

POINT DISTRIBUTION AND PERFECT DIRECTIONS IN \mathbb{F}_p^2

VSEVOLOD F. LEV

Department of Mathematics, The University of Haifa at Oranim, Tivon, ISRAEL

ABSTRACT. Let $p \geq 3$ be a prime, $S \subseteq \mathbb{F}_p^2$ a nonempty set, and $w: \mathbb{F}_p^2 \rightarrow \mathbb{R}$ a function with $\text{supp } w = S$. Applying an uncertainty inequality due to András Bíró and the present author, we show that there are at most $\frac{1}{2}|S|$ directions in \mathbb{F}_p^2 such that for every line l in any of these directions, one has

$$\sum_{z \in l} w(z) = \frac{1}{p} \sum_{z \in \mathbb{F}_p^2} w(z),$$

except if S itself is a line and w is constant on S (in which case all, but one direction have the property in question). The bound $\frac{1}{2}|S|$ is sharp.

As an application, we give a new proof of a result of Rédei-Megyesi about the number of directions determined by a set in a finite affine plane.

Communicated by Jean-Louis Verger-Gaugry

1. Introduction

Let p be an odd rational prime, and let \mathbb{F}_p denote the p -element field. A *direction* in the affine plane \mathbb{F}_p^2 is a pencil of p parallel lines; thus, there are $p + 1$ distinct directions.

Given a function $w: \mathbb{F}_p^2 \rightarrow \mathbb{R}$ (which can be thought of as a weight assignment), we say that a direction is *perfect* with respect to w if every line in this direction gets its exact share of the total mass of w ; that is, for every

© 2020 BOKU-University of Natural Resources and Life Sciences and Mathematical Institute, Slovak Academy of Sciences.

2010 Mathematics Subject Classification: Primary: 05B25; Secondary: 51E99.

Keywords: Uniform distribution, affine plane.

Licensed under the Creative Commons Attribution-NC-ND 4.0 International Public License.

line l in the direction in question, we have

$$\sum_{z \in l} w(z) = \frac{1}{p} \sum_{z \in \mathbb{F}_p^2} w(z).$$

Write $S := \text{supp } w$. Choosing a line $l \subset \mathbb{F}_p^2$ uniformly at random and considering the variance of the random variable $\sum_{z \in l} w(z)$, it is easy to show that for all $p + 1$ directions to be perfect it is necessary and sufficient that w be a constant function. Consequently, if all directions are perfect, then either $S = \mathbb{F}_p^2$, or $S = \emptyset$. In a similar way one can show that a necessary and sufficient condition for all, but exactly one direction to be perfect is that w is constant on any line in the unique “imperfect” direction; in this case S is a union of parallel lines, and therefore $|S| \geq p$.

How many perfect directions can there be given that S is small (but not empty)? One easily verifies that if p is sufficiently large, then for $|S| = 1$ there are no perfect directions, for $|S| = 2$ and $|S| = 3$ there is at most one perfect direction, while for $|S| = 4$ there can be two perfect directions. The goal of this note is to show that, generally, the number of perfect directions does not exceed $|S|/2$.

THEOREM 1. *Let $p \geq 3$ be a prime. If $S \subseteq \mathbb{F}_p^2$ is nonempty, then for any function $w: \mathbb{F}_p^2 \rightarrow \mathbb{R}$ with $\text{supp } w = S$ there are at most $\frac{1}{2}|S|$ perfect directions, unless S is a line and w is constant on S (in which case there are p perfect directions).*

A set $S \subseteq \mathbb{F}_p^2$ is said to *determine* a direction if there is a line in this direction containing at least two points of S . If $|S| = p$ and w is the indicator function of S , then any direction not determined by S is perfect. Thus, by Theorem 1, if $|S| = p$ and S is not a line, then there are at most $\frac{p-1}{2}$ directions not determined by S . It follows that any set $S \subseteq \mathbb{F}_p^2$ of size $|S| = p$ determines at least $\frac{p+3}{2}$ directions, unless S is a line. This is a well-known result due to Rédei and Megyesi [R73], with alternative proofs given by Lovász and Schrijver [LS83], and by Dress, Klin, and Muzichuk [DKM92]. Our Theorem 1 thus supplies yet another proof of this result. In contrast with other proofs, our argument does not rely on the polynomial method, employing Fourier analysis instead.

We refer the reader to [G03] for a historical account and summary of related results.

The following examples show that the estimate of Theorem 1 is, in a sense, best possible.

EXAMPLE 1. The special orthogonal group $\text{SO}(2, p)$ is cyclic of order $p - (-1/p)$, where (\cdot/p) is the Legendre symbol. Assuming that $2n$ is an even integer dividing $p - (-1/p)$, let $H \leq \text{SO}(2, p)$ be the subgroup of order $|H| = 2n$, and let $H_0 < H$

PERFECT DIRECTIONS IN \mathbb{F}_p^2

be the subgroup of H of order $|H_0| = n$. Fix arbitrarily a nonzero point $z \in \mathbb{F}_p^2$, define S to be the orbit of z under the action of H , and for $x \in S$ let $w(x) = 1$ if x actually belongs to the orbit of z under the action of H_0 , and $w(x) = -1$, otherwise. We leave it to the reader to verify that there are $n = \frac{1}{2}|S|$ directions determined by the pairs $(x, y) \in S \times S$ with $w(x) \neq w(y)$, and that all these directions are perfect.

The next example originates, essentially, from Lovász-Schrijver [LS83].

EXAMPLE 2. Let S be the graph of the function $z \mapsto z^{\frac{p+1}{2}}$, $z \in \mathbb{F}_p$; that is, $S = \{(z, z^{\frac{p+1}{2}}) : z \in \mathbb{F}_p\}$. Then S determines $\frac{p+3}{2}$ directions, and since $|S| = p$, the $\frac{p-1}{2} = \lfloor |S|/2 \rfloor$ undetermined directions are perfect with respect to the indicator function of S .

EXAMPLE 3. If $l_1, l_2 \subset \mathbb{F}_p^2$ are *nonparallel* lines, and w is the difference of the indicator functions of these lines, then $S = (l_1 \cup l_2) \setminus (l_1 \cap l_2)$, $|S| = 2(p-1)$, and there are $p-1 = |S|/2$ perfect directions. Similarly, if S is a union of two *parallel* lines, and w is constant and nonzero on each of these lines, then $|S| = 2p$ and there are $p = |S|/2$ perfect directions.

We prove Theorem 1 in the next section, and discuss related open problems in the concluding Section 3.

2. The proof of Theorem 1

We begin with setting up the notation and recalling basic facts and properties of the Fourier transform on finite abelian groups.

For a subfield \mathbb{K} of the field \mathbb{C} and a finite, nonempty set G , by $L_{\mathbb{K}}(G)$ we denote the space of all functions from G to \mathbb{K} with the inner product defined by

$$\langle f, g \rangle := \frac{1}{|G|} \sum_{z \in G} f(z) \overline{g(z)}, \quad f, g \in L_{\mathbb{K}}(G),$$

the overline denoting the complex conjugation.

Suppose that G is a finite abelian group. *Dual* to G is the group of all homomorphisms from G to \mathbb{C}^\times . The dual group is denoted \widehat{G} , its elements are called *characters*, the identity element of \widehat{G} is the *principal* character. The Fourier transform of a function $f \in L_{\mathbb{K}}(G)$ is the function $\widehat{f} \in L_{\mathbb{C}}(\widehat{G})$ defined by

$$\widehat{f}(\chi) := \langle f, \chi \rangle, \quad \chi \in \widehat{G}.$$

The function $f \in L_{\mathbb{K}}(G)$ is constant if and only if its Fourier transform is zero or supported on the principal character.

For a subgroup $H \leq G$, the set of all characters $\chi \in \widehat{G}$ containing H in their kernel is a subgroup of \widehat{G} , denoted H^\perp ; thus,

$$H^\perp = \{\chi \in \widehat{G} : \chi(h) = 1 \quad \text{for any } h \in H\} \leq \widehat{G}.$$

If $H \leq G$ is nonzero and proper, then so is $H^\perp \leq \widehat{G}$. Writing 1_H and 1_{H^\perp} for the indicator functions of H and H^\perp , respectively, we have $\widehat{1_H} = (|H|/|G|) \cdot 1_{H^\perp}$.

For a function $g \in L_{\mathbb{K}}(G)$ and an element $z \in G$, let $g_z \in L_{\mathbb{K}}(G)$ be defined by

$$g_z(x) := \overline{g(z-x)}, \quad x \in G.$$

The *convolution* of functions $f, g \in L_{\mathbb{K}}(G)$ is the function

$$f * g : z \mapsto \langle f, g_z \rangle, \quad z \in G.$$

The Fourier transform of a convolution is the product of Fourier transforms:

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g}, \quad f, g \in L_{\mathbb{K}}(G).$$

Our argument relies on the following uncertainty inequality for the rational-valued functions on a finite affine plane.

THEOREM 2 ([BL, Theorem 1]). *For any prime $p \geq 3$ and any function $f \in L_{\mathbb{Q}}(\mathbb{F}_p^2)$, either*

$$\frac{1}{2} |\text{supp } f| + \frac{1}{p-1} |\text{supp } \widehat{f}| \geq p + 1,$$

or there is a direction in \mathbb{F}_p^2 such that f is constant on every line in this direction.

It may be worth commenting that the proof of Theorem 2 is a mixture of Fourier-analytic and finite-geometry considerations. In particular, it uses the classical estimate for the size of the smallest blocking set in a finite affine plane.

We now turn to the proof of Theorem 1.

If w is a constant function, then $S = \mathbb{F}_p^2$ and the assertion is immediate; assume thus that w is not constant. The case $p = 3$ is easy to verify, and we further assume that $p \geq 5$.

By the Dirichlet simultaneous approximation theorem, there exist arbitrarily large integers Q , along with the corresponding integer-valued functions w_Q on \mathbb{F}_p^2 , such that

$$\left\| w - \frac{w_Q}{Q} \right\|_{\infty} < \frac{1}{2pQ}.$$

As a result, if Q is sufficiently large, then $\text{supp } w_Q = \text{supp } w$, and for $x, y \in S$ we have $w(x) = w(y)$ if and only if $w_Q(x) = w_Q(y)$; also, a direction is perfect with respect to w if and only if it is perfect with respect to w_Q . Consequently, passing from w to w_Q , we can ensure that, in addition to being nonconstant, w is also integer-valued.

PERFECT DIRECTIONS IN \mathbb{F}_p^2

To every direction in \mathbb{F}_p^2 there corresponds a nonzero, proper subgroup $H < \mathbb{F}_p^2$; specifically, the subgroup represented by the line through the origin in the corresponding direction. As an immediate corollary from the definitions, the direction corresponding to a subgroup $H < \mathbb{F}_p^2$ is perfect if and only if the convolution $w * 1_H$ is a constant function; that is, the product $\widehat{w} \cdot 1_{H^\perp}$ vanishes at every nonprincipal character; in other words, \widehat{w} vanishes on every character from H^\perp with the possible exception of the principle character.

Denote the number of perfect directions by N , so that the number of imperfect directions is $p + 1 - N$. The group $\widehat{\mathbb{F}_p^2} \cong \mathbb{F}_p^2$ is a union of its $p + 1$ nonzero, proper subgroups, with every nonprincipal character $\chi \in \widehat{\mathbb{F}_p^2}$ lying in exactly one subgroup, and the principal character lying in all subgroups. Therefore, since \widehat{w} vanishes on the subgroups corresponding to the perfect directions, we have

$$|\text{supp } \widehat{w}| \leq (p - 1)(p + 1 - N) + 1. \quad (1)$$

On the other hand, applying Theorem 2 to the function w , we conclude that either

$$\frac{1}{2} |\text{supp } w| + \frac{1}{p - 1} |\text{supp } \widehat{w}| \geq p + 1, \quad (2)$$

or there is a direction ∂ such that w is constant on every line in this direction. In the former case, combining (2) and (1), and recalling that $p \geq 5$, we get

$$p + 1 \leq \frac{1}{2} |S| + \left((p + 1 - N) + \frac{1}{p - 1} \right) < \frac{1}{2} (|S| + 1) + p + 1 - N,$$

implying $N \leq \frac{1}{2} |S|$. In the latter case, denoting by k the number of lines in the direction ∂ on which w is nonzero, we have $|S| = kp$, while $N = p$ (all directions except ∂ are perfect). Consequently, $N \leq \frac{1}{2} |S|$, unless $k = 1$, meaning that there is a line on which w is constant and nonzero, and outside of which w vanishes.

This completes the proof of Theorem 1.

3. Open problems: restricting the weights

Suppose that $w \in L_{\mathbb{C}}(\mathbb{F}_p^2)$ is not constant, and let $S = \text{supp } w$. If $|S| < p$, then in every direction there is a line disjoint from S ; hence, for perfect directions to exist, the average value of w on \mathbb{F}_p^2 must be zero. This suggests the following problem: how many perfect directions can there be for a function w with a small support given that the average of w is *nonzero*?

As we have just saw, one needs $|S| \geq p$ in order to have any perfect directions at all.

If $|S| = p$, then for any direction determined by S there is a line in this direction disjoint from S ; therefore, none of the directions determined by S is perfect. On the other hand, if w is constant on S , then any direction not determined by S is perfect. It follows that the largest possible number of perfect directions is equal to the largest possible number of undetermined directions, which is $p + 1$ less the smallest possible number of determined directions. Apart from the trivial case where S is a line, the smallest possible number of determined directions is $(p + 3)/2$ by the of Rédei-Megyesi result; thus, the largest possible number of perfect directions (for S not being a line, $|S| = p$, and the average of w nonzero) is $(p + 1) - \frac{1}{2}(p + 3) = \frac{1}{2}(p - 1)$.

For $|S| = p + 1$, one perfect direction is very easy to arrange, and a simple combinatorial argument shows that there cannot be two or more perfect directions. Notice that this contrasts sharply the situation where $|S| = p$.

For $|S| = p + 2$ one can have two perfect directions (set $w(z) = 1/2$ for $z \in \{(0, 0), (0, 1), (1, 0), (1, 1)\}$, and $w(z) = 1$ for $z = (x, x)$ with $x \in [2, p - 1]$); however, it is not clear to us whether there can be three or more perfect directions, nor what happens for $|S| \geq p + 3$.

Replacing the nonzero average assumption with the stronger assumption that w attains real *nonnegative* values seems to result in an equally interesting problem.

REFERENCES

- [BL] BÍRÓ, A.—LEV, V.: *Uncertainty in finite planes* (submitted).
- [DKM92] DRESS, A. W. M.—KLIN, M. H.—MUZICHUK, M. E.: *On p -configurations with few slopes in the affine plane over \mathbb{F}_p and a theorem of W. Burnside's*, Bayreuth. Math. Schr. **40** (1992), 7–19.
- [G03] GÁCS, A.: *On a generalization of Rédei's theorem*, *Combinatorica* **23** (2003), no. 4, 585–598.
- [LS83] LOVÁSZ, L.—SCHRIJVER, A.: *Remarks on a theorem of Rédei*, *Studia Sci. Math. Hungar.* **16** (1983), no. 3–4, 449–454.
- [R73] RÉDEI, L.: *Lacunary Polynomials over Finite Fields*. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1973.

Received March 8, 2019
Accepted November 4, 2020

Vsevolod F. Lev
Department of Mathematics
The University of Haifa at Oranim
Tivon 36006
ISRAEL
E-mail: seva@math.haifa.ac.il