Notes on the Bourgain-Katz-Tao theorem

February 28, 2011

1 Introduction

NOTE: these notes are taken (and expanded) from two different notes of Ben Green on sum-product inequalities.

The basic Bourgain-Katz-Tao inequality says that for every $\varepsilon > 0$ there exists $\delta > 0$ such that if $A \subseteq \mathbb{F}_p$ satisfies

$$p^{\varepsilon} \ < \ |A| \ < \ p^{1-\varepsilon},$$

then

$$\max(|A+A|, |A.A|) \ > \ |A|^{1+\varepsilon}.$$

Since the time this theorem first appeared many strengthenings have appeared in the literature; for instance, Bourgain, Glibichuk and Konyagin have shown that the lower bound of p^{ε} on $|A|$ can be replaced with just $|A| \geq 2$.

In this note I will not give the original proof, but will instead give a proof that combines some results of Konyagin with a certain proposition appearing in the Bourgain-Katz-Tao paper to get a relatively short proof.

2 The proof

The proof will amount to combining together the following two lemmas, the first one due to Konyagin, and the second one due to Bourgain, Katz and Tao:

Proposition 1 *Suppose that $B \subseteq \mathbb{F}_p$. Then,*

$$|3B^2 - 3B^2| \ = \ |B.B + B.B + B.B - B.B - B.B - B.B| \ \geq \ \frac{1}{2}\min(|B|^2, p).$$

Proposition 2 *Suppose that $A \subseteq \mathbb{F}_p$ and that $|A + A|, |A^2| \leq K|A|$. Then, there is some subset $B \subseteq A$ with $|B| \geq K^{-c}|A|$ and $|B.B - B.B| \leq K^c|B|$.*

Now let us see how these imply the theorem: first, suppose that $|A + A|, |A.A| \leq |A|^{1+\delta}$, where we will take $\delta > 0$ as small as desired in terms of ε in order to produce a contradiction.

Applying Proposition , using $K = |A|^\delta$ to obtain a subset $B \subseteq A$ satisfying $|B| \geq |A|^{1-c\delta}$ and

$$|B^2 - B^2| \leq K^c|B| \ = \ |A|^{c\delta}|B| \ \leq \ |B|^{1+c\delta/(1-c\delta)}. \tag{1}$$

Note that

$$|B^2| \ \leq \ |A^2| \ \leq \ |A|^{1+\delta} \ \leq \ |B|^{(1+\delta)/(1-c\delta)}.$$

Now we consider two cases: either $|B| > \sqrt{p}$ or else $|B| < \sqrt{p}$.

If $\sqrt{p} < |B| \leq |A| < p^{1-\varepsilon}$, then from Proposition 1 we have that

$$|3B^2 - 3B^2| \ \geq p/2 \ \geq \ |B|^{1/(1-\varepsilon)}/2 \ > \ |B|^{1+\varepsilon}/2 \ > \ |B|^{1+\varepsilon/2},$$

for $p > p_0(\varepsilon)$ (which we can assume – turns out to be an easy exercise involving Cauchy-Davenport). On the other hand, if $|B| < \sqrt{p}$, then we have

$$|3B^2 - 3B^2| \ \geq \ |B|^2/2 \ > \ |B|^{1+\varepsilon/2}, \text{ for } 0 < \varepsilon < 1.$$

So either way we get

$$|3B^2 - 3B^2| \ \geq \ |B|^{1+\varepsilon/2} \ \geq \ |B^2|^{(1-c\delta)(1+\varepsilon/2)/(1+\delta)}.$$

Choosing now $\delta > 0$ small enough in terms of $\varepsilon > 0$, we can assume that

$$|3B^2 - 3B^2| \ \geq \ |B^2|^{1+\varepsilon/3}.$$

Next we apply Plunnecke-Ruzsa-Petridis to this last inequality as follows: let L satisfy $|B^2 - B^2| = L|B^2|$. Then, from P-R-P we deduce that

$$|B^2|^{1+\varepsilon/3} \ \leq \ |3B^2 - 3B^2| \leq L^6|B^2|.$$

So, $L \geq |B^2|^{\varepsilon/18}$, which implies that

$$|B^2 - B^2| \;\geq\; |B^2|^{1+\varepsilon/18} \;\geq\; |B|^{1+\varepsilon/18}.$$

This then will contradict (1) for

$$\frac{c\delta}{1-c\delta} \;<\; \frac{\varepsilon}{18}.$$

And so, for δ this small, we must either have that our assumption $|A+A| \leq |A|^{1+\delta}$ or $|A.A| \leq |A|^{1+\delta}$ is false; in other words, we must have that

$$\text{either } |A+A| \;\geq\; |A|^{1+\varepsilon/18c} \;\text{ or }\; |A.A| \;\geq\; |A|^{1+\varepsilon/18c}.$$

2.1 Proof of Proposition 1

We begin with a lemma.

Lemma 1 *Suppose $B \subseteq \mathbb{F}_p$. Then, there exists $x \in \mathbb{F}_p^\times$ such that $|B+x*B| \geq \frac{1}{2}\min(|B|^2, p)$.*

Proof of the lemma. Basically we compute an average over additive energy as follows: let

$$S \;:=\; \sum_{\substack{x\in\mathbb{F}_p \\ x\neq 0}} E(B, x*B) \;=\; |\{b_1, b_2, b_3, b_4, x \;:\; b_1 - b_2 = x(b_3 - b_4)\}|.$$

For each of the $|B|^2(|B|-1)^2$ quadruples (b_1, b_2, b_3, b_4) with $b_1 \neq b_2$ and $b_3 \neq b_4$ there is a unique x that satisfies the above. For the remaining $|B|^2$ quadruples where $b_1 = b_2$ and $b_3 = b_4$ there are $p-1$ choices for x. So,

$$|S| \;=\; |B|^2(|B|-1)^2 + (p-1)|B|^2.$$

It follows from simple averaging that there exists $x \in \mathbb{F}_p^\times$ such that

$$E(B, x*B) \;\leq\; \frac{|B|^2(|B|-1)^2}{p-1} + |B|^2.$$

Then, using the fact that for sets B and C we have

$$|B+C| \;\geq\; \frac{|B|^2|C|^2}{E(B,C)},$$

it follows that

$$|B + x * B| \;\geq\; \frac{|B|^4}{E(B, x * B)} \;\geq\; \frac{|B|^2}{(|B|-1)^2/(p-1)+1}.$$

There are two possibilities to consider: either $|B| \geq \sqrt{p}$, or else $|B| < \sqrt{p}$. For the former case we obtain

$$|B + x * B| \;\geq\; \frac{1}{(1 - 1/\sqrt{p})^2/(p-1) + 1/p} \;>\; p/2.$$

And for the latter case we have

$$|B + x * B| \;\geq\; \frac{|B|^2}{1+1} \;=\; |B|^2/2.$$

This completes the proof. ∎

Now we resume the proof of our Proposition: given $y \in \mathbb{F}_p^\times$ we either have that $|B + y * B| \;=\; |B|^2$ or else there exists $(b_1, b_2, b_3, b_4) \in B \times B \times B \times B$ such that

$$b_1 + yb_4 \;=\; b_3 + yb_2,$$

which is true if and only if $y \in (B - B)/(B - B)$.

Suppos that $(B - B)/(B - B) \neq \mathbb{F}_p$. We have then that there exists $y \in (B-B)/(B-B)$ such that $y+1 \notin (B-B)/(B-B)$, which then implies that

$$|B + (y+1) * B| \;=\; |B|^2.$$

If we write $y = (b_1 - b_3)/(b_2 - b_4)$, then we have

$$3B^2 - 3B^2 \supseteq\; (b_2 - b_4) * A + (b_1 - b_3 + b_2 - b_4) * A \;\supseteq\; (b_2 - b_4) * (A + (y+1) * A),$$

which implies $|3B^2 - 3B^2| \geq |B + (y+1) * B| \geq |B|^2$.

Now suppose that $(B - B)/(B - B) = \mathbb{F}_p$. Then, from the Lemma above we deduce that there exists $x \in (B - B)/(B - B)$ such that

$$|B + x * B| \;\geq\; \frac{1}{2}\min(|B|^2, p).$$

Proceeding much as before, we deduce that

$$3B^2 - 3B^2 \;\supseteq\; 2B^2 - 2B^2 \;\supseteq\; (b_2 - b_4)(B + x * B),$$

which implies

$$|3B^2 - 3B^2| \;\geq\; |B + x * B| \;\geq\; \frac{1}{2}\min(|B|^2, p).$$

∎

2.2 Proof of Proposition 2

let $N = |A|$. For sets $C, D \subseteq G$ (our additive group), we shall adopt the simplifying notation $|C| \lesssim |D|$ to mean $|C| \leq c_1 K^{c_2} |D|$, where $c_1, c_2 > 0$, and where K is as in the hypotheses of the proposition. Also, $|C| \gtrsim |D|$ will have the analogous meaning.

We will require the following version of the Balog-Szemeredi-Gowers Theorem.

Theorem 1 *Suppose that B is a subset of an additive group G, where $|B| = N$ and $E(B,B) \geq N^3/K$. Then, there exists $B' \subseteq B$ with $|B'| \gtrsim N$, such that for every pair $b_1, b_2 \in B$ we have that there $\gtrsim N^7$ eight-tuples $(a_1, ..., a_8) \in A \times \cdots \times A$ such that*

$$b_1 - b_2 \ = \ (a_1 - a_2) + (a_3 - a_4) + (a_5 - a_6) + (a_7 - a_8).$$

We also will require Plunnecke-Ruzsa-Petridis:

Theorem 2 *Suppose that $|C + C| \leq K|C|$. Then, $|kC - \ell C| \leq K^{k+\ell}|C|$. The same conclusion holds if we instead assume $|C - C| \leq K|C|$.*

And now we resume the proof of the Proposition: we begin by showing that if $|A.A| \lesssim N$ and $|A + A| \lesssim N$, then there exists a subset $A' \subseteq A$ with $|A'| \gtrsim N$ such that for any integers $k, \ell \geq 1$ we have that

$$|(A' - A')A^k/A^\ell| \ \lesssim \ N.$$

(Such a result would put us "in the ballpark" of proving the Proposition, and should give us confidence that it can in fact be proved.) To see that such a set A' exists, we begin by noting that $|A + A| \lesssim N$ implies that $E(A, A) \gtrsim N^3$; and then, Theorem 1 above tells us that for any pair $(a', a'') \in A' \times A'$ we have that the equation

$$a' - a'' \ = \ a_1 - a_2 + a_3 - a_4 + a_5 - a_6 + a_7 - a_8$$

has $\gtrsim N^7$ solutions with $a_1, ..., a_8 \in A$. And now if we multiply both sides by an arbitrary element $c \in A^k/A^\ell$, we get

$$c(a' - a'') \ = \ ca_1 - ca_2 + \cdots + ca_7 - ca_8.$$

The right-hand-side here can be written in $\gtrsim N^7$ ways with the ca_i's elements of A^{k+1}/A^ℓ. Thus, each element of $(A'-A')A^k/A^\ell$ has $\gtrsim N^7$ representations as a sum-and-difference of 8 elements of A^{k+1}/A^ℓ. Since by Plunnecke-Ruzsa-Petridis (multiplicative analogue) we have that $|A^{k+1}/A^\ell| \lesssim N$, it follows that

$$N^7|(A'-A')A^k/A^\ell| \ \lesssim\ \#\ \text{possible } 8-\text{tuples } (ca_1,...,ca_8)\ \leq\ N^8,$$

as claimed.

Next, we apply Theorem 1 again, this time a multiplicative analogue: we let $A'' \subseteq A'$ such that for any pair a_1'', a_2'' we have that the equation

$$a_1''/a_2''\ =\ a_1'a_2'a_3'a_4'/a_5'a_6'a_7'a_8'$$

has $\gtrsim N^7$ solutions with $a_1',...,a_8' \in A'$.

Suppose that a_3'', a_4'' is another pair of elements in A'' (possibly the same as a_1'', a_2'') and note that

$$a_1''a_4'' - a_2''a_3''\ =\ \frac{a_1'a_2'a_3'a_4'a_2''a_4'' - a_3''a_2''a_5'a_6'a_7'a_8'}{a_5'a_6'a_7'a_8'}$$

The idea now is to write the right-hand-side as a sum of six elements of $(A'-A')A^k/A^\ell$ for $k=5$ and $\ell=4$, and then to count solutions to

$$a_1''a_4'' - a_2''a_3''\ =\ x_1+x_2+x_3+x_4+x_5+x_6. \tag{2}$$

in much the same way as is used to prove Theorem 1. The magic identities to produce these x_i's are given as follows: let $P := a_5'a_6'a_7'a_8'$, and then let

$$\begin{aligned}
x_1 &= a_1'a_2'a_3'a_4'a_2''(a_4''-a_8')/P\\
x_2 &= a_1'a_2'a_3'a_4'(a_2''-a_7')a_8'/P\\
x_3 &= a_1'a_2'a_3'(a_4'-a_6')a_7'a_8'/P\\
x_4 &= a_1'a_2'(a_3'-a_5')a_6'a_7'a_8'/P\\
x_5 &= a_1'(a_2'-a_3'')a_5'a_6'a_7'a_8'/P\\
x_6 &= (a_1'-a_2'')a_3''a_5'a_6'a_7'a_8'/P.
\end{aligned}$$

Now, one can check that for fixed a_1'', a_2'', a_3'' and a_4'', the obvious mapping

$$\varphi\ :\ (x_1,...,x_6)\ \rightarrow\ (a_1', a_2', a_3'/a_5', a_4'/a_6', a_7', a_8')$$

(determined by solving for these parameters in terms of the x_i's) is injective. Basically, the map is defined as follows: note that for fixed $a_1'', a_2'', a_3'', a_4''$ we have that x_6 determines a_1' uniquely. And then if one knows x_5, one quickly obtains a_2'. Then, knowledge of $a_1', a_2', x_5, x_6, x_4$ determines a_3'/a_5'. Also note that knowledge of x_1 determines a_8', since $a_1'a_2'a_3'a_4'/P = a_1''/a_2''$, and since we are given this ratio. The other variables can be obtained in a similar manner.

So, the mapping

$$\psi \ : \ (a_1', ..., a_8') \ \to \ (x_1, ..., x_6)$$

(given by the definition of the x_i's above) is at worst N^2-to-1.

What this means is that those $\gtrsim N^7$ possibilities for $a_1', ..., a_8'$ we had earlier (that determine a_1''/a_2'') determine $\gtrsim N^7/N^2 = N^5$ sequences $(x_1, ..., x_6)$. In other words, for each 4-tuple $(x_1'', x_2'', x_3'', x_4'') \in A'' \times A'' \times A'' \times A''$ there are $\gtrsim N^5$ sequences $(x_1, x_2, x_3, x_4, x_5, x_6) \in (A' - A')A^5/A^4$ satisfying (2). It follows that

$$N^5|A''A'' - A''A''| \ \lesssim \ \#\, \text{possible } 6\text{−tuples } x_1, ..., x_6 \in (A' - A')A^5/A^4 \ \lesssim \ N^6,$$

which proves the Proposition.