Sum sets, Product sets, and Combinatorial Geometry

Douglas Barnes

October 14, 2023

Contents

Abstract

Suppose A is a finite subset of $\mathbb{R}$. The Erdős-Szemerédi problem asks: how small can $\max\{|A+A|,|AA|\}$ be? We will show that for $|A|$ large, $\max\{|A+A|,|AA|\}$ cannot be $O\left(|A|^{4/3}\right)$, one of the best known results for this problem. We will also look at additive combinatorics in groups, in particular a generalisation of the Cauchy-Davenport inequality to all groups: if $A, B \subset G$, then $|A+B| \geq \min\{p(G),|A|+|B|-1\}$, where $p(G)$ is the size of the smallest subgroup of G. Lastly we will consider $A \subset \mathbb{F}_p$ and estimate how large $\max\{|A+A|,|AA|\}$ must be relative to p.

1 Sums and Products in $\mathbb{R}$

1.1 The Smallest and Largest Sum Sets and Product Sets

For A, B finite subsets of $\mathbb{R}$ we define

$$\begin{aligned} A+B &= \{a+b : a \in A \ b \in B\} \quad \text{(sum set)} \\ AB &= \{ab : a \in A \ b \in B\} \quad \text{(product set)} \\ -A &= \{-a : a \in A\} \\ a+B &= \{a+b : b \in B\} \end{aligned}$$

A quick warmup would be to ask, how big can $A+A$ be? Every element in this set is either a sum of two distinct elements in A (there are $\binom{|A|}{2}$ ways to do this) or a sum of the same element twice (there are $|A|$ ways to do this). In the worst case, all of these are distinct, thus

$$\begin{aligned} |A+A| &\le \binom{|A|}{2} + |A| \\ &= \frac{1}{2}\left(|A|^2 + |A|\right) \end{aligned}$$

This argument also tells us how we would obtain the upper bound for a prescribed $|A| = n$. We need $a + a'$ to be distinct for every $a, a' \in A$ (up to commuting), so for instance we could consider $A_n := \{1, 2, \ldots, 2^{n-1}\}$. Since the binary expansion of numbers is unique, each $a + a'$ is distinct. Therefore the upper bound is tight (meaning that the bound is attainable for all prescribed $|A| = n$).

In fact, this argument would work for any commutative operation instead of '+'. In particular, we have the similar bound $|AA| \le \binom{|A|}{2} + |A|$. One clever idea shows that the bound is also tight for $|AA|$: For any set A, we can define $2^A := \{2^a : a \in A\}$. This set has the key property that its product set, $2^A 2^A$, has the same cardinality as $A + A$. Indeed, $2^A 2^A = 2^{A+A}$ because for any $a, b \in A$, we have $2^a 2^b = 2^{a+b}$, thus

$$|2^A 2^A| = |2^{A+A}| = |A + A|$$

Therefore, we can choose $B_n = 2^{A_n}$, then $|B_n| = |A_n|$ and $|B_n B_n| = \binom{|B_n|}{2} + |B_n|$ for all n. Hence the upper bound is tight. Impressively, B_n also maximises its sum set simultaneously as the sums are still distinct binary expansions, thus $|B_n + B_n| = \binom{|B_n|}{2} + |B_n|$.

Theorem 1.1. (Trivial Upper bound) For $A \subset \mathbb{R}$ with $|A| = n$,

$$\begin{aligned} |A+A| &\le \binom{n}{2} + n \\ |AA| &\le \binom{n}{2} + n \end{aligned}$$

and these inequalities are tight. They can also be equalities simultaneously, in other words, the inequality

$$\min\{|A+A|, |AA|\} \le \binom{n}{2} + n$$

is tight.

Our next question is, how small can $A + A$ and AA be? Certainly they cannot be smaller than A since we can take any $a \in A$ then $a + A \subseteq A + A$ and $|a + A| = |A|$, thus $|A + A| \ge |A|$. Our next claim is that we can actually do a bit better than that.

Theorem 1.2. (Trivial Lower Bound) For any $A \subset \mathbb{R}$ with $|A| = n$, $|A + A| \ge 2n - 1$, and this bound is tight.

Proof. A first guess at what might make $A+A$ small would be an arithmetic progression as intuitively there would be a lot of overlapping in the sums. The simplest AP is of course the integers $A := \{1, 2, \ldots, n\}$. Then $A + A = \{2, 3, \ldots, 2n\}$ is of size $2n-1$.

To prove we cannot get any smaller, one could realise that the above example is more about numbers being ordered from 1 to n than the set itself being $\{1, \ldots, n\}$. Suppose $A = \{x_1, \ldots, x_n\}$ with $x_1 < x_2 < \cdots < x_n$. Then the inequalities below hold,

$$\begin{aligned} & x_1 + x_1 \\ < \; & x_1 + x_2 \\ < \; & x_2 + x_2 \\ < \; & x_2 + x_3 \\ & \ldots \\ < \; & x_{n-1} + x_n \\ < \; & x_n + x_n \end{aligned}$$

Therefore, the $2n-1$ sums above are distinct.

□

One could notice from the above proof that the only property of '+' that if $x_1 < \cdots < x_n$, then the chain of inequalities listed in the proof hold. This property can be phrased precisely as,

$$b < b' \implies (a + b < a + b' \text{ and the commuted version } b + a < b' + a)$$

Under the assumption $0 \notin A$, this statement is true if we replace $+$ with $\times$. Thus, this lower bound also holds for $|AA|$ and the minimising example would be $2^{\{1,\ldots,n\}}$.

If $0 \in A$, then in AA we have all the nonzero products, and zero. In other words,

$$AA = (A \backslash \{0\})(A \backslash \{0\}) \cup \{0\}$$

We know $|A\backslash\{0\}A\backslash\{0\}| \geq 2(n-1) - 1$, so $|AA| \geq 2n - 2$.

Corollary 1.2.1. (Trivial Lower Bound for Multiplication) For any $A \subset \mathbb{R}$ with $|A| = n$,

$$|AA| \geq \begin{cases} 2n - 1 & \text{if } 0 \notin A \\ 2n - 2 & \text{if } 0 \in A \end{cases}$$

and this bound is tight.

Proof. We just saw the proof of the bounds. To show the bounds are tight, for the $0 \notin A$ case we know there are sets with $|A + A| = 2n - 1$ (e.g. $\{1, 2, \ldots, n\}$) so as discussed previously, $|2^A 2^A| = 2n - 1$. Therefore, a minimising example is $2^{\{1,2,\ldots,n\}}$. □

1.2 The Erdős-Szemerédi Problem: Minimising the Sum Set and Product Set simultaneously

Sum-set product-set questions suddenly become a lot less dull when we ask, can both $|A+A|$ and $|AA|$ be small simultaneously? In other words, can $\max\{|A+A|, |AA|\}$ be small?

We already saw that our example of a set that maximised $|AA|$ also happened to maximise $|A+A|$, thus showing $\min\{|A+A|, |AA|\}$ can achieve its upper bound of $\binom{|A|}{2} + |A|$. It is natural to ask whether $\max\{|A+A|, |AA|\}$ can achieve its lower bound of $2|A|-1$. This is equivalent to having both $|A+A|$ and $|AA|$ equal to $2|A|-1$. Sadly, we cannot achieve the bound in the same way as before because our minimising set for $|AA|$ is not a minimising set for $|A+A|$ (in fact, it is a maximising set).

It turns out that it is not possible to achieve this lower bound. One simple way to prove this is to show all sets which satisfy $|A+A| = 2|A|-1$ are arithmetic progressions and all sets which satisfy $|AA| = 2|A|-1$ are geometric progressions. Since no set is both an arithmetic progression and a geometric progression, we can conclude a set cannot have $\max\{|A+A|, |AA|\} = 2|A|-1$.

Lemma 1.3. If A is a finite subset of $\mathbb{R}$ with $|A+A| = 2|A|-1$, then A is a subset of an AP.

Proof. Let $A = \{x_1, \dots, x_n\}$ with $x_1 < \cdots < x_n$. The set $A+A$ must be precisely the elements listed in the proof of Theorem 1.2. I.e,

$$A + A = \{x_1 + x_1,\ x_1 + x_2, \dots,\ x_k + x_k,\ x_k + x_{k-1}, \dots,\ x_n + x_n\} \qquad (*)$$

We will prove inductively that the entire sequence $x_1, \dots, x_n$ is a subset of an AP. This is equivalent to showing $x_k - x_{k-1} = x_1 - x_2$ for all k.

Assume $x_1, \dots, x_m$ satisfy the above. Then $x_{m-1} + x_{m+1}$ is an element of $A+A$, but is not written explicitly in this form in $(*)$, so it must equal one of the terms we listed. By assumption of the (x_i) increasing, we have

$$x_{m-1} + x_m < x_{m-1} + x_{m+1} < x_m + x_{m+1}.$$

The LHS and RHS are terms written in $(*)$ and the only term in $(*)$ which lies between them is $x_m + x_m$, thus

$$\begin{aligned} x_{m-1} + x_{m+1} &= x_m + x_m \\ \therefore x_{m+1} - x_m &= x_m - x_{m-1} \\ &= x_1 - x_2 \qquad \text{(induction)} \end{aligned}$$

□

Replacing '+' with '×' in the above proof yields the similar claim for product sets.

Lemma 1.4. If A is a finite subset of $\mathbb{R}$ with $|AA| = 2|A|-1$ and $0 \notin A$, then A is a subset of a GP

Corollary 1.4.1. There is no finite subset A of $\mathbb{R}$ with $0 \notin A$ and $\max\{|A+A|, |A|\} = 2|A|-1$

[The case when $0 \in A$ is more of an uninteresting techanicality.]

It turns out finding the exact minimum of $\max\{|A+A|, |AA|\}$ over all $A \subset \mathbb{R}$ of prescribed cardinality $|A| = n$ is simply too difficult of a problem to solve, so we instead we ask whether we can find its asymptotic order for n large.

Notation

- We say $f(n) = O(g(n))$ if there exists a constant $C > 0$ such that $f(n) \leq Cg(n)$ for all n sufficiently large. In other words f is asymptotically bounded above by g
- We say $f(n) = \Omega(g(n))$ if there exists a constant $C > 0$ such that $f(n) \geq Cg(n)$ for all n sufficiently large. In other words, f is asymptotically bounded below by g.
- We say $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. In other words, f and g have the same asymptotic order.

Question Let $g(n)$ be the smallest possible value of $\max\{|A+A|, |AA|\}$ over all $A \subset \mathbb{R}$ size n. For which α is $g(n) = O(n^\alpha)$?

We first make some basic observations. Since $|A+A|$ and $|AA|$ are bounded above by a quadratic in $|A|$ (Theorem 1.1), $\max\{|A+A|, |AA|\}$ is also bounded above by a quadratic in $|A|$. Therefore $g(n) = O(n^2)$, and so $\alpha \geq 2$ is sufficient. Also, $|A+A|$ and $|AA|$ are larger than $|A|$, so $\alpha \geq 1$ is necessary.

Consider $A = \{1, \dots, n\}$, which we know makes $|A+A|$ minimal. The set AA is the distinct numbers in a n by n multiplication table which we saw in elementary school, though finding the size of $|AA|$ is no elementary task.

1	2	3	$\dots$	n
2	4	6	$\dots$	$2n$
3	6	9	$\dots$	$3n$
			$\dots$	
n	$2n$	$3n$	$\dots$	n^2

Figure 1: The n by n multiplication table

It was not until 2008 that Ford[1] showed $|AA| = O\left(\frac{n^2}{(\log n)^c (\log\log n)^{3/2}}\right)$ for some positive constant c. Since $|A+A| = 2n-1$ is much smaller than $|AA|$, we know $|AA| = \max\{|A+A|, |AA|\}$. Although this example shows the maximum can be asymptotically smaller than $O(n^2)$, it is not $O(n^\alpha)$ for any $\alpha < 2$.

The conjecture of Erdős-Szemerédi is that α cannot be smaller than 2.

Conjecture 1.5. (Erdős-Szemerédi[2]) $g(n)$ is not $O(n^{2-\epsilon})$ for any $\epsilon > 0$. In other words, for any $c, \epsilon > 0$, there exists N such that for all $A \subset \mathbb{R}$ of cardinality N, $\max\{|A+A|, |AA|\} \geq c|A|^{2-\epsilon}$.

Progress towards this conjecture has been made by proving statements of the form 'If $g(n) = O(n^\alpha)$, then $\alpha \geq \beta$ for some $\beta > 1$'. Proving for $\beta = 2$, would solve the conjecture positively. Over the years, many have tried to get β as close to 2 as possible, though there is still a long way to go.

According to [3],

Year	β	Author
1983	$1 + \delta$ for some $\delta > 0$ sufficiently small	Erdős and Szemerédi[2]
1997	$1 + \frac{1}{31}$	Nathanson[4]
1998	$1 + \frac{1}{15}$	Ford[5]
1997	$1 + \frac{1}{4}$	Elekes[6]
2005	$1 + \frac{3}{11}$	Solymosi[7]
2009	$1 + \frac{1}{3}$	Solymosi[8]
2016	$1 + \frac{1}{3} + \frac{5}{9813}$	Konyagin and Shkredov[9]

1.3 Elekes' Bound

Elekes significantly improved the results of Erdős, Szemerédi, and Nathanson by applying combinatorial geometry. Although using geometry is certainly not what one first thinks after reading the problem, the most surprising part is the simplicity of his proof, given one important lemma.

Lemma 1.6. (Szemerédi-Trotter)[10] Suppose we have a set $\mathcal{P}$ of points in the plane and a set $\mathcal{L}$ of straight lines. Let $t \leq \sqrt{|\mathcal{P}|}$. If each $l \in \mathcal{L}$ contains at least t points in $\mathcal{P}$, then

$$|\mathcal{L}| \leq C\frac{|\mathcal{P}|^2}{t^3}$$

for C a (large) constant independent of $\mathcal{L}, \mathcal{P}$ and t.

Theorem 1.7. (Elekes' Bound) For any constant c, there exists N large such that for all A of cardinality larger than N, $\max\{|A+A|, |AA|\} > c|A|^{1+\frac{1}{4}}$. In other words, $\beta > 1 + \frac{1}{4}$.

Proof. Let $\mathcal{P} = (A+A) \times AA$ (in the Cartesian sense) and $\mathcal{L} = \{y = a(x-a') : a, a' \in A\}$.

Consider a particular $y = a(x-a')$ in $\mathcal{L}$ and fix $b \in A$. By putting $x = a' + b$ into the equation, one can see this line contains the point $(a'+b, ab) \in \mathcal{P}$. Since we can repeat this for any $b \in A$ and get a distinct point each time, we have shown each line in $\mathcal{L}$ intersects at least $|A|$ points in $\mathcal{P}$.

Therefore by Lemma 1.6 (Szemerédi-Trotter) with $t = |A|$ and $|\mathcal{P}| = |A+A||AA| > t^2$,

$$\begin{aligned}
|\mathcal{L}| &\leq C\frac{|\mathcal{P}|^2}{t^3} \\
|A|^2 &\leq C\frac{|A+A|^2|AA|^2}{|A|^3} \\
|A|^{\frac{5}{2}} &\leq C|A+A||AA| \\
|A|^{\frac{5}{2}} &\leq C\max\{|A+A|, |AA|\}^2 \\
\therefore \max\{|A+A|, |AA|\} &\geq C'|A|^{1+\frac{1}{4}}
\end{aligned}$$

Thus, $\max\{|A+A|, |AA|\}$ cannot be asymptotically smaller than $|A|^{1+\frac{1}{4}}$

□

1.4 Solymosi's Bound

The improvement to Elekes' Bound made by Solymosi still involves geometry, but we will need a new ingredient.

Definition 1.8. The *multiplicative energy* of A, $E_\times(A) := |\{(a,b,c,d) \in A \times A \times A \times A : ab = cd\}|$

Why might we be interested in multiplicative energy? Suppose we want to compute $|AA|$ but we know $E_\times(A)$ is small. The most simple approach would be: start with an empty list and iterate through every pair $(a,b) \in A^2$. Given (a,b), we write down ab at the end of our list if ab does not appear in our list already. Since $E_\times(A)$ is small, it is unlikely that ab appears in our list already, because this would give a pair (a,b,c,d) with $ab = cd$, and we know there are few of those. Thus the final length of our list (which equals $|AA|$) must be large. We can quantify this idea precisely,

Lemma 1.9. **($|AA|$ and $E_\times(A)$ cannot be small simultaneously)** For any $A \subset \mathbb{R}$,

$$|AA|E_\times(A) \geq |A|^4$$

Proof. An equivalent way to write $E_\times(A)$ is,

$$\begin{aligned}
E_\times(A) &= \sum_{(a,b)\in A^2} \sum_{(c,d)\in A^2} 1_{ab=cd} \\
&= \sum_{(a,b)\in A^2} \sum_{(c,d)\in A^2} \sum_{x\in AA} 1_{ab=cd=x} \\
&= \sum_{x\in AA} \sum_{(a,b)\in A^2} \sum_{(c,d)\in A^2} 1_{ab=x}1_{cd=x} \\
&= \sum_{x\in AA} |\{(a,b)\in A^2 : ab = x\}|^2 \quad (*)
\end{aligned}$$

Then by the Cauchy-Schwarz inequality, one has

$$\begin{aligned}
\sum_{x\in AA} 1^2 \sum_{x\in AA} |\{(a,b)\in A^2 : ab = x\}|^2 &\geq \left(\sum_{x\in AA} |\{(a,b)\in A^2 : ab = x\}|\right)^2 \\
&= |A|^4 \\
\therefore |AA|E_\times &\geq |A|^4
\end{aligned}$$

□

This proves that $|AA|$ and $E_\times$ are related, but why should we work with $E_\times$ instead of $|AA|$? The key observation is that multiplicative energy is equal to 'quotient energy',

$$E_\times(A) = |\{(a,b,c,d)\in A^4 : a/d = c/b\}|$$

by simply dividing through by bd (we can assert $x/0 := \infty$ and $\infty = \infty$, but we will ignore such technicalities)

Why might we care about 'quotient energy'? If $(a,b,c,d)\in A^4$ satisfy $a/d = c/b$, then (d,a) and (b,c) lie on the same line through the origin $y = mx$ where $m = a/d = c/b$ (geometry!). Thus,

$$E_\times(A) = |\{(a,b,c,d)\in A^4 : (d,a) \text{ and } (b,c) \text{ lie on the same line through the origin}\}|$$

The phrasing for the set whose cardinality we are taking above (lets call it S) is quite awkward. To get a more approachable form for $E_\times(A)$, we can carry out the same analysis as in Lemma 1.9. Alternatively, to give a bit more insight, we can argue this by counting $|S|$ in another way.

Fix a line l through the origin. Suppose (d,a) and (b,c) are (not necessarily distinct) points in $A\times A$ which lie on l. Then (a,b,c,d) is a tuple in S. Since there are $|(A\times A)\cap l|^2$ ways to choose (d,a) and (b,c) (in an ordered way), there are $|(A\times A)\cap l|^2$ tuples in S corresponding to the line l. Thus,

$$E_\times(A) = \sum_{l \text{ is a line through the origin}} |(A\times A)\cap l|^2$$

Define $A/A := \{a/b : a, b \in A\}$. It will be useful to express things in terms of the gradient $m(l)$ a line l because the lines for which $(A \times A) \cap l$ is nonempty are precisely those where $m(l) \in A/A$. Hence,

$$E_{\times}(A) = \sum_{m \in A/A} r(l(m))^2$$

where $r(l) = |(A \times A) \cap l|$ and $l(m)$ is the line through the origin with gradient m.

Combining with Lemma 1.6 we have,

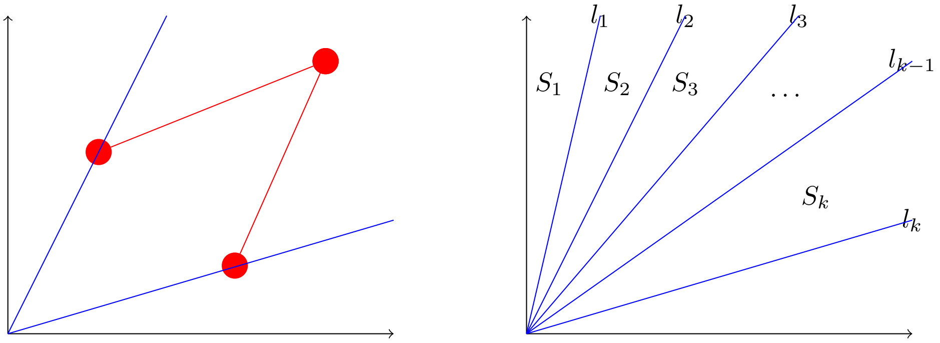
$$|AA| \sum_{m \in A/A} r(l(m))^2 \geq |A|^4 \qquad (*)$$

If we could upper bound the sum above by something involving $|A + A|$, we could get a new bound by using reasoning similar to the end of Elekes' proof. We'll need a couple more good ideas for this to work though.

So far we have the set of lines $\{l(m) : m \in A/A\}$ which cover $A \times A$. The only thing we haven't involved yet is $A + A$. Solymosi's idea is to consider the set of points $\mathcal{P} := A \times A + A \times A$ in the plane. On one hand, $\mathcal{P} = (A + A) \times (A + A)$, thus $|P| = |A + A|^2$. Another way to count the number of points in $\mathcal{P}$ is to count the number of points that lie between adjacent lines in $\{l(m) : m \in A/A\}$.

In general if we have any two lines through the origin in $\mathbb{R}^2$ and sum two points on these lines, the resulting point will lie between the two lines in the component with the smaller angle (because this operation is equivalent to a reflection of (0,0) through the line joining the two points) as in (a).

Repeating this argument over a set of lines $D := \{l_1, \ldots, l_k\}$ with gradients $m_1 > \cdots > m_k$, then for all i, $l_i + l_{i-1} \subset S_i$ as in (b), where S_i is region between l_i and l_{i-1} with the smaller angle.



(a) Adding points on lines

(b) Partition of first quadrant by the lines

In particular, $(l_i + l_{i-1}) \cap \mathcal{P} \subset S_i \cap \mathcal{P}$, and so

$$\begin{aligned}
|\mathcal{P}| &= \sum_1^k |S_i \cap \mathcal{P}| \qquad \text{(partition)} \\
&\geq \sum_2^k |(l_i + l_{i-1}) \cap \mathcal{P}| \qquad \text{(what we just argued)} \\
&= \sum_2^k |(l_i \cap \mathcal{P}) + (l_{i-1} \cap \mathcal{P})|
\end{aligned}$$

Note that if $X, Y \subset \mathbb{R}$ have unique sums (i.e. $x + y \neq x' + y'$ for all $x' \neq x$ in X and $y' \neq y$ in Y), then $|X + Y| = |X||Y|$. The sets $l_i \cap \mathcal{P}$ and $l_{i-1} \cap \mathcal{P}$ have this property for all i. Indeed, if we have four points $a, a' \in l_i$ and $b, b' \in l_j$ with $a + b = a' + b'$ then $a - a' = b - b'$, but adding points on the same line gives another point on the line so $a - a' \in l_i \cap l_j$. But $l_i \cap l_j = \{0\}$ therefore $a = a'$ and $b = b'$ i.e the sums in the sum-set are unique. Thus,

$$|\mathcal{P}| \geq \sum_{i=2}^k r(l_i) r(l_{i-1})$$

Altogether,

$$|AA| \sum_{m \in A/A} r(l(m))^2 \geq |A|^4 \qquad (*)$$

and

$$|A + A|^2 \geq \sum_2^k r(l_i) \cdot r(l_{i-1}) \qquad (**)$$

where $D = \{l_1, \ldots, l_k\}$ is any choice of lines.

The next brilliant trick is that we can choose D in a clever way so that both the sum of squares in $(*)$ and product-sum in $(**)$ become very nice to work with. This method is known as *dyadic decomposition.*

Since $r(l) \leq |A|$ for all l (there are $|A|$ possible x-coordinates of an intersection), we can divide our sum into $\log |A| + 1$ smaller sums,

$$\sum_{m \in A/A} r(l(m))^2 = \sum_{j=0}^{\log |A|} \underbrace{\left(\sum_{m \in (A/A)} r(l(m))^2 \cdot 1_{r(l(m)) \in [2^j, 2^{j+1})} \right)}_{A(j)}$$

Choose J such that $A(J)$ is maximal and let D be the set of lines $\{l(m) : r(l(m)) \in [2^J, 2^{J+1}]\}$

$$\begin{aligned}\sum_{m\in A/A} r(l(m))^2 &\le (\log|A|+1)\cdot A(J)\\ &\le 2\log|A|\cdot|D|2^{2(J+1)}\end{aligned}$$

For this choice of D, $(*)$ becomes,

$$|AA||D|2^{2J+3}\log|A| \ge |A|^4$$

And $(**)$ becomes,

$$\begin{aligned}|A+A|^2 &\ge (|D|-1)2^{2(J-1)}\\ &\ge |D|2^{2J-3}\end{aligned}$$

Combining these we have,

$$8|A+A|^2 \ge |D|2^{2J} \ge \frac{|A|^4}{8|AA|\log|A|}$$

and if we do the algebra on the LHS and RHS,

$$\begin{aligned}|A+A||A+A||AA| &\ge \frac{|A|^4}{64\log|A|}\\ \therefore\ \max\{|A+A|,|AA|\}^3 &\ge \frac{|A|^4}{64\log|A|}\\ \therefore\ \max\{|A+A|,|AA|\} &= \Omega\left(\frac{|A|^{4/3}}{(\log|A|)^{1/3}}\right)\\ &= \Omega\left(|A|^{4/3}\right) \quad \square\end{aligned}$$

2 Sums and Products in Groups

2.1 The Cauchy-Davenport Inequality for $\mathbb{F}_p$

We have asked questions about $\mathbb{R}$, which has additive and multiplicative structure. The nice behaviour of $\mathbb{R}$ meant that when we asked questions about $A+A$ or AA individually, they were generally easy to answer. If we try to generalise and instead consider a group $(G,\cdot)$ and ask how small $A\cdot A$ can be, this question is much harder. One simple example shows this situation can be quite different from $\mathbb{R}$. Trivially, for any $A\subseteq G$, $|A\cdot A|\ge|A|$. For a general group, this bound is (usually) sharp, because if we take A to be a subgroup of G, then $|A\cdot A|=|A|$. If G has no proper non-trivial subgroups, its no longer obvious what the minimum value of $|A\cdot A|$ should be. In the case where G is finite, this property implies G is isomorphic to $(\mathbb{F}_p,+)$, and this becomes a familiar problem.

Theorem 2.1. (Cauchy-Davenport)$_{[12]}$ For $A,B\subset\mathbb{F}_p$, $|A+B|\ge\min\{p,|A|+|B|-1\}$.

Proof. Induct on $|B|$ and assume $|B| \geq 2$ and $|A| < p$.

We may WLOG assume $0 \in B$. This is because $|A+B| = |A+B+k|$ for all k, so we can replace B with $B+k$ without changing $|B|$ or $|A+B|$. In particular we can take $k = -b$ for any $b \in B$. This is an important assumption and we will use it multiple times.

We first claim $|A+B| > |A|$. Suppose $|A+B| = |A|$, then $A+B = A$ since $0 \in B$.

Define $S(A) := \{h \in \mathbb{F}_p : A+h = A\}$, the *stabliser* of A. This is a subgroup of $\mathbb{F}_p$ and $B \subseteq S(A)$. Since $|B| \geq 2$, $S(A)$ is non-trivial. However, the only nontrivial subgroup of $\mathbb{F}_p$ is $\mathbb{F}_p$ itself. This is a contradiction because it implies $A = \mathbb{F}_p$: if $k \notin A$ then for any fixed $a \in A$,

$$\begin{aligned} k - a &\in S(A) \\ \therefore\ A + (k-a) &= A \\ \therefore\ a + (k-a) &\in A \\ \therefore k &\in A \end{aligned}$$

a contradiction. Therefore $|A+B| > |A|$.

The next idea is to notice that the "$|A| + |B| - 1$" term in the Cauchy-Davenport inequality is invariant if we remove some elements from B and add the same number of elements into A to get new sets A' and B'. If we do this in such a way that we do not create new sums i.e. $A' + B' \subseteq A + B$, then we would have,

$$|A+B| \geq |A'+B'| \geq \min\{|A'| + |B'| - 1, p\} = \min\{|A| + |B| - 1, p\} \quad (*)$$

by induction on $|B|$ and therefore the Cauchy-Davenport inequality would hold for A and B.

The correct surgical operation is called the e-transform of (A, B). Lets see how one might arrive at this.

We know $0 \in B$, so there are some elements of A in $A+B$. Also, there are some elements of $A+B$ not in A since $|A+B| > |A|$. In particular, we may suppose $a \in A$ has the property that $a+B$ is not a subset of $A+B$. The idea is to force these two types of elements to interact.

From a's point of view, there are two types of elements of B: there are some 'useless' elements of B which when summed with a, are still in A, i.e. $B_{\text{useless}} := \{b \in B : a+b \in A\}$, and there are 'useful' elements of B which when summed with a, are no longer in A, i.e. $B_{\text{useful}} := \{b \in B : a+b \notin A\}$.

The key observation is,

$$(a + B_{\text{useful}}) + B_{\text{useless}} \subseteq A + B \quad (\dagger)$$

Therefore, there is nothing stopping us from putting $a + B_{\text{useful}}$ into A, i.e. $A' = A \cup (a + B_{\text{useful}})$, and replacing B with B_{useless}, i.e. $B' = B_{\text{useless}}$. Since neither B_{useful} nor B_{useless} are empty, we are good to procceed by induction. We will spell out the details in the next lemmas.

□

Definition 2.2. Let A, B be subsets of $\mathbb{F}_p$ with $0 \in B$ and $e \in A$. The e-transform of (A, B), is the pair

(A', B') where

$$\begin{aligned} B_{\text{useless}} &:= \{b \in B : e + b \in A\} \\ B_{\text{useful}} &:= \{b \in B : e + b \notin A\} \\ A' &:= A \cup (e + B_{\text{useful}}) \\ B' &:= B_{\text{useless}} \end{aligned}$$

Lemma 2.3. The e-transform has the following properties

(i) $|A| + |B| = |A'| + |B'|$

(ii) $|A| \geq |A'|$ and $0 < |B'| \leq |B|$ with equality iff $e + B \subseteq A$

(iii) $A' + B' \subseteq A + B$

Proof.
(i) Since A and $e + B_{\text{useful}}$ are disjoint by definition of B_{useful}, $|A'| = |A| + |B_{\text{useful}}|$. Also, $|B'| = |B_{\text{useful}}|$. Thus $|A| + |B| = |A'| + |B'|$.

(ii) $|B'| > 0$ since $0 \in B_{\text{useless}}$. The rest of the inequalities follow from the proof of (i).

(iii) $A' = A \cup (e + B_{\text{useful}})$, so it suffices to consider each term in the union separately and show,

(a) $A + B' \subseteq A + B$ (obviously true as $B' \subseteq B$)

(b) $(e + B_{\text{useful}}) + B' \subseteq A + B$

For (b), suppose $b \in B_{\text{useful}}$ and $b' \in B_{\text{useless}}$. Then

$$\begin{aligned} (e + b) + b' &= (e + b') + b \\ &= a + b \quad \text{(for some } a \in A \text{ by definition of } B_{\text{useless}}) \\ &\in A + B \\ \therefore A' + B' &\subseteq A + B \end{aligned}$$

as required.

□

Corollary 2.3.1. (Cauchy-Davenport in the language of e-transforms) For $A, B \subset \mathbb{F}_p$,

$$|A + B| \geq \min\{p, |A| + |B| - 1\}$$

.

Proof. Induct on B. We have already shown $|A + B| > |A|$ and WLOG $0 \in B$. Since $A + B$ is not a subset of A, there exists $a \in A$ such that $a + B$ is not a subset of A. Let (A', B') be the e-transform of (A, B) by a. Since $a + B$ is not a subset of A, we know $|B'| < |B|$ and $A' + B' \subseteq A + B$. Then by induction,

$$|A + B| \geq |A' + B'| \geq \min\{p, |A'| + |B'| - 1\} = \min\{p, |A| + |B| - 1\}$$

□

One interesting remark is that e-transforms had very little to do with $\mathbb{F}_p$. All we really required was an abelian group. Indeed, if $(G, +)$ is an abelian group with identity element 0, we can replace '$\mathbb{F}_p$' with 'G' and the lemma and definition of e-transforms still holds. The only place we used the fact that p is prime was to prove $|A + B| > |A|$, so we can try to generalise. Since we're doing induction, we also assumed (and used) the fact that $|A' + B'| > |A'|$, so our generalisation is not as simple as one might hope.

Corollary 2.3.2. Fix k and let $(G, +)$ be an abelian group such that for all $A, B \subset G$ with $1 < |B| < k$, we have $|A + B| > |A|$. Then in fact, $|A + B| \geq \min\{|G|, |A| + |B| - 1\}$.

(N.B. the case where A or B is infinite is trivial)

This means, provided G has the property for k, sum sets involving subsets cardinality at most k have gap in the possible cardinality for the sum set. Later we will see an incredible result that says we can take k to equal the size of the smallest subgroup of G for *any* group G (abelian or not) and the conclusion of Corollary 2.3.2 remains true.

To prove $\mathbb{F}_p$ had the property that $|A + B| > |A|$ for all $A, B \subset \mathbb{F}_p$, we only needed to show that $S(A)$, a subgroup of $\mathbb{F}_p$, must be trivial whenever $A \neq \mathbb{F}_p$. This was easy because $\mathbb{F}_p$ only has two subgroups, the trivial group and itself. Sadly, the only finite groups with this property are precisely the $\mathbb{F}_p$ by Cauchy's theorem. However, we can adapt our proof to a large class of infinite groups.

Definition 2.4. A group is *torsion-free* if it is infinite with no non-trivial finite subgroups

Lemma 2.5. If $(G, +)$ is a group and $A \subset G$ is finite, then $S(A)$ is finite. In particular if G is torsion-free, then $S(A)$ is the trivial group.

Proof. If $h \in S(A)$ then $A \cdot h = A$. In particular, for some $a, b \in A$, $ah = b$. Thus $h \in A^{-1} \cdot A$ (where $A^{-1} := \{a^{-1} : a \in A\}$ has cardinality $|A|$), and $|A^{-1} \cdot A| \leq |A|^2$ therefore $|S(A)| \leq |A|^2$. Since $S(A)$ is finite and the only finite subgroup of a torsion-free group is the trivial group, we are done. □

Corollary 2.5.1. Let $(G, +)$ be a torsion-free abelian group. Then $|A + B| \geq |A| + |B| - 1$ for all $A, B \subset G$. In other words, the Cauchy-Davenport inequality holds in G.

2.2 The Cauchy-Davenport Inequality for Groups

We previously saw that if G has a finite non-trivial proper subgroup A, then the Cauchy-Davenport inequality fails because $|A + A| = |A| < 2|A| - 1$. It turns out that these are in some sense the 'worst' examples.

Definition 2.6. We say a group $(G, \cdot)$ is *Cauchy-Davenport-like* if for all $A, B \subset G$, $|A \cdot B| \geq \min\{p(G), |A| + |B| - 1\}$ where $p(G)$ is the size of the smallest non-trivial subgroup of G (or equivalently if G is finite, the smallest prime divisor of $|G|$).

For example, we just proved all torsion-free abelian groups are Cauchy-Davenport-like. This inequality is trivial when $|A|$ or $|B|$ are greater than or equal to the cardinality of the smallest non-trivial subgroup of G. In particular, the inequality now holds when A is a subgroup. It is no longer clear how we would come up with a group which doesn't satisfy this condition, and it turns out there are none!

Theorem 2.7. (Kneser 1953)[12] If G is an abelian group, then G is Cauchy-Davenport-like.

Theorem 2.8. (Károlyi 2005)[13] If G is a finite group, then G is Cauchy-Davenport-like

Theorem 2.9. (Ruzsa 2009)[14] If G is a group, then G is Cauchy-Davenport-like

Kneser's theorem is slightly more than what is written here and says a more general fact involving the stabiliser subgroup $S(A)$. Károlyi's proof requires deep facts about the 'solvability' of a group. We will showcase here a surprisingly elementary proof of Ruzsa's result.

Theorem 2.10. (DeVos 2016)[15] If $(G, \cdot)$ is a group, then G is Cauchy-Davenport-like

Proof. Suppose $A, B \subset G$ with $|A|, |B| < p(G)$ is a counterexample to the Cauchy-Davenport-like inequality, i.e. $|A \cdot B| \leq \min\{p(G), |A| + |B| - 1\}$. We may assume,

1. $|A \cdot B|$ is minimum
2. $|A| + |B|$ is maximal subject to 1
3. $|B|$ is minimum subject to 1 and 2

It follows that $|B| \leq |A|$, otherwise the pair (B^{-1}, A^{-1}) satisfies 1 and 2, but contradicts minimality of 3.

Assume $|B| \geq 2$. The plan here is the same as in the proof of Cauchy-Davenport. We will come up with a new pair (A', B') such that $A' \cdot B' \subseteq A \cdot B$, but $|A'| + |B'| \leq |A| + |B|$ and $|B'| < |B|$, contradicting our minimality assumptions.

Fix $g \in G \backslash \{1\}$ such that $gB \cap B$ is non-empty. For example, if $x, y \in B$, then we can take $g = yx^{-1}$, then $y \in gB$, so $gB \cap B \neq \emptyset$. If $gB = B$, then $g^n Bg = B$ for all $n \in \mathbb{N}$. Fix $b \in B$. Then for every $0 \leq n < \text{order}(g)$, $g^n b$ are distinct and contained in B. But $|B| < p(g) \leq \text{order}(g)$ by assumption, a contradiction. Thus $B \cap gB$ is a proper nonempty subset of B.

Our candidate for B' will be $B \cap gB$. It is certainly the case that $A \cdot (B \cap gB) \subseteq A \cdot B$, however, we need to make A bigger otherwise we have no hope of contradicting minimality assumption 2. Fortunately, we can make A bigger. If $ag^{-1} \in Ag^{-1}$, then for any $gb \in B \cap gB$ we have $ag^{-1}gb \in A \cdot B$. Thus,

$$(A \cup Ag^{-1}) \cdot (B \cap gB) \subseteq A \cdot B$$

and so our candidate pair is $(A', B') = (A \cup Ag^{-1}, B \cap gB)$.

We know that $|B'| < |B|$ and $|A' \cdot B'| \leq |A \cdot B|$, so to contradict minimality of (A, B), all we need to show is

(a) (A', B') does not satisfy the Cauchy-Davenport-like inequality

(b) $|A'| + |B'| \geq |A| + |B|$

In fact, all we need to show is (b), because (b) $\implies$ (a). Indeed, if $|A'| + |B'| \geq |A| + |B|$, then

$$|A' \cdot B'| \leq |A \cdot B| \leq \min\{p(G), |A| + |B| - 1\} \leq \min\{p(G), |A'| + |B'| - 1\}$$

Thus (A', B') would be a counterexample to the Cauchy-Davenport-like inequality.

Sadly, we have no reason to believe (b) is true. All we know is B' is non empty, it could be tiny, and we have no control over the size of $|A'|$ either. The key idea that will save us (and the real reason why (A', B') was a great pair to look at) is,

$$|B \cap gB| + |B \cup gB| = 2|B|$$

If B' is small, then $B \cup gB$ is big. Similarly for A',

$$|A \cup Ag^{-1}| + |A \cap Ag^{-1}| = 2|A|$$

Altogether,

$$(|A'| + |B'|) + (|\underbrace{A \cap Ag^{-1}}_{A''}| + |\underbrace{B \cup gB}_{B''}|) = 2(|A| + |B|) \qquad (\triangle)$$

If (A', B') didn't work out (i.e. (b) didn't hold), our new candidate counterexample will be (A'', B''), which is like a flipped around version of (A', B'). There are a few things to check,

(i) A'' is non-empty.

(ii) $|A'' \cdot B''| \leq |A \cdot B|$

(iii) $|A''| + |B''| > |A| + |B|$

(iv) (A'', B'') does not satisfy the Cauchy-Davenport-like inequality

If we can show all of these (under the assumption (b) does not hold), then (A'', B'') contradicts minimality condition 2 of (A, B) and we can conclude that G is Cauchy-Davenport-like.

(i) holds because,

$$\begin{aligned} |A'| + |B'| &< |A| + |B| \\ &\leq 2|A| \\ \therefore |A'| &< 2|A| \end{aligned}$$

Since $A' = A \cup Ag^{-1}$, it follows that A and Ag^{-1} cannot be disjoint, thus A'' is non-empty

(ii) holds by the same argument used to show $A' \cdot B' \subseteq A \cdot B$.

(iii) holds by applying (b) to $(\triangle)$

(iv) is implied by (ii) and (iii) as we saw for (A', B')

□

2.3 Balog-Szemerédi-Gowers Theorem

Recall, that for $A \subset \mathbb{R}$, we defined the 'multiplicative energy' of A as,

$$E_\times(A) = \{(a, b, c, d) \in A^4 : ab = cd\}$$

We can generalise this idea to groups.

Definition 2.11. If $(G, +)$ is an abelian group and $A \subset G$, we define the *additive energy* of A as,

$$E(A) := |\{(a, b, c, d) \in A^4 : a + b = c + d\}|$$

If G is written multiplicatively, we refer to the same quantity as the *multiplicative energy.*

Previously we noted that $E(A)$ and $|A + A|$ are obviously related, and Lemma 1.6 quantified that with the bound $|A + A|E(A) \geq |A|^4$. This was in $\mathbb{R}$, but our argument works in a general group G.

Theorem 2.12. **($|A+A|$ and $E(A)$ cannot both be small)** If $(G,+)$ is an abelian group and

$$|A+A|E(A) \geq |A|^4$$

(N.B. G need not even be abelian, but we will focus on abelian groups in this section)

This bound does not tell us that we cannot have both $|A+A|$ and $E(A)$ large. In the next lemma, we will give the largest possible asymptotic orders for $|A+A|$ and $E(A)$ and show that these can be obtained simultaneously.

Lemma 2.13. **($|A+A|$ and $E(A)$ can be as large as possible simultaneously[11])**

(i) $|A| \leq |A+A| \leq |A|^2$, so the largest asymptotic order is $|A+A| = \Theta(|A|^2)$

(ii) $E(A) \leq |A|^3$, so the largest asymptotic order is $E(A) = \Theta(|A|^3)$

(iii) In $G = \mathbb{R}$, it is possible to have both $|A+A|$ and $E(A)$ asymptotically as large as possible simultaneously for $|A|$ arbitrarily large. In other words, there is a sequence of sets A_n with $|A_n| \to \infty$, $|A_n + A_n| = \Theta(|A_n|^2)$, and $E(A_n) = \Theta(|A_n|^3)$.

Proof. We have mostly seen these results already

(i) For the lower bound, pick any $a \in A$, then $|a+A| = |A|$. Also $a + A \subseteq A + A$. Thus $|A+A| \geq |A|$.

For the upper bound, there is a surjection from $A \times A$ to $A+A$ by $(a,a') \to a + a'$. Thus $|A+A| \leq |A|^2$.

(ii) By Theorem 2.12, $|A+A|E(A) \geq |A|^4$. Since $|A+A| \geq |A|$, we have $E(A) \leq |A|^3$.

(iii) Fix n and let $A = A_n$. The idea is to write $A = B \sqcup C$ for some $B = B_n$ and $C = C_n$ such that

(a) $|B|$ and $|C|$ equal $\frac{1}{2}|A|$ (or at least on the order of $|A|$ for all n)

(b) $E(B)$ is large, i.e. $E(B) = \Theta(|B|^3)$

(c) $|C+C|$ is large, i.e. $|C+C| = \Theta(|C|^2)$

Then (a) implies $E(B) = \Theta(|A|^3)$ and $|C+C| = \Theta(|A|^2)$. Since $E(A) \geq E(B)$ and $|A+A| \geq |C+C|$, it follows that $E(A) = \Theta(|A|^3)$ and $|A+A| = \Theta(|A|^3)$.

Let us give an explicit construction in $\mathbb{R}$. In Section 1.1 we saw $C := \{2, \ldots, 2^n\}$ maximises $|C+C|$ and $B := \{1, \ldots, n\}$ minimises $|B+B|$ to $\Theta(|B|)$. Therefore by Theorem 2.12, $E(B) = \Theta(|B|^3)$. To ensure B and C are disjoint, we can instead consider $B := \{2^n+1, \ldots, 2^n+n\}$. These sets satisfy (b) and (c), so we can define $A = B \sqcup C$.

□

Another way of thinking about our construction for (iii) is: We have a set B which has high additive energy, but $|B+B|$ is very small (minimal even in our case). We add some new elements to B (i.e. union C to get A) to pump up $|B+B|$ to maximality, and we don't need to add that many new elements, so $E(B)$ is still maximal relative to the new size of the set. However, we still have this huge subset $B \subset A$, which has $|B+B|$ small. The question the Balog-Szemerédi-Gowers theorem aims to answer is, if A has $E(A)$ and $|A+A|$ large, must there be a big subset B of A with $|B+B|$ small?

Theorem 2.14. **(Balog-Szemerédi-Gowers[11])** Let A be a finite subset of an abelian group $(G,+)$ with $E(A) = \Theta(|A|^3)$. Then there is a large subset $B \subseteq A$ with $|B+B| = \Theta(|B|)$.

More precisely, if for some $K > 1$,

$$E(A) \geq |A|^3/K \qquad \text{(i.e. } E(A) \text{ big)}$$

then there is a $B \subseteq A$ with

$$\begin{aligned} |B| &\geq K^{-c}|A| \qquad (|B| \text{ big}) \\ \text{and } |B+B| &\leq K^{c'}|B| \qquad (|B+B| \text{ small}) \end{aligned}$$

where c and c' are constants dependent only on K.

Originally this theorem was proven by Balog and Szemerédi, but their proof makes c and c' very large compared to K. The improvement due to Gowers made these constants much more practical. The actual result proven by Gowers doesn't look related to this question at all. In fact, it is much stronger. We will state it, then show that it does in fact imply Theorem 2.14.

Theorem 2.15. (Gowers[16]) Fix $K > 1$ and let A and A' be a finite non-empty subsets of the same abelian group with $|A| = |A'|$ and let X be a subset of $A \times A'$ with

$$|X| \geq |A||A'|/K \qquad (\text{i.e. } X \text{ is a big subset of } A \times A')$$

Define

$$E_X(A, A') := |\{a + a' : (a, a') \in X\}|$$

and suppose

$$E_X(A, A') \geq |A|^3/K \qquad (\text{i.e. } E_X(A, A') \text{ is large})$$

Then there exist $B \subseteq A$ and $B' \subseteq A'$ with

$$\begin{aligned} |B| &\geq cK^{-c}|A| \\ |B'| &\geq cK^{-c}|A'| \end{aligned}$$

for some absolute constant c (i.e. they are large subsets) such that for every $b \in B$ and $b' \in B'$, there are at least $cK^{-c}|A|^5$ solutions $(b_1, b_2, b_3, b_1', b_2', b_3') \in B^3 \times B'^3$ to the equation

$$b - b' = (b_1 - b_1') - (b_2 - b_2') + (b_3 - b_3').$$

To show Gowers' Theorem implies BSG, we will need two lemmas which we will not prove.

Lemma 2.16. (Plünnecke's Inequality[11]) Let X be a finite subset of an abelian group. Then for any $K > 0$,

$$|X - X| \leq K|X| \implies |X + X| \leq K^2|X|$$

[We'll see a much stronger form of Plünnecke's Inequality later]

Lemma 2.17. (Ruzsa Triangle Inequality[11]) If X, Y, Z are finite subsets of the same abelian group, then

$$|X||Y - Z| \leq |X - Y||X - Z|.$$

[If we define $\rho(A, B) = \log \frac{|A-B|}{\sqrt{|A||B|}}$, the 'Ruzsa distance', then the Ruzsa Triangle Inequality says $\rho(B, C) \leq \rho(B, A) + \rho(A, C)$]

Corollary 2.17.1. (Gowers' theorem implies BSG[11])

Proof. Assume the hypothesis of BSG, so we have A, a subset of an abelian group, and $K > 1$ such that

$$E(A) \geq |A|^3/K.$$

Let $A' = A$ and $X = A \times A$. Then

$$\begin{aligned} E_X(A, A') &= E(A) \\ &\geq |A|^3/K \end{aligned}$$

By Gowers' theorem, there exist large subsets $B, B' \subseteq A$ such that for any $b, b' \in B$, there are at least $cK^{-c}|A|^5$ solution tuples to the equation,

$$b - b' = (b_1 - b_1') - (b_2 - b_2') + (b_3 - b_3') \qquad (*)$$

So for each element of $B - B'$ on the LHS, we have a large set of solution tuples. For different elements of $B - B'$, these sets are disjoint. Also, each of these solution tuples lives inside $|A|^6$. Thus,

$$\begin{aligned} |B - B'| \times cK^{-c}|A|^5 &\leq |A|^6 \\ \therefore\ |B - B'| &\leq \frac{1}{c}K^c|A| \quad (\dagger) \end{aligned}$$

Now we will use the previous two lemmas to show B satisfies the conclusion of BSG. By the Ruzsa Triangle inequality with $X = B'$ and $Y = Z = B$,

$$|B'||B - B| \leq |B' - B|^2$$

Putting this into (†),

$$\begin{aligned} |B'||B - B| &\leq \frac{1}{c^2}K^{2c}|A|^2 \\ |B - B| &\leq CK^C|A| \qquad \text{(because } |B'| \geq cK^{-c}|A|) \end{aligned}$$

where C is a new absolute constant.

By Plünnecke's inequality,

$$\begin{aligned} |B + B| &\leq C^2K^{2C}|A| \\ &\leq K^{c'}|A| \qquad \text{(for some absolute } c' > 2C) \end{aligned}$$

Recall $|B| \geq cK^{-c}|A|$, thus $|B| \geq K^{-\bar{c}}|A|$ for some $\bar{c}$ absolute. Therefore B satisfies the Balog-Szemerédi-Gowers (Theorem 2.14) conclusion as required and the constants $\bar{c}$ and c' are absolute. □

3 Sums and Products in $\mathbb{F}_p$

3.1 Overview

The Cauchy-Davenport inequality gave an answer to how small sum-sets can be in $\mathbb{F}_p$, but we are yet to consider the multiplicative structure of the field. In this section, we will explore some similar problems which will serve as useful lemmas in later sections.

3.2 Dilated Cauchy-Davenport

Over a (not necessarily prime order) finite field F, the minimum of $|A+B|$ is trivially attained when $A=B$ is a subfield. One way we can make this question interesting is to ask how small is $\max\{|A+\xi B| : \xi \in F^\times\}$?. This extra ξ dilation factor means that subfields are now terrible examples, because if $A=B<F$, consider any $\xi \notin A$. Then $a+\xi b$ is unique for every $a,b \in A$, thus the dilated sumset is maximal. Indeed, if $a+\xi b = a'+\xi b'$, then $a-a' = \xi(b'-b)$. If $a=a'$ or $b=b'$, then $a=a'$ and $b=b'$. Otherwise, $\xi = (a-a')(b'-b)^{-1} \in A^\times$, a contradiction.

Theorem 3.1. (Dilated Cauchy-Davenport)[12] Let A,B be finite non-empty subsets of a finite field F. Then

$$\max_{\xi \in F^\times} |A+\xi B| \geq \min\{\frac{1}{2}|A||B|, \frac{1}{10}|F|\} \qquad (*)$$

Proof. Note this lower bound is huge compared to our previous results.

Suppose $|A||B| > \frac{1}{2}|F|$. Then $\min\{\frac{1}{2}|A||B|, \frac{1}{10}|F|\} = \frac{1}{10}|F|$ because $|A||B| \geq \frac{1}{5}|F|$. We could remove some elements from A and B such that $|A'||B'| \geq \frac{1}{5}|F|$ still, but $|A'||B'| < \frac{1}{2}|F|$. Since this doesn't change the LHS of $(*)$ and $|A'+\xi B'| \leq |A+\xi B|$ for all ξ, we may WLOG assume $|A||B| \leq \frac{1}{2}|F|$.

Let $\xi \in F^\times$. Consider the sets $C_a(\xi) = a+\xi B$ for every $a \in A$. We will perform the inclusion-exclusion principle on them.

$$\begin{aligned} |A+\xi B| &= \left|\bigcup_{a\in A} C_a\right| \\ &\geq \sum_{a\in A}|C_a| - \frac{1}{2}\sum_{a,a'\in A, a\neq a'}|C_a \cap C_{a'}| \qquad \text{(inclusion-exclusion principle)} \end{aligned}$$

Lets look at each term separately. Since ξ is invertible,

$$\begin{aligned} |B| &= |C_a| \quad (\forall a) \\ \therefore \sum_{a\in A}|C_a| &= |A||B| \end{aligned}$$

and

$$\begin{aligned} \sum_{a,a'\in A, a\neq a'}|C_a \cap C_{a'}| &= \sum_{a,a'\in A: a\neq a'}\left(\sum_{b,b'\in B} 1_{a+b\xi = a'+b'\xi}\right) \\ &= \sum_{a,a'\in A: a\neq a'}\ \sum_{b,b'\in B: b'\neq b} 1_{\xi=(a-a')^{-1}(b'-b)} \end{aligned}$$

The trick here is to notice that we have no idea if our fixed ξ satisfies $(a-a')^{-1}(b'-b)$, but we know $(a-a')^{-1}(b'-b)$ equals something in $F^\times$. So, if we sum over all $\xi \in F$, for any (a,a',b,b'), there will be exactly one ξ equal to $(a-a')^{-1}(b'-b)$.

$$\begin{aligned}\sum_{\xi \in F^\times} \sum_{a,a' \in A, a \neq a'} |C_a(\xi) \cap C_{a'}(\xi)| &= \sum_{a,a' \in A : a \neq a'} \sum_{b,b' \in B : b' \neq b} \sum_{\xi \in F^\times} 1_{\xi = (a-a')^{-1}(b'-b)} \\ &= \sum_{a,a' \in A : a \neq a'} \sum_{b,b' \in B : b' \neq b} 1 \\ &\leq |A|^2 |B|^2\end{aligned}$$

Putting this all into the inclusion-exclusion inequality,

$$\begin{aligned}\sum_{\xi \in F^\times} |A + \xi B| &\geq \sum_{\xi \in F^\times} |A||B| - \frac{1}{2}|A|^2|B|^2 \\ \therefore \frac{1}{|F^\times|} \sum_{\xi \in F^\times} |A + \xi B| &\geq |A||B| - \frac{|A|^2|B|^2}{2(|F|-1)} \\ &\geq |A||B| - \frac{|A|^2|B|^2}{2(|F|/2)} \\ &\geq \frac{1}{2}|A||B| \qquad \text{(We assumed } |A||B| \leq \frac{1}{2}|F|\text{)}\end{aligned}$$

Since the average of $|A + \xi B|$ over all $\xi \in F^\times$ (the LHS) is at least $\frac{1}{2}|A||B|$, there must be some ξ^* with $|A + \xi^* B| \geq \frac{1}{2}|A||B|$.

□

3.3 Bounds on $|p(A)|$ for a polynomial p

We've seen $|A + A| = O(|A|^2)$. A very similar argument would show $|A + A + A| = O(|A|^3)$, and extend to more terms. We can make this question more interesting though. If $|A + A|$ is small compared to $|A|$, then we would expect $|A + A + A|$ to also be small compared to $|A|$ too. Our next lemma quantifies this notion.

Lemma 3.2. (Plünnecke–Ruzsa Inequality$_{[11]}$) Let A, B be non-empty finite subsets of the same abelian group such that $|A + B| \leq K \min(|A|, |B|)$. Then,

$$|A \pm A \cdots \pm A| \leq CK^C|A|$$

where C is a constant dependent only on the length of the additive combination.

In particular, note the case when $B = A$ and the additive combination is $A + A + A$, which shows our initial expectation was correct. Also note the case when $B = -A$ and the additive combination is $A + A$, we retreive Lemma 2.16 (Plünnecke's inequality). Indeed, this result underpins many fundamental results in additive combinatorics. The proof relies on the Lemma 2.17 (Ruzsa Triangle Inequality).

One thing we have not talked about yet is combinations of sum sets and product sets. For example, $|AA + A|$. These naturally lead to polynomials. There is a rich theory about these combinations, but surprisingly we will only need to quantify the intuitive claim that if $|A + A|$ and $|AA|$ are small, then $|AA + AA|$ is small (or equivalently, by Plünnecke, $|AA - AA|$ is small). Although the claim is intuitive, the proof is far from simple and requires Gowers' Theorem (Theorem 2.15).

Lemma 3.3. Suppose $A \subset F$ satisfies

$$|A+A|, |AA| \leq K|A|$$

Then there is a large subset $A' \subseteq A$ with

$$|A'| \geq cK^{-C}|A|$$
$$|A'A' - A'A'| \leq CK^{C}|A'|$$

for some absolute constants c and C.

The proof of the bound of $|p(A)|$ is really about this well behaved subset $A' \subset A$. We will only attempt to bound $|p(A')|$. To obtain the bound, we say $x \in F$ is *good* if $xA \subset S + (A - A)$ for some small set S of cardinality $|S| \leq CK^{C}$. Using the fact that $|A'A' - A'A'|$ is small, one can show that every element of A' is good and if x and y are good, then so are $x \pm y$ and xy. Therefore, every element of $p(A')$ is good.

Theorem 3.4. (Polynomial Bound$_{[12]}$) Suppose $A \subset F$ and A' is the set obtained from Lemma 3.3. Then for any polynomial p of several variables and integer coefficients, we have

$$|p(A', \dots, A')| \leq CK^{C}|A|$$

3.4 The Sum-Product Estimate

One of the main results about sum sets and product sets in $\mathbb{F}_p$ is the Sum-Product Estimate. It is answers one version of the Erdős-Szemerédi problem framed in $\mathbb{F}_p$ instead of $\mathbb{R}$. The proof relies on Theorem 3.1 (Dilated Cauchy-Davenport) and Theorem 3.4 (Polynomial Bound).

Theorem 3.5. (Bourgain-Katz-Tao$_{[12]}$) Let $A \subset \mathbb{F}_p$ such that

$$p^{\delta} < |A| < p^{1-\delta}$$

for some $\delta > 0$. Then,

$$\max\{|A+A|, |AA|\} \geq c|A|^{1+\epsilon}$$

for some positive constants c and ϵ depending only on δ.

Recall that the first result in $\mathbb{R}$ by Erdős-Szemerédi took this form. One can show that this result is a lot tougher to improve. In [17] it is shown that for every p, there is a subset $A \subset \mathbb{F}_p$ such that $\max\{|A+A|, |AA|\} = o(|A|^{3/2})$, which is much smaller than $|A|^2$, and so it is difficult to imagine a meaningful translation of the Erdős-Szemerédi conjecture from $\mathbb{R}$ into the prime order fields.

In [12] many interesting corollaries of Theorem 3.5 are obtain. In particular, one can prove a version of Lemma 1.6 (Szemerédi-Trotter) for finite fields.

4 Bibliography

[1] K. Ford, The distribution of integers with a divisor in a given interval, Annals of Math. (2) 168 (2008), 367-433.

[2] P. Erdős, E. Szemerédi, On sums and products of integers, Studies in pure mathematics, 213–218, Birkhauser, Basel, 1983.

[3] A. Sheffer, The Sum Product Problem

[4] M. Nathanson, On sums and products of integers, Proceedings of the American Mathematical Society 125 (1997), 9–16.

[5] K. Ford, Sums and products from a finite set of real numbers, The Ramanujan Journal 2 (1998), 59–66.

[6] G. Elekes, On the number of sums and products, Acta Arith. 81 (1997), 365–367.

[7] J. Solymosi, On the number of sums and products, Bulletin of the London Mathematical Society 37 (2005), 491–494.

[8] J. Solymosi, Bounding multiplicative energy by the sumset, Advances in mathematics 222 (2009), 402–408.

[9] S. Konyagin and I. D. Shkredov, New results on sum-products in R arXiv:1602.03473.

[10] E. Szemerédi and W Trotter, Extremal problems in discrete geometry, Combinatorica 3 (1983), 381–392.

[11] Y. Zhao, Graph Theory and Additive Combinatorics

[12] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press (2006) p200

[13] G. Károlyi, The Cauchy-Davenport theorem in group extensions, L'Enseignement Mathématique 51 (2005), 239-254.

[14] Geroldinger, Alfred; Ruzsa, Imre Z., eds. (2009). Combinatorial number theory and additive group theory.

[15] DeVos, Matt, On a Generalization of the Cauchy-Davenport Theorem (2016)

[16] T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Funct. Anal. 8 (1998), no. 3, 529–551

[17] F. de Zeeuw, A course on sum-product bounds (2017)