

1. BOUNDS ON $|A + B|$

Our main goal during the first five weeks of this course is to prove the Bourgain-Katz-Tao theorem which states that, given a reasonable subset A in $F := \mathbb{Z}/p\mathbb{Z}$, $|A \cdot A + A \cdot A|$ is big relative to $|A|$. The idea is to find a polynomial P such that

$$P(A, A, \dots, A) = F$$

However, if the BKT theorem is false, then we will show that

$$|P(A, A, \dots, A)| \leq |A|^{1+C\varepsilon}$$

so, roughly, the theorem will follow by choosing appropriate ε (depending on δ). This week we will find various upper and lower bounds on the size of the sumset $A + B$; next week, we will use the latter to help us find the above polynomial, and the week after we will use the former inequalities to prove the “sumset estimates”, a first step towards the second half of the proof of BKT.

Recall exercise 0.1: among other things, this gives the trivial lower bound

$$|A| + |B| - 1 \leq |A + B|$$

for finite, non-empty $A, B \subseteq \mathbb{Z}$. Why is this true? By translation invariance, we may shift A and B so that $\max A = \min B = 0$; then $A \cup B \subseteq A + B$, so

$$|A| + |B| - 1 = |A \cup B| \leq |A + B|$$

since $A \cap B = \{0\}$. This nice result certainly relies upon the fact that the integers are ordered. Indeed, what happens when we ask for a similar bound in the finite field $F := \mathbb{Z}/p\mathbb{Z}$ for a prime p ?

Theorem 1.1 (Cauchy-Davenport inequality). *Let $A, B \subseteq F$. Then*

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

Proof. If $|A| + |B| - 1 \geq p$, so that $|A| + |B| > |F|$, then $|A| + |x - B| > |F|$ for any $x \in F$ by translation invariance. Thus by the pigeonhole principle, A intersects $(x - B)$ for all $x \in F$, i.e. given $x \in F$, there exist $a \in A$ and $b \in B$ such that $a = x - b$, or $x = a + b$. Therefore $A + B = F$, so $|A + B| = p$ as needed in this case.

Now assume that $|A| + |B| - 1 < p$ with $|A| > 1$; this is fair since the result is trivial if $|A| = 1$. We must show that

$$(2) \quad |A + B| \geq |A| + |B| - 1$$

Suppose we had a counterexample to inequality (2) (and hence a counterexample to the theorem); that is, suppose there were sets $A, B \subseteq F$ such that $|A + B| < |A| + |B| - 1$. Also suppose that this counterexample is minimal in the sense that $|A|$ is as small as possible. (Everything in sight is finite, so the existence of such a minimal counterexample is not an issue.) For the moment, translate so that $A \cap B \neq \emptyset$. This will enable us to construct a new counterexample to inequality (2): let $A' = A \cap B$ and $B' = A \cup B$. Then:

- $|A'| + |B'| = |A| + |B|$
- $|A' + B'| \leq |A + B|$; in fact

$$\begin{aligned} A' + B' &= A' + (A \cup B) \\ &\subseteq (A' + A) \cup (A' + B) \\ &\subseteq (B + A) \cup (A + B) = A + B \end{aligned}$$

Therefore A', B' is another counterexample, as claimed. Furthermore, it is minimal since $A' \subseteq A$. Thus $A' = A$, that is, $A \subseteq B$. Thus we have shown that whenever we have a minimal counterexample A, B to 2, then $A \subseteq B$.³

To wit! If A, B is a minimal counterexample as above, then $(A + x), B$ is one as well for any $x \in F$, so $A + x \subseteq B$ whenever $(A + x) \cap B \neq \emptyset$. But the latter is equivalent to the existence of $a \in A, b \in B$ satisfying $a + x = b$, and this is true if $x \in B - A$. To summarize: $x \in B - A$ implies $A + x \subseteq B$. Hence $B - A + A \subseteq B$, so certainly $|B + (A - A)| = |B|$.

Finally, we recall exercise 0.2: $|C + D| = |C|$ if and only if C is the union of cosets of some finite subgroup H , and D is contained in some coset of the same subgroup H . In the current context, with $C = B$ and $D = A - A$, this implies

$$B = \bigcup (H + x_i) \text{ and } A - A \subseteq H + x$$

where $x, x_i \in F$ and $H \leq F$ is a finite (additive) subgroup. Therefore $H = \{0\}$ or $H = F$, and it is easy to see that neither of these are possible (recall that we're assuming $|A| > 1$). We conclude that there is no (minimal) counterexample to the theorem! \square

We may promote the additive factor of the right-hand side of Theorem 1.1 to a multiplicative one if we allow ourselves to dilate one of the given sets:

Lemma 1.2. *If $A, B \subseteq F$, then there exists a $\xi \in F^*$ such that*

$$(3) \quad |A + B \cdot \xi| \geq \min\left(\frac{|A||B|}{2}, \frac{|F|}{10}\right)$$

Proof. If $\frac{|A||B|}{2} > \frac{|F|}{4}$, then we may remove some elements from A and B without affecting the right-hand side of inequality (3); that is, we replace A and B with subsets $A' \subset A$ and $B' \subset B$ such that $|A'||B'| > |F|/5$ which assures that $|A+B| \geq |A'+B'|$ but still $\min(|A'||B'|/2, |F|/10) = |F|/10 = \min(|A||B|/2, |F|/10)$, and thus proving the assertion for A', B' implies the result for A, B . Thus we may assume that $|A||B| \leq |F|/2$.

Let $\xi \in F^*$. Then

$$(4) \quad |A + B \cdot \xi| = \left| \bigcup_{a \in A} a + B \cdot \xi \right|$$

$$(5) \quad \geq \sum_{a \in A} |a + B \cdot \xi| - \frac{1}{2} \sum_{a \neq a'} |(a + B \cdot \xi) \cap (a' + B \cdot \xi)|$$

$$(6) \quad \geq \sum_{a \in A} |B \cdot \xi| - \frac{1}{2} \sum_{a \neq a'} \sum_{b, b' \in B} \delta_{a+b\xi, a'+b'\xi}$$

$$(7) \quad = |A||B| - \frac{1}{2} \sum_{a \neq a', b \neq b'} \delta_{\xi, \frac{a-a'}{b-b'}}$$

Inequality (5) follows by the inclusion-exclusion principle: suppose $x \in A + B \cdot \xi$ and x is contained in exactly n of the sets $a + B \cdot \xi$ for some $n \leq |A|$. Then the

³One might think that we are done, because it should be easy to translate A so that A and B intersect but A is not contained in B ; however, it is impossible to guarantee this in general due to the cyclic nature of F . This subtlety came to light during a discussion with J. DeBlois and J. Callahan.

first sum counts x exactly n times and the second sum counts x

$$2((n-1) + (n-2) + \dots + 1) = n(n-1)$$

times. Thus the inequality is valid since $1 \geq n - \frac{n(n-1)}{2}$ for all positive n ; x is counted by (4) once and by (5) $n - \frac{n(n-1)}{2}$ times.

Now we average this result over all of F^* :

$$\begin{aligned} \frac{1}{|F^*|} \sum_{\xi \in F^*} |A + B \cdot \xi| &\geq \frac{1}{|F^*|} \sum_{\xi \in F^*} \left(|A||B| - \frac{1}{2} \sum_{a \neq a', b \neq b'} \delta_{\xi, \frac{a-a'}{b-b'}} \right) \\ &= |A||B| - \frac{1}{2} \frac{1}{|F^*|} \sum_{a \neq a', b \neq b'} 1 \\ &\geq |A||B| - \frac{1}{2} \frac{|A|^2 |B|^2}{|F| - 1} \\ &\geq \frac{1}{2} |A||B| \end{aligned}$$

since $|A||B| \leq \frac{1}{2}|F| \leq |F| - 1$. Therefore, by the pigeonhole principle, there exists a $\xi \in F^*$ such that $|A + B \cdot \xi| \geq \frac{1}{2}|A||B|$. \square

Exercise 1.1. Suppose $A \subseteq F$, and $|A| \geq \min\{|F|/10, 2\}$. What can you say about $A + A + \dots + A$ (1,000 terms in the sum)?

Now we look at an upper bound for $|A + B|$, which we will use in a couple weeks to derive the sumset estimates from Plünnecke's theorem:

Lemma 1.3 (Ruzsa). Suppose U, V, W are finite, non-empty subsets of some abelian group Z . Then

$$|V - W| \leq \frac{|U + V||U + W|}{|U|}$$

Proof. Let $s : V \times W \rightarrow V - W$ be the subtraction map:

$$s(x, y) = x - y$$

Then s is certainly onto, and thus there exists a partial inverse $f : V - W \rightarrow V \times W$ such that $s \circ f \equiv \text{id}_{V-W}$.

Let $\Delta_U := \{(u, u) : u \in U\} \subseteq Z \times Z$, so

$$(V \times W) + \Delta_U \subseteq (U + V) \times (U + W).$$

Therefore, in particular, for all $x \in V - W$,

$$(8) \quad f(x) + \Delta_U \subseteq (U + V) \times (U + W)$$

Now we claim that the sets $f(x) + \Delta_U, f(y) + \Delta_U$ are disjoint for $x \neq y$: otherwise, there are $u, u' \in U$ such that $f(x) + (u, u) = f(y) + (u', u')$. But then, by the linearity of s , we have

$$x = s(f(x)) + s(u, u) = s(f(y)) + s(u', u') = y$$

which is clearly a contradiction.

But $|f(x) + \Delta_U| = |\Delta_U| = |U|$ for all $x \in V - W$, so by (8) and the above claim, we see that

$$\begin{aligned} |V - W||U| &= \sum_{x \in V - W} |f(x) + \Delta_U| \\ &= \left| \bigcup_{x \in V - W} f(x) + \Delta_U \right| \\ &\leq |U + V||U + W| \end{aligned}$$

as needed. \square

Ruzsa has several clever results like this; you will prove one more now, and we will see another one later when we finish the proof of BKT.

Exercise 1.2. *Let Z be an abelian group and $A, B \subseteq Z$ be finite, non-empty subsets.*

- (a) *Find $X \subseteq Z$ such that $|X| \leq |A + B|/|A|$ and $B \subseteq X + A - A$. (This is known as Ruzsa's Quotient Lemma.)*
- (b) *What does this say when*

$$A \leq Z \text{ and } B = \bigcup_{i=1}^n A + z_i$$

(where $z_i \in Z$)? (Don't forget that for us, $H \leq G$ always means that H is a subgroup of G whenever G is a group.)

For more on the results discussed in this section, see [1].

References.

- [1] Terry Tao. Math 254a: Some highlights of arithmetic combinatorics, 2003.