ACTA ARITHMETICA
165.3 (2014)

Combinatorial Nullstellensatz approach to polynomial expansion

by

Fedor Petrov (St. Petersburg)

Let $\mathbb{F}$ be a field and $f(x, y) \in \mathbb{F}[x, y]$ be a polynomial of two variables. For non-empty sets $A, B \subset \mathbb{F}$ denote

$$f(A, B) = \{f(x, y) : x \in A,\ y \in B\}.$$

There are numerous works concerning estimates of $|f(A, B)|$ in terms of $|A|$ and $|B|$ for various polynomials f. Probably, the first result in this area is the Cauchy–Davenport theorem, stating that for $f(x, y) = x + y$ and $\mathbb{F} = \mathbb{F}_p$ for prime p one has $|f(A, B)| \geq \min(|A| + |B| - 1, p)$. The Combinatorial Nullstellensatz of Alon [1] is one of the most flexible ways to prove the Cauchy–Davenport theorem. In particular, it easily generalizes to restricted sumset estimates like the Erdős–Heilbronn conjecture (unlike purely combinatorial methods).

There are many asymptotic results for other polynomials f. Bourgain [2] proved that for $f(x, y) = x^2 + xy$, given $\alpha \in (0, 1)$ there exists $\beta > \alpha$ such that for $\mathbb{F} = \mathbb{F}_p$ (here p is a large enough prime), and $|A|, |B| \geq p^\alpha$ one has $|f(A, B)| \geq p^\beta$. Several generalizations are given in [4]. This phenomenon (the estimate is asymptotically much better than in the Cauchy–Davenport case) is called *polynomial expanding*. It is intimately connected to sum-product estimates and was intensively studied in recent papers (see, e.g., [2–7]). The main methods are spectral graph theory and Fourier analysis. Tao in a recent paper [6] also uses some algebraic geometry.

The aim of this paper is to give a proof of some weak (Cauchy–Davenport type) estimate for the Bourgain-type expanders $g(x) + yh(x)$. The possible advantage of this result is that estimates are very explicit (without implicit asymptotical constants) and say something for all fields.

2010 *Mathematics Subject Classification*: Primary 12E05; Secondary 05E40.
Key words and phrases: Cauchy–Davenport theorem, polynomial expansion, polynomial method, Combinatorial Nullstellensatz.

DOI: 10.4064/aa165-3-6

Our proof is in the spirit of Combinatorial Nullstellensatz. However, we do not use it as a blackbox, but apply the idea of the proof.

THEOREM. *Let $\mathbb{F}$ be a field, $g(x), h(x) \in \mathbb{F}[x]$, and A and B be non-empty finite subsets of $\mathbb{F}$ with $|A| = a$ and $|B| = b$. Assume also that $d = \deg g(x) > \deg h(x)$ and A does not contain roots of $h(x)$. Assume further that $k \leq (a-1)/d + b - 1$ and the binomial coefficient $\binom{k}{b-1}$ does not vanish in $\mathbb{F}$. Then*

$$|\{g(x) + yh(x) : x \in A,\, y \in B\}| > k.$$

The theorem immediately yields the following

COROLLARY. *Let $p = \operatorname{char} \mathbb{F}$ (and $p = \infty$ if $\operatorname{char} \mathbb{F} = 0$). Then*

$$|\{g(x) + yh(x) : x \in A, y \in B\}| \geq \min(a/d + b - 1, p).$$

In particular, for Bourgain's expander we get $|\{x^2 + xy : x \in A, y \in B\}| \geq \min(a/2 + b - 1, p)$ provided that $0 \notin A$.

Proof of the Theorem. Assume the contrary. The condition $\binom{k}{b-1} \neq 0$ implies that $k < |\mathbb{F}|$, hence there exists a set C of cardinality k such that $g(x) + yh(x) \in C$ for all $x \in A$ and $y \in B$. Clearly $k \geq b$ (just fix x and vary y). Denote

$$P(x, y) := \prod_{c \in C} (g(x) + yh(x) - c) = \sum_{i,j} \lambda_{i,j} g(x)^i h(x)^j y^j$$

for some pairs (i, j) of non-negative integers and some coefficients $\lambda_{i,j}$ in $\mathbb{F}$. Such a polynomial $P(x, y)$ vanishes on $A \times B$. Consider some $\mathbb{F}$-valued functions $\alpha(x), \beta(y)$ defined on A and B respectively. Look at the following sum, which eventually vanishes:

$$\begin{aligned} \sum_{x \in A,\, y \in B} \alpha(x)\beta(y)P(x, y) &= \sum_{i,j} \lambda_{i,j} \sum_{x \in A,\, y \in B} \alpha(x)\beta(y)g(x)^i h(x)^j y^j \\ &= \sum_{i,j} \lambda_{i,j} \Big(\sum_{x \in A} \alpha(x) g(x)^i h(x)^j \Big) \Big(\sum_{y \in B} \beta(y) y^j \Big). \end{aligned} \tag{0.1}$$

Our goal is to choose functions α, β so that there exists a unique non-zero term in the last expression in (0.1). Let us choose β so that

$$\sum_{y \in B} \beta(y) y^j = \begin{cases} 0 & \text{if } 0 \leq j \leq b - 2, \\ 1 & \text{if } j = b - 1. \end{cases}$$

Such a β does exist, since the Vandermonde determinant for the set B does not vanish. Then all terms in (0.1) with $j < b - 1$ vanish. If $j \geq b - 1$, then we may expand

$$g(x)^i h(x)^j = h(x)^{b-1} \sum_{\nu=0}^{d(k-b+1)} \eta_{i,j}(\nu) x^\nu.$$

Let us choose α so that

$$\sum_{x\in A} \alpha(x)h(x)^{b-1}x^i = \begin{cases} 0 & \text{if } 0 \le i < d(k-b+1), \\ 1 & \text{if } i = d(k-b+1). \end{cases}$$

Since $d(k-b+1) \le a-1$, this is (part of) a Vandermonde system again (for unknowns $\alpha(x) \cdot h(x)^{b-1}$), and therefore has a solution. For this choice of α all summands

$$\sum_{x\in A} \alpha(x)h(x)^{b-1}\eta_{i,j}(\nu)x^\nu$$

corresponding to fixed i, j and fixed $\nu < d(k-b+1)$ vanish. Now note that $\eta_{i,j}(d(k-b+1)) = 0$ unless $j = b-1$, $i = k-b+1$ (here we use the fact that $\deg h(x) < d$). And if $j = b-1$, $i = k-b+1$, we have

$$\eta_{k-b+1,b-1}(d(k-b+1)) = \binom{k}{b-1} M^{k-b+1},$$

where M is the leading coefficient of $g(x)$. So, by our assumption this expression does not vanish in $\mathbb{F}$. Finally, we indeed have a unique non-vanishing term in (0.1), as desired. ∎

Remark. Let $\mathbb{F}$ be a field of p^n elements for a prime p, B be any subfield, of say p^m elements, and $A = B \setminus \{0\}$. Then $f(A, B) = B$ for any polynomial f and we get no non-trivial bound. But already for $|B| = b = p^m + 1$ and $|A| = a \ge C \cdot p^m$, $0 < C < 1$, for, say, $f(x, y) = x^2 + xy$, we get an estimate $|f(A, B)| \ge (1 + C/2)p^m - 1$, since the corresponding binomial coefficient is not divisible by p. It would be interesting to have a structured version of this result, i.e. to prove that if $|f(A, B)|$ is close to $|B|$, then B is close to a subfield. Also, the constant $1+C/2$ does not seem to be sharp and probably the correct constant is $1 + C$.

Acknowledgements. This research was partly supported by RFBR grants 14-01-00373-a, 13-01-00935-a, 13-01-12422-ofi-m and President of Russia grant MK-6133.2013.1.

I am grateful to Ilya Shkredov for calling my attention to this question and for many fruitful discussions, and to Norbert Hegyvári for pointing out the work [4]. I also thank the referee for carefully reading the manuscript and proposing several improvements of exposition.

References

[1] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. 8 (1999), 7–29.

[2] J. Bourgain, *More on the sum-product phenomenon in prime fields and its applications*, Int. J. Number Theory 1 (2005), 1–32.

[3] D. Hart, L. Li and C.-Y. Shen, *Fourier analysis and expanding phenomena in finite fields*, Proc. Amer. Math. Soc. 141 (2013), 461–473.

[4] N. Hegyvári and F. Hennecart, *Explicit constructions of extractors and expanders*, Acta Arith. 140 (2009), 233–249.

[5] I. D. Shkredov, *On monochromatic solutions of some nonlinear equations in* $\mathbb{Z}/p\mathbb{Z}$, Math. Notes 88 (2010), 603–611.

[6] T. Tao, *Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets*, arXiv:1211.2894 (2012).

[7] V. H. Vu, *Sum-product estimates via directed expanders*, Math. Res. Lett. 15 (2008), 375–388.

Fedor Petrov
St. Petersburg Department
of V. A. Steklov Institute of Mathematics RAS
Fontanka 27
191023 St. Petersburg, Russia
and
Faculty of Mathematics and Mechanics
St. Petersburg State University
Universitetsky prospekt, 28
198504 Peterhof, St. Petersburg, Russia
E-mail: fedor@pdmi.ras.ru

Received on 3.2.2014
and in revised form on 25.6.2014 (7719)