10. Sum-product theory

Tues March 18

The best bounds in projection theory are different in different fields. The best bounds for projections of balls in $\mathbb{C}^2$ are different than in $\mathbb{R}^2$. The best bounds for projections in $\mathbb{F}_{p^2}^2$ are different than for $\mathbb{F}_p^2$. Most of the recent work in projection theory is concerned with understanding these differences, and they are important for many applications.

The key example is simplest in the finite field setting. It goes as follows.

Example 10.1. *Let p be a prime, $q = p^2$, $X = \mathbb{F}_p^2 \subset \mathbb{F}_q^2$, $D = \mathbb{F}_p \subset \mathbb{F}_q$. For $\theta \in \mathbb{F}_q$, let $\pi_\theta : \mathbb{F}_q^2 \to \mathbb{F}_q$ be defined by $\pi_\theta(x_1, x_2) = x_1 + \theta x_2$. Then set $S = \max_{\theta \in D} |\pi_\theta(X)|$. We have $\pi_\theta(X) = \mathbb{F}_p$ for all $\theta \in D$, so $S = p$. Then we have $|X| = p^2 = q, S = |D| = p = q^{1/2}$.*

So the sizes of the projections of X can be small even when X is large. However, the same cannot happen over $\mathbb{F}_p$:

Theorem 10.2 (Bourgain-Katz-Tao)**.** *Let $X \subset \mathbb{F}_p^2$ with $|X| = p^s$ for $0 \leq s < 2$. Let $D \subset \mathbb{F}_p$ with $|D| = p^t$ for $0 < t \leq 1$. Then $S = \max_{\theta \in D} |\pi_\theta(X)| \geq p^{s/2+\epsilon(s,t)}$ where $\epsilon(s,t) > 0$.*

There is an example in $\mathbb{C}^2$ which is analogous to Example 10.1. In this example $X = \mathbb{R}^2 \subset \mathbb{C}^2$. And there is a theorem called the Bourgain projection theorem which says that no set in $\mathbb{R}^2$ can behave similarly to this example. We will dicuss the Bourgain projection theorem in detail in a few lectures. We begin with the finite field setting which is somewhat cleaner. The setting of balls in $\mathbb{R}^2$ is analogous with some additional issues.

Note that the key difference between $\mathbb{F}_p$ and $\mathbb{F}_q$ that allows an example like Example 10.1 to exist while no such example exists over $\mathbb{F}_p$ is the existence of a subfield $\mathbb{F}_q$. A way to quantify the properties of a subfield is a set X with small sum and product sets. As such, we should study the sizes of such sets. This study is called sum-product theory.

Sum-product theory uses tools from additive combinatorics. The set of tools that go into the proof of Theorem 10.2 is very different from the tools that we have studied in projection theory so far. In this lecture, we introduce sum-product theory and some of the key tools from additive combinatorics. This is the first of four lectures on this area. Over the four lectures we will flesh out the different tools from the area and use them to prove the BKT projection theorem.

10.1. **Sum-product theory.**

Notation 10.3. *For $A \subset \mathbb{F}_p$, let*

$$A + A = \{a_1 + a_2 : a_i \in A\}, \quad A \cdot A = \{a_1 a_2 : a_i \in A\}.$$

Also, let $A^{\oplus n} = \underbrace{A + A + \cdots + A}_{n}$.

If A is an arithmetic progression, then its sumset is only a little bigger than A. If A is a geometric progression, then its product set is only a little bigger than A. Erdos and Szemeredi conjectured that for any set of numbers A, either the sumset or the product set is much bigger than A. This principle has turned out to be crucial for modern developments in projection theory. We introduce this subject, including a whole different set of tools from combinatorial number theory building on work of Plunnecke, Ruzsa and Edgar-Miller.

Lemma 10.4. *If $A \subset \mathbb{F}_p$, then either*

(1) $\frac{A-A}{A-A} = \mathbb{F}_p$, *or*

(2) $\left|\frac{(A\cdot A)^{\oplus 3} - (A \cdot A)^{\oplus 3}}{A-A}\right| \geq |A|^2$.

Remark. Some version of this trick goes back to the work of Edgar-Miller, and it was adapted by Bourgain-Katz-Tao and Garaev.

Proof. First, note that if $c \notin \frac{A-A}{A-A}$, then $|A + cA| = |A|^2$. Indeed, if this was not the case then there would be some $a_1, a_2, a_1', a_2' \in A$ with $a_1 + ca_2 = a_1' + ca_2'$. But this implies $c = \frac{a_1' - a_1}{a_2 - a_2'} \in \frac{A-A}{A-A}$.

Next, note that if $\frac{A-A}{A-A} \neq \mathbb{F}_p$ then there is some $b \in \frac{A-A}{A-A}$ with $b+1 \notin \frac{A-A}{A-A}$. Indeed, we can set $b+1$ to be the smallest element of $\mathbb{F}_p \setminus \frac{A-A}{A-A}$, which would imply $b \in \frac{A-A}{A-A}$.

Now, if $\frac{A-A}{A-A} \neq \mathbb{F}_p$, then we have

$$\left| A + \left(\frac{A-A}{A-A} + 1\right) A \right| \geq |A|^2,$$

which implies 2 after putting the LHS over a common denominator. □

10.2. **Freiman-Ruzsa theorem.** One question to ask in sum-product theory is when the set $A + A$ is small.

Example 10.5. (1) *If $A = [L]$, then $|A + A| \leq 2|A|$.*

(2) *More generally, if A is an arithmetic progression $A = \{a + nd\}_{n \in [L]}$, then $|A + A| \leq 2|A|$.*

(3) *Even more generally, we can consider $A = \{a + n_1 d_1 + \cdots + n_r d_r\}_{n_i \in [L_i]}$. Then $A + A \subset \{2a + n_1 d_1 + \cdots + n_r d_r\}_{2 \leq n_i \leq 2L_i}$, so $|A + A| \leq 2^r |A|$. In this case we call A a* ***generalized arithmetic progression (GAP)*** *of dimension r and volume $L_1 \cdots L_r$.*

Theorem 10.6 (Freiman-Ruzsa)**.** *If $A \subset \mathbb{Z}$ and $|A+A| \leq K|A|$, then A is contained in a GAP of dimension $r(K)$ and* vol $\leq V(K) \cdot |A|$.

This is a deep theorem that we will not prove, and the quantitative bounds on $r(K)$ and $V(K)$ are weak. In the original paper, the bounds were of the form $r(K) = \exp(K^c), V(K) = \exp(\exp(K^c))$, so the theorem is only meaningful if K is small.

Conjecture 10.7. *There is a meaningful bound if $K = |A|^\delta$ for some $\delta > 0$.*

10.3. **Ruzsa triangle inequality.**

Theorem 10.8 (Ruzsa)**.** *Let Z be an abelian group and $A, B, C \subset Z$. Then $|A||B - C| \leq |A - B||A - C|$.*

Corollary 10.9. *If $|A + A| \leq K|A|$, then $|A - A| \leq K^2|A|$.*

Proof. Use Ruzsa's triangle inequality with $A = A, B, C = -A$. Then we have

$$|B - C| = |(-A) - (-A)| = |A - A|, \quad |A - B| = |A - C| = |A - (-A)| = |A + A|.$$

So Ruzsa's triangle inequality tells us that $|A||A - A| \leq |A + A|^2$, which implies the corollary. □

Proof of Ruzsa triangle inequality. We will construct an injective map $\phi : A \times (B - C) \to (A - B) \times (A - C)$. For all $d \in B - C$, fix some $b(d) \in B, c(d) \in C$ with $d = b(d) - c(d)$. Then set $\phi(a, d) = (a - b(d), a - c(d))$. We need to show that ϕ is injective. Suppose $\phi(a, d) = (x, y)$. Then we will recover a, d from x, y and the choices of $b(d), c(d)$. Note that we have $y - x = b(d) - c(d) = d$, so we can recover d. Then from d we know $b(d)$, so we can recover $a = x + b(d)$. □

10.4. **Plunnecke inequality.**

Theorem 10.10 (Plunnecke)**.** *Let Z be an abelian group and $A, B \subset Z$ with $|A + B| \leq K|A|$. Then $|B^{\oplus m} - B^{\oplus n}| \leq K^{m+n}|A|$.*

Corollary 10.11. *If $|A + A| \leq K|A|$ then $|A - A| \leq K^2|A|$, $|A + A + A| \leq K^3|A|$.*

Corollary 10.12. *If $|A - A| \leq K|A|$ then $|A + A| \leq K^2|A|$.*

Proof. Use Plunnecke's inequality with $B = -A$. □

Lemma 10.13. *If $A \subset \mathbb{F}_p, |A| = p^s$ for $0 \leq s < 1$, then $|A^3 - A^3| \geq p^{s+\epsilon(s)}$ for some $\epsilon(s) > 0$.*

Proof. Let $B = (A^2)^{\oplus 3} - (A^2)^{\oplus 3}, C = A - A$. Then by Lemma 10.4 we have $\left|\frac{B}{C}\right| \geq p^{s+\gamma(s)}$ for some $\gamma > 0$. Now, assume for contradiction that $|A^3 - A^3| \leq K|A|$ where

$K \lessapprox 1$. Then we have $|A^3| \leq K|A|$, and since $|A| \leq |A^3|$, we have $|A^3 - A^3| \leq K|A^3|$. Then Plunnecke's inequality implies

$$|(A^3)^{\oplus m} - (A^3)^{\oplus n}| \leq K^{m+n}|A^3| \leq K^{m+n+1}|A|.$$

In particular, this implies $|B \cdot C|, |A \cdot B|, |A \cdot C| \leq K^{O(1)}|A|$. Then the Ruzsa triangle inequality (on $\mathbb{F}_p$ as a multiplicative set) implies

$$|A|\left|\frac{B}{C}\right| \leq |A \cdot B||A \cdot C| \leq K^{O(1)}|A|^2,$$

so we have $p^{s+\gamma} \leq \left|\frac{B}{C}\right| \leq K^{O(1)}|A| = K^{O(1)}p^s$, which contradicts $K \lessapprox 1$. □

In fact, there is actually a stronger statement:

Theorem 10.14 (Bourgain-Katz-Tao)**.** *If $A \subset \mathbb{F}_p$ with $|A| = p^s$, then* $\max(|A \cdot A|, |A + A|) \geq p^{s+\epsilon(s)}$.

Notation 10.15. *We define* $\mathrm{Poly}_K(A) = (A^K)^{\oplus K} - (A^K)^{\oplus K}$.

Corollary 10.16. *If $0 < s < t < 1$, then there exists a $K = K(s,t)$ such that for all $A \subset \mathbb{F}_p$ with $|A| = p^s$, we have $|\mathrm{Poly}_K(A)| \geq p^t$.*

Proof. Apply Lemma 10.13 many times. □

The following proof is due to Petridis.

Proof of Plunnecke's inequality. The proof depends on a key lemma.

Lemma 10.17. *If $|A + B| \leq K|A|$, then there exists a $X \subset A$ such that for all $C \subset Z$ we have*

$$\frac{|X + C + B|}{|X + C|} \leq K.$$

Proof. Choose $X \subset A$ to minimize the value $\frac{|X+B|}{|X|}$. Then set $\frac{|X+B|}{|X|} = \underline{K} \leq K$. We will show by induction on $|C|$ that $\frac{|X+C+B|}{|X+C|} \leq \underline{K}$ for all $C \subset Z$.

For the base case, when $|C| = 1$ we have $\frac{|X+C+B|}{|X+C|} = \frac{|X+B|}{|X|} = \underline{K}$. For the inductive step, let $C' = C \cup \{c\}$, and assume that $\frac{|X+C+B|}{|X+B|} \leq \underline{K}$. Then set

$$Y = \{x \in X : x + c + B \subset X + C + B\}.$$

Note that by construction we have $Y + \{c\} + B \subset X + C + B$. Now, let us bound $|X + C' + B|$ and $|X + C'|$. First, we have

$$\begin{aligned} |X + C' + B| &= |X + C + B| + |(X + \{c\} + B) \setminus (X + C + B)| \\ &\leq |X + C + B| + |(X + \{c\} + B \setminus (Y + \{c\} + B| \\ &= |X + C + B| + |X + B| - |Y + B|. \end{aligned}$$

Next, we have

$$\begin{aligned} |X+C'| &= |X+C| + |\{x \in X : x+c \notin X+C\}| \\ &= |X+C| + |X| - |\{x \in X : x+c \in X+C\}| \\ &\geq |X+C| + |X| - |Y|. \end{aligned}$$

Recall that we have $|X+C+B| \leq \underline{K}|X+C|$ and $|X+B| = \underline{K}|X|$, and we also have $|Y+B| \geq \underline{K}|Y|$ by the definition of X. So we have

$$|X+C'+B| \leq |X+C+B| + |X+B| - |Y+B| \leq \underline{K}|X+C| + \underline{K}|X| - \underline{K}|Y| \leq \underline{K}|X+C'|,$$

completing the proof. □

Now, let us return to the proof of Plunnecke's inequality. By the key lemma, there is some $X \subset A$ such that $|X+C+B| \leq K|X+C|$. Plugging in $C = \{c\}$ yields $|X+B| \leq K|X|$. Then plugging in $C = B$ gives $|X+B+B| \leq K|X+B| \leq K^2|X|$. Continuing in this fashion, we get $|X+B^{\oplus m}| \leq K^m|X|$.

Now, Ruzsa's triangle inequality implies

$$|X||B^{\oplus m} - B^{\oplus n}| \leq |X+B^{\oplus m}||X+B^{\oplus n}| \leq K^{m+n}|X|^2,$$

so we get

$$|B^{\oplus m} - B^{\oplus n}| \leq K^{m+n}|X| \leq K^{m+n}|A|.$$

□

18.156 Projection Theory
Spring 2025