The Sum-Product Theorem

Arithmetic Combinatorics (Fall 2016)
Rutgers University
Swastik Kopparty
Last modified: Monday 24th October, 2016

In this lecture we prove the sum-product theorem of Bourgain-Katz-Tao and Konyagin.
As discussed in earlier lectures, the power of this theorem is that it is sensitive to the presence of subfields, and it can thus help us prove properties of prime fields (for example) which may not hold for general fields.

Theorem 1. *Let $\mathbb{F}$ be a field and let $A \subseteq \mathbb{F}$ be a finite set.*
Suppose

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

$$|AA| \leq K|A|.$$

Then there exists a finite subring[1] *$\mathbb{L} \subseteq \mathbb{F}$, with $|\mathbb{L}| \leq \mathsf{poly}(K) \cdot |A|$, and a nonzero element $c \in \mathbb{F}$ such that $|A \setminus cL| \leq \mathsf{poly}(K)$.*

Thus A is essentially a dense subset of a dilation of a field.
If $A \subseteq \mathbb{F}_p$ for a prime p, with $|A| \leq p^{1-\epsilon}$, then applying the above theorem with $K = |A|^{O(\epsilon)}$, we get that either $|A+A|$ or $|AA|$ is at least $|A|^{1+\epsilon}$.

1 Elements that interact additively and multiplicatively with A

The difficulty here is to produce a perfectly additively and multiplicatively closed set $\mathbb{L}$ out of an approximate version A.
Here are some relevant comments. If A is a dense random subset of an additive subgroup, then how do we find that subgroup? $A-A$ is that subgroup. But if A has some additional spurious random elements outside the subgroup, then finding that subgroup requires some quantitative considerations: the subgroup turns out to be the set of all elements that are represented in $A-A$ with high multiplicity.
In the setting of the sum-product theorem, our plan will be to consider the set A' of all elements that highly interact (both additively and multiplicatively) with A: with the hope that A' will be contained within the final subring $\mathbb{L}$ that we are after. Once we identify this A', we then show that $(A'-A')/(A'-A')$ is the full subring $\mathbb{L}$.
Here is a crucial definition.

Definition 2. *For a real number C and set $S \subseteq \mathbb{F}$, we say the element $b \in \mathbb{F}$ is C-good for S if $|b \cdot S - S| \leq C|S|$.*

The C-good elements of a set S satisfy many nice properties.

1. **Multiplying good elements**

   Lemma 3. *If a and b are C-good for S, then $a \cdot b$ is C^2-good for S.*

   Proof. By the Ruzsa triangle inequality:

   $$|ab \cdot S - S| \leq \frac{|ab \cdot S - b \cdot S| \cdot |b \cdot S - S|}{|b \cdot S|} = \frac{|a \cdot S - S| \cdot |b \cdot S - S|}{|S|} \leq C^2|S|.$$

   □

[1] Note that every finite subring of a field $\mathbb{F}$ is either a finite field or the set $\{0\}$.

2. **Adding good elements**

Lemma 4. *If $|S+S| \leq C_0|S|$, and if a and b are C-good for S, then $a+b$ is $(C_0^2C^5)$-good for S.*

Proof. By the Ruzsa covering lemma, there exists sets X_a and X_b of size at most C_0 such that $a \cdot S \subseteq X_a + (S-S)$ and $b \cdot S \subseteq X_b + (S-S)$. Then

$$(a+b)\cdot S - S \subseteq a\cdot S + b\cdot S - S \subseteq X_a + S - S + X_b + S - S - S \subseteq X_a + X_b + 2S - 3S.$$

By the sumset inequalities, $|2S-3S| \leq C^5|S|$. The claim then follows by our bound on $|X_a|$ and $|X_b|$. □

3. **Not too many good elements**

Lemma 5. *Let $S \subseteq \mathbb{F}$ and let $C \leq |S|/2$.*

$$|\{b \in \mathbb{F} \mid b \text{ is } C\text{-good for } S\}| \leq (2C)\cdot|S|.$$

Proof. Let

$$T = \{b \in \mathbb{F} \mid b \text{ is } C\text{-good for } S\}.$$

If $b \in T$, then by definition we have $|b\cdot S - S| \leq C|S|$. This implies that the additive energy $E(b\cdot S, S) \geq \frac{1}{C}|S|^3$. Thus:

$$\sum_{b\in T} E(b\cdot S, S) \geq \frac{|T|\cdot|S|^3}{C}.$$

On the other hand,

$$\begin{aligned}
\sum_{b\in T} E(b\cdot S, S) &= \sum_{b\in T} |\{(s_1,s_2,s_3,s_4) \in S^4 \mid s_1b + s_2 = s_3b + s_4\}| \\
&= \sum_{b\in T} \sum_{s_1,s_2,s_3,s_4\in S} \mathbf{1}_{b(s_1-s_3)=(s_4-s_2)} \\
&\leq \sum_{s_1,s_2,s_3,s_4\in S} |\{b\in T \mid b(s_1-s_3) = (s_4-s_2)\}| \\
&\leq |S|^4 + |T||S|^2.
\end{aligned}$$

Putting everything together, we get

$$|T| \leq \frac{|S|^4}{|S|^3/C - |S|^2} \leq 2C|S|,$$

(here we used the assumption that $C \leq |S|/2$). □

To summarize, the set of all C-good elements for any set S with small sumset is not too much larger than S, and is approximately closed under addition and multiplication (with some loss of goodness).
The following key lemma can be used to upgrade the approximate additive/multiplicative closedness into genuine additive/multiplicative closedness. It says that when S is such that $|2S^2-2S^2|$ is small, the goodness of an element for S must either be very small or very large. Combined with the previous properties, it implies that the set of C-good elements for S is itself closed under addition and multiplication.

Lemma 6. *Suppose $S \subseteq \mathbb{F}$ is such that $|2S^2-2S^2| \leq C|S|$. Suppose $C < |S|^{0.05}$. Then for all $b \in \mathbb{F}$, exactly one of the following occurs:*

- *b is C-good for S,*
- *b is not C^{10}-good for S.*

Proof. We take cases on whether $b \in (S-S)/(S-S)$ or not.
If $b \notin (S-S)/(S-S)$, then there are no nontrivial solutions to $s_1 b - s_2 = s_3 b - s_4$ with $s_1, s_2, s_3, s_4 \in S$. Thus $|b \cdot S - S| = |S|^2 > C^{10}|S|$, and so b is not C^{10}-good for S in this case.
If $b \in (S-S)/(S-S)$, then

$$|b \cdot S - S| \leq |((S-S)/(S-S)) \cdot S - S| \leq |(S-S) \cdot S - (S-S) \cdot S| = |2S^2 - 2S^2| \leq C|S|,$$

and so b is C-good for S in this case. □

Corollary 7. *Suppose $S \subseteq \mathbb{F}$ is such that Suppose $|2S^2 - 2S^2| \leq C|S|$.*
Let $\mathbb{L}$ be the set of C-good elements for S. Then:

- *$\mathbb{L}$ is a subring of $\mathbb{F}$,*
- *$|\mathbb{L}| \leq C|S|$.*

2 Proof of the sum-product theorem

Now we can prove the sum-product theorem.

Proof. Our plan is to use the previous corollary to find the ring $\mathbb{L}$. To do this we need to find a set S related to A for which $|2S^2 - 2S^2| \leq C|S|$.
Define S to be the set of all K^{10}-good elements for A. By properties of goodness, all elements of $2S^2 - 2S^2$ are K^{100}-good for A. We also know that there cannot be more than $K^{100}|A|$ elements that are K^{100}-good for A. Thus $|2S^2 - 2S^2| \leq K^{100}|A|$.
For this to be useful in the corollary, we will need $|A|$ to be not much larger than $|S|$. Further, we
We show this now.

Claim 8. *There exists some $c \in \mathbb{F}$ such that $|cS \cap A| \geq \frac{1}{2K} \cdot |A|$. In particular,*

$$|S| \geq \frac{1}{2K} \cdot |A|.$$

Proof. This claim is where we use the hypothesis that $|AA| \leq K|A|$.
We have that for all $a \in A$, $a \cdot A \subseteq AA$.
Thus $\sum_{z \in AA} \sum_{a \in A} 1_{aA}(z) = |A|^2$. By Cauchy-Schwarz,

$$\sum_{z \in AA} (\sum_{a \in A} 1_{aA}(z))^2 \geq \frac{|A|^4}{|AA|} \geq \frac{1}{K}|A|^3.$$

Thus:

$$\sum_{a,a' \in A} \sum_{z \in AA} 1_{aA}(z) 1_{a'A}(z) \geq \frac{1}{K}|A|^3.$$

In other words:

$$\sum_{a,a' \in A} |aA \cap a'A| \geq \frac{1}{K}|A|^3.$$

By averaging, there exists some $c \in A$ such that:

$$\sum_{a \in A} |aA \cap cA| \geq \frac{1}{K}|A|^2.$$

Let $U = \{a \in A \mid |aA \cap cA| \geq \frac{1}{2K}|A|$. Then

$$\sum_{a \in A \setminus U} |aA \cap cA| \leq \frac{1}{2K}|A|^2,$$

and so:

$$\sum_{a \in U} |aA \cap cA| \geq \frac{1}{2K}|A|^2,$$

In particular, $|U| \geq \frac{1}{2K}|U|$.
Now we show that for each $u \in U$,

$$|uA - cA| \leq K^{10}|A|.$$

This follows from Ruzsa's triangle inequality:

$$|uA - cA| \leq \frac{|uA - (uA \cap cA)| \cdot |(uA \cap cA) - cA|}{|uA \cap cA|} \leq \frac{|uA - uA| \cdot |cA - cA|}{|uA \cap cA|} \leq 2K^3|A| \leq K^{10}|A|.$$

Thus for all $u \in U$, (u/c) is K^{10}-good for A, and so $U \subseteq cS$. This completes the proof of the claim. □

Summarizing, we get a subring $\mathbb{L} \subseteq \mathbb{F}$ such that $|\mathbb{L}| \leq \mathsf{poly}(K) \cdot |A|$ and $|c\mathbb{L} \cap A| \geq \frac{1}{2K}|A|$.
By the Ruzsa triangle inequality,

$$|A - c\mathbb{L}| \leq \frac{|A - (A \cap c\mathbb{L})| \cdot |(A \cap c\mathbb{L}) - c\mathbb{L}|}{|A \cap c\mathbb{L}|} \leq \frac{|A - A| \cdot |c\mathbb{L} - c\mathbb{L}|}{|A \cap c\mathbb{L}|} \leq \mathsf{poly}(K) \cdot |A|.$$

Thus by the Ruzsa covering lemma, A can be covered by $\mathsf{poly}(K)$ additive translates of $c\mathbb{L} - c\mathbb{L} = c\mathbb{L}$.
Doing the same argument multiplicatively, we get that A can be covered by $\mathsf{poly}(K)$ multiplicative translates of $c\mathbb{L}$.
But a nontrivial additive translate and a nontrivial multiplicative translate of $c\mathbb{L}$ cannot have more than 1 element in common: if distinct $x, y \in \mathbb{L}$ are such that $cx + d \in e\mathbb{L}$ and $cy + d \in e\mathbb{L}$, then $d, e \in c\mathbb{L}$ (by solving the linear equations). Thus corresponding to each choice of a nontrivial additive translate and nontrivial multiplicative translate from the above collections, there can be exactly one element of A which lies in both of them. Thus there are at most $\mathsf{poly}(K)$ elements of A which do not lie in $c\mathbb{L}$.
This completes the proof of the sum-product theorem. □

In the above proof, we took S to be the $\mathsf{poly}(K)$-good elements for A, and then took $\mathbb{L}$ to be the $\mathsf{poly}(K)$-good elements for S. Once we know the sum-product theorem, it follows that the set S is itself the subring $\mathbb{L}$. But it is not clear (to me) how to show this directly.