European Journal of Combinatorics 34 (2013) 1365–1382

Contents lists available at SciVerse ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

# Conditional expanding bounds for two-variable functions over prime fields

Norbert Hegyvári [a], François Hennecart [b]

[a] ELTE TTK, Eötvös University, Institute of Mathematics, H-1117 Pázmány st. 1/c, Budapest, Hungary

[b] Université de Saint-Étienne, Institut Camille Jordan, 23, rue Michelon, 42023 Saint-Étienne, France

ARTICLE INFO

*Article history:*
Available online 14 June 2013

ABSTRACT

In this paper we provide in $\mathbb{F}_p$ expanding lower bounds for two variables functions $f(x, y)$ in connection with the product set or the sumset. The sum–product problem has been immensely studied in the recent past. A typical result in $\mathbb{F}_p^*$ is the existence of $\Delta(\alpha) > 0$ such that if $|A| \asymp p^\alpha$ then

$$\max(|A + A|, |A \cdot A|) \gg |A|^{1+\Delta(\alpha)},$$

Our aim is to obtain analogous results for related pairs of two-variable functions $f(x, y)$ and $g(x, y)$: if $|A| \asymp |B| \asymp p^\alpha$ then

$$\max(|f(A, B)|, |g(A, B)|) \gg |A|^{1+\Delta(\alpha)}$$

for some $\Delta(\alpha) > 0$.



*To Yahya*

## 1. Introduction

We denote by $\mathbb{F}_p$ the field with $p$ elements and by $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ its multiplicative group. Expanding properties of functions in $\mathbb{F}_p^*$ have been widely investigated in the last decade. If $A \subset \mathbb{F}_p$, we denote by $|A|$ its cardinality and write $|A| \asymp p^\alpha$ if $c_1 p^\alpha < |A| < c_2 p^\alpha$ for some fixed real numbers $0 < c_1 < c_2$. Throughout the paper we will use Vinogradov's symbol $\gg$ in the following way: $X \gg Y$ means that there exists an absolute constant $\kappa > 0$ such that $X \geq \kappa Y$ where $X$ and $Y$ are numbers generally depending on certain parameters as the prime number $p$, the subsets $A, B, \ldots$ of $\mathbb{F}_p$.

For a given function $f(x, y)$ and two subsets $A, B$ of $\mathbb{F}_p^*$, we denote

$$f(A, B) = \{f(a, b) : (a, b) \in A \times B\}.$$

*E-mail addresses:* hegyvari@elte.hu (N. Hegyvári), francois.hennecart@univ-st-etienne.fr (F. Hennecart).

0195-6698/$ – see front matter 
http://dx.doi.org/10.1016/j.ejc.2013.05.021

The sumset corresponds to the function $x + y$ and is denoted by $A + B$; the product-set corresponds to the function $xy$ and is denoted by $A \cdot B$.

A function $f : \mathbb{F}_p^* \times \mathbb{F}_p^* \to \mathbb{F}_p$ being given, what can be said on

$$\inf_{\substack{A \subset \mathbb{F}_p^* \\ |A|,|B| \asymp p^\alpha}} \frac{\log |f(A, B)|}{\ln p},$$

for $0 < \alpha < 1$? A function is called an expander (according to $\alpha$) if the above quantity is uniformly in $p$ bigger than $\alpha$. For instance, $f(x, y) = x(x + y)$ is known to be an expander for any $\alpha$ (cf. [2]). A wide family of expanders has also been provided in [10].

A related question due to Erdős and Szemerédi is the sum–product problem, which takes its roots from the analogous problem in $\mathbb{R}$. For $A$ to be a finite subset in a ring, we denote

$$SP(A) = \max(|A + A|, |A \cdot A|).$$

The best known statement for real numbers asserts that for $A \subset \mathbb{R}$,

$$SP(A) \geq \frac{|A|^{4/3}}{2(\log |A|)^{1/3}},$$

(see [18]).

For a set $A$ in $\mathbb{F}_p^*$, the growth will be plainly limited according to the size of $\log |A|/ \log p$. We may confer [5] for a complete description of the recent improvements for the size of $SP(A)$. In particular for large subset $A$ of $\mathbb{F}_p$ Garaev (cf. [6]) obtained the bound $SP(A) \gg \min\left(\sqrt{p|A|}, |A|^2/\sqrt{p}\right)$. His proof uses exponential sums. This result implies $SP(A) \gg |A|^{5/4}$ if $|A| \asymp p^{2/3}$. This bound has also been obtained in [17] by the use of a graph-theoretical approach. In the same paper Solymosi proved also the bound $\max(|A + B|, |f(A) + C|) \gg \min(p|A|, |A|^2|B||C|/p)^{1/2}$ where $f$ is any polynomial with integral coefficients and degree greater than one. In [21] Vu introduces the class of non-degenerate polynomials $f(x, y)$ over a finite field $\mathbb{F}$. For such a polynomial one has $\max(|A + A|, |f(A, A)|) \gg \min(|A|^{2/3}|\mathbb{F}|^{1/3}, |A|^{3/2}|\mathbb{F}|^{-1/4})$ for any $A \subset \mathbb{F}$. In [9] Hart, Li and Shen studied such expanding phenomena in connection with the sum–product property and obtained the lower bound for the size of $\max(|u(A) * B|, |v(A) \circ C|)$ where $u, v$ are polynomials over $\mathbb{F}$ and $*, \circ \in \{+, \times\}$. All these lower bounds are non trivial only for $|A|, |B| > |\mathbb{F}|^{1/2}$. In [9] the notion of expansion is also extended for subsets $E$ of $\mathbb{F}^2$ which are not necessarily a cartesian product $A \times B$ and gives a non trivial lower bound for $\max(|f(E)|, |E + F|)$ where $f : \mathbb{F}^2 \to \mathbb{F}$ is a non-degenerate polynomial of degree $k$ and $E, F$ are subsets of $\mathbb{F}^2$ with $|E| \gg k|\mathbb{F}|$.

For small subsets $A$ of the prime field $\mathbb{F}_p$, namely if $|A| \leq \sqrt{p}$, it has been proved in [13] that $SP(A) \gg |A|^{13/12}$. We will use this fact in Section 6. In [15], the author provides a generalization of this lower bound by showing $\max(|A + A|, |f(A, A)|) \gg |A|^{13/12}$ for $|A| \leq \sqrt{p}$ and where $f(x, y) = x(g(x) + y)$ for any arbitrary function $g : \mathbb{F}_p \to \mathbb{F}_p$. One will express this property by notifying that the function $f(x, y)$ satisfies a conditional expanding property relatively to the sum $x + y$.

All the above quoted results brought to light relative expansion properties according to a pair of two-variable functions, properties which are closely connected to the sum–product problem. In this note, we are interested in a somewhat more general conditional expanding statement of the following kind:

$$|A|, |B| \asymp p^\alpha \Rightarrow \max(|f(A, B)|, |g(A, B)|) \gg |A|^{1+\Delta}.$$

We will first obtain results with $g(x, y) = xy$ or $x+y$ combined with some more complicated functions $f(x, y)$. For it we will use a generalization of Solymosi's approach in [17] by the mean of $d$-regular graphs, yielding to Theorems 2.2–2.4. Then we will use it in connection with an explicit statement of the Balog–Szemerédi–Gowers Theorem as done in [5,7] in the case $A = B$ (cf. Theorems 2.5 and 2.6). We will also focus our study on the function $xy(x^k + y^k)$ in Section 6 for small subsets of $\mathbb{F}_p$ and in Section 8 for finite sets of real numbers.