Sumsets in quadratic residues *

Shkredov I.D.

Annotation.

We describe all sets $A \subseteq \mathbb{F}_p$ which represent the quadratic residues $R \subseteq \mathbb{F}_p$ as $R = A + A$ and $R = A^+A$. Also, we consider the case of an approximate equality $R \approx A + A$ and $R \approx A^+A$ and prove that $A$ has a structure in the situation.

1. Introduction

Let $p$ be a prime number, $\mathbb{F}_p$ be the finite field, and $R$ be a the set of all quadratic residues. In other words, $R$ is the set of all squares in $\mathbb{F}_p \setminus \{0\}$. There are many interesting conjectures about the set $R$ (see e.g. [6, 14, 16]). We begin with a hypothesis of A. Sárközy [16].

Conjecture A. The set $R$ cannot be represented as a sumset $R = A + B$, where the cardinality of each set $A, B$ is at least 2.

Here, as usual,

$$A + B := \{a + b : a \in A, b \in B\}.$$ 

In the paper we will also need in another definition. For a set $A$ put

$$A^+A := \{a + a' : a, a' \in A, a \neq a'\}.$$ 

In [16] the following result was obtained (see also [17]).

Theorem 1.1 Let $p$ be a prime number. Suppose that $R = A + B$, $|A|, |B| \geq 2$. Then

$$\frac{p^{1/2}}{3 \log p} < |A|, |B| < p^{1/2} \log p.$$ 

Some generalizations and improvements of Theorem 1.1 can be found in [17, 21].

Another well–known conjecture (see e.g. [6]) asks, in particular, the following.

Conjecture B. Let $\varepsilon \in (0, 1)$ be a real number and $p$ be a sufficiently large prime number. Suppose that $A + A \subseteq R$ or $A - A \subseteq R \cup \{0\}$. Then $|A| \ll p^{\varepsilon}$.

Some results in the direction can be found in [1, 5, 9]. At the moment the best known bound has the form $|A| \ll \sqrt{p}$, see e.g. [1]. A lower bound for the case $A - A \subseteq R \cup \{0\}$ is due to S. Graham and C. Ringrose [9]. It asserts us that $|A| \gg \log p \cdot \log \log \log p$ for infinitely many primes $p$. A uniform lower bound of the form $|A| \geq (\frac{1}{2} + o(1)) \log p$, where $p$ is an

*This work was supported by grant RFFI NN 11-01-00759, Russian Government project 11.G34.31.0053, Federal Program ”Scientific and scientific–pedagogical staff of innovative Russia” 2009–2013, grant mol_a_yed 12–01–33080 and grant Leading Scientific Schools N 2519.2012.1.
arbitrary prime, can be found in [5]. Conjecture B can be reformulated in terms of the clique number of the Paley graph $P_n$, see e.g. [3].

Exponential sums with multiplicative characters over sumsets have been studied by various authors (see e.g. [4], [7], [8], [12], [13], [14]). The classical general result of [7], [8] states

$$\sigma(A, B) := \left| \sum_{x,y} \chi(x+y)B(x)A(y) \right| \leq \sqrt{|A||B|}$$

(1)

for any sets $A, B \subseteq \mathbb{F}_p$, and an arbitrary non principal multiplicative character $\chi$. The bound is nontrivial if $|A||B| > p^{1+\delta}$, $\delta > 0$. A.A. Karatsuba and M.–C. Chang to contribute significantly in to the theory of such exponential sums. For example, Karatsuba proved a non–trivial upper bound for the sum $\sigma(A, B)$ provided by $|A| > p^{s_1}, |B| > p^{1/2+s_2}, s_1, s_2 > 0$. Chang obtained plenty results for specific $A$ and $B$, e.g. $A$ has small sumset or, conversely, $A$ is a well–spaced set (see [4] for details). In his survey [14] Karatsuba formulated a hypothesis (see Problem 6).

**Conjecture C.** Let $A, B \subseteq \mathbb{F}_p$, $|A|, |B| \sim \sqrt{p}$. Then

$$\left| \sum_{x,y} \chi(x+y)B(x)A(y) \right| \leq c(\delta)|A||B|p^{-\delta}, \quad \delta > 0.$$  

(2)

The last hypothesis in the section which again is called Paley graph conjecture (see e.g. [4]) predicts a non–trivial upper bound for the sum (1) for $|A|, |B| > p^\varepsilon, \varepsilon > 0$.

**Conjecture D.** Let $A, B \subseteq \mathbb{F}_p$, $|A|, |B| > p^\varepsilon, \varepsilon > 0$. Then

$$\left| \sum_{x,y} \chi(x+y)B(x)A(y) \right| \leq c(\varepsilon)|A||B|p^{-\delta}, \quad \delta = \delta(\varepsilon) > 0.$$  

(3)

Clearly, Conjecture D is the strongest one and implies all another. Trivially, Conjecture A follows from Conjectures B or Conjecture C. It is known that the correspondent functional version of Conjecture C is false, see e.g. section 5. In the paper we give partial answer on Conjecture A. Let us formulate our main result.

**Theorem 1.2** Let $p$ be a prime number, $R \subseteq \mathbb{F}_p$ be the set of quadratic residues and $A \subseteq \mathbb{F}_p$ be a set.

1) If $A + A = R$ then $p = 3$ and $A = \{2\}$.

2) If $A \hat{+} A = R$ then $p = 3, 7, 13$ and there are just four possibilities for $A$, see Example 4.1.

Also, we improve a little bit Theorem 1.1 as well as consider the cases of approximate equalities, in some sense, that is $A + A \approx R$ and $A \hat{+} A \approx R$, see sections 3, 4. Note that an improvement of Sárközy’s theorem was obtained independently by I. Shparlinski in [21] using Karatsuba’s bound from [13]. As for Conjecture B, we reprove a recent result of C. Bachoc, M. Matolcs, I.Z. Rusza [1] in the direction. Interestingly, our method does not use the main lemma of paper [1].

In their proof the authors [16, 17, 21] used the well–known Weil bound for exponential sums with multiplicative characters (see e.g. [11])

$$\left| \sum_{x} \chi(x)\chi(x+x_1)\cdots\chi(x+x_d) \right| \leq (d-1)\sqrt{p}$$  

(4)
for different nonzero \( x_1, \ldots, x_d \in \mathbb{F}_p \) and any non principal character \( \chi \), as well as some combinatorial tools. Our main idea exploit the fact that quadratic residues are "more random then a random set" and, hence, structured. The last statement is the most transparent at the case \( p \equiv 3 \pmod{4} \) (or, equivalently, \( (-1)^p = -1 \), in terms of Legendre symbol). It is known that \( R \) is a perfect difference set (see e.g. Lemma 2.8 from section 2) in the situation, that is the number of solutions \( x = a - b \) with \( a, b \in R \) does not depend on \( x \neq 0 \). Of course a random set of density 1/2 satisfies the property with probability zero. So, because of we use such properties of \( R \) instead of its random behavior it is very natural that perfect difference sets appear in our proofs. For example, all sets \( A \) from the second part of Theorem 1.2 turn out to be perfect difference sets.

The author is grateful to S. Yekhanin for very useful discussions and S. Konyagin for intense interest to the paper.

2. Notation and auxiliary results

We start with definitions and notation used in the paper. Let \( G \) be a finite abelian group. It is well–known [15] that the dual group \( \hat{G} \) is isomorphic to \( G \) in the case. Let \( f \) be a function from \( G \) to \( \mathbb{C} \). We denote the Fourier transform of \( f \) by \( \hat{f} \),

\[
\hat{f}(\xi) = \sum_{x \in G} f(x) e(-\xi \cdot x),
\]

where \( e(x) = e^{2\pi i x} \). We rely on the following basic identities

\[
\sum_{x \in G} f(x) \overline{f}(x) = \frac{1}{|G|} \sum_{\xi \in \hat{G}} \overline{\hat{f}}(\xi) \overline{\hat{g}}(\xi).
\]

\[
\sum_{y \in G} \left| \sum_{x \in G} f(x) g(y - x) \right|^2 = \frac{1}{|G|} \sum_{\xi \in \hat{G}} |\hat{f}(\xi)|^2 |\hat{g}(\xi)|^2.
\]

If

\[
(f \ast g)(x) := \sum_{y \in G} f(y) g(x - y) \quad \text{and} \quad (f \circ g)(x) := \sum_{y \in G} f(y) g(y + x) = (g \circ f)(-x)
\]

then

\[
\hat{f} \ast \hat{g} = \hat{f \circ g} \quad \text{and} \quad \hat{f} \circ \hat{g} = \hat{f} \ast \hat{g}.
\]

Note also that

\[
(f \ast g)(x) = (f \circ g)(x) = (f \circ g)(-x) \quad \text{and} \quad (f \circ g)(x) = (f \ast g)(x) = (f \ast g)(-x),
\]

where for a function \( f : G \rightarrow \mathbb{C} \) we put \( f^c(x) := f(-x) \). Clearly, \((f \ast g)(x) = (g \ast f)(x), x \in G.\) By \( \langle f, g \rangle \) denote the scalar product of two complex functions \( f \) and \( g \). Put \( \langle f \rangle = \langle f, 1 \rangle \), where 1 is the constant function on \( G \). We will write \( \sum_x \) and \( \sum_\xi \) instead of \( \sum_{x \in G} \) and \( \sum_{\xi \in \hat{G}} \) for simplicity.

We use in the paper the same letter to denote a set \( S \subseteq G \) and its characteristic function \( \mathbb{1}_S : G \rightarrow \{0, 1\} \). By \( |S| \) denote the cardinality of \( S \). Given \( a \in G \) we write \( \delta_a(x) \) for the delta function at the point \( a \). For a positive integer \( n \), we set \([n] = \{1, \ldots, n\} \). All logarithms \( \log \) are base 2. Signs \( \ll \) and \( \gg \) are the usual Vinogradov’s symbols.
For a sequence \( s = (s_1, \ldots, s_k) \in G^k \) put \( A_s = A \cap (A - s_1) \cap \cdots \cap (A - s_k) \). Let
\[
E_k(A) = \sum_{x \in G} (A \circ A)(x)^k = \sum_{s_1, \ldots, s_k \in G} |A_s|^2.
\] (10)

If \( k = 2 \) then \( E_k(A) \) is denoted by \( E(A) \) and is called the additive energy of \( A \), see [22]. Some results on the quantities \( E_k(A) \) can be found in [18, 19]. For any complex function \( f \) and a positive integer \( k \) denote by \( C_{k+1}(f)(x_1, \ldots, x_k) \) the quantity
\[
C_{k+1}(f)(x_1, \ldots, x_k) = \sum_z f(z)f(z + x_1) \cdots f(z + x_k).
\]

The next lemma is a very special case of Lemma 4 of paper [20] and is the simplest generalization of the second formula from (10).

**Lemma 2.1** Let \( f, g \) be two complex functions on an abelian group \( G \). Suppose that \( k \) is a positive integer. Then
\[
\sum_{x_1, \ldots, x_k} C_{k+1}(f)(x_1, \ldots, x_k) C_{k+1}(g)(x_1, \ldots, x_k) = \sum_z (f \circ g)^{k+1}(z).
\]

Now consider the case \( G \) be the field. If \( q = p^s \), \( p \) is a prime number then we write \( \mathbb{F}_q \) for such finite field. In the case \( q = p \) by \( R \) and \( N \) denote the sets of quadratic residues and non–residues of \( \mathbb{F}_p \), correspondingly. Clearly, \( |R| = |N| = \frac{p-1}{2} := t \), and \( 0 \notin R, 0 \notin N \). By \( \chi_0 \) denote the principle character, and denote the Legendre symbol on \( \mathbb{F}_p \) by \( \chi \). Given nonzero \( \lambda \in \mathbb{F}_p \) and a set \( A \subseteq \mathbb{F}_p \) we will write
\[
\lambda \cdot A := \{ \lambda \cdot a \ : \ a \in A \}.
\]
Thus \( 2A := A + A \neq 2 \cdot A \) in general.

**Definition 2.2** Let \( \varphi, \psi \) be two characters on \( \mathbb{F}_q \). The Jacobi sum \( J(\chi, \psi) \) is defined by
\[
J(\varphi, \psi) = \sum_x \varphi(x)\psi(1-x).
\]

We need in a lemma (see [2], chapters 1–2).

**Lemma 2.3** For any non principle character \( \psi \), we have
\[
J(\psi, \overline{\psi}) = -\psi(-1).
\] (11)

Whence
\[
(\psi \circ \overline{\psi})(x) = p\delta_0(x) - 1, \quad (\psi \ast \overline{\psi})(x) = \chi(-1)(p\delta_0(x) - 1).
\] (12)

Further
\[
G(p) := \sum_x \chi(x)e^{2\pi ix/p} = \begin{cases} \sqrt{p} & \text{if} \quad p \equiv 1 \mod 4 \\ i\sqrt{p} & \text{if} \quad p \equiv -1 \mod 4 \end{cases}
\]

In particular, for any \( x \neq 0 \) the following holds \( |\widehat{R}(x)| \leq \frac{\sqrt{p}+1}{2} \).

**Proof.** Indeed, by the definition of Gauss sum, we have for all \( x \in \mathbb{F}_p \) that
\[
\widehat{R}(x) = \frac{1}{2}(p\delta_0(x) - 1 + G(p)\chi(-x))
\]
and the result follows. □

Recall a well–known consequence of the lemma.

**Lemma 2.4** Let \( g, h : \mathbb{F}_p \rightarrow \mathbb{C} \) be any complex functions. Then

\[
\left| \sum_{x,y} g(x) h(y) \chi(x + y) \right| \leq \|g\|_2 (p\|h\|_2^2 - |\langle h \rangle|^2)^{1/2} \leq \|g\|_2 \|h\|_2 \sqrt{p},
\]

(13)

and

\[(g \circ \chi) \circ (h \circ \chi))(x) = p(h \circ g)(x) - \langle g \rangle \cdot \langle h \rangle .\]

(14)

In particular

\[
\sum_x (g \circ \chi)(x)(h \circ \chi)(x) = p\langle g, h \rangle - \langle g \rangle \cdot \langle h \rangle .
\]

(15)

Note that inequality (13) is sharp (see e.g. section 5). Formula (15) of lemma above implies the ”Cauchy–Schwartz” inequality in \( \mathbb{F}_p \).

**Corollary 2.5** For any complex function \( f : \mathbb{F}_p \rightarrow \mathbb{C} \), we have

\[
\|f\|_2^2 = \frac{|\langle f \rangle|^2}{p} + \frac{1}{p} \sum_x |(f \circ \chi)(x)|^2 \geq \frac{|\langle f \rangle|^2}{p} .
\]

(16)

Also, using Lemma 2.4 one can obtain simple upper bounds for the cardinalities of sets \( A, B \) such that \( A + B \subseteq R \) or \( A + B \subseteq N \) (see e.g. the proof of Theorem 3.2 below or [3, 6]).

Applying Lemma 2.1 we can easily improve Theorem 1.1 from [16] (similar result was obtained in [21]).

**Corollary 2.6** Let \( A + B = R \). Then as \( p \to \infty \), one has

\[
\left( \frac{1}{6} - o(1) \right) \sqrt{p} \leq |A|, |B| \leq (3 + o(1)) \sqrt{p} .
\]

Proof. We can assume that \( A \) and \( B \) are sufficiently large sets (see [16]). By Lemma 2.1, we have

\[
|A|^4 |B| = \sum_{x \in B} (\chi \circ A)^4(x) \leq \sum_x (\chi \circ A)^4(x) = \sum_{x,y,z} C_4(\chi)(x,y,z) C_4(A)(x,y,z) .
\]

Formula (4) gives

\[
|C_4(\chi)(x,y,z)| \leq 3 \sqrt{p}
\]

with three exceptions : \( x = y \neq 0, z = 0 \), further \( x = z \neq 0, y = 0 \), and \( y = z \neq 0, x = 0 \). Thus

\[
|A|^4 |B| \leq 3 \sqrt{p} |A|^4 + 3p |A|^2
\]

and we obtain that \( |A|, |B| \leq (3 + o(1)) \sqrt{p} \). Because of \( |A||B| \geq t = (p - 1)/2 \), we get \( |A|, |B| \geq \left( \frac{1}{6} - o(1) \right) \sqrt{p} \). This completes the proof. □

At the end of the section we recall the notion of perfect difference sets.

**Definition 2.7** Let \( G \) be a group. A set \( A \subseteq G \) is called a perfect difference set if the convolution \( (A \circ A)(x) \) does not depend on the choice of \( x \neq 0 \).
Because of $(A \circ A)(0) = |A|$ the definition above says that $(A \circ A)(x) = (|A| - \lambda)\delta_0(x) + \lambda,$ where $\lambda \geq 1$ is some constant. We will say that $A$ is a $\lambda$-perfect difference set in the case and just perfect difference set for $\lambda = 1$. Generally speaking, let $\mathcal{L}$ be the algebra of the functions of the form $a\delta_0(x) + b$, where $a$ and $b$ are some complex constants. Clearly, a function $\varphi$ belongs to $\mathcal{L}$ iff $\hat{\varphi} \in \mathcal{L}$. Denote by $\mathcal{D}$ the set of all perfect difference functions, that is all functions $\varphi$ such that $\varphi \circ \varphi$ or, equivalently, $\hat{\varphi} \cdot \hat{\varphi}$ belongs to $\mathcal{L}$. For example, Lemma 2.3 says that $\chi \in \mathcal{D}$. It is easy to check that $\mathcal{D}$ is closed under convolutions $\ast$ and $\circ$. Moreover, if $\varphi \in \mathcal{D}$, $\hat{\varphi}(x) \neq 0, x \in G$ and $\varphi \circ \psi$ or $\varphi \ast \psi \in \mathcal{D}$ then $\psi \in \mathcal{D}$. Finally, if $f \in \mathcal{D}$ then $\alpha + \beta f \in \mathcal{D}$ for any $\alpha, \beta \in \mathbb{C}.

We need in a simple lemma.

**Lemma 2.8** For all $x \neq 0$, we have

$$(R \circ R)(x) = \frac{p - 3}{4} - \frac{\chi(x)}{4} (1 + \chi(-1)).$$  \hspace{1cm} (17)

**Proof.** Since

$$R(x) = \frac{1}{2} (\chi_0(x) + \chi(x))$$

it follows that for $x \neq 0$

$$(R \circ R)(x) = \frac{1}{4} \sum_z (\chi_0(z) + \chi(z))(\chi_0(z + x) + \chi(z + x)) =$$

$$= \frac{p - 2}{4} - \frac{1}{4} (\chi(x) + \chi(-x)) + \frac{1}{4} \sum_z \chi(z + x))$$

and the result follows from Lemma 2.3. \hfill \Box

In particular, if $p \equiv -1 \pmod{4}$ then $R \in \mathcal{D}$.

Let $A \subseteq \mathbb{Z}_P$ be a perfect difference set. A residue $m$ is called a multiplier of $A$ if $mA = A$. We formulate the multiplier theorem, see e.g. [10].

**Theorem 2.9** Let $A$ be a $\lambda$-perfect difference set, $A \subseteq \mathbb{Z}_P$. Suppose that $m$ be any prime number such that $m \mid (|A| - \lambda)$, $(m, P) = 1$ and $m > \lambda$. Then $m$ is a multiplier of some translation of $A$.

Clearly, the set of multipliers of $A$ forms a group and, moreover, one can choose a translation of $A$ fixing by the group (see [10]).

Recall also a beautiful theorem of Singer (see e.g. [10]) concerning finite projecting geometries.

**Theorem 2.10** Suppose that $P$ is a number of the form $P = n^2 + n + 1$, $n = q^s$, where $s \geq 1$ and $q$ is a prime number. Then there is a perfect difference set $A \subseteq \mathbb{Z}_P$ such that $(A \circ A)(x) = 1$ for all $x \neq 0$.

### 3. Sumsets and differences

We begin with a simple lemma.

**Lemma 3.1** Let $c$ be an integer, and $\psi : G \to \mathbb{Z}$ be a function. Then

$$\|\psi\|_2^2 \geq c \sum_x |\psi(x)| - (c - 1) \cdot \sum_{x : 0 < |\psi(x)| < c} |\psi(x)|.$$  \hspace{1cm} (18)
Further

\[ \|\psi\|_2^2 = c \sum_x \psi(x) + \sum_k |\{x : \psi(x) = k\}| \cdot (k^2 - ck). \]  

(19)

Proof. Let \( \sigma = \sum_x \psi(x) \). We can suppose that \( \sigma > 0 \), otherwise consider the function \(-\psi\).

For any integer \( k \) put

\[ p_k = |\{x : \psi(x) = k\}|. \]

Then

\[ \sigma = \sum_k k p_k = \sum_{k : |k| \geq c} k p_k + \sum_{k : 0 < |k| < c} k p_k = \sigma_1 + \sigma_2, \]

and hence

\[ \|\psi\|_2^2 = \sum_k k^2 p_k = \sum_{k : |k| \geq c} k^2 p_k + \sum_{k : 0 < |k| < c} k^2 p_k \geq c \sigma_1 + \sigma_2 = c \sigma - (c - 1)\sigma_2 \geq c \sigma - (c - 1)|\sigma_2| \]

as required. Formula (19) follows similarly. This completes the proof. \( \square \)

Now we can prove a small generalization of the first part of our main Theorem 1.2.

**Theorem 3.2** Let \( p \) be a prime number, \( R \subseteq \mathbb{F}_p \) be the set of quadratic residues and \( A \subseteq \mathbb{F}_p \) be a set. If \( A + A = R \) then \( p = 3 \) and \( A = \{2\} \). Moreover for all sufficiently large \( p \), we have

\[ \max \left\{ |R \setminus (A + A)|, \sum_{x \in (A + A) \backslash R} (A * A)(x) \right\} \geq \left( \frac{1}{6} - o(1) \right) |A|. \]

(20)

Proof. Suppose that \( A, B \) are two sets such that \( A + B \subseteq R \). Let \( a = |A|, b = |B| \). Define the function \( \varepsilon(x) \) by the formula

\[ (A \circ \chi)(x) = aB(x) + \varepsilon(x). \]

(21)

We have \( \varepsilon(x) = 0, x \in B \). Using Lemma 2.4, we get

\[ \|\varepsilon\|_2^2 = pa - a^2 - a^2 b. \]

(22)

Further

\[ \langle \varepsilon \rangle = -ab, \]

(23)

thus, by the Cauchy–Schwartz inequality

\[ a^2 b^2 \leq (p - b)(pa - a^2 - a^2 b) \]

or

\[ p + \frac{ab}{p} \geq ab + a + b. \]

(24)

On the other hand, by formula (13) of Lemma 2.4 or just by inequality (22), one has \( ab < p \).

Now suppose that \( A = B \) and \( A + A = R \). If \( a = 1 \) then \( \frac{p-1}{2} = 1 \), whence, \( p = 3 \) and, clearly, \( A = \{2\} \). Thus, suppose that \( a > 1 \). Because of \( A + A = R \), we obtain \( \binom{a}{2} + a \geq \frac{p-1}{2} \)
or, in other words, \( a^2 + a \geq p - 1 \). Using the last estimate, the fact \( a^2 < p \) and inequality (24), we get

\[
p + 1 > p + \frac{a^2}{p} \geq a^2 + 2a \geq p - 1 + a
\]

with contradiction.

Now, let us prove the second part of the theorem. Put

\[
|R \setminus (A + A)| := \zeta_1 a \quad \text{and} \quad \sum_{x \in (A + A) \setminus R} (A \ast A)(x) := \zeta_2 a.
\]

Let also \( \zeta = \max\{\zeta_1, \zeta_2\} \). We need to obtain the lower bound for \( \zeta \). Suppose that \( \zeta \leq \frac{1}{6} + o(1), \)

\[
p \to \infty. \quad \text{We have}
\]

\[
\left(\frac{a}{2}\right) + a \geq \frac{p - 1}{2} - \zeta_1 a \geq \frac{p - 1}{2} - \zeta a
\]

or, in other words,

\[
a^2 + a(1 + 2\zeta) \geq p - 1. \tag{25}
\]

Put

\[
(A \circ \chi)(x) = aA(x) + \varepsilon(x).
\]

As in (23) the average value of \( \varepsilon(x) \) equals \(-a^2\), and we estimate \( l_2 \)-norm of the function as in (22)

\[
\|\varepsilon\|_2^2 = \sum_{x} ((A \circ \chi)(x) - aA(x))^2 = pa - a^2 - a^3 - 2a \sum_{x \in A} (A \circ \chi)(x) =
\]

\[
= pa - a^2 - a^3 + 2a \sum_{x} (1 - \chi(x))(A \ast A)(x) =
\]

\[
= pa - a^2 - a^3 + 2a \sum_{x \in (A + A) \setminus R} (1 - \chi(x))(A \ast A)(x) \leq pa - a^2 - a^3 + 4\zeta a^2. \tag{26}
\]

By the Cauchy–Schwarz inequality

\[
a^4 \leq \|\varepsilon\|_2^2 \leq pa - a^2 - a^3 + 4\zeta a^2. \tag{27}
\]

Note that from the last estimate it follows that \( a \ll \sqrt{p} \). Using (27) and inequality (25), we obtain after some calculations that \( \zeta \geq \frac{1}{6} - o(1) \). This completes the proof. \( \square \)

Now we reprove a result of C. Bachoc, M. Matolcsi, I.Z. Rusza from [1].

**Theorem 3.3** Let \( p \) be a prime number, \( R \subseteq \mathbb{F}_p \) be the set of quadratic residues and \( A \subseteq \mathbb{F}_p \) be a set. If \( A - A \subseteq R \cup \{0\} \) then

\[
p \geq \begin{cases} |A|^2 + |A| - 1 & \text{if } |A| \text{ is even} \\ |A|^2 + 2|A| - 2 & \text{if } |A| \text{ is odd.} \end{cases}
\]

**Proof.** Put \( |A| = a \). Clearly, \( p \equiv 1 \pmod{4} \). As in the previous theorem, we have

\[
(A \ast \chi)(x) = (a - 1)A(x) + \varepsilon(x), \tag{28}
\]
where \( \varepsilon(x) = 0 \) for \( x \in A \). As above

\[
\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2, \quad \text{and} \quad \langle \varepsilon \rangle = -a(a-1).
\]

Further

\[
\varepsilon(x) = |R \cap (x - A)| - |N \cap (x - A)| = 2|R \cap (x - A)| - a \tag{29}
\]

for all \( x \notin A \). First of all consider the case \( a \) is an even number. By formula (29) the values of \( \varepsilon(x) \) are even for all \( x \) (recall that \( \varepsilon(x) = 0 \) on \( A \)). Using Lemma 3.1 with \( c = 2 \), we obtain

\[
\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2 \geq 2a(a-1)
\]

or, in other words,

\[ p \geq a^2 + a - 1 \]

as required.

Now suppose that \( a \) is odd and \( a > 1 \). Of course \( \varepsilon(x) = 0 \) on \( A \), and by formula (29) all other values of \( \varepsilon(x) \) are odd. First of all note that there is \( x \notin A \) such that \( \varepsilon(x) \neq -1 \). Indeed, otherwise, applying (28), we get

\[
\langle A, \chi \rangle = \langle \varepsilon, \chi \rangle = pA(0) - a - (a-1)\langle A, \chi \rangle. \tag{30}
\]

Shifting, we can suppose that \( 0 \in A \) and, hence, \( \langle A, \chi \rangle = a - 1 \). Substituting into (30) gives \( p = a^2 \) with contradiction. (Note that nevertheless it can be the case for the field \( \mathbb{F}_q \) with \( q \) equals a prime power, see [1]). Now give an another proof of the fact. Put \( p_k := |\{x \in \mathbb{F}_p : \varepsilon(x) = k\}|, k \in \mathbb{Z} \). Clearly, \( p_0 = a \) and \( p_{2l} = 0 \) for all nonzero integer \( l \). As before, using formula (19) of Lemma 18 with \( c = -2 \) and the fact that the quantity \( p_{-1} \) does not exceed \( (p - 1)/2 \) (consider \( \varepsilon(x) \pmod{p} \) and note that \( \chi(x) \equiv x^{(p-1)/2} \pmod{p} \)), we obtain

\[
\|\varepsilon\|_2^2 = pa - a^2 - a(a-1)^2 = -2\langle \varepsilon \rangle + \sum_{k} (k^2 + 2k)p_k \geq 2a(a-1) - p_{-1} + \sum_{k \neq -1,0} p_k =
\]

\[
= 2a(a-1) + 3p - 4p_{-1} - 3a \geq 2a(a-1) + p + 2 - 3a
\]

or, in other words,

\[ p \geq a^2 + a - 4 + \frac{p + 2}{a} \]

After some calculations we get \( p \geq a^2 + 2a - 2 \), provided by \( a > 1 \). This completes the proof.

\[ \square \]

4. Restricted sumsets

The aim of the section is to prove the second part of our main Theorem 1.2.

Write any prime \( p \) as \( p = n^2 + \Delta, 1 \leq \Delta \leq 2n \). We are interested in sets \( A \subseteq \mathbb{F}_p \) such that \( A + A = R \). Let us consider some examples.

**Example 4.1** There are examples of perfect difference sets \( A \subseteq \mathbb{F}_p \) with \( A + A = R \):

(a) \( p = 3, A = \{0, 1\} \).
(b) \( p = 7, A = \{3, 5, 6\} \).
(c) \( p = 13, A = \{0, 1, 3, 9\}, A = \{0, 4, 10, 12\} \).

Note that in all these examples \( p = n^2 + n + 1, |A| = n + 1, n = q^s, q \) is a prime number or 1.
In particular $\Delta = n+1$. The existence of a perfect difference set in $\mathbb{F}_p$ for $p$ of such a form guaranties by Singer’s theorem 2.10. Note also, that it is easy to check using the multiplier theorem and another tools (see the beginning of the proof of Proposition 4.2 and Theorem 4.3 below) that the sets above form the complete list of (perfect difference) sets $A \subseteq \mathbb{F}_p$ with $A+A = R$ for $p = 3, 7, 13$.

In our proof of the second part of main Theorem 1.2 we begin with the situation when $A$ is a perfect difference sets. Surprisingly, it turns out that it is the most important case.

**Proposition 4.2** Let $p$ be a prime number, $p = n^2 + n + 1$, $R \subseteq \mathbb{F}_p$ be the set of quadratic residues and $A \subseteq \mathbb{F}_p$ be a perfect difference set. Suppose that $A+\hat{A} = R$. Then the set $A$ must be a set from Example 4.1.

**Proof.** Let $a = |A|$. Because of $A$ is a perfect difference set, we have $a = n+1$. Firstly, $(A+\hat{A}) \cap 2 \cdot A = \emptyset$ and, consequently, $R \cap 2 \cdot A = \emptyset$. In particular either $A \subseteq R \cup \{0\}$ or $A \subseteq N$. Secondly, by Theorem 2.9 there is $s \in \mathbb{F}_p$ such that the set $A+s$ is fixed by a multiplier $m \neq 1$. Then $(A+s)+\hat{(A+s)} = R + 2s$ and hence $m(R + 2s) = mR + 2sm = R + 2s$. If $m \in R$ we have automatically $s = 0$. If $m \in N$ then $mR = N$, and hence $N(x) = R(x + 2s(m-1))$. In other words

$$\chi_0(x) - \chi(x) = \chi_0(x + 2s(m-1)) + \chi(x + 2s(m-1)).$$

Clearly, the case $s = 0$ is impossible. Multiplying by $\chi(x)$, summing and using Lemma 2.3, we get

$$p - 1 = 1 - \chi(-2s(m-1)).$$

That implies $p = 1$ or $p = 3$. The case $p = 3$ is Example 4.1 (a). Thus for $p > 3$, we obtain that any multiplier of $A$ belongs to $R$. Below we assume that $n > 1$ and, hence, $p > 3$. By Theorem 2.9 and the previous arguments any prime factor of $n$ is a quadratic residue, which implies that $n$ belongs to $R$ itself. We have $p = n^2 + n + 1$, $n^3 \equiv 1 \pmod{p}$ and hence the order of $n$ is three (in particular $p \equiv 1 \pmod{3}$). The same follows from the fact that $n \equiv 0 \pmod{3}$ if $0 \in A$ and $n \equiv -1 \pmod{3}$ if $0 \notin A$. Take an arbitrary nonzero $x \in A$. Because of $n > 1$, we see that $x, xn, xn^2$ are different and belong to $A$. Whence $x + xn^2 \equiv x - (n+1)x \equiv -nx \in R$, so $x \in -R$. That is equivalent $A \setminus \{0\} \subseteq -R$.

Our arguments rest on the identity

$$R(x) = \frac{1}{2}((A \ast A)(x) - (2 \cdot A)(x))$$

(31)

which is a consequence of the fact that $A$ is a perfect difference set.

First of all suppose that $A \subseteq N$. Then $A \subseteq -R$, hence, $-1 \in N$, $p \equiv -1 \pmod{4}$ and $2 \in R$. Since $R \in \mathcal{D}$ and, simultaneously, $A \in \mathcal{D}$ it follows from formula (31) that

$$((A \ast A) \circ 2 \cdot A)(x) + (2 \cdot A \circ (A \ast A))(x) \in \mathcal{L}.$$ Using identity (31) again, we see that

$$(R \circ (2 \cdot A))(x) + ((2 \cdot A) \circ R)(x) \in \mathcal{L}.$$ It follows that

$$|R \cap (2 \cdot A + x)| + |R \cap (2 \cdot A - x)| = a, \quad \forall x \neq 0.$$ (32)

We know the number 2 belongs to $R$. If $x \in 2 \cdot A$ then

$$|R \cap (2 \cdot A + x)| = |R \cap (A + x/2)| = a - 1$$

because of $x/2 \in A$ and $A + \hat{A} = R$. On the other hand, using the fact $2 \in R$ again, we get

$$\sum_{x \in 2 \cdot A} |R \cap (2 \cdot A - x)| = \sum_x R(x)(A \circ A)(x) = t$$ (33)
and hence there is \( x \in 2 \cdot A \) such that \( |R \cap (2 \cdot A - x)| \geq t/a \). Combining the last inequality with (32), we obtain
\[
a - 1 + \frac{t}{a} \leq a
\]
or \( a \leq 3 \). That is Example 4.1 (b).

It remains consider the situation \( A \subseteq R \cup \{0\} \). In the case \( p \equiv 1 \pmod{4} \) and \( 2 \in \mathbb{N} \) but, unfortunately, \( R \notin \mathcal{D} \), and, thus, we need in more delicate arguments. Using (31), one can see that
\[
(R \circ R)(x) = \frac{1}{4}(((A^* \circ (A^*) \circ A))(x) + (2 \cdot A \circ (2 \cdot A))(x) - ((2R + 2 \cdot A) \circ 2 \cdot A)(x) - 2 \cdot A \circ (2R + 2 \cdot A)) = \frac{1}{4}((A^* \circ (A^*) \circ A))(x) - (2 \cdot A \circ (2 \cdot A))(x) - 2(R \circ 2 \cdot A)(x) - 2(2 \cdot A \circ R)(x).
\]
Because of \( E(A) = 2a^2 - a \), and \( A^* \circ A \in \mathcal{D} \), we have
\[
((A^* \circ (A^*) \circ A))(x) = \frac{a^4 - E(A)}{p - 1} = \frac{a^4 - 2a^2 + a}{p - 1} = a^2 + a - 1, \quad \forall x \neq 0.
\]
Combining the last formula, Lemma 2.8, and the fact \( A \in \mathcal{D} \), we obtain
\[
p - 3 - 2\chi(x) = a^2 + a - 1 - 1 - 2(R \circ 2 \cdot A)(x) - 2(2 \cdot A \circ R)(x), \quad \forall x \neq 0.
\]
In other words
\[
a + \chi(x) = (R \circ 2 \cdot A)(x) + (2 \cdot A \circ R)(x), \quad \forall x \neq 0.
\] (34)

Let \( A^* = A \setminus \{0\} \). Using the arguments similar (32)—(33), we see that for all \( x \in 2 \cdot A^* \) the following holds \( |R \cap (2 \cdot A + x)| = |N \cap (A + x/2)| = 1 \) and
\[
\sum_{x \in 2 \cdot A^*} |R \cap (2 \cdot A - x)| = \sum_{x} N(x)(A^* \circ A)(x) = \sum_{x} N(x)(A \circ A)(x) - |A \cap N| = t.
\]
Whence there is \( x \in 2 \cdot A^* \) such that \( |R \cap (2 \cdot A - x)| \leq t/(a - 1) \). For any \( x \in 2 \cdot A^* \), we have \( \chi(x) = -1 \). Applying (34), we obtain
\[
a - 1 \leq 1 + \frac{t}{a - 1}
\]
or \( a \leq 4 \) (if \( 0 \notin A \) then it is easy to check similarly that \( a \leq 3 \)). That is Example 4.1 (c). Indeed, \( A \subseteq R \cup \{0\} \), \( R = \{1, 3, 4, 9, 10, 12\} \) and it is easy to see that \( A \) either \( \{0, 1, 3, 9\} \) or \( \{0, 4, 10, 12\} \) (note that \( |A| - 1 = 3 \) is a multiplier of \( A \)). This completes the proof. \( \square \)

Note that Example 4.1 shows the possibility of the cases \( \Delta = 2, 3 \) as well as \( \Delta = n + 1 \).

Now we can consider the general situation. Of course, the third part of theorem below is the main one but it follows from the first. The second part shows that \( A \) with \( A^+ + A = R \) is close to a perfect difference set in some sense.

**Theorem 4.3** Let \( p \) be a prime number, \( p = n^2 + \Delta, 1 \leq \Delta \leq 2n \), \( R \subseteq \mathbb{F}_p \) be the set of quadratic residues and \( A \subseteq \mathbb{F}_p \) be a set.

1) If \( A^+ + A = R \) and \( A \) is not from Example 4.1 (a) then \( |A| = n + 1, 3 \leq \Delta \leq n + 1 \) and
\[ |2 \cdot A \cap R| \leq \frac{\sqrt{3|A| - 3|A| + 1}}{2}. \] If \(0 \notin A\) then \(\chi(2) = 1\), and \(|A| \leq 6\). If \(0 \in A\) then \(\chi(2) = -1\) and if \(\Delta = n + 1\) then \(A\) is a perfect difference set.

2) If \(A + A = R\) then it is close to a perfect difference set in the sense

\[ E(A) = 2|A|^2 - |A| + \mathcal{E}_1, \] (35)

where

\[ \mathcal{E}_1 \leq 6(|A| - \Delta) + 2|A| + \min\{|A| - \Delta|A|, |A|\sqrt{3(|A| - \Delta)}, (|A| - \Delta)^2\}, \]

and

\[ (A \circ A)(x) = (|A| - 1)\delta_0(x) + 1 + \mathcal{E}_2(x), \] (36)

where \(\sum_x \mathcal{E}_2(x) = |A| - \Delta, \|\mathcal{E}_2\|^2 = \mathcal{E}_1 + \Delta - |A|\).

3) If \(A + A = R\) then \(A\) is a perfect difference set such that if \(|A|\) is even then \(|A| \leq 6\) and if \(|A|\) is odd then \(|A| \leq 5\).

**Proof.** 1) Put \(a = |A|\). The assumption \(A + A = R\) implies that \((\frac{a}{2}) \geq \frac{p-1}{2}\). In other words, \(a^2 - a \geq p - 1\). The last inequality is equivalent to \(a \geq n + 1\). We can assume that \(a \geq 3\) because otherwise we have Example 4.1 (a). One can also check that for \(a \geq 3\) the case \(p = 5\) is impossible, and hence we will assume that \(p \geq 7\). Below we will use the fact that \(A + A \subseteq R\) only. Put

\[ d := \sum_{x \in A} (\chi(2x) - 1) = \eta a. \]

Clearly, \(\eta \in [-2, 0]\). Let us obtain some further estimates on \(d\) and \(\eta\). By Lemma 2.4, we get

\[ \sum_x (A \circ \chi)^2(x) = pa - a^2. \] (37)

Further, similar to (21), we have

\[ (A \circ \chi)(x) = (a - 1 + \chi(2x))A(x) + \varepsilon(x) \] (38)

where \(\varepsilon(x) = 0\) for all \(x \in A\). Hence

\[ a(a - 1)^2 + 2(a - 1)(d + a) + a - \omega = \sum_{x \in A} (a - 1 + \chi(2x))^2 \leq pa - a^2, \]

where \(\omega = 1\) if \(0 \in A\) and \(\omega = 0\) otherwise. It is easy to calculate that the last inequality and the bound \(a^2 - a \geq p - 1\) imply that

\[ d \leq -a - \frac{a - \omega}{2(a - 1)} < -a. \] (39)

In particular, \(\eta \in [-2, -1]\). In the case \(0 \notin A\), we have

\[ (d + a)^2 + a(a - 1)^2 + 2(a - 1)(d + a) + a \leq pa - a^2 \]

and after some manipulations, we obtain

\[ d \leq -2a + 1 + \sqrt{a^2 - 3a + 1}, \] (40)
\[ d \leq -2a + 1 + \sqrt{a\Delta - 3a + 1}, \quad (41) \]

provided by \( p = (a - 1)^2 + \Delta \). Note that in the case \( \Delta \geq 3 \). Now suppose that \( 0 \in A \). Write \( A = A^* \bigcup \{0\} \). Then \( A^* \subseteq R \), and the set \( 2 \cdot A^* \) belongs either \( R \) or \( N \). In the first case \( d = -1 \) and that is impossible by (39). If \( 2 \cdot A^* \subseteq N \) then \( d = -2a + 1 \), \( \chi(2) = -1 \), and (40), (41) take place. Thus in any case

\[ |2 \cdot A \cap R| \leq \frac{\sqrt{a^2 - 3a + 1}}{2}, \quad (42) \]

and

\[ |2 \cdot A \cap R| \leq \frac{\sqrt{a\Delta - 3a + 1}}{2}, \quad (43) \]

provided by \( p = (a - 1)^2 + \Delta \). One of the main ideas of the further proof is an exploitation of inequalities (39), (42), (43). They mean that the distribution of the intersections \( |R \cap (A+x)|, x \in \mathbb{F}_p \) is an asymmetric a little bit.

Returning to (38), we get for all \( x \notin A \) that

\[ \varepsilon(x) = |R \cap (A + x)| - |N \cap (A + x)| = 2|R \cap (A + x)| - a + A(-x). \quad (44) \]

Clearly,

\[ \langle \varepsilon \rangle = -a^2 - d. \quad (45) \]

As above, we have

\[ \sum_{x \in A} (a - 1 + \chi(2x))^2 = a(a - 1)^2 + 2(a - 1)(d + a) + a - \omega = a^3 + 2(a - 1)d - \omega, \]

where, as before, the quantity \( \omega \) equals \( |A \cap \{0\}| \). As in Theorem 3.2, we obtain an analog of (22)

\[ \| \varepsilon \|_2^2 = pa - a^2 - a^3 - 2(a - 1)d + \omega. \quad (46) \]

Thus by the Cauchy–Schwartz inequality and identity (45), we get

\[ \frac{(a^2 + d)^2}{p - a} \leq pa - a^2 - a^3 - 2(a - 1)d + \omega. \quad (47) \]

In other words

\[ a^2(p - 1) + ab(\eta) - c(\eta) := a^2(p - 1) + a(\eta^2 + 2\eta + 2np + 2p - 2\eta p - p^2 - \omega \frac{p - a}{a}) \leq 0. \quad (48) \]

It is easy to check that the formula for the right root of (48), namely,

\[ x(\eta) = \frac{-b(\eta) + \sqrt{b^2(\eta) + 4(p - 1)c(\eta)}}{2(p - 1)} \]

contains an decreasing function \(-b(\eta)\) and an increasing function

\[ g(\eta) := b^2(\eta) + 4(p - 1)c(\eta) = \]

\[ = \eta^4 + (4 + 4p)\eta^3 + (4 + 4p^2 + 12p)\eta^2 + 16np^2 + 4p^3 + \omega \frac{4(p - 1)(p - a)}{a}. \]
on \( \eta \in [-2, -1] \). Indeed, one can see that \( g'(-2) = 0 \) and \( g'' \) grows on \( \eta \in [-2, -1] \). Put 
\( e = \omega^{\frac{4(p-1)(p-n)}{n}} \). Because of \( a \geq \sqrt{p} \), we have \( e \leq 4p^{3/2} \). Hence, we should substitute \( \eta = -2 \) into \( b(\eta) \), \( \eta = -1 \) into \( g(\eta) \), and check the following inequality:

\[
a \leq \frac{2p + \sqrt{4p^3 - 12p^2 + 8p + 1 + e}}{2(p-1)} \leq \sqrt{p} + 1 < n + 2. \tag{49}
\]

One can insure that, indeed, the second bound from (49) holds, provided by \( p \geq 7 \). Thus, for any \( \eta \), we have \( a = n + 1 \). Recalling \( a^2 - a \geq p - 1 \), we obtain

\[
a^2 - a = n^2 + n \geq p - 1 = n^2 + \Delta - 1. \tag{50}
\]

Whence \( 3 \leq \Delta \leq n + 1 \) and in the case \( \Delta = n + 1 \) all sums \( a' + a'' \) are different for different \( a', a'' \in A \). Using, the arguments above, we see that if \( 0 \in A \) and \( \Delta = n + 1 \) then \( A \) is a perfect difference set.

Finally, consider the case \( 0 \notin A \). We will prove, in particular, that \( \chi(2) = 1 \) in the situation. By (38) one has

\[
\varepsilon(0) = \sum_{x \in A} \chi(x) = \chi(2) \sum_{x \in A} \chi(2x) = \chi(2)(d + a).
\]

Further, identity (38) and the last formula imply

\[
\sum_x \varepsilon(x) \chi(x) = -a - \chi(2)(a^2 + da - d).
\]

Hence, as in (47), excluding zero point from the function \( \varepsilon(x) \), and, additionally, using Corollary 2.5, we get

\[
\frac{(a^2 + d + \chi(2)(d + a))^2 + (a + \chi(2)(a^2 + da - d))^2}{p} \leq pa - a^2 - a^3 - 2(a - 1)d - (d + a)^2. \tag{51}
\]

After some manipulations, we obtain for \( \chi(2) = -1 \) that

\[
\begin{align*}
  h_{a,d}(\Delta) := a\Delta^2 + (a^3 - 6a^2 + 2a - 4da + 2d - d^2)\Delta - & \\
  -6a^4 + 13a^3 - 8a^2 + 14a^2d - 2d^2a^2 - 6da^3 + a - 10da + 4d^2a + 2d - 2d^2 & \geq 0 \tag{52}
\end{align*}
\]

the maximum of \( h_{a,d}(\Delta) \) is attained at \( \Delta = a \) and is equal to

\[-(2a^2 - 3a + 2)d^2 - (6a^3 - 10a^2 + 8a - 2)d - 5a^4 + 8a^3 - 6a^2 + a.\]

The integer maximum of the last expression is attained at \( d \in [-1.5a, -1.5a + 1] \). Substituting the integer values of \( d \) from the interval, we obtain a contradiction. Almost the same is true in the case \( \chi(2) = 1 \). In the situation

\[
\begin{align*}
  h^*_{a,d}(\Delta) := a\Delta^2 + (a^3 - 6a^2 + 2a - 4da + 2d - d^2)\Delta + & \\
  +a - 2d^2a^2 - 6d^2 + 5a^3 - 8a^2 + 2d - 6a^4 + 4d^2a - 10da + 6a^2d - 6da^3 & \geq 0 \tag{53}
\end{align*}
\]

Again the maximum of \( h^*_{a,d}(\Delta) \) is attained at \( \Delta = a \) and is equal to

\[-(2a^2 - 3a + 6)d^2 - (6a^3 - 2a^2 + 8a - 2)d - 5a^4 - 6a^2 + a \geq 0.\]
Applying Fourier transform and estimates (39), (41), (43), (55), we get

\[ A \]

Using this, Gauss sums bound of Lemma 2.3, inequality \( \Delta \geq \) where

\[ Z \]

provided by

\[ a \]

values of \( d \) will use later. If \( a = 3 \) then \( p = 7, \chi(2) = 1, \Delta = a, |A+A| = \left( \frac{3}{2} \right) = 3, R = \{1, 2, 4\} \). If \( A \cap R = \emptyset \) then \( A \) is from Example 4.1 (b). Further, it is easy to see that \( 0 \notin A \), and \( A \) can intersect \( R \) just at one point. If \( 1 \in A \) then we have a contradiction because 5,6 cannot belong to \( A \) in the case. The same is true for \( 2 \in A \) and \( 4 \in A \). Thus \( A \) is from Example 4.1 (b), provided by \( a = 3 \). Finally, if \( a = 5 \) then \( p = 19 \) because of \( \Delta \geq 3 \). Hence \( \chi(2) = -1, 0 \notin A, d = -2a + 1 = -9 \). Substituting this into (47), we obtain a contradiction. The remain cases \( a = 4, 6 \) as well as the situation \( 0 \notin A \) will be considered later in the third part of the proof.

2) The fact \( R = A+A \) implies that

\[ (A \ast A)(x) = 2R(x) + (2 \cdot A)(x) + Z(x), \] (54)

where \( Z(x) \geq 0 \). It is easy to see that \( \text{supp} \, Z \subseteq R \). Summing (54), we obtain

\[ \|Z\|_1 = a^2 - 2t - a = n + 1 - \Delta = a - \Delta := z. \]

Using this, Gauss sums bound of Lemma 2.3, inequality \( \Delta \geq 3 \), and identity (54), we get

\[ |\hat{A}(x)|^2 \leq 3n + 2 < 3a, \; \forall x \neq 0. \] (55)

Further, multiplying (54) by \( (A \ast A)(x) \) and summing, we have

\[ \mathcal{E}(A) = \sum_x (2R(x) + (2 \cdot A)(x))(A \ast A)(x) + \sum_x Z(x)(A \ast A)(x) = \]

\[ = 4t + a + 2z + 4 \sum_x R(x)(2 \cdot A)(x) + \sum_x (2 \cdot A)(x)Z(x) + \sum_x Z(x)(A \ast A)(x). \]

Applying Fourier transform and estimates (39), (41), (43), (55), we get

\[ \mathcal{E}(A) = 2p - 2 + a + 2z + 4(2 \cdot A, R) + \langle 2 \cdot A, Z \rangle + \theta_1(\min\{za, \frac{a^2z}{p} + a\sqrt{3z}\}) \leq \]

\[ \leq 2a^2 - a + \theta_2(4(a - \Delta) + 2a + \min\{az, a\sqrt{3z}\}) \] (56)

where \( |\theta_1|, |\theta_2| \leq 1 \). Thus \( \mathcal{E}_1 \leq 4z + 2a + \min\{az, a\sqrt{3z}\} \). Squaring (54), summing and using (41), (43), we obtain

\[ \mathcal{E}(A) = 4t + a + 4z + 2(2 \cdot A, Z) + 4(2 \cdot A, R) + \|Z\|_2^2 = 2a^2 - a + \theta_3(6(a - \Delta) + 2a + z^2), \]

where \( 0 \leq \theta_3 \leq 1 \). Hence \( \mathcal{E}_1 \leq 6z + 2a + z^2 \).

Finally

\[ (a - 1)^2 + \sum_x \mathcal{E}_2^2(x) = (a - 1)^2 + \sum_{x \\neq 0} ((A \circ A)(x) - 1)^2 = \sum_x ((A \circ A)(x) - 1)^2 = \]

\[ = \mathcal{E}(A) - 2a^2 + p. \] (57)

Because of \( p = (a - 1)^2 + \Delta \), the last identity and formula (35), we obtain \( \|\mathcal{E}_2\|_2^2 = \mathcal{E}_1 + \Delta - a. \)
3) Let $a$ be an even number. Recalling (44) we see that $\varepsilon(x)$ is even for $x \notin -A$. Using Lemma 3.1 with $c = -2$, we get
\[ \|\varepsilon\|_2^2 = pd - a^2 - a^3 - 2(a-1)d + \omega \geq 2(a^2 + d) - (a - \omega). \]
After some computations, we obtain
\[ 2 + \Delta - 2d \geq 5a. \] (58)
Thus, either $\Delta = a = n+1$ and $d = -2a + 1, -2a$ or $\Delta = a-1, a-2$ and $d = -2a$. In the first case $A$ is a perfect difference set. Now suppose that $A$ is not a perfect difference set and consider the second situation. Because of $d = -2a$, we see that $0 \notin A$. Returning to (50), we get $\Delta = a-2 = n-1$. It means, in particular, that inequality (58) is actually, equality. Using formula (19) of Lemma 3.1, we see that $\varepsilon(x) = 0$ on $A$, $\varepsilon(x) = -1$ on $-A$ and $\varepsilon(x) = 0, -2$ on the rest. But $2 \cdot A \subseteq N$, hence $A \subseteq R$ or $A \subseteq N$ and thus by (44), we have $\varepsilon(0) = \pm a$ with contradiction. In particular, we have considered the remain cases $a = 4, 6$.

Now we should deal with the situation $a$ is an odd number and $0 \in A$. Whence $d = -2a+1$ and we can suppose that $\Delta \leq a - 1$ because $A$ is a perfect difference set otherwise. Using formula (19) of Lemma 18 with $c = -2$, applying the arguments from the proof of Theorem 3.3, we obtain
\[ \|\varepsilon\|_2^2 = pa - a^3 + 3a^2 - 6a + 3 \geq 2(a^2 - 2a + 1) + \sum_{k} (k^2 + 2k)p_k \geq \]
\[ \geq 2(a^2 + 2a - 1) - p_1 + 3 \sum_{k \neq 0, -1, -2} p_k = 2(a^2 - 2a + 1) + 3p - 4p_1 - 3(p_0 + p_2). \]
Here, again $p_k := |\{x \in \mathbb{F}_p : \varepsilon(x) = k\}|$, $k \in \mathbb{Z}$. Clearly, $p_0 + p_2 \leq 2a - 1$. As above, $p_1 \leq (p - 1)/2$. Hence
\[ pa - a^3 + 3a^2 - 6a + 3 \geq 2(a^2 - 2a + 1) + p + 2 - 6a + 3. \]
In other words
\[ \Delta(a - 1) - 2a^2 + 7a - 5 \geq 0 \]
with contradiction for $a \geq 5$ because of $A$ is not a perfect difference set by our assumption and, hence, $\Delta \leq a - 1$. This completes the proof. \hfill \Box

Clearly, the third part of Theorem 4.3 combining with Proposition 4.2 give the second part of the main Theorem 1.2.

Note 4.4. The method of the proving Theorem 4.3 above is analytical, thus we can say something about the structure of the set $A$ in a little bit more general situation. It was the reason to include the second part in the theorem. More precisely, suppose that a formula
\[ (A \ast A)(x) = 2R(x) + (2 \cdot A)(x) + Z(x) \] (59)
with "small" function $Z$ takes place. Then summing (59), we have
\[ p - 1 + |A| - \|Z\|_1 \leq |A|^2 \leq p - 1 + |A| + \|Z\|_1, \quad \text{and} \quad \langle Z \rangle = |A|^2 - 2t - a. \]
Further, for all \( x \neq 0 \) the following holds

\[
|\hat{A}(x)|^2 \leq \sqrt{p} + 1 + |A| + \|Z\|_1,
\]

and

\[
\mathcal{E}(A) = \sum_x (2R(x) + (2 \cdot A)(x))(A \cdot A)(x) + \sum_x Z(x)(A \cdot A)(x) \leq 4t + 5a + 3\|Z\|_1 + \sum_x Z(x)(A \cdot A)(x) \leq
\]

\[
4t + 6a + 3\|Z\|_1 + (\sqrt{p} + 1 + |A| + \|Z\|_1)^{1/2}|A|^{1/2}\|Z\|_2,
\]

(60)

provided by \( \langle Z \rangle \leq pa^{-1} \), say. Similarly, if we put

\[
(A \circ A)(x) = (|A| - 1)\delta_0(x) + 1 + \mathcal{E}_2(x),
\]

Then, as in (57), we get by (60) that

\[
\sum_x \mathcal{E}^2_2(x) = \sum_x ((A \circ A)(x) - 1)^2 - (a - 1)^2 = \mathcal{E}(A) - 2a^2 + p - (a - 1)^2 \leq
\]

\[
3p - 3 + 8a - 3a^2 + 3\|Z\|_1 + (\sqrt{p} + 1 + |A| + \|Z\|_1)^{1/2}|A|^{1/2}\|Z\|_2.
\]

Thus, if \( |R\Delta(A \hat + A)| \) is small than \( A \) is structured and close to a perfect difference set.

5. Concluding remarks

Now we describe an alternative way to obtain the results of sections 3, 4.

Our aim is to define an analog of ”Fourier transform” relatively to a multiplicative character \( \chi \). Put

\[
f(x) = \frac{1}{\sqrt{p}} \left( \chi(x) - \frac{1}{\sqrt{p}} \right).
\]

Clearly, \( f \) is a perfect difference function. Note that

\[
\|f\|_\infty \leq \frac{1}{\sqrt{p}} \left( 1 + \frac{1}{\sqrt{p}} \right). \tag{61}
\]

Let \( g \) be an arbitrary function. We write \( g_s(x) \) for \( g(x + s) \). By Lemma 2.3, we have

\[
\langle f_s, f_t \rangle = \delta_{s,t} \quad \text{and} \quad \sum_y f_y(s)f_y(t) = \delta_{s,t}, \tag{62}
\]

where \( s, t \in \mathbb{F}_p \) are arbitrary. Further \( \langle f_s, 1 \rangle = \langle 1, f_s \rangle = -1 \) and

\[
(f_s \circ f_t)(x) = \sum_z f_s(z)f_t(x + z) = \langle f_s, f_{t+x} \rangle = \delta_{s,t+x}. \tag{63}
\]

For an arbitrary function \( g \) write \( g^\lambda(x) = g(\lambda x) \). We have

\[
f_s^\lambda(x) = \chi(\lambda)f_{s/\lambda}(x) + \frac{\chi(\lambda) - 1}{p}, \tag{64}
\]

17
where $\lambda$ is any nonzero element. Applying formula (12) once more, we obtain

$$
(f^\lambda \circ \overline{f}^\mu)(x) = \chi(\lambda)\chi(\mu) \cdot \delta_{s/\lambda,x+t/\mu} + \frac{1 - \chi(\lambda)\chi(\mu)}{p}.
$$

Now we can define the "Fourier transform" corresponding to the character $\chi$.

**Definition 5.1** Let $\varphi : \mathbb{F}_p \to \mathbb{C}$ be a function. By $\tilde{\varphi}$ denote the function

$$
\tilde{\varphi}(x) = \sum_y \varphi(y)f_x(y) = \langle \varphi, f_x \rangle = (\varphi \circ f)(x).
$$

For example $\tilde{1} = -1$, $\tilde{\delta_s}(x) = f_s(x)$ and $\tilde{f}(x) = \delta_s(x)$.

Because of $D$ is closed under convolutions $\ast$, $\circ$, and $\hat{f}(x) \neq 0$, $x \in \mathbb{F}_p$, we see that $\varphi \in D$ iff $\tilde{\varphi} \in D$ (formula (70) below also implies the fact). The next lemma follows from the definitions.

**Lemma 5.2** Let $\varphi, \psi : \mathbb{F}_p \to \mathbb{C}$ be any functions. Then

$$
(\varphi^s) = (\tilde{\varphi})_{-s}, \quad \forall s \in \mathbb{F}_p.
$$

$$
(\varphi^-)(x) = \overline{\varphi(x)} \quad \text{and} \quad (\varphi^-)(x) = \varphi(x) \quad \text{if} \quad \chi \in \mathbb{R}.
$$

$$
(\varphi^\lambda)^-(x) = \chi(\lambda)\tilde{\varphi}^\lambda(x) + \frac{\langle \varphi, \chi(\lambda) - 1 \rangle}{p}, \quad \forall \lambda \neq 0.
$$

$$
\varphi(x) = \sum_y \tilde{\varphi}(y)f_x(y).
$$

$$
\sum_x \varphi(x)\overline{\psi(x)} = \sum_y \tilde{\varphi}(y)\overline{\psi(y)}
$$

$$
(\varphi \circ \psi)^-(x) = (\varphi \circ \tilde{\psi})(x).
$$

Further for any $\lambda, \mu \neq 0$, we have

$$
(\varphi^\lambda \circ \overline{\psi}^\mu)(x) = \chi(\lambda)\chi(\mu) \cdot (\overline{\psi}^\mu \circ \tilde{\varphi}^\lambda)(x) + \frac{1 - \chi(\lambda)\chi(\mu)}{p} \langle \varphi, \overline{\psi} \rangle.
$$

In particular

$$
(\varphi \circ \overline{\psi})(x) = (\tilde{\varphi} \circ \overline{\psi})(-x) = (\overline{\psi} \circ \tilde{\varphi})(x)
$$

and

$$
(\varphi \ast \overline{\psi})(x) = \chi(-1)(\tilde{\varphi} \ast \overline{\psi})(-x) + \frac{1 - \chi(-1)}{p} \langle \varphi, \overline{\psi} \rangle.
$$

**Proof.** We just need to check (73) because another formulas are almost trivial. Applying (69), (70) and the fact $f_s = -1$, $s \in \mathbb{F}_p$, we obtain

$$
(\varphi^\lambda \circ \overline{\psi}^\mu)(x) = \sum_z \varphi^\lambda(z)\overline{\psi}^\mu(z+x) =
$$

$$
= \sum_{y,y',z} \left( \chi(\lambda)\tilde{\varphi}^\lambda(y) + \frac{\langle \varphi, \chi(\lambda) - 1 \rangle}{p} \right) \left( \chi(\mu)\overline{\psi}^\mu(y') + \frac{\langle \psi, \chi(\mu) - 1 \rangle}{p} \right) f_z(y)f_{z+x}(y') =
$$
\[
\begin{align*}
&= \chi(\lambda) \bar{\chi}(\mu) \cdot \sum_y \varphi^\Lambda(y) \bar{\psi}_\mu(y - x) + \frac{1 - \chi(\lambda) \bar{\chi}(\mu)}{p} \cdot \langle \varphi \rangle \langle \bar{\psi} \rangle = \\
&= \chi(\lambda) \bar{\chi}(\mu) \cdot (\bar{\psi}_\mu \circ \varphi^\Lambda)(x) + \frac{1 - \chi(\lambda) \bar{\chi}(\mu)}{p} \cdot \langle \varphi \rangle \langle \bar{\psi} \rangle .
\end{align*}
\]

This concludes the proof. \(\square\)

In particular, formula (74) says that \(E(A) = E(\tilde{A})\). The transform above can be used to obtain the results of sections 3, 4. Indeed, the arguments here are just calculation of \(\tilde{A}, \tilde{B}\). Similarly, one can define the "Fourier transform" relatively any perfect difference set as well as a function from \(D\).

There is a general question about "Fourier coefficients" of subsets of \(\mathbb{F}_p\). Partial answer to the question give us the proof of the statements of sections 3, 4.

Suppose that \(A \subset \mathbb{F}_p\) is a set, and \(\chi\) is an arbitrary character. Consider the function
\[
E(x) = E_A(x) = E_{A,\chi}(x) := (A \circ \chi)(x).
\]
Alternatively, one can take convolutions of \(A\) with the function \(f\) above, that is \(\tilde{A}\). Our question is the following: what can we say nontrivial about the function \(E(x)\)? There is a list of simple properties of \(E(x)\). Clearly,
\[
\langle E_A \rangle = 0 \quad \text{and} \quad \|E_A\|_2^2 = p|A| - |A|^2.
\]

Higher moments of \(E\) can be estimated using Weil’s bound (4) and Lemma 2.1 as it was done in the proof of Corollary 2.6. Of course, there is the "cocycle" property of \(E(x)\), namely,
\[
E_A(xy) = \chi(x) E_{x^{-1}A}(y), \quad x \neq 0.
\]

In particular, it means that \(|E_A(x)|\) is fixed by the multiplier group of \(A\), that is the set \(\{x \in \mathbb{F}_p : xA = A\}\). Further,
\[
\sum_{x,y} \chi(x + y) A(x) E_A(y) = \sum_z (A \circ \chi)^2(z) = p|A| - |A|^2
\]
and hence
\[
|\sum_{x,y} \chi(x + y) A(x) E_A(y)| \gg \sqrt{p} \|E\|_2 \|E_A\|_2 \tag{76}
\]
provided by \(|A| \ll p\). In particular, formula (76) shows that inequality (13) of Lemma 2.4 is tight. Using estimate (61) and Lemma 5.2 one can easily prove an uncertainty principle for any function \(g\) (in particular for \(A\), namely
\[
p \left(1 + \frac{1}{\sqrt{p}}\right)^{-2} \leq |\text{supp } g| \cdot |\text{supp } \bar{g}|.
\]

If \(A\) is a Singer’s perfect difference set then the character \(\chi\) can be represented as the convolution \((A * E_{A,\chi})(x)\). Indeed
\[
(A * E_A)(x) = (A * (A \circ \chi))(x) = (\chi * (A \circ A))(x) = (\chi * (|A| - 1) \delta_0 + 1))(x) = (|A| - 1) \chi(x).
\]

Finally, the size of each level set
\[
L_c := \{x \in \mathbb{F}_p : E_A(x) = c\}, \quad c \in \mathbb{F}_p
\]
is bounded by \((p - 1)/2\) because of \(E(x) \pmod{p}\) is a nonzero polynomial from \(\mathbb{F}_p[x]\) of degree \((p - 1)/2\) with the leading term \(|A|x^{(p-1)/2}\). Are there further properties of \(E(x)\)? For example, what can we say about the maximum/minimum value of \(E(x)\)?

19
References

[1] Bachoc C., Matolcsi M., Rusza I.Z., Squares and differences sets in finite fields // arXiv:1305.0577v1 [math.CO] 2 May 2013.

[2] Berndt B. C., Evans R. J., Williams K. S., Gauss and Jacobi sums / Jonh Wiley & sons, 1997.

[3] Bollobas B., Random Graphs / CUP, Cambridge, 2001.

[4] Chang M.-C. On a question of Davenport and Lewis and new character sum bounds in finite fields // Duke Math. J., 145 (2008), 409–442.

[5] Cohen S.D. Clique numbers of Paley graphs // Quaestiones Math.11 (2) (1988), 225–231.

[6] Croot E., Lev V. Open problems in additive combinatorics // Additive combinatorics CRM Proc. Lecture Notes AMS, Providence, RI, 43 (2007), 207–233.

[7] Davenport H., Erdős P. The distribution of quadratic and higher residues // Publ. Math. Debrecen, 2 (1952), 252–265.

[8] Erdős P., Shapiro H.N. On the least primitive roots of a prime // Pacific J. Math., 7:1 (1957), 861–865.

[9] Graham S., Ringrose C. Lower bounds for least quadratic non-residues // Analytic Number Theory (Allterton Park, IL, 1989), 269–309.

[10] Hall M. Combinatorial Theory / California Institute of Technology, 1967.

[11] Johnsen J., On the distribution of powers in finite fields / J. Reine Angew. Math., 251 (1971) 10–19.

[12] Karatsuba A. A. Distribution of power residues and non-residues in additive sequences // Soviet Math. Dokl., 12 (1971), 235–235.

[13] Karatsuba A. A. The distribution of values of Dirichlet characters on additive sequences // Soviet Math. Dokl., 44:1 (1992), 145–148.

[14] Karatsuba A. A. Arithmetic problems in the theory of Dirichlet characters / Russ. Math. Surv., 63:4 (2008) 43–92.

[15] Rudin W. Fourier analysis on groups / Wiley 1990 (reprint of the 1962 original).

[16] Sárközy A. On additive decompositions of the set of the quadratic residues modulo p // Acta Arith. (to appear).

[17] Dartyge C., Sárközy A. On additive decompositions of the set of primitive roots modulo p // Monatsh. Math. (to appear).

[18] Schoen T., Shkredov I. D., Higher moments of convolutions, arXiv:1110.2986v2 [math.CO] 1 Nov 2011.
[19] Shkredov I. D., V’ugin I. V., On additive shifts of multiplicative subgroups, Mat. Sbornik, 203:6 (2012), 81–100.

[20] Shkredov I. D., Some new inequalities in additive combinatorics // arXiv:1208.2344v3 [math.CO].

[21] Shparlinksi I. E., Additive decompositions of subgroups of finite fields // arXiv:1301.2872v1 [math.NT] 14 Jan 2013.

[22] Tao T., Vu V. Additive combinatorics / Cambridge University Press 2006.

Division of Algebra and Number Theory,
Steklov Mathematical Institute,
ul. Gubkina, 8, Moscow, Russia, 119991
and
Delone Laboratory of Discrete and Computational Geometry,
Yaroslavl State University,
Sovetskaya str. 14, Yaroslavl, Russia, 150000
and
IITP RAS,
Bolshoy Karetny per. 19, Moscow, Russia, 127994
ilya.shkredov@gmail.com