Additive Combinatorics

Harry Armitage

January 30, 2021

Contents

1 Elementary Tools

Asymptotic notation: for functions f, g we will write $f = O(g)$ to mean there is a constant $c > 0$ such that, for large enough x, $|f(x)| \leq c|g(x)|$. Sometimes, we will write $f = O_h(g)$ if c depends on h. We will also sometimes write $f \ll g$ to mean $f = O(g)$ (or indeed $g \gg f$, or $f \ll_h g$). We will also write such things as $(x+h)^2 = x^2 + O_h(x)$. We will often write $\log X$ - it will typically be irrelevant which base, but it will be assumed that X is large.

All sets will be finite and nonempty unless otherwise specified. Usually, they will be subsets of some abelian group, denoted by G. If finite, we will write $N = |G|$, for instance $G = \mathbb{Z}/N\mathbb{Z}$ or $\mathbb{F}_p^n$ (where $N = p^n$). Much of what we do is valid for any abelian group, some of it only for finite groups, and some only for specific groups. Often, it can be generalised and sometimes not - e.g. $\mathbb{F}_p^n$ vs $\mathbb{Z}/N\mathbb{Z}$.

We will write $\mathbb{1}_A(x)$ for the indicator function on a subset $A \subseteq G$, i.e. $\mathbb{1}_A(x) = 1$ if $x \in A$, and 0 if not. We also define the convolution of functions $f, g : G \to G$ by

$$(f * g)(x) = \sum_{y \in G} f(y)g(x-y) = \sum_{y+z=x} f(y)g(z)$$

We define the "difference convolution" by

$$(f \circ g)(x) = \sum_{z \in G} f(x+z)g(z) = \sum_{y-z=x} f(y)g(z)$$

We define an inner product on function $G \to \mathbb{C}$ by

$$\langle f, g \rangle = \sum_{x \in G} f(x)\overline{g(x)}$$

We have the trivial but useful adjoint property that

$$\langle f * g, h \rangle = \langle f, h \circ \bar{g} \rangle$$

which follows from $x + y = z \iff x = z - y$.

2 Sum Sets

Given $A, B \subset G$ we define

$$A + B \coloneqq \{a + b : a \in A, b \in B\}$$
$$A - B \coloneqq \{a - b : a \in A, b \in B\}$$

Note that these are set operations, and don't necessarily follow any nice algebraic properties. For instance $(A + B) - B \neq A$, and in general is a much larger set.

We have trivial bounds $|A| \leq |A + B| \leq |A||B|$ - the first follows as, for fixed b, $\{a + b : a \in A\}$ is a set of size $|A|$ contained in $A + B$, and the second follows as $+$ is a surjection $A \times B \twoheadrightarrow A + B$.

When $A = B$, this surjection maps (a_1, a_2) and (a_2, a_1) to the same element, and hence $|A + A| \leq \frac{|A|(|A|+1)}{2} = \frac{1}{2}|A|^2 + O(|A|)$.

Are these trivial bounds sharp?

If A is a subgroup, then $|A + A| = |A|$ (or if A is a coset of a subgroup).

If $A = \{1, 2, 4, \ldots, 2^k\}$, then $|A + A| = \frac{|A|(|A|+1)}{2}$, as all pairwise sums are distinct. We can also have $A = \{1, 4, 16, \ldots, 2^{2k}\}$, $B = \{2, 8, \ldots, 2^{2k+1}\}$, and get $|A + B| = |A||B|$.

Lemma 2.1. $|A + A| \leq |A| \iff$ *A is a coset of a subgroup.*

Proof. Since both properties are invariant under translation, without loss of generality take $0 \in A$. So $A \subseteq A + A$, so since $|A + A| = |A|$, we must have $A = A + A$. Hence A is closed under addition. For any $a \in A$ there are $|A|$ many distinct translates $a + a'$ for $a' \in A$. By closure, these are all in A, and so one must be 0. Hence $a + a' = 0$, and we have inverses. □

In groups where there are many finite subgroups, we have many A such that $|A + A| = |A|$. What about in $\mathbb{Z}$? Here, there are no nontrivial finite subgroups, and so this result tells us that, if $|A| > 1$, then $|A + A| > |A|$.

Lemma 2.2. *If $A \subset \mathbb{Z}$ then $|A + A| \geq 2|A| - 1$. Equality holds if and only if A is an arithmetic progression (i.e. $|A + A| < 2|A| \implies$ A is an arithmetic progression).*

Proof. Suppose we order A like $\{a_1 < a_2 < \ldots a_n\}$. This induces an ordering on some elements of $A + A$:

$$2a_2 < a_1 + a_2 < a_1 + a_3 < \ldots < a_1 + a_n < a_2 + a_n < a_3 + a_n < \ldots < 2a_n$$

This gives $2n - 1$ distinct sums in $A + A$.

For the second part, it suffices to show that if equality holds then, for any $1 \leq i < n$ there is some $j > i$ with $a_j - a_i = a_2 - a_1$, as then $a_j = a_1 + (j - 1)(a_2 - a_1)$, and we have an arithmetic progression.

Consider for $2 \leq i < n$, the sum $a_2 + a_i \in A + A$. Since $|A + A| = 2n - 1$, the above ordered list is all of $A + A$, and so one of them is $a_2 + a_i$. Since $i < n$, $a_2 + a_i < a_j + a_n$ for all $2 \leq j \leq n$, and so $a_2 + a_i = a_1 + a_j$. □

What about if $A \subseteq \mathbb{F}_p$, for p a prime?

Lemma 2.3 (Cauchy-Davenport)**.** *If $A, B \subset \mathbb{F}_p$, then $|A + B| \geq \min(|A| + |B| - 1, p)$.*

Proof. We fix $B \subset \mathbb{F}_p$, and then prove the inequality for all $A \subset \mathbb{F}_p$ by induction on $|B|$.

When $|B| = 1$, this is trivial, since $|A + B| = |A| = \min(|A|, p)$.

Suppose that $|B| \geq 2$, so we have $b_1 \neq b_2$ distinct elements of B, and let $z = b_1 - b_2 \neq 0$. If $A + z \subset A$ then, for any fixed $a \in A$, we have $a + z \in A$, so $a + kz \in A$ for all $k \in \mathbb{N}$ by induction on k. Hence $A = \mathbb{F}_p$, as $\mathbb{F}_p$ is cyclic, and so we are done as $|A + B| = p = \min(|A| + |B| - 1, p)$.

Otherwise, $A + z \nsubseteq A$, and so there exists $a \in A$ such that $a + z \notin A$. Let $x = a - b_1$. Then $B + x$ contains some element not in A, namely $a + z = b_2 + x$, and some element in A, namely $a = b_1 + x$.

So $1 \leq |A \cap (B + x)| < |B|$. Now note that:

$$A + B \supseteq ((A - x) \cup B) + (A \cap (B + x))$$

To verify this, if $a' + b' \in RHS$, then either:

1. $a' \in A - x$. Then since $b' \in B + x$, $a' + b' \in A + B - x + x = A + B$.
2. $a' \in B$. Then since $b' \in A$, $a' + b' \in A + B$.

Hence if $A' = (A - x) \cup B$, $B' = A \cap (B + x)$, then $1 \leq |B'| < |B|$, $|A' + B'| \leq |A + B|$. By induction, $|A + B| \geq \min(|A'| + |B'| - 1, p)$.

But $|A'| = |(A-x) \cup B| = |A-x| + |B| - |(A-x) \cap B| = |A| + |B| - |B'|$. Hence $|A| + |B| = |A'| + |B'|$. □

This trick, transforming from $(A, B) \to ((A - x) \cup B, A \cap (B + x))$, is sometimes called the ***Dyson e-transform***.

We can characterise the case of equality as APs: if $|A + B| = |A| + |B| - 1$ then, aside from edge cases, A and B must be APs of the same step seize ("Vosper's Theorem").

We say that A has ***small doubling*** if $|A + A| \leq K|A|$ where K is "small" (e.g. $O(1)$). We've seen two examples of sets with small doubling:

- Cosets of subgroups ($K = 1$).
- Arithmetic progressions ($K = 2 - \frac{1}{|A|} = 2 + O(1)$).

There are two ways to generate new sets with small doubling from old.

1. Pass to a large subset. If $|A + A| \leq K|A|$ and $X \subset A$, then $|X + X| \leq |A + A| \leq \left(K\frac{|A|}{|X|}\right)|X|$. If $|X| \geq K^{-O(1)}|A|$, then A has doubling K implies X has doubling at most $K^{O(1)}$.
2. Pass to a sumset. If $|A + A| \leq K|A|$ and $X = A + Y$, then $|X + X| \leq |A + A + Y + Y| \leq |Y|^2|A + A| \leq (K|Y|^2)|X|$. So if A has doubling K and $X = A + Y$ where $|Y| \leq K^{O(1)}$, then X has doubling $\leq K^{O(1)}$. In fact it suffices if $|Y + Y| \leq K^{O(1)}|Y|$ and $|X| \geq K^{-O(1)}|A||Y|$.

This accounts for all sets with small doubling. That is, if $|A + A| \leq 100|A|$, then A is obtained from a coset or AP via these two operations. We'll state this more precisely and prove it later on.

3 Sumset Calculus

How are the sizes of sumsets related to each other?

Lemma 3.1 (Ruzsa's Triangle Inequality)**.** *For any sets A, B, C, $|A + B| \leq \frac{|A+C||B-C|}{|C|}$.*

Proof. For each $x = A + B$, fix an arbitrary representation $x = a_x + b_x$. Consider the map $C \times (A + B) \to (A + C) \times (B - C)$ given by $(c, x) \mapsto (c + a_x, b_x - c)$. This is clearly well defined - to finish the proof we will show that it is injective.

Note that we can recover x from the image of (c, x) by noting $(c + a_x) + (b_x - c) = a_x + b_x = x$. Then we can also recover c by subtracting a_x from $c + a_x$, and hence this map is injective. □

What about iterated sumsets? We write kA for the k-fold sumset of A, i.e. the set of all sums $a_1 + \ldots + a_k$ where $a_i \in A$.

Note that $|A| \leq |kA| \leq |A|^k$. This does not mean A dilated by k!

If $|A$ is small, we might want to know whether $|A + A|$ being small implies that $|kA|$ are also relatively small? The answer turns out to be yes! This is known as Plünnecke's inequality, which says that if $|A+A| \leq K|A|$, then $|kA| \leq K^k|A|$. The original proof by Plünnecke is graph-theoretic - it can be found in Tao & Vu. More recently, Petridis has found an alternative proof which is presented here. It uses the following lemma:

Lemma 3.2 (Plünnecke-Petridis Inequality)**.** *For any A, B there exists $X \subseteq A$ such that, for all C*

$$\frac{|C + X + B|}{|C + X|} \leq \frac{|A + B|}{|A|} \tag{$*$}$$

Proof. Note that $(*)$ holds whenever $|C| = 1$, and hence

$$\frac{|X + B|}{|X|} \leq \frac{|A + B|}{|A|} \tag{$**$}$$

We will chose $X \subseteq A$ such that $(**)$ holds and $\frac{|X+B|}{|X|}$ is minimal. Note that $X = A$ satisfies $(**)$, and so this choice makes sense.

We then show that $(*)$ holds for all C by induction on $|C|$. The case $|C| = 1$ is immediate.

Now suppose that $|C| > 1$, and choose some $c \in C$, and let $C' = C \setminus \{c\}$. Then:

$$C + X = (C' + X) \sqcup (c + X')$$

for some $X' \subseteq X$, maximal such that $C' + X$ and $c + X'$ are disjoint. By maximality, $c + (X \setminus X') \subseteq C' + X$, and so $c + (X \setminus X') + B \subseteq C' + X + B$. Hence:

$$C + X + B = (C' + X + B) \cup ((C + X + B) \setminus (c + X \setminus X' + B))$$

Taking cardinalities of both sides,

$$\begin{aligned} |C + X + B| &\leq |C' + X + B| + |c + X + B| - |c + X \setminus X' + B| \\ &= |C' + X + B| + |X + B| - |X \setminus X' + B| \\ &\leq \frac{|A + B|}{|A|}|C' + X| + |X + B| - \frac{|X + B|}{|X|}|X \setminus X'| \end{aligned}$$

using the inductive hypothesis and the fact that $\frac{|X\setminus X'+B|}{|X\setminus X'|} \geq \frac{|X+B|}{|X|}$ by minimality. Continuing, we have:

$$\begin{aligned} |C + X + B| &\leq \frac{|A + B|}{|A|}|C' + X| + |X + B|\left(1 - \frac{|X \setminus X'|}{|X|}\right) \\ &= \frac{|A + B|}{|A|}|C' + X| + \frac{|X + B|}{|X|}|X'| \\ &\leq \frac{|A + B|}{|A|}(|C' + X| + |X'|) \\ &= \frac{|A + B|}{|A|}|C + X| \end{aligned}$$

□

Corollary 3.3 (Plünnecke's Inequality)**.** *If $|A+B| \leq K|A|$, then there exists $X \subseteq A$ such that, for all $k \geq 1$,*

$$|X + kB| \leq K^k|X|$$

In particular, $|kB| \leq K^k|A|$.

Proof. This follows immediately from the Plünnecke-Petridis Inequality by induction on k. For $k = 1$, we have $|X + B| \leq K|X|$, by taking any C with $|C| = 1$. In general, take $C = (k-1)B$, and then

$$|X + kB| = |C + X + B| \leq K|X + C| = K|X + (k-1)B| \leq K \cdot K^{k-1}|X| = K^k|X|$$

by induction. The second claim follows since trivially,

$$|kB| \leq |X + kB| \text{ and } K^k|X| \leq K^k|A|$$

□

By coupling this with Ruzsa's triangle Inequality (RTI), we get a form for mixed sums and differences.

Corollary 3.4. *Suppose $|A+B| \leq K|A|$. For any $k, \ell \in \mathbb{N}$ with $k + \ell \geq 2$,*

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

Proof. By RTI with X as above,

$$|kB - \ell B| \leq \frac{|X + kB||X + \ell B|}{|X|} \leq \frac{K^k|X|K^\ell|X|}{|X|} = K^{k+\ell}|X| \leq K^{k+\ell}|A|$$

□

4 Additive Energy

The size of the sumset is one way to measure the 'structure' of A, but not the only way. One advantage of using $\frac{|A+A|}{|A|}$ is that it controls the same quantity for subsets automatically: i.e., if $X \subset A$, then $|X + X| \leq |A + A|$. However, it has the disadvantage that $\frac{|A+A|}{|A|}$ can grow out of control quickly if we add in a small number of elements. It's often more convenient to use "additive energy" to measuer structure.

Definition 4.1. *The* **additive energy** *of A, $E(A)$ is defined to be*

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

Note that while small sumsets occur in 'structured' sets, here this corresponds to large additive energy. For example, if A is an arithmetic progression, then $E(A) \approx |A|^3$.

If A is a geometric progression, then $E(A) \approx |A|^2$, as $2^k + 2^\ell = 2^r + 2^s \iff \{k, \ell\} = \{r, s\}$.

We have an alternate definition of $E(A)$ - note that

$$\begin{aligned} E(A) &= \sum_{a,b\in A}\sum_{c,d\in A}\sum_{x} \mathbb{1}_{a+b=x}\mathbb{1}_{c+d=x} \\ &= \sum_{x}\left(\sum_{a,b\in A}\mathbb{1}_{a+b}=x\right) \\ &= \sum_{x}\mathbb{1}_A * \mathbb{1}_A(x)^2 \\ &= \|\mathbb{1}_A * \mathbb{1}_A\|_2^2 \end{aligned}$$

(recall that the L^p norm of $f : G \to \mathbb{C}$ is defined by $\|f\|_p = (\sum_x |f(x)|^p)^{1/p}$, and $\|f\|_\infty = \sum_{x\in G}|f(x)|$).

Its status as an L^2-norm explains why $E(A)$ is so useful in analytic arguments. Also note that the size of the sumset $|A+A|$ is the size of the support of $\mathbb{1}_A * \mathbb{1}_A$, sometimes called the "$L^0$-norm". Note that the L^1-norm of A is $\sum_{a,b\in A}\sum_x \mathbb{1}_{a+b=x} = \sum_{a,b\in A} 1 = |A|^2$.

It should also be noted that

$$\begin{aligned} E(A) &= \#\{(a,b,c,d)\in A^4 : a-c=b-d\} \\ &= \sum_x \mathbb{1}_A \circ \mathbb{1}_A(x)^2 = \|\mathbb{1}_A \circ \mathbb{1}_A\|_2^2 \end{aligned}$$

Lemma 4.2. *$|A|^2 \le E(A) \le |A|^3$ and $E(A) \ge \frac{|A|^4}{|A+A|}$.*

i.e., small sumset $\implies$ large energy.

Proof. $|A|^2 \le E(A)$ comes from counting solutions to $a+b=c+d$ where $a=c$ and $b=d$.

$E(A) \le |A|^3$ is because once we have fixed a, b, c, then either there are 1 or 0 choices for d.

To connect $E(A)$ with the size of the sumset, we use the Cauchy-Schwarz inequality, i.e.

$$\sum a_i b_i \le \left(\sum |a_i|^2\right)^{1/2}\left(\sum |b_i|^2\right)^{1/2}$$

We have

$$\begin{aligned} |A|^2 &= \sum_x \mathbb{1}_A * \mathbb{1}_A(x)\times 1 \\ &= \sum_x \mathbb{1}_A * \mathbb{1}_A(x)\times \mathbb{1}_{A+A}(x) \\ &\le \left(\sum_x \mathbb{1}_A * \mathbb{1}_A(x)^2\right)^{1/2}\left(\sum_x \mathbb{1}_{A+A}(x)^2\right)^{1/2} \\ &= E(A)^{1/2}|A+A|^{1/2} \end{aligned}$$

Similarly, we have $E(A) \ge \frac{|A|^4}{|A-A|}$. □

The converse to small sumset $\implies$ large energy does not hold. If we take A to be the union of an arithmetic progression and geometric progression of equal sizes, then $|A+A| \gg |A|^2$ (from the geometric progression), but $E(A) \gg |A|^3$ (from the arithmetic progression).

A itself is not structured much, but a large subset of A is. One might hope that this construction is the only thing that can go wrong. More precisely, that if A has large energy, then there is a large subset of A with small doubling. The answer to this hope is yes! - the Balog-Szemerédi-Gowers Lemma.

Lemma 4.3 (Balog-Szemerédi-Gowers)**.** *If $E(A) \geq K^{-1}|A|^3$ for some $K \geq 1$, then there exists $A' \subseteq A$ such that:*

1. $|A'| \gg K^{-1}|A|$
2. $|A' - A'| \ll K^7|A|$.

Note that the dependence on K is polynomial, and also that we can recover a bound for $|A'+A'|$ via the Ruzsa triangle inequality:

$$|A'+A'| \leq \frac{|A'+A'| \cdot |A'+A'|}{|A'|} \leq K^{14}|A|$$

We will use the "first moment method" - a simple application of probability which is very useful in combinatorics. It essentially says that if X is a real-valued random variable then $X \geq \mathbb{E}X$ with positive probability.

Proof (following Schoen). Firstly, we will find a large subset $X \subset A$ such that there are 'many' differences in $X - X$ with 'many' different representations as elements of $A - A$. Note that, if all of $A - A$ had $\geq K^{-O(1)}|A|$ representations, then $E(A) = \sum_x \mathbb{1}_A \circ \mathbb{1}_A(x)^2 \geq |A-A|K^{-O(1)}|A|^2$, and on the other hand $\leq |A|^3$, then $|A - A| \leq K^{O(1)}|A|$.

We will then find some $X' \subseteq X$ such that $|X' - X'|$ is small as required. We'll break these steps up into the following lemmas. □

Lemma 4.4. *If $E(A) \geq K^{-1}|A|^3$ then for any $0 < c < 1$ there is some $X \subseteq A$ such that $|X| \gg K^{-1}|A|$ and for all but at most $c|X|^2$ many pairs $(a, b) \in X^2$,*

$$\mathbb{1}_A \circ \mathbb{1}_A(a-b) \gg c^2K^{-3}|A|$$

Proof. The set X will be of the form $A \cap (A+s)$ for some $s \in A - A$ randomly chosen. We choose $s \in A - A$ with probability $\frac{\mathbb{1}_A \circ \mathbb{1}_A(s)}{|A|^2}$. Then:

$$\begin{aligned}
\mathbb{E}|X| &= \sum_s \mathbb{P}(s \text{ chosen})|A \cap (A+s)| \\
&= \sum_s \frac{\mathbb{1}_A \circ \mathbb{1}_A(s)}{|A|^2} \sum_{a \in A} \mathbb{1}_A(a-s) \\
&= \frac{1}{|A|^2} \sum_s \mathbb{1}_A \circ \mathbb{1}_A(s)^2 \\
&= \frac{E(A)}{|A|^2}
\end{aligned}$$

For any $G \subset A^2$, we calculate $\mathbb{E}|X^2 \cap G|$.

Using linearity of expectation:

$$\begin{aligned}\mathbb{E}|X^2 \cap G| &= \sum_{(a,b)\in G} \mathbb{P}(a,b \in X) \\ &= \sum_{(a,b)\in G} \sum_s \frac{\mathbb{1}_A \circ \mathbb{1}_A(s)}{|A|^2} \mathbb{1}_A(a-s)\mathbb{1}_A(b-s) \\ &= \frac{1}{|A|^2} \sum_{(a,b)\in G} \sum_s \mathbb{1}_A \circ \mathbb{1}_A(s)\mathbb{1}_A(a-s)\mathbb{1}_A(b-s)\end{aligned}$$

We bound the inner sum above by Cauchy-Schwarz:

$$\begin{aligned}\sum_s \mathbb{1}_A \circ \mathbb{1}_A(s)\mathbb{1}_A(a-s)\mathbb{1}_A(b-s) &\leq \left(\sum_s \mathbb{1}_A \circ \mathbb{1}_A(s)^2\right)^{1/2} \left(\sum_{s\in G} \mathbb{1}_A(a-s)\mathbb{1}_A(b-s)\right)^{1/2} \\ &= E(A)^{1/2} \mathbb{1}_A \circ \mathbb{1}_A(a-b)^{1/2}\end{aligned}$$

It then follows that:

$$\mathbb{E}|X^2 \cap G| \leq \frac{E(A)^{1/2}}{|A|^2} \sum_{(a,b)\in G} \mathbb{1}_A \circ \mathbb{1}_A(a-b)^{1/2}$$

In particular, if $G \subset A^2$ is the set of pairs (a,b) such that:

$$\mathbb{1}_A \circ \mathbb{1}_A(a-b) \leq \frac{c^2}{4} \frac{E(A)^3}{|A|^8}$$

then

$$\mathbb{E}|X^2 \cap G| \leq \frac{c}{2} \frac{E(A)^2}{|A|^4}$$

using the trivial bound that $|G| \leq |A|^2$.

Furthermore, by Cauchy-Schwarz again, $\mathbb{E}|X|^2 \geq (\mathbb{E}|X|)^2$, so $\mathbb{E}|X|^2 \geq \frac{E(A)^2}{|A|^4}$.

Hence, by the first moment method, there is some $X \subseteq A$ such that

$$|X|^2 - \frac{1}{c}|X^2 \cap G| \geq \frac{1}{2} \frac{E(A)^2}{|A|^4}$$

Hence we have:

1. $|X|^2 \geq \frac{1}{2}\frac{E(A)^2}{|A|^4} \geq \frac{1}{2}\frac{|A|^2}{K^2}$, so $|X| \gg \frac{|A|}{K}$.
2. $|X^2 \cap G| \leq c|X|^2$

□

It remains to find some large $A' \subset X$ such that $|A' - A'|$ is small.

Proof of BSG.. We apply the previous lemma to A with $c = \frac{1}{8}$, to obtain some X as stated.

Since $\mathbb{1}_A \circ \mathbb{1}_A(a-b) = \mathbb{1}_A \circ \mathbb{1}_A(b-a)$, we can define a graph H with vertex set X, such that a, b are connected by an edge in H if and only if $a \neq b$ and $\mathbb{1}_A \circ \mathbb{1}_A(a-b) \gg K^{-3}|A|$.

By **Lemma 4.4**, there are at most $\frac{1}{8}|X|^2$ many pairs $(a,b) \in X^2$ where this condition fails, and hence H has at least $\binom{|X|}{2} - \frac{1}{16}|X|^2$ edges.

If $d(x)$ denotes the degree of a vertex $x \in H$, then:

$$\sum_{x \in X} d(x) \geq \frac{7}{8}|X|^2 - |X|$$

Let A' be the subset of X consisting of those elements of degree at least $\frac{3}{4}|X|$ in H.

The contribution to the degree count from $x \notin A'$ is at most $\frac{3}{4}|X|^2$, and hence:

$$|X||A'| \geq \sum_{x \in A'} d(x) \geq \frac{1}{8}|X|^2 - |X|$$

and hence $|A'| \gg |X|$.

We now claim that, for any $x \in A' - A'$, there at $\gg K^{-6}|A|^2|X|$ many quadruples $(a_1, a_2, a_3, a_4) \in A^4$ such that $x = a_1 - a_2 + a_3 - a_4$. Assuming this, since the number of such quadruples is at most $|A|^4$, we have:

$$|A|^4 \gg |A' - A'|K^{-6}|A|^2|X|$$

Then, rearranging we will have:

$$|A' - A'| \ll K^6 \frac{|A|^2}{|X|} \ll K^7|A|$$

Fix some $a, b \in A'$ such that $x = a - b$. By choice of A', there are $\geq \frac{1}{2}|X|$ many $c \in X$ such that $(a,c), (b,c)$ are edges in H.

Hence there are $\gg K^{-3}|A|$ many $(a_1, a_2) \in A^2$ such that $a_1 - a_2 = a - c$ and $\gg K^{-3}|A|$ many $(a_3, a_4) \in A^2$ such that $a_3 - a_4 = b - c$. Since different c give different quadruples for fixed x, in total we have:

$$\gg \left(\frac{1}{2}|X|\right)\left(K^{-3}|A|\right)\left(K^{-3}|A|\right) \gg |X|K^{-6}|A|$$

many such quadruples. □

Addendum/Big Picture Remarks. The goal of BSG is to go from $E(A)$ is large (i.e. $\geq K^{-1}|A|^3$) to getting $A' \subset A$ with $|A' - A'| \ll |A'|$, where A' is a 'large' subset of A.

Recall that $E(A)$ is $\sum_x \mathbb{1}_A \circ \mathbb{1}_A(x)^2$, where $\mathbb{1}_A \circ \mathbb{1}_A(x)$ is the number of ways of writing x as a difference in $A - A$. dd Let S dbe the set $\{x : \mathbb{1}_A \circ \mathbb{1}_A(x) \geq \frac{1}{2K}|A|\}$ (note that trivially $\mathbb{1}_A \circ \mathbb{1}_A(x) \leq |A|$), so $x \in S$ implies that x really can be written as a difference in a large number of ways. We want to know how big S is.

One the one hand,

$$\sum_{x \notin S} \mathbb{1}_A \circ \mathbb{1}_A(x)^2 < \frac{1}{2K}|A| \sum_x \mathbb{1}_A \circ \mathbb{1}_A(x) = \frac{1}{2K}|A|^3$$

Now since $\sum_x \mathbb{1}_A \circ \mathbb{1}_A(x)^2 = \frac{1}{K}|A|^3$, we must have:

$$|S||A|^2 \geq \sum_{x \in S} \mathbb{1}_A \circ \mathbb{1}_A(x)^2 \geq \frac{1}{2K}|A|^3$$

and hence

$$|S| \gg \frac{1}{K}|A|$$

For an upper bound on S, we note that $|S|\frac{1}{2K}|A| \leq \sum_{x \in S} \mathbb{1}_A \circ \mathbb{1}_A(x) \leq \sum_x \mathbb{1}_A \circ \mathbb{1}_A(x) = |A|^2$, and so $|S| \ll K|A|$. So up to some constant terms, $|S|$ is essentially $|A|$.

Since $x \in S$ implies that x is represented many times in $A - A$, we must have $S \subset A - A$. So we would be done if we could find $A' \subset A$ such that $A' - A' \subset S$.

This can't be done in general, but we can find a large $A' \subset A$ such that "99%" of all pairs $(a', b') \in A'^2$ have $a' - b' \in S$ - this is **4.4**. Such an S is often called a "symmetry set". We then want to get to a "100%" statement: we know that 99% of the (a', b') have $a' - b' \in S$, so we expect for most $a', b' \in S$, there are $\gg |A'|$ many $c \in A'$ such that $a' - c, b' - c \in S$.

We then write $a' - b' = (a' - c) - (b' - c) \in S - S$. So we can write $a' - c \in S$ as $a_1 - a_2$ in many ways, and likewise for $b' - c$. So $a' - b'$ can be written in $\gg K|A'||A|^2$ many ways, and so in total have $\gg |A' - A'||A|^3$ many such quadruples. But trivially there are at most $|A|^4$ quadruples, so $|A' - A'| \ll K|A|$.

5 Covering

We say that A is K-covered by B if there is X with $|X| \leq K$ such that $A \subseteq X + B$. I.e., we can contain A in at most K-many translates of B.

For example, if A is K-covered by B, where $|B| \ll |A|$ and $|B|$ has small doubling, then A must also have small doubling:

$$|A + A| \leq |X + X + B + B| \ll K^2|B + B| \ll_K |B| \ll |A|$$

We can often get more from covering than this suggests. For instance, we can control iterated sums: if $A + B$ is efficiently covered by A itself, then so is $A + nB$ for small n. If $A + B \subset A + X$, then $A + nB \subset A + nX$.

Before we use this concept, we need to show how to produce efficient coverings. The first way is due to Ruzsa, and is simple and useful.

Lemma 5.1 (Ruzsa Covering Lemma)**.** *If $|A + B| \leq K|B|$, then A is K-covered by $B - B$.*

Proof. Let X be maximal such that $(x + B)_{x \in X}$ are disjoint.

We can control the size of X:

$$|X||B| = |X + B| \leq |A + B| \leq K|A|$$

and so $|X| \leq K$.

If $a \in X$, then obviously $a \in X + B - B$. If $a \in A \setminus X$, then $a + B$ must intersect $x + B$ for some $x \in X$ (by maximality). I.e. there are $b_1, b_2 \in B$ such that $a + b_1 = x + b_2$. But then $a = x + b_1 - b_2 \in X + B - B$, and so $A \subseteq X + B - B$. □

Note that we are covering A by $B-B$, not B itself. This is because $B-B$ is much 'smoother' than B itself - e.g. what if B is a large random subset of G. On average, G needs $\gg \log|G|$ translates of B to cover everything, so even though $|G+B| \leq |G| \ll |B|$, but if $G \subset X+B$, then $X \gg \log|G|$ (with high probability). So G is not efficiently covered by B, even though $|G+B| \ll |B|$. But $B-B=G$ with high probability. Indeed, any $B \subset G$ with $|B| > \frac{1}{2}|G|$ has $B-B=G$, since for any $x \in G$, consider B and $x+B$. These are subsets of G of size $> \frac{1}{2}|G|$, so they must intersect. I.e. there are $b_1, b_2 \in B$ with $b_1 = x + b_2$.

We now present an application of Ruzsa's covering lemma and Plünnecke's inequality - a non-trivial inverse sumset result.

As we saw earlier, if H is a subgroup of G and $Ax+H$ with $|A| \gg |H|$, then $|A+A| \ll |A|$. We will show that this is the only way that A can have small doubling in groups of small torsion (e.g. $G = \mathbb{F}_p^n$, not in subsets of $\mathbb{Z}$ or $\mathbb{Z}/N\mathbb{Z}$).

Theorem 5.2. *If $A \subset \mathbb{F}_p^n$ is such that $|A+A| \leq K|A|$, then there is a subgroup $H \leq \mathbb{F}_p^n$ and x such that $A \subseteq x+H$ and $|A| \gg_{p,K} |H|$.*

Proof. Without loss of generality, $0 \in A$. The idea is to take $H = \langle A \rangle$. But trivially we only have $|H| \leq p^{|A|}$ - we will use the small doubling of A to control the size of H. □