UNCERTAINTY IN FINITE PLANES

ANDRÁS BIRÓ[†] AND VSEVOLOD F. LEV

Abstract. We establish a number of uncertainty inequalities for the additive group of a finite affine plane, showing that for p prime, a nonzero function $f\colon \mathbb{F}_p^2 \to \mathbb{C}$ and its Fourier transform $\hat{f}\colon \widehat{\mathbb{F}_p^2} \to \mathbb{C}$ cannot have small supports simultaneously. The "baseline" of our investigation is the well-known Meshulam's bound, which we sharpen, for the particular groups under consideration, taking into account not only the sizes of the support sets $\operatorname{supp} f$ and $\operatorname{supp} \hat{f}$, but also their structure.

Our results imply in particular that, with some explicitly classified exceptions, one has $|\operatorname{supp} f||\operatorname{supp} \hat{f}| \ge 3p(p-2)$; in comparison, the classical uncertainty inequality gives $|\operatorname{supp} f||\operatorname{supp} \hat{f}| \ge p^2$.

1. Introduction and background

The uncertainty principle asserts that a nonzero function and its Fourier transform cannot be both highly concentrated on small sets. In this paper we will be concerned with Fourier analysis on finite abelian groups with the uniform probability measure, the most known and classical realization of the general uncertainty principle in these settings being as follows (see, for instance, [5, 8, 11]).

Theorem A. *If G is a finite abelian group, then for any nonzero function $f \in L(G)$ one has*

$$|\operatorname{supp} f||\operatorname{supp} \hat{f}| \ge |G|.$$

In the statement of Theorem A and throughout, we denote by $L(G)$ the vector space of all complex-valued functions on the finite abelian group G, and by $\hat{f}$ the Fourier transform of a function $f \in L(G)$ with respect to the unform probability measure; that is,

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{g \in G} f(g)\,\overline{\chi}(g), \quad \chi \in \widehat{G}$$

where $\widehat{G}$ is the group dual to G, and $\overline{\chi}$ is the character conjugate to χ. (See Section 3 for the summary of notation used.)

2000 *Mathematics Subject Classification.* Primary: 42A99; secondary: 65T50, 20K01.

Key words and phrases. Uncertainty principle, Fourier transform.

[†] Research partially supported by NKFIH (National Research, Development and Innovation Office) grants K-109789, K 119528 and by the MTA Rényi Intézet Lendület Automorphic Research Group.

Theorem A can be significantly improved for groups of prime order, which we identify with the additive groups of the corresponding fields and denote $\mathbb{F}_p$.

Theorem B (Biró [2], Tao [10]). *If p is a prime, then for any nonzero function $f \in L(\mathbb{F}_p)$ one has*

$$|\operatorname{supp} f| + |\operatorname{supp} \hat{f}| \ge p + 1.$$

The inequality of Theorem B was established by the first-named author of the present paper, who has contributed it as a problem to the year 1998 Miklós Schweitzer mathematical competition, and then independently rediscovered by Tao. Tao has also shown that the inequality is sharp, and provided some applications.

Theorem B has been extended by Meshulam onto arbitrary finite abelian groups.

Theorem C (Meshulam [7]). *Suppose that G is a finite abelian group, and $f \in L(G)$. If $d_1 < d_2$ are two consecutive divisors of $|G|$ such that $d_1 \le |\operatorname{supp} f| \le d_2$, then*

$$|\operatorname{supp} \hat{f}| \ge \frac{|G|}{d_1 d_2}\,(d_1 + d_2 - |\operatorname{supp} f|).$$

Notice that in the case where $G = \mathbb{F}_p$ with p prime, Theorem C reduces to Theorem B. Indeed, Meshulam's proof of Theorem C uses induction, with Theorem B serving the base case.

As it has been observed by Tao, Theorem C shows that in the Euclidean plane, the points $(|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|)$ lie on or above the convex polygonal line through the points $(|H|, |G/H|)$, where H ranges over all subgroups of G. At the same time, Theorem A merely states that the points $(|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|)$ lie on or above the hyperbola determined by the points $(|H|, |G/H|)$.

Suppose that H is a subgroup, and g is an element of a finite abelian group G. Let

$$H^{\perp} := \{\chi \in \widehat{G} \colon H \le \ker \chi\}.$$

It is a basic fact that a function $f \in L(G)$ is a scaled restriction of a character $\psi \in \widehat{G}$ onto the coset $g + H$ if and only if the Fourier transform $\hat{f}$ is a scaled restriction of the evaluation homomorphism $\chi \mapsto \overline{\chi}(g)$ onto the coset $\psi H^{\perp}$. We have then $|\operatorname{supp} f| = |H|$ and $|\operatorname{supp} \hat{f}| = |H^{\perp}| = |G|/|H|$, so that Theorem A is sharp in this case. Tao conjectured, however, that the estimate of Theorem A can be substantially sharpened, provided that $|\operatorname{supp} f|$ and $|\operatorname{supp} \hat{f}|$ stay away from any divisor of $|G|$. Theorem C confirms this conjecture.

2. Summary of results

It is well-known that the construction at the end of the previous section is the only one for which equality holds in Theorem A. This makes it plausible to expect that, in fact, it might be possible to improve the estimate of Theorem A assuming only that $\operatorname{supp} f$ is not "too close" to a coset of a subgroup of G, and $\operatorname{supp} \hat{f}$ is not "too close" to a coset of a subgroup of $\widehat{G}$ (in contrast with the much stronger assumption that $|\operatorname{supp} f|$ and $|\operatorname{supp} \hat{f}|$ stay away from any divisor of $|G|$). In this paper we establish several results of this sort in the special case where the underlying group is elementary abelian of rank 2; that is, $G = \mathbb{F}_p^2$ with p prime.

For comparison purposes, we notice that for the rank-2 elementary abelian groups, Theorem C can be rendered in a rather different way. Namely, suppose that $f \in L(\mathbb{F}_p^2)$ is a nonzero function. If $\min\{|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|\} \ge p$, then

$$\min\{|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|\} + \frac{1}{p} \max\{|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|\} \ge p + 1; \tag{1}$$

otherwise $\max\{|\operatorname{supp} f|, |\operatorname{supp} \hat{f}|\} \ge p$ by Theorem A, and then Theorem C leads to

$$|\operatorname{supp} \hat{f}| \ge \begin{cases} p(p+1-|\operatorname{supp} f|) & \text{if } |\operatorname{supp} f| \le p \le |\operatorname{supp} \hat{f}|, \\ p^{-1}(p^2+p-|\operatorname{supp} f|) & \text{if } |\operatorname{supp} \hat{f}| \le p \le |\operatorname{supp} f|, \end{cases}$$

which shows that (1) holds true in this case, too. It is equally easy to see that, conversely, for the groups under consideration, (1) implies the estimate of Theorem C. Thus, (1) is an equivalent restatement of Theorem C for the groups $G = \mathbb{F}_p^2$.

We conjecture that, perhaps, much more can be true.

Conjecture 1. *If p is a prime, then for any nonzero function $f \in L(\mathbb{F}_p^2)$, and any integer $k \in [1, p]$, writing for brevity $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, we have*

$$\frac{1}{k} \min\{|S|, |X|\} + \frac{1}{p+1-k} \max\{|S|, |X|\} \ge p + 1,$$

unless at least one of the sets $S \subseteq \mathbb{F}_p^2$ and $X \subseteq \widehat{\mathbb{F}_p^2}$ is a dense subset of a union of a small number of proper cosets of the corresponding group. (Perhaps, it suffices to assume that neither S, nor X can be covered by fewer than $\min\{k, p+1-k\}$ cosets.)

Equivalently, if for some $k \in [1, p]$ and $\varepsilon \in (0, 1)$ we have $\min\{|S|, |X|\} \le (1-\varepsilon)k(p+1)$, then $\max\{|S|, |X|\} \ge \varepsilon(p+1)(p+1-k)$, unless the subgroup structure of $\mathbb{F}_p^2$ is involved, as indicated.

We will occasionally use the notation $S = \operatorname{supp} f$ and $X = \operatorname{supp} \hat{f}$ without redefining it anew each time.

The left-hand side of the inequality of Conjecture 1 is minimized, over all *real* $k > 0$, for

$$k = \frac{p+1}{\max\left\{\sqrt{|X|/|S|}, \sqrt{|S|/|X|}\right\} + 1} \le \frac{p+1}{2},$$

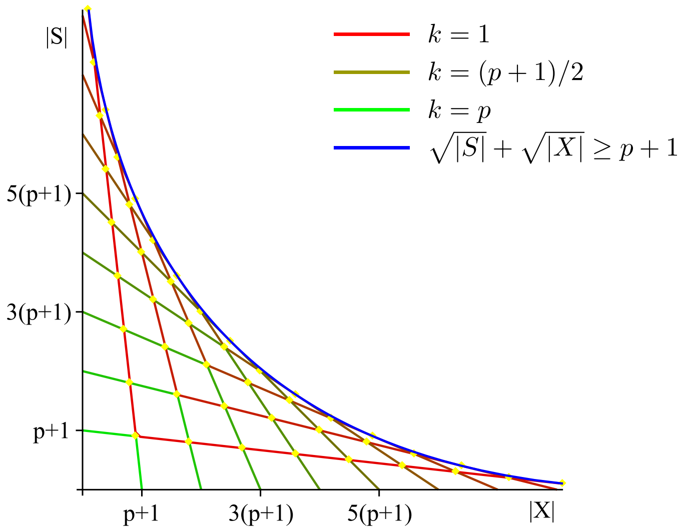
the corresponding minimum value being $(\sqrt{|X|}+\sqrt{|S|})^2/(p+1)$. As a result, recalling Theorem B, it is very tempting to further conjecture, as an "almost-corollary" of Conjecture 1, that for any nonzero function $f \in L(\mathbb{F}_p^2)$ one has

$$\sqrt{|X|}+\sqrt{|S|} \ge p+1, \tag{2}$$

provided that neither S nor X is contained in a union of fewer than $p/2$ cosets.

The bounds of Conjecture 1 corresponding to various values of k, along with the enveloping bound (2), are shown in Figure 1. The yellow dots are points of the form $(m(p+1-n), n(p+1-m))$ where $1 \le m, n \le p$ are integers; their relevance will become clear later.

Figure 1. Conjecture 1.



The case $k = 1$ of Conjecture 1 is Theorem C in the form (1), the case $k = p$ follows from it since for any real numbers $m \le M$, one has

$$\frac{1}{p}\,m + M \ge m + \frac{1}{p}\,M.$$

In general, for a positive integer $\kappa < p/2$, the case $k = \kappa$ of Conjecture 1 implies the case $k = p+1-\kappa$, and for $p/2 < \kappa < p$, the case $k = \kappa$ implies the case $k = \kappa + 1$.

Our first principal result establishes the case $k = 2$ of the conjecture for *rational-valued* functions.

Theorem 1. *If $p \geq 3$ is a prime, and $f \in L(\mathbb{F}_p^2)$ is a nonzero rational-valued function, then writing $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, we have*

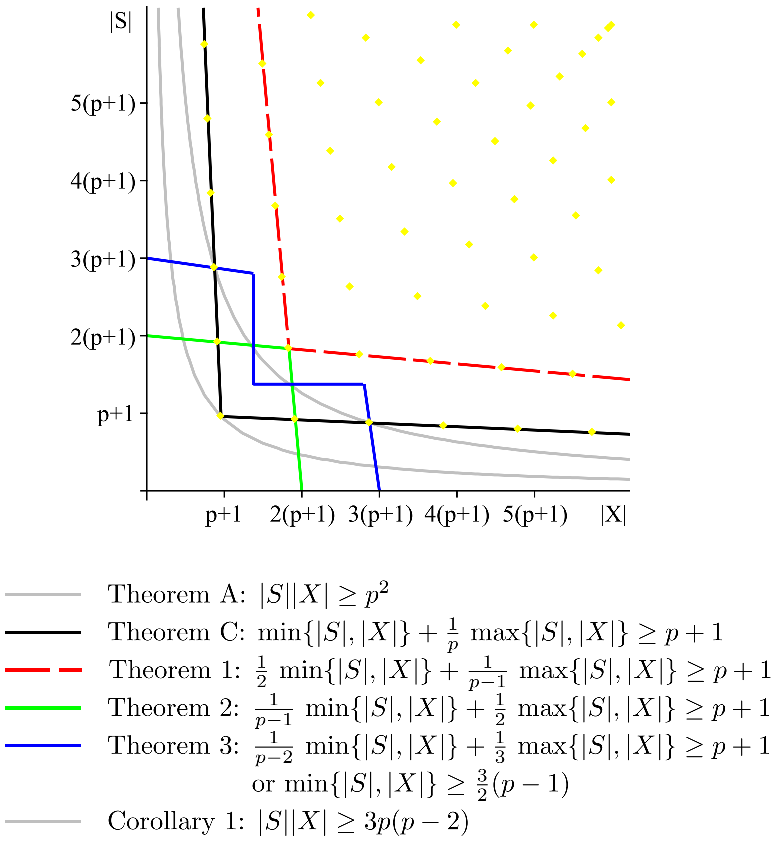
$$\frac{1}{2}\min\{|S|,|X|\} + \frac{1}{p-1}\max\{|S|,|X|\} \geq p+1,$$

except if there exists a nonzero, proper subgroup $H < \mathbb{F}_p^2$ such that f is constant on each H-coset (in which case $X = H^\perp$ if the sum of all values of f is nonzero, and $X = H^\perp \setminus \{1\}$ if the sum is equal to 0).

Remark 1. Denoting by 1_{H_1} and 1_{H_2} the indicator functions of distinct, nonzero, proper subgroups $H_1, H_2 < \mathbb{F}_p^2$, and letting $f := 1_{H_1} - 1_{H_2}$, we have $|S| = |X| = 2(p-1)$, so that the estimate of Theorem 1 holds as an equality in this case.

The reader is invited to review Figure 2 where the bounds of Theorems A and C are shown in gray (the lower hyperbola) and black, respectively, and the bound of Theorem 1 is represented by the red dashed line.

Figure 2. Bound comparison.



Next, we settle the case $k=p-1$ of Conjecture 1. To state the corresponding result, we notice that the definition of an orthogonal subgroup at the end of Section 1 establishes a bijection between the subgroups of the group $\mathbb{F}_p^2$ and those of the dual group $\widehat{\mathbb{F}_p^2}$, the inverse bijection being given by

$$F \mapsto F^\perp := \cap_{\chi\in F} \ker\chi, \quad F \le \widehat{\mathbb{F}_p^2}.$$

We say that the subgroups $H \le \mathbb{F}_p^2$ and $H^\perp \le \widehat{\mathbb{F}_p^2}$ (equivalently, $F \le \widehat{\mathbb{F}_p^2}$ and $F^\perp \le \mathbb{F}_p^2$) are orthogonal to each other.

Theorem 2. *If $p\ge 3$ is a prime, and $f\in L(\mathbb{F}_p^2)$ is a nonzero function, then letting $S:=\operatorname{supp} f$ and $X:=\operatorname{supp}\hat f$ we have*

$$\frac{1}{p-1}\min\{|S|,|X|\}+\frac12\max\{|S|,|X|\}\ge p+1,$$

except if S and X are cosets of a pair of nonzero, proper, mutually orthogonal subgroups of $\mathbb{F}_p^2$ and $\widehat{\mathbb{F}_p^2}$, respectively.

The bound furnished by Theorem 2 is shown in green in Figure 2.

Remark 2. The inequality of the theorem readily implies $\max\{|S|,|X|\}\ge 2(p-1)$.

Remark 3. Equality is attained, for instance, if f takes the value 1 on a coset of a nonzero, proper subgroup of $\mathbb{F}_p^2$, the value -1 on another coset of the same subgroup, and vanishes outside of these two cosets; in this case $|S|=2p$ and $|X|=p-1$.

Remark 4. The exceptional case of the theorem is described by Lemma 7 in the appendix: namely, in this case there exist a nonzero, proper subgroup $H<\mathbb{F}_p^2$, a character $\chi_0\in\widehat{\mathbb{F}_p^2}$, an element $g_0\in\mathbb{F}_p^2$, and a nonzero coefficient $c\in\mathbb{C}$ such that

$$f(g)=\begin{cases} c\chi_0(g) & \text{if } g\in g_0+H,\\ 0 & \text{if } g\notin g_0+H.\end{cases}$$

Although we were unable to fully prove Conjecture 1 for $k=p-2$, we could at least give a proof under the extra assumption $\min\{|S|,|X|\}<\frac32(p-1)$. The resulting estimate, visualized in Figure 2 by the blue line, can also be viewed as a contribution towards the case $k=2$.

Theorem 3. *If $p\ge 3$ is a prime, and $f\in L(\mathbb{F}_p^2)$ is a nonzero function, then letting $S:=\operatorname{supp} f$ and $X:=\operatorname{supp}\hat f$, we have either*

$$\frac{1}{p-2}\min\{|S|,|X|\}+\frac13\max\{|S|,|X|\}\ge p+1,$$

or

$$\min\{|S|,|X|\}\ge\frac32(p-1),$$

except if the smallest of the sets S and X is a coset of a nonzero, proper subgroup of the corresponding group, possibly with one element missing, and the largest is either a coset, or a union of two cosets of the orthogonal subgroup.

Remark 1. As an easy corollary of the theorem, if $p \geq 11$ is a prime, and $f \in L(\mathbb{F}_p^2)$ is a nonzero function, then letting $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, we have either

$$\min\{|S|, |X|\} \geq \frac{3}{2}(p-1),$$

or

$$\max\{|S|, |X|\} \geq 3p-1,$$

unless S and X are exceptional as specified in the statement of the theorem.

Remark 2. The exceptional cases of the theorem are classified by Lemma 7; specifically, in these cases one of the following holds:

i) there exist a nonzero, proper subgroup $H < \mathbb{F}_p^2$, an element $g_0 \in \mathbb{F}_p^2$, characters $\chi_1, \chi_2 \in \widehat{\mathbb{F}_p^2}$ with $\chi_2 \notin \chi_1 H^{\perp}$, and coefficients $c_1, c_2 \in \mathbb{C}$ at most one of which is equal to 0, such that

$$f(g) = \begin{cases} c_1\chi_1(g) + c_2\chi_2(g) & \text{if } g \in g_0 + H, \\ 0 & \text{if } g \notin g_0 + H; \end{cases}$$

ii) there exist a nonzero, proper subgroup $H < \mathbb{F}_p^2$, elements $g_1, g_2 \in \mathbb{F}_p^2$ with $g_2 \notin g_1 + H$, a character $\chi_0 \in \widehat{\mathbb{F}_p^2}$, and coefficients $c_1, c_2 \in \mathbb{C}$ at most one of which is equal to 0, such that

$$f(g) = \begin{cases} c_i\chi_0(g) & \text{if } g \in g_i + H,\ i \in \{1,2\}, \\ 0 & \text{if } g \notin (g_1 + H) \cup (g_2 + H). \end{cases}$$

As a consequence of Theorems 2, 3, and C, we have

Corollary 1. *If $p > 3$ is a prime, and $f \in L(\mathbb{F}_p^2)$ is a nonzero function, then letting $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$ we have*

$$|S||X| \geq 3p(p-2),$$

unless either $\min\{|S|, |X|\} \leq 2$, or the smallest of the sets S and X is a coset of a nonzero subgroup of the corresponding group, possibly with one element missing, and the largest is either a coset, or a union of two cosets of the orthogonal subgroup.

For the reader not convinced by Figure 2, where the estimate of Corollary 1 corresponds to the upper gray hyperbola, we include the formal proof in the appendix.

The proof of Corollary 1 relies on Theorems 2, 3, and C. Using, instead of Theorem 3, one of the Theorems 4 and 5 below, one can find constants $K > 3$ and N such that

$|S||X| \ge Kp^2$, unless S or X is contained in a union of N proper cosets. Indeed, it is easy to see that, assuming Conjecture 1, for *any* real K there exists $N = N(K)$ with the property just mentioned. While we seem to be far from establishing Conjecture 1 in full generality, we feel that it may be possible to prove at least the estimate $|S||X| \ge Kp^2$ developing further the ideas behind the proofs of Theorems 4 and 5.

Theorem 4. *If $p \ge 31$ is a prime and $f \in L(\mathbb{F}_p^2)$ is a nonzero function, then writing $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, for any $\varepsilon \in (0,1)$ we have either*

$$\min\{|S|, |X|\} \ge 2(1-\varepsilon)p$$

or

$$\max\{|S|, |X|\} \ge \varepsilon p^{3/2},$$

except if the smallest of the sets S and X is contained in a coset of a nonzero, proper subgroup of the corresponding group.

Remark 1. The bound $p \ge 31$ is certainly not best possible. It can be relaxed by fine-tuning the parameters of our proof and, perhaps, can be dropped altogether.

Remark 2. The exceptional case of Theorem 4, where the smallest of the sets S and X is contained in a coset of a proper subgroup, is directly addressed in Lemma 7.

Remark 3. To put Theorem 4 in a context, the reader is recommended to review the paragraph following Conjecture 1 observing, on the other hand, that the assertion of Theorem 4 can be equivalently written as

$$\frac{1}{2}\min\{|S|, |X|\} + \frac{1}{\sqrt{p}}\max\{|S|, |X|\} \ge p,$$

apart from the exceptional case specified in the theorem. Thus, Theorem 1 gives a stronger estimate than Theorem 4, while the latter theorem does not impose the rationality assumption.

Remark 4. The coefficient $2(1-\varepsilon)$ in the statement of Theorem 4 cannot be replaced with 2. This is readily seen by fixing two distinct nonzero, proper subgroups $H_1, H_2 < \mathbb{F}_p^2$, and letting f to be the difference of their indicator functions: $f = 1_{H_1} - 1_{H_2}$; in this case $|S| = |X| = 2(p-1)$.

Theorem 5. *If p is a prime, and $f \in L(\mathbb{F}_p^2)$ is a nonzero function, then writing $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, for any $\varepsilon \in (0,1)$ we have either*

$$\min\{|S|, |X|\} \ge 3\,(1-\varepsilon)p,$$

or

$$\max\{|S|, |X|\} \ge \frac{1}{6}\,\varepsilon p^{4/3},$$

except if the smallest of the sets S and X is contained in a coset of a nonzero, proper subgroup, or in a union of two such cosets (possibly corresponding to different subgroups).

Remark 1. In the situation where $|X| \le |S|$, the exceptional cases of Theorem 5 are classified by Lemmas 7–9 in the appendix; the situation where $|S| \le |X|$ can be dealt with using duality.

Remark 2. The two inequalities of Theorem 5 can be merged together to read

$$\frac{1}{3}\min\{|S|,|X|\} + \frac{6}{p^{1/3}}\max\{|S|,|X|\} \ge p,$$

to be compared against the case $k = 3$ of Conjecture 1.

Remark 3. The coefficient $3(1-\varepsilon)$ cannot be replaced with 3. This is readily seen by taking three pairwise distinct, nonzero, proper subgroups $H_1, H_2, H_3 < \mathbb{F}_p^2$, and letting $f := 1_{H_1} + 1_{H_2} - 2 \cdot 1_{H_3}$; in this case $|S| = |X| = 3(p-1)$.

Theorem 5 is easily seen to imply Theorems 2 and 3 for sufficiently large primes p, apart from the slightly less accurate classification of the exceptional cases. We believe, hoverer, that the two latter theorems are worth stating separately as their proofs are short, non-technical, and based on the ideas distinct from those used in the proof of Theorem 5.

In the next section we briefly summarize the basic definitions, notation, and facts about the Fourier transform in finite abelian groups. Section 4 contains some simple, but important observations preparing the ground for the proofs of Theorems 1–5; the proofs themselves are presented in Sections 5–9, respectively. In the appendix we state and prove Lemmas 6–9 classifying the exceptional cases arising in Theorems 2–5, and also prove Corollary 1; these results were referred to above and, with the exception of Lemma 6, are not used elsewhere.

3. Fourier transform: notation and basics

Although familiarity with Fourier transform is assumed, the brief review below can be useful. For the reader's convenience, we include here the notation that has already been introduced above. The proofs, on the other hand, are omitted; they can be found in any standard textbook on the subject, like [11].

For a finite abelian group G, we denote by $L(G)$ the vector space of all complex-valued functions on G, and by $\widehat{G}$ the dual character group. Every finite abelian group is isomorphic to its dual, and is naturally isomorphic to its "double-dual"; this allows one to switch the roles of G and $\widehat{G}$.

We are primarily interested in the situation where G is the elementary abelian p-group of rank 2, which we denote $\mathbb{F}_p^2$, where p is a prime.

For a character $\chi\in\widehat{G}$, by $\overline{\chi}$ we denote the conjugate character; that is, $\overline{\chi}(g)=\chi(-g)$ is the complex conjugate of $\chi(g)$, for any $g\in G$. The principal character will be denoted 1; thus, $1=1_G$, with the convention that 1_A denotes the indicator function of the set A.

The Fourier transform of a function $f\in L(G)$ is the function $\hat f\in L(\widehat{G})$ defined by

$$\hat f(\chi)=\frac{1}{|G|}\sum_{g\in G}f(g)\,\overline{\chi}(g),\quad \chi\in\widehat{G},$$

and the inversion formula is

$$f(g)=\sum_{\chi\in\widehat{G}}\hat f(\chi)\,\chi(g),\quad g\in G.$$

The values $\hat f(\chi)$ are called the Fourier coefficients of the function f.

The convolution f_1*f_2 of the functions $f_1,f_2\in L(G)$ is defined by

$$f_1*f_2\colon g\mapsto\frac{1}{|G|}\sum_{\substack{g_1,g_2\in G\\ g_1+g_2=g}}f_1(g_1)f_2(g_2),\quad g\in G.$$

We have $\widehat{f_1*f_2}=\widehat{f_1}\cdot\widehat{f_2}$ and, conversely, $\widehat{f_1f_2}=\widehat{f_1}*\widehat{f_2}$ for any $f_1,f_2\in L(G)$, with the convolution on the dual group defined by

$$u_1*u_2\colon\chi\mapsto\sum_{\substack{\chi_1,\chi_2\in\widehat{G}\\ \chi_1\chi_2=\chi}}u_1(\chi_1)u_2(\chi_2),\quad \chi\in\widehat{G},$$

where $u_1,u_2\in L(\widehat{G})$. (The minor normalization inconsistency arising here can be formally resolved by looking at the ordered pairs $(G,\widehat{G})$ instead of single groups G.)

The subgroup of $\widehat{G}$ orthogonal to a given subgroup $H\le G$ is

$$H^\perp:=\{\chi\in\widehat{G}\colon H\le\ker\chi\},$$

and the subgroup of G orthogonal to a given subgroup $F\le\widehat{G}$ is

$$F^\perp:=\cap_{\chi\in F}\ker\chi.$$

The subgroup $H^\perp$ is naturally isomorphic to the character group $\widehat{G/H}$.

We have $\widehat{1_H}=(|H|/|G|)\cdot 1_{H^\perp}$ and, more generally, $\widehat{1_{g+H}}(\chi)=(|H|/|G|)\,\overline{\chi}(g)\cdot 1_{H^\perp}(\chi)$ for any element $g\in G$ and character $\chi\in\widehat{G}$.

Finally, $(H^\perp)^\perp=H$ for any subgroup $H\le G$, and similarly $(F^\perp)^\perp=F$ for any subgroup $F\le\widehat{G}$; as a result, one can speak about pairs of mutually orthogonal subgroups.

4. Basic observations

Let G be a finite abelian group.

For a function $f \in L(G)$, a subgroup $H \le G$, and an element $g \in G$, the Fourier coefficients of the function $f \cdot 1_{g+H}$ (coinciding with f on the coset $g+H$ and vanishing outside of it) are

$$\begin{aligned}\widehat{f \cdot 1_{g+H}}(\chi) &= (\hat{f} * \widehat{1_{g+H}})(\chi) \\ &= \sum_{\psi \in \widehat{G}} \hat{f}(\chi\psi) \cdot \frac{\psi(g)}{|H^\perp|}\, 1_{H^\perp}(\overline{\psi}) \\ &= \frac{1}{|H^\perp|} \sum_{\psi \in H^\perp} \hat{f}(\chi\psi)\psi(g), \quad \chi \in \widehat{G}. \end{aligned} \tag{3}$$

A more explicit form of this relation is

$$\sum_{\psi \in H^\perp} \hat{f}(\chi\psi)\psi(g) = \frac{\overline{\chi}(g)}{|H|} \sum_{h \in H} f(g+h)\,\overline{\chi}(h), \quad \chi \in \widehat{G}. \tag{4}$$

Given a subgroup $H \le G$ and a nonzero function $f \in L(G)$, let $S := \operatorname{supp} f$ and $X := \operatorname{supp} \hat{f}$, and denote by n_S the smallest positive number of elements of S contained in a coset of H, and by n_X the smallest positive number of characters from X contained in a coset of $H^\perp$:

$$n_S := \min\{|(s+H) \cap S| \colon s \in S\},\ n_X := \min\{|\chi H^\perp \cap X| \colon \chi \in X\}. \tag{5}$$

Also, let K_S be the number of H-cosets having a nonempty intersection with S, and let K_X be the number of $H^\perp$-cosets having a nonempty intersection with X:

$$K_S := |S+H|/|H|,\ K_X := |XH^\perp|/|H^\perp|. \tag{6}$$

Thus, S and X depend on f, while n_S, n_X, K_S, and K_X depend on both f and H, although this dependence is not reflected explicitly by our notation.

Recall that a group is called *prime* if it has prime order (in which case it is cyclic).

Lemma 1. *Suppose that H is a subgroup of the finite abelian group G, and $f \in L(G)$ is a nonzero function, and let S, X, n_S, n_X, K_S, and K_X be as above. If H is prime, then $K_X \ge |H|+1-n_S$, whence $|X| \ge n_X(|H|+1-n_S)$. Similarly, if H is co-prime (meaning that G/H is prime), then $K_S \ge |H^\perp|+1-n_X$, whence $|S| \ge n_S(|H^\perp|+1-n_X)$.*

Proof. Fix $g \in G$ with $|(g+H) \cap S| = n_S$, and consider the function $f_g \in L(H)$ defined by $f_g(h) := f(g+h)$, $h \in H$. In terms of this function, (4) can be rewritten as

$$\overline{\chi}(g)\, \widehat{f_g}(\chi|_H) = \sum_{\psi \in H^\perp} \hat{f}(\chi\psi)\psi(g), \quad \chi \in \widehat{G}, \tag{7}$$

where $\chi|_H$ denotes the restriction of χ onto H. Since $|\operatorname{supp} f_g| = n_S$ and H is prime, by Theorem B there are at least $|H| + 1 - n_S$ characters $\eta \in \widehat{H}$ with $\widehat{f_g}(\eta) \neq 0$. Every such character $\eta \in \widehat{H}$ extends to a character $\chi \in \widehat{G}$ with $\chi|_H = \eta$. For this character χ, the left-hand side of (7) is nonzero; hence, the right-hand side is nonzero either, showing that $\chi H^\perp$ has a nonempty intersection with X. Moreover, if $\chi'|_H \neq \chi''|_H$, then $\chi' H^\perp \neq \chi'' H^\perp$, so that different characters $\eta \in \widehat{H}$ result in different cosets $\chi H^\perp$.

This proves the first assertion of the lemma. The second one follows by duality; that is, essentially, by repeating the argument with G, H, and f replaced with $\widehat{G}$, $H^\perp$, and $\hat{f}$, respectively (which is legitimate since $|H^\perp| = |\widehat{G/H}| = |G/H|$ shows that $H^\perp$ is prime). □

Although fairly straightforward, Lemma 1 is of crucial importance for the proofs of Theorems 1–5.

It may be worth noting that the argument employed in the proof of Lemma 1 can be used to give an inductive proof of Theorem A. Namely, choosing arbitrarily a nonzero proper subgroup $H < G$ (the induction basis where G is a prime group is to be given a separate treatment), and using the induction hypothesis instead of the assumption that H and G/H are prime, we get $|X| \geq n_X \cdot |H|/n_S$ and $|S| \geq n_S \cdot |H^\perp|/n_X$, which yields $|S||X| \geq |H||H^\perp| = |G|$.

As another illustration of our approach, we derive Theorem C for the group $G = \mathbb{F}_p^2$. By duality, we can assume that $|X| \leq |S|$. Fix a nonzero, proper subgroup $H < \mathbb{F}_p^2$, and define n_S, n_X, K_S, K_X as above. By Lemma 1,

$$\begin{aligned} |X| + \frac{1}{p}\,|S| &\geq n_X(p+1-n_S) + \frac{1}{p}\,n_S(p+1-n_X) \\ &= p + 1 + \frac{p+1}{p}\,(n_X-1)(p-n_S) \\ &\geq p+1, \end{aligned}$$

as wanted.

5. Proof of Theorem 1

Recall, that for a prime power q, a blocking set in the affine plane $\mathbb{F}_q^2$ is a set that blocks (meets) every line. A union of two nonparallel lines is a blocking set of size $2q-1$, and a classical result by Jamison [6] and Brouwer-Schrijver [4] (see also [1, 3]) says that, in fact, any blocking set in $\mathbb{F}_q^2$ has size at least $2q-1$. We need a stability version of this result.

Lemma 2. *Suppose that q is a prime power, k and m are positive integers, and $S \subseteq \mathbb{F}_q^2$ is a set blocking every line in $\mathbb{F}_q^2$ with the exception of at most k pencils of parallel lines, each of these pencils containing at most m nonblocked lines. Then $|S| \ge 2q - k - m$.*

Proof. We refer the directions of the nonblocked lines as *special*; thus, there are at most k special directions.

If S is a blocking set, then $|S| \ge 2q - 1$ and the proof is over. Suppose thus that there is a line $l \subseteq \mathbb{F}_q^2$ avoiding S. Notice that the direction of l is special.

Consider an embedding of $\mathbb{F}_q^2$ into the projective plane $\mathrm{PG}(2, q)$, with $\mathrm{PG}(2, q) \setminus \mathbb{F}_q^2$ designated as the *line at infinity.* Let $\mathcal{S} \subseteq \mathrm{PG}(2, q)$ be the set consisting of (the image of) S and the points at infinity corresponding to the special directions; thus, $|\mathcal{S}| \le |S| + k$. Also, let ℓ be the line in $\mathrm{PG}(2, q)$ containing l, and let $\wp$ be the point of infinity incident with ℓ; that is, $\{\wp\} = \ell \setminus l$.

Clearly, $\mathcal{S}$ blocks every line in $\mathrm{PG}(2, q)$, with ℓ being blocked by the point $\wp$ only. Consequently, the set $\mathcal{S} \setminus \{\wp\}$ blocks every line in $\mathrm{PG}(2, q)$, excepting m lines at most.

We now get back to the affine world by identifying $\mathrm{PG}(2, q) \setminus \ell$ with $\mathbb{F}_q^2$. Corresponding to the set $\mathcal{S} \setminus \{\wp\}$ under this identification is a set $S' \subseteq \mathbb{F}_q^2$ which blocks every line in $\mathbb{F}_q^2$ with the possible exception of at most m lines. Adding at most m points to this set, we get a blocking set in $\mathbb{F}_q^2$, whence $|S'| \ge (2q - 1) - m$ by the Jamison-Brouwer-Schrijver result. It follows that

$$|S| \ge |\mathcal{S}| - k = |S'| + 1 - k \ge (2q - 1) - m + 1 - k = 2q - k - m,$$

as wanted. □

Turning to the proof of Theorem 1, we write for brevity $G := \mathbb{F}_p^2$, and identify G and $\widehat{G}$ with the additive group of the two-dimensional vector space over the field $\mathbb{F}_p$; thus, we call the elements of G and $\widehat{G}$ *points*, and cosets of their nonzero, proper subgroups *lines*. If $H < G$ is a nonzero, proper subgroup, then H-cosets in G will be referred to as H-lines, and $H^\perp$-cosets in $\widehat{G}$ as $H^\perp$-lines. Notice that the origin of $\widehat{G}$ is the principal character.

For a character $\chi \in \widehat{G}$, we have $\chi \in X$ if and only if the sum $\sum_{g \in S} f(g)\overline{\chi}(g)$ is a nonzero element of the cyclotomic field of order p. As an immediate corollary, if $\chi \in X$, then also $\chi^j \in X$ for each $j \in [1, p-1]$; that is, X is a union of several proper subgroups of $\widehat{G}$, with the possible exception of the principal character that can be missing from X. In other words, $X \cup \{1\}$ is a union of lines in $\widehat{G}$ passing through the origin. It follows that either $X \cup \{1\}$ is a proper subgroup of $\widehat{G}$, in which case the assertion is immediate from Lemma 6 ii), or $|X| \ge 2(p-1)$, which readily gives the estimate sought in the case where $|S| \ge |X|$.

Suppose therefore that $|S| < |X|$ and then, for a contradiction, that

$$\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| < p+1. \tag{8}$$

Fix a nonzero, proper subgroup $H < G$, and let the quantities n_S, n_X, K_S, K_X be defined by (5) and (6). Substituting the inequalities

$$|X| \ge n_X(p+1-n_S),\ |S| \ge n_S(p+1-n_X)$$

of Lemma 1 into (8), after routine algebraic manipulations we get $(n_S-2)(p-1-n_X) < 0$; thus, either $n_X = p$, or $n_S = 1$. In the former case X is a union of $H^\perp$-lines, and since X intersects nontrivially every $H^\perp$-line not passing through the origin, all such lines are in fact contained in X; hence $|X| \ge |\widehat{G}| - |H^\perp| = p^2 - p$, implying $|S| = 1$ in view of (8) and readily leading to a contradiction.

We therefore have $n_S = 1$, for any choice of the subgroup $H < G$. Applying Lemma 1, we conclude that $K_X = p$, and it follows that X contains the principal character (otherwise any line through the origin, not contained in X, would have an empty intersection with X). Consequently, X is a union of nonzero, proper subgroups of $\widehat{G}$.

Denote by $\mathcal{H}$ be the set of all those proper subgroups $H < G$ with $H^\perp \subseteq X$, and write $k := |\mathcal{H}|$; thus, $|X| = k(p-1)+1$. If we had $k = 1$, then X were a subgroup and Lemma 6 would show that S is a union of X-cosets, contrary to our present assumption $|S| < |X|$; thus, $k \ge 2$. Clearly, we have $n_X = k-1$ for every subgroup $H \in \mathcal{H}$, and $n_X = 1$ for every subgroup $H \notin \mathcal{H}$. As a result, Lemma 1 shows that S meets every line in G, except that in each of the k directions corresponding to the subgroups $H \in \mathcal{H}$, there can be up to $k-2$ lines avoiding S. By Lemma 2, we have

$$|S| \ge 2p - k - (k-2).$$

Recalling that $|X| = k(p-1)+1$, we obtain

$$\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| > (p-k+1) + k = p+1,$$

which proves the assertion.

6. Proof of Theorem 2

In this section and also in Sections 7-9 below we keep using the conventions of the previous section, writing $G := \mathbb{F}_p^2$ and using geometric terminology for the elements and subgroups of G and $\widehat{G}$.

By duality, we can assume that

$$|X| \le |S|, \tag{9}$$

and then for a contradiction that

$$\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| < p+1. \tag{10}$$

Fix a nonzero, proper subgroup $H < G$, and let n_S and n_X be defined by (5). By Lemma 1,

$$\begin{aligned}\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| &\geq \frac{1}{2}\,n_S(p+1-n_X) + \frac{1}{p-1}\,n_X(p+1-n_S)\\ &= p+1+\frac{p+1}{2(p-1)}\,(p-n_X-1)(n_S-2).\end{aligned}$$

Comparing with (10), we see that either $n_X = p$, or $n_S = 1$.

If, for a subgroup $H < G$, we have $n_X = p$, then X is a union of $H^\perp$-cosets. Moreover, if in this case we had $|S| \geq 2p$, this would imply

$$\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| > p+1,$$

contradicting (10). Thus, $|X| \leq |S| < 2p$ by (9), showing that X is in fact a unique $H^\perp$-coset and then, in view of Lemma 6 ii), that S is an H-coset.

To complete the proof, we consider the situation where $n_S = 1$ for every nonzero, proper subgroup H. By Lemma 1, in this case every line in $\widehat{G}$ contains a point from X; that is, X is a blocking set in $\widehat{G}$. Applying the result by Jamison-Brouwer-Schrijver mentioned at the beginning of Section 5, we conclude that $|X| \geq 2p-1$. Hence, by (9),

$$\frac{1}{2}\,|S| + \frac{1}{p-1}\,|X| \geq \Big(\frac{1}{2}+\frac{1}{p-1}\Big)(2p-1) > p+1,$$

in a contradiction with (10).

7. Proof of Theorem 3

We assume, without loss of generality, that $|X| \leq |S|$, and that

$$|X| < \frac{3}{2}\,(p-1) \tag{11}$$

and

$$\frac{1}{3}\,|S| + \frac{1}{p-2}\,|X| < p+1, \tag{12}$$

aiming to show that S and X have the structure detailed in the statement of the theorem.

Notice that from (12) and Theorem C,

$$p+1 > \frac{1}{3}\,|S| + \frac{1}{p-2}\,\left(p+1-\frac{1}{p}\,|S|\right),$$

implying

$$|S| < 3p. \tag{13}$$

Fix a nonzero, proper subgroup $H < G$, and define n_X, n_S, K_X, K_S by (5) and (6). Substituting the inequalities

$$|X| \geq n_X(p+1-n_S), \quad |S| \geq n_S(p+1-n_X) \tag{14}$$

of Lemma 1 into (12), simplifying, and factoring, we get

$$(n_S-3)(p-2-n_X) < 0;$$

consequently, we have either $n_S \in \{1,2\}$, or $n_X \in \{p-1,p\}$. In the latter case (11) yields $|X| < 2n_X$, whence X is contained in an $H^{\perp}$-coset, and indeed $n_X \geq p-1$ shows that X misses at most one element of this coset. Moreover, substituting $|X| = n_X$ into (14) gives $n_S = p$; along with (13), this shows that S is either a coset, or a union of two cosets of H.

It thus remains to consider the situation where $n_S \in \{1,2\}$, for any choice of a nonzero, proper subgroup $H < G$. By Lemma 1, in this case we have $K_X \geq p-1$, meaning that for every given direction in $\widehat{G}$, there is at most one line in that direction free of points of X. Since there are $p+1$ directions, and any two lines in different directions meet in exactly one point, we can add to X at most $(p+1)/2$ points to get a set which meets every line; that is, a blocking set. Recalling that, by a result of Jamison-Brouwer-Schrijver (see the beginning of Section 5), any blocking set in $\mathbb{F}_p^2$ has size at least $2p-1$, we obtain

$$|X| \geq (2p-1) - \frac{1}{2}\,(p+1) = \frac{3}{2}\,(p-1),$$

a contradiction.

8. Proof of Theorem 4

We need the following lemma.

Lemma 3. *For any prime p, and any finite set $P \subseteq \mathbb{F}_p^2$ with $2 \leq |P| \leq 4p$, not contained in a single line, there is a direction determined by P such that every line in this direction contains fewer than $\sqrt{|P|} + \max\{1, |P|/(2p)\}$ points of P.*

Proof. Denote by d the number of directions determined by P. Szőnyi [9] has shown that if $|P| \leq p$, then $d \geq \frac{|P|+3}{2}$; on the other hand, if $|P| > p$, then among the p lines in $\mathbb{F}_p^2$ in every given direction, there must be a line containing two or more points of P, showing that $d = p+1$. Thus, $d > \min\{|P|/2, p\}$ in any case.

Suppose that in every direction determined by P, there is a line containing at least M points of P; we want to show that $M < \sqrt{|P|} + \max\{1, |P|/(2p)\}$. Let $l_1, \dots, l_d$ be lines in different directions with $|l_i \cap P| \geq M$, for each $i \in [1, d]$. We use a well-known consequence of the Cauchy-Schwartz inequality asserting that for any system of finite sets $A_1,\dots,A_d$, one has

$$(|A_1|+\dots+|A_d|)^2 \le |A_1\cup\dots\cup A_d| \sum_{i,j=1}^{d} |A_i\cap A_j|. \tag{15}$$

We let $A_i := l_i\cap P$ ($i\in[1,d]$) and observe that then $|A_i\cap A_j|\le 1$ whenever $i\ne j$, and that $|A_1\cup\dots\cup A_d|\le|P|$. Writing $\sigma := |A_1|+\dots+|A_d|$, from (15) we obtain $\sigma^2\le|P|(d^2-d+\sigma)$. It follows that

$$\Big(\sigma-\frac12\,|P|\Big)^2 \le |P|(d^2-d)+\frac14\,|P|^2 < |P|d^2,$$

whence $\sigma<\frac12|P|+d\sqrt{|P|}$. On the other hand, we have $\sigma\ge dM$. This yields $M<\sqrt{|P|}+|P|/(2d)$, and to complete the proof, we recall that $d>\min\{|P|/2,p\}$. □

Proof of Theorem 4. We recall our convention to write $G=\mathbb{F}_p^2$ and to think of G and $\widehat{G}$ geometrically, referring to their elements and nonzero, proper subgroups as points and lines, respectively.

Without loss of generality, we assume that $3\le|X|\le|S|$, and then for a contradiction that

$$|X|<2(1-\varepsilon)p \quad\text{and}\quad |S|<\varepsilon p^{3/2}, \tag{16}$$

while X is not contained in a coset of a proper subgroup.

We notice that if $\varepsilon\ge\frac12+\frac{1}{4\sqrt p}$, then Theorem C along with (16) gives

$$p+1\le|X|+\frac1p\,|S|<2(1-\varepsilon)p+\varepsilon\sqrt p\le\Big(1-\frac{1}{2\sqrt p}\Big)\,p+\Big(\frac12+\frac{1}{4\sqrt p}\Big)\sqrt p=p+\frac14,$$

a contradiction; thus,

$$\varepsilon<\frac12+\frac{1}{4\sqrt p}\,. \tag{17}$$

By Lemma 3, there is a nonzero, proper subgroup $H<G$ such that every $H^\perp$-line contains fewer than $\sqrt{|X|}+1$ points of X while, on the other hand, there is an $H^\perp$-line containing at least two points of X. Throughout the proof, we consider this subgroup H fixed, and define n_S,n_X,K_S,K_X by (5) and (6).

The assumption that every $H^\perp$-line contains fewer than $\sqrt{|X|}+1$ points of X, in view of (16), implies $n_X<\sqrt{2p}+1$. Therefore, by (16) and Lemma 1,

$$\varepsilon p^{3/2}>|S|\ge n_S(p+1-n_X)>\frac12\,n_Sp,$$

which yields

$$n_S<2\varepsilon\sqrt p. \tag{18}$$

Applying (16) and Lemma 1 once again,

$$2(1-\varepsilon)p > |X| \ge n_X(p+1-n_S) > (1-\varepsilon)n_Xp.$$

This gives $n_X=1$. As a result, by Lemma 1, we have $K_S=p$, meaning that every H-line has a nonempty intersection with S. Hence, averaging and using (16),

$$n_S \le K_S^{-1}|S| < \varepsilon\sqrt{p} \tag{19}$$

(cf. (18)).

We say that a character $\chi\in X$ is *isolated* if its $H^\perp$-line does not contain any other character from X; that is, if $(\chi H^\perp)\cap X=\{\chi\}$. Let N denote the number of isolated characters; in other words, N is the number of $H^\perp$-lines containing exactly one point of X. Since

$$K_X \ge p+1-n_S$$

by Lemma 1, we have

$$|X| \ge N + 2(p+1-n_S-N);$$

consequently,

$$N > 2(p-n_S)-|X|. \tag{20}$$

For an element $g\in G$, let k_g be the number of points of S on the H-line passing through g:

$$k_g = |(S-g)\cap H|;$$

that is, $k_g = |\operatorname{supp}(f\cdot 1_{g+H})|$. By (19), there exists $g_0\in G$ with

$$k_{g_0} < \varepsilon\sqrt{p}. \tag{21}$$

Considering g_0 fixed, for each $g\in G$ we define the function $\Delta_g\in L(G)$ by

$$\Delta_g := f * \big(f\cdot(1_{g+H}-1_{g_0+H})\big),$$

and let $T:=\operatorname{supp}\Delta_g$ and $Y:=\operatorname{supp}\widehat{\Delta_g}$ (thus, T and Y depend on g). We have

$$\widehat{\Delta_g} = \hat f\cdot(\widehat{f\cdot 1_{g+H}} - \widehat{f\cdot 1_{g_0+H}})$$

whence, by (3),

$$\widehat{\Delta_g}(\chi) = p^{-1}\hat f(\chi)\sum_{\psi\in H^\perp}\hat f(\chi\psi)\big(\psi(g)-\psi(g_0)\big), \quad \chi\in\widehat G.$$

It follows that $Y\subseteq X$, and that $\chi\in X\setminus Y$ if and only if

$$\sum_{\psi\in H^\perp}\hat f(\chi\psi)\big(\psi(g)-\psi(g_0)\big)=0. \tag{22}$$

In particular, the N isolated characters are all contained in $X \setminus Y$; therefore, letting $K_Y := |YH^\perp|/|H^\perp|$, by (20) we get

$$K_Y \le p - N < |X| - p + 2n_S \tag{23}$$

and

$$|Y| \le |X| - N < 2(|X| - p + n_S),$$

the latter estimate implying

$$|Y| < \Big(2 - \frac{7}{2}\,\varepsilon\Big)p \tag{24}$$

in view of (16) and (19). On the other hand,

$$|T| \le |\operatorname{supp}(f * (f \cdot 1_{g+H}))| + |\operatorname{supp}(f * (f \cdot 1_{g_0+H}))| \le |S|(k_g + k_{g_0}). \tag{25}$$

We notice that Δ_g vanishes identically if and only if (22) holds true for all characters $\chi \in X$. Assuming that (22) is *wrong* for some character $\chi \in X$ and element $g \in G$ with

$$k_g \le \frac{3}{2}\,\varepsilon\sqrt{p}, \tag{26}$$

so that, in particular, Δ_g does *not* vanish identically, we will now get a contradiction.

To this end, we first observe that substituting (16), (21), and (26) into (25) yields

$$|T| < \frac{5}{2}\,\varepsilon^2 p^2. \tag{27}$$

If Y were situated on a single $H^\perp$-line, then by the assumption that every $H^\perp$-line contains fewer than $\sqrt{|X|} + 1$ elements of X, and in view of $Y \subseteq X$ and (16), we would have $|Y| < \sqrt{2p} + 1$, and then Theorem C and (27) would give

$$p + 1 \le |Y| + \frac{1}{p}\,|T| < \sqrt{2p} + 1 + \frac{5}{2}\,\varepsilon^2 p,$$

contradicting (17). Thus, Y resides on at least two distinct $H^\perp$-lines; that is, $K_Y \ge 2$.

Let

$$n_T := \min\{|(t + H) \cap T| \colon t \in T\} \quad \text{and} \quad n_Y := \min\{|(\chi H^\perp) \cap Y| \colon \chi \in Y\}.$$

By (24) we have

$$n_Y \le |Y|/2 < \Big(1 - \frac{7}{4}\,\varepsilon\Big)p$$

and then, in view of (27) and Lemma 1,

$$\frac{5}{2}\,\varepsilon^2 p^2 > |T| \ge n_T(p + 1 - n_Y) > \frac{7}{4}\,\varepsilon n_T p.$$

It follows that

$$n_T < \frac{3}{2}\varepsilon p,$$

whence

$$K_Y \ge p+1-n_T > \Big(1-\frac{3}{2}\,\varepsilon\Big)p$$

by Lemma 1. Therefore, from (23), (16), and (19), we get

$$\Big(1-\frac{3}{2}\varepsilon\Big)p < K_Y < (1-2\varepsilon)p + 2\varepsilon\sqrt{p},$$

a contradiction.

We therefore conclude that, letting

$$A := \Big\{g \in G\colon k_g \le \frac{3}{2}\,\varepsilon\sqrt{p}\Big\},$$

equality (22) holds true for all characters $\chi \in X$ and elements $g \in A$.

Clearly, the set A is a union of H-lines, and we denote by K_A the number of these lines. By (16), and since $K_S = p$, we have

$$\varepsilon\, p^{3/2} > |S| \ge \frac{3}{2}\,\varepsilon\sqrt{p}\,(p-K_A),$$

resulting in

$$K_A > \frac{1}{3}\,p. \tag{28}$$

Changing the viewpoint, we now fix a character $\chi \in X$ and denote the sum in the left-hand side of (22) by $R(g)$, considering it as a function of g. Observing that the term corresponding to the principal character $\psi = 1$ vanishes and can be dropped from the sum, we see that $|\operatorname{supp}\widehat{R}| \le |\chi H^\perp \cap X|$, and that if χ is not isolated, then R does not vanish identically. On the other hand, we have shown that $R(g)=0$ whenever $g \in A$, and it follows that $|\operatorname{supp} R| \le |G \setminus A| = (p-K_A)p$. Using (1), we conclude that for any nonisolated character $\chi \in X$,

$$|\chi H^\perp \cap X| + (p-K_A) \ge |\operatorname{supp}\widehat{R}| + \frac{1}{p}\,|\operatorname{supp} R| \ge p+1,$$

implying

$$|\chi H^\perp \cap X| > K_A.$$

Recalling (28) and (16), this shows that any $H^\perp$-line determined by X contains, in fact, at least $K_A > \frac{1}{3}\,p > \sqrt{2p}+1 > \sqrt{|X|}+1$ points of X. This, however, contradicts the choice of H at the beginning of the proof. □

9. Proof of Theorem 5

The proof of Theorem 5 is a further elaboration on that of Theorem 4.

In addition to Lemma 3, we need two more lemmas.

Lemma 4. *Suppose that $p \geq 3$ is a prime, and that a set $P \subset \mathbb{F}_p^2$ satisfies $\frac{3p+7}{2} \leq |P| \leq 2p+7$. If P is not contained in a union of two lines, then there is a direction in $\mathbb{F}_p^2$ such that some line in this direction contains at least three points of P, and any line in this direction contains at most $\frac{p+5}{2}$ points of P.*

Proof. We say that a line $l \subset \mathbb{F}_p^2$ is *rich* if $|l \cap P| \geq 3$, and that it is *powerful* if $|l \cap P| \geq \frac{p+7}{2}$. Furthermore, we say that a *direction* in $\mathbb{F}_p^2$ is rich if there is a rich line in this direction. There is at least one rich line: otherwise for any fixed point $x \in P$, each of the $p+1$ lines through x would contain at most one point of P other than x, leading to $|P| \leq p+2$. Aiming at a contradiction, we assume that there is a powerful line in every rich direction.

If we could find four distinct rich directions, then choosing a powerful line in each of them and counting only those points of P lying in the union of these lines, we would get

$$|P| \geq 4 \cdot \frac{p+7}{2} - \binom{4}{2} = 2p+8,$$

a contradiction. This shows that there are at most three rich directions and, consequently, at most three rich lines trough any point of P.

Let l be a powerful line. If there is yet another powerful line, say l', which is parallel to l, then we fix a point $x \in P \setminus (l \cup l')$ and with every point $g \in l$ associate the point $g' \in l'$ such that g, g' and x are collinear. By the pigeonhole principle, there are at least $2 \cdot \frac{p+7}{2} - p = 7$ pairs $(g, g') \in l \times l'$ such that both g and g' belong to P; this shows that there are at least seven rich lines through x, which, as we saw above, is impossible. A similar argument applies if there is a powerful line l' which is not parallel to l, except that in this case the intersection point of l and l' gets associated to itself, and there is a unique point on l not associated to any point of l', and a unique point on l' not associated to any point of l; this results in at least $2\left(\frac{p+7}{2} - 2\right) - (p-2) = 5$ pairs $(g, g') \in l \times l'$ with $g \neq g'$ and $g, g' \in P$, and hence to at least five rich lines through x, a contradiction.

We thus conclude that there is a unique powerful line l and, consequently, a unique rich direction. Fix a point $x \in P \setminus l$. The line through x parallel to l is not powerful; therefore, contains at most $\frac{p+5}{2}$ points of P, including x itself. Any other line through x has the direction other than that of l, and therefore is not rich; as a result, contains at most one point of P other than x. This shows that

$$|P| \leq \frac{p+5}{2} + p < \frac{3p+7}{2},$$

a contradiction. □

Lemma 5. *Suppose that p is a prime, $h \in L(\mathbb{F}_p)$ is a nonzero function, and $A \subseteq \mathbb{F}_p$ is a set with $|A| > \frac{2}{3}p$. If for any $a_1, \ldots, a_4 \in A$ such that $a_1 + a_2 = a_3 + a_4$ we have $h(a_1)h(a_2) = h(a_3)h(a_4)$, then either $|\operatorname{supp} \hat{h}| = 1$, or $|\operatorname{supp} \hat{h}| \geq |A|$.*

Proof. If h vanishes on the whole set A, then $|\operatorname{supp} h| \le p-|A|$, whence $|\operatorname{supp} \hat{h}| \ge |A|+1$ by Theorem B. Suppose thus that the set $A_1 := A \cap \operatorname{supp} h$ is nonempty, and let $A_0 := A \setminus A_1$. If A_0 is nonempty either, then $|A_0 - A_1| \ge |A_0| + |A_1| - 1 = |A| - 1$ by the well-known Cauchy-Davenport theorem; consequently, $|A_0 - A_1| + |A| \ge 2|A| - 1 > p$, and the pigeonhole principle gives $A_0 - A_1 + A = \mathbb{F}_p$. Hence, for any $a \in A$ there exist $a_0 \in A_0$, $a_1 \in A_1$, and $a' \in A$ with $a_0 + a' = a_1 + a$, implying $h(a) = h(a_0)h(a')/h(a_1) = 0$. This contradicts the assumption that h does not vanish on the whole set A, and thus shows that A_0 is empty; that is, $A \subseteq \operatorname{supp} h$.

Since $|A| > \frac{1}{2}\,p$, every element $g \in \mathbb{F}_p$ can be represented as $g = a_1 - a_2$ with $a_1, a_2 \in A$, and we let $\chi(g) := h(a_1)/h(a_2)$; notice that this definition is legitimate as for any other representation $g = a_1' - a_2'$ with $a_1', a_2' \in A$ we have $h(a_1')/h(a_2') = h(a_1)/h(a_2)$. We now claim that $\chi(g_1 - g_2) = \chi(g_1)/\chi(g_2)$ for any $g_1, g_2 \in \mathbb{F}_p$. To see this, we notice that the intersection $(A - g_1) \cap (A - g_2) \cap A$ is nonempty by the pigeonhole principle, and find $a_1, a_2, a \in A$ with $a_1 - g_1 = a_2 - g_2 = a$; this gives

$$g_1 = a_1 - a,\ \ g_2 = a_2 - a,\ \ g_1 - g_2 = a_1 - a_2,$$

as a result of which

$$\chi(g_1 - g_2) = h(a_1)/h(a_2) = \chi(g_1)/\chi(g_2).$$

We conclude that χ is a character of the group $\mathbb{F}_p$. Moreover,

$$\chi(a_1 - a_2) = h(a_1)/h(a_2),\ \ a_1, a_2 \in A$$

shows that $h\overline{\chi}$ is constant on A; that is, there exists a nonzero $C \in \mathbb{C}$ such that $h(a) = C\chi(a)$ for any $a \in A$. Consequently, the difference function $\Delta := h - C\chi$ is supported outside of A. Hence, either it is identically zero, or $|\operatorname{supp} \widehat{\Delta}| \ge p + 1 - (p - |A|) = |A| + 1$ by Theorem B, in which case $|\operatorname{supp} \hat{h}| \ge |A|$. □

Proof of Theorem 5. We assume, without loss of generality, that $|X| \le |S|$, and then for a contradiction that

$$|X| < 3(1-\varepsilon)p \quad \text{and} \quad |S| < \frac{1}{6}\,\varepsilon p^{4/3}, \tag{29}$$

while X is not contained in a union of two lines.

If we had $\varepsilon^3 \le 216p^{-1}$, then (29) would give $|X| \le |S| < p$, contradicting Theorem A; hence $\varepsilon^3 > 216p^{-1}$, implying $p > 216$.

If we had $|X| \le \frac{3p+5}{2}$, then Theorem 4 would result in

$$|S| \ge \frac{\sqrt{p}}{2}\left(2p - \frac{3p+5}{2}\right) = \frac{1}{4}\,(p-5)\sqrt{p} > \frac{1}{6}\,\varepsilon p^{4/3},$$

contradicting (29). Thus,

$$|X| \ge \frac{3p+7}{2}; \tag{30}$$

combining this with (29), we get

$$\frac{3}{2}\,p < |X| < 3(1-\varepsilon)p,$$

and it follows that $\varepsilon < 1/2$. The inequalities

$$\frac{216}{p} < \varepsilon^3 < \frac{1}{8}$$

are tacitly used in the computations below.

Recalling (30) and applying Lemma 4 if $|X| \le 2p$, and Lemma 3 if $2p < |X| < 3p$, and observing that if $|X| > 2p$, then there is a line in every given direction containing at least three points of X, we conclude that there is a nonzero, proper subgroup $H < G$ such that every $H^\perp$-line contains at most

$$\max\left\{\frac{p+5}{2}, \sqrt{3p}+\frac{3}{2}\right\} = \frac{p+5}{2}$$

points of X, while there is an $H^\perp$-line containing at least three points of X. Throughout the proof, we consider this subgroup H fixed, and define n_S, n_X, K_S, K_X by (5) and (6).

From (29) and the assumption that X is not contained in a union of two lines, we get

$$n_X \le \frac{1}{3}\,|X| < \ (1-\varepsilon)p,$$

whence, by (29) and Lemma 1,

$$\frac{1}{6}\,\varepsilon p^{4/3} > |S| \ge n_S(p+1-n_X) > \varepsilon n_S p;$$

consequently,

$$n_S < \frac{1}{6}\,p^{1/3}.$$

Applying (29) and Lemma 1 once again,

$$3\,(1-\varepsilon)p > |X| \ge n_X(p+1-n_S) > n_X\Big(p - \frac{1}{6}\,p^{1/3}\Big) > (1-\varepsilon)n_X p.$$

This gives $n_X \le 2$. As a result, by Lemma 1, we have $K_S \ge p-1$. Hence, averaging and using (29),

$$n_S \le K_S^{-1}|S| < \frac{\varepsilon}{6}\,\frac{p^{4/3}}{p-1}. \tag{31}$$

Denoting by N the number of $H^\perp$-lines containing exactly one or exactly two points of X, we have by Lemma 1

$$|X| \ge N + 3(K_X - N) \ge N + 3(p+1-n_S-N),$$

whence

$$2N > 3(p-n_S) - |X|. \tag{32}$$

Fix an element $\gamma \in G \setminus H$, and consider the functions

$$F_g := f \cdot (1_{g+\gamma+H} - 1_{g+H}), \quad g \in G.$$

By (3), we have

$$\widehat{F_g}(\chi) = \frac{1}{p} \sum_{\psi \in H^\perp} \hat{f}(\chi\psi)(\psi(\gamma) - 1)\psi(g), \ \chi \in \widehat{G}. \tag{33}$$

In the case where the $H^\perp$-line through a character $\chi \in X$ contains exactly one more character of X, say $\chi\psi$ with some $\psi \in H^\perp$, this gives

$$\widehat{F_g}(\chi) = \frac{1}{p} \hat{f}(\chi\psi)(\psi(\gamma) - 1)\psi(g);$$

it follows that if $g_1, g_2, g_3, g_4 \in G$ satisfy

$$g_1 + g_2 = g_3 + g_4, \tag{34}$$

then

$$\widehat{F_{g_1}}(\chi)\widehat{F_{g_2}}(\chi) - \widehat{F_{g_3}}(\chi)\widehat{F_{g_4}}(\chi) = 0.$$

This conclusion stays true also if the $H^\perp$-line through χ does not contain any points of X other than χ, as in this case, by (33), we have $\widehat{F_{g_i}}(\chi) = 0$ for each $i \in [1, 4]$.

For a quadruple $\mathbf{g} = (g_1, g_2, g_3, g_4) \in G^4$ satisfying (34), let

$$\Delta_{\mathbf{g}} := f * (F_{g_1} * F_{g_2} - F_{g_3} * F_{g_4});$$

thus,

$$\widehat{\Delta_{\mathbf{g}}}(\chi) = \hat{f}(\chi) \left(\widehat{F_{g_1}}(\chi)\widehat{F_{g_2}}(\chi) - \widehat{F_{g_3}}(\chi)\widehat{F_{g_4}}(\chi)\right), \quad \chi \in \widehat{G}. \tag{35}$$

Write

$$T := \operatorname{supp} \Delta_{\mathbf{g}}, \ Y := \operatorname{supp} \widehat{\Delta_{\mathbf{g}}},$$
$$n_T := \min\{|(t + H) \cap T| \colon t \in T\}, \ n_Y := \min\{|(\chi H^\perp) \cap Y| \colon \chi \in Y\},$$
$$K_T := |T + H|/|H|, \ K_Y := |Y H^\perp|/|H^\perp|.$$

By (35), we have $Y \subseteq X$, and we have shown above that $\widehat{\Delta_{\mathbf{g}}}(\chi) = 0$ for any character $\chi \in X$ with $|\chi H^\perp \cap X| \le 2$. Along with (29), (32), and (31), this gives

$$2K_Y \le 2p - 2N < |X| - p + 3n_S < 2\Big(1 - \frac{5}{4}\,\varepsilon\Big)p,$$

implying

$$n_T \ge p + 1 - K_Y > \frac{5}{4}\,\varepsilon p \tag{36}$$

in view of Lemma 1. On the other hand, letting

$$k_g = |(S - g) \cap H|$$

(so that $k_g = |\operatorname{supp}(f \cdot 1_{g+H})|$) we have

$$|T| \le |S|\big((k_{g_1} + k_{g_1+\gamma})(k_{g_2} + k_{g_2+\gamma}) + (k_{g_3} + k_{g_3+\gamma})(k_{g_4} + k_{g_4+\gamma})\big). \tag{37}$$

Suppose that $\Delta_{\mathbf{g}} \ne 0$. By the assumption that every $H^\perp$-line contains at most $\frac{p+5}{2}$ points of X, and since $Y \subseteq X$, we have

$$n_Y \le \frac{p+5}{2}$$

and then, by Lemma 1 and (36),

$$|T| \ge n_T(p+1-n_Y) > \frac{5}{4}\,\varepsilon p \cdot \frac{p-3}{2} > \frac{1}{2}\,\varepsilon p^2.$$

Comparing this with (37), we obtain

$$|S|\big((k_{g_1} + k_{g_1+\gamma})(k_{g_2} + k_{g_2+\gamma}) + (k_{g_3} + k_{g_3+\gamma})(k_{g_4} + k_{g_4+\gamma})\big) > \frac{1}{2}\,\varepsilon p^2, \tag{38}$$

provided that $\mathbf{g} = (g_1, \dots, g_4) \in G^4$ satisfies (34), and $\Delta_{\mathbf{g}} \ne 0$.

Let $\Gamma < G$ be the subgroup generated by γ. We have

$$\sum_{g\in\Gamma}(k_g + k_{g+\gamma}) = 2\sum_{g\in\Gamma}|S \cap (g+H)| = 2|S|;$$

as a result, denoting by A the set of all those $g \in \Gamma$ with $k_g + k_{g+\gamma} < 6|S|/p$, we have $|A| > \frac{2}{3}\,p$. Moreover, as it follows from (38) and (29), if $\mathbf{g} = (g_1, \dots, g_4) \in A^4$ satisfies (34), and $\Delta_{\mathbf{g}} \ne 0$, then

$$\frac{1}{2}\,\varepsilon p^2 < 72|S|^3 p^{-2} < 72 \cdot \frac{1}{216}\,\varepsilon^3 p^2,$$

a contradiction.

We conclude that for any $\mathbf{g} \in A^4$ satisfying (34), we have $\Delta_{\mathbf{g}} = 0$; that is, by (35),

$$\widehat{F_{g_1}}(\chi)\widehat{F_{g_2}}(\chi) = \widehat{F_{g_3}}(\chi)\widehat{F_{g_4}}(\chi), \quad \chi \in X.$$

For every character $\chi \in X$ we now consider the function $h_\chi \in L(\Gamma)$ defined by

$$h_\chi(g) := \widehat{F_g}(\chi),\ g \in \Gamma.$$

Identifying $H^\perp$ with the character group $\widehat{\Gamma}$, in view of (33) we have $|\operatorname{supp}\widehat{h_\chi}| = \kappa_\chi - 1$, where $\kappa_\chi = |\chi H^\perp \cap X|$ is the number of points of X on the $H^\perp$-line through χ. Applying Lemma 5 we derive that either $\kappa_\chi \le 2$, or $\kappa_\chi \ge |A| + 1 > \frac{2}{3}\,p > \frac{p+5}{2}$, for any character $\chi \in X$. This, however, contradicts the choice of H at the beginning of the proof. □

Appendix: Classifying the exceptions

In this section we prove Lemmas 6–9 classifying the exceptional cases of Theorems 1–5, and also prove Corollary 1.

Recall, that for a subgroup H of a finite abelian group G, a function $f \in L(G)$ is called *H-periodic* if $f(g+h)=f(g)$ for any $g \in G$ and $h \in H$. A set $S \subseteq G$ is H-periodic if its indicator function 1_S is H-periodic; that is, $g \in S$ if and only if $g+h \in S$, for any $g \in G$ and $h \in H$. Equivalently, a function f is H-periodic if it is constant on H-cosets, and a set S is H-periodic if it is a union of H-cosets.

Lemma 6. *Suppose that H is a subgroup of a finite abelian group G, and $f \in L(G)$.*

i) *We have* $\operatorname{supp} f \subseteq H$ *if and only if $\hat f$ is $H^\perp$-periodic. Also, if* $\operatorname{supp} f \subseteq g+H$ *for some $g \in G$, then* $\operatorname{supp} \hat f$ *is $H^\perp$-periodic.*

ii) *We have* $\operatorname{supp} \hat f \subseteq H^\perp$ *if and only if f is H-periodic. Also, if* $\operatorname{supp} \hat f \subseteq \chi H^\perp$ *for some $\chi \in \widehat G$, then* $\operatorname{supp} f$ *is H-periodic.*

We omit the straightforward verification.

Lemma 7. *Suppose that H is a subgroup, g is an element, and $\chi \in \widehat G$ is a character of a finite abelian group G, and that $f \in L(G)$ is a nonzero function.*

i) *If* $\operatorname{supp} f \subseteq g+H$ *and* $\operatorname{supp} \hat f = \chi_1 H^\perp \cup \dots \cup \chi_k H^\perp$ *where $\chi_1,\dots,\chi_k \in \widehat G$ and the union is disjoint (cf. Lemma 6), then there are nonzero coefficients $c_1,\dots,c_k \in \mathbb C$ such that*
$$f(z)=\begin{cases} c_1\chi_1(z)+\dots+c_k\chi_k(z) & \text{if } z \in g+H,\\ 0 & \text{if } z \notin g+H.\end{cases}$$

ii) *If* $\operatorname{supp} \hat f \subseteq \chi H^\perp$ *and* $\operatorname{supp} f = (g_1+H)\cup\dots\cup(g_k+H)$ *where $g_1,\dots,g_k \in G$ and the union is disjoint (cf. Lemma 6), then there are nonzero coefficients $c_1,\dots,c_k \in \mathbb C$ such that*
$$f(z)=\begin{cases} c_i\chi(z) & \text{if } z \in g_i+H,\ i\in[1,k],\\ 0 & \text{if } z \notin (g_1+H)\cup\dots\cup(g_k+H).\end{cases}$$

Proof. For the first part of the lemma we notice that for any $z \in g+H$, by the inversion formula we have
$$f(z)=\sum_{i=1}^k \sum_{\psi\in H^\perp} \hat f(\chi_i\psi)\chi_i(z)\psi(z)=\sum_{i=1}^k c_i\chi_i(z)$$
where, by (3) and in view of $f\cdot 1_{g+H}=f$,
$$c_i=\sum_{\psi\in H^\perp}\hat f(\chi_i\psi)\psi(g)=|H^\perp|\widehat{f\cdot 1_{g+H}}(\chi_i)=|H^\perp|\hat f(\chi_i)\neq 0.$$

This proves the first assertion.

Turning to the second assertion, we observe that the inversion formula gives

$$f(z)=\sum_{\psi\in H^\perp}\hat f(\chi\psi)\chi(z)\psi(z),\ z\in G.$$

It follows that the function $\overline{\chi}f$ is H-periodic, and since $\operatorname{supp}\overline{\chi}f=\operatorname{supp}f$, this function is constant and nonzero on each coset $g_i+H,\ i\in[1,k]$. Denoting by c_i its values on the corresponding cosets completes the proof. □

Lemma 8. *Suppose that G is a finite abelian group, $H<G$ is a proper, prime subgroup, and $\chi_1,\chi_2\in\widehat{G}$ are characters with $\chi_2H^\perp\neq\chi_1H^\perp$. For a function $f\in L(G)$, we have $\operatorname{supp}\hat f\subseteq\chi_1H^\perp\cup\chi_2H^\perp$ if and only if there are H-periodic functions $f_1,f_2\in L(G)$ such that*

$$f(g)=\chi_1(g)f_1(g)+\chi_2(g)f_2(g),\ g\in G.$$

Moreover, writing in this case $N:=|\operatorname{supp}f_1\cup\operatorname{supp}f_2|$, we have

$$\left(1-\frac{1}{|H|}\right)N\le|\operatorname{supp}f|\le N.$$

Proof. By the inversion formula, if $\operatorname{supp}\hat f\subseteq\chi_1H^\perp\cup\chi_2H^\perp$, then for any $g\in G$ we have

$$f(g)=\chi_1(g)\sum_{\psi\in H^\perp}\hat f(\chi_1\psi)\psi(g)+\chi_2(g)\sum_{\psi\in H^\perp}\hat f(\chi_2\psi)\psi(g),$$

and the existence of the functions f_1,f_2 follows by observing that the two sums in the right-hand side depend on the coset $g+H$ only. Conversely, it is easily seen that if f is of the indicated form, then $\operatorname{supp}\hat f\subseteq\chi_1H^\perp\cup\chi_2H^\perp$.

Furthermore, the estimate $|\operatorname{supp}f|\le N$ is immediate. For the remaining estimate $|\operatorname{supp}f|\ge\left(1-|H|^{-1}\right)N$, we notice that if, for some $g\in G$, at least one of $f_1(g)$ and $f_2(g)$ is nonzero, then all but at most one element of the coset $g+H$ lie in $\operatorname{supp}f$, as it follows from the nonsingularity of the matrices

$$\begin{pmatrix}\chi_1(g_1)&\chi_2(g_1)\\ \chi_1(g_2)&\chi_2(g_2)\end{pmatrix},\qquad g_1,g_2\in g+H,\ g_1\neq g_2$$

(this is where primality of H is required). □

Lemma 9. *Suppose that $G=H_1\oplus H_2$ is a decomposition of the finite abelian group G into a direct sum of nonzero subgroups $H_1,H_2<G$, and let $f\in L(G)$. For $\operatorname{supp}\hat f$ to be contained in a union of a coset of $H_1^\perp$ and a coset of $H_2^\perp$, it is necessary and sufficient that there existed functions $f_1\in L(H_1)$ and $f_2\in L(H_2)$ and a character $\chi\in\widehat{G}$ such that*

$$f(h_1+h_2)=\chi(h_1+h_2)\big(f_1(h_1)+f_2(h_2)\big),\quad h_1\in H_1,h_2\in H_2.$$

Moreover, if in this case $|\operatorname{supp} f| < \frac{1}{2}|G|$, *then the functions* f_1, f_2 *can be so chosen that*

$$|\operatorname{supp} f| \le |H_1||\operatorname{supp} f_2| + |H_2||\operatorname{supp} f_1| \le \left(1 + \frac{2|\operatorname{supp} f|}{|G|}\right)|\operatorname{supp} f|.$$

Proof. Sufficiency is easy to verify. For the necessity, let χ be the character lying in both cosets on which $\hat{f}$ is supported. By the inversion formula, for any $h_1 \in H_1$ and $h_2 \in H_2$ we have

$$\begin{aligned} f(h_1+h_2) &= \sum_{\psi \in H_1^\perp} \hat{f}(\chi\psi)\,\chi\psi(h_1+h_2) + \sum_{\substack{\psi \in H_2^\perp \\ \psi \ne 1}} \hat{f}(\chi\psi)\,\chi\psi(h_1+h_2) \\ &= \chi(h_1+h_2) \sum_{\psi \in H_1^\perp} \hat{f}(\chi\psi)\psi(h_2) + \chi(h_1+h_2) \sum_{\substack{\psi \in H_2^\perp \\ \psi \ne 1}} \hat{f}(\chi\psi)\psi(h_1), \end{aligned}$$

and we let

$$f_1(h_1) := \sum_{\substack{\psi \in H_2^\perp \\ \psi \ne 1}} \hat{f}(\chi\psi)\psi(h_1),\ h_1 \in H_1$$

and

$$f_2(h_2) := \sum_{\psi \in H_1^\perp} \hat{f}(\chi\psi)\psi(h_2),\ h_2 \in H_2.$$

Turning to the second assertion, the inequality

$$|\operatorname{supp} f| \le |H_2||\operatorname{supp} f_1| + |H_1||\operatorname{supp} f_2|$$

is immediate (if $h_1 + h_2 \in \operatorname{supp} f$, where $h_1 \in H_1,\ h_2 \in H_2$, then either $h_1 \in \operatorname{supp} f_1$, or $h_2 \in \operatorname{supp} f_2$), and we proceed to prove the remaining inequality. We write for brevity $S := \operatorname{supp} f$ and $Z := G \setminus S$, and assume that $|Z| > \frac{1}{2}|G|$. For $j \in \{1,2\}$ let

$$I_j := \operatorname{Im}(f_j) \text{ and } \nu_j(z) := |\{h \in H_j \colon f_j(h) = z\},\ z \in \mathbb{C}.$$

Having f_1 and f_2 suitably translated, we further assume that

$$\nu_1(0) = \max\{\nu_1(z) \colon z \in I_1\},$$

and we choose $z_0 \in I_2$ with

$$\nu_2(z_0) = \max\{\nu_2(z) \colon z \in I_2\}$$

and write $m_1 := \nu_1(0)$ and $m_2 := \nu_2(z_0)$.

From

$$\frac{1}{2}|G| < |Z| = \sum_{z \in I_1 \cap (-I_2)} \nu_1(z)\nu_2(-z) \le m_1 \sum_{z \in I_2} \nu_2(z) = m_1|H_2|$$

we conclude that $m_1 > \frac{1}{2}\,|H_1|$, and similarly $m_2 > \frac{1}{2}\,|H_2|$. Consequently, if we had $z_0 \neq 0$, this would imply

$$\begin{aligned}\frac{1}{2}\,|G| &< |Z| \\ &\le m_1(|H_2| - m_2) + (|H_1| - m_1)m_2 \\ &= m_1|H_2| - (2m_1 - |H_1|)m_2 \\ &< m_1|H_2| - (2m_1 - |H_1|) \cdot \frac{1}{2}\,|H_2| \\ &= \frac{1}{2}\,|G|,\end{aligned}$$

a contradiction. Thus, $z_0 = 0$; as a result, writing $n_j := |H_j| - m_j$ and observing that $n_j < \frac{1}{2}\,|H_j|$ $(j \in \{1,2\})$ we get

$$\begin{aligned}|S| &\ge m_1(|H_2| - m_2) + (|H_1| - m_1)m_2 \\ &= n_1|H_2| + n_2|H_1| - 2n_1n_2 \\ &\ge \max\{n_1|H_2|, n_2|H_1|\}.\end{aligned}$$

Hence, $n_1n_2 \le |S|^2/|G|$, which further leads to

$$n_1|H_2| + n_2|H_1| \le |S| + 2n_1n_2 \le |S| + \frac{2|S|^2}{|G|}.$$

It remains to notice that $n_j = |\operatorname{supp} f_j|,\ j \in \{1,2\}$. □

Finally, we prove Corollary 1.

Proof of Corollary 1. Without loss of generality we assume that $3 \le |X| \le |S|$, and that we are not in the exceptional situation where X is a coset of a nonzero subgroup of the corresponding group, possibly with one element missing, and S is either a coset, or a union of two cosets of the orthogonal subgroup. Also, we assume that $|S| \le p^2 - 2p$ as otherwise the assertion follows in view of $|X| \ge 3$.

If $|S| \le 2p - 1$, then we use Theorem 2 to get $\frac{1}{p-1}\,|X| + \frac{1}{2}\,|S| \ge p + 1$; this gives

$$|S||X| \ge \frac{1}{2}\,(p-1)|S|(2p + 2 - |S|) \ge \frac{1}{2}\,(p-1) \cdot 3(2p-1) > 3p(p-2).$$

If $2p \le |S| \le 3p - 1$, then we apply Theorem 3 to get either $\frac{1}{p-2}\,|X| + \frac{1}{3}\,|S| \ge p + 1$, or $|X| \ge \frac{3}{2}(p-1)$. In the former case

$$|S||X| \ge \frac{1}{3}(p-2)|S|(3p + 3 - |S|) \ge \frac{4}{3}\,(p-2)(3p-1) > 3p(p-2),$$

in the latter case $|S||X| \ge 3p(p-1) > 3p(p-2)$.

Finally, if $|S| \geq 3p$, then using Theorem C and the assumption $|S| \leq p^2 - 2p$ we get

$$|S||X| \geq \frac{1}{p}\,|S|\left(p^2+p-|S|\right) \geq 3p(p-2).$$

□

Acknowledgement

We are grateful to Miki Simonovits for his kind assistance with the illustrations.

References

[1] N. Alon, Tools from higher algebra, in: *Handbook of combinatorics* Vol. 1, 2, 1749–1783, Elsevier Sci. B. V., Amsterdam, 1995.

[2] A. Biró, 1998 Schweitzer competition (Problem 3), *http://www.math.u-szeged.hu/˜mmaroti/schweitzer/schweitzer-1998.pdf.*

[3] A. Bishnoi, P.L. Clark, A. Potukuchi and J.R. Schmitt, On zeros of a polynomial in a finite grid, *Combinatorics, Probability and Computing* **27** (3) (2018), 310–333.

[4] A.E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Comb. Theory, Ser. A* **24** (2) (1978), 251–253.

[5] D.L. Donoho, P.B. Stark Uncertainty principles and signal recovery, *SIAM J. Appl. Math.* **49** (1989), 906–931.

[6] R.E. Jamison, Covering finite fields with cosets of subspaces, *J. Comb. Theory, Ser. A* **22** (3) (1977), 253–266.

[7] R. Meshulam, An uncertainty inequality for finite abelian groups, *European J. Comb.* **27** (2006), 63–67.

[8] K.T. Smith, The uncertainty principle on groups, *SIAM J. Appl. Math.* **50** (1989), 876–882.

[9] T. Szőnyi, Around Rédei's theorem, Combinatorics (Assisi, 1996), *Discrete Math.* **208/209** (1999), 557–575.

[10] T. Tao, An uncertainty principle for cyclic groups of prime order, *Mathematical Research Letters* **12** (2005), 121–127.

[11] A. Terras, *Fourier Analysis on Finite Groups and Applications,* Cambridge University Press, Cambridge, 1999.

E-mail address: biro.andras@renyi.mta.hu

A. Rényi Institute of Mathematics, Hungarian Academy of Sciences, 1053 Budapest, Reáltanoda u. 13–15, Hungary

E-mail address: seva@math.haifa.ac.il

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel