On irregularities of distribution of binary sequences relative to arithmetic progressions, II. (Special sequences)

Cécile Dartyge, **Katalin Gyarmati** and **András Sárközy**
Eötvös Loránd University, Department of Algebra and Number Theory
H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary
E-mail: gykati@cs.elte.hu and sarkozy@cs.elte.hu

Abstract

In Part I of this paper we studied the irregularities of distribution of binary sequences relative to short arithmetic progressions. First we introduced a quantitative measure for this property. Then we studied the typical and minimal values of this measure for binary sequences of a given length. In this paper our goal is to give constructive bounds for these minimal values.

1 Introduction

First we recall some definitions and results from Part I of this paper [2].

K. F. Roth [12] was the first who studied the irregularities of distribution of sequences relative to arithmetic progressions. It follows from his results that

Theorem 1 (Roth [12]). *If $N, Q \in \mathbb{N}$ with $Q \leqslant N^{1/2}$ and $E_N = (e_1, e_2, ..., e_N) \in \{-1, +1\}^N$, then there are integers a, t, q such that*

$$1 \leqslant a \leqslant a + (t-1)q \leqslant N, \quad q \leqslant Q$$

2010 Mathematics Subject Classification: Primary 11K38, secondary 11B25.

Keywords and phrases: arithmetic progressions, irregularities of distribution, binary sequences.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K100291 and NK104183 and ....

and

$$\left|\sum_{j=0}^{t-1} e_{a+jq}\right| > c_1 Q^{1/2}$$

with some absolute constant c_1.

Binary sequences with strong pseudorandom properties play a crucial role in cryptography and elsewhere. Thus in [7] Mauduit and Sárközy initiated a new constructive and quantitative approach to study pseudorandomness of binary sequences

$$E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N. \tag{1}$$

Among others, in [7] they introduced the following measures of pseudorandomness of binary sequences:

Definition 1. The *well-distribution measure* of the binary sequence (1) is defined by

$$W(E_N) = \max_{a,b,t} \left|\sum_{j=0}^{t-1} e_{a+jb}\right|$$

where $a, b, t \in \mathbb{N}$ and $1 \leqslant a \leqslant a + (t-1)b \leqslant N$.

Definition 2. For $k \in \mathbb{N}$, $k \leqslant N$ the *correlation measure of order* k of the sequence (1) is defined as

$$C_k(E_N) = \max_{M,D} \left|\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k}\right|.$$

Then the sequence $E_N \in \{-1, +1\}^N$ is said to possess strong pseudorandom properties or, briefly, it is considered a "good" PR (= pseudorandom) sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for "small" k) are small. There are many papers written on these measures and constructions of "good" PR sequences, see Part I of this paper [2] for some related results and references.

We pointed out in Part I that in the applications one also needs binary sequences of form (1) such that their "short" but "not too short" subsequences

$$E_N(n, M) = (e_{n+1}, e_{n+2}, \ldots, e_{n+M}) \tag{2}$$

(say of length M with $N^{1-c} < M < N$ for some $c > 0$) also possess strong PR properties. Thus our goal is to look for binary sequences of this type. First in this series we focus on the measure W (and we will study C_k, resp. the combination of W and C_k later).

It follows from Theorem 1 and an upper bound estimate for $\min_{E_N\in\{-1,+1\}^N} W(E_N)$ given by Matoušek and Spencer [6] that for all $N \in \mathbb{N}$ we have

$$c_2 N^{1/4} < \min_{E_N\in\{-1,+1\}^N} W(E_N) < c_3 N^{1/4}. \tag{3}$$

Note that Matoušek and Spencer proved their upper bound by an existence proof, and no constructive proof is known. Indeed, the best known construction (presented in [4] in 1978) gives only

$$W(E_N) < c_4 N^{1/3} (\log N)^{2/3}. \tag{4}$$

In Part I first we introduced a weighted version W_α of the measure W for studying subsequences:

Definition 3. If E_N is the binary sequence E_N in (1) and $0 \leqslant \alpha \leqslant 1/2$, then the *weighted α-well-distribution measure* of E_N is defined as

$$W_\alpha(E_N) = \max_{0\leqslant n<n+M\leqslant N} M^{-\alpha} W(E_N(n,M)).$$

We also needed the following modification of this measure:

Definition 4. If E_N is the binary sequence E_N in (1) and $0 \leqslant \alpha \leqslant 1/2$, then the modified α-well-distribution measure of E_N is defined as

$$\overline{W}_\alpha(E_N) = \max_{0<M<N}\left(M^{-\alpha} \max_{1\leqslant a\leqslant a+(M-1)b\leqslant N} \left| \sum_{j=0}^{M-1} e_{a+jb} \right| \right).$$

Next we showed that for a truly random $E_N \in \{-1,+1\}^N$ the W_α measure of it is around $N^{1/2-\alpha}$ (we present this result here in a slightly simplified but less sharp form):

Theorem 2. *Assume that $0 \leqslant \alpha \leqslant 1/2$. Then for all $\varepsilon > 0$ there are numbers $N_0 = N_0(\varepsilon)$ and $\delta = \delta(\varepsilon)$ such that if $N > N_0$, then for a truly random sequence $E_N = \{-1,+1\}^N$ (i.e. choosing each $E_N \in \{-1,+1\}^N$ with probability $1/2^N$) we have*

$$P\left(\delta N^{1/2-\alpha} < W_\alpha(E_N) < 6N^{1/2-\alpha}(\log N)^{1/2}\right) > 1-\varepsilon.$$

Write

$$m_\alpha(N) = \min_{E_N\in\{-1,+1\}^N} W_\alpha(E_N)$$

and

$$\overline{m}_\alpha(N) = \min_{E_N\in\{-1,+1\}^N} \overline{W}_\alpha(E_N).$$

A trivial lower bound for $m_\alpha(N)$ is

$$m_\alpha(N) \gg N^{1/4-\alpha} \quad \textit{for all} \quad 0 \leqslant \alpha \leqslant 1/2. \tag{5}$$

We conjectured that much more is true:

Conjecture 1. *For $0 \leqslant \alpha \leqslant 1/2$ we have*

$$c_5 N^{1/4-\alpha/2} < m_\alpha(N) < c_6 N^{1/4-\alpha/2}. \tag{6}$$

Note that by (3) this is true for $\alpha = 0$. For $\alpha > 0$ we have not been able to improve on (5). Thus instead we proved two theorems which can be considered as partial results towards the lower bound part of this conjecture: first we gave a lower bound for $\overline{m}_\alpha(N)$, and then we proved a lower bound for $\overline{W}_\alpha(E_N)$ from which it follows that for almost all $E_N \in \{-1,+1\}^N$ the W_α measure of E_N is greater than the lower bound in (6) divided by a logarithm factor:

$$W_\alpha(E_N) \gg \frac{N^{1/4-\alpha/2}}{(\log N)^{1/4-\alpha/2}}.$$

In this paper our goal is to study certain *special sequences E_N with small values of $W_\alpha(E_N)$*. First in Section 2 we will show that the Rudin–Shapiro sequence possesses small W_α measure for all α. Then in Sections 3 and 4 we will give upper bounds for small values of W_α in case of Legendre symbol sequences. Finally, in Section 5 we will give lower bound for W_α for the Legendre symbol construction.

2 Upper bound for small values of W_α uniformly in α for the Rudin–Shapiro sequence

Unfortunately, we have not been able to prove that the upper bound in (3) can be extended to the case of general α as presented in Conjecture 1; namely, we have not been able to extend the *existence* proof given by Matoušek and Spencer in [6]. On the other hand, we will be able to extend and sharpen the *constructive* upper bound (4) in various directions by giving *constructive* proofs. First in this section we will give a partial answer to the questions asked at the end of Section 1 in [2]: we will show that the truncated Rudin–Shapiro sequence is well-distributed in short blocks of consecutive elements of it, in other words, W_α is small *uniformly in* α for this sequence.

The Rudin–Shapiro [13], [15] sequence plays a role of basic importance in harmonic analysis. Its definition is the following:

First we define pairs of polynomials $P_{2^n}(z)$, $Q_{2^n}(z)$ $(n = 0, 1, 2, \dots)$ of degree $2^n - 1$ by the following recursion: Let

$$P_1(z) = Q_1(z) = 1,$$

and if $P_{2^n}(z)$ and $Q_{2^n}(z)$ have been defined for a non-negative integer n, then let

$$P_{2^{n+1}}(z) = P_{2^n}(z) + z^{2^n} Q_{2^n}(z) \quad \text{and} \quad Q_{2^{n+1}}(z) = P_{2^n}(z) - z^{2^n} Q_{2^n}(z). \tag{7}$$

It can be shown easily by induction on n that

$$\left|P_{2^n}(z)\right|^2 + \left|Q_{2^n}(z)\right|^2 = 2^{n+1} \quad \text{for} \quad n = 0, 1, 2, \dots \quad \text{and all } |z| = 1$$

whence

$$\left|P_{2^n}(z)\right| \leqslant \sqrt{2}\cdot 2^{n/2} \text{ and } \left|Q_{2^n}(z)\right| \leqslant \sqrt{2}\cdot 2^{n/2} \text{ for } n = 0, 1, 2, \dots \text{ and all } |z| = 1.$$

It follows from these upper bounds and the Parseval formula that the maximum of the polynomials $P_{2^n}(z)$, $Q_{2^n}(z)$ on the unit circle is less than a constant multiple of their mean square; this is the most important property of these polynomials.

Clearly, the construction above defines a unique binary sequence $R = (r_0, r_1, \dots) \in \{-1, +1\}^\infty$ such that

$$P_{2^n}(z) = \sum_{j=0}^{2^n-1} r_j z^j \quad \text{for } n = 0, 1, 2, \dots;$$

this sequence R is called Rudin–Shapiro sequence. Its elements have the following properties:

$$\begin{aligned} r_0 &= 1, \\ r_{2n} &= r_n \qquad (\text{for } n = 1, 2, \dots), \\ r_{2n+1} &= (-1)^n r_n \quad (\text{for } n = 0, 1, 2, \dots) \end{aligned}$$

and

$$r_{2^{n+1}a+b} = r_a r_b \qquad \text{for non-negative integers } a, b \text{ and } n \text{ such that } b < 2^n.$$

(Their proofs and further formulas can be found in [11].)

Write $R_N = (r_0, r_1, \dots, r_{N-1})$. Denote the coefficients of the polynomial $Q_{2^n}(z)$ by $s_0, s_1, \dots, s_{2^n-1}$ so that $Q_{2^n}(z) = \sum_{j=0}^{2^n-1} s_j z^j$, and write $S_{2^n} = (s_0, s_1, \dots, s_{2^n-1})$. Then by (7) we have

$$\sum_{j=0}^{2^n-1} r_j z^j + z^{2^n} \sum_{i=0}^{2^n-1} s_i z^i = \sum_{j=0}^{2^n-1} r_j z^j + \sum_{i=0}^{2^n-1} s_i z^{2^n+i} = \sum_{j=0}^{2^{n+1}-1} r_j z^j$$

whence

$$S_{2^n} = \left(s_0, s_1, \dots, s_{2^n-1}\right) = \left(r_{2^n}, r_{2^n+1}, \dots, r_{2^{n+1}-1}\right). \tag{8}$$

Mauduit and Sárközy [8] proved that

Theorem 3 (Mauduit and Sárközy [8])**.** *We have*

$$W(R_N) \leqslant 2(2+\sqrt{2})N^{1/2} \quad \textit{for all} \quad N \in \mathbb{N}.$$

We will also need

Corollary 1. *For all n*

$$W(S_{2^n}) \leqslant 4\big(\sqrt{2}+1\big)2^{n/2} \quad \textit{for} \quad n = 0, 1, 2, \dots.$$

Proof of Corollary 1. In the remaining sections we will use some facts which are nearly trivial. We will call these facts propositions, and in some cases we will give a hint, but we will always omit the details.

Proposition 1. *If a binary sequence $D_{M+N} \in \{-1,+1\}^{M+N}$ is the concatenation of the sequences $A_M = (a_1, a_2, \dots, a_M)$ and $B_N = (b_1, b_2, \dots, b_N)$: $D_{M+N} = (a_1, \dots, a_M, b_1, \dots, b_N)$, then we have*

$$\max\big(W(A_M), W(B_N)\big) \leqslant W(D_{M+N}).$$

All the sums $a_x + a_{x+y} + \dots + a_{x+ty}$ considered when computing $W(A_M)$ are also considered when computing $W(D_{M+N})$.

By (8), $R_{2^{n+1}} = \big(r_0, r_1, \dots, r_{2^n-1}, r_{2^n}, r_{2^n+1}, \dots, r_{2^{n+1}-1}\big)$ is a concatenation of R_{2^n} and S_{2^n} thus by Proposition 1 and Theorem 3 we have

$$W\big(S_{2^n}\big) \leqslant W\big(R_{2^{n+1}}\big) \leqslant 2\big(2+\sqrt{2}\big)2^{(n+1)/2} = 4\big(\sqrt{2}+1\big)2^{n/2}$$

which proves the corollary. □

Now we are ready to prove our main result in this section:

Theorem 4. *Let $N \in \mathbb{N}$, and for $n \in \{0, 1, \dots\}$, $M \in \mathbb{N}$, $0 \leqslant n < n+M \leqslant N$ write $R_N(n, M) = (r_n, r_{n+1}, \dots, r_{n+M-1})$. Then for each of these pairs (n, M) we have*

$$W(R_N(n, M)) < 40M^{1/2}. \tag{9}$$

It follows trivially from this theorem that

Corollary 2. *For all $0 \leqslant \alpha \leqslant 1/2$ and every $N \in \mathbb{N}$ we have*

$$W_\alpha(R_N) < 40N^{(1/2)-\alpha}, \tag{10}$$

in particular,

$$W_{1/2}(R_N) < 40.$$

By (9), the Rudin–Shapiro sequence completely satisfies the requirement formulated at the end of Section 1 of [2] as far as the measure W is concerned: for every subsequence of length M the measure W is $\ll M^{1/2}$, we could not expect better than that.

Proof of Theorem 4. We will need

Proposition 2. *If a, t are any non-negative integers, then $\big(r_{a2^t}, r_{a2^t+1}, \ldots, r_{(a+1)2^t-1}\big)$ is one of the 4 sequences R_{2^t}, $-R_{2^t}$ $\big(= \big(-r_0, -r_1, \ldots, -r_{2^t-1}\big)\big)$, S_{2^t}, $-S_{2^t}$.*

This follows from the recursive formula (7).

Proposition 3. *Let $E_N = (e_1, e_2, \ldots, e_N) \in \{-1, +1\}^N$ and $1 \leqslant n_0 < n_1 < \cdots < n_k \leqslant N+1$, and write*

$$E_N^{(i)} = \big(e_{n_i}, e_{n_{i+1}}, \ldots, e_{n_{i+1}-1}\big) \quad \text{for } i = 0, 1, \ldots, k-1$$

and $E_N(n_0, n_k - 1) = \big(e_{n_0}, e_{n_0+1}, \ldots, e_{n_k-1}\big)$. Then we have

$$W\big(E_N(n_0, n_k-1)\big) \leqslant \sum_{i=0}^{k-1} W(E_N^{(i)}).$$

On the left-hand side we have the absolute value of the greatest sum $\sum\limits_j e_{a+jb}$ where the subscripts $a+jb$ form an arithmetic progression contained in $(n_0, n_0+1, \ldots, n_k-1)$. The numbers $n_1, n_2, \ldots, n_{k-1}$ split this arithmetic progression into at most k pieces, and the absolute values of the sums over these pieces can be estimated by $W(E_N^{(1)}), W(E_N^{(2)}), \ldots, W(E_N^{(k)})$. It remains to refer to the triangle inequality.

Now we are ready to prove (9). Define the integer t by $M/2 < 2^t < M$. There is an integer m with $2^t \mid m$ which belongs to the set $\mathcal{H} = \{n, n+1, \ldots, n+M-1\}$. Write $m_i = m + i2^t$ for $i = -2$, -1, 0 and 1, but we drop m_i if it is negative. For the remaining (at most 4) m_i's we form the sequence $R^{(i)} = \big(r_{m_i}, r_{m_i+1}, r_{m_i+2}, \ldots, r_{m_i+2^t-1}\big)$. Each of these sequences is of the form described in Proposition 2 and their concatenation includes the subsequence $R_N(n, M)$, thus by Propositions 1, 2 and 3, Theorem 3 and Corollary 1 we have

$$\begin{aligned} W(R_N(n,M)) &\leqslant \sum_{-2\leqslant i\leqslant 1} W(R^{(i)}) = \sum_{-2\leqslant i\leqslant 1} W\big(R_N(m_i, 2^t)\big) \leqslant \\ &\leqslant \sum_{-2\leqslant i\leqslant 1} \max\big(W(R_{2^t}), W(S_{2^t})\big) \leqslant 4\cdot 4\big(\sqrt{2}+1\big)2^{t/2} < 40M^{1/2} \end{aligned}$$

which completes the proof of Theorem 4. □

We have seen that the behaviour of the measure W is completely satisfactory for the truncated Rudin–Shapiro sequence. On the other hand, in case of the correlation measure the situation is just the opposite. Indeed, by Theorem 3 in [8] we have

Theorem 5. *For $N \in \mathbb{N}$ and $N \geqslant 4$ we have*

$$C_2(R_N) > \frac{1}{6}N.$$

Thus if we want to make $W_\alpha(E_N)$ and the correlation measures $C_k(E_N)$ small simultaneously, then we have to look for a different sequence. We will return to this problem in a subsequent paper.

3 Upper bounds for small values of W_α for fixed α by using the Legendre symbol

Recall from Section 1 that by (3) we have

$$m_0(N) = \min_{E_N \in \{-1,+1\}^N} W(E_N) < c_3 N^{1/4}$$

and this is sharp apart from the value of the constant c_3 but the proof of this is an existence proof. The best known construction presented in 1978 in [4] gives only the much weaker bound in (4), and since that no improvement has been made on this estimate. This upper bound was achieved by considering the following construction:

If $N \in \mathbb{N}$ and p is a prime with $p \leqslant N$, then define the sequence $E_N^p = (e_1, e_2, \ldots, e_N)$ by

$$e_n = \begin{cases} \left(\frac{n}{p}\right) & \text{for } p \nmid n, \\ +1 & \text{for } p \mid n \end{cases} \qquad (\text{for all } 1 \leqslant n \leqslant N) \tag{11}$$

where $\left(\frac{n}{p}\right)$ denotes the Legendre symbol. Choosing here p as the greatest prime p with $p < \left(\frac{N}{\log N}\right)^{2/3}$, it is easy to see by using the Pólya–Vinogradov inequality [10], [16] that this sequence satisfies (4) with E_N^p in place of E_N.

First we will extend this construction to estimate small values of W_α for any *fixed* α, and we will also improve on it slightly (in particular, we will be able to remove the logarithm factor from (4)).

Theorem 6. *For every α with $0 \leqslant \alpha \leqslant 1/2$ there is a number $N_0 = N_0(\alpha)$ such that if $N \in \mathbb{N}$, $N > N_0$ then there is a prime p with*

$$\frac{1}{2}N^{\frac{2(1-\alpha)}{3}} < p \leqslant N^{\frac{2(1-\alpha)}{3}} \tag{12}$$

so that for the sequence E_N^p defined by (11) we have

$$W_\alpha(E_N^p) < c_5 N^{\frac{1-\alpha}{3}} \tag{13}$$

where c_5 is an absolute constant (independent of α).

Compare this upper bound with the upper bound for $W_\alpha(R_N)$ in (10): in (10) the exponent of N is $\frac{1}{2} - \alpha$ while here in (13) the exponent is $\frac{1-\alpha}{3}$ which is smaller than $\frac{1}{2} - \alpha$ for $0 \leqslant \alpha < 1/4$.

In the $\alpha = 0$ special case we get from Theorem 6 that

Corollary 3. *For $N \in \mathbb{N}$, $N > N_0$ there is a prime p with*

$$\frac{1}{2}N^{2/3} < p \leqslant N^{2/3}$$

such that for the sequence E_N^p we have

$$W(E_N^p) = W_0(E_N^p) < c_5 N^{1/3}.$$

(Indeed, this is better than (4) by a factor $(\log N)^{2/3}$.)

Proof of Theorem 6. The proof will be based on a result of Montgomery and Vaughan [9]:

Lemma 1. *There is an absolute constant c_6 such that for $N \in \mathbb{N}$, $N \geqslant 2$ there is a prime p satisfying*

$$\frac{N}{2} < p \leqslant N$$

and

$$\left| \sum_{n=X+1}^{X+Y} \left(\frac{n}{p}\right) \right| < c_6 p^{1/2} \quad \text{for all } \ X \in \mathbb{Z},\ Y \in \mathbb{N}. \tag{14}$$

(Here and in the rest of this paper we define $\left(\frac{n}{p}\right) = 0$ for $p \mid n$.)

Proof of Lemma 1. This follows from (ii) in the Corollary in [9] by taking any $\theta > 1/2$ there (and using also the prime number theorem). □

For $Y \in \mathbb{N}$ write

$$d(p,Y) = \max_{X\in\mathbb{Z}} \left| \sum_{n=X+1}^{X+Y} \left(\frac{n}{p}\right) \right|. \tag{15}$$

We will also need

Lemma 2. *If $M, N \in \mathbb{N}$, $n \in \{0,1,\dots,N-1\}$, $n+M \leqslant N$ and p is a prime with $p \leqslant N$, then we have*

$$W\big(E_N^p(n,M)\big) \leqslant \max_{Y\leqslant M} d(p,Y) + \frac{2M}{p} + 2. \tag{16}$$

Proof of Lemma 2. By the definitions of $W(E_N)$, $E_N^p = (e_1, e_2, \dots, e_N)$ and $E_N(n,M)$ we have

$$\begin{aligned} W\big(E_N^p(n,M)\big) &= \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| = \\ &= \max_{a,b,t} \left| \sum_{j=0}^{t-1} \left(\frac{a+jb}{p}\right) + \sum_{\substack{0\leqslant j<t \\ p\mid a+jb}} 1 \right| \end{aligned} \tag{17}$$

where $a, b, t \in \mathbb{N}$ and

$$n+1 \leqslant a \leqslant a+(t-1)b \leqslant n+M. \tag{18}$$

It follows from (18) that

$$(t-1)b = (a+(t-1)b) - a \leqslant (n+M) - (n+1) = M-1 \tag{19}$$

whence

$$t \leqslant \frac{M-1}{b} + 1 < \frac{M}{b} + 1 \leqslant M+1$$

so that

$$t \leqslant M. \tag{20}$$

If $(b,p) = 1$ then by the definition of $d(p,Y)$ and (20) we have

$$\begin{aligned} &\left| \sum_{j=0}^{t-1} \left(\frac{a+jb}{p}\right) + \sum_{\substack{0\leqslant j<t \\ p\mid a+jb}} 1 \right| \leqslant \\ &\leqslant \left| \sum_{j=0}^{t-1} \left(\frac{a+jb}{p}\right) \right| + \sum_{\substack{0\leqslant j<t \\ p\mid a+jb}} = 1 = \end{aligned}$$

$$= \left|\sum_{j=0}^{t-1}\left(\frac{ab^{-1}+j}{p}\right)\right| + \left|\{j:\ jb \equiv -a \pmod p,\ 0 \leqslant j < t\}\right| \leqslant$$

$$\leqslant d(p,t) + \left(\frac{t}{p}+1\right) \leqslant \max_{t\leqslant M} d(p,t) + \frac{M}{p} + 1 \quad (\text{for } (b,p)=1). \tag{21}$$

If $(b,p) > 1$ then we have $b \geqslant p$ thus it follows from (19) that

$$(t-1)p \leqslant (t-1)b \leqslant M-1$$

whence

$$t \leqslant \frac{M-1}{p} + 1 < \frac{M}{p} + 1.$$

Thus we have

$$\left|\sum_{j=0}^{t-1}\left(\frac{a+jb}{p}\right) + \sum_{\substack{0\leqslant j<t\\ p|a+jb}} 1\right| \leqslant 2\sum_{j=0}^{t-1} 1 = 2t < \frac{2M}{p} + 2 \quad (\text{for } (b,p) > 1). \tag{22}$$

(16) follows from (17), (21) and (22) which completes the proof of the lemma. □

In order to prove the statement of the theorem we use Lemma 1 with $N^{\frac{2(1-\alpha)}{3}}$ in place of N. We get for N large enough that there is a prime p satisfying (12) such that (14) holds. Then by the definition of W_α, (12), (14), (15) and Lemma 2 we have

$$\begin{aligned} W_\alpha(E_N^p) &= \max_{0\leqslant n<n+M\leqslant N} M^{-\alpha} W\big(E_N^p(n,M)\big) \leqslant \\ &\leqslant \max_{0\leqslant n<n+M\leqslant N} M^{-\alpha}\left(\max_{Y\leqslant M} d(p,Y) + 2\frac{M}{p} + 2\right) \leqslant \\ &\leqslant \max_{M\leqslant N} M^{-\alpha}\left(c_6 p^{1/2} + 2\frac{M}{p} + 2\right) < \\ &< \max_{M\leqslant N} c_7\left(p^{1/2} + \frac{M^{1-\alpha}}{p}\right) \leqslant c_7\left(p^{1/2} + \frac{N^{1-\alpha}}{p}\right) < c_8 N^{\frac{1-\alpha}{3}} \end{aligned} \tag{23}$$

which completes the proof of Theorem 6. □

For $0 < \alpha\ (\leqslant 1/2)$ one can improve further on the upper bound in (13) by using the Burgess inequality:

Theorem 7. *For every α with $0 \leqslant \alpha \leqslant 1/2$ there is a number $N_1 = N_1(\alpha)$ such that if $N \in \mathbb{N}$, $N > N_1$ and p is a prime which satisfies the inequalities in Lemma 1 with $N^{\frac{8(1-\alpha)}{12-5\alpha}}(\log N)^{-\frac{8\alpha}{12-5\alpha}}$ in place of N:*

$$\frac{1}{2}N^{\frac{8(1-\alpha)}{12-5\alpha}}(\log N)^{-\frac{8\alpha}{12-5\alpha}} < p \leqslant N^{\frac{8(1-\alpha)}{12-5\alpha}}(\log N)^{-\frac{8\alpha}{12-5\alpha}} \tag{24}$$

and (14) *holds, then we have*

$$W_\alpha(E_N^p) < c_9 N^{\frac{(1-\alpha)(4-5\alpha)}{12-5\alpha}} (\log N)^{\frac{8\alpha}{12-5\alpha}} \tag{25}$$

where c_9 *is an absolute constant (independent of* α*).*

Observe that the exponent $\frac{(1-\alpha)(4-5\alpha)}{12-5\alpha}$ in the upper bound in (25) is smaller than the exponent $\frac{1-\alpha}{3}$ in (13) in Theorem 6 for all $0 < \alpha$ (in particular, for $\alpha = 1/2$ these exponents are $\frac{3}{38}$ and $\frac{1}{6}$, respectively).

Proof of Theorem 7. By the Burgess inequality [1] we have

Lemma 3. *If* p *is a prime number and* $H \in \mathbb{N}$, $r \in \mathbb{N}$ *then*

$$d(p,H) = \max_{X \in \mathbb{Z}} \left| \sum_{n=X+1}^{X=H} \left(\frac{n}{p}\right) \right| < c_{10} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{1/r}$$

where c_{10} *is an absolute constant.*

(Here $c_{10} = 30$ can be taken [17].)

In order to estimate $W_\alpha(E_N^p)$ in the theorem again we use Lemma 2:

$$\begin{aligned} W_\alpha(E_N^p) &= \max_{0 \leqslant n < n+M \leqslant N} M^{-\alpha} W\big(E_N^p(n,M)\big) \leqslant \\ &\leqslant \max_{M \leqslant N} M^{-\alpha} \left(\max_{H \leqslant M} d(p,H) + 2\frac{M}{p} + 2 \right) \leqslant \\ &\leqslant \max_{M \leqslant N} \left(M^{-\alpha} \max_{H \leqq M} d(p,H) + 2\frac{M^{1-\alpha}}{p} + 2M^{-\alpha} \right) \leqq \\ &\leqslant \max_{M \leqslant N} \left(M^{-\alpha} \max_{H \leqslant M} d(p,H) \right) + 4\frac{N^{1-\alpha}}{p} \end{aligned} \tag{26}$$

since we have $p < N^{1-\alpha}$ by the upper bound for p in (24) and $\alpha \leqslant 1/2$. By $\alpha \geqslant 0$ here we have

$$\begin{aligned} \max_{M \leqslant N} \left(M^{-\alpha} \max_{H \leqslant M} d(p,H) \right) &\leqslant \max_{H \leqslant N} d(p,H) \max_{H \leqslant M \leqslant N} M^{-\alpha} = \\ &= \max_{H \leqslant N} H^{-\alpha} d(p,H) = \max_{H \leqslant N} F(H) \end{aligned} \tag{27}$$

where $F(H) = H^{-\alpha} d(p,H)$.

It remains to estimate $F(H)$ for $H \in (0, N]$. To do this, we split the interval $(0, N]$ into subintervals. To define these subintervals we introduce the following notations:

Let R be a positive integer large enough in terms of α which will be fixed later. Let $t_1 = N$, $t_2 = p^{5/8}(\log p)^{-1}$,

$$t_r = p^{\frac{r^2+r-1}{4(r-1)r}} \log p \quad \text{for} \quad r = 3, 4, \dots, R+1$$

and $t_{R+2} = 0$ (where p is the prime p defined in the theorem). A simple computation shows that if N is large enough (in terms of α), then we have

$$0 = t_{R+2} < t_{R+1} < \cdots < t_2 < t_1 = N. \tag{28}$$

Let $I_r = (t_{r+1}, t_r]$ for $r = 1, 2, \dots, R+1$. Then it follows from (28) that the interval $(0, N]$ is a disjoint union of the intervals I_r:

$$(0, N] = \bigcup_{i=1}^{R+1} I_r, \quad I_r \cap I_{r'} = \varnothing \quad \text{for} \quad 1 \leqslant r < r' \leqslant R+1. \tag{29}$$

First for $H \in I_1$ we estimate $F(H)$ by (14):

$$\begin{aligned} F(H) = H^{-\alpha} d(p, H) < t_2^{-\alpha} c_6 p^{1/2} = c_6 p^{-5\alpha/8} (\log p)^{\alpha} p^{1/2} = \\ = c_6 p^{1/2 - 5\alpha/8} (\log p)^{\alpha} = c_6 G(1) = c_6 p^{u_1} (\log p)^{v_1} \quad (\text{for} \quad H \in I_1) \end{aligned} \tag{30}$$

with $G(1) = p^{u_1}(\log p)^{v_1}$, $u_1 = 1/2 - 5\alpha/8$, $v_1 = \alpha$.

For H belonging to the r-th interval $I_r = (t_{r+1}, t_r]$ with $1 < r < R+1$ we use the Burgess inequality in Lemma 3 with this r (indeed, I_r is defined so that this r value should give the optimal bound):

$$F(H) = H^{-\alpha} d(p, H) < c_{10} H^{-\alpha} H^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{1/r} = c_{10} H^{1-\alpha-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{1/r}.$$

By $\alpha \leqslant 1/2$ the exponent of H is non-negative, thus we get

$$F(H) < c_{10} t_r^{1-\alpha-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{1/r}$$

whence for $r = 2$ we have

$$\begin{aligned} F(H) < c_{10} t_2^{1/2-\alpha} p^{3/16} (\log p)^{1/2} = \\ = c_{10} p^{5/16 - 5\alpha/8} (\log p)^{\alpha - 1/2} p^{3/16} (\log p)^{1/2} = \\ = c_{10} p^{1/2 - 5\alpha/8} (\log p)^{\alpha} = c_{10} G(2) = c_{10} p^{u_2} (\log p)^{v_2} \quad (\text{for } H \in I_2) \end{aligned} \tag{31}$$

with $G(2) = p^{u_2}(\log p)^{v_2}$, $u_2 = \frac{1}{2} - \frac{5\alpha}{8}$ and $v_2 = \alpha$, while for $2 < r < R+1$ we get

$$F(H) < c_{10} \Big(p^{\frac{r^2+r-1}{4(r-1)r}} \log p \Big)^{1-\alpha-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\frac{1}{r}} =$$

$$= c_{10} p^{\frac{r+2}{4r} - \alpha \frac{r^2+r-1}{4(r-1)r}} (\log p)^{1-\alpha} = c_{10} G(r) =$$
$$= c_{10} p^{u_r} (\log p)^{v_r} \quad (\text{for } \ H \in I_r, \ 2 < R < R+1) \tag{32}$$

with $G(r) = p^{u_r}(\log p)^{v_r}$, $u_r = \frac{r+2}{4r} - \alpha \frac{r^2+r-1}{4(r-1)r}$ and $v_r = 1 - \alpha$.

Finally, for $H \in I_{R+1}$ we use the trivial estimate

$$F(H) = H^{-\alpha} d(p, H) \leqslant H^{-\alpha} H = H^{1-\alpha} \leqslant t_{R+1}^{1-\alpha} =$$
$$= \left(p^{\frac{R^2+3R+1}{4R(R+1)}} \right)^{1-\alpha} (\log p)^{1-\alpha} =$$
$$= G(R+1) = p^{u_{R+1}} (\log p)^{v_{R+1}} \quad (\text{for } H \in I_{R+1}) \tag{33}$$

with $G(R+1) = p^{u_{R+1}}(\log p)^{v_{R+1}}$, $u_{R+1} = \frac{R^2+3R+1}{4R(R+1)}(1-\alpha)$, $v_{R+1} = 1 - \alpha$.

By (30) and (31) we have

$$G(1) = G(2) = p^{1/2 - 5\alpha/8} (\log p)^{\alpha}. \tag{34}$$

For $2 \leqslant r < R$ we have

$$u_r - u_{r+1} = \left(\frac{r+2}{4r} - \alpha \frac{r^2+r-1}{4(r-1)r} \right) - \left(\frac{r+3}{4(r+1)} - \alpha \frac{r^2+3r+1}{4r(r+1)} \right) =$$
$$= \frac{1}{2r(r+1)} - \alpha \frac{1}{2(r-1)(r+1)} = \frac{(1-\alpha)r - 1}{2(1-r)r(r+1)}$$

whence

$$u_r \begin{cases} > u_{r+1} & \text{for } \alpha < 1/2 \text{ or } \alpha = 1/2, \ r > 2, \\ = u_{r+1} & \text{for } \alpha = 1/2, \ r = 2, \end{cases} \tag{35}$$

and clearly

$$v_r = v_{r+1} \quad \text{for } \ r = 2, \ \alpha = 1/2. \tag{36}$$

It follows from (34), (35) and (36) that

$$p^{1/2 - 5\alpha/8} (\log p^{\alpha}) = G(1) = G(2) \geqslant G(3) > G(4) > \cdots > G(R). \tag{37}$$

By (33), for $R \to \infty$ clearly we have

$$G(R+1) = p^{\left(\frac{1}{4} + o(1)\right)(1-\alpha)} \quad (\text{for } \ R \to \infty). \tag{38}$$

Comparing the exponents of p in (37) and (38), we get that

$$\frac{1}{2} - \frac{5}{8}\alpha > \frac{1}{4}(1-\alpha)$$

by $\alpha \leqslant 1/2$. Thus it follows from (37) and (38) that for every R large enough we have

$$G(R+1) < G(1). \tag{39}$$

Now we fix the value of R: let R be the smallest integer R with $R > 2$ for which (39) holds. Then it follows from (26), (27), (29), (30), (31), (32), (33), (37) and (39) that

$$W_\alpha(E_N^p) < c_{11} p^{1/2-5\alpha/8} (\log p)^\alpha + 4\frac{N^{1-\alpha}}{p} \tag{40}$$

whence (25) follows using that the prime p satisfies (24) (note that this choice of p balances the two terms in (40)) and this completes the proof of Theorem 7. □

4 Upper bounds under hypothesis for the Legendre symbol construction

In Section 3 we estimated $W_\alpha(E_N^p)$ for the Legendre symbol sequence E_N^p in (11) by using the best known estimates for Legendre symbol sums. However, these estimates are probably very far from being sharp so that $W_\alpha(E_N^p)$ is much smaller than our upper bounds. Thus it seems worth to study what upper bound can be given for $W_\alpha(E_N^p)$ having a plausible hypothesis on the size of Legendre symbol sums? Such a hypothesis was formulated, e.g., by L. Zhao in [17]: If χ is a non-principal character modulo a prime number p and we set

$$S_\chi(N) = \sum_{M < n \leqslant M+N} \chi(n),$$

then "the expected bound is

$$S_\chi(N) \ll \sqrt{N}\, p^\varepsilon." \tag{41}$$

We will call (41) hypothesis H, and we will estimate $W_\alpha(E_N^p)$ under this hypothesis.

Theorem 8. *Assume that hypothesis H holds with* $\chi(n) = \left(\frac{n}{p}\right)$, *i.e., for every* $\varepsilon > 0$ *there is a number* $p_0 = p_0(\varepsilon)$ *such that for every prime* $p > p_0$ *we have*

$$d(p, Y) = \max_{X \in \mathbb{Z}} \left| \sum_{n=X+1}^{X+Y} \left(\frac{n}{p}\right) \right| \ll Y^{1/2} p^\varepsilon \ (\textit{for all } p > p_0 \textit{ and } Y \in \mathbb{N}). \tag{42}$$

Then for every α and ε with $0 \leqslant \alpha \leqslant 1/2$ and $\varepsilon > 0$ there is a number $N_0 = N_0(\alpha, \varepsilon)$ such that if $N \in \mathbb{N}$, $N > N_0$, then there is a prime p with

$$\frac{1}{2} N^{\frac{2-2\alpha}{3-2\alpha}} < p \leqslant N^{\frac{2-2\alpha}{3-2\alpha}} \quad \left(\leqslant N^{1-\alpha}\right) \tag{43}$$

so that for the sequence E_N^p defined by (11) we have

$$W_\alpha(E_N^p) < N^{\frac{(1-\alpha)(1-2\alpha)}{3-2\alpha}+\varepsilon}. \tag{44}$$

Note that the exponent $\frac{(1-\alpha)(1-2\alpha)}{3-2\alpha}$ in this upper bound is significantly smaller than the exponent $\frac{(1-\alpha)(4-5\alpha)}{12-5^\alpha}$ in (25).

Proof of Theorem 8. By Lemma 1 there is a prime p satisfying (43) with

$$\max_{Y \in \mathbb{N}} d(p, Y) = \max_{Y \in \mathbb{N}} \max_{X \in \mathbb{Z}} \left| \sum_{n=X+1}^{X+Y} \left(\frac{n}{p}\right) \right| < c_6 p^{1/2}. \tag{45}$$

We will show that for this prime p the sequence E_N^p satisfies (44).

As in (23), by Lemma 2, (42), (43) and (45) we have

$$\begin{aligned}
W_\alpha(E_N^p) &= \max_{0 \leqslant n < n+M \leqslant N} M^{-\alpha} W\left(E_N^p(n, M)\right) \leqslant \\
&\leqslant \max_{1 \leqslant M \leqslant N} M^{-\alpha} \left(\max_{Y \leqslant M} d(p, Y) + 2\frac{M}{p} + 2 \right) \leqslant \\
&\leqslant \max_{1 \leqslant M \leqslant N} M^{-\alpha} \left(\max_{Y \leqslant M} \min\left(Y^{1/2} p^\varepsilon, c_6 p^{1/2}\right) + 2\frac{M}{p} + 2 \right) \leqslant \\
&\leqslant \max_{1 \leqslant M \leqslant p^{1-2\varepsilon}} M^{-\alpha} \max_{Y \leqslant M} \min\left(Y^{1/2} p^\varepsilon, c_6 p^{1/2}\right) + \\
&\quad + \max_{p^{1-2\varepsilon} < M \leqslant N} M^{-\alpha} \max_{Y \leqslant M} \min\left(Y^{1/2} p^\varepsilon, c_6 p^{1/2}\right) + \\
&\quad + \max_{1 \leqslant M \leqslant N} M^{-\alpha} \left(2\frac{M}{p} + 2 \right) \leqslant \\
&\leqslant \max_{1 \leqslant M \leqslant p^{1-2\varepsilon}} M^{1/2-\alpha} p^\varepsilon + \max_{p^{1-2\varepsilon} < M \leqslant N} M^{-\alpha} c_6 p^{1/2} + 2\left(\frac{N^{1-\alpha}}{p} + 1\right) \ll \\
&\ll p^{(1-2\varepsilon)(1/2-\alpha)+\varepsilon} + p^{-\alpha(1-2\varepsilon)+1/2} + \frac{N^{1-\alpha}}{p} \ll \\
&\ll p^{-\alpha(1-2\varepsilon)+1/2} + \frac{N^{1-\alpha}}{p} = p^{1/2-\alpha} p^{2\alpha\varepsilon} + \frac{N^{1-\alpha}}{p} \leqslant \\
&\leqslant p^{1/2-\alpha} N^\varepsilon + \frac{N^{1-\alpha}}{p} \leqslant
\end{aligned}$$

$$\leqslant N^{\frac{(1-\alpha)(1-2\alpha)}{3-2\alpha}+\varepsilon} + N^{\frac{(1-\alpha)(1-2\alpha)}{3-2\alpha}}$$

(observe that by choosing p in the interval (43) the two terms have been balanced apart from an N^{ε} factor) whence (44) follows. □

5 Lower bound for W_α for the Legendre symbol construction

In this section our goal is to give a lower bound for W_α for the Legendre symbol sequence E_{p-1}^p defined as in (11):

$$E_{p-1}^p = \left(\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots, \left(\frac{p-1}{p}\right)\right). \tag{46}$$

Such a lower bound follows easily from a result of Sárközy ([14] Corollary 4, proved there by adapting Roth's method applied in the proof of his result presented as Theorem 1 above) which was also used in Part I of this paper. In this way one gets

$$W_\alpha(E_{p-1}^p) \gg 2^\alpha p^{1/4-\alpha/2} \tag{47}$$

for all $0 \leqslant \alpha \leqslant 1/2$. However, by using a recent result of Gong [5], we will be able to improve on this estimate significantly:

Theorem 9. *Let p be a prime with $p > 2$, and define the sequence E_{p-1}^p by (46). Then for all $0 \leqslant \alpha \leqslant 1/2$ we have*

$$W_\alpha(E_{p-1}^p) > \frac{1}{10} p^{1/2-\alpha}.$$

Note that the exponent on the right-hand side is the double of the exponent in the upper bound in (6) and in (47), and comparison with Theorem 2 shows that the order of magnitude of W_α for the Legendre symbol sequence is at least as large as for a random sequence of the same length.

Proof of Theorem 9. Throughout the proof we will identify $\mathbb{F}_p$ with the field of the modulo p residue classes, and we will use the same notation for a residue class and an integer representing it. The proof will be based on the following result of Gong:

Lemma 4 (Gong [5])**.** *For any subset $\mathcal{D} \subset \mathbb{F}_p$ and any multiplicative character $\chi \neq \chi_0$ modulo p we have the identity*

$$\sum_{a \in \mathbb{F}_p} \left| \sum_{x \in \mathcal{D}} \chi(x+a) \right|^2 = p|\mathcal{D}| - |\mathcal{D}|^2. \tag{48}$$

Proof of Lemma 4. With $\mathbb{F}_p^*$ in place of $\mathbb{F}_p$ this is presented and proved by Gong as Theorem 2 in [5]. However, $0 \notin \mathcal{D}$ is not used in the proof of the lemma, and the proof goes through in exactly the same way if we replace the assumption $\mathcal{D} \subset \mathbb{F}_p^*$ by $\mathcal{D} \subset \mathbb{F}_p$, thus we may use the lemma in the form presented above. □

(We remark that here we will need only the special case of Lemma 4 when $\mathcal{D}$ consists of consecutive residues, i.e., it is of form $\mathcal{D} = \{n, n+1, \ldots, n+m\}$, and this special case of the lemma was proved and used already in 1952 by Davenport and Erdős [3]. However, we prefered to present the lemma here in this more general form since in the sequel of this paper and other related problems where we will use the same method we will need this greater generality.)

We will use Lemma 4 with $\mathcal{D} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ and the character $\chi(n)$ generated by the Legendre symbol modulo p (so that $\chi(n) = \left(\frac{n}{p}\right)$ for $(p, n) = 1$ and $\chi(n) = 0$ for $p(n)$). Let a' be an a value which defines a maximal term in the sum in (48) so that this term is at least as large as the average of the terms:

$$\left|\sum_{x\in\mathcal{D}} \chi(x+a')\right|^2 \geqslant |\mathcal{D}| - \frac{|\mathcal{D}|^2}{p} = |\mathcal{D}|\left(1 - \frac{p-1}{2p}\right) > \frac{|\mathcal{D}|}{2}$$

whence

$$\left|\sum_{x\in\mathcal{D}} \chi(x+a')\right| > 2^{-1/2}|\mathcal{D}|^{1/2}. \tag{49}$$

Write

$$\mathcal{D}_1 = \mathcal{D} + \{a'\} = \left\{a'+1, a'+2, \ldots, a'+\frac{p-1}{2}\right\}.$$

Then either we have

$$\mathcal{D}_1 \subset \{1, 2, \ldots, p-1\}, \quad |\mathcal{D}_1| = |\mathcal{D}| = \frac{p-1}{2} \tag{50}$$

or $\mathcal{D}_1$ can be represented in the form

$$\mathcal{D}_1 = \{-b, -(b-1), \ldots, -1, 0, 1, 2, \ldots, c\} = \mathcal{D}_2 \cup \{0\} \cup \mathcal{D}_3 \tag{51}$$

with

$$\mathcal{D}_2 = \{-b, -b+1, \ldots, -1\}, \quad \mathcal{D}_3 = \{1, 2, \ldots, c\}, \quad \max\big(|\mathcal{D}_2|, |\mathcal{D}_3|\big) < \frac{p-1}{2}. \tag{52}$$

Now we define the set $\mathcal{D}' \subset \mathbb{F}_p$ so that $\mathcal{D}' = \mathcal{D}_1$ in case (50), while if (51) and (52) hold, then let $\mathcal{D}'$ be that one of $\mathcal{D}_2$ and $\mathcal{D}_3$ for which $\left|\sum_{y\in\mathcal{D}_i}\chi(y)\right|$ is greater. In this second case by (49) we have

$$2^{-1/2}|\mathcal{D}|^{1/2} < \left|\sum_{x\in\mathcal{D}}\chi(x+a')\right| = \left|\sum_{y\in\mathcal{D}_1}\chi(y)\right| = \left|\sum_{y\in\mathcal{D}_2}\chi(y) + \sum_{y\in\mathcal{D}_3}\chi(y)\right| \leqslant$$
$$\leqslant \left|\sum_{y\in\mathcal{D}_2}\chi(y)\right| + \left|\sum_{y\in\mathcal{D}_3}\chi(y)\right| \leqslant 2\left|\sum_{y\in\mathcal{D}'}\chi(y)\right|$$

whence

$$\left|\sum_{y\in\mathcal{D}'}\chi(y)\right| > 2^{-3/2}|\mathcal{D}|^{1/2}. \tag{53}$$

In the first case (50) we have

$$\left|\sum_{y\in\mathcal{D}'}\chi(y)\right| = \left|\sum_{y\in\mathcal{D}_1}\chi(y)\right| = \left|\sum_{x\in\mathcal{D}}\chi(x+a')\right|$$

from which again (53) follows by (49).

It follows from the definition of $\mathcal{D}'$ that in both cases it is of the form

$$\mathcal{D}' = \{n+1, n+2, \ldots, n+M\} \tag{54}$$

with

$$1 \leqslant n+1 < n+M \leqslant p-1 \tag{55}$$

and, by also using (50) and (52), we have

$$M = |\mathcal{D}'| \leqslant \frac{p-1}{2}. \tag{56}$$

We obtain from (53), (54), (55) and (56) that

$$W(E_{p-1}^p) \geqslant M^{-\alpha}W\big(E_{p-1}^p(n,M)\big) \geqslant M^{-\alpha}\big|e_{n+1}+e_{n+2}+\cdots+e_{n+M}\big| =$$
$$= M^{-\alpha}\left|\sum_{y\in\mathcal{D}'}\chi(y)\right| = M^{-\alpha}\left|\sum_{i=1}^{M}\left(\frac{n+i}{p}\right)\right| > |\mathcal{D}'|^{-\alpha}2^{-3/2}|\mathcal{D}|^{1/2} \geqslant$$
$$\geqslant |\mathcal{D}|^{-\alpha}2^{-3/2}|\mathcal{D}|^{1/2} = 2^{-3/2}|\mathcal{D}|^{1/2-\alpha} = 2^{-3/2}\left(\frac{p-1}{2}\right)^{1/2-\alpha} \geqslant$$
$$\geqslant 2^{-3/2}\left(\frac{p}{4}\right)^{1/2-\alpha} = 2^{-3/2}(2^{-2})^{1/2-\alpha}p^{1/2-\alpha} \geqslant 2^{-5/2}p^{1/2-\alpha} > \frac{1}{10}p^{1/2-\alpha}$$

which completes the proof of the theorem. □

References

[1] D. A. Burgess: On character sums and primitive roots, *PROC. LONDON MATH. SOC.* **12** (3) (1962), 179–192.

[2] C. Dartyge, K. Gyarmati and A. Sárközy: On irregularities of distribution of binary sequences relative to arithmetic progressions, I. (General results), *UNIF. DISTRIB. THEORY*, to appear.

[3] H. Davenport and P. Erdős: The distribution of quadratic and higher residues, *PUBL. MATH. DEBRECEN* **2** (1952), 252-265.

[4] P. Erdős and A. Sárközy: Some solved and unsolved problems in combinatorial number theory, *MATH. SLOVACA* **28** (1978), 407–421.

[5] K. Gong: An elementary approach to character sums over multiplicative subgroups, *INTEGERS* **16** (2016), #A13.

[6] J. Matoušek and J. Spencer: Discrepancy in arithmetic progression, *J. AMER. MATH. SOC.* **9** (1996), 195–204.

[7] C. Mauduit and A. Sárközy: On finite pseudorandom binary sequences, I. Measure of pseudorandomness, the Legendre symbol, *ACTA ARITH.* **82** (1997), 365–377.

[8] C. Mauduit and A. Sárközy: On finite pseudorandom binary sequences, II. The Champernowne, Rudin–Shapiro, and Thue–Morse sequences, a further construction, *J. NUMBER THEORY* **73** (1998), 256–276.

[9] H. L. Montgomery and R. C. Vaughan: Mean values of character sums, *CAN. J. MATH.* **31**(3) (1979), 470–487.

[10] G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste, *GÖTTINGER NACHRICHTEN* 1918, 21–29.

[11] M. Queffélec: *Substitution Dynamical Systems – Spectral Analysis*, Lecture Notes in Math., Vol. 1294, Springer, New York/Berlin, 1987.

[12] K. F. Roth: Remark concerning integer sequences, *ACTA ARITH.* **9** (1964), 257–260.

[13] W. Rudin: Some theorems on Fourier coefficients, *PROC. AMER. MATH. SOC.* **10** (1959), 855–859.

[14] A. Sárközy: Some remarks concerning irregularities of distribution of sequences of integers in arithmetic progressions, IV, *ACTA MATH. ACAD. SCI. HUNGAR.* **30**(1-2) (1977), 155–162.

[15] H. S. Shapiro: Extremal problems for polynomials and power series, Doctoral thesis, M. I. T., 1957.

[16] A. I. Vinogradov: On the symmetry property for sums with Dirichlet characters, *IZV. AKAD. NAUK UZSR, SER. FIZ.-MAT. NAUK* 1965 (1), 21–27.

[17] L. Zhao: Burgess bound for character sums, http://www.researchgate.net/publication/237203641.