Notes on the sum product theorem

Contents

1 The Plünnecke-Ruzsa sumset calculus

Definition 1. If A, B are finite subsets of a semigroup G, A nonempty, define the *magnification ratio* of A, B to be

$$\mu(A,B) = \min_{\emptyset \neq X \subseteq A} \frac{|XB|}{|X|}.$$

Note that if $\emptyset \neq X \subseteq A$ has $\frac{|XB|}{|B|} = \mu(A,B)$ then $\frac{|XB|}{|B|} = \mu(X,B)$.

Theorem 1 (Petridis)**.** *If X, B are finite subsets of a semigroup G, X nonempty satisfying $\frac{|XB|}{|X|} = \mu(X,B)$, then for all finite subsets C of G such that $|cX| = |X|$ for all $c \in C$, we have*

$$|CXB| \leq \frac{|CX||XB|}{|X|}.$$

Proof. Induct on $|C|$. If C is empty we are done, so suppose $C = C' \cup \{c\}$, $c \notin C'$. Letting $Y = \{x \in X \mid cx \in C'X\}$, we have

$$\begin{aligned} |CXB| &\leq |C'XB| + |c(XB \setminus YB)| \\ &\leq \frac{|C'X||XB|}{|X|} + |XB| - |YB| \\ &\leq \frac{(|CX| - |X| + |Y|)|XB|}{|X|} + |XB| - \mu(X,B)|Y| \\ &= \frac{|CX||XB|}{|X|}. \end{aligned}$$

□

Theorem 2 (Ruzsa triangle inequality). *If X, Y, Z are finite subsets of a group G, then $|X||YZ| \leq |YX^{-1}||XZ|$.*

Theorem 3 (Ruzsa covering lemma). *If A, B are finite subsets of a group G and A is nonempty, then there is a set $S \subseteq B$ with $|S| \leq \mu(A, B)$ and $B \subseteq A^{-1}AS$.*

Proof. Let $\emptyset \neq X \subseteq A$ be such that $\frac{|XB|}{|X|} = \mu(A, B)$. Take S to be a maximal subset of B such that Xs, Xs' are disjoint for every pair of distinct elements $s, s' \in S$. Then $|X||S| = |XS| \leq |XB|$ and $B \subseteq X^{-1}XS \subseteq A^{-1}AS$. □

Lemma 1 (Plünnecke tensor power trick). *If A, B are finite subsets of a semigroup G, A', B' are finite subsets of a semigroup G', and A, A' are nonempty, then*

$$\mu(A \times A', B \times B') = \mu(A, B)\mu(A', B').$$

Theorem 4 (Plünnecke-Ruzsa sumset inequality). *If $A, B_1, ..., B_h$ are finite subsets of an abelian semigroup G with A nonempty, such that for all $b \in (h-1)(B_1 \cup \cdots \cup B_h)$ we have $|A + b| = |A|$, then*

$$\mu(A, B_1 + \cdots + B_h) \leq \frac{|A + B_1|}{|A|} \cdots \frac{|A + B_h|}{|A|}.$$

In particular, if A is cancellative we have $|B_1 + \cdots + B_h| \leq \frac{|A+B_1|}{|A|} \cdots \frac{|A+B_h|}{|A|}|A|$.

Proof. Write $\alpha_i = \frac{|A+B_i|}{|A|}$. Choose a large integer n such that $\frac{n}{\alpha_i}$ is an integer for all i, and set $n_i = \frac{n}{\alpha_i}$. By adding copies of $\mathbb{N}$ to G, we can assume there exist $T_1, ..., T_h \subseteq G$ with $|T_i| = n_i$ such that all sums

$$y + t_1 + \cdots + t_h, \;\; y \in A + B_1 + \cdots + B_h, \;\; \forall 1 \leq i \leq h \;\; t_i \in T_i$$

are distinct. Set $B = \bigcup_i (B_i + T_i)$. We have

$$|A + B| \leq \sum_i |A + B_i||T_i| = \sum_i n_i \alpha_i |A|,$$

so $\mu(A, B) \leq \sum_i n_i \alpha_i = hn$. Let $\emptyset \neq X \subseteq A$ be such that $\frac{|X+B|}{|X|} = \mu(A, B)$. Applying Theorem 1 h times, we see that $|X + hB| \leq \mu(A, B)^h |X| \leq (hn)^h |X|$. Thus,

$$n_1 \cdots n_h |X + B_1 + \cdots + B_h| = |X + B_1 + \cdots + B_h + T_1 + \cdots + T_h| \leq |X + hB| \leq (hn)^h |X|,$$

so

$$\mu(A, B_1 + \cdots + B_h) \leq \frac{(hn)^h}{n_1 \cdots n_h} = h^h \alpha_1 \cdots \alpha_h.$$

Applying the tensor power trick (Lemma 1), we have

$$\mu(A, B_1 + \cdots + B_h)^k = \mu(\times^k A, \times^k B_1 + \cdots + \times^k B_h) \leq h^h \alpha_1^k \cdots \alpha_h^k,$$

and taking k to infinity finishes the proof. □

Proposition 1 (Bourgain). *Let $A_1, ..., A_h, B_1, ..., B_h, C_1, ..., C_h$ be finite subsets of an abelian group G such that for each i $A_i \cap C_i$ is nonempty. Then*

$$|B_1 + \cdots + B_h| \leq \frac{|B_1 + C_1|}{|A_1 \cap C_1|} \cdots \frac{|B_h + C_h|}{|A_h \cap C_h|} |A_1 + \cdots + A_h|.$$

1.1 Approximate variants

Lemma 2. *If A, B are finite subsets of an abelian group G, then there exist $x \in B - A, y \in A + B$ such that*

$$|B \cap (A + x)| \geq \frac{|A||B|}{|A + B|},$$
$$|B \cap (-A + y)| \geq \frac{|A||B|}{|A + B|}.$$

Proof. By Cauchy-Schwarz, we have

$$\#\{(a, b, a', b') \in A \times B \times A \times B \mid a + b = a' + b'\} \geq \frac{|A|^2|B|^2}{|A + B|}.$$

By the pigeonhole principle we can find an x of the form $b - a'$ and a y of the form $a + b$ with the required properties. □

Theorem 5 (Approximate covering lemma)**.** *If A, B are finite subsets of an abelian group G with A nonempty, then for any $m \geq 1$ there are sets $S_+ \subseteq B - A$, $S_- \subseteq A + B$ such that*

$$|B \cap (A + S_+)| \geq (1 - 1/m)|B|,$$
$$|B \cap (-A + S_-)| \geq (1 - 1/m)|B|,$$

and

$$|S_+|, |S_-| < \log(m)\mu(A, B) + 1.$$

Proof. Assume WLOG that $\mu(A, B) = \frac{|A+B|}{|A|}$. Iteratively apply Lemma 2 and use the inequality $-\log(1 - \frac{|A|}{|A+B|}) \geq \frac{|A|}{|A+B|}$. □

Theorem 6 (Approximate Plünnecke-Ruzsa)**.** *If $A, B_1, ..., B_h$ are finite subsets of an abelian semigroup G with A nonempty, such that for all $b \in (h-1)(B_1 \cup \cdots \cup B_h)$ we have $|A + b| = |A|$, then for any $m \geq 1$ there is a set $X \subseteq A$ with*

$$|X| > (1 - 1/m)|A|$$

and

$$|X + B_1 + \cdots + B_h| \leq \frac{hm^{h-1} - 1}{h - 1} \frac{|A + B_1|}{|A|} \cdots \frac{|A + B_h|}{|A|}|X|.$$

Proof. We'll show that in fact we can find such X with

$$|X + B_1 + \cdots + B_h| \leq \left(m^h|X| - \left(m^h - \frac{hm^{h-1} - 1}{h - 1}\right)|A|\right) \frac{|A + B_1|}{|A|} \cdots \frac{|A + B_h|}{|A|}.$$

Suppose for contradiction that there is some $m \geq 1$ for which we can not find such an X. Let n be the infimum of all such m. Since A only has finitely many subsets, we can find a set $\emptyset \neq Y \subseteq A$ with $|Y| \geq (1 - 1/n)|A|$ and

$$|Y + B_1 + \cdots + B_h| \leq \left(n^h|Y| - \left(n^h - \frac{hn^{h-1} - 1}{h - 1}\right)|A|\right) \frac{|A + B_1|}{|A|} \cdots \frac{|A + B_h|}{|A|}.$$

Note that if $|Y| > (1-1/n)|A|$ then the derivative of the right hand side of the above with respect to n is positive, so by the definition of n we must have $|Y| = (1-1/n)|A|$ for any set Y as above.

By the Plünnecke-Ruzsa inequality (Theorem 4), we have

$$\mu(A \setminus Y, B_1 + \cdots + B_h) \le \frac{|A+B_1|}{|A \setminus Y|} \cdots \frac{|A+B_h|}{|A \setminus Y|} \le n^h \frac{|A+B_1|}{|A|} \cdots \frac{|A+B_h|}{|A|},$$

so there is some $\emptyset \ne X' \subseteq A \setminus Y$ such that

$$|X' + B_1 + \cdots + B_h| \le n^h \frac{|A+B_1|}{|A|} \cdots \frac{|A+B_h|}{|A|} |X'|.$$

Taking $Y' = Y \cup X'$, we have

$$\begin{aligned} |Y' + B_1 + \cdots + B_h| &\le |Y + B_1 + \cdots + B_h| + |X' + B_1 + \cdots + B_h| \\ &\le \left(n^h|Y| + n^h|X'| - \left(n^h - \frac{hn^{h-1} - 1}{h-1} \right) |A| \right) \frac{|A+B_1|}{|A|} \cdots \frac{|A+B_h|}{|A|} \\ &= \left(n^h|Y'| - \left(n^h - \frac{hn^{h-1} - 1}{h-1} \right) |A| \right) \frac{|A+B_1|}{|A|} \cdots \frac{|A+B_h|}{|A|}, \end{aligned}$$

but $|Y'| > (1-1/n)|A|$, a contradiction. □

Theorem 7 (Ruzsa)**.** *If A, B, C are finite subsets of a semigroup G with A nonempty, such that for any $b \in B, c \in C$ we have $|cA| = |Ab| = |A|$, then for any $m \ge 1$ there is a set $X \subseteq A$ with*

$$|X| > (1 - 1/m)|A|$$

and

$$|CXB| \le (2m-1)\frac{|CA|}{|A|}\frac{|AB|}{|A|}|X|.$$

Proof. Since left multiplication by C commutes with right multiplication by B, we can make an auxiliary abelian semigroup G' out of disjoint copies of $A, B, C, CA, AB, B \times C, CAB, \{0\}$ in an obvious way. Now apply Theorem 6 to G'. □

1.2 Energy

Definition 2. If A, B are finite subsets of a semigroup, define their *energy* to be

$$E(A, B) = \#\{(a, b, c, d) \in A \times B \times A \times B \mid ab = cd\}.$$

When $A = B$, we abbreviate this by $E(A)$.

Proposition 2 (Cauchy-Schwarz)**.** *If A, B are finite nonempty subsets of a semigroup, then*

$$E(A, B) \ge \frac{|A|^2|B|^2}{|AB|}.$$

Definition 3. If A, B are finite subsets of an abelian group G and $x \in G$, set

$$(A * B)(x) = \#\{(a, b) \in A \times B \mid a + b = x\},$$
$$(A \circ B)(x) = \#\{(a, b) \in A \times B \mid b - a = x\}.$$

Lemma 3 (Sanders, Schoen)**.** *If A is a finite nonempty subset of an abelian group, $0 \le \alpha < 1$, and $c \ge 0$, then there is a set $X \subseteq A$ with $|X| > \alpha \frac{E(A)}{|A|^2}$ and*

$$\#\left\{(x,y) \in X \times X \mid (A \circ A)(x-y) > c\frac{E(A)}{|A|^2}\right\} \ge \left(1 - \frac{c}{1-\alpha}\right)|X|^2.$$

Proof. We will choose $X = A \cap (A+d)$ for some $d \in A - A$. We have

$$\sum_{(A \circ A)(d) \le \alpha \frac{E(A)}{|A|^2}} (A \circ A)(d)^2 \le \alpha \frac{E(A)}{|A|^2} \sum_d (A \circ A)(d) = \alpha E(A),$$

so

$$\sum_{(A \circ A)(d) > \alpha \frac{E(A)}{|A|^2}} (A \circ A)(d)^2 \ge (1-\alpha)E(A).$$

Setting

$$S = \left\{(a,b) \in A \times A \mid (A \circ A)(a-b) \le c\frac{E(A)}{|A|^2}\right\},$$

we have

$$\sum_d \#\{(a,b) \in S \mid a,b \in A+d\} = \sum_{(a,b)\in S} (A \circ A)(a-b) \le c\frac{E(A)}{|A|^2}|S| \le cE(A).$$

Thus

$$\sum_{(A \circ A)(d) > \alpha \frac{E(A)}{|A|^2}} (1-\alpha)\#\{(a,b) \in S \mid a,b \in A+d\} - c(A \circ A)(d)^2 \le 0,$$

so there must be some d with $(A \circ A)(d) > \alpha \frac{E(A)}{|A|^2}$ and

$$(1-\alpha)\#\{(a,b) \in S \mid a,b \in A+d\} - c(A \circ A)(d)^2 \le 0.$$

Taking $X = A \cap (A+d)$ for this d, we have $|X| = (A \circ A)(d)$ and

$$\#\left\{(x,y) \in X \times X \mid (A \circ A)(x-y) > c\frac{E(A)}{|A|^2}\right\} = |X|^2 - \#\{(a,b) \in S \mid a,b \in A+d\}.$$

□

Theorem 8 (Balog, Gowers, Schoen, Szemerédi)**.** *If A is a finite nonempty subset of an abelian group, then there is a set $A' \subseteq A$ with $|A'| > \frac{E(A)}{6|A|^2}$ and*

$$|A' - A'| < 486\frac{|A|^{10}}{E(A)^3}.$$

Proof. Take $\alpha = \frac{1}{2}, c = \frac{1}{9}$ in Lemma 3 to find a set $X \subseteq A$ with $|X| > \frac{E(A)}{2|A|^2}$ and

$$\#\left\{(x,y) \in X \times X \mid (A \circ A)(x-y) > \frac{E(A)}{9|A|^2}\right\} \ge \frac{7}{9}|X|^2.$$

Make a graph $\mathcal{H}$ with vertex set X, having an edge between x and y exactly when $(A \circ A)(x - y) > \frac{E(A)}{9|A|^2}$. Letting A' be the set of vertices in $\mathcal{H}$ having degree greater than $\frac{2}{3}|X|$, we see that $|A'| \geq \frac{|X|}{3} > \frac{E(A)}{6|A|^2}$. For any $a, b \in A'$, we can find more than $\frac{1}{3}|X|$ vertices $x \in X$ connected to both a, b in $\mathcal{H}$, and for each such x we can write

$$a - b = (a - x) - (b - x),$$

and we can write the right hand side in the form $(a_1 - a_2) - (a_3 - a_4)$ with $a_1, a_2, a_3, a_4 \in A$, $a_1 - a_2 = a - x$, in at least $\frac{E(A)^2}{81|A|^4}$ different ways. Thus we have

$$|A' - A'| \cdot \frac{1}{3}|X| \cdot \frac{E(A)^2}{81|A|^4} < |A|^4,$$

so

$$|A' - A'| < 486 \frac{|A|^{10}}{E(A)^3}.$$

□

2 The sum-product theorem

2.1 Characteristic Zero

Definition 4. For any distinct points $a, b \in \mathbb{R}^n$, set

$$D(a, b) = \left\{ p \in \mathbb{R}^n \mid \angle pab \leq \frac{\pi}{6}, \angle pba \leq \frac{\pi}{6} \right\}.$$

Lemma 4. *For any four points $a, b, c, d \in \mathbb{R}^n$ with $a \neq b, c \neq d, \{a, b\} \neq \{c, d\}$, if all of the inequalities*

$$|ab| \leq |bc|, \quad |ab| \leq |bd|, \quad |cd| \leq |ad|, \quad |cd| \leq |bd|$$

hold then the interiors of $D(a, b)$ and $D(c, d)$ do not intersect.

Proof. If $|ab| + |cd| \leq |bd|$, then since $D(a, b)$ is contained in the sphere of radius $|ab|$ around b and $D(c, d)$ is contained in the sphere of radius $|cd|$ around d, their interiors can't intersect. Otherwise, we can find a point $x \in \mathbb{R}^n$ such that $|bx| = |ab|, |dx| = |cd|$. Since $|ab|, |cd|$ are assumed to be at most $|bd|$, bd is the longest edge of triangle bdx, so we must have $\angle bxd \geq \frac{\pi}{3}$. Thus we can find some point m on the line segment bd with $\angle mxb \geq \frac{\pi}{6}$ and $\angle mxd \geq \frac{\pi}{6}$. Since a is outside the sphere of radius $|cd| = |dx|$ centered at d, we have $\angle abm \geq \angle xbm$, and similarly $\angle cdm \geq \angle xdm$. Thus, if we rotate the ray mx around the line bd we get a cone which separates the interior of $D(a, b)$ from the interior of $D(c, d)$. □

Corollary 1 (Gilbert, Pollak)**.** *Let P be a finite set of points in $\mathbb{R}^n$, and let T be a minimum spanning tree on P. For any distinct edges $\{a, b\}, \{c, d\}$ of T, the interiors of $D(a, b)$ and $D(c, d)$ do not intersect.*

Proof. Since T is a tree, there is a unique path in T connecting the edge $\{a, b\}$ to the edge $\{c, d\}$. We may assume without loss of generality that this path connects a to c without passing through b or d. Then if we replace edge $\{a, b\}$ with either $\{b, c\}$ or $\{b, d\}$ we again get a spanning tree, so by minimality we must have $|ab| \leq |bc|, |bd|$. Similarly we have $|cd| \leq |ad|, |bd|$. Now apply Lemma 4. □

Proposition 3. *Suppose $a, b, c, d \in \mathbb{H}^\times$ are nonzero quaternions with $\angle b0d \le \frac{\pi}{6}$. Then $(a+c)(b+d)^{-1}$ is in the interior of $D(ab^{-1}, cd^{-1})$.*

Proof. Writing $b = md$, we have

$$(a+c)(b+d)^{-1} = (a+c)d^{-1}(m+1)^{-1} = ab^{-1} + (cd^{-1} - ab^{-1})(m+1)^{-1},$$

so it's enough to check that if $\angle m01 \le \frac{\pi}{6}$ then $(m+1)^{-1}$ is in the interior of $D(0,1)$. Since $\angle(m+1)10 \ge \frac{5\pi}{6}$, we have $\angle 1(m+1)^{-1}0 \ge \frac{5\pi}{6}$, so $(m+1)^{-1}$ is in the interior of $D(0,1)$ by the fact that the angles of a triangle sum to π. □

Theorem 9 (Konyagin, Rudnev, Solymosi)**.** *Suppose $A \subseteq \mathbb{H}^\times$ is a finite set of nonzero quaternions such that for any $a, b \in A$ we have $\angle a0b \le \frac{\pi}{6}$. Then*

$$|A+A|^2|AA| \ge \frac{|A|^4 - |A||AA|}{\log\frac{|AA|^2}{|A|} + \gamma},$$

where γ is the Euler-Mascheroni constant.

Proof. By Cauchy-Schwarz, we have

$$\#\{(a,b,c,d) \in A \times A \times A \times A \mid ab = cd\} \ge \frac{|A|^4}{|AA|}.$$

Write $m(x) = \#\{(a,c) \in A \times A \mid c^{-1}a = x\}$, $n(x) = \#\{(b,d) \in A \times A \mid db^{-1} = x\}$. By Cauchy-Schwarz again, we have

$$\sum_x m(x)^2 \sum_y n(y)^2 \ge \Big(\sum_x m(x)n(x)\Big)^2 \ge \frac{|A|^8}{|AA|^2}.$$

Thus we may assume without loss of generality that

$$\sum_x n(x)^2 \ge \frac{|A|^4}{|AA|},$$

since otherwise we may replace A by $\bar{A}$. Choose a numbering $x_1, ..., x_{|AA^{-1}|}$ of the elements of AA^{-1} such that $n(x_1) \ge n(x_2) \ge \cdots$. Choose $1 \le k \le |AA^{-1}|$ such that $(k-1)n(x_k)^2$ is maximized. Then by choice of k we have

$$\frac{|A|^4}{|AA|} \le \sum_{i=1}^{|AA^{-1}|} n(x_i)^2 \le |A| + (k-1)n(x_k)^2 \sum_{i=2}^{|AA^{-1}|} \frac{1}{i-1},$$

so

$$(k-1)n(x_k)^2 \ge \frac{|A|^4 - |A||AA|}{H_{|AA^{-1}|-1}|AA|},$$

where $H_n = \sum_{i=1}^n \frac{1}{i}$ denotes the nth harmonic number. Note that by the Ruzsa triangle inequality 2 we have $|AA^{-1}| \le \frac{|AA|^2}{|A|}$, so

$$H_{|AA^{-1}|-1} \le \log\frac{|AA|^2}{|A|} + \gamma.$$

Let T be a minimum spanning tree on $\{x_1, ..., x_k\}$. For any edge $\{x_i, x_j\}$ in T, if $a, b, c, d \in A$ have $ab^{-1} = x_i$ and $cd^{-1} = x_j$, then by Proposition 3 the ratio $(a+c)(b+d)^{-1}$ will be in the interior of $D(ab^{-1}, cd^{-1})$. Thus by Corollary 1 we have an injection

$$\{(\{x_i, x_j\}, a, b, c, d) \in T \times A \times A \times A \times A \mid ab^{-1} = x_i, cd^{-1} = x_j\} \hookrightarrow (A+A) \times (A+A),$$

taking $(\{x_i, x_j\}, a, b, c, d)$ to $(a+c, b+d)$. Since T has $k-1$ edges and $n(x_i) \geq n(x_k)$ for $1 \leq i \leq k$, we have

$$|A+A|^2 \geq (k-1)n(x_k)^2 \geq \frac{|A|^4 - |A||AA|}{H_{|AA^{-1}|-1}|AA|}. \qquad \square$$

2.2 Finite fields

Lemma 5. *If $A, B \subseteq \mathbb{F}_q$, $G \subseteq \mathbb{F}_q^\times$, then there is some $\xi \in G$ with*

$$|A + \xi B| \geq \frac{|A||B||G|}{|A||B| + |G|}.$$

Proof. Define a function $f : G \mapsto \mathbb{N}$ by

$$f(\xi) = \#\{(a, b, a', b') \in A \times B \times A \times B \mid a + \xi b = a' + \xi b'\}.$$

We have

$$\sum_{\xi \in G} f(\xi) \leq |A|^2|B|^2 + |A||B||G|,$$

so there must be some $\xi \in G$ with $f(\xi) \leq \frac{|A|^2|B|^2}{|G|} + |A||B|$. By Cauchy-Schwarz, we have

$$|A + \xi B| \geq \frac{|A|^2|B|^2}{f(\xi)} \geq \frac{|A||B||G|}{|A||B| + |G|}. \qquad \square$$

Theorem 10 (Bourgain, Garaev, Katz, Li, Shen, ...)**.** *If p is prime and $A \subseteq \mathbb{F}_p$ then*

$$|A+A|^9|AA|^4 \geq \frac{|A|^{14}}{256} \min\left(1, \frac{p}{|A|^2}\right),$$
$$|A+A|^8|AA|^4 \geq \frac{|A|^{13}}{2^{23}} \min\left(1, \frac{3^7 p}{|A|^2}\right).$$

Proof. We'll prove the second bound (for the first bound, take $X = A$ and $Z = W = Y$ instead of using the approximate variations on the sumset calculus). By the approximate Plünnecke-Ruzsa theorem (Theorem 6), we can find $X \subseteq A$ with $|X| \geq \frac{3}{4}|A|$ and

$$|X + A + A + A| \leq 24\frac{|A+A|^3}{|A|^3}|X|.$$

By the Cauchy-Schwarz inequality, we have

$$\sum_{x \in X, a \in A} |xA \cap Xa| \geq \frac{|X|^2|A|^2}{|XA|},$$

so by the pigeonhole principle there is some $a_0 \in A$ with

$$\sum_{x \in X} |xA \cap Xa_0| \geq \frac{|X|^2|A|}{|XA|}.$$

Let $X = \{x_1, ..., x_{|X|}\}$, set $n_i = |x_i A \cap Xa_0|$, and suppose WLOG that $n_1 \geq \cdots \geq n_{|X|}$. Choose k maximizing the quantity $k^{3/4} n_k$, set $Y = \{x_1, ..., x_k\}$, and set $N = n_k$. We have

$$\frac{|X|^2|A|}{|XA|} \leq \sum_{i=1}^{|X|} n_i \leq \sum_{i=1}^{|X|} i^{-3/4} k^{3/4} n_k < 4|X|^{1/4}|Y|^{3/4}N,$$

so

$$|Y|^3 N^4 \geq \frac{|X|^7|A|^4}{256|XA|^4}.$$

For any $y \in Y$ we have $|yA \cap Xa_0| \geq N$, so by Ruzsa's triangle inequality (Theorem 2) we have

$$|yA - Xa_0| \leq \frac{|yA + yA \cap Xa_0||yA \cap Xa_0 + Xa_0|}{|yA \cap Xa_0|} \leq \frac{|y(A+A)||(X+X)a_0|}{N} \leq \frac{|A+A|^2}{N},$$

and similarly by Plünnecke-Ruzsa (Theorem 4) we have

$$|yA + Xa_0| \leq \frac{|yA \cap Xa_0 + yA||yA \cap Xa_0 + Xa_0|}{|yA \cap Xa_0|} \leq \frac{|A+A|^2}{N}.$$

There are now two cases.

Case 1: If $\frac{Y-Y}{(Y-Y)\setminus\{0\}} = \mathbb{F}_p$, then by Lemma 5 we can find $\xi \in \mathbb{F}_p^\times$ such that $|A + \xi A| \geq \frac{1}{2}\min(|A|^2, p)$. Write $\xi = \frac{c-d}{a-b}$ with $a, b, c, d \in Y$. By Plünnecke-Ruzsa, we have

$$|(a-b)A + (c-d)A| \leq |aA - bA + cA - dA| \leq \frac{|Xa_0 + aA||Xa_0 - bA||Xa_0 + cA||Xa_0 - dA|}{|Xa_0|^3},$$

so

$$|A+A|^8 \geq \frac{|A|^2|X|^3N^4}{2}\min\left(1, \frac{p}{|A|^2}\right).$$

Since $|X|^3N^4 \geq |Y|^3N^4 \geq \frac{|X|^7|A|^4}{256|AA|^4}$ and $|X| \geq \frac{3}{4}|A|$, we have

$$\begin{aligned} |A+A|^8|AA|^4 &\geq \frac{|X|^7|A|^6}{2^9}\min\left(1, \frac{p}{|A|^2}\right) \\ &\geq \frac{3^7|A|^{13}}{2^{23}}\min\left(1, \frac{p}{|A|^2}\right). \end{aligned}$$

Case 2: If $\frac{Y-Y}{(Y-Y)\setminus\{0\}} \neq \mathbb{F}_p$, then we can find $\xi \in \left(\frac{Y-Y}{(Y-Y)\setminus\{0\}} + 1\right) \setminus \frac{Y-Y}{(Y-Y)\setminus\{0\}}$. Writing $\xi = \frac{c-d}{a-b} + 1$ with $a, b, c, d \in Y$, we see that for any $Z, W \subseteq Y$ have

$$|Z||W| = |Z + \xi W| \leq |(a-b)Z + (a-b)W + (c-d)W|.$$

In particular, if $\emptyset \neq Z' \subseteq Z$ is chosen such that $\mu((a-b)Z, (a-b)W+(c-d)W) = \frac{|(a-b)Z'+(a-b)W+(c-d)W|}{|Z'|}$, then by Plünnecke-Ruzsa we have

$$|Z'||W| \leq |(a-b)Z' + (a-b)W + (c-d)W| \leq \frac{|Z+W|}{|Z|}\frac{|(a-b)Z+(c-d)W|}{|Z|}|Z'|,$$

so

$$|Z|^2|W| \leq |A+A||(a-b)Z+(c-d)W|.$$

Applying the approximate covering lemma (Lemma 5) to $aA \cap Xa_0$, aY, we find a set S with $|S| < 3\frac{|A+A|}{N}$ such that

$$|aY \cap (Xa_0 + aS)| \geq \frac{6}{7}|Y|.$$

Let $Y' = Y \cap (a^{-1}Xa_0 + S)$. Applying it again, we find a set S' with $|S'| < 3\frac{|A+A|}{N}$ such that

$$bY' \cap (-Xa_0 + bS') \geq \frac{6}{7}|Y'|,$$

and let $Z = Y' \cap (-b^{-1}Xa_0 + S)$. Similarly, find sets $W \subseteq Y, S'', S'''$ such that $|W| \geq \frac{6^2}{7^2}|Y|$, $cW \subseteq Xa_0 + cS'', dW \subseteq -Xa_0 + dS'''$, $|S''|, |S'''| \leq 3\frac{|A+A|}{N}$. We have

$$\begin{aligned}|(a-b)Z+(c-d)W| &\leq |aZ - bZ + cW - dW| \\ &\leq |S||S'||S''||S'''||Xa_0 + Xa_0 + Xa_0 + Xa_0| \\ &\leq 3^4\frac{|A+A|^4}{N^4} \cdot 24\frac{|A+A|^3}{|A|^3}|X|,\end{aligned}$$

so

$$|X||A+A|^8 \geq \frac{24|A|^3|Y|^3N^4}{7^6}.$$

By the inequalities $|X| \geq \frac{3}{4}|A|$ and $|Y|^3N^4 \geq \frac{|X|^7|A|^4}{256|AA|^4}$ we have

$$\begin{aligned}|A+A|^8|AA|^4 &\geq \frac{3|X|^6|A|^7}{2^5 \cdot 7^6} \\ &\geq \frac{3^7|A|^{13}}{2^{17} \cdot 7^6} \\ &\geq \frac{|A|^{13}}{2^{23}}.\end{aligned}$$

□

Theorem 11 (Garaev)**.** *Let q be a prime power. If $A, B \subseteq \mathbb{F}_q$, $C \subseteq \mathbb{F}_q^\times$, then*

$$|A+B||AC| \geq \min\left(\frac{|A|q}{2}, \frac{|A|^2|B||C|}{4q}\right).$$

Proof. Let

$$J = \{(x,b,c,y) \in (A+B) \times B \times C \times AC \mid x = b + yc^{-1}\}.$$

We have an injection $A \times B \times C \hookrightarrow J$ given by $(a, b, c) \mapsto (a + b, b, c, ac)$, so $|J| \geq |A||B||C|$. Let $\phi_0, ..., \phi_{q-1}$ be the additive characters of $\mathbb{F}_q$, ϕ_0 the trivial character. We have

$$\begin{aligned} |J| &= \frac{1}{q}\sum_{n=0}^{q-1}\sum_{x\in A+B}\sum_{b\in B}\sum_{c\in C}\sum_{y\in AC}\phi_n(b - x + yc^{-1}) \\ &\leq \frac{|A+B||B||C||AC|}{q} + \frac{1}{q}\sum_{n=1}^{q-1}\left|\sum_{x\in A+B}\phi_n(x)\right|\left|\sum_{b\in B}\phi_n(b)\right|\sum_{c\in C}\left|\sum_{y\in AC}\phi_n(yc^{-1})\right|. \end{aligned}$$

By Cauchy-Schwarz, for $n \neq 0$ we have

$$\begin{aligned} \left(\sum_{c\in C}\left|\sum_{y\in AC}\phi_n(yc^{-1})\right|\right)^2 &\leq |C|\sum_{d\in\mathbb{F}_q}\left|\sum_{y\in AC}\phi_n(dy)\right|^2 \\ &= q|C||AC|, \end{aligned}$$

and applying Cauchy-Schwarz one more time we have

$$\begin{aligned} \frac{1}{q}\sum_{n=1}^{q-1}\left|\sum_{x\in A+B}\phi_n(x)\right|\left|\sum_{b\in B}\phi_n(b)\right|\sum_{c\in C}\left|\sum_{y\in AC}\phi_n(yc^{-1})\right| &\leq \frac{\sqrt{q|C||AC|}}{q}\sum_{n=1}^{q-1}\left|\sum_{x\in A+B}\phi_n(x)\right|\left|\sum_{b\in B}\phi_n(b)\right| \\ &\leq \sqrt{q|A+B||B||C||AC|}. \end{aligned}$$

Thus

$$|A||B||C| \leq \frac{|A+B||B||C||AC|}{q} + \sqrt{q|A+B||B||C||AC|}. \qquad \square$$

A much better sum-product bound was recently obtained by Rudnev, using a three-dimensional variant of the Szemerédi-Trotter theorem due to Kollár. The proof is sketched below.

Lemma 6 (Kollár). *Let $\mathcal{L}$ be a set of m distinct lines in $\mathbb{P}^3$.*

1) *There exists a surface S of degree at most $\sqrt{6m} - 2$ which contains $\mathcal{L}$.*
2) *For any irreducible surface U of degree $g \leq \sqrt{6m}$ there exists a surface T of degree at most $\frac{6m}{g}$ which contains $\mathcal{L}$ and does not contain U.*

Proposition 4 (Kollár). *For $i = 1, ..., n-1$ let H_i be a hypersurface in $\mathbb{P}^n$ of degree a_i, and suppose their intersection $B = H_1 \cap \cdots \cap H_{n-1}$ is 1-dimensional. Let $C \subseteq B$ be a reduced subcurve. Then the arithmetic genus of C satisfies*

$$p_a(C) \leq p_a(B) = 1 + \frac{1}{2}\left(\sum_i a_i - n - 1\right)\prod_i a_i.$$

Proof. By induction on n together with the Kodaira vanishing theorem for $\mathbb{P}^n$, one can show that $h^0(B, \mathcal{O}_B) = 1$, so $p_a(B) = h^1(B, \mathcal{O}_B) - h^0(B, \mathcal{O}_B) + 1 = h^1(B, \mathcal{O}_B)$. If J is the ideal sheaf of C on B, we have

$$0 \to J \to \mathcal{O}_B \to \mathcal{O}_C \to 0,$$

so by the long exact sequence of cohomology we have

$$H^1(B, \mathcal{O}_B) \to H^1(C, \mathcal{O}_C) \to H^2(B, J),$$

and $H^2(B, J) = 0$ since B is 1-dimensional. Thus

$$p_a(C) = h^1(C, \mathcal{O}_C) - h^0(C, \mathcal{O}_C) + 1 \leq h^1(B, \mathcal{O}_B) = p_a(B).$$

The formula for $p_a(B)$ follows by directly computing the Hilbert polynomial of B. □

Proposition 5 (Kollár). *Let $S, T \subseteq \mathbb{P}^3$ be surfaces of degrees a, b with no common components, and let C be a reduced curve contained in $S \cap T$. For a point $p \in C$ let $r(p)$ be the multiplicity of C at p.*

1) C has at most ab components.

2) $\sum_{p \in C} r(p) - 1 \leq \frac{ab}{2}(a + b - 2)$.

Following Rudnev, we give a concrete description of Plücker coordinates for lines in $\mathbb{P}^3$.

Definition 5. For a line L in $\mathbb{P}^3$ containing points $[q_0 : q_1 : q_2 : q_3], [u_0 : u_1 : u_2 : u_3]$, set

$$P_{ij} = q_i u_j - q_j u_i,$$

and define the Plücker coordinates of L to be $[P_{01} : P_{02} : P_{03} : P_{23} : P_{31} : P_{12}]$. Writing this as $[\omega : \nu]$, if $q_0 = u_0 = 1$ and we set $q = (q_1, q_2, q_3), u = (u_1, u_2, u_3)$ then $\omega = u - q, \nu = q \times \omega$. Define the Klein quadric $\mathcal{K}$ to be the 4-dimensional hypersurface

$$\mathcal{K} = \{[\omega : \nu] \in \mathbb{P}^5 \mid \omega \cdot \nu = 0\}.$$

Proposition 6. *Two lines with Plücker coordinates $[\omega : \nu], [\omega' : \nu']$ intersect if and only if*

$$\omega \cdot \nu' + \omega' \cdot \nu = 0,$$

and this occurs if and only if the line connecting $[\omega : \nu], [\omega' : \nu']$ is contained in $\mathcal{K}$. Every plane contained in $\mathcal{K}$ is either an α-plane, corresponding to the set of lines through a specific point in $\mathbb{P}^3$, or a β-plane, corresponding to the set of lines contained in a specific plane in $\mathbb{P}^3$. Any two α-planes meet in a point, any two β-planes meet in a point, and an α-plane and a β-plane meet in a line if and only if the point corresponding to the α-plane is contained in the plane corresponding to the β-plane.

Definition 6. A *ruling* Γ of a surface $S \subset \mathbb{P}^3$ is a closed curve $\Gamma \subset \mathcal{K}$ such that each point of Γ corresponds to a line contained in S. The *degree* of a ruling Γ is defined to be its degree as a curve in $\mathbb{P}^5$. A line contained in S which is not contained in any ruling of S is called *special*.

Proposition 7. *For any three skew lines $L_1, L_2, L_3 \subset \mathbb{P}^3$, the union of the collection of all lines which intersect all three of L_1, L_2, L_3 is a smooth quadric surface S. Conversely, every smooth quadric surface S has two irreducible rulings Γ_1, Γ_2 of degree 2.*

Corollary 2. *Every irreducible ruled surface S is either a plane, a cone, a smooth quadric surface, or else has a unique ruling and contains at most two special lines which do not intersect each other. If S is not a plane, the degree d of an irreducible ruling is equal to the degree of S. Any nonspecial line intersects at most $d - 2$ other nonspecial lines.*

Theorem 12 (Cayley, Monge, Salmon, Voloch)**.** *Let $S \subset \mathbb{P}^3$ be a surface of degree d, with $d < p$ if the characteristic is p. If S has no ruled components, then there is a surface T of degree $11d - 24$ such that S and T have no components in common, and every line contained in S is contained in $S \cap T$.*

Sketch. The surface T is defined by the equation cutting out those points p of S for which there exists a line which is triply tangent to S at p (such a p is called a *flecnodal* point). The equation for T can be computed explicitly using resultants. Next, one shows that if a component of S consists entirely of flecnodal points, then that component must be ruled. □

Theorem 13 (Kollár)**.** *Let $\mathcal{L}$ be a collection of m distinct lines in $\mathbb{P}^n$ such that for any three distinct lines $L_1, L_2, L_3 \in \mathcal{L}$ the number of lines from $\mathcal{L}$ intersecting all three of L_1, L_2, L_3 is at most $\sqrt{m}$. If the characteristic is p, suppose that $m < \frac{11}{6}p^2$. Then the total number of intersection points between lines in $\mathcal{L}$ is at most*

$$\left(\frac{\sqrt{6}}{2} + \frac{(36 - \frac{1}{2})\sqrt{6}}{\sqrt{11}}\right) m^{\frac{3}{2}} < \sqrt{754}m^{\frac{3}{2}}.$$

Proof. By choosing a generic projection to $\mathbb{P}^3$, we may assume without loss of generality that $n = 3$. We may also assume that $m \geq 754$. Find a surface S of degree $d \leq \sqrt{6m} - 2$ containing $\mathcal{L}$, and assume that the degree of S is minimal. Choose an ordering $S_1, ...$ of the irreducible components of S such that, letting $\mathcal{L}_i = \{l \in \mathcal{L} \mid l \subset S_i \setminus (S_1 \cup \cdots \cup S_{i-1})\}$, we have $\frac{|\mathcal{L}_i|}{\deg S_i}$ nonincreasing in i. Write $m_i = |\mathcal{L}_i|, d_i = \deg S_i$. The number of intersections between lines contained in different sets $\mathcal{L}_i, \mathcal{L}_j$ is at most

$$\sum_{j<i} m_i d_j \leq \sum_{j<i} \frac{m_i d_j + m_j d_i}{2} = \frac{md - \sum_i m_i d_i}{2}.$$

If S_i is a cone, then there is at most 1 intersection point between lines in $\mathcal{L}_i$ (the cone point). If S_i is a plane, then any two lines in S_i intersect, so by assumption $m_i \leq \sqrt{m}$, and the number of intersection points between lines in $\mathcal{L}_i$ is at most

$$\frac{m_i(m_i - 1)}{2} \leq \frac{(m_i - 1)\sqrt{m}}{2}.$$

If S_i is a smooth quadric surface, then either one of the rulings on S_i contains at most two lines from $\mathcal{L}_i$ or by assumption both rulings contain at most $\sqrt{m}$ lines from $\mathcal{L}_i$, so the number of intersection points between lines in $\mathcal{L}_i$ is at most

$$\max\left(m_i - 1, 2(m_i - 2), \frac{m_i\sqrt{m}}{2}\right) \leq \frac{m_i\sqrt{m}}{2}.$$

If S_i is ruled of degree at least 3, then since there are at most two special lines in S_i and since nonspecial lines meet at most $d_i - 2$ other nonspecial lines, the number of intersection points between lines in $\mathcal{L}_i$ is at most

$$\frac{m_i(d_i - 2 + 2) + 2m_i}{2} = \frac{m_i d_i}{2} + m_i.$$

If S_i is not ruled, then by Lemma 6 and Theorem 12 we can find a surface T of degree at most $\min\left(11d_i - 24, \frac{6m_i}{d_i}\right)$ which contains $\mathcal{L}_i$ but not S_i (note that if we take $\deg T = 11d_i - 24$ then

$d_i \leq \sqrt{\frac{6}{11}m} < p$). Thus by Proposition 5 the number of intersections between lines in $\mathcal{L}_i$ is at most

$$\min\left(\frac{d_i(11d_i-24)}{2}(12d_i-26), 3m_i\Big(d_i+\frac{6m_i}{d_i}-2\Big)\right) \leq \frac{m_i d_i}{2} + \frac{(36-\frac{1}{2})\sqrt{6}}{\sqrt{11}} m_i^{\frac{3}{2}}.$$

Putting everything together, we see that the total number of intersection points between lines in $\mathcal{L}$ is at most

$$\frac{md}{2} + \sum_i \frac{(36-\frac{1}{2})\sqrt{6}}{\sqrt{11}} m_i\sqrt{m} \leq \left(\frac{\sqrt{6}}{2} + \frac{(36-\frac{1}{2})\sqrt{6}}{\sqrt{11}}\right) m^{\frac{3}{2}}. \qquad \square$$

Corollary 3 (Rudnev)**.** *Suppose we have n points and n planes in $\mathbb{P}^3$ such that no more than $\sqrt{n}$ points lie on any line and no more than $\sqrt{n}$ planes all contain a common line. Assume further that if the characteristic is p we have $n \leq \frac{11}{12}p^2$. Then the number of point-plane incidences is at most $\sqrt{6032}n^{\frac{3}{2}}$.*

Proof. Taking Plücker coordinates, we get a collection of n α-planes and n β-planes, and every incidence between a point and a plane becomes a pair of an α-plane and a β-plane which intersect in a line. Intersecting the configuration with a general hyperplane which does not contain the intersection of any two α-planes or the intersection of any two β-planes, we get a configuration of $2n$ lines in $\mathbb{P}^4$. Call a line coming from an α-plane an α-line, and similarly define β-lines. Any two α-lines do not intersect, any two β-lines do not intersect, and intersections between α-lines and β-lines correspond to point-plane incidences. For any two α-lines, any β-line intersecting them corresponds to a plane containing the line through the corresponding points, so at most $\sqrt{n}$ lines from the configuration intersect any pair of α-lines. Similarly, at most $\sqrt{n}$ lines from the configuration intersecting any pair of β-lines. Thus we can apply Theorem 13 to see that the number of incidences is at most

$$\sqrt{754}(2n)^{\frac{3}{2}} = \sqrt{6032}n^{\frac{3}{2}}. \qquad \square$$

Theorem 14 (Roche-Newton, Rudnev, Shkredov)**.** *If A is a finite subset of the nonzero elements of a field with characteristic p satisfying $|A|^2|AA| \leq \frac{11}{12}p^2$, then*

$$|A+A|^2|AA|^3 \geq \frac{|A|^6}{6032}.$$

Proof. We estimate the number N of solutions to the equation

$$a + bcd^{-1} = e + fgh^{-1},$$

with $a, b, c, d, e, f, g, h \in A$, in two ways. By taking $c = d, g = h$ and applying Cauchy-Schwarz we see that

$$N \geq \frac{|A|^4}{|A+A|}|A|^2.$$

Now to each tuple $(a, h, bc) \in A \times A \times AA$ we associate the point (a, bc, h^{-1}), and to each tuple $(d, e, fg) \in A \times A \times AA$ we associate the plane $\{(x, y, z) \mid x + d^{-1}y = e + fgz\}$. This gives us a collection of $|A|^2|AA|$ points and $|A|^2|AA|$ planes in $\mathbb{P}^3$ such that at most $|AA| \leq \sqrt{|A|^2|AA|}$ points (respectively planes) lie on any line. By Corollary 3, we see that

$$\sqrt{6032}(|A|^2|AA|)^{\frac{3}{2}} \geq N \geq \frac{|A|^6}{|A+A|}. \qquad \square$$

By a similar argument, we obtain the following.

Theorem 15 (Roche-Newton, Rudnev, Shkredov)**.** *Let A, B, C be finite subsets of a field of characteristic p. If $\max(|A|,|B|,|C|)^2 \leq |A||B||C| \leq \frac{11}{12}p^2$, then*

$$|A+BC|^2 \geq \frac{|A||B||C|}{6032}.$$

2.3 General rings

Theorem 16 (Katz-Tao Lemma)**.** *Let A be a nonempty finite set of non-zero-divisors of a ring R. There is a subset $B \subseteq A$ such that*

$$|B| \geq \frac{|A|^2}{4|AA|}$$

and such that for any natural numbers k, l we have

$$|kBB - lBB| \leq \left(384\frac{|A+A|^3|AA|^7}{|A|^{10}}\right)^{k+l}|kA - lA|.$$

Proof. By Theorem 7 we can find a subset $X \subseteq A$ with $|X| \geq \frac{|A|}{2}$ and

$$|AXA| \leq 3\frac{|AA|^2}{|A|^2}|X|.$$

By Cauchy-Schwarz we have

$$\sum_{x\in X}\sum_{y\in A}|xA \cap Xy| \geq \frac{|X|^2|A|^2}{|XA|} \geq \frac{|X|^2|A|^2}{|AA|},$$

so we can pick some $y \in A$ such that

$$\sum_{x\in X}|xA \cap Xy| \geq \frac{|X|^2|A|}{|AA|}.$$

Setting

$$B = \left\{x \in X \mid |xA \cap Xy| \geq \frac{|X||A|}{2|AA|}\right\},$$

we have

$$|B| \geq \frac{|X||A|}{2|AA|}.$$

We now show by induction on h that if $b_1, ..., b_k \in B^h$, then

$$|b_1A + \cdots + b_kA| \leq \left(\frac{4|A+A||AA|}{|A|^2}\right)^{hk}|kA|.$$

Suppose that we have shown this already for h. Letting $b_1, ..., b_k \in B^h$ and $x_1, ..., x_k \in B$, since the b_is and x_is are non-zero-divisors we have

$$|b_ix_iA + b_ix_iA| = |A+A|$$

and

$$|b_i x_i A \cap b_i A y| = |x_i A \cap A y| \geq \frac{|A|^2}{4|AA|},$$

so by Proposition 1 we have

$$\begin{aligned} |b_1 x_1 A + \cdots + b_k x_k A| &\leq \frac{|A+A|}{|x_1 A \cap A y|} \cdots \frac{|A+A|}{|x_k A \cap A y|} |b_1 A y + \cdots + b_k A y| \\ &\leq \left(\frac{4|A+A||AA|}{|A|^2} \right)^{(h+1)k} |kA|, \end{aligned}$$

completing the induction. A similar statement with both additions and subtractions can be proved in the same way.

Now choose an element $m \in BA$ such that, setting

$$C = \{(b, a) \in B \times A \mid ba = m\},$$

we have

$$|C| \geq \frac{|B||A|}{|BA|} \geq \frac{|A|^2}{2|AA|^2}|X|.$$

Fixing a representation $uv + tw$ for each sum in $BB + BB$, we have an injection

$$(BB + BB) \times C \times C \hookrightarrow \{(c, d, s) \mid c, d \in B^3, s \in cA + dA\},$$

sending $(uv + tw, (b, a), (b', a'))$ to $(uvb, twb', (uv + tw)m)$. Thus, using $|B^3| \leq |AXA| \leq 3\frac{|AA|^2}{|A|^2}|X|$, we have

$$\begin{aligned} |BB + BB| &\leq \left(\frac{|B^3|}{|C|} \right)^2 \left(\frac{4|A+A||AA|}{|A|^2} \right)^6 |A+A| \\ &\leq 6^2 \frac{|AA|^8}{|A|^8} \cdot 4^6 \frac{|A+A|^6 |AA|^6}{|A|^{12}} |A+A| \\ &= 384^2 \frac{|A+A|^6 |AA|^{14}}{|A|^{20}} |A+A|. \end{aligned}$$

By the same argument, for any natural numbers k, l we get

$$|kBB - lBB| \leq \left(384 \frac{|A+A|^3 |AA|^7}{|A|^{10}} \right)^{k+l} |kA - lA|.$$

More generally, we even have

$$|kB^h - lB^h| \leq \left(\frac{|B^{h+1}|}{|C|} \left(\frac{4|A+A||AA|}{|A|^2} \right)^{h+1} \right)^{k+l} |kA - lA|. \qquad \square$$

Theorem 17 (Self-improving property)**.** *Let A be a finite subset of a ring R, and let D be a nonempty subset of $A - A$. If x is an element of R and $r \in R^*$ is a non-zero-divisor such that*

$$|xA + rA| < \frac{|A|^2}{|D|}$$

then there is an element $d \in (A-A) \setminus D$ such that

$$|xAA + rAA| \leq \frac{|2AA - AA|}{|dA|}|3AA - 2AA|.$$

If we take D to be the set of zero-divisors of $A - A$ and we assume that $D \neq A - A$, then we have

$$|xA + rA| \leq \frac{|2AA - 2AA|}{|A|}|3AA - 3AA|.$$

Proof. By Cauchy-Schwarz, we have

$$\#\{(a, b, a', b') \in A \times A \times A \times A \mid xa + rb = xa' + rb'\} \geq \frac{|A|^4}{|xA + rA|},$$

so

$$\#\{(d, e) \in (A - A) \times (A - A) \mid xd = re\} \geq \frac{|A|^2}{|xA + rA|} > |D|.$$

Since r is a non-zero-divisor, each pair (d, e) with $xd = re$ corresponds to a different value of d. Thus we can find $d \in (A - A) \setminus D$ with $xd \in r(A - A)$. By the Ruzsa covering lemma, there is a set $S \subseteq AA$ with

$$|S| \leq \frac{|dA + AA|}{|dA|} \leq \frac{|2AA - AA|}{|dA|}$$

and

$$AA \subseteq dA - dA + S.$$

Thus we have

$$|xAA + rAA| \leq |xdA - xdA + xS + rAA| \leq |S||r(3AA - 2AA)| \leq \frac{|2AA - AA|}{|dA|}|3AA - 2AA|.$$

For the last claim, we apply the Ruzsa covering lemma to find $S' \subseteq AA - AA$ with

$$AA - AA \subseteq dA - dA + S'$$

to get

$$|xA+rA| \leq |(xA+rA)(A-A)| \leq |xdA-xdA+xS'+rA(A-A)| \leq \frac{|2AA - 2AA|}{|A|}|3AA-3AA|. \quad \square$$

From here on, we take A to be a subset of a ring R such that $A - A$ contains a non-zero-divisor, and we let D be the set of zero-divisors in $A - A$. For any $r \in R$, we define the set S_r to be

$$S_r = \left\{x \in R \mid |xA + rA| < \frac{|A|^2}{|D|}\right\}.$$

Proposition 8. $|A - A|, |A + A| \leq |2AA - 2AA|$.

Proposition 9. *If $r \in R^*$ then $|S_r| < |A - A|^2$. If we also have*

$$|D| \leq \frac{|A|^3}{2|2AA - 2AA||3AA - 3AA|},$$

then

$$|S_r| < \frac{2|A - A|^2|2AA - 2AA||3AA - 3AA|}{|A|^3}.$$

Proof. Let $x \in S_r$. By the same argument as in Theorem 17, we have

$$\#\{(d,e) \in ((A-A)\setminus D)\times(A-A) \mid xd = re\} \geq \frac{|A|^2}{|xA+rA|} - |D| \geq \frac{|A|^3}{|2AA-2AA||3AA-3AA|} - |D|.$$

Since for each $(d,e) \in ((A-A)\setminus D)\times(A-A)$ there is at most one x such that $xd = re$, we see that

$$|S_r| \leq \frac{(|A-A|-|D|)|A-A|}{\frac{|A|^3}{|2AA-2AA||3AA-3AA|} - |D|}. \qquad \square$$

Proposition 10. *If $r \in R^*$ and*

$$|D| < \frac{|A|^6}{|A+A||2AA-2AA|^2|3AA-3AA|^2},$$

then S_r is closed under addition (and is therefore an additive group).

Proof. For $x, y \in S_r$, we have

$$|(x+y)A+rA| \leq \frac{|xA+rA|}{|A|}\frac{|yA+rA|}{|A|}|A+A| \leq \frac{|A+A||2AA-2AA|^2|3AA-3AA|^2}{|A|^4} < \frac{|A|^2}{|D|}. \qquad \square$$

Proposition 11. *If*

$$|D| < \frac{|A|^8}{|A+A||2AA-2AA|^3|3AA-3AA|^3},$$

then S_1 is closed under multiplication (and is therefore a ring).

Proof. Suppose $x, y \in S_1$. Apply the Ruzsa covering lemma to find $S \subseteq yA$ with

$$|S| \leq \frac{|yA+A|}{|A|}$$

and

$$yA \subseteq A - A + S.$$

Then we have

$$|xyA+A| \leq |xA - xA + xS + A| \leq \frac{|A+A||2AA-2AA|^3|3AA-3AA|^3}{|A|^6} < \frac{|A|^2}{|D|}. \qquad \square$$

Proposition 12. *If $r \in R^*$, $a \in (A-A)\setminus D$, and*

$$|D| < \frac{|A|^{10}}{|A+A||2AA-2AA|^4|3AA-3AA|^4},$$

then $S_rS_a \subseteq S_{ra}$.

Proof. Take $x \in S_r$ and $y \in S_a$. We have

$$|yA+Aa| \leq \frac{|yA+aA|}{|A|}\frac{|Aa+aA|}{|A|}|A| \leq \frac{|yA+aA||2AA-2AA|}{|A|}.$$

Take $S \subseteq yA$ with

$$|S| \leq \frac{|yA + Aa|}{|A|}$$

and

$$yA \subseteq Aa - Aa + S.$$

Take $S' \subseteq xA - xA$ with

$$|S'| \leq \frac{|xA - xA + rA|}{|A|} \leq \frac{|xA + rA|}{|A|} \frac{|-xA + rA|}{|A|} \frac{|A + A|}{|A|}$$

and

$$xA - xA \subseteq rA - rA + S'.$$

Then

$$\begin{aligned} |xyA + raA| &\leq |xAa - xAa + xS + raA| \leq |S||rAa - rAa + S'a + raA| \\ &\leq |S||S'||Aa - Aa + aA| \leq \frac{|A + A||2AA - 2AA|^4|3AA - 3AA|^4}{|A|^8} < \frac{|A|^2}{|D|}. \end{aligned}$$

□

Proposition 13. *If $r, s \in R$ then $sS_r \subseteq S_{sr}$.*

Proposition 14. *If $r \in R$ and $|D| < \frac{|A|^2}{|A+A|}$, then $r \in S_r$.*

Proposition 15. *If $r, s \in R$, then $r \in S_s \iff s \in S_r$.*

Proposition 16. *If $r, s \in R^*$, $S_r \cap S_s \cap R^* \neq \emptyset$, and*

$$|D| < \frac{|A|^7}{|2AA - 2AA|^3|3AA - 3AA|^3},$$

then $S_r = S_s$.

Proof. Take $t \in S_r \cap S_s \cap R^*$ and $x \in S_r$. We have

$$|rA + sA| \leq \frac{|tA + rA|}{|A|} \frac{|tA + sA|}{|A|} |A|.$$

Then

$$|xA + sA| \leq \frac{|xA + rA|}{|A|} \frac{|rA + sA|}{|A|} |A| \leq \frac{|2AA - 2AA|^3|3AA - 3AA|^3}{|A|^5} < \frac{|A|^2}{|D|}.$$

□

Theorem 18 (Inhomogeneous sum-product theorem)**.** *Let R be a ring, $A \subseteq R$. If*

$$|(A - A) \setminus R^*| < \min\left(\frac{|A|^2}{|A + AA|}, \frac{|A|^8}{2|A + A||2AA - 2AA|^3|3AA - 3AA|^3}\right),$$

then there is a subring $S \subseteq R$ such that $A \subseteq S$ and

$$|S| < \frac{2|A - A|^2|2AA - 2AA||3AA - 3AA|}{|A|^3}.$$

Proof. We take $S = S_1$, then $A \subseteq S_1$ by the assumption $|AA + A| < \frac{|A|^2}{|D|}$. Previous propositions show that S_1 is a ring and give the required bound on the size of S_1. □

Theorem 19 (Homogeneous sum-product theorem with invertible element)**.** *If R has a 1, $A \subseteq R$ has an invertible element a, and*

$$|(A - A) \setminus R^*| \le \frac{|A|^8}{2|A + A||2AA - 2AA|^3|3AA - 3AA|^3},$$

then there is a subring $S \subseteq R$ such that

$$A \subseteq aS = Sa$$

and

$$|S| < \frac{2|A - A|^2|2AA - 2AA||3AA - 3AA|}{|A|^3}.$$

Proof. We take $S = S_1$. As before, we have S_1 a ring with the required size bound. We have

$$|a^{-1}AA + A| = |AA + aA| \le |AA + AA| < \frac{|A|^2}{|D|}$$

by our assumption, so $a^{-1}A \subseteq S$, that is, $A \subseteq aS$. Since $SS = S$, we have

$$|aSa^{-1}A + A| \le |aSa^{-1}aS + aS| = |aS| \le |S| < \frac{2|2AA - 2AA|^3|3AA - 3AA|}{|A|^3} < \frac{|A|^2}{|D|},$$

so $aSa^{-1} \subseteq S$. Since S is finite, this implies that $aS = Sa$. □

References

[1] J. Bourgain. Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary. *J. Anal. Math.*, 97:317–355, 2005.

[2] M. Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *Int. Math. Res. Not. IMRN*, (11):Art. ID rnm035, 11, 2007.

[3] M. Z. Garaev. The sum-product estimate for large subsets of prime fields. *Proc. Amer. Math. Soc.*, 136(8):2735–2739, 2008.

[4] Nets Hawk Katz and Chun-Yen Shen. A slight improvement to Garaev's sum product estimate. *Proc. Amer. Math. Soc.*, 136(7):2499–2504, 2008.

[5] János Kollár. Szemerédi-Trotter-type theorems in dimension 3. *Adv. Math.*, 271:30–61, 2015.

[6] Sergei V. Konyagin and Misha Rudnev. On new sum-product-type estimates. *SIAM J. Discrete Math.*, 27(2):973–990, 2013.

[7] Giorgis Petridis. New proofs of Plünnecke-type estimates for product sets in groups. *Combinatorica*, 32(6):721–733, 2012.

[8] O. Roche-Newton, M. Rudnev, and I. D. Shkredov. New sum-product type estimates over finite fields. *ArXiv e-prints*, August 2014.

[9] M. Rudnev. On the number of incidences between planes and points in three dimensions. *ArXiv e-prints*, July 2014.

[10] Imre Z. Ruzsa. Sumsets and structure. In *Combinatorial number theory and additive group theory*, Adv. Courses Math. CRM Barcelona, pages 87–210. Birkhäuser Verlag, Basel, 2009.

[11] Tomasz Schoen. New bounds in Balog-Szemerédi-Gowers theorem. *Combinatorica*, pages 1–7.

[12] József Solymosi. Bounding multiplicative energy by the sumset. *Adv. Math.*, 222(2):402–408, 2009.

[13] Terence Tao. The sum-product phenomenon in arbitrary rings. *Contrib. Discrete Math.*, 4(2):59–82, 2009.