

OVERVIEW AND OUTLINE

Arithmetic combinatorics is the study of finite subsets of abelian groups and rings. For example, let $A, B \subseteq \mathbb{Z}$ be finite, non-empty subsets of the integers. What can we say about the following sets?

$$\begin{aligned} A + B &= \{a + b \mid a \in A, b \in B\} \\ A - B &= \{a - b \mid a \in A, b \in B\} \\ A \cdot B &= \{ab \mid a \in A, b \in B\} \end{aligned}$$

Our main goal is to prove from first principles a recent theorem of Jean Bourgain, Nets Katz, and Terry Tao on the growth of subsets in finite fields of prime order (see [1]):

Theorem 0.1 (BKT). *Let $\delta > 0$ be given. Then there exist constants $c = c(\delta) > 0$ and $\varepsilon = \varepsilon(\delta) > 0$ (depending only on δ) such that for any prime p and any subset $A \subseteq F := \mathbb{Z}/p\mathbb{Z}$ with $|F|^\delta < |A| < |F|^{1-\delta}$, we have*

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\varepsilon}$$

Since a subring S of a ring R has the property that $|S + S| = |S|$ and $|S \cdot S| = |S|$, we can restate the conclusion of the theorem in the following way. In general, if $A, B \subseteq Z$ are subsets of some abelian group, then we will let $|A| \lesssim |B|$ denote $|A| = O(|B|)$, i.e. there is a constant C (independent of A and B) such that $|A| \leq C|B|$. Now, if Z is a ring—so both addition and multiplication are defined—we can call $A \subseteq Z$ an **approximate subring** if $|A + A| \lesssim |A|$ and $|A \cdot A| \lesssim |A|$. The theorem says that finite fields of prime order contain no approximate subrings.

As a warm-up, let's think a little bit about subsets of \mathbb{Z} . From now on, A and B will always denote finite, non-empty subsets of the group or ring under consideration (unless stated otherwise). It may be helpful to observe that translating given sets A and B does not affect $|A + B|, |A - B|$, etc. For example, the sum of the translated sets has the same size as the sum itself:

$$|(A + x) + (B + y)| = |A + B + (x + y)| = |A + B|$$

Exercise 0.1. *Let $Z = \mathbb{Z}$, the ring of integers.*

- (a) *Let $A, B \subseteq Z$. Show $|A| + |B| - 1 \leq |A + B| \leq |A||B|$.*
- (b) *Given $m, n \geq 1$ and $m + n - 1 \leq s \leq mn$, construct $A, B \subseteq Z$ such that $|A| = m, |B| = n$, and $|A + B| = s$.*

A statement similar to (a) for $Z = \mathbb{Z}/p\mathbb{Z}$ where p is prime is called the Cauchy-Davenport inequality. This and a similar lower bound (in terms of a multiplicative factor rather than an additive one) will play a crucial role in the proof of Theorem 0.1, and we will prove both inequalities next time.

One can often think of arithmetic combinatorics as “approximate group theory”. If $H \leq Z$ is a finite subgroup¹ of an abelian group Z , then H is closed under addition and subtraction: $H + H = H - H = H$. In particular, $|H + H| = |H|$ as we noted above in the case that Z is a ring. On the other hand, given a subset $A \subseteq Z$ such that $|A + A| \lesssim |A|$, what can we say about $|A - A|, |A + A - A|$, etc.?

¹We will always use the $H \leq G$ notation to distinguish H as a subgroup rather than just a subset of G .

Exercise 0.2. Let $A, B \subseteq Z$ be finite, non-empty subsets of an abelian group Z . Show that $|A + B| = |A|$ if and only if there is a finite subgroup $H \leq Z$ such that A is the union of cosets of H and B is contained in some coset of H .

In particular, if $A = B$, this exercise says that $|A + A| = |A|$ if and only if A is the coset of some finite subgroup. It turns out that if A is **essentially closed under addition**, in the sense that $|A + A| \lesssim |A|$, then we can say something interesting about the size of sets of the form $A \pm A \pm \dots \pm A$. More generally, if A is **essentially B invariant**, i.e. $|A + B| \lesssim |A|$, then $|mB - nB| \lesssim |A|$ (where $mB = B + B + \dots + B$, m times).² This is known as sumset estimates, and it will follow from a more general theorem called Plünnecke’s theorem.

Since the BKT theorem deals with sizes of subsets, we will focus on results from arithmetic combinatorics on cardinality, not structure. However, one can often find non-trivial information about the *structure* of, say, $A + B$, given information on A and B . For example, a very deep theorem called Frieman’s theorem says that if a subset is essentially closed under addition, then it is very close to being a (generalized) arithmetic progression! We will not require these sorts of results, so, in order to save time, we will not cover them. For more on Frieman’s theorem, see Lecture 2 of [3].

Our strategy for proving the BKT theorem is this: after proving the Cauchy-Davenport inequality and its refinement, we will be able to show that

$$(1) \quad F = A \cdot \xi_1 + A \cdot \xi_2 + \dots + A \cdot \xi_k$$

for k relatively small, depending only on δ . We need a bit more notation. Let $P \in \mathbb{Z}[X_1, X_2, \dots, X_n]$ be a polynomial with integral coefficients in n variables, and let $P(A, A, \dots, A)$ be its evaluation at the subset A with respect to our notation above. For example, if $P(X, Y) = X - Y$, then $P(A, A) = A - A$. Now, given the “linear surjection” result as in equation 1, we will deduce the existence of a polynomial P such that $P(A, A, \dots, A) = F$. However, assuming that the conclusion of the theorem is false, we will find—using standard results such as sumset estimates and the Gowers-Balog-Szemerédi theorem—that for our polynomial P , we have $|P(A, A, \dots, A)| \lesssim |A|^{1+C\varepsilon}$ for some constant C and any $\varepsilon > 0$. Thus we will arrive at a contradiction by choosing a sufficiently small ε since $|A| < |F|^{1-\delta} < |F|$.

Although the BKT result is only for finite fields of prime order, similar results may be obtained for arbitrary finite fields. The difference is, of course, that there are nontrivial subfields $1 < K < \mathbb{F}_q$ when q is not prime, so in particular $|K + K| = |K \cdot K| = |K|$, contradicting the conclusion of Theorem 0.1. However, this is essentially all that can happen. For more on this, see Theorem 4.3 in [1] as well as Theorem 2.4 in [2].

Our primary resources for this seminar are Tao’s notes on arithmetic combinatorics [3] and the BKT paper [1]; in particular, with the exception of the proof of Gowers’ result that we will encounter in Week 5, all the results and proofs are from these two sources. My sole contributions are reorganization, exposition, and the occasional correction of a typo. I also add some details to Tao’s proofs in order to aid my understanding of the arguments, and I hope these are illuminating rather than distracting.

Here is my proposed outline for the rest of the course:

²I admit that I’m being rather loose with the \lesssim notation. For now, just think of it as meaning “small relative to”. In the next few lectures, I hope to be a bit more careful.

- Week 1** Bounds on $|A + B|$
- Lower bounds on $|A + B|$ and $|A + \xi B|$: Cauchy-Davenport, Cauchy-Davenport refinement;
 - Upper bounds on $|A + B|$: Ruzsa lemmata
- Week 2** Linear surjections onto F
- $F = A\xi_1 + \dots + A\xi_k$, $k = O(1/\delta)$;
 - if there is a linear map $B^k \rightarrow F$, then there is a linear map $\tilde{B}^{k-1} \rightarrow F$ for a related \tilde{B}
- Week 3** Sumset estimates
- Plünnecke's theorem: roughly, $|A + B| \lesssim |A| \implies |A' + B + B| \lesssim |A'|$ for some $A' \subseteq A$
 - Cartesian product trick: transfer a problem in Z to one in $Z \times Z$
- Week 4** $|AA - AA| \lesssim |A|$ implies $|P(A, A, \dots, A)| \lesssim |A|$ for all polynomials P
- notion of “essentially contained”
 - notion of “good elements” and properties of good elements
 - finish proof of BKT
- Week 5** No approximate subrings implies $|A \cdot A - A \cdot A| \lesssim |A|$
- Cauchy-Schwartz inequality
 - Popularity argument
 - the Gowers-Balog-Szemerédi theorem
- Weeks 6–8** Applications of BKT
- incidence problem
 - Erdős distance problem
 - Kakeya problem
 - $SL_2(p)$ has small diameter (Helfgott)
 - constructions of extractors
 - ...?

References.

- [1] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.
- [2] H. A. Helfgott. Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, 2005.
- [3] Terry Tao. Math 254a: Some highlights of arithmetic combinatorics, 2003.

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.

2. LINEAR SURJECTIONS ONTO $\mathbb{Z}/p\mathbb{Z}$

We are still working toward the proof of the BKT result from [1]. Today we will use the results from last week—namely, Theorem 1.1 and Lemma 1.2—to find a polynomial P that depends only on δ such that $P(A, A, \dots, A) = F$. On the one hand, this is rather incredible: for any fixed δ , the same polynomial P works for $p = 101$ and primes $> 10^{10^{10}}$! On the other hand, this result may not be too surprising, given the restrictions on $|A|$. In any event, the fact that P is independent of everything (except δ) is what allows us to prove the BKT theorem.

The first step towards finding P is the following:

Lemma 2.1. *Let $\delta > 0$ be given. Suppose $A \subset F := \mathbb{Z}/p\mathbb{Z}$ for some prime p such that $p^\delta < |A| < p^{1-\delta}$. Then there is a $k = k(\delta)$ and there are $\xi_1, \dots, \xi_k \in F^*$ such that*

$$A \cdot \xi_1 + A \cdot \xi_2 + \dots + A \cdot \xi_k = F$$

Proof. First, I claim that there are $k = k(\delta)$ and $\xi_i \in F^*$ such that $|A \cdot \xi_1 + \dots + A \cdot \xi_k| \geq |F|/10$. To that end, choose k to be some big number, bigger than $2/\delta$. Then by Lemma 1.2, there are $\xi_i \in F^*$ such that

$$|A \cdot \xi_1 + \dots + A \cdot \xi_k| \geq \frac{|A|^k}{2^{k-1}} > \frac{p^{\delta k}}{2^{k-1}} > \frac{p^2}{2^{k-1}}$$

by the assumption on $|A|$. But, for any fixed k , $\lim_{p \rightarrow \infty} \frac{10p}{2^{k-1}} \rightarrow \infty$, so there is a $N \in \mathbb{N}$ such that $10p/2^{k-1} \geq 1$ for all $p \geq N$. Therefore,

$$|A \cdot \xi_1 + \dots + A \cdot \xi_k| > \frac{p^2}{2^{k-1}} > \frac{p}{10}$$

for all $p \geq N$.

For the primes $p < N$, clearly some $k' = O(N)$ applications of Theorem 1.1 will do the trick, and this proves the claim since N depends only on k and k depends only on δ .

Now, by Exercise 1.1, if $B := A \cdot \xi_1 + \dots + A \cdot \xi_k$, then $1000B := B + B + \dots + B = F$ (again by the Cauchy-Davenport inequality, Theorem 1.1). \square

Another way of stating the conclusion of this Theorem is that there is a linear surjection $\pi : A^k \rightarrow F$, defined by

$$\pi(a_1, a_2, \dots, a_k) = \sum_{i=1}^k a_i \xi_i$$

for some $\xi_i \in F$. Our goal, then, is to replace A^k with a polynomial expression in A , and we do this one step at a time:

Lemma 2.2. *Let $B \subseteq F$ be a nonempty subset of $F = \mathbb{Z}/p\mathbb{Z}$ (p prime), and suppose that there is a linear surjection $f : B^k \rightarrow F$ for some $k > 1$, say $f(b_1, \dots, b_k) = \sum b_i \xi_i$ for some $\xi_i \in F$. Then there is a linear surjection $\tilde{B}^{k-1} \rightarrow F$ where*

$$\tilde{B} = B \cdot (B - B) + B \cdot (B - B)$$

Proof. First notice that f cannot be injective since, if it were, then $|F| = |B|^k$, a contradiction since $k > 1$. Therefore there are $(b_1, \dots, b_k) \neq (b'_1, \dots, b'_k) \in B^k$ such that

$$(b_1 - b'_1)\xi_1 + \dots + (b_k - b'_k)\xi_k = 0$$

Suppose WLOG that $b_k \neq b'_k$. We know that $F = B \cdot \xi_1 + \dots + B \cdot \xi_k$, so since F is a field, we also know that

$$\begin{aligned}
F &= F(b_k - b'_k) \\
&= B \cdot \xi_1(b_k - b'_k) + \dots + B \cdot \xi_k(b_k - b'_k) \\
&= B \cdot \xi_1(b_k - b'_k) + \dots + B \cdot \xi_{k-1}(b_k - b'_k) - B \cdot \xi_1(b_1 - b'_1) - \dots - B \cdot \xi_{k-1}(b_{k-1} - b'_{k-1}) \\
&= \xi_1 \cdot B \cdot (b_k - b'_k) - \xi_1 \cdot B \cdot (b_1 - b'_1) + \dots + \xi_{k-1} \cdot B \cdot (b_k - b'_k) - \xi_{k-1} \cdot B \cdot (b_{k-1} - b'_{k-1}) \\
&\subseteq \xi_1 \cdot (B \cdot (B - B) + B \cdot (B - B)) + \dots + \xi_{k-1} \cdot (B \cdot (B - B) + B \cdot (B - B))
\end{aligned}$$

Thus we conclude that $F = \tilde{B}\xi_1 + \dots + \tilde{B}\xi_{k-1}$. \square

Putting it all together for the sake of proving the BKT result (Theorem 0.1), let $\delta > 0$ be given, and suppose $A \subseteq F$ with $p^\delta < |A| < p^{1-\delta}$. Then Lemma 2.1 implies that $F = A \cdot \xi_1 + \dots + A \cdot \xi_k$ for some $\xi_i \in F$ and $k \sim 1/\delta$. If we iterate Lemma 2.2 k times, we get a polynomial P depending only on δ such that $F = P(A, A, \dots, A)$! We will dedicate the next three lectures to showing that if the BKT theorem is false, then $|P(A, \dots, A)| \ll |F|$ for all polynomials P to arrive at a contradiction. This is sort of what one might expect, at least according to the notation: if $|A + A|$ and $|A \cdot A|$ are both small, then any polynomial expression in A should be small, too.

Next week, we will prove the first main ingredient in the second half of the proof: sumset estimates. This says that if A is essentially B -invariant, then $|nB - mB|$ cannot be much larger than $|A|$ (in a way we will make explicit next week). This is a corollary to Plünnecke's Theorem, which says that if $|A + B| \leq K|A|$ for some $K \geq 1$, then there is a nonempty subset $A' \subseteq A$ such that $|A' + B + B| \leq K^2|A'|$. Although this is a very nice, concrete result, it leaves something to be desired since A' could be very small; for more on this, see lecture 1 in [1].

In order to prepare to prove Plünnecke's theorem, we need to introduce some notions from graph theory. Let Z be an abelian group. A **commutative graph** (of depth 2) is a directed graph with vertex sets $V_0, V_1, V_2 \subset Z$ and edge sets $E_{0 \rightarrow 1}, E_{1 \rightarrow 2}$ such that 1) for all edges $e \in E_{i \rightarrow i+1}$, the initial point of e is in V_i and the terminal point is in V_{i+1} and 2) if $(a \rightarrow a+b) \in E_{0 \rightarrow 1}$ and $(a+b \rightarrow a+b+c) \in E_{1 \rightarrow 2}$, then $(a \rightarrow a+c) \in E_{0 \rightarrow 1}$ and $(a+c \rightarrow a+b+c) \in E_{1 \rightarrow 2}$. The second condition is called the **commuting square property**.

Given two commutative graphs G and \tilde{G} , one can define their Cartesian product $G \times \tilde{G}$ to have vertex sets $V_0 \times \tilde{V}_0, V_1 \times \tilde{V}_1$, and $V_2 \times \tilde{V}_2$ (where the V_i and \tilde{V}_i are the vertex sets of G and \tilde{G} , respectively) and edge sets $E_{0 \rightarrow 1} \times \tilde{E}_{0 \rightarrow 1}$ and $E_{1 \rightarrow 2} \times \tilde{E}_{1 \rightarrow 2}$, where the product of two edges $(a \rightarrow b), (\tilde{a} \rightarrow \tilde{b})$ is

$$(a \rightarrow b) \times (\tilde{a} \rightarrow \tilde{b}) = ((a, \tilde{a}) \rightarrow (b, \tilde{b}))$$

Exercise 2.1. Show that if G and \tilde{G} are commutative graphs, then $G \times \tilde{G}$ is as well.

For example, let $A, B \subseteq Z$ and define $G[A, B]$ to be the commutative graph with vertex sets $A, A+B, s$ and $A+B+B$ and all obvious possible edges from A to $A+B$ and from $A+B$ to $A+B+B$. Then by working through the definition one can show that $G[A, B] \times G[A', B'] = G[A \times A', B \times B']$ for any $A', B' \subseteq Z$. Note that if we let $G(X)$ denote all the points in V_1 that are endpoints of edges starting at $X \subseteq V_0$, and similarly $G^2(X)$ be those points in V_2 that are reachable via paths starting in $X \subseteq V_0$, then we may restate the conclusion of Plünnecke's theorem this

way: there is a $A' \subseteq A$ such that $|G[A, B]^2(A')| \leq K^2|A'|$. We will prove a more general statement about commutative graphs next time.

We require one more notion to facilitate next week's lesson. Let A and B be subsets of a finite graph G . Define $MAXFLOW(A \rightarrow B, G)$ to be the maximum number of disjoint paths connecting a vertex in A to one in B . Also define $MINCUT(A \rightarrow B, G)$ to be the minimum number of vertices one must remove from G to disconnect A from B .

Exercise 2.2 (Menger's Theorem). $MAXFLOW(A \rightarrow B, G) = MINCUT(A \rightarrow B, G)$.

Next time, we will use these ideas to prove Plünnecke's theorem using graph theory. Then, using the Ruzsa bound on $|A+B|$ that we proved last week (Lemma 1.3), we will derive the sunset estimates as a corollary.

References.

- [1] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.

3. PLÜNNECKE'S THEOREM AND SUMSET ESTIMATES

We begin our discussion today by investigating some nice properties of commutative graphs, which we will use to prove Plünnecke's Theorem. As usual, we follow Tao's notes (see [1]) very closely. First, let Z be an abelian group and consider a commutative graph G with vertex sets $V_0, V_1, V_2 \subseteq Z$ and edge sets $E_{0 \rightarrow 1}, E_{1 \rightarrow 2}$. Then the edge $(a \rightarrow a + b) \in E_{0 \rightarrow 1}$ induces an injection

$$f : \{(a + b \rightarrow a + b + c) \in E_{1 \rightarrow 2}\} \hookrightarrow E_{0 \rightarrow 1}$$

by setting $f((a + b \rightarrow a + b + c)) = (a \rightarrow a + c)$. The commuting square property implies that f is well-defined, i.e. that $(a \rightarrow a + c) \in E_{0 \rightarrow 1}$, and f is injective since, if $(a + b \rightarrow a + b + c')$ were another edge emanating from $a + b \in V_1$, then $f((a + b \rightarrow a + b + c)) = f((a + b \rightarrow a + b + c'))$ implies that $c = c'$ as claimed. We say that f is the **pullback map** induced by $(a \rightarrow a + b) \in E_{0 \rightarrow 1}$.

Now given a collection of edges $\{(a_i \rightarrow a_i + b_i)\}_{i=1}^n \subseteq E_{0 \rightarrow 1}$, consider the composition map defined over all edges in $E_{1 \rightarrow 2}$ starting at $a_i + b_i$ for some $1 \leq i \leq n$ by the rule

$$(a_i + b_i \rightarrow a_i + b_i + c) \mapsto (a_i \rightarrow a_i + c)$$

formed by using the pullback map induced by the edge $(a_i \rightarrow a_i + b_i)$. Suppose that we're given two edges in the domain, say $a_i + b_i \rightarrow a_i + b_i + c$ and $a_j + b_j \rightarrow a_j + b_j + c'$. If $a_i + b_i \neq a_j + b_j$ and $a_i + b_i + c \neq a_j + b_j + c'$, then we claim that this map is still injective, i.e. that the above two edges map to distinct edges in $E_{0 \rightarrow 1}$. In this case, we must have $c \neq c'$, so if $a_i = a_j$, then $a_i + c \neq a_j + c'$. Therefore the two edges $a_i \rightarrow a_i + c$ and $a_j \rightarrow a_j + c'$ are distinct, and hence the map is injective.

We have shown that if we pullback from a set of edges in $E_{1 \rightarrow 2}$ whose initial points and terminal points are distinct—for example, edges that are in disjoint paths from V_0 to V_2 —then we get a set of maps whose union is still an injection. One may also define **pushforward maps** induced by edges in $E_{1 \rightarrow 2}$, either by direct construction (as for pullback maps above) or by considering pullback maps in G^\dagger , the commutative graph formed from G by switching V_0 and V_2 and reversing edges, that is the “mirror image” of G . The fact that we get injections by pulling back and pushing forward along disjoint paths will be important in the proof of the following proposition, which immediately implies Plünnecke's Theorem:

Proposition 3.1. *Let G be a commutative graph such that $|V_1| \leq K|V_0|$ for some $K \geq 1$. Then $|G^2(A')| \leq K^2|A'|$ for some $A' \subseteq V_1$.*

Note that the particular statement in the case that $K = 1$ of Plünnecke's theorem—i.e. $A, B \subseteq Z$ and $G = G[A, B]$ —is true with $A' = A$: by Exercise 0.2, A is a union of cosets of some subgroup $H \leq Z$ and $B \subseteq H + x$ for some $x \in Z$. But then $B + B \subseteq H + H + x + x = H + (x + x)$, so Exercise 0.2 again shows that $|A + B + B| \leq |A|$. However, we need the full generality of Proposition 3.1 when $K = 1$ in order to prove the theorem for arbitrary $K \geq 1$, as we will see shortly.

Proof (of Proposition 3.1, $K = 1$). Let $s := \text{MAXFLOW}(V_0 \rightarrow V_2; G)$. Since V_1 disconnects V_0 from V_2 in G , Menger's Theorem (Exercise 2.2) implies that $s \leq |V_1| \leq |V_0|$, where the second inequality follows by assumption. By applying Menger's Theorem again, we know that there is a disconnecting set $S \subseteq V_0 \cup V_1 \cup V_2$ such that $|S| = s$. Write $S_j := S \cap V_j$.

The idea is to push S_1 into V_0 in order to form an appropriate A' . To that end, let G' be the subgraph of G whose edges $E'_{0 \rightarrow 1} \cup E'_{1 \rightarrow 2}$ consist of edges in paths

from $V'_0 := V_0 \setminus S_0$ to $V'_2 := V_2 \setminus S_2$. Since S disconnects V'_0 from V'_2 in G' , all such paths must go through S_1 . In addition, $\text{MINCUT}(V_0 \rightarrow V_2; G') = |S_1|$ since if it were any smaller, we could find a set smaller than S that disconnected V_0 from V_2 in G , contradicting the definition of s . Therefore, again by Menger's theorem, there are $|S_1|$ disjoint paths in G' . Let $W_0 \subseteq V'_0$ denote the initial points and $W_2 \subseteq V'_2$ the terminal points of these paths. Clearly $|W_0| = |S_1| = |W_2|$.

Now we note that since G is commutative, so is G' : if $(a \rightarrow a + b) \in E'_{0 \rightarrow 1}$ and $(a + b \rightarrow a + b + c) \in E'_{1 \rightarrow 2}$, then since G is commutative we know that $(a \rightarrow a + c) \in E_{0 \rightarrow 1}$ and $(a + c \rightarrow a + c + b) \in E_{1 \rightarrow 2}$. But $a \rightarrow a + c \rightarrow a + c + b$ is a path from $a \in V'_0$ to $a + b + c \in V'_2$, so its edges are in $E'_{0 \rightarrow 1}$ and $E'_{1 \rightarrow 2}$ as needed. To put this fact to use, recall from the discussion preceding the statement of the proposition that by pulling back along the $|S_1|$ disjoint paths through S_1 , we get an injection from *all the edges in $E'_{1 \rightarrow 2}$* to those edges E_{W_0} in $E'_{0 \rightarrow 1}$ that start in W_0 . Similarly, by pushing forward along these disjoint paths, we get an injection from $E'_{0 \rightarrow 1}$ to the edges E_{W_2} in $E'_{1 \rightarrow 2}$ that end in W_2 . Therefore

$$E'_{0 \rightarrow 1} \hookrightarrow E_{W_2} \subseteq E'_{1 \rightarrow 2} \hookrightarrow E_{W_0} \subseteq E'_{0 \rightarrow 1}$$

and thus all five sets are the same size.

In particular, all edges in $E'_{0 \rightarrow 1}$ start in W_0 , so we may replace S_1 with W_0 to get a set $S_0 \cup W_0 \cup S_2$ disconnecting V_0 from V_2 in G . Set $A' = V_0 \setminus (S_0 \cup W_0)$. Then $G^2(A') \subseteq S_2$ since otherwise there would be a path from V_0 to V_2 whose endpoints are neither in $S_0 \cup W_0$ nor S_2 , contradicting $|S_0 \sqcup W_0 \sqcup S_2| = s$. Finally, since $|S_0| + |W_0| + |S_2| = s \leq |V_0|$, we have

$$\begin{aligned} |G^2(A')| &\leq |S_2| \\ &\leq |V_0| - (|S_0| + |W_0|) \\ &= |A'| \end{aligned}$$

as needed. \square

Although the proof may seem a bit long-winded, I believe that it deserves this space because each time I have discussed it with others, we have gotten confused. Hopefully its length has not deterred you from digesting it.

In order to pass from $K = 1$ to the general case $K \geq 1$, we make the following definition. Let G be a commutative graph. Define the **magnification ratio** $D(G)$ by

$$D(G) := \min_{\emptyset \neq A' \subseteq V_0} \frac{|G^2(A')|}{|A'|}$$

Then Proposition 3.1 says that $|V_1|/|V_0| \leq 1$ implies that $D(G) \leq 1$. In order to finish proving Plünnecke's theorem, we must show that $|V_1|/|V_0| \leq K$ implies that $D(G) \leq K^2$ for any $K \geq 1$. In order to prove the general case, we will use the Cartesian product trick, so the following lemma will be useful:

Lemma 3.2. *If G and \tilde{G} are commutative graphs, then $D(G \times \tilde{G}) = D(G) \cdot D(\tilde{G})$.*

Before proving the lemma, we note that $D(G \times \tilde{G})$ is well-defined by Exercise 2.1. We will also require the following observation, which we leave as an exercise:

Exercise 3.1. *Given commutative graphs G and \tilde{G} and subsets $A \subseteq V_0$ and $\tilde{A} \subseteq \tilde{V}_0$,*

$$(G \times \tilde{G})^2(A \times \tilde{A}) = G^2(A) \times \tilde{G}^2(\tilde{A})$$

Proof (of Lemma 3.2). Write $d = D(G)$ and $\tilde{d} = D(\tilde{G})$. Then by the definition of magnification ratio, there are subsets $A' \subseteq V_0$ and $\tilde{A}' \subseteq \tilde{V}_0$ such that

$$|G^2(A')| = d|A'| \text{ and } |G^2(\tilde{A}')| = d|\tilde{A}'|$$

Therefore, by Exercise 3.1,

$$\begin{aligned} |(G \times \tilde{G})^2(A' \times \tilde{A}')| &= |G^2(A')| \cdot |\tilde{G}^2(\tilde{A}')| \\ &= d\tilde{d}|A'||\tilde{A}'| = d\tilde{d}|A' \times \tilde{A}'| \end{aligned}$$

So, since

$$\frac{|(G \times \tilde{G})^2(A' \times \tilde{A}')|}{|A' \times \tilde{A}'|} = d\tilde{d}$$

we have shown that $D(G \times \tilde{G}) \leq d\tilde{d}$.

It remains to show the opposite inequality, i.e. for any $U \subseteq V_0 \times \tilde{V}_0$,

$$\frac{|(G \times \tilde{G})^2(U)|}{|U|} \geq d\tilde{d}$$

To do so, we factor the set $(G \times \tilde{G})^2(U)$. First let $I_{V_0} = G[V_0, \{0\}]$ be the commutative graph whose three vertex sets are all equal to (disjoint copies of) V_0 and whose edges correspond to loops on the vertices of V_0 , that is the graph consisting of $|V_0|$ disjoint paths of length two. Similarly define $I_{\tilde{V}_2} = G[\tilde{V}_2, \{0\}]$. First I claim that

$$(9) \quad (G \times \tilde{G})^2(U) = (G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$$

To see this, let $z \in (G \times \tilde{G})^2(U)$. This means that there is a point $x \in U$ and edges e, e' that form a path from x to z through some $y \in V_1 \times \tilde{V}_1$. Write $z = (a + b + c, \tilde{a} + \tilde{b} + \tilde{c})$, where $x = (a, \tilde{a})$ and $y = (a + b, \tilde{a} + \tilde{b})$. Note that by exercise 3.1, $(a \rightarrow a + b + c) \in G^2(U_0)$ and $(\tilde{a} \rightarrow \tilde{a} + \tilde{b} + \tilde{c}) \in \tilde{G}^2(\tilde{U}_0)$ where $U = U_0 \times \tilde{U}_0$. Consider the path

$$(10) \quad (a, \tilde{a}) \rightarrow (a, \tilde{a} + \tilde{b} + \tilde{c}) \rightarrow (a + b + c, \tilde{a} + \tilde{b} + \tilde{c})$$

The first is an edge from U to $(I_{V_0} \times \tilde{G})^2(U)$, and the second is from $(I_{V_0} \times \tilde{G})^2$ to $(G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$. Therefore $(G \times \tilde{G})^2(U) \subseteq (G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)$. To prove the other inclusion, note that we may collapse a path of the form (10) to one from U to $(G \times \tilde{G})^2(U)$, and equation (9) follows.

Now I claim that $D(I_{V_0} \times \tilde{G}) = \tilde{d}$ and $D(G \times I_{\tilde{V}_2}) = d$; this follows from Exercise 3.1, and the fact that, for example, $|I_{V_0}^2(X)| = |X|$ for any $X \subset V_0$. Therefore, by this and the above claim, we compute

$$\begin{aligned} |(G \times \tilde{G})^2(U)| &= |(G \times I_{\tilde{V}_2})^2(I_{V_0} \times \tilde{G})^2(U)| \\ &\geq D(G \times I_{\tilde{V}_2})|(I_{V_0} \times \tilde{G})^2(U)| \\ &\geq D(G \times I_{\tilde{V}_2})D(I_{V_0} \times \tilde{G})|U| \\ &= d\tilde{d}|U| \end{aligned}$$

so we are done. \square

To finish the proof of Plünnecke's theorem, we require some more notation. For any $k \in \mathbb{N}$, define $G_k := G[A, B]$ where $A = \{0\}$ and $B = \{e_1, \dots, e_k\}$ is the standard basis for $Z = \mathbb{Z}^k$. Then $|V_0| = 1$, $|V_1| = k$, and

$$D(G_k) = |G_k^2(A)| = \binom{k}{2} + k = \frac{k(k+1)}{2}$$

As before, define G_k^\dagger to be the reflected (commutative) graph of G_k , i.e. swap V_0 and V_2 and reverse all the edges. Then $|V_0^\dagger| = k(k+1)/2$, $|V_1^\dagger| = k$, and $D(G_k^\dagger) = \frac{2}{k(k+1)}$.

Proof (of Proposition 3.1). Let k be an integer between $2K - 1$ and $2K$ so that

$$\left(\frac{|V_1|}{|V_0|}\right) \frac{2}{k+1} \leq 1$$

Then for the vertex sets of $\tilde{G} := G \times G_k^\dagger$, we have

$$\begin{aligned} \frac{|\tilde{V}_1|}{|\tilde{V}_0|} &= \frac{|V_1||V_1^\dagger|}{|V_0||V_0^\dagger|} \\ &= \left(\frac{|V_1|}{|V_0|}\right) \left(\frac{k}{k(k+1)/2}\right) \leq 1 \end{aligned}$$

Therefore the case $K = 1$ applies to $G \times G_k^\dagger$, and thus $D(G \times G_k^\dagger) \leq 1$, and Lemma 3.2 yields

$$(11) \quad D(G) \leq \frac{1}{D(G_k^\dagger)} = \frac{k(k+1)}{2} \leq 10K^2$$

This is on the right track, but we have picked up a factor of 10 that we should like to get rid of. No matter; applying (11) to $G^M = G \times G \times \dots \times G$, we see (using Lemma 3.2 and the fact that $|V_1^M|/|V_0^M| = |V_1|^M/|V_0|^M \leq K^M$) that

$$D(G)^M = D(G^M) \leq 10K^{2M}$$

so $D(G) \leq 10^{1/M} K^2$ for arbitrary M , so we're done. \square

Note that for all $k > 1$, $G_k^\dagger \neq G[A, B]$ for any A, B , so we could not apply the argument above using Exercise 0.2 to the product graph \tilde{G} .

Clearly we may iterate Plünnecke's theorem to higher sums:

$$\begin{aligned} |A + B| &\leq K|A| \\ |A' + B + B| &\leq K^2|A| \\ |A'' + (B + B) + (B + B)| &\leq K^4|A| \\ |A_n + nB| &\leq K^C|A_n| \end{aligned}$$

for some absolute constant $C = C(n)$ depending only on n . By the above computations, since $m \leq n$ implies that $mB \subseteq x + nB$, we may take $C(n) = 2^{\lceil \log_2 n \rceil}$; furthermore, by modifying the proof of Proposition 3.1, it's possible to show:

Exercise 3.2. *In the above setup, show that it is possible to take $C(n) = n$.*

Furthermore, we may use these bounds plus Lemma 1.3 to see that (WLOG, $n \geq m$):

$$\begin{aligned} |nB - mB| &\leq \frac{|A_n + nB||A_n + mB|}{|A_n|} \\ &\leq \left(\frac{|A_n + nB|}{|A_n|} \right)^2 |A_n| \\ &\leq K^{2C(n)} |A_n| \leq K^{2C(n)} |A| \end{aligned}$$

This is the much-anticipated Sumset estimates, which we now record as a theorem for future reference:

Theorem 3.3 (Sumset estimates). *Let $A, B \subseteq Z$ be nonempty subsets of an abelian group Z such that $|A + B| \leq K|A|$ for some $K \geq 1$. Then*

$$|nB - mB| \leq K^{C(n,m)} |A|$$

We will use the Sumset estimates next week to show that if $F = \mathbb{Z}/p\mathbb{Z}$ has no approximate subrings, then $|A \cdot A - A \cdot A|$ is small relative to A , and the week after that we will use this to show that then $|P(A, A, \dots, A)|$ is small relative to $|A|$ for any polynomial P , which will contradict our conclusion from last time and prove that F has no approximate subrings.

References.

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

4. $|A \cdot A - A \cdot A|$ SMALL IMPLIES $|P(A, \dots, A)|$ SMALL

Recall that our goal is to prove the BKT theorem, which roughly says that no finite field F of prime order has approximate subrings. The first half of the proof was to find a polynomial $P \in \mathbb{Z}[X_1, \dots, X_n]$ such that $P(A, \dots, A) = F$ for all such fields F and any reasonably sized subset $A \subseteq F$. Last week, we proved the sumset estimates, Theorem 3.3, which will help us today to control the size of $|nA - mA|$ given a good understanding of the size of $|A - A|$. This will show up again next week when we show that if F has an approximate subring A , then $|A \cdot A - A \cdot A|$ is small, too. Given this and the following Theorem, we can deduce the BKT theorem, which we shall do shortly:

Theorem 4.1. *Suppose that $A \subseteq F$ is nonempty and contains $1 \in F$. Furthermore suppose that $|A \cdot A - A \cdot A| \leq K|A|$ for some $K \geq 1$. Then*

$$|P(A, \dots, A)| \leq CK^C|A|$$

for all polynomials P and some constant C (depending only on P).

Before we begin the proof of the theorem, we need to set up some notation and prove a few preliminary results. We will say that A is **essentially contained** in B (denoted $A \Subset B$) if there is a subset $X \subseteq F$ such that $|X| \leq DK^D$ for some constant D (independent of A , B , and F) and $A \subseteq X + B$. Note that this is a transitive property: if $A \Subset B$ and $B \Subset C$, then there are X_A and X_B with $|X_A| \leq D_A K^{D_A}$ and $A \subseteq X_A + B$ (and similarly for X_B). Thus

$$A \subseteq X_A + B \subseteq X_A + X_B + C$$

but $|X_A + X_B| \leq (D_A K^{D_A})(D_B K^{D_B}) \leq D_C K^{D_C}$ for some D_C independent of A, B, C and F , so $A \Subset C$ as claimed.⁴

Now we prove another useful lemma by Ruzsa, which has a similar flavor to Lemma 1.3 and Exercise 1.2:

Lemma 4.2. *Let $A, B \subseteq F$ such that $|A + B| \leq CK^C|A|$. Then $B \Subset A - A$.*

Proof. Let $X \subseteq B$ be maximal with respect to the property that the $x + A$ are disjoint for $x \in X$. Then

$$|X||A| = \sum |x + A| = \left| \bigcup (x + A) \right| \leq |A + B|$$

by translation invariance and the fact that $X \subseteq B$. Thus X has the desired cardinality, so it remains to show that $B \subseteq X + A - A$. But the maximality of X ensures that for all $b \in B$, the sets $b + A$ and $x + A$ intersect for some $x \in X$. That is, for every b , there are $a_1, a_2 \in A$ and $x \in X$ such that $b + a_1 = x + a_2$, or $b = x + a_2 - a_1$, which is in $X + A - A$. \square

We will make another convenient definition so we don't need to keep track of pesky constants. We will say that an element $x \in F$ is **good** if $x \cdot A \Subset A - A$. Now we use Lemma 4.2 to find some good elements in F :

Proposition 4.3. *Assuming the hypotheses of Theorem 4.1:*

- (1) *All elements of A are good*
- (2) *$x, y \in F$ good $\Rightarrow x + y$ good*

⁴In order to improve readability of this text, we will suppress such detailed arguments involving constants implied by this notation. See the appendix for more details.

(3) $x, y \in F$ good $\Rightarrow xy$ good

Proof of 1. For all $a_1, a_2, a_3 \in A$, we certainly have

$$a_1 a_2 - a_3 = a_1 a_2 - a_3 \cdot 1 \in A \cdot A - A \cdot A$$

by the assumption on A . Therefore

$$|A \cdot A - A| \leq |A \cdot A - A \cdot A| \leq K|A|$$

So applying Lemma 4.2 with $B = A \cdot A$, we find that $A \cdot A \subseteq A - A$, which implies that all elements of A are good. \square

Proof of 2. Suppose that $x \cdot A \subseteq A - A$ and $y \cdot A \subseteq A - A$. Then

$$(x + y) \cdot A \subseteq x \cdot A + y \cdot A \subseteq A - A + A - A$$

But by the hypothesis on A , we know $A \subseteq A \cdot A$, so

$$|A - A| \leq |A \cdot A - A \cdot A| \leq K|A|$$

Therefore $|A - A + A - A + A| \leq K^C|A|$ by sumset estimates (Theorem 3.3) where C is some absolute constant.⁵ Therefore, by applying Lemma 4.2 with $B = A - A + A - A$, we see that

$$(12) \quad A - A + A - A \subseteq A - A$$

Therefore, since \subseteq is transitive, $(x + y) \cdot A \subseteq A - A$ as needed. \square

Exercise 4.1. Prove part 3 of Proposition 4.3.

Exercise 4.2. Use Proposition 4.3 to show that for any polynomial $P \in \mathbb{Z}[X_1, \dots, X_n]$, all elements $x \in P(A, \dots, A)$ are good.

Now we may prove the Theorem.

Proof of Theorem 4.1. We will temporarily use the notation $A^1 := A, A^k := A^{k-1} \cdot A$. The result follows from this:

claim: $A^k \subseteq A - A$ for all $k \geq 1$.

Indeed, if this were true, then applying a similar argument to that in Exercise 4.2 yields

$$P(A, \dots, A) \subseteq A - A,$$

which says that there is a set $X \subseteq F$ with $|X| \leq CK^C$ for some constant C and

$$\begin{aligned} P(A, \dots, A) &\subseteq X + A - A \\ \Rightarrow |P(A, \dots, A)| &\leq |X||A - A| \\ &\leq CK^C|A \cdot A - A \cdot A| \leq (C + 1)K^{(C+1)}|A| \end{aligned}$$

So, it remains to prove the claim, which we will do by induction. The case when $k = 1$ is trivial, and the case $k = 2$ was dealt with in the proof of part 1 of Proposition 4.3. Now we assume that $k > 2$ and that the claim has been proven for A^{k-1} . Thus there is a subset $X \subseteq F$ such that $A^{k-1} \subseteq X + A - A$ and $|X| \leq CK^C$ for some constant C independent of A . That is, for every $a_{k-1} \in A^{k-1}$, there exists an $x \in X$ and $a, a' \in A$ such that

$$a_{k-1} = x + a - a' \Rightarrow x = a_{k-1} - a + a'$$

⁵Indeed, by exercise 3.2, we may take $C = 5$.

so we may ensure that $X \subseteq A^{k-1} - A + A$ by removing superfluous elements from X . But then by Exercise 4.2, we notice that all elements of X are good since $A^{k-1} - A + A$ is certainly a polynomial expression in A . Now we multiply by A to get

$$A^k \subseteq X \cdot A + A \cdot A - A \cdot A$$

But for each $x \in X$, there is a small Y_x such that

$$x \cdot A \subseteq Y_x + A - A$$

since x is good, so

$$X \cdot A \subseteq \bigcup (Y_x + A - A) \subseteq \bigcup (Y_x) + A - A$$

But $Y = \cup Y_x$ is small, and $A^k \subseteq (Y + A - A) + A \cdot A + A \cdot A$, so

$$A^k \subseteq A - A + A - A + A - A$$

Now we apply sumset estimates and Ruzsa's lemma again—as in the proof of the second part of the proposition—to finish the proof of the claim. \square

Proof of Theorem 0.1. Let $\delta > 0$ be given. Recall that Lemmas 2.1 and 2.2 combine to give us a polynomial P depending only on δ such that $P(A, \dots, A) = F := \mathbb{Z}/p\mathbb{Z}$ for any prime p and all $A \subset F$ with $p^\delta < |A| < p^{1-\delta}$. First we note that BKT is automatically true for small p depending only on δ since, given any such bound on p , there are only finitely many such F and A , so it is easy to find c and ε that satisfy the conclusion of the theorem for those p . (We will later put a constraint on p based only on δ .) If the conclusion were false, then there would be an $A \subseteq F$ such that $|A + A|$ and $|A \cdot A|$ are both $\leq K|A|^{1+\varepsilon} = K|A|^\varepsilon|A|$ for all $\varepsilon > 0$ and some K depending on ε . From next week's results, we know that this implies

$$|A \cdot A - A \cdot A| \leq CK^C|A|^{1+C\varepsilon}$$

for some constant C , and then by today's main result (Theorem 4.1), $|P(A, \dots, A)| \leq DK^D|A|^{1+D\varepsilon}$ for a constant D (since P is fixed). Now we choose $\varepsilon > 0$ so that $\delta + D\varepsilon(\delta - 1) > 0$. Notice that ε depends only on δ and D , but D is a universal constant, so we may demand that p satisfies

$$p^{\delta + D\varepsilon(\delta - 1)} > DK^D$$

by the above discussion. Putting this all together, along with the bounds on $|A|$ in the hypotheses, we get

$$p > DK^D|A|^{1+D\varepsilon} \geq |P(A, \dots, A)| = p$$

which is a contradiction, proving the theorem. \square

We will fill the gap of the proof next week when we present Gowers' version of the Balog-Szemerédi theorem in order to show that an approximate subring A also has small $A \cdot A - A \cdot A$.

5. AN APPROXIMATE SUBRING A HAS SMALL $|A \cdot A + A \cdot A|$

Today we will fill the gap left from last time, namely that if a subset $A \subseteq F$ has small sumset $A + A$ and product set $A \cdot A$ has small sum-product set $A \cdot A + A \cdot A$. This may seem clear given the notation, but it actually takes a bit of work to prove. The key ingredient is Tim Gowers' quantitative version of a theorem of Balog-Szemerédi (see [1]). According to Gowers in [2], the original proof of Balog-Szemerédi may be traced through to find bounds on the constants at play, but the bounds are poor and of little use in practice. Gowers found a nice, elementary proof (requiring only Hölder's inequality, a proof of which we include in the appendix for the sake of completeness) that not only reproves the Balog-Szemerédi theorem, but also gives good information on the constants involved.

Recall that during weeks 1 and 2 we found a polynomial P such that, in the situation of Theorem 0.1, $P(A, \dots, A) = F$. Last week, we showed in full detail that if the sum-product set $A \cdot A - A \cdot A$ is small, then $P(A, \dots, A)$ is small in such a way that lead to a contradiction. Thus we were able to conclude that the BKT theorem was true. The missing piece is this (recall that the \lesssim notation means $O(\cdot)$ where the implied constant is independent of the argument):

Theorem 5.1. *Let $A \subseteq F$ such that $|A + A|, |A \cdot A| \leq K|A|$ for some constant K . Then there is a subset $A' \subseteq A$ with $|A'| \approx |A|$ and $|A' \cdot A' + A' \cdot A'| \lesssim |A'|$.*

The careful reader will now notice that, unless there is a stronger result than this, we must have been lying a little bit last week in the proof of BKT. So far, I have always been promising that if A is an approximate subring, then its product-sum set is small, but this is not necessarily true. In general, we must pass to a large subset, but this does not affect the proof of BKT since the polynomial P depends only on δ ; in particular, it is independent of the subset A . Thus, although it's not the result one might have expected, it is sufficient for our purposes.

Before we prove Theorem 5.1, we will state and prove Gowers' result. We let G denote some (additive) abelian group. The notation that we use is Gowers', and as he states in [2], it is non-standard, so we spend a minute on it here. Let $f, g : G \rightarrow \mathbb{Z}$, and define a convolution operator $*$ by

$$(f * g)(x) = \sum_{x=s-t} f(s)g(t)$$

We will identify a set A with its characteristic function χ_A , so then

$$A * A(x) = \sum_{x=s-t} \chi_A(s)\chi_A(t)$$

is the number of ways that an element $x \in G$ may be written as a difference in $A - A$. Similarly, for each x , the quantity $(A * A(x))^2$ is the number of quadruples $(a, b, c, d) \in A^4$ such that $a - b = x = c - d$, so $\|A * A(x)\|_2^2$ is the number of quadruples $(a, b, c, d) \in A^4$ such that $a - b = c - d$. Now we state Gowers' result ([2], Proposition 12):

Proposition 5.2. *Let $A \subseteq G$, where G is an abelian group, $|A| = m$ is finite, and suppose that $\|A * A\|_2^2 \geq c_0 m^3$ for some constant c_0 . Then there is a constant C (depending only on c_0) and a subset $A' \subseteq A$ such that $|A'| \geq \frac{m}{C}$ and $|A' - A'| \leq Cm$. In fact, for all $a, a' \in A'$, there are at least m^7/C solutions (a_1, \dots, a_8) to the equation*

$$a - a' = (a_1 - a_2) - (a_3 - a_4) - ((a_5 - a_6) - (a_7 - a_8))$$

Proof. The function $f(x) = A * A(x) : G \rightarrow \mathbb{Z}$ is nonnegative and it is easy to see that f satisfies:

- $\|f\|_\infty \leq m$
- $\|f\|_1 = m^2$

Therefore $f(x) \geq c_0m/2$ for at least $c_0m/2$ values of x ; otherwise, there would exist a subset $S \subseteq G$, $|S| < c_0m/2$, such that $f(x) \geq c_0m/2$ if and only if $x \in S$, so

$$\begin{aligned} \|f\|_2^2 &= \sum_{x \in S} f(x)^2 + \sum_{x \notin S} f(x)^2 \\ &\leq |S| \|f\|_\infty^2 + \frac{c_0m}{2} \sum_{x \in G} f(x) \\ &< \frac{c_0m}{2} m^2 + \frac{c_0m}{2} m^2 = c_0m^3 \end{aligned}$$

which contradicts the assumption on $\|f\|_2^2$. Call $x \in G$ a **popular difference** if $f(x) \geq c_0m/2$ and define a graph Γ to have vertex set equal to A and an edge between $a, b \in A$ if and only if $a - b$ is a popular difference.

Now we claim that the average degree in Γ is at least $\frac{c_0^2m}{4}$. To see this, first we note that by above, there are at least $c_0m/2$ values of x such that x is a popular difference. But $f(x)$ is the number of ways that x may be written as $x = a - a'$ for $a, a' \in A$, so there are at least $c_0m/2$ popular differences in $A - A$. Therefore, there are at least $c_0m/2$ distinct differences $a - a' \in A - A$ such that $f(a - a') \geq c_0m/2$, so for each of these pairs there are at least $c_0m/2$ pairs (x, y) such that $x - y = a - a'$, each of which corresponds to a distinct edge in Γ , so there are at least $(c_0m/2)^2$ distinct edges in Γ . Thus the claim follows.

By the claim, there are at least $c_0^2m/8$ vertices with degree at least $c_0^2m/8$. Set $\delta = c_0^2/8$ and let a_1, \dots, a_n be those vertices with high degree (where $n \geq \delta m$), and let $N_1(a_i)$ denote the 1-neighborhood in Γ of a_i . By a technical combinatorial lemma, which we relegate to the appendix (see Lemma B.1), there is a subset $A' \subseteq \{a_1, \dots, a_n\}$ such that $|A'| \geq \delta^5 n / \sqrt{2}$ and $|N_1(a_i) \cap N_1(a_j)| \geq \delta^2 m / 2$ for at least 90% of the pairs $(a_i, a_j) \in (A')^2$. Set $\alpha = \delta^2 / \sqrt{2}$, so $|A'| \geq \alpha m$.

Define a new graph Γ' with vertex set A' and edges (a_i, a_j) whenever $|N_1(a_i) \cap N_1(a_j)| \geq \delta^2 m / 2$. By the above, the average degree is $9/10|A'|$, so at least $4/5|A'|$ vertices have degree at least $4/5|A'|$. Let A'' be all such vertices. First observe that

$$|A''| \geq \alpha m = \frac{\delta^6}{\sqrt{2}} m = \left(\frac{c_0^2}{8}\right)^6 \frac{\sqrt{2}}{2} m$$

so A'' has the desired cardinality. Finally, we claim that A'' has small difference set $A'' - A''$. To see this, let $a_i, a_j \in A''$. By the definition of Γ' , the degrees of a_i and a_j are at least $4/5|A'|$ in Γ' , so there exist at least $3/5|A'|$ points $a_k \in A'$ connected to both a_i and a_j in Γ' . By the definition of Γ' , $|N_1(a_i) \cap N_1(a_k)|$ and $|N_1(a_j) \cap N_1(a_k)|$ are at least $\delta^2 m / 2$. Now suppose that $b \in N_1(a_i) \cap N_1(a_k)$. Then $(a_i, b), (a_k, b) \in E(\Gamma)$, the edge set of Γ , so $a_i - b$ and $a_k - b$ are popular differences. Thus, there are at least $(c_0m/2)^2$ ways of writing

$$a_i - a_k = (a_i - b) - (a_k - b) = (p - q) - (r - s)$$

for $(p, q, r, s) \in A^4$, and a similar statement is true for $a_j - a_k$. By unravelling definitions, putting together inequalities, and summing over the at least $3/5|A'|$

points a_k that are connected to both a_i and a_j , one finds that there are at least

$$(3/5)|A'|\delta^4 c_0^4 m^6 / 64 \geq \alpha \delta^4 c_0^4 m^7 / 120$$

ways of writing $a_i - a_j$ as an element of $4A - 4A$. \square

Exercise 5.1. *Provide the details for the end of the proof of Proposition 5.2.*

We will use a slight generalization of the proposition to prove the main result for today. See [3] for an outline of a proof:

Lemma 5.3. *Let $A, B \subseteq G$, $|A| = |B|$, and $|A+B| \leq K|A|$. Then there are subsets $A' \subseteq A$ and $B' \subseteq B$ such that $|A'| \geq C|A|$ and $|B'| \geq C|B|$ for some constant C (depending only on K) and, for fixed $a' \in A'$ and $b' \in B'$, there are at least $|A|^5/C$ solutions to*

$$a' - b' = (a_1 - b_1) - (a_2 - b_2) + a_3 - b_3$$

with $a_i \in A$ and $b_i \in B$.

Exercise 5.2. *Either modify the proof of Proposition 5.2 or expand Tao's argument from [3] to prove the lemma.*

Proof (of Theorem 5.1). The lemma implies that there are subsets $C, D \subseteq A$ such that $|C|, |D| \approx |A|$ and every element of $C - D$ has approximately $|A|^5$ representations of the form

$$c - d = (a_1 - a_2) - (a_3 - a_4) + (a_5 - a_6)$$

with $a_i \in A$. In anticipation of using the full hypothesis that A is an approximate subring, we multiply by an arbitrary element of $A \cdot A \cdot A/A \cdot A$ to find approximately $|A|^5$ representations of the form

$$(13) \quad (b_1 - b_2) - (b_3 - b_4) + (b_5 - b_6)$$

(with $b_i \in A \cdot A \cdot A \cdot A/A \cdot A$) for elements in $(C - D) \cdot A \cdot A \cdot A/A \cdot A$. By removing 0 from A (if necessary), we may apply the multiplicative form of sumset estimates (Theorem 3.3), we know that $|A \cdot A \cdot A \cdot A/A \cdot A| \leq K^6|A|$. Therefore, since the total number of possible representations of the form (13) is $|A|^6$, we must have

$$(14) \quad |(C - D) \cdot A \cdot A \cdot A/A \cdot A| \approx |A|$$

Now we refine C and D in order to find the desired subset $A' \subseteq A$. Since $C \cdot D \subseteq A \cdot A$ and A is an approximate subring, we know that $|C \cdot D| \approx |A|$. Therefore $|C \cdot D| \approx |C| \approx |D|$, so by the multiplicative form of Lemma 5.3, there are subsets $C' \subseteq C$ and $D' \subseteq D$ with $|C'| \approx |C| \approx |A| \approx |D| \approx |D'|$ such that every element of $C' \cdot D'$ has approximately $|A|^5$ representations of the form

$$\frac{c_1 d_1 c_3 d_3}{c_2 d_2}, c_i \in C, d_i \in D$$

with $c_i \in C$ and $d_i \in D$.

Let $c, c' \in C'$ and $d, d' \in D'$ be arbitrary. Then by the pigeonhole principle, there exist $c_2 \in C$ and $d_2 \in D$ such that there are approximately $|A|^3$ solutions to

$$cd = \frac{c_1 d_1 c_3 d_3}{c_2 d_2}$$

We may rewrite this as

$$cd - c'd' = x_1 - x_2 + x_3 - x_4$$

where

$$\begin{aligned} x_1 &= \frac{(c_1 - d')d_1c_3d_3}{c_2d_2} \\ x_2 &= \frac{d'(c' - d_1)c_3d_3}{c_2d_2} \\ x_3 &= \frac{d'c'(c_3 - d_2)d_3}{c_2d_2} \\ x_4 &= \frac{d'c'd_2(c_2 - d_3)}{c_2d_2} \end{aligned}$$

For fixed c', d', c_2, d_2 , it is not hard to see that the map sending (c_1, c_3, d_1, d_3) to (x_1, x_2, x_3, x_4) is injective, and hence a bijection onto its image. Therefore, since all the x_j lie in $(C - D) \cdot A \cdot A \cdot A / A \cdot A$, we thus have approximately $|A|^3$ ways of representing $cd - c'd' \in C' \cdot D' - C' \cdot D'$ in the form $x_1 - x_2 + x_3 - x_4$. By 14 (and an argument similar to that preceding 14), we have

$$(15) \quad |C'D' - C'D'| \lesssim |A|$$

Therefore we surely have $|C'D'| \leq |C'D' - C'D'| \lesssim |A| \approx |C'|$, and thus by the multiplicative form of Lemma 5.3⁶ there are large subsets $C'' \subseteq C'$ and $D'' \subseteq D'$ such that

$$(16) \quad |C''/D''| \lesssim |C'|$$

Finally, we consider the map $\pi : C'' \times D'' \rightarrow C''/D''$ defined in the obvious way, $(x, y) \mapsto x/y$. Since we have the bound (16), the pigeonhole principle guarantees the existence of an $x/y \in C''/D''$ such that

$$|\pi^{-1}(x/y)| \geq \frac{|C''||D''|}{|C''/D''|} \approx |A|$$

But for all $(c, d) \in \pi^{-1}(x/y)$, we know $c = d(x/y)$. Thus

$$|C'' \cap (D'' \cdot (x/y))| = |\pi^{-1}(x/y)| \approx |A|$$

Now we set $A' := C'' \cap (D'' \cdot (x/y))$, so $|A'| \approx |A|$, and, by translation invariance,

$$|A' \cdot A' - A' \cdot A'| \leq |C' \cdot D' - C' \cdot D'| \lesssim |A|$$

which completes the proof. \square

So we have seen the original proof of the BKT theorem from first principles in complete detail⁷ and I hope that it has provided a good introduction to arithmetic combinatorics. The main tools that we used were the Cauchy-Davenport inequality, sum-set (and product-set) estimates, and a quantitative version of the Balog-Szemerédi Theorem. We also used a few clever lemmas of Imre Ruzsa as well as many impressive arguments of Bourgain, Katz, and Tao. All of the proofs presented here are either from Tao's notes [3], the BKT paper [1], or Gowers' paper on arithmetic progressions of length four [2]. One of the curiosities of the complete proof of BKT, as presented in this course, is that we never had to leave the world of cardinalities of sets; for example, we never applied deep structure theorems like

⁶Tao et al. say this follows from product-set estimates, i.e. the multiplicative form of sumset estimates (our Theorem 3.3), but I can't see it.

⁷See the appendix for more on "complete detail".

Freiman's theorem, although they may have been helpful at times. During the next few weeks, we will look briefly at some generalizations and applications of BKT.

References.

- [1] A. Balog and E. Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14:263–268, 1994.
- [2] W.T. Gowers. A new proof of szemerédi's theorem of arithmetic progressions of length four. *Geom. Funct. Anal.*, 8:529–551, 1998.
- [3] Terry Tao. Math 254a: Some highlights of arithmetic combinatorics, 2003.

6. KONYAGIN'S EXTENSION (PRESENTED BY VLADO)

Today we will prove the following extension of the BKT theorem due to Konyagin [2], and we will follow a proof by Ben Green in his notes from MIT [1]:

Theorem 6.1. *For all $\delta > 0$, there exists a constant $c = c(\delta)$ such that for all primes p and for all subsets $A \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $|A| < p^{1-\delta}$, we have*

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

This is a very nice result because it gets rid of the assumption that A is relatively big. Its proof relies on three results that we have seen previously: sunset/product-set estimates (Theorem 3.3), approximate subrings have small difference of products (Theorem 5.1), and small difference of products implies small polynomial expressions (Theorem 4.1). We begin our proof by defining a rational expression that grows well in general, and is analogous to the set $B \cdot (B - B) + B \cdot (B - B)$ that we encountered in Lemma 2.2. We define the rational expression J by

$$J(A) = \left\{ a_5 \left(\frac{a_1 a_2 - a_3 a_4}{a_3 - a_1} - a_6 \right) : a_i \in A, a_1 \neq a_3 \right\}$$

As usual, let $F := \mathbb{Z}/p\mathbb{Z}$. We begin with a lemma, which is very similar in spirit to our Theorem 5.1.

Lemma 6.2. *If $|A + A|$ and $|A \cdot A|$ are both less than or equal to $K|A|$, then there is an $A'' \subseteq A$ such that $|A''| \geq K^{-c}|A|$ and $|J(A'')| \leq K^c|A|$.*

Proof. By Lemma 5.1, there is a subset $A' \subseteq A$ such that the difference of products is small: $|A'A' - A'A'| \leq K^c$ for some c . Let $X = P(A', \dots, A')$ where $P(X_1, \dots, X_6) = X_5(X_1X_2 - X_3X_4 + X_6X_3 - X_6X_1)$, and fix $x \in X$ with $x \neq 0$. Then we may define a bijection by right multiplication by $1/x^2$:

$$f : \frac{X}{(A' - A') \setminus \{0\}} \hookrightarrow \frac{X}{X \setminus \{0\}}, \quad f\left(\frac{x_0}{a_1 - a_2}\right) = \frac{x_0}{x^2(a_1 - a_2)}$$

Then we have the following estimates, where $Y := X \setminus \{0\}$:

$$|J(A')| \leq \left| \frac{X}{(A' - A') \setminus \{0\}} \right| \leq \left| \frac{X}{X \setminus \{0\}} \right| \leq C \left| \frac{Y}{Y} \right|$$

So, by Theorem 4.1, we have

$$|X \cdot X| \leq K^c|A'| \leq K^c|X|$$

Therefore, by product-set estimates, $|Y/Y| \leq K^c|Y| \leq K^{c'}|A'|$ as needed. (Note that the constant c may change from step to step, but it's still just a constant.) \square

Now we state the main proposition, from which Konyagin's main result will follow quite easily:

Proposition 6.3. *For $A \subseteq \mathbb{Z}/p\mathbb{Z}$,*

- *if $|A| \leq \sqrt{p}$, then $|J(A)| \geq |A|^3/(2|A - A|)$;*
- *if $|A| > \sqrt{p}$, then $|J(A)| \geq p/2$.*

We will say that $\xi \in F$ is **involved with** A if $|A(A + \xi)| < |A|^2$. We require a basic lemma (cf. Lemma 2.2).

Lemma 6.4. *Suppose that ξ is involved with A . Then $J(A)$ contains $A(A + \xi)$.*

Proof. Since ξ is involved, there are $(a_1, a_2) \neq (a_3, a_4)$ such that

$$a_1(a_2 + \xi) = a_3(a_4 + \xi)$$

Therefore $\xi = \frac{a_1 a_2 - a_3 a_4}{a_3 - a_1}$, so for all $a_5, a_6 \in A$ we have $a_5(a_6 + \xi) \in J(A)$ by the definition of J . \square

Now we use the Cauchy-Schwartz inequality to make an averaging argument (cf. Lemma 2 in [2]):

Lemma 6.5. *Suppose that $A \subset F$. Then there is a $\xi \in F$ such that*

$$|A \cdot (A + \xi)| \geq \frac{|A|^2 p}{|A|^2 + p}$$

Proof. See [1], Lemma 5.3. \square

We also omit the proof of the next lemma, which we have taken directly from [1] as well:

Lemma 6.6. *Suppose that $A \subseteq F$ satisfies $|A| \leq \sqrt{p}$ and $|A - A| \leq K|A|$. Then there is some $\xi \in F$ such that ξ is involved with A but not very involved, i.e.*

$$\frac{|A|^2}{2K} \leq |A \cdot (A + \xi)| < |A|^2$$

Proof. See [1], lemma 5.4. \square

Proof of Proposition 6.3. Suppose first that $|A| > \sqrt{p}$. Since $A \cdot (A + \xi) \subseteq F$ and $|F| < |A|^2$, every value of ξ is involved with A . So, by Lemma 6.5, there is some $\xi \in F$ such that

$$p/2 \leq |A \cdot (A + \xi)| < |A|^2$$

Then by Lemma 6.4, we know that $p/2 \leq |A \cdot (A + \xi)| \leq |J(A)|$, so we're done with the first case. For the second, apply Lemma 6.6 to find a ξ that is involved but not very involved and then apply Lemma 6.4 again to conclude that

$$|A|^2/2K \leq |A \cdot (A + \xi)| \leq |J(A)|$$

where $K = |A - A|/|A|$. This completes the proof of the proposition. \square

To finish, we outline a proof of the main theorem; details are left as an exercise, and one is encouraged to use arguments similar to those found at the end of section 4.

Proof of Theorem 6.1. Suppose that $A \subseteq F$ is an approximate subring. Then by Lemma 6.2, there is a subset $A' \subseteq A$ with $|A'| \geq K^{-c}|A|$ and $|J(A')| \leq K^c|A|$. By sumset estimates, we also know that $|A' - A'| \leq |A - A| \leq K|A|$, so by Proposition 6.3, we know that either $|J(A)| \geq p/2$ or

$$|J(A)| \geq |A|^3/2|A - A| = O(|A|^2)$$

so $|J(A')| \gg \min(p, K^{-c}|A|^2)$. By comparing this and the other bound above on $|J(A)|$, one should get a contradiction... these are the details that I leave to the reader. \square

So we have seen that the lower bound on $A \subseteq F$ is unnecessary in the BKT theorem. Clearly, one cannot hope to get rid of the upper bound on A , so the Konyagin extension of the BKT theorem seems best possible. For a great, self-contained proof of the full theorem, see [1].

References.

- [1] Ben Green. Sum-product estimates.
- [2] S.V. Konyagin. A sum-product estimate in fields of prime order, 2003.

7. NOTES ON AN INVERSE THEOREM (BY ANINDYA C. PATTHAK)

- (1) Finite field philosophy : translate questions regarding $\mathbb{Z}/N\mathbb{Z}$ over finite fields.
for eg., What is the largest value of $|A|$ (where $A \subseteq [N]$) with no solutions $x + z = 2y$.
- (2) Offers linear algebraic technique
- (3) Bourgain's observation : some generic machinery to convert arguments on the finite field setting to arguments which work for arbitrary group G by using a kind of an "approximate linear algebra".

We will assume knowledge of basic fourier transform over an arbitrary abelian group.

7.1. Roth's proof : A step into uniformity. Consider $A \subseteq \mathbb{Z}/N\mathbb{Z}$ of density δ (i.e., $|A| = \delta N$). We are interested in length three AP in A . For a set A , by abusing notation, we denote its characteristic function by A .

Now let $A, B, C \subseteq \mathbb{Z}/N\mathbb{Z}$. Then

$$\begin{aligned} \mathbb{E}_{xd} A(x)B(x+d)C(x+2d) &= N^{-2} \sum_{xd} \sum_{rst} \hat{A}(r)\hat{B}(s)\hat{C}(t)w^{-r \cdot x}w^{-s \cdot (x+d)}w^{-t \cdot (x+2d)} \\ &= N^{-1} \sum_x \sum_{rs} \hat{A}(r)\hat{B}(-2s)\hat{C}(s)w^{-x \cdot (r-s)} \\ &= \sum_r \hat{A}(r)\hat{B}(-2r)\hat{C}(r). \end{aligned}$$

If $\max_r \hat{C}(r) \leq \gamma N$ (and assume $|A| = |B|$) then note that the above is bounded by $\gamma N \|\hat{A}\|_2 \|\hat{B}\|_2 = \gamma N^2 |B|$. In that case, we say that the set C is γ -uniform.

Roughly the proof (roughly) follows in two cases : If the set is γ -uniform for a suitable γ , then set $B = A \cap [N/3, 2N/3]$. Then it is shown that exists $(x, y, z) \in A \times B^2$ which is a genuine progression. On the other hand, if the set is not γ -uniform, then it has large fourier component, and then some work is needed to come up with a with a genuine arithmetic progression P of size roughly $\Omega(N^{1/2})$ such that $\frac{|A \cap P|}{|P|} \geq \delta + \epsilon$ for some $\epsilon > 0$. For more details see [2].

7.2. Gowers generalization. We first define convolution. Let $f, g : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$ be two function then

$$f * g(x) \stackrel{\text{def}}{=} \sum_y f(y)\overline{g(x+y)}.$$

We now record a lemma which kind of paves way to the generalization of uniformity to the higher order.

Lemma 7.1. *Let f be a function $f : \mathbb{Z}_N \rightarrow D \subseteq \mathbb{C}$ (D denotes the unit disc). Then the following are equivalent.*

- (1) f is α -uniform i.e., $\max_r |\hat{f}(r)| \leq \alpha N$.
- (2) $\sum_r |\hat{f}(r)|^4 \leq c_1 N^4$, where $c_1 \leq \alpha^2 \leq c_1^{1/2}$.
- (3) $\sum_k |\sum_s f(s)\overline{f(s-k)}|^2 \leq c_1 N^3$.

Proof. Straightforward. (Or see [1].) □

Now observe that

$$\begin{aligned} \sum_k \left| \sum_s f(s) \overline{f(s-k)} \right|^2 &= \sum_k \sum_{st} f(s) \overline{f(s-k)} \overline{f(t)} f(t-k) \\ &= \sum_u \sum_{sv} f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \end{aligned}$$

It turns out that this definition (of pseudorandom set) is not strong enough to prove Szemerédi's theorem for AP of length 4. This is because an α -uniform set need not contain roughly the expected number of length four AP. However, the definition that works is the following.

A function $f : \mathbb{Z}_N \rightarrow D$ is said to be quadratically α -uniform if

$$\sum_{u,v} \left| \sum_s f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \right|^2 \leq \alpha N^4,$$

which can be put into

$$\mathbb{E}_{x, y_1, y_2, y_3} \left(\prod_{S \subseteq [3]} C^{|S|} f\left(x + \sum_{i \in S} y_i\right) \right) \leq \alpha$$

where C is the conjugation operator, which is also known as the (eighth power of) Gowers U^3 -norm.

In general for $d \geq 1$, Gowers U^d th norm is defined as

$$U^d(f) \stackrel{\text{def}}{=} \|f\|_{U^d}^{2^d} \stackrel{\text{def}}{=} \mathbb{E}_{x, y_1, \dots, y_d} \left[\prod_{S \subseteq [d]} C^{|S|} f\left(x + \sum_{i \in S} y_i\right) \right].$$

claim: If a set is quadratically α -uniform, then it is $\sqrt{\alpha}$ uniform.

Proof. Expanding (3) of Lemma 7.1, we get

$$\begin{aligned} \sum_k \sum_{st} |f(s) \overline{f(s-k)} \overline{f(t)} f(t-k)| &= \sum_k \sum_{su} |f(s) \overline{f(s-k)} \overline{f(s-u)} f(s-u-k)| \\ &= \sum_{uv} \left| \sum_s f(s) \overline{f(s-u)} \overline{f(s-v)} f(s-u-v) \right|. \end{aligned}$$

The Claim follows from Cauchy-Schwartz. \square

Remark. The above claim holds for any d and $d+1$ order uniformity, i.e., $(d+1)$ th order uniformity implies d th order uniformity. However, the reverse does not hold. Functions similar to Bent function can be shown to violate the reverse connection.

Proposition 7.2. (Inverse theorem for Gowers norm of order two) $U^2(f) \geq \alpha \implies \|\hat{f}\|_\infty \geq \sqrt{\alpha}$.

Proof. Immediate from Lemma 7.1. \square

7.3. Inverse theorem for Gowers norm of order three.

Question 7.3. Suppose $U^3(f) \geq \delta$, what can we say about f ?

Proposition 7.4. ([3]) (Inverse theorem for U^3 norm over \mathbb{F}_5^n) Suppose that $f : \mathbb{F}_5^n \rightarrow [-1, 1]$ is a function for which $U^3(f) \geq \delta$. Then there exists a matrix $M \in \mathbb{F}_5^{n \times n}$ and a vector r so that

$$|\mathbb{E}_x f(x) w^{(x, Mx+r)}| \geq \Omega(1).$$

([4]) (*Inverse theorem for U^3 norm over \mathbb{F}_2^n*) Suppose that $f : \mathbb{F}_2^n \rightarrow [-1, 1]$ is a function for which $U^3(f) \geq \delta$. Then there exists a quadratic function g such that

$$\text{dist}(f, g) \leq \frac{1}{2} - \epsilon'.$$

7.4. Inverse theorem over \mathbb{F}_2 . We now on follow [4]. Assume that f is a perfect degree two polynomial i.e., $f(x) = (-1)^{\langle Ax, x \rangle + a}$ for some binary matrix and a constant $a \in \{0, 1\}$. Define

$$f_y(x) \stackrel{\text{def}}{=} f(x + y)f(x).$$

Then note that

$$f_y(x) = (-1)^{\langle By, x \rangle + a'}$$

where $B = A + A^t$ is a zero-diagonal symmetric matrix. In particular this implies that $\hat{f}_y(By) = 1$ (for the moment, ignore the sign). Now if f is not a perfect two degree polynomial, still something like this holds which we now demonstrate.

Lemma 7.5. *Let B be a symmetric matrix with zero diagonal (i.e., symplectic) such that $\mathbb{E}_y \hat{f}_y^2(By) \geq \epsilon$, then there exists a quadratic polynomial g such that*

$$\|f - g\| \leq \frac{1}{2} - \epsilon'.$$

Proof. See [4]. □

Also we need to show that

Lemma 7.6. $U^3(f) \geq \delta \implies \mathbb{E}_y \hat{f}_y^2(By) \geq \epsilon$ for a symplectic matrix B .

We also need a quantitative analog of Balog-Szemerédi theorem. We follow Gowers [1, 2]. We begin with a combinatorial lemma.

Lemma 7.7. *Let X be a set of size m , and let A_1, \dots, A_n are subsets of X such that $\sum_{i, j \in [n]} |A_i \cap A_j| \geq \delta^2 mn^2$. Then there is a set $K \subseteq [n]$ of size at least $\delta^5 n / \sqrt{2}$, such that, for at least 16/17 fraction (or 90%) of the pairs of $(i, j) \in K^2$ $|A_i \cap A_j| \geq \delta^2 m / 2$.*

In particular, the result holds if $|A_i| \geq \delta m$ for all $i \in [n]$.

Proof. Let $B_i = \{j | i \in A_j\}$. Define $E_i = B_i^2$. For any given $x, y \in [n]$, We first calculate

$$p_{xy} \stackrel{\text{def}}{=} \Pr_{i \in [m]} [(x, y) \in E_i] = \frac{|A_x \cap A_y|}{m}.$$

Now choose independently and uniformly randomly j_1, \dots, j_5 and set

$$X = \cap_{k \in [5]} E_{j_k}.$$

Clearly, $\Pr[(x, y) \in X] = p_{xy}^5$. Thus

$$\mathbb{E}X = \sum_{xy} p_{xy}^5.$$

However, since $\sum_{xy} p_{xy} \geq \delta^2 n^2$, and since $\left(\frac{\sum p_{xy}}{n^2}\right)^5 \leq \left(\frac{\sum p_{xy}^5}{n^2}\right)$, we obtain $\mathbb{E}X \geq \delta^{10} n^2$. For the random choice of X , consider the subset $Y \stackrel{\text{def}}{=} \{(i, j) \in X : |A_i \cap A_j| \leq \delta^2 m / 2\}$ (i.e., all (i, j) such that $p_{ij} \leq \delta^2 / 2$). Clearly then $\mathbb{E}Y \leq (\delta^2 / 2)^5 n^2$. Thus $\mathbb{E}|X - 16Y| \geq \delta^{10} n^2 / 2$.

Thus there exists a choice of j_r such that $|X| \geq 16|Y|$ and $EX \geq \delta^1 0n^2/2$. Set $K^2 = X$ (i.e., $K \stackrel{\text{def}}{=} \cap B_{j_r}$).

For the second statement, let $s_i = |B_i|$. Then note $\frac{\sum_i s_i^2}{m} \geq \left(\frac{\sum_i s_i}{m}\right)^2 \geq \left(\frac{\delta m \cdot n}{m}\right)^2 \geq \delta^2 n^2$. □

We are now ready to prove the Balog-Szemerédi theorem. Given a set $A \in \mathbb{Z}^D$, by abuse of notation by A we also mean its characteristics function. Then note that

$$A * A(x) = \sum_y A(y)A(x+y) = \#\{(w, z) \in A^2 : x = w - z\}$$

Furthermore, note that

$$\begin{aligned} \|A * A\|_2^2 &= \sum_x A * A(x)^2 \\ &= \sum_{xyz} A(y)A(z)A(x+y)A(x+z) \\ &= \sum_{\substack{u-y=w-z \\ (u,w,y,z) \in A^4}} 1 = \#\{(u, y, z, w) \in A^4 : u - y = w - z\} \end{aligned}$$

We now consider the following proposition. [This is the same as Theorem 5.2 from Week 5, and the above lemma is the one promised to be included in the appendix. –ed.]

Proposition 7.8. *Let A be a subset of \mathbb{Z}^D of size m such that $\|A * A\|_2^2 \geq c_0 m^3$. Then there exists a subset $A'' \subset A$ of size at least cm such that $|A'' - A''| \leq Cm$. Moreover, C and c depends only on c_0 .*

Proof. Let define $f(x) = A * A(x)$. Then clearly $\|f\|_1 = m^2$, $\|f\|_\infty \leq m$, $\|f\|_2^2 \geq c_0 m^3$. Thus by an simple averaging argument

$$|A_1 \stackrel{\text{def}}{=} \{x : f(x) \geq c_0 m/2\}| \geq c_0 m/2.$$

Now define a graph G on the vertices of A , where $y \sim z$ iff $y - z \in A_1$ (and so is $(z - y)$). Clearly the average degree of the graph is at least $c_0^2 m^2 / (4m) = (c_0^2/4)m$. Thus again by averaging argument, there exists a set of vertices $A_2 \subseteq A$ of size $n \geq (c_0^2/8)m$ such that each of them has degree at least $(c_0^2/8)m$. Denote $\delta \stackrel{\text{def}}{=} c_0^2/8$. Denote the elements of A_2 as a_1, \dots, a_n , and their immediate neighbors by N_1, \dots, N_n . Note that for each i , $|N_i| \geq \delta m$. Thus by the previous lemma there exists a set $K \subset [n]$ such that 90% of the indices of $(i, j) \in K^2$ it holds $|N_i \cap N_j| \geq \delta^2 m/2$. Note that $|K| \geq \delta^5 n / \sqrt{2}$.

We now define a graph H on the vertices set of K where the edges are $\{(i, j) : |N_i \cap N_j| \geq \delta^2 m/2\}$. By the lemma above, the average degree of this graph is at least $9/10$. Thus applying averaging argument once again we note that there is a set of size at least $4|K|/5$ such that each of them has average degree $4|K|/5$ in H . Call this set A'' , this is the set that has small difference set. To see this, note that let $a_i, a_j \in A''$. Then note that a_i and a_j has at least $3|K|/5$ common neighbors. For each common neighbor a_k , it holds that $|N_i \cap N_k| \geq \delta^2 m/2$. For each $b \in N_i \cap N_k$, from the definition of graph G , $a_i - b$ and $b - a_k$ are popular differences, say p and q , respectively. Furthermore, each such popular difference,

say p , can be written as $p_1 - p_2$ in $c_0m/2$ ways. Thus $a_i - a_k$ can be written as $(a_i - b) - (a_k - b) = (p_1 - p_2) - (q_1 - q_2)$ in $\delta^2m/2 \times (c_0m/2)^2$. Similarly $a_j - a_k$ can be written as $(r_1 - r_2) - (s_1 - s_2)$ in $\delta^2m/2 \times (c_0m/2)^2$. Thus $a_i - a_j$ can be written as $(p_1 - p_2) - (q_1 - q_2) - (r_1 - r_2) + (s_1 - s_2)$ in at least $3|K|/5 \cdot (\delta^2m/2 \times c_0^2m^2/4)^2$ i.e., $\frac{3}{5} \cdot \frac{\delta^9 c_0^4 m^7}{2^7}$ many ways. Thus $A'' - A''$ can not have more than Cm many distinct element, for some C . □

References.

- [1] W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *GFAA (Geometric and Functional Analysis)*, 8, 1998.
- [2] W. T. Gowers. A new proof of Szemerédi's theorem. *GFAA (Geometric and Functional Analysis)*, 11(3):465–588, 2001.
- [3] B. Green and T. Tao. An inverse theorem for the Gowers U^3 norm. *math.NT/0503014*, 2005.
- [4] A. Samorodnitsky. Low-degree tests at large distance. In *ECCC report No 54*, 2006.

APPENDIX Appendix A. HANDLING CONSTANTS WITH CARE

Our goal for this appendix is to expand some of the arguments involving implicit constants in order to allay any uneasiness that may have been effected by the apparent lack of rigor.

(coming soon...)

APPENDIX Appendix B. GOWERS' TECHNICAL LEMMA

The objective of this appendix is to provide proofs of Gowers' technical lemma used to prove Proposition 5.2 as well as a proof of Hölder's inequality, which is the only non-elementary result that the proof of that lemma requires.

Much to my surprise, Anindya reproved Gowers' quantitative version of the Balog-Szemerédi theorem in his notes on the Gowers' norm, and in so doing he typed up the technical combinatorial lemma required in Gowers' proof. As promised in Week 5, I am providing it here in the appendix, although you may also find it in Anindya's notes for Week 7.

Lemma B.1. *Let X be a set of size m , and let A_1, \dots, A_n are subsets of X such that $\sum_{i,j \in [n]} |A_i \cap A_j| \geq \delta^2 m n^2$. Then there is a set $K \subseteq [n]$ of size at least $\delta^5 n / \sqrt{2}$, such that, for at least $16/17$ fraction (or 90%) of the pairs of $(i, j) \in K^2$ $|A_i \cap A_j| \geq \delta^2 m / 2$.*

In particular, the result holds if $|A_i| \geq \delta m$ for all $i \in [n]$.

Proof. Let $B_i = \{j \mid i \in A_j\}$. Define $E_i = B_i^2$. For any given $x, y \in [n]$, We first calculate

$$p_{xy} \stackrel{\text{def}}{=} \Pr_{i \in [m]} [(x, y) \in E_i] = \frac{|A_x \cap A_y|}{m}.$$

Now choose independently and uniformly randomly j_1, \dots, j_5 and set

$$X = \bigcap_{k \in [5]} E_{j_k}.$$

Clearly, $\Pr[(x, y) \in X] = p_{xy}^5$. Thus

$$\mathbb{E}X = \sum_{xy} p_{xy}^5.$$

However, since $\sum_{xy} p_{xy} \geq \delta^2 n^2$, and since $\left(\frac{\sum p_{xy}}{n^2}\right)^5 \leq \left(\frac{\sum p_{xy}^5}{n^2}\right)$, we obtain $\mathbb{E}X \geq \delta^{10} n^2$. For the random choice of X , consider the subset $Y \stackrel{\text{def}}{=} \{(i, j) \in X : |A_i \cap A_j| \leq \delta^2 m / 2\}$ (i.e., all (i, j) such that $p_{ij} \leq \delta^2 / 2$). Clearly then $\mathbb{E}Y \leq (\delta^2 / 2)^5 n^2$. Thus $\mathbb{E}|X - 16Y| \geq \delta^{10} n^2 / 2$.

Thus there exists a choice of j_r such that $|X| \geq 16|Y|$ and $\mathbb{E}X \geq \delta^{10} n^2 / 2$. Set $K^2 = X$ (i.e., $K \stackrel{\text{def}}{=} \bigcap B_{j_r}$).

For the second statement, let $s_i = |B_i|$. Then note $\frac{\sum_i s_i^2}{m} \geq \left(\frac{\sum_i s_i}{m}\right)^2 \geq \left(\frac{\delta m \cdot n}{m}\right)^2 \geq \delta^2 n^2$. □

Finally, to complete the proof of the BKT theorem, we present the following theorem, well-known from analysis:

Theorem B.2 (Hölder's Inequality).