Period Math Hung (2015) 71:210–223
DOI 10.1007/s10998-015-0104-1

On pseudorandom binary sequences constructed by using finite fields

Richárd Sebők[1]

Published online: 16 October 2015

Abstract By using finite fields of order p^r with $r \geq 2$ and their quadratic characters, Sárközy and Winterhof presented a construction for binary sequences of length p^r with strong pseudorandom properties. In the special case $r = 2$ Gyarmati improved on their estimates for the pseudorandom measures of these sequences. Here we extend Gyarmati's result and sharpen the estimates of Sárközy and Winterhof for any prime power p^r.

Keywords Binary sequences · Pseudorandomness · Finite fields · Well-distributions · Correlation

Mathematics Subject Classification Primary 11K45

1 Introduction

Pseudorandom binary sequences play a crucial role in cryptography. The algorithm generating the pseudorandom binary sequence is called *pseudorandom bit generator* and it is usually characterized in terms of the "next bit test": the generator satisfies this test if there is no polynomial time algorithm such that having the first k bits it predicts the $k+1$-st bit with probability much greater than $1/2$. However, this test is suitable only for recursive construction; the non-existence of polynomial time algorithm cannot be proved, the probability much greater than $1/2$ is not a strict mathematical notion (see [17] for further details). Another frequently used classical definition of pseudorandomness uses linear complexity profile, but there is a lower bound in [2] for linear complexity profile in terms of the correlation measure (for definition see (1.1)).

✉ Richárd Sebők
sebokr@cs.elte.hu

[1] Department of Algebra and Number Theory, Eötvös Loránd University, Pázmány Péter sétány 1/C, Budapest 1117, Hungary

Thus Mauduit and Sárközy proposed a new, more constructive and quantitative approach. First in [17] they introduced the following measures for studying pseudorandom (briefly PR) properties of finite binary sequences:

The *well-distribution measure* of the binary sequence

$$E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N$$

is defined by

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

where the maximum is taken over all $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ such that $1 \le a + b \le a + bt \le N$. The *correlation measure of order k* of E_N is defined as

$$C_k(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right|, \tag{1.1}$$

where the maximum is taken over all $D = (d_1, \dots, d_k)$ with non-negative integers $d_1 < \dots < d_k$ and $M \in \mathbb{N}$ such that $M + d_k \le N$. The *combined* (well-distribution-correlation) *PR-measure of order k of* E_N is defined as

$$\begin{aligned} Q_k(E_N) &= \max_{a,b,t,D} |Z(a, b, t, D)| \\ &= \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \dots e_{a+jb+d_k} \right| \end{aligned} \tag{1.2}$$

where the maximum is taken over all a, b, t, $D = (d_1, d_2, \dots, d_k)$ such that all the subscripts $a + jb + d_l$ belongs to $\{1, \dots, N\}$.

Then the sequence E_N is considered as a sequence possessing strong PR properties (briefly, as a "good" PR sequence) if each of the PR measures $W(E_N)$ and for fixed k, $C_k(E_N)$ and $Q_k(E_N)$ are small in terms of N. This is justified by the fact that for a random sequence $E_N \in \{-1, +1\}^N$ these measures are smaller than $c_1 N^{1/2} (\log N)^{c_2}$ (with constant c_1, c_2 depending on k), as it was shown by Cassaigne, Mauduit and Sárközy [3] (and later their estimate was sharpened by Alon et al. [1,13]). It was also shown in [17] that the Legendre symbol sequence

$$E_{p-1} = \left(\left(\frac{1}{p} \right), \left(\frac{2}{p} \right), \dots, \left(\frac{p-1}{p} \right) \right) \tag{1.3}$$

possesses strong PR properties in this sense (see Theorem 2.1 below). Since that, many "good" PR sequences have been constructed by different authors, a survey of these results is presented by Gyarmati in [9]. Apart from the constructions given in [5,6,10,20], a common feature of these construction is that they are of modular nature with a prime modulus p (so that the length of the sequence is p or $p - 1$), in other words, finite fields $\mathbb{F}_p$ of prime order are used. Thus one might wants look for constructions of different nature, in particular, for modular construction with *composite* moduli m. Rivat and Sárközy [19] extended the most important modular constructions from prime moduli to "RSA moduli" $m = pq$, where p and q are of the same order of magnitude, and they showed that the sequence obtained in this way have weak PR properties: e.g., the correlation of order 4 is large (see also [4,14–16]). In the case when $m = uv$, $(u, v) = 1$ and both u and v are large, probably the situation is similar. The only remaining interesting case is when m is a prime power p^r with $r \ge 2$;

indeed, the four exceptional constructions presented in [5,6,10,20] are of this type. In this paper our goal is to continue the work in this direction: we will generalize a result in [10] from $r = 2$ to $r \geq 2$, and we will sharpen the results in [20].

2 Preliminaries

In [17] Mauduit and Sárközy proved that the following estimate for the combined measure of order k of the Legendre symbol sequence (1.3):

Theorem 2.1 *There is a number p_0 such that if $p > p_0$ is a prime number, $k \in \mathbb{N}$ then for the Legendre symbol sequence (1.3) we have*

$$Q_k(E_{p-1}) \leq 9kp^{1/2} \log p. \tag{2.1}$$

(Note that clearly we have $W(E_N) \leq Q_1(E_N)$ and $C_k(E_N) \leq Q_k(E_N)$ for every binary sequence E_N so that this result shows that the Legendre symbol sequence (1.3) possesses strong PR properties.)

By using the Legendre symbol, in [7] Goubin et al. constructed a large family of binary sequences with good pseudorandom properties.

Theorem 2.2 *If p is a prime number, $f(x) \in \mathbb{F}_p[x]$ has degree $k(> 0)$ and no multiple zero in $\overline{\mathbb{F}_p}$ (= the algebraic closure of $\mathbb{F}_p$), and the binary sequence $E_p = (e_1, \ldots, e_p)$ is defined by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for} \quad (f(n), p) = 1 \\ +1 & \text{for} \quad p | f(n), \end{cases} \tag{2.2}$$

then we have

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

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

(i) $l = 2$;
(ii) $l < p$, *and 2 is a primitive root modulo* p;
(iii) $(4k)^l < p$.

Then we also have

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

In [18] Mauduit and Sárközy proved an inequality in the connection of the well distribution measure and the correlation measure of order 2, which we will need later:

Theorem 2.3 *For all $E_N = \{e_1, \ldots, e_N\} \in \{-1, +1\}^N$, we have*

$$W(E_N) \leq 3\sqrt{NC_2(E_N)}. \tag{2.3}$$

(Note that in [8], Gyarmati generalized this theorem.)

We will also need the multidimensional extension of the theory of pseudorandomness of binary sequences. In [12] Hubert, Mauduit and Sárközy introduced the following definitions:

Denote by I_N^n the set of n-dimensional vectors whose coordinates are integers between 0 and $N - 1$:

$$I_N^n = \{\mathbf{x} = (x_1, \ldots x_n) : x_i \in \{0, 1, \ldots, N - 1\}\}.$$

This set is called an *n-dimensional N -lattice* or briefly an *N -lattice*. They extended the definition of binary sequences to more dimensions by considering functions of type

$$\eta(\mathbf{x}) : I_N^n \to \{-1, +1\},$$

called *binary lattice*.

If $\mathbf{x} = (x_1, \ldots, x_n)$ so that $\eta(\mathbf{x}) = \eta((x_1, \ldots, x_n))$ then we will simplify the notation by writing $\eta(\mathbf{x}) = \eta(x_1, \ldots, x_n)$.

Let $\mathbf{u_1}, \mathbf{u_2}, \ldots, \mathbf{u_n}$ be n linearly independent n-dimensional vectors over the fields of the real numbers such that the i-th coordinate of $\mathbf{u_i}$ is a positive integer and the other coordinates of $\mathbf{u_i}$ are 0, so that, writing $z_i = |\mathbf{u_i}|$, $\mathbf{u_i}$ is of the form $(0, \ldots, 0, z_i, 0, \ldots, 0)$. Let $t_1, t_2, \ldots, t_n$ be integers with $0 \le t_1, t_2, \ldots, t_n < N$. Then we call the set

$$B_N^n = \{\mathbf{x} = x_1\mathbf{u_1} + \cdots + x_n\mathbf{u_n} : 0 \le x_i z_i \le t_i (< N) \quad \text{for} \quad i = 1, \ldots, n\}$$

n-dimensional box N -lattice or briefly a *box N -lattice*.

Later Gyarmati et al. [11] introduced the following measure of pseudorandomness of binary lattices: The *correlation measure of order l* of the lattice $\eta : I_N^n \to \{-1, +1\}$ is defined by

$$C_l(\eta) = \max_{B', \mathbf{d_1}, \ldots, \mathbf{d_k}} \left| \sum_{\mathbf{x} \in B'} \eta(\mathbf{x} + \mathbf{d_1}) \ldots \eta(\mathbf{x} + \mathbf{d_l}) \right|,$$

where the maximum is taken over all distinct $\mathbf{d_1}, \ldots, \mathbf{d_l} \in I_N^n$ and all box lattices B' of the special form

$$B' = \{\mathbf{x} = (x_1, \ldots, x_n) : 0 \le x_1 \le t_1 (< N), \ldots, 0 \le x_n \le t_n (< N)\}$$

such that $B' + \mathbf{d_1}, \ldots, B' + \mathbf{d_l} \in I_N^n$.

In [12], in Theorem 2 the authors presented a construction based on the quadratic character of $\mathbb{F}_q^\times$, so that for $a \in \mathbb{F}_q^\times$ we have $\gamma(a) = +1$ if a is a quadratic residue and $\gamma(a) = -1$ otherwise.

Consider $\mathbb{F}_q$ as an r dimensional vector space over $\mathbb{F}_p$, and let $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_r}$ be a basis of this vector space. Then $\eta(x) : I_p^r \to \{-1, +1\}$ is defined by

$$\eta(\mathbf{x}) = \begin{cases} \gamma(x_1\mathbf{v_1} + \cdots + x_n\mathbf{v_n}) & \text{for} \quad (x_1, \ldots, x_n) \ne (0, \ldots, 0) \\ 1 & \text{for} \quad (x_1, \ldots, x_n) = (0, \ldots, 0) \end{cases} \tag{2.4}$$

for any $x_1, \ldots, x_n \in \mathbb{F}_p$, and $\eta(\mathbf{x}) = \eta(x_1, \ldots, x_n)$.

Theorem 2.4 (Mauduit and Sárközy) *If p is a prime, $n \in \mathbb{N}$, $k \in \mathbb{N}$, and the n-dimensional binary p-lattice is defined by (2.4) , then we have*

$$C_k(\eta) < kq^{1/2}(1 + \log p)^n. \tag{2.5}$$

By using finite fields $\mathbb{F}_q$ of order $q = p^r$ (with any $r \in \mathbb{N}$), in [20] Sárközy and Winterhof constructed binary sequences of length p^r with strong pseudorandom properties. Take the following ordering of the elements of $\mathbb{F}_q$: as $\mathbb{F}_q$ is an r-dimensional vector space over $\mathbb{F}_p$, consider any basis $\theta_0, \theta_1, \ldots, \theta_{r-1}$ of this vector space. Take the unique representation of any integer $n \in \{0, 1, \ldots, q-1\}$ in the number system of base p:

$$n = \varepsilon_0 + \varepsilon_1 p + \varepsilon_2 p^2 + \cdots + \varepsilon_{r-1} p^{r-1},$$

with $0 \le \varepsilon_i < p$ for $0 \le i \le r-1$. We assign the element

$$\xi_n = \varepsilon_0\theta_0 + \varepsilon_1\theta_1 + \varepsilon_2\theta_2 + \cdots + \varepsilon_{r-1}\theta_{r-1}$$

of $\mathbb{F}_q$ to the integer n. Then for a polynomial $f_q(x) \in \mathbb{F}_q[x]$ of degree $l > 0$ with no multiple zero in $\overline{\mathbb{F}_q}$ define the binary sequence $L_q = (l_0, l_1, \ldots, l_{q-1}) \in \{-1, +1\}^q$ by

$$l_n = \begin{cases} \gamma(f(\xi_n)) & \text{if} \quad f(\xi_n) \neq 0 \\ 1 & \text{if} \quad f(\xi_n) = 0 \end{cases} \tag{2.6}$$

for $n = 0, 1, \ldots, q-1$.

Theorem 2.5 (Sárközy and Winterhof) *For $r \geq 2$ we have*

(i)

$$W(L_q) < c_1 3^{r-1} r l^{1/r} p^{r-1/2}$$

and if $r \geq 3$ and $l < p$ then this can be improved to

$$W(L_q) < c_2 2^{3r/2} r^{1/2} l^{1/2} q^{3/4} (\log p)^{r/2}, \quad \text{and}$$

(ii) if either $k = 2$ and $l < p$, or $4^{r(k+l)} < p$, then

$$C_k(L_q) < c_3 2^{(r-1)k} r 2^r k l q^{1/2} (\log p)^r$$

where c_1, c_2, c_3 are positive absolute constants.

Observe that in the $q = p^2$ (i.e., $r = 2$) special case Theorem 2.5 gives in the important special case $f(x) = x$ in the following form:

Corollary 2.6 *If $q = p^2$ and the sequence $L_q = L_{p^2} = (l_0, l_1, \ldots, l_{p^2-1}) \in \{-1, +1\}^{p^2}$ is defined by $l_n = \gamma(\xi_n)$ for $\xi_n \neq 0$ and $l_0 = 1$, then we have*

(i)

$$W(L_{p^2}) < 6c_1 p^{3/2} = 6c_1 q^{3/4} \quad \text{for} \quad r \geq 3, \quad \text{and}$$

(ii) if either $k = 2$, or $4^{r(k+1)} < p$, then

$$C_k(L_{p^2}) < 8c_3 k 2^k q^{1/2} (\log p)^2.$$

In [10] Gyarmati studied the $q = p^2$ special case again. First she proved that if η is a two dimensional N-lattice with small correlation measures, then one can prepare a binary sequence of length N^2 from it which is also has small correlation measure. Indeed, define $E_{N^2}(\eta) \in \{-1, +1\}^{N^2}$ so that we take the first (from the bottom) row of the lattice then the second row of the lattice, etc.:

$$e_{i \cdot N + j} = \eta((j-1, i)) \quad \text{for} \quad i = 0, 1, \ldots, N-1, \quad j = 1, 2, \ldots, N.$$

She proved:

Theorem 2.7 (Gyarmati) *For any two dimensional binary N-lattice η for $1 < l < N$ we have*

$$C_l(E_{N^2}(\eta)) \leq (l+2) C_l(\eta). \tag{2.7}$$

Now we apply this theorem in the special case when $N = p$ is a prime, and η is the binary p-lattice defined in (2.4) with $n = 2$, and θ_0, θ_1 in place of $\mathbf{v_1}, \mathbf{v_2}$. Then E_{N^2} coincides with the sequence L_{p^2} occurring in Corollary 2.6, thus combining Theorems 2.4 and 2.7 we get

$$C_k(L_{p^2}) = C_k(E_{N^2}(\eta)) \le (k+2)C_k(\eta)$$
$$< (k+2)kq^{1/2}(1+\log p)^2 < c_4k^2q^{1/2}(\log p)^2. \tag{2.8}$$

Observe that this improves on the upper bound in Corollary 2.6 *(ii)* considerably: apart from an absolute constant factor this bound is smaller in terms of k by an exponential factor 2^k.

3 The new results

In the rest of the paper we will restrict ourselves to the special case $f(x) = x$ of the construction (2.6), so that now $q = p^r$ and the sequence $L_q = (l_0, l_1, \ldots, l_{q-1}) \in \{-1, +1\}^q$ is defined by

$$l_n = \begin{cases} \gamma(\xi_n) & \text{for} \quad n = 1, 2, \ldots, q-1, \\ 1 & \text{for} \quad n = 0. \end{cases} \tag{3.1}$$

Theorem 3.1 *If p is a prime number and $q = p^r$, $k \in \mathbb{N}$, $k < q$, then*

$$W(L_q) \le 3^{r/2}\sqrt{(r+2)2}\, q^{3/4}(1+\log p)^{r/2} + 1 \tag{3.2}$$

and

$$C_k(L_q) \le (k+1)^{r-2}(r+k)kq^{1/2}(1+\log p)^r + 1. \tag{3.3}$$

Thus for any choice of the basis $\theta_0, \theta_1, \ldots, \theta_{r-1}$, the sequence L_q generated by this construction possesses good PR properties. In this way we may generate many "good" binary sequences of length q. Two different bases may generate the same sequence L_q, however, it is easy to see that counting only the distinct sequences, still we got many (more than cp^r) sequences.

Note that in the special case $f(x) = x$ Theorem 2.5 gives

$$W(L_q) \le c_2 2^{3r/2} r^{1/2}\, q^{3/4}(\log p)^{r/2} \quad (\text{for } r \ge 3) \tag{3.4}$$

and if either $k = 2$ or $4^{r(k+1)} < p$, then

$$C_k(L_q) \le c_3 2^{(r-1)k} 2^r rkq^{1/2}(\log p)^r. \tag{3.5}$$

Comparing Theorem 3.1 with these results we find that, apart from a constant factor, in (3.2) the factor $3^{r/2}(1+\log p)^{r/2}$ replaces the greater factor $2^{3r/2}(\log p)^{r/2}$ and in (3.3) the factor $(k+1)^{r-2}(r+k)(1+\log p)^r$ replaces the much greater factor $2^{(r-1)k}2^r r(\log p)^r$. Thus, our Theorem 3.1 improves considerably on the $f(x) = x$ spacial case of Theorem 2.5.

Moreover, in the special case $r = 2$ it follows from (3.3) in our Theorem 3.1 that

$$C_k(L_q) < c_5k^2q^{1/2}(\log p)^2$$

which, apart from the constant factor, is the same upper bound as the one in (2.8). Thus, indeed, our Theorem 3.1 generalizes the upper bound (2.8) which can be obtained by Gyarmati's approach in [10].

4 Proof of the theorem

First, we will show that (3.2) follows from (3.3). Indeed, assuming (3.3) by Theorem 2.3 we have

$$W(L_q) \le 3\sqrt{NC_2(E_N)} \le 3\sqrt{3^{r-2}(r+2)2q^{1/2}(1+\log p)^r q^{1/2}}$$
$$= 3\cdot 3^{(r-2)/2}\sqrt{(r+2)2}\, q^{3/4}(1+\log p)^{r/2},$$

which proves (3.2).

Next we prove (3.3). By (1.1)

$$|V(L_q, M, D)| = \left|\sum_{n=0}^{M} l_{n+d_1} l_{n+d_2} \dots l_{n+d_k}\right|$$
$$= \left|\sum_{n=0}^{M} \gamma(\xi_{n+d_1})\gamma(\xi_{n+d_2}) \dots \gamma(\xi_{n+d_k})\right|$$

for $0 \le d_1 < \dots < d_k$, $M + d_k \le q-1$.

Lemma 4.1 *For $j = 1, \dots, k$ let $\omega_j(n)$ denote the function*

$$\omega_j(n) = \xi_{n+d_j} - \xi_n$$

where $n + d_j \le M + d_k \le N$. Then

$$\omega_i(n) \ne \omega_j(n) \quad \text{for} \quad 1 \le i < j \le k \tag{4.1}$$

for all n, where $0 \le n \le M$.

Proof We will give a formula for

$$\omega_j(n) = \xi_{n+d_j} - \xi_n.$$

Represent n and d_j in the form

$$n = a_0 + a_1 \cdot p + \dots + a_{r-1} \cdot p^{r-1},$$
$$d_j = d_{j,0} + d_{j,1} \cdot p + \dots + d_{j,r-1} \cdot p^{r-1}$$

with

$$a_0, d_{j,0}, a_1, d_{j,1}, \dots, a_{r-1}, d_{j,r-1} \in \{0, 1, 2, \dots, p-1\}.$$

Let $c_{-1} = 0$, and for all $i = 0, \dots, r-2$ define c_i by

$$c_i = a_i + d_{j,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor. \tag{4.2}$$

Then we have

$$n + d_j = a_0 + d_{j,0} + \left\lfloor \frac{c_{-1}}{p} \right\rfloor - \left\lfloor \frac{c_0}{p} \right\rfloor \cdot p$$
$$+ \left(a_1 + d_{j,1} + \left\lfloor \frac{c_0}{p} \right\rfloor - \left\lfloor \frac{c_1}{p} \right\rfloor \cdot p\right) \cdot p$$

$$+\left(a_2+d_{j,2}+\left\lfloor\frac{c_1}{p}\right\rfloor-\left\lfloor\frac{c_2}{p}\right\rfloor\cdot p\right)\cdot p^2+\cdots$$
$$+\left(a_{r-1}+d_{j,r-1}+\left\lfloor\frac{c_{r-2}}{p}\right\rfloor\right)\cdot p^{r-1}.$$

By the definition of ξ_n we have

$$\begin{aligned}\xi_{n+d_j}&=\left(a_0+d_{j,0}+\left\lfloor\frac{c_{-1}}{p}\right\rfloor-\left\lfloor\frac{c_0}{p}\right\rfloor\cdot p\right)\cdot\theta_0\\&+\left(a_1+d_{j,1}+\left\lfloor\frac{c_0}{p}\right\rfloor-\left\lfloor\frac{c_1}{p}\right\rfloor\cdot p\right)\cdot\theta_1\\&+\left(a_2+d_{j,2}+\left\lfloor\frac{c_1}{p}\right\rfloor-\left\lfloor\frac{c_2}{p}\right\rfloor\cdot p\right)\cdot\theta_2+\cdots\\&+\left(a_{r-1}+d_{j,r-1}+\left\lfloor\frac{c_{r-2}}{p}\right\rfloor\right)\cdot\theta_{r-1},\end{aligned}$$

so that

$$\begin{aligned}\omega_j(n)=\xi_{n+d_j}-\xi_n&=\left(d_{j,0}+\left\lfloor\frac{c_{-1}}{p}\right\rfloor-\left\lfloor\frac{c_0}{p}\right\rfloor\cdot p\right)\theta_0\\&+\left(d_{j,1}+\left\lfloor\frac{c_0}{p}\right\rfloor-\left\lfloor\frac{c_1}{p}\right\rfloor\cdot p\right)\cdot\theta_1\\&+\left(d_{j,2}+\left\lfloor\frac{c_1}{p}\right\rfloor-\left\lfloor\frac{c_2}{p}\right\rfloor\cdot p\right)\cdot\theta_2+\cdots\\&+\left(d_{j,r-1}+\left\lfloor\frac{c_{r-2}}{p}\right\rfloor\right)\cdot\theta_{r-1}\\&=d_{j,0}\cdot\theta_0+\left(d_{j,1}+\left\lfloor\frac{c_0}{p}\right\rfloor\right)\cdot\theta_1+\cdots+\left(d_{j,r-1}+\left\lfloor\frac{c_{r-2}}{p}\right\rfloor\right)\cdot\theta_{r-1}.\end{aligned}\tag{4.3}$$

Now assume that contrary to our claim there exists an n such that $\omega_i(n)=\omega_j(n)$ for some $i<j$ indices, so that

$$\begin{aligned}\omega_j(n)&=d_{j,0}\cdot\theta_0+\left(d_{j,1}+\left\lfloor\frac{c_0}{p}\right\rfloor\right)\cdot\theta_1+\cdots+\left(d_{j,r-1}+\left\lfloor\frac{c_{r-2}}{p}\right\rfloor\right)\cdot\theta_{r-1}\\&=d_{i,0}\cdot\theta_0+\left(d_{i,1}+\left\lfloor\frac{c_0'}{p}\right\rfloor\right)\cdot\theta_1+\cdots+\left(d_{i,r-1}+\left\lfloor\frac{c_{r-2}'}{p}\right\rfloor\right)\cdot\theta_{r-1}=\omega_i(n)\end{aligned}\tag{4.4}$$

For every l the coefficient of θ_l is the same on the two sides:

$$d_{j,l}+\left\lfloor\frac{c_{l-1}}{p}\right\rfloor\equiv d_{i,l}+\left\lfloor\frac{c_{l-1}'}{p}\right\rfloor\pmod p$$

for every $l\in\{0,1,2,\ldots,r-1\}$. Since

$$0\le d_{j,l}+\left\lfloor\frac{c_{l-1}}{p}\right\rfloor\le p,$$

thus one of the following three cases occurs:

$$d_{j,l}+\left\lfloor\frac{c_{l-1}}{p}\right\rfloor=d_{i,l}+\left\lfloor\frac{c_{l-1}'}{p}\right\rfloor,$$

$$d_{j,l} = 0, \quad \left\lfloor \frac{c_{l-1}}{p} \right\rfloor = 0, \quad d_{i,l} = p-1, \quad \left\lfloor \frac{c'_{l-1}}{p} \right\rfloor = 1,$$
$$d_{j,l} = p-1, \quad \left\lfloor \frac{c_{l-1}}{p} \right\rfloor = 1, \quad d_{i,l} = 0, \quad \left\lfloor \frac{c'_{l-1}}{p} \right\rfloor = 0.$$

Let l be the smallest index such that $d_{j,l} \neq d_{i,l}$. Such an index exists, since $j \neq i$, so $d_j \neq d_i$, and note that, by (4.4), we have $d_{j,0} = d_{i,0}$. For all k, m: $\left\lfloor \frac{c_k}{p} \right\rfloor, \left\lfloor \frac{c'_m}{p} \right\rfloor \in \{0, 1\}$, thus

$$d_{j,l} + \left\lfloor \frac{c_{l-1}}{p} \right\rfloor \equiv d_{i,l} + \left\lfloor \frac{c'_{l-1}}{p} \right\rfloor \pmod{p}$$

and $d_{j,l} \neq d_{i,l}$, and $0 \leq d_{i,l} \leq p-1$ and $0 \leq d_{j,l} \leq p-1$, so then

$$\left\lfloor \frac{c_{l-1}}{p} \right\rfloor \neq \left\lfloor \frac{c'_{l-1}}{p} \right\rfloor.$$

But by the definition of c (and so c') in (4.2), we have

$$c_{l-1} = a_{l-1} + d_{j,l-1} + \left\lfloor \frac{c_{l-2}}{p} \right\rfloor$$

and

$$c'_{l-1} = a_{l-1} + d_{i,l-1} + \left\lfloor \frac{c'_{l-2}}{p} \right\rfloor.$$

By the choice of l, $d_{j,m} = d_{i,m}$ for $m \in \{0, 1, 2, \ldots, l-1\}$, thus

$$c_m = c'_m$$

for every $m \in \{0, 1, 2, \ldots, l-1\}$, thus $c_{l-1} = c'_{l-1}$, which is a contradiction which proves the lemma. □

By the multiplicativity of γ we have

$$\begin{aligned} \left|V(L_q, M, D)\right| &= \left|\sum_{n=0}^{M} \gamma(\xi_{n+d_1})\gamma(\xi_{n+d_2}) \ldots \gamma(\xi_{n+d_k})\right| \qquad (4.5) \\ &= \left|\sum_{n=0}^{M} \gamma(\xi_n + \omega_1(n))\gamma(\xi_n + \omega_2(n)) \ldots \gamma(\xi_n + \omega_k(n))\right| \\ &= \left|\sum_{n=0}^{M} \gamma((\xi_n + \omega_1(n))(\xi_n + \omega_2(n)) \ldots (\xi_n + \omega_k(n)))\right|. \end{aligned}$$

Write M in the form

$$M = m_0 + m_1 p + m_2 p^2 + \cdots + m_{r-1} p^{r-1},$$

with $0 \leq m_i < p$ for $i \in \{0, 1, \ldots, r-1\}$. Then

$$m_{r-1} \text{ denotes the last digit of } M. \qquad (4.6)$$

By (4.3) we have

$$\omega_j(n) = d_{j,0} \cdot \theta_0 + \left(d_{j,1} + \left\lfloor \frac{c_0}{p} \right\rfloor\right) \cdot \theta_1 + \cdots + \left(d_{j,r-1} + \left\lfloor \frac{c_{r-2}}{p} \right\rfloor\right) \cdot \theta_{r-1}.$$

Thus for a fixed n the value of $\omega_j(n)$ only depends on the c_i's, for $0 \le i \le r-2$, so that it depends on the first $r-1$ digit of d_j.

We will prepare a partition of $\{\xi_n | 1 \le n \le M\}$ of the form $\bigcup_\alpha I_\alpha$ based on the size of the subscript j of $\omega_j(n)$ and of the subscript i of θ_i and then we want to give a good estimation on

$$\left| \sum_\alpha \sum_{\xi_n \in I_\alpha} \gamma(f(\xi_n)) \right|.$$

But this is a bit difficult, mainly because it could happen that $d_{j,i} < d_{e,i}$, while $d_{j,l} > d_{e,l}$ for $j \ne e$ and $0 \le i < l \le r-1$. So instead of reordering the d_j's, we will take their digits independently, and for the i-th digits, we will define $(0 \le)\delta_{1,i} \le \delta_{2,i} \le \cdots \le \delta_{k,i} (< p)$ as the reordered set of the i-th digits $d_{1,i}, d_{2,i}, \ldots, d_{k,i}$.

To give a good upper bound on the elements of the partition, we will use a result of A. Winterhof:

Theorem 4.2 (Winterhof) *Let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$ and consider the linear vector space formed by the elements of $\mathbb{F}_q$ over $\mathbb{F}_p$, and let $v_1, \ldots, v_n$ be a basis of this vector space. Denote χ a multiplicative character of $\mathbb{F}_q$ of order $d > 1$, $f \in \mathbb{F}_q[x]$ is a non-constant polynomial which is not a d-th power and which has m distinct zeros in its splitting field over $\mathbb{F}_q$, and $k_1, \ldots, k_n$ are non-negative integers with $k_1 \le p, \ldots, k_n \le p$, then writing*

$$B = \left\{ \sum_{i=1}^{n} j_i v_i : \ 0 \le j_i < k_i \right\},$$

we have

$$\left| \sum_{z \in B} \chi(f(z)) \right| < m q^{1/2} (1 + \log p)^n. \tag{4.7}$$

Proof This is a part of Theorem 2 in [22] (where its proof was based on A. Weil's theorem [21]). □

A set $B \subset \mathbb{F}_q$ of the form appearing in Theorem 4.2 will be called a box lattice.

We define the sets of I_α, where $\alpha \in \{0, 1, \ldots, k\}^{r-1}$, and $\alpha(i)$ is the i-th coordinate of α as

$$I_\alpha = \left\{ \xi_n : a_i + \delta_{\alpha(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \ge p \right\}$$

for $i = \{0, 1, \ldots r-2\}$, where $n = a_0 + a_1 \cdot p + \cdots + a_{r-1} \cdot p^{r-1}$ and $\delta_{\alpha(i),0} = 0$ and $\delta_{\alpha(i),k+1} = p$. Note that this gives a restriction only for the first $r-1$ digits of n, when $\xi_n \in I_\alpha$. For the last coordinate of n, we have the trivial upper bound $a_{r-1} \le m_{r-1}$.

If $0 \le n < n' \le M$, such that $n = n' + l \cdot p^{r-1}$, then all the digits $a_0, a_1, \ldots, a_{r-2}$ are the same (except the last one a_{r-1}), thus from $n \in I_\alpha$, $n' \in I_\alpha$ also occurs. There are at most $(k+1)^{r-1}$ subsets I_α, and most of them can be translated to a box lattice. With Theorem 4.2 we can give a good upper bound for them. But in some cases, it may occur that I_α is not a translated box lattice, some elements form an "excess".

Let S_α be the excess of I_α, in the sense as $I_\alpha = B_\alpha \cup S_\alpha$, where B_α is the greatest translated box lattice in I_α, in the following way: we want to find the largest number b such that

$$B_\alpha = \Bigg\{\xi_n \in I_\alpha : a_i + \delta_{\alpha(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \geq p$$
$$\text{for } i = \{0, 1, \ldots, r-2\} \quad \text{and} \quad a_{r-1} \leq b\Bigg\} \subseteq I_\alpha, \tag{4.8}$$

holds.

We will see later in Lemma 4.6 that each of these excesses can be considered as unions of $r-1$ translated box lattices, and thus each of them can be estimated with Theorem 4.2.

Let $M = m_0 + m_1 \cdot p + \cdots m_{r-1} \cdot p^{r-1}$. ξ_M is the greatest element in the sense that for all $\xi_n \in \bigcup_\alpha I_\alpha, n \leq M$. Thus for $n = a_0 + a_1 \cdot p + \cdots + a_{r-1} \cdot p^{r-1}$, if we compare the a_i's with the m_i's, from the last one till the first one, all $a_i \leq m_i$ until for a j index, $a_j < m_i$.

Lemma 4.3 *For all the elements of $\bigcup_\alpha S_\alpha$, their last coordinate, a_{r-1} are equal with m_{r-1} (as in (4.6)).*

Proof We will prove this by contradiction. If there were an $\xi_{n'}$ such that $a'_{r-1} < m_{r-1}$, and $\xi_{n'} \in \bigcup_\alpha S_\alpha$, all the others $\xi_{n''}$ are in $\bigcup_\alpha I_\alpha$, where $0 < n'' < M$, then all the elements with last coordinate a'_{r-1} are in $\bigcup_\alpha I_\alpha$, so for an index α' for which $\xi_{n'} \in I_{\alpha'}$ (and $S_\alpha \cap S_{\alpha*} = \emptyset$ for every $\alpha* \neq \alpha$, thus $\xi_{n'} \in S_{\alpha'}$ also must hold for this α' index),

$$A_{\alpha'} = \Bigg\{\xi_n : a_i + \delta_{\alpha'(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha'(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \geq p$$
$$\text{for} \quad i = \{0, 1, \ldots, r-2\}, \quad \text{and} \quad a_{r-1} < m_{r-1}\}$$

is a translated box lattice, so it is in the greatest translated box lattice, $A_{\alpha'} \subseteq B_{\alpha'} \subseteq I_{\alpha'}$, and $\xi_{n'} \in A_{\alpha'} \subseteq B_{\alpha'}$, so $\xi_{n'} \notin S_{\alpha'}$, contradiction. This proves the lemma. □

Lemma 4.4 *If there is an $n = a_0 + a_1 \cdot p + \cdots + a_{r-1} \cdot p^{r-1}$ such that $\xi_n \in S_\alpha$, then for all the elements $\xi_{n'} \in I_\alpha$, where $n' = a'_0 + a'_1 \cdot p + \cdots + a'_{r-2} \cdot p^{r-2} + a_{r-1} \cdot p^{r-1}$, $\xi_{n'} \in S_\alpha$ hold.*

Proof By contradiction, if $\xi_{n'} \notin S_\alpha$, then $\xi_{n'} \in B_\alpha$, which is the greatest translated box lattice inside of I_α. By Lemma 4.3, we also know that $a_{r-1} = m_{r-1}$. So $\xi_{n'} \in B_\alpha$ means that now b in (4.8) $m_{r-1} = b$ holds,

$$B_\alpha = \Bigg\{\xi_{n''} \in I_\alpha : a''_i + \delta_{\alpha(i),i} + \left\lfloor \frac{c''_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a''_i + \delta_{\alpha(i)+1,i} + \left\lfloor \frac{c''_{i-1}}{p} \right\rfloor \geq p$$
$$\text{for} \quad i = \{0, 1, \ldots, r-2\}, \quad \text{and} \quad a''_{r-1} \leq m_{r-1}\Bigg\},$$

which means that $\xi_n \in B_\alpha$ which contradicts to our assumption that $\xi_n \in S_\alpha = I_\alpha \setminus B_\alpha$. This proves the lemma. □

When we look carefully, we are able to make some observation about the second greatest digit of the excess, a_{r-2}.

Lemma 4.5 *There cannot be a $\xi_n \in S_\alpha$ and a $\xi_{n'} \in S_{\alpha'}$, such that $\alpha(i) = \alpha'(i)$ for all $i \in \{0, 1, \ldots, r-3\}$, but $\alpha(r-2) \neq \alpha'(r-2)$.*

Proof By contradiction, if such n and n' would exist, that for their first $r-3$ digits,

$$a'_i + \delta_{i,\alpha(i)} + \left\lfloor \frac{c'_{i-1}}{p} \right\rfloor < p$$

hold if and only if

$$a_i + \delta_{i,\alpha(i)} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p$$

for $i = 0, 1, \ldots, r-3$ and for every α, except for their $r-2$nd and $r-1$st coordinate, and from the indirect assumption there exist an α such that

$$a'_{r-2} + \delta_{r-2,\alpha(r-2)} + \left\lfloor \frac{c'_{r-3}}{p} \right\rfloor < p, \quad \text{and}$$
$$a_{r-2} + \delta_{r-2,\alpha(r-2)} + \left\lfloor \frac{c_{r-3}}{p} \right\rfloor \geq p.$$

From that, we get that

$$a'_{r-2} < a_{r-2}$$

occurs, while we already know that from Lemma 4.3 that $a_{r-1} = a'_{r-1} = m_{r-1}$. So

$$A_{\alpha'} = \left\{ \xi_n : a_i + \delta_{\alpha'(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha'(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \geq p \right.$$
$$\left. \text{for} \quad i = \{0, 1, \ldots, r-2\}, \quad \text{and} \quad a_{r-1} = m_{r-1} \right\} \subseteq I_{\alpha'}$$

so also $A_{\alpha'} \subseteq B_{\alpha'} \subseteq I_{\alpha'}$ hold. But according to Lemma 4.4, all the elements of $I_{\alpha'}$, with the last coordinate m_{r-1} must be in the excess, which give us a contradiction, proving the lemma. □

For $q = p^r$, there are at most $(k+1)^{r-1}$ different I_α, and by Lemma 4.5, only $(k+1)^{r-2}$ pieces of I_α got an excess, the rest of them are translated box lattices.

For all I_α, there is a uniquely determined $\xi_{v_\alpha} \in \mathbb{F}_q$ such that

$$B'_\alpha = I_\alpha - S_\alpha - \xi_{v_\alpha} = B_\alpha - \xi_{v_\alpha}$$

is a box lattice in the sense of Theorem 4.2, with $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{r-1}\}$ as a basis of $\mathbb{F}_q$.

The only thing left is to consider the polynomials f_α's, when we switch from I_α to B'_α. Note that for an element $\xi_n \in I_\alpha$ $f_\alpha(\xi_n) = f_\alpha((\xi_n - \xi_{v_\alpha}) + \xi_{v_\alpha})$, where $\xi_n - \xi_{v_\alpha} \in B'_\alpha$. So we can change our polynomials $f_\alpha(\xi_n) : I_\alpha \to \mathbb{F}_q$ for $f_j(\xi_n + \xi_{v_\alpha}) : B'_\alpha \to \mathbb{F}_q$, which are also polynomials with the same degrees, and also have k distinct roots.

$$\left| \sum_\alpha \sum_{\xi_n \in I_\alpha} \gamma(f_\alpha(\xi_n)) \right| \leq \sum_\alpha \left| \sum_{\xi_n \in I_\alpha} \gamma(f_j \alpha(\xi_n)) \right|$$
$$= \sum_\alpha \left| \sum_{\xi_n \in B'_\alpha} \gamma(f_\alpha(\xi_n + \xi_{v_\alpha})) \right| + \sum_\alpha \left| \sum_{\xi_n \in S_\alpha} \gamma(f_\alpha(\xi_n)) \right| \tag{4.9}$$

Now for the first sum in (4.9), we can apply Winterhof's result (Theorem 4.2), for each B'_α

$$\sum_\alpha \left| \sum_{\xi_n \in B'_\alpha} \gamma(f_\alpha(\xi_n + \xi_{v_\alpha})) \right| < (k+1)^{r-1} k q^{1/2} (1 + \log p)^r \tag{4.10}$$

For the second sum in (4.9), it is enough to give an upper bound for only one excess.

Lemma 4.6 *The excess of I_α, S_α can be divided into $r-1$ disjoint translated box lattices.*

Proof Take an α, such that $S_\alpha \neq \emptyset$ and let n'_α be the greatest number for which $\xi_{n'_\alpha} \in I_\alpha$ holds with $\xi_{n'_\alpha} = a'_0 \cdot \theta_0 + a'_1 \cdot \theta_1 + \ldots a'_{r-1} \cdot \theta_{r-1}$. By Lemma 4.3, all the elements in S_α got the same last coordinate, namely $a'_{r-1} (= m_{r-1})$. We define an algorithm which will divide the remaining elements of the excess S'_α into translated box lattices. At the start of our algorithm, take $S'_\alpha = S_\alpha$ and for a simpler notion take $j = 2$.

Let us assume the last $j-1$ coordinates are equal for all the elements still left in the S'_α, these coordinates are the $r-1$st, $r-2$nd, $\ldots$, $r-j+1$st. Now take all the elements in S'_α which $r-j$th coordinates are smaller than a'_{r-j}, the $r-j$th coordinates of ξ_{n_α}. Denote the union of these elements as B_α^{j-1}. B_α^{j-1} is a translated box lattice. We have

$$S'_\alpha = \left\{ \xi_n \in I_\alpha : a_i + \delta_{\alpha(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \geq p \right.$$
$$\left. \text{for} \quad i = \{0, 1, \ldots, r-j\}, \quad \text{and} \quad \text{for} \quad i = \{r-j+1, \ldots, r-1\}, a_i = a'_i \right\},$$

and

$$B_\alpha^{j-1} = \left\{ \xi_n \in I_\alpha : a_i + \delta_{\alpha(i),i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor < p \quad \text{and} \quad a_i + \delta_{\alpha(i)+1,i} + \left\lfloor \frac{c_{i-1}}{p} \right\rfloor \geq p \right.$$
$$\text{for} \quad i = \{0, 1, \ldots, r-j-1\}, \quad \text{and} \quad a_{r-j} < a'_{r-j},$$
$$\left. \text{and} \quad \text{for} \quad i = \{r-j+1, \ldots, r-1\}, a_i = a'_i \right\}.$$

Let us replace S'_α be $S'_\alpha \setminus B_\alpha^{j-1}$. The last j coordinates of the elements of this set will be equal, and we can continue our algorithm until the last $r-1$ coordinates are equal. Then only the first coordinates are different, and the elements of S'_α form a translated box lattice, B_α^{r-1}. □

Since we divided the excess into $r-1$ disjoint translated box lattices, we can use Theorem 4.2 to give an upper bound for each of them.

$$\sum_\alpha \left| \sum_{\xi_n \in S_\alpha} \gamma(f_\alpha(\xi_n)) \right| < (k+1)^{r-2}(r-1)kq^{1/2}(1+\log p)^r \tag{4.11}$$

So with (4.9), (4.10) and (4.11), we estimate for (4.5) as

$$|V(L_q, M, D)| = \left| \sum_\alpha \sum_{\xi_n \in I_\alpha} \gamma(f_\alpha(\xi_n)) \right| \tag{4.12}$$
$$< (k+1)^{r-1}kq^{1/2}(1+\log p)^r + (k+1)^{r-2}(r-1)kq^{1/2}(1+\log p)^r$$
$$= (k+1)^{r-2}(r+k)kq^{1/2}(1+\log p)^r$$

which proves the theorem.

5 Further problems

There are a few related problems which have not been settled yet.

Problem 5.1 For a random binary sequence E_q of length q we have $W(E_q) \ll q^{1/2+\varepsilon}$ by [3], and for the sequence L_q studied here we have $W(L_q) \ll q^{3/4+\varepsilon}$ by Theorem 2.5. What is the smallest c with $W(L_q) \ll q^{c+\varepsilon}$?

Problem 5.2 Can we extend Gyarmati's Theorem 2.7 so that under a suitable condition on η, how small must $W(E_{N^2})$ be?

Problem 5.3 Can one extend Gyarmati's Theorem 2.7 from two dimensional lattices to r dimensional lattices for any $r \geq 2$?

Problem 5.4 Can one extend our Theorem 3.1 on the sharpening of Theorem 2.5 from $f(x) = x$ to a large family of polynomials $f(x)$?

I hope to return to some of these problems in subsequent papers.

Acknowledgments I would like to thank Professors K. Gyarmati and A. Sárközy for the valuable discussions.

References

1. N. Alon, Y. Kohayakawa, C. Mauduit, C.G. Moreira, V. Rödl, Measures of pseudorandomness for finite sequences: typical values. Proc. Lond. Math. Soc. **95**, 778–812 (2007)
2. N. Brandstätter, A. Winterhof, Linear complexity profile of binary sequences with small correlation measure. Period. Math. Hung. **52**, 1–8 (2006)
3. J. Cassaigne, C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences VII: the measures of pseudorandomness. Acta Arith. **103**, 17–118 (2002)
4. Z. Chen, X. Du, C. Wu, Pseudo-randomness of certain sequences of $k$symbol with length pq. J. Comput. Sci. Technol. **26**, 276–282 (2011)
5. J. Folláth, Construction of pseudorandom binary sequences using additive characters over $GF(2^k)$. Period. Math. Hung. **57**, 73–81 (2008)
6. J. Folláth, Construction of pseudorandom binary sequences using additive characters over $GF(2^k)$, II. Period. Math. Hung. **60**, 127–135 (2010)
7. L. Goubin, C. Mauduit, A. Sárközy, Construction of large families of pseudorandom binary sequences. J. Number Theory **106**(1), 56–69 (2004)
8. K. Gyarmati, An inequality between the measures of pseudorandomness. Ann. Univ. Sci. Bp. Eötvös Sect. Math. **46**, 157–166 (2003)
9. K. Gyarmati, Measures of pseudorandomness, in *Radon Series in Computational and Applied Mathematics*, ed. by P. Charpin, A. Pott, A. Winterhof (de Gruyter, Berlin, 2013), pp. 43–64
10. K. Gyarmati, On the correlation of subsequences. Unif. Distrib. Theory **7**, 169–195 (2012)
11. K. Gyarmati, C. Mauduit, A. Sárközy, Measures of pseudorandomness of finite binary lattices, III (Q_k, correlation, normality, minimal values.). Unif. Distrib. Theory **5**, 183–207 (2010)
12. P. Hubert, C. Mauduit, A. Sárközy, On pseudorandom binary lattices. Acta Arith. **125**, 51–62 (2006)
13. Y. Kohayakawa, C. Mauduit, C. G. Moreira, V. Rödl. *Measures of Pseudorandomness for Finite Sequences: Minimal and Typical Values*, *Proceeding of WORDS'03*, TUCS Gen. Publ. 27, Turku Centre for Computer Science, 159–169 (2003)
14. H. Liu, J. Gao, A note on certain modular construction of pseudorandom binary sequences with composite moduli. Period. Math. Hung. **67**, 175–178 (2013)
15. H. Liu, J. Gao, Pseudorandom binary sequences with composite moduli (Chinese). Acta Math. Sin. (Chin. ser.) **55**, 869–880 (2012)
16. H. Liu, T. Zhan, X. Wang, On the correlation of pseudorandom binary sequences with composite moduli. Publ. Math. Debr. **74**, 195–214 (2009)
17. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol. Acta Arith. **82**, 365–377 (1997)
18. C. Mauduit, A. Sárközy, On the measures of pseudorandomness of binary sequences. Discrete Math. **271**, 195–207 (2003)
19. J. Rivat, A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli. Period. Math. Hung. **51**, 75–107 (2005)
20. A. Sárközy, A. Winterhof, Measures of pseudorandomness for binary sequences constructed using finite fields. Discrete Math. **309**, 1327–1333 (2009)
21. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris (1948)
22. A. Winterhof, Some estimates for character sums and applications. Des. Codes Cryptogr. **22**, 123–131 (2001)