Will Rosenbaum Sumsets

Department of Mathematics
University of California, Los Angeles

Additive Combinatorics
October 19, 2011

In this essay, we consider finite subsets of some abelian group G. We call such sets ***additive sets***. We define the sum of two sets $U, V \subset G$ to be

$$U + V = \{u + v \,|\, u \in U,\ v \in V\}.$$

Similarly, we define

$$U - V = \{u - v \,|\, u \in U,\ v \in V\}$$

and

$$kU - \ell V = \{u_1 + \cdots + u_k - v_1 - \cdots - v_\ell \,|\, u_i \in U,\ v_j \in V\}.$$

We are most interested in how large or small these sets can be. In this vein, we have the following definitions.

Definition. Let U be an additive set. Define the ***doubling constant*** of U to be

$$\sigma[U] = \frac{|U+U|}{|U|}.$$

Similarly, for additive sets A and B, we define

$$\sigma[U,V] = \frac{|U+V|}{|U|^{1/2}\,|V|^{1/2}}.$$

Definition. Let U and V be additive sets. Then the ***Ruzsa distance*** between U and V is

$$d(U,V) = \log \frac{|U-V|}{|U|^{1/2}\,|V|^{1/2}}.$$

On occasion, we may also use the notation

$$\delta[U] = \frac{|U-U|}{|U|} \quad \text{and} \quad \delta[U,V] = \frac{|U-V|}{|U|^{1/2}\,|V|^{1/2}}$$

where $\delta[U]$ is the ***difference constant*** of U.

The main goal of this note is to prove the following three inequalities — the so-called Ruzsa inequalities. Throughout we assume that U, V and W are additive sets in some ambient abelian group G:

I. $d(U,W) \leq d(U,V) + d(V,W)$

II. $d(U,-V) \leq 3d(U,V)$

III. If $d(U,V), d(U,W), d(V,W) \leq \log K$, then $|U+V+W| \leq K^C\,|U|^{1/3}\,|V|^{1/3}\,|W|^{1/3}$ for some absolute constant $C \geq 1$.

1 Basic estimates

We begin with a warm-up. The Rusza distance d between two sets is not a metric. Inequality I shows that d satisfies the triangle inequality and the fact that $|U-V| = |V-U|$ shows that d is symmetric. However, $d(U,U)$ is rarely zero. Under what circumstances is $d(U,U) = 0$?

If U is a coset of a (finite) subgroup of G, say $U = a + H$ for some $H < G$, then $d(U,U) = 0$. Indeed, under this condition,

$$|U-U| = |(a+H)-(a+H)| = |\{h-h' \,|\, h \in H\}| = |H|\,,$$

whence $d(U,U) = 0$. Conversely, suppose $d(U,U) = 0$. Since $|(U-\{a\})-(U-\{a\})| = |U-U|$ for any $a \in G$, we may assume without loss of generality that $0 \in U$. Therefore, $U \subset U-U$. Suppose U is not a subgroup of G. Then U is not closed under subtraction; i.e., there exists $u, v \in U$ such that $u - v \notin U$. Thus $U \subsetneq U-U$ so that $|U| < |U-U|$. Therefore, $d(U,U) \neq 0$. Thus we have established the following fact:

Fact. An additive subset U satisfies $d(U,U) = 0$ if and only if U is a coset of a subgroup of G.

There are some trivial bounds for σ and δ:

1. $1 \leq \sigma[U] \leq \frac{1}{2}(|U|+1)$

2. $1 \leq \delta[U] \leq |U| - 1 + 1/|U|$.

In both cases, the lower bounds are achieved by cosets of subgroups (i.e., arithmetic progressions) while the upper bounds are achieved by, for example, geometric progressions in $\mathbb{Z}$. Sets satisfying $\delta[U] = |U| - 1 + 1/|U|$ are known as ***Sidon sets***. Note that U is a Sidon set if and only if $u - v = u' - v'$ has no nontrivial solutions for $u, v, u', v' \in U$.

Although upper bounds in both 1 and 2 are achieved by geometric progressions, there are families of subsets of $\mathbb{Z}$ which are asymptotically equal to the upper bound in 1 but not 2 and vice versa. In particular, Rusza proved[1] (using a probabilistic argument) that for all sufficiently large n, there exist sets A and B with $|A|, |B| = n$ satisfying

$$|A+A| \leq n^{2-c} \quad \text{but} \quad |A-A| \geq n^2 - n^{2-c}$$

and

$$|B-B| \leq n^{2-c} \quad \text{but} \quad |B+B| \geq \frac{1}{2}n^2 - n^{2-c}$$

for some absolute constants $c > 0$.*

* In each expression c may denote a different absolute constant.

Now let us begin proving inequalities I – III.

Theorem. (*triangle inequality*) Suppose U, V and W are additive sets. Then

$$d(U,W) \leq d(U,V) + d(V,W).$$

[1] Rusza, I.Z. *Acta Math. Hung.* **59 (3-4)** (1992), 439-447.

Proof. Combining the logs in the definition of d on the right hand side and canceling the factors of $|U|^{1/2}$ and $|W|^{1/2}$, the triangle inequality is equivalent to

$$|U-W| \leq \frac{|U-V|\,|V-W|}{|V|}.$$

This inequality follows from the identity $u-w=(u-v)+(v-w)$ for $u\in U$, $v\in V$ and $w\in W$. Consider the map

$$\varphi : (U-V)\times(V-W)\to G \quad \text{given by} \quad \varphi(u-v,v'-w)=u-v+v'-w.$$

For each $u-w\in U-W$, $\left|\varphi^{-1}(u-w)\right|\geq |V|$ because $u-w$ has at least $|V|$ representatives in $(U-V)\times(V-W)$, viz. $(u-v,v-w)$ for each $v\in V$. This gives the desired inequality. □

Theorem. Let U and V be additive sets. Then

$$d(U,-V)\leq 3d(U,V).$$

Proof. First, notice that the theorem is equivalent to

$$|U+V|\leq \frac{|U-V|}{|U|\,|V|} \qquad (*)$$

so we we content ourselves to prove $(*)$. For each $x\in G$, define

$$s(x)=\left|\{(u,v)\in U\times V \,|\, u+v=x\}\right| \quad \text{and} \quad r(x)=\left|\{(u,v)\in U\times V \,|\, u-v=x\}\right|.$$

We will prove $(*)$ in two steps. First we will show that for some x, $s(x)\geq |U|\,|V|\,/\,|U-V|$. Then we will demonstrate that for such an x, $s(x)\,|U+V|\leq |U-V|^2$, whence the claim follows.

By double counting,

$$\sum_{x\in G} s(x)=\sum_{x\in G} r(x)=|U|\,|V|.$$

Further

$$\sum_{x\in G} s(x)^2=\sum_{x\in G} r(x)^2$$

as both are equal to the number elements $(u,u',v,v')\in U^2\times V^2$ with $u+v=u'+v'$.* Now we apply the Cauchy-Schwarz inequality to $\sum r(x)^2$. Recall that the Cauchy-Schwarz inequality states that

$$\left(\sum_x a_x b_x\right)^2\leq\left(\sum_x a_x^2\right)\left(\sum_x b_x^2\right).$$

Applying this with $a_x=r(x)$ and $b_x=1$ for $x\in U-V$ and 0 otherwise, we obtain

$$\begin{aligned}
|U|^2\,|V|^2 &= \Big(\sum r(x)\Big)^2 \\
&\leq \Big(\sum r(x)^2\Big)\left(\sum_{x\in U-V} 1\right) \\
&= |U-V|\sum r(x)^2 \\
&= |U-V|\sum s(x)^2.
\end{aligned}$$

* The number of quadruples (u,u',v,v') with $u+v=u'+v'$ is called the ***additive eneregy*** of U and V.

We can obtain the desired lower bound on the maximal $s(x)$ by

$$|U|^2 |V|^2 \leq |U-V| \sum s(x)^2 \leq |U-V| \left(\max_x s(x)\right) \sum s(x) = |U-V|\,|U|\,|V| \max_x s(x)$$

which gives the desired bound of

$$\max_x s(x) \geq \frac{|U|\,|V|}{|U-V|}.$$

Let $S = \{(u,v) \in U \times V \,|\, u+v = x\}$ where $|S| \geq |U|\,|V| \,/\, |U-V|$. We will show that

$$|S|\,|U+V| \leq |U-V|^2$$

by constructing an injective map $\psi : S \times (U+V) \to (U-V)^2$. To this end, for each $w \in U+V$, define $\alpha(w) \in U$ and $\beta(w) \in V$ with $\alpha(w)+\beta(w) = w$. Define ψ by

$$\psi(u,v,w) = (u-\beta(w), \alpha(w)-v) \qquad (u,v) \in S,\ w \in U+V.$$

To see that ψ is injective, suppose $\psi(u,v,w) = \psi(u',v',w')$. Then we have

$$u-\beta(w) = u'-\beta(w'), \qquad \alpha(w)-v = \alpha(w')-v', \quad \text{and} \quad u+v = u'+v'$$

where the last equation holds by the definition of S. Then

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

Since $w = w'$, it immediately follows that $u = u'$ and $v = v'$ as well, so the map ψ is injective as claimed. This gives the second inequality in

$$\frac{|U|\,|V|}{|U-V|}\,|U+V| \leq |S|\,|U+V| \leq |U-V|^2.$$

Multiplying the first and last terms by $|U-V|$ and dividing by $|U|^{3/2}\,|V|^{3/2}$ gives the theorem. □

2 Ruzsa calculus

We begin by introducing some new notation, referred to as ***rough notation***. Throughout, $K \geq 2$ is some parameter that measures the "roughness" of an approximation. Given quantities X and Y we write $X \lessapprox Y$ (read "X is roughly less than Y") to mean that $X \leq K^C Y$ where, as usual, C is some absolute constant. If $X \lessapprox Y$ and $Y \lessapprox X$, we write $X \approx Y$ and say that X is "roughly equal" to Y.

Notation. If U and V are additive sets, then we write $U \sim V$ if

$$\frac{|U-V|}{|U|^{1/2}\,|V|^{1/2}} \approx 1, \quad \text{or equivalently} \quad |U-V| \approx |U|^{1/2}\,|V|^{1/2}.$$

Notice that we do not necessarily have $U \sim U$. In fact, by II, $U \sim U$ if and only if $\sigma[U] \approx 1$.

Proposition. (*Ruzsa calculus*) Let U, V and W be additive sets. Then

(i) Suppose $U \sim V$. 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) If $U \sim V$, $\sigma[W] \approx 1$ and there exists x such that

$$|U \cap (x + W)| \approx |U| \approx |W|$$

then $U \sim V \sim W$.

(iv) If $\sigma[U], \sigma[W] \approx 1$ and there exists x with $|U \cap (x + W)| \approx |U| \approx |W|$, then $U \sim W$.

(v) If $U \sim V \sim W$, then $W \sim U + V$.

Proof. (i) Since $U \sim V$ we have

$$\frac{|U - V|}{|U|^{1/2} |V|^{1/2}} \leq K^C.$$

By II, we have

$$\frac{|U + V|}{|U|^{1/2} |V|^{1/2}} \leq \frac{|U - V|^3}{|U|^{3/2} |V|^{3/2}} \leq (K^C)^3 = K^{3C}$$

which proves the first equation.* Since

$$|U| \leq |U - V| \leq K^C |U|^{1/2} |V|^{1/2},$$

we have

$$|U|^{1/2} \leq K^C |V|^{1/2} \implies |U| \leq K^{2C} |V|$$

which $|U| \lessapprox |V|$. Symmetrically, we have $|V| \lessapprox |U|$ hence $|U| \approx |V|$. Finally, notice that the Ruzsa triangle inequality implies that

$$\frac{|U - U|}{U} \leq \frac{|U - V|}{|U|^{1/2} |V|^1 / 2} \cdot \frac{|V - U|}{|U|^{1/2} |V|^1 / 2} \leq K^{2C}$$

which gives the final expression.

(ii) This also follows from the triangle inequality, for

$$\frac{|U - W|}{|U|^{1/2} |W|^{1/2}} \leq \frac{|U - V|}{|U|^{1/2} |V|^{1/2}} \cdot \frac{|V - W|}{|V|^{1/2} |W|^{1/2}} \leq K^C \cdot K^{C'} = K^{C+C'}.$$

* Since all quantities in these expressions are greater than 1, we trivially have that each quantity is $\lessapprox 1$, with $C = 0$.

(iii) Without loss of generality, we may assume that $x = 0$ by replacing W with $x + W$, so we have $|U \cap W| \approx |U| \approx |W|$. Since $U \cap W \subset U, W$ Ruzsa's triangle inequality implies that

$$\frac{|U - W|}{|U|^{1/2}|W|^{1/2}} \leq \frac{|U - U \cap W|}{|U|^{1/2}|U \cap W|^{1/2}} \cdot \frac{|U \cap W - W|}{|U \cap W|^{1/2}|W|^{1/2}}$$

hence

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

By (i), $U \sim U$ implies that $|U - U| \approx |U|$. Similarly, $\sigma[W] \approx 1$ implies that $W \sim -W$, hence $W \sim W$ so we also have $|W - W| \sim |W|$. Since $|U \cap W| \approx |U| \approx |W|$ by hypothesis, we have

$$\begin{aligned} |U \cap W||U - W| \lessapprox |U||W| &\implies |U - W| \lessapprox |U|, |W| \\ &\implies |U - W| \approx |U|, |W| \\ &\implies \frac{|U - W|}{|U|^{1/2}|W|^{1/2}} \approx 1 \\ &\implies U \sim W. \end{aligned}$$

(iv) This is just a special case of (iii).

(v) The idea is to establish the following claim.

Claim. There is a set S with $S \sim U + V$.

Granting the claim for the moment, we can prove (v). By (i), we have $\sigma[U + V] \approx 1$. Further. $U \sim W$ implies that

$$\begin{aligned} \frac{|U - W|^2}{|U||W|} \approx 1 &\implies |U - W|^2 \approx |U||W| \\ &\implies |U - W|^2 \approx |U|^2, |W|^2 \qquad \text{(by (i))} \\ &\implies |U - W| \approx |U|, |W|. \end{aligned}$$

Write $r(x)$ for the number of pairs $(u, w) \in U \times W$ with $u - w = x$, and note that $r(x) = |U \cap (x + W)|$. Since

$$\sum_x r(x) = |U||W| \approx |U||U - W|,$$

there exists x with $r(x) \gtrapprox |U|$. Indeed, the sum on the left has $|U - W|$ nonzero elements, so the average element in the sum is $\approx |U|$. By replacing x with $x' = x + v$ for arbitrary $v \in V$, we get

$$|U| \lessapprox |(U + V) \cap (x' + W)| \leq |U + V| \approx |U|.$$

Since $\sigma[W], \sigma[U+V] \approx 1$, part (iv) implies that

$$|U+V| \approx |W| \approx |(U+V) \cap (x'+W)|$$

hence

$$U+V \sim W$$

as desired.

Proof of claim. Let

$$L = \frac{|U+V|}{|U|^{1/2}\,|V|^{1/2}}.$$

By II, we have $L \leq K^C$. The idea of the proof is to take S to be the set of "popular" sums in $U+V$. Define

$$s(x) = |\{(u,v) \in U \times V \,|\, u+v=x\}|$$

and take

$$S = \left\{ x \in U \times V \,\middle|\, s(x) \geq \frac{1}{2L}\,|U|^{1/2}\,|V|^{1/2} \right\}.$$

By the same application of the Cauchy-Schwarz inequality appearing in the proof of II, we have

$$\sum_x s(x)^2 \geq \frac{1}{L}\,|U|^{3/2}\,|V|^{3/2} = \frac{|U|^2\,,|V|^2}{|U+V|}.$$

The contribution of $x \notin S$ in this sum is at most

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

Hence

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

Since $s(x) \leq |U|\,,|V|$ for all x, it follows that

$$|S| \geq \frac{1}{2L}\,|U|^{1/2}\,|V|^{1/2} = \frac{1}{2}\frac{|U|\,|V|}{|U+V|} \approx |U|\,. \qquad (*)$$

Thus we have established that S is "large."

Suppose $u \in U$, $v \in V$ and $s \in S$. Then there exist at least $\frac{1}{2L}\,|U|^{1/2}\,|V|^1\,/2$ distinct pairs $(u',v') \in U \times V$ with $u'+v' = s$. Each pair gives distinct representations of $u+v+s = (u+v')+(u'+v)$ in $U+V+S$ as a sum of elements in $U+V$. Therefore,

$$|U+V+S| \cdot \frac{1}{2L}\,|U|^{1/2}\,|V|^{1/2} \leq |U+V|^2 \implies |U+V+S| \leq \frac{|U+V|^3}{|U|\,|V|} \approx |U| \approx |V|$$

because $U \sim V$ implies that $|U+V| \approx |U| \approx |V|$. The inequalities $|U|, |V| \leq |U+V+S|$ imply that $|U+V+S| \approx |U| \approx |V|$. Finally, combining $(*)$ with the inequality $|S| \leq |U+V+S|$ gives

$$|U+V+S| \approx |U+V| \approx |S|.$$

The claim follows from

$$|U+V+S|^2 \approx |U+V|\,|S|.$$

□

Corollary. (*Ruzsa triple sumset inequality*) Suppose U, V and W are additive sets with $d(U,V), d(U,W), d(V,W)$ $\log K$. Then

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

Proof. The hypothesis of the corollary implies that $U \sim V \sim W$. Hence by (v), $W \sim U+V$ and symmetrically $V \sim U+W$ and $U \sim V+W$. Therefore,

$$|U+V+W| \approx |U+V|^{1/2} |W|^{1/2} \approx |U|^{1/4} |V|^{1/4} |W|^{1/2}.$$

We also obtain analogous results for the different permutations of U, V and W. Multiplying these expressions together gives

$$|U+V+W|^3 \approx |U|\,|V|\,|W|$$

whence the corollary follows. □

Corollary. (*iterated sumset inequality*) Suppose $\sigma[U] \leq K$. Then for any non-negative integers k, ℓ not both zero, there exists a constant $\gamma(k,\ell)$ such that

$$|kA - \ell A| \ll K^{\gamma(k,\ell)} |A|$$

Remark. Under the hypotheses of the final corollary, the *Plünnecke-Ruzsa inequalities* give a bound of

$$|kA - \ell A| \leq K^{k+\ell} |A|$$

but deriving such a bound would take us too far afield.