be the set of pairs (u,v) with $u+v=x$ so that, by the preceding discussion, we have the lower bound $|S| \geqslant |U|^{1/2}|V|^{1/2}/|U-V|$. For $w \in U+V$, assign arbitrary $\alpha(w) \in U$ and $\beta(w) \in V$ such that $\alpha(w)+\beta(w)=w$, and consider the map $\psi : S \times (U+V) \to (U-V) \times (U-V)$ defined by $\psi(u,v,w) = (u-\beta(w), v-\alpha(w))$. This map is well-defined and, furthermore, injective. Indeed if $\psi(u,v,w) = \psi(u',v',w')$ then, using the fact that $u+v=u'+v'=x$, we have

$$\begin{aligned} w &= \alpha(w)+\beta(w) \\ &= u+v-(u-\beta(w))+(\alpha(w)-v)) \\ &= u'+v'-(u'-\beta(w'))+(\alpha(w')-v) \\ &= \alpha(w')+\beta(w') = w', \end{aligned}$$

from which it follows easily that $u=u'$ and $v=v'$.

The injectivity of ψ immediately implies that $|S||U+V| \leqslant |U-V|^2$, from which we at once obtain the bound $|U+V| \leqslant |U-V|^3/|U||V|$, which is equivalent to the stated inequality. □

Remark. The number of solutions to $u+v=u'+v'$ is called the *additive energy* between U and V. We will explore this concept more fully in Chapter **??**.

The two Ruzsa inequalities are often combined several times to establish that some particular pair of sets is close in Ruzsa distance. When relatively coarse bounds suffice it is extremely convenient to use a kind of notational calculus that we shall now describe. Let $K \geqslant 2$ be some ambient parameter, and write $X \lessapprox Y$ to mean $X \leqslant K^C Y$and $X \approx Y$ to mean $X \lessapprox Y$ and $Y \lessapprox X$. Different instances of the notation, of course, might entail different values of the absolute constant C. The notation is supposed to represent "roughly equal to" and "roughly less than", where the notion of "roughly" is somehow linked to the parameter K. If K is quite large, these will be rather weak notions, whereas if K is small they will be more precise.

Now let A and B be two sets in some ambient abelian group, and write $A \sim B$ to denote $|A-B|/|A|^{1/2}|B|^{1/2} \approx 1$. Note carefully that we do *not* necessarily have $A \sim A$, and in fact by the second Ruzsa inequality this happens if and only if the doubling constant $\sigma[A]$ is bounded by a polynomial in the approximation parameter K.

The rules of Ruzsa calculus may be written as follows.

PROPOSITION 2.1 (Ruzsa Calculus). *Suppose that U, V and W are sets in some ambient abelian group.*

(i) *Suppose that $U \sim V$. Then $U \sim -V$, $|U| \approx |V|$ and $\sigma[U], \sigma[V] \approx 1$.*
(ii) *If $U \sim V$ and $V \sim W$, then $U \sim W$.*
(iii) *Suppose that $U \sim V$, that $\sigma[W] \approx 1$ and that there is some x such that $|U \cap (x+W)| \approx |U| \approx |W|$. Then $U \sim V \sim W$.*
(iv) *Suppose that $\sigma[U], \sigma[W] \approx 1$ and that there is some x such that $|U \cap (x+W)| \approx |U| \approx |W|$. Then $U \sim W$.*

Proof. To see that $|U| \approx |V|$, note that if $U \sim V$ then

$$|U| \leqslant |U-V| \approx |U|^{1/2}|V|^{1/2}$$

whence $|U| \lessapprox |V|$, and similarly $|V| \lessapprox |U|$. Everything else stated in (i) and (ii) is an immediate consequence of the Ruzsa inequalities. To prove (iii), we may assume without loss of generality (by replacing W by $x+W$) that $x = 0$. Note first that as an instance of the Ruzsa triangle inequality and the inclusions $U \cap W \subseteq U, W$ we have

$$|U \cap W||U-W| \leqslant |(U \cap W) - U||(U \cap W) - W| \leqslant |U-U||W-W|.$$

However it follows from (i) and (ii) that $U \sim U$, that is to say $|U-U| \approx |U|$. Furthermore the assumption that $\sigma[W] \approx 1$ implies that $W \sim -W$ and hence by another application of (i) and (ii) we have $W \sim W$, and therefore $|W-W| \approx |W|$. Combining all this information with $|U \cap W| \approx |U| \approx |W|$ gives $|U-W| \approx |U| \approx |W|$, whence $U \sim W$ as required.

Finally, note that (iv) is simply a special case of (iii), stated separately for future convenience. □

Finally, one frequently needs to be able to control sums of more than two sets. The following inequality of Ruzsa implies, together with the preceding two, everything that is needed.

THEOREM 2.3 (Ruzsa's triple sumset inequality). *Suppose that U, V, W are three finite sets in some ambient abelian group and that $d(U,V), d(U,W), d(V,W) \leqslant \log K$. Then*

$$|U+V+W| \leqslant K^C |U|^{1/3}|V|^{1/3}|W|^{1/3}.$$

In the language of Ruzsa calculus, if $U \sim V \sim W$ then $W \sim U+V$.

Proof. We use, albeit sparingly, the language of Ruzsa calculus with parameter K. We leave it as an exercise for the reader to confirm that the two statements in this theorem imply one another; this is a good exercise to test you have understood "rough" notation properly.

The argument is due to Tao [**?**], and the heart of the matter is to establish the following claim: there is a set S with $S \sim U+V$. Once this is known it follows by Ruzsa calculus that $\sigma[U+V] \approx 1$. Furthermore by assumption that $d(U,W) \leqslant \log K$ we have $|U-W| \approx |U| \approx| W|$. Write $r(x)$ for the number of pairs (u,w) with $u-w=x$ and note that $r(x) = |U \cap (x+W)|$. Noting that $\sum_x r(x) = |U||W|$, it follows that there is some x such that $r(x) \gtrapprox |U|$. Replacing x by $x' := x+v$ for some arbitrary $v \in V$, it follows that $|(U+V) \cap (x'+W)| \gtrapprox |U|$. Since (by yet another application of Ruzsa calculus) we have $\sigma[W] \approx 1$, it follows from rule (iv) of Ruzsa calculus that $W \sim U+V$, as required.

It remains to establish the claim. Write $L = |U+V|/|U|^{1/2}|V|^{1/2}$, and note that the second Ruzsa inequality implies the bound $L \leqslant K^3$. The idea now is to take S to be the set of *popular sums* in $U+V$. Writing $s(x)$ for the number of pairs (u,v) with $x=u+v$, take S to be the set of those $x \in U+V$ for which $s(x) \geqslant \frac{1}{2L}|U|^{1/2}|V|^{1/2}$ (this happens to be the "right" definition: it will become clear why in a very short while).

We begin by establishing that S is reasonably large. By the same Cauchy-Schwarz argument used in the proof of Theorem 2.2 we have $\sum_x s(x)^2 \geqslant \frac{1}{L}|U|^{3/2}|V|^{3/2}$. The contribution to this sum from $x \notin S$ is bounded by

$$\sup_{x \notin S} s(x) \cdot \sum_x s(x) \leqslant \frac{1}{2L}|U|^{1/2}|V|^{1/2} \cdot |U||V|,$$

and so

$$\sum_{x \in S} s(x)^2 \geqslant \frac{1}{2L}|U|^{3/2}|V|^{3/2}.$$

Since $s(x) \leqslant |U|$ and $s(x) \leqslant |V|$ for all x, it follows that $|S| \geqslant \frac{1}{2L}|U|^{1/2}|V|^{1/2}$.

Now suppose that $u \in U, v \in V$ and $s \in S$. Then there are $\geqslant \frac{1}{2L}|U|^{1/2}|V|^{1/2}$ pairs $(u'v')$ such that $u'+v'=s$, and for each of them we may write

$$u+s+v = (u+v')+(v+u').$$

These give *distinct* representations of $u+s+v$ as the sum of two elements of $U+V$. It follows that

$$|U+S+V| \cdot \frac{1}{2L}|U|^{1/2}|V|^{1/2} \leqslant |U+V|^2.$$

Recalling the assumption that $U \sim V$, which implies by Ruzsa calculus that $|U+V| \approx| U| \approx| V|$, it follows thta $|U+S+V| \approx| U| \approx| V| \approx| S|$. It follows by Ruzsa calculus that $U+V \sim S$ as claimed. □

COROLLARY 2.1 (Iterated sumset inequality). *Suppose that $\sigma[A] \leqslant K$ and that l, k are nonnegative integers, not both zero. Then there is some constant $\gamma(k,l)$ such that $|kA-lA| \ll K^{\gamma(k,l)}|A|$.*

By much more involved arguments of a rather graph-theoretical nature it is possible to establish the *Plünnecke-Ruzsa* inequalities, which furnish the bound $|kA-lA| \leqslant K^{k+l}|A|$ in this corollary. For details the original paper [**?**] of Ruzsa may be consulted.