Concatenation of Legendre symbol sequences

Katalin Gyarmati

Abstract

In the applications it may occur that our initial pseudorandom binary sequence is not long enough, thus we have to take the concatenation of it with another pseudorandom binary sequences. Here we will consider concatenation of Legendre symbol sequences so that the resulting longer sequence has strong pseudorandom properties.

2000 AMS Mathematics Subject Classification: 11K45.

List of keywords and phrases: pseudorandom, concatenation, Legendre symbol.

1 Introduction

In a series of papers Mauduit and Sárközy (partly with further coauthors) studied finite pseudorandom binary sequences

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

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. K67676 and PD72264 and the János Bolyai Research Fellowship.

In particular, in Part I [9] first they introduced the following measures of pseudorandomness:

Write

$$U(E_N, t, a, b) = \sum_{j=0}^{t-1} e_{a+jb}$$

and, for $D = (d_1, \dots, d_\ell)$ with non-negative integers $d_1 < \cdots < d_\ell$,

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}. \tag{1}$$

Then the *well-distribution measure* of E_N is defined as

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

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a + (t-1)b \le N$, while the *correlation measure of order* ℓ of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|, \tag{2}$$

where the maximum is taken over all $D = (d_1, d_2, \dots, d_\ell)$ and M such that $1 \le d_1 < d_2 < \cdots < d_\ell < M + d_\ell \le N$.

Then the sequence E_N is considered as a "good" pseudorandom sequence if both measures $W(E_N)$, $C_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$).

It was shown in [9] that the Legendre symbol forms a "good" pseudorandom sequence. More exactly, let p be an odd prime, and

$$N = p - 1, \ e_n = \left(\frac{n}{p}\right), \ E_N = \{e_1, \dots, e_N\}.$$

Then by Theorem 1 in [9] we have

$$W(E_N) \ll p^{1/2} \log p \ll N^{1/2} \log N$$

and

$$C_\ell(E_N) \ll \ell p^{1/2} \log p \ll \ell N^{1/2} \log N.$$

Numerous binary sequences have been tested for pseudorandomness by J. Cassaigne, Z. Chen, X. Du, L. Goubin, X. Guozhen, S. Ferenczi, S. Li, H. Liu, C. Mauduit, L. Mérai, S. Oon, J. Rivat, A. Sárközy, G. Xiao, C. Zhixiong and others. In the best constructions we have $W(E_N) \ll N^{1/2}(\log N)^c$ and $C_\ell(E_N) \ll N^{1/2}(\log N)^{c_\ell}$, where $c, c_2, c_3, \ldots$ are positive constants. However, most of these constructions produced only a "few" pseudorandom sequences; usually for a fixed integer N, the construction provided only one pseudorandom sequence E_N of length N. First L. Goubin, C. Mauduit, A. Sárközy [2] succeeded in constructing a large family of pseudorandom binary sequences. Their construction was the following:

Construction 1 *Suppose that p is a prime number, and $f(x) \in \mathbb{F}_p[x]$ is a polynomial with degree $k > 0$ and no multiple zero in $\overline{\mathbb{F}}_\mathbf{p}$. Define the binary sequence $E_p = \{e_1, \ldots, e_p\}$ by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1, \\ +1 & \text{for } p \mid f(n). \end{cases} \tag{3}$$

It turns out that under some not too restrictive conditions on p or the degree of the polynomial, the pseudorandom measures of E_p are small. Indeed Goubin, Mauduit and Sárközy [2] proved the following.

Theorem A *If p is a prime and $f(x)$ is a polynomial as it is described in Construction 1, then for the sequence E_p defined by* (3) *we have*

$$W(E_p) < 10kp^{1/2} \log p.$$

Moreover, assume that for $\ell \in \mathbb{N}$ one of the following assumptions holds:

(i) $\ell = 2$;

(ii) $\ell < p$ and 2 is a primitive root modulo p;

(iii) $(4k)^\ell < p$.

Then we also have

$$C_\ell(E_p) < 10k\ell p^{1/2} \log p.$$

Since then numerous other large families of pseudorandom sequences have been constructed (see [3], [4], [5], [7], [8] and [10]).

In this paper first we will give a further condition on the polynomial $f(x)$ which guarantees that the correlation measures are small (so that the somewhat inconvenient assumptions (i)-(iii) can be replaced by another, perhaps, simpler one). It is very easy to generate polynomials which satisfy this condition. Next we will adapt the method of this construction for constructing pseudorandom sequences whose concatenation also possesses strong pseudorandom properties.

Theorem 1 *Suppose that p is an odd prime, $R \in \mathbb{N}$, $f(x) \in \mathbb{F}_p[x]$ is a polynomial which is of the form*

$$f(x) = \left(x^2 - a_1\right)\left(x^2 - a_2\right)\cdots\left(x^2 - a_k\right)(x - 1), \tag{4}$$

where $0 \le k \le R$, the a_i's are different quadratic non-residues modulo p so that $\left(\frac{a_i}{p}\right) = -1$ for $1 \le i \le k$. For each of these polynomials f, consider the binary sequence $E_p = E_p(f)$ defined by (3), and let $\mathcal{F}$ denote the family of all binary sequences obtained in this way. Then for any $2 \le \ell \in \mathbb{N}$ and for

all $f \in \mathcal{F}$ *we have*

$$C_\ell(E_p(f)) \ll R\ell p^{1/2} \log p. \tag{5}$$

Remark We note that a second degree polynomial $x^2 - a$ is irreducible over $\mathbb{F}_p$ if and only if a is quadratic non-residue modulo p.

If $f(x)$ is a polynomial of form (4) then its single zero is $x = 1$.

In Theorem 1 we did not estimate the well-distribution measure. For $f \in \mathcal{F}$ by Theorem A trivially we have

$$W(E_p(f)) \ll Rp^{1/2} \log p. \tag{6}$$

It is a natural question why do we not consider polynomials of form $f(x) = (x^2 - a_1)(x^2 - a_2) \cdots (x^2 - a_k)$? In this case the sequence $E_p(f)$ would be symmetric ($e_n = e_{p-n}$ for $1 \le n \le p$) which causes difficulties in the applications (see [6]).

Although $\mathcal{F}$ in Theorem A contains many binary sequences with strong pseudorandom properties, it may occur that there are certain relations between them. Let $E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)} \in \{-1, +1\}^p$ be binary sequences of length p. Let $\{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}\} \in \{-1, +1\}^{tp}$ denote the sequence of length tp obtained by writing the elements of $E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)} \in \{-1, +1\}^p$ successively. Our question is the following: for a fixed sequence $E_p^{(1)} \in \mathcal{F}$ how do we choose further sequences $E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)} \in \mathcal{F}$ such that the longer sequence $\{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}\} \in \{-1, +1\}^{tp}$ will have strong pseudorandom properties? It is not true that for any choices of different $E_p^{(1)}, E_p^{(2)}, \dots, E_p^{(t)} \in \mathcal{F}$ the sequence $\{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}\} \in$

$\{-1,+1\}^{tp}$ also has strong pseudorandom properties. Consider the following example:

$$\begin{aligned}
E_p^{(1)} &= E_p\left((x-1)\right) \in \mathcal{F},\\
E_p^{(2)} &= E_p\left((x^2-a_1)(x-1)\right) \in \mathcal{F},\\
E_p^{(3)} &= E_p\left((x^2-a_2)(x-1)\right) \in \mathcal{F},\\
E_p^{(4)} &= E_p\left((x^2-a_1)(x^2-a_2)(x-1)\right) \in \mathcal{F},
\end{aligned}$$

Then $E_{4p} = \{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, E_p^{(4)}\}$ has week pseudorandom properties. Indeed; the correlation of order 4 is "large":

$$\begin{aligned}
C_4(E_{4p}) &\geq |V(E_{4p}, p, (0, p, 2p, 3p))|\\
&= \sum_{n=1}^{p} \left(\frac{n-1}{p}\right)\left(\frac{(n^2-a_1)(n-1)}{p}\right)\\
&\quad \left(\frac{(n^2-a_2)(n-1)}{p}\right)\left(\frac{(n^2-a_1)(n^2-a_2)(n-1)}{p}\right) - 1\\
&= \sum_{n=1}^{p} \left(\frac{(n^2-a_1)^2(n^2-a_2)^2(n-1)^4}{p}\right) - 1 \geq p-2.
\end{aligned}$$

Next we will give a sufficient condition for the sequence $\{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \ldots, E_p^{(t)}\} \in \{-1,+1\}^{tp}$ having strong pseudorandom properties.

Theorem 2 *Suppose that p is an odd prime and*

$$\begin{aligned}
f_1(x) &= (x^2-a_{11})(x^2-a_{12})\ldots(x^2-a_{1r_1})(x-1),\\
f_2(x) &= (x^2-a_{21})(x^2-a_{22})\ldots(x^2-a_{2r_2})(x-1),\\
&\vdots\\
f_t(x) &= (x^2-a_{t1})(x^2-a_{t2})\ldots(x^2-a_{tr_t})(x-1),
\end{aligned} \tag{7}$$

where $a_{i1}, a_{i2}, \ldots, a_{ir_i}$ *are different quadratic non-residues modulo* p *for* $1 \leq i \leq t$. *Moreover suppose that* $a_{i1} = a_{vs}$ *if and only if* $i = v$ *and* $1 = s$. *Let*

$$R = \max_{1 \leq i \leq t} r_i + 1 = \max_{1 \leq i \leq t} \deg f_i(x).$$

Define $E_p^{(i)} \in \mathcal{F}$ *by* $E_p(f_i)$ *in* (3) *with* f_i *in place of* f *for* $1 \leq i \leq t$. *Then* $E_{tp} = \{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \ldots, E_p^{(t)}\} \in \{-1, +1\}^{tp}$ *has strong pseudorandom properties: for any* $2 \leq \ell \in \mathbb{N}$ *we have*

$$W(E_{tp}) \ll tRp^{1/2} \log p, \tag{8}$$

$$C_\ell(E_{tp}) \ll R\ell t 2^{\ell-1} p^{1/2} \log p. \tag{9}$$

Proof of Theorem 1

We will need the following lemma:

Lemma 1 *Suppose that* p *is a prime,* χ *is a non-principal character modulo* p *of order* d, $f(x) \in \mathbb{F}_p[x]$ *has* s *distinct roots in* $\overline{\mathbb{F}}_p$, *and it is not a constant multiple of the* d*-th power of a polynomial over* $\mathbb{F}_p$. *Let* y *be a real number with* $0 < y \leq p$. *Then for any* $x \in \mathbb{R}$*:*

$$\left| \sum_{x < n \leq x+y} \chi(f(n)) \right| < 9sp^{1/2} \log p.$$

Poof of Lemma 1

This is a trivial consequence of Lemma 1 and Lemma 2 in [1]. Indeed, there this result is deduced from Weil's theorem [11].

For any integers $d_1, d_2, \ldots, d_\ell$ and $M \in \mathbb{N}$ with

$$0 \leq d_1 < d_2 < \cdots < d_\ell < M + d_\ell \leq p, \tag{10}$$

the congruence

$$f(n+d_i) \equiv 0 \pmod{p},\ 1 \le n < M,\ 1 \le i \le \ell$$

has at most ℓ solutions ($n \equiv 1 - d_i \pmod{p}$). Thus writing $\left(\frac{0}{p}\right) = 0$, we have

$$\begin{aligned} V(E_p, M, D) &= \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right| \\ &\le \left| \sum_{n=1}^{M} \left(\frac{f(n+d_1)}{p}\right) \left(\frac{f(n+d_2)}{p}\right) \dots \left(\frac{f(n+d_\ell)}{p}\right) \right| + \ell \\ &= \left| \sum_{n=1}^{M} \left(\frac{f(n+d_1) f(n+d_2) \dots f(n+d_\ell)}{p}\right) \right| + \ell \end{aligned}$$

Write $h(x) = f(x+d_1) f(x+d_2) \dots f(x+d_\ell)$. Then $h(x)$ has no multiple roots. Since the irreducible factors

$x + d_i - 1$ and $x + d_j - 1$,

$x + d_i - 1$ and $(x+d_j)^2 - a_s$,

$(x+d_i)^2 - a_q$ and $(x+d_j)^2 - a_s$

are different if d_i and d_j are different and $a_q,\ a_s$ are quadratic non-residues.

Thus we may apply Lemma 1 with $\left(\frac{n}{p}\right), 2$ and $h(x)$ in place of χ, d and $f(x)$, respectively. The degree of $h(x)$ is clearly less than $R\ell$, thus applying Lemma 1 we obtain

$$|V(E_p, M, D)| \le \left| \sum_{n=1}^{M} \left(\frac{h(n)}{p}\right) \right| + \ell < 9R\ell p^{1/2} \log p + \ell \ll R\ell p^{1/2} \log p$$

for all $d_1, d_2, \dots, d_\ell, M$ satisfying (10) which proves (5).

Proof of Theorem 2

By the definition of the well-distribution measure, it is easy to see that

$$W(E_{tp}) \le W(E^{(1)}) + W(E^{(2)}) + \dots + W(E^{(t)}). \tag{11}$$

By (6) we have $W(E^{(i)}) \ll Rp^{1/2}\log p$. Using this and (11) we get (8).

Next we prove (9).

Lemma 2 *Let $f_1, f_2, \dots, f_t \in \mathbb{F}_p[x]$ be different polynomials. Suppose that for all $1 \le i_1 \le i_2 \le \cdots \le i_\ell \le t$, $b_1, b_2, \dots, b_\ell \in \mathbb{F}_p$ (where $b_s \ne b_r$ if $i_s = i_r$) the polynomial*

$$\prod_{j=1}^{\ell} f_{i_j}(x + b_j)$$

is never of the form $cg(x)^2$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Define $E_p^{(i)} \in \mathcal{F}$ by $E_p(f_i)$ in (3) with f_i in place of f. Then the correlation measure of $E_{tp} = \{E_p^{(1)}, E_p^{(2)}, E_p^{(3)}, \dots, E_p^{(t)}\} \in \{-1, +1\}^{tp}$ is

$$C_\ell(E_{tp}) \ll R\ell t 2^{\ell-1} p^{1/2}\log p. \tag{12}$$

We will prove Lemma 2 later. Let $f_1, f_2, \dots, f_t$ be polynomials of the form (7). In order to prove (9), by Lemma 2 it is sufficient to prove that a product of the form

$$\prod_{j=1}^{\ell} f_{i_j}(x + b_j),$$

where $1 \le i_1 \le i_2 \le \cdots \le i_\ell \le t$, $b_1, b_2, \dots, b_\ell \in \mathbb{F}_p$ and $b_s \ne b_r$ if $i_s = i_r$, is never of the form $cg(x)^2$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Here

$$f_{i_1}(x + b_1) = ((x + b_1)^2 - a_{i_1 1})((x + b_1)^2 - a_{i_1 2}) \dots ((x + b_1)^2 - a_{i_1 r_{i_1}})(x - 1).$$

Consider the multiplicity of the irreducible factor $(x + b_1)^2 - a_{i_1 1}$ in the product

$$\prod_{j=1}^{\ell} f_{i_j}(x + b_j).$$

It is clear that $(x+b_1)^2 - a_{i_1 1}$ appears once in the factorization of $f_{i_1}(x+b_1)$. Suppose that one of $f_{i_2}(x+b_2), f_{i_3}(x+b_3), \dots, f_{i_\ell}(x+b_\ell)$ contains $(x+b_1)^2 - a_{i_1 1}$

as an irreducible factor. Say, $f_{i_j}(x+b_j)$ $(j \geq 2)$ has an irreducible factor, namely, $(x+b_j)^2 - a_{i_j d}$ which is $(x+b_1)^2 - a_{i_1 1}$. Then

$$(x+b_j)^2 - a_{i_j d} = (x+b_1)^2 - a_{i_1 1}$$
$$x^2 + 2b_j x + b_j^2 - a_{i_j d} = x^2 + 2b_1 x + b_1^2 - a_{i_1 1}.$$

From this $b_1 \equiv b_j \pmod{p}$ and $a_{i_j d} \equiv a_{i_1 1} \pmod{p}$ follows. Since $b_1 \equiv b_j \pmod{p}$ we have $i_1 \neq i_j$. But then $a_{i_j d}$ and $a_{i_1 1} \pmod{p}$ are different, which is a contradiction.

Thus $(x+b_1)^2 - a_{i_1 1}$ appears once in the factorization of $\prod_{j=1}^{\ell} f_{i_j}(x+b_j)$. So $\prod_{j=1}^{\ell} f_{i_j}(x+b_j)$ is never of the form $cg(x)^2$ with $c \in \mathbb{F}_p$, $g(x) \in \mathbb{F}_p[x]$. Thus we may use Lemma 2, which proves Theorem 2. It remains to prove Lemma 2.

Proof of Lemma 2 $C_\ell(\{E_p^{(1)}, E_p^{(2)}, \ldots, E_p^{(t)}\})$ is defined as the maximum of V's, see (2). Let $\{E_p^{(1)}, E_p^{(2)}, \ldots, E_p^{(t)}\} = \{e_1, e_2, \ldots, e_{tp}\}$. We will prove that for $\mathcal{D} = (d_1, d_2, \ldots, d_\ell)$ with non negative integers $d_1 < d_2 < \cdots < d_\ell$, $M \in \mathbb{N}$ we have

$$\left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_\ell} \right| \leq 10 R \ell t 2^{\ell-1} p^{1/2} \log p. \tag{13}$$

For each d_i and n define $a_{i,n}$ and $y_{i,n}$ by

$$n + d_i = (y_{i,n} - 1)p + a_{i,n} \tag{14}$$

where $1 \leq a_{i,n} \leq p$. Then

$$e_{n+d_i} = \begin{cases} \left(\frac{f_{y_{i,n}}(n+d_i)}{p}\right) & \text{for } (f_{y_{i,n}}(n+d_i), p) = 1, \\ +1 & \text{for } p \mid f_{y_{i,n}}(n+d_i). \end{cases} \tag{15}$$

Suppose that we fix any positive integers $j_1 \le j_2 \le \cdots \le j_\ell$ and we would like to determine the integers $1 \le n \le M$ such that

$$e_{n+d_1} = \begin{cases} \left(\frac{f_{j_1}(n+d_1)}{p}\right) & \text{for } (f_{j_1}(n+d_1), p) = 1, \\ +1 & \text{for } p \mid f_{j_1}(n+d_1). \end{cases}$$

$$e_{n+d_2} = \begin{cases} \left(\frac{f_{j_2}(n+d_2)}{p}\right) & \text{for } (f_{j_2}(n+d_2), p) = 1, \\ +1 & \text{for } p \mid f_{j_2}(n+d_2). \end{cases}$$

$$\vdots$$

$$e_{n+d_\ell} = \begin{cases} \left(\frac{f_{j_\ell}(n+d_\ell)}{p}\right) & \text{for } (f_{j_\ell}(n+d_\ell), p) = 1, \\ +1 & \text{for } p \mid f_{j_\ell}(n+d_\ell). \end{cases}$$

Then by (14) and (15)

$$\begin{aligned} j_1 &= \left[\frac{n+d_1-1}{p}\right] + 1 \\ j_2 &= \left[\frac{n+d_2-1}{p}\right] + 1 \\ &\vdots \\ j_\ell &= \left[\frac{n+d_\ell-1}{p}\right] + 1. \end{aligned} \tag{16}$$

Here $1 \le j_i = \left[\frac{n+d_i-1}{p}\right] + 1 \le \left[\frac{tp-1}{p}\right] + 1 = t$. It is easy to see that the integers n which satisfy (16) form an interval. We will denote this interval by $I_{j_1,j_2,\ldots,j_\ell} \subseteq [1, 2, \ldots, tp]$. (it can be the empty interval). Since $j_1 = \left[\frac{n+d_1}{p}\right] + 1$

we see that $|I_{j_1,j_2,\dots,j_\ell}| \le p$. Then by the triangle inequality we have

$$\begin{aligned}\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\cdots e_{n+d_\ell}\right| &\le \Bigg|\sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} \\ &\qquad \sum_{\substack{n\in I_{j_1,j_2,\dots,j_\ell}\\ p\nmid f_{j_1}(n+d_1)\cdots f_{j_\ell}(n+d_\ell)}} \left(\frac{f_{j_1}(n+d_1)}{p}\right)\dots\left(\frac{f_{j_\ell}(n+d_\ell)}{p}\right)\Bigg| \\ &\quad + \left|\sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} \sum_{\substack{n\in I_{j_1,j_2,\dots,j_\ell}\\ p\mid f_{j_1}(n+d_1)\cdots f_{j_\ell}(n+d_\ell)}} 1\right| \\ &\le \Bigg|\sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} \\ &\qquad \sum_{\substack{n\in I_{j_1,j_2,\dots,j_\ell}\\ p\nmid f_{j_1}(n+d_1)\cdots f_{j_\ell}(n+d_\ell)}} \left(\frac{f_{j_1}(n+d_1)\dots f_{j_\ell}(n+d_\ell)}{p}\right)\Bigg| \\ &\quad + \sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} \ell. \end{aligned} \tag{17}$$

The theorem is trivial for $\ell \ge p^{1/2}\log p$. For $\ell < p^{1/2}\log p$ by (17) and Lemma 2

$$\begin{aligned}\left|\sum_{n=1}^{M} e_{n+d_1}e_{n+d_2}\cdots e_{n+d_\ell}\right| &\le \sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} \left(9R\ell p^{1/2}\log p+\ell\right) \\ &\le \sum_{j_1=1}^{k}\sum_{j_2=1}^{k}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} 10R\ell p^{1/2}\log p. \end{aligned} \tag{18}$$

It remains to estimate $\sum_{j_1=1}^{t}\sum_{j_2=1}^{t}\cdots\sum_{\substack{j_\ell=1\\ I_{j_1,j_2,\dots,j_\ell}\neq\emptyset}}^{t} 1$. It is clear that j_1 may take t different values. Next we study that for fixed j_1, how many different values

may j_i assume. For the fixed j_1 we have

$$j_1 = \left[\frac{n+d_1-1}{p}\right] + 1.$$

Thus

$$\begin{aligned}
j_1 - 1 \le \frac{n+d_1-1}{p} &< j_1 \\
(j_1-1)p \le n+d_1-1 &< j_1 p \\
(j_1-1)p + d_i - d_1 \le n+d_i-1 &< j_1 p + d_i - d_1 \\
j_1 - 1 + \frac{d_i-d_1}{p} \le \frac{n+d_i-1}{p} &< j_1 + \frac{d_i-d_1}{p} \\
j_1 - 1 + \left[\frac{d_i-d_1}{p}\right] \le \left[\frac{n+d_i-1}{p}\right] &\le j_1 + \left[\frac{d_i-d_1}{p}\right] \\
j_1 + \left[\frac{d_i-d_1}{p}\right] \le \left[\frac{n+d_i-1}{p}\right] + 1 &\le j_1 + 1 + \left[\frac{d_i-d_1}{p}\right] \\
j_1 + \left[\frac{d_i-d_1}{p}\right] \le j_i \le j_1 + 1 + \left[\frac{d_i-d_1}{p}\right]&.
\end{aligned}$$

It follows that for fixed j_1 each j_i $(2 \le i \le \ell)$ may assume at most 2 different values. Thus by (18)

$$\left|\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_\ell}\right| \le 10R\ell t 2^{\ell-1} p^{1/2} \log p,$$

which completes the proof.

References

[1] R. Ahlswede, C. Mauduit, A. Sárközy, *Large families of pseudorandom sequences of k symbols and their complexity, Part I, II.*, Lecture Notes in Computer Science 4123, General Theory of Information Transfer and Combinatorics, Springer, Berlin / Heidelberg 2006, 293-325.

[2] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[3] K. Gyarmati, *A note to the paper "On a fast version of a pseudorandom generator"*, Annales Univ. Sci. Budapest. Eötvös, to appear.

[4] K. Gyarmati,*On a family of pseudorandom binary sequences*, Periodica Math. Hungar. 49 (2004), 45-63.

[5] K. Gyarmati, *On a fast version of a pseudorandom generator*, Lecture Notes in Computer Science 4123, General Theory of Information Transfer and Combinatorics, Springer, Berlin / Heidelberg 2006, 326-342.

[6] K. Gyarmati, *On a pseudorandom property of binary sequences*, Ramanujan J. 8 (2004), 289-302.

[7] K. Gyarmati, A. Sárközy, A. Pethő, *On linear recursion and pseudorandomness*, Acta Arith. 118 (2005), 359-374.

[8] Christian Mauduit, Joël Rivat, András Sárközy, *Construction of pseudorandom binary sequences using additive characters*. Monatshefte Math. 141 (2004), 197-208.

[9] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequence I: Measures of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365-377.

[10] Joël Rivat, András Sárközy, *Modular construction of pseudorandom binary sequences with composite moduli*. Periodica Math. Hungar. 51 (2005), 75-107.

[11] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.

Eötvös Loránd University

Department of Algebra and Number Theory

H-1117 Budapest, Pázmány Péter sétány 1/C, Hungary

email: gykati@cs.elte.hu