Discrete Mathematics 338 (2015) 2020–2025

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Improving results on the pseudorandomness of sequences generated via the additive order of a finite field

László Mérai [a,b], Oğuz Yayla [c,*]

[a] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenberger Strasse 69, A-4040 Linz, Austria

[b] Eötvös Loránd University, Department of Computer Algebra, Pázmány Péter sétany 1/C, H-1117 Budapest, Hungary

[c] Department of Mathematics, Hacettepe University, Beytepe 06800 Ankara, Turkey

ARTICLE INFO

Article history:
Received 4 December 2014
Received in revised form 19 February 2015
Accepted 14 April 2015
Available online 6 June 2015

Keywords:
Pseudorandomness
Additive order
Lattice test
Correlation measure
Linear complexity profile

ABSTRACT

We improve several results in the area of pseudorandom sequences. First, we obtain an improved bound on the general lattice test for digital explicit inversive and digital explicit nonlinear pseudorandom number generators. Second, we improve the bound on the correlation measure of binary sequences generated by the quadratic character of finite fields. Finally, we improve the bound on the correlation measure of digital explicit inversive pseudorandom numbers, and the bound on their linear complexity profile.

Although we follow essentially the earlier proofs, we improved a crucial step, namely a better estimate on the number of nonempty intersections of 'boxes' of a finite field is given.

1. Introduction

Let $q = p^r$ be a prime power and $\mathbb{F}_q$ be the finite field with q elements. We identify the finite field $\mathbb{F}_p$ with the set of integers $\{0, 1, \dots, p-1\}$. Let $\beta_1, \dots, \beta_r \in \mathbb{F}_q$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. We define the additive order of $\mathbb{F}_q$ in the following way: for $n \in \{0, 1, \dots, q-1\}$ let

$$\xi_n = n_1\beta_1 + n_2\beta_2 + \cdots + n_r\beta_r$$

if

$$n = n_1 + n_2 p + \cdots + n_r p^{r-1}, \quad 0 \le n_1, n_2, \dots, n_r < p.$$

We define $\xi_{n+q} = \xi_n$ for $n \in \{0, 1, \dots, q-1\}$. Let $\mathcal{W} \subseteq \mathbb{F}_q$ be defined as follows:

$$\mathcal{W} = \{w_2\beta_2 + \cdots + w_r\beta_r : w_2, \dots, w_r \in \{0, 1\}\}.$$

For an element $\omega \in \mathcal{W}$ and $a \in \{0, 1, \dots, q-1\}$ we define

$$S_{a,\omega} = \{\xi_n : 0 \le n < q,\ \xi_{n+a} = \xi_n + \xi_a + \omega\}.$$

Let $d_1, \dots, d_k$ be integers with $0 \le d_1 < \cdots < d_k < q$. We look for an upper bound on the number of nonempty elements in the following set of $\mathbb{F}_q$

$$\{S_{d_1,\omega_1} \cap \cdots \cap S_{d_k,\omega_k} : \omega_1, \dots, \omega_k \in \mathcal{W}\}. \tag{1}$$

[*] Corresponding author.
E-mail addresses: merai@cs.elte.hu (L. Mérai), oguz.yayla@hacettepe.edu.tr (O. Yayla).

http://dx.doi.org/10.1016/j.disc.2015.04.015
0012-365X/© 2015 Elsevier B.V. All rights reserved.

For earlier bounds see [3,4,6,10,11]. In [3,6,10,11] the authors used the trivial upper bound $2^{k(r-1)}$, and recently Gómez-Pérez and Gómez [4] obtained the bound $(6rk)^{r-1}$. The main contribution of this paper is to show that the number of nonempty elements in (1) is bounded by $(k+1)^{r-1}$. This refinement ensures improvements of several results for $r \geq 2$ on the pseudorandomness of sequences generated via the additive order in finite fields. We note that our results coincide with the previous results for $r = 1$. In Section 2 we describe these improvements in detail.

Before stating the main result, we give the definition of a box and a remark on the set $S_{a,\omega}$. Let $N_{i,1}$ and $N_{i,2}$ be integers such that $0 \leq N_{i,1} < N_{i,2} < p$. We call a set of the form

$$\{\ell_1\beta_1 + \cdots + \ell_r\beta_r : N_{i,1} \leq \ell_i < N_{i,2}, i = 1, 2, \ldots, r\}$$

as a *box*. Let $w_1 = 0, \omega = w_1\beta_1 + \cdots + w_r\beta_r \in \mathcal{W}$ and $a = a_1 + a_2 p + \cdots + a_r p^{r-1}$ for some $a_1, a_2, \ldots, a_r \in \{0, 1, \ldots, p-1\}$. Then $S_{a,\omega}$ has the form

$$S_{a,\omega} = \Big\{\ell_1\beta_1 + \ell_2\beta_2 + \cdots + \ell_r\beta_r : \max\{0, pw_{i+1} - a_i - w_i\} \leq \ell_i < \min\{p, pw_{i+1} - a_i - w_i + p\},$$
$$i = 1, 2, \ldots, r-1,\ 0 \leq \ell_r < p\Big\}.$$

Hence, $S_{a,\omega}$ is a box. We now state our main theorem.

Theorem 1. *Let $d_1, \ldots, d_k$ be integers with $0 \leq d_1 < \cdots < d_k < q$ and let $\omega_1, \ldots, \omega_k \in \mathcal{W}$. Then the set*

$$S_{d_1,\omega_1} \cap \cdots \cap S_{d_k,\omega_k} = \{\xi_n : 0 \leq n < q, \xi_{n+d_i} = \xi_n + \xi_{d_i} + \omega_i, i = 1, 2, \ldots, k\} \tag{2}$$

is a box or an empty set. If $\omega_1, \ldots, \omega_k$ run over $\mathcal{W}$, then there are at most $(k+1)^{r-1}$-many nonempty sets among them.

Using Theorem 1 one can obtain a similar result in the incomplete case.

Corollary 1. *Let $M \in \{0, 1, \ldots, q-1\}$ and $\mathcal{E} = \{\xi_0, \xi_1, \ldots, \xi_{M-1}\} \subseteq \mathbb{F}_q$. Let $d_1, \ldots, d_k$ be integers with $0 \leq d_1 < \cdots < d_k < q$ and let $\omega_1, \ldots, \omega_k \in \mathcal{W}$. Then, the set*

$$S_{d_1,\omega_1} \cap \cdots \cap S_{d_k,\omega_k} \cap \mathcal{E} = \{\xi_n : 0 \leq n < M, \xi_{n+d_i} = \xi_n + \xi_{d_i} + \omega_i, i = 1, 2, \ldots, k\} \tag{3}$$

can be split into a union of boxes, such that if $\omega_1, \ldots, \omega_k$ run over $\mathcal{W}$, then the number of boxes is $O((k+1)^{r-1})$.

Before presenting the proofs of theorem and corollary, we give some of their applications in Section 2. In particular, we improve the results given in [4,10,11], and [3] in Sections 2.1–2.3 respectively. Next, in Section 3 we give the proofs of Theorem 1 and Corollary 1.

2. Applications

In this section we apply Theorem 1 and Corollary 1 to obtain better results on pseudorandomness of certain sequences.

2.1. On the lattice structure of digital explicit inversive and nonlinear generators

Let

$$\overline{\gamma} = \begin{cases} \gamma^{-1} & \text{if } \gamma \in \mathbb{F}_q^*, \\ 0 & \text{if } \gamma = 0. \end{cases}$$

For given $\alpha \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_q$, a sequence $\gamma_0, \gamma_1, \ldots$ generated by

$$\gamma_n = \overline{\alpha\xi_n + \beta}, \quad n = 0, 1, \ldots \tag{4}$$

is called *digital explicit inversive pseudorandom number generator* (or *Niederreiter–Winterhof generator*), see [7]. The inversive pseudorandom number generator is a special case of *digital explicit nonlinear pseudorandom number generators* (η_n) defined by

$$\eta_n = f(\xi_n) \tag{5}$$

for some polynomial $f(X) \in \mathbb{F}_q[X]$, see [8]. Note that for the inversive generator we have $f(X) = (\alpha X + \beta)^{q-2}$.

In this section we study the general lattice test (first introduced by Niederreiter and Winterhof [9]) for the digital explicit inversive and nonlinear generators. Let (η_n) be a T-periodic sequence over $\mathbb{F}_q$. For given integers $s \geq 1, 0 < d_1 < d_2 < \cdots < d_{s-1} < T$, and $N \geq 2$, we say that (η_n) passes the *s-dimensional N-lattice test with lags* $d_1, d_2, \ldots, d_{s-1}$ if the vectors

$$\{\underline{\eta}_n - \underline{\eta}_0 : 1 \leq n < N\}$$

span $\mathbb{F}_q^s$, where

$$\underline{\eta}_n = (\eta_n, \eta_{n+d_1}, \ldots, \eta_{n+d_{s-1}}), \quad 0 \leq n < N.$$

The greatest dimension s such that (η_n) satisfies the s-dimensional N lattice test for all lags $d_1, \ldots, d_{s-1}$ is denoted by $S(\eta_n, N)$.

Pirsic and Winterhof [10] studied the lattice structure of inversive and nonlinear pseudorandom number generators. They used the upper bound $2^{k(r-1)}$ on the number of possible boxes (2), and obtain that

$$S(\gamma_n, N) \geq \frac{\log(N) - \log\log(N) - 1}{r-1} - 1 \tag{6}$$

and

$$S(\eta_n, N) \geq \frac{\log(N/D)}{r-1} - 1$$

for $2 \leq N \leq q$ and $r \geq 2$, where (γ_n) is defined by (4), and (η_n) is defined by (5) with a nonidentical zero function $f(X) \in \mathbb{F}_q[X]$ of degree D.

Later Gómez-Pérez and Gómez [4] improved the bound (6)

$$S(\gamma_n, N) \geq \frac{1}{6}\left(\frac{N}{r^{r-1}}\right)^{1/r} \tag{7}$$

for $2 \leq N \leq q$ and $r \geq 2$.

Using Theorem 1 in the proof of [10] gives the following improved bounds:

$$S(\gamma_n, N) \geq \left(\frac{N}{2}\right)^{1/r} - 1$$

and

$$S(\eta_n, N) \geq \left(\frac{N}{D}\right)^{1/(r-1)} - 1$$

for $2 \leq N \leq q$ and $r \geq 2$. We remark that in these bounds the constant terms do not depend on r anymore.

2.2. On the correlation measure of binary sequences defined by the quadratic character

Let

$$E_N = \{e_0, \ldots, e_{N-1}\} \in \{-1, +1\}^N$$

be a binary sequence of length N. The *correlation measure of order* k of E_N is defined as

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=0}^{M-1} e_{n+d_1} e_{n+d_2} \ldots e_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and M such that $0 \leq d_1 < d_2 < \cdots < d_k \leq N - M$. This measure was first introduced by Mauduit and Sárközy [5]. For a “good” pseudorandom sequence E_N, $C_k(E_N)$ (for “small” k) is small and is ideally greater than $N^{1/2}$ only by at most a power of $\log N$, see [1].

The linear complexity profile is an important cryptographic characteristic of pseudorandom sequences. A low linear complexity profile has turned out to be undesirable for cryptographic applications.

We recall that the *linear complexity profile* $L(R_T, N)$ of the sequence $R_T = (r_0, r_1, \ldots, r_{T-1})$ is a non-decreasing sequence where the Nth term is defined as the shortest length L of a linear recurrence relation over $\mathbb{F}_2$

$$r_{n+L} = c_{L-1} r_{n+L-1} + \cdots + c_0 r_n, \quad 0 \leq n \leq N - L - 1,$$

which is satisfied by this sequence.

Let χ be the quadratic character of $\mathbb{F}_q$. Sárközy and Winterhof [11] defined a binary sequence $L_q = (l_0, l_1, \ldots, l_{q-1}) \in \{-1, 1\}^q$ by

$$l_n = \begin{cases} \chi(f(\xi_n)) & \text{if } f(\xi_n) \neq 0, \\ 1 & \text{if } f(\xi_n) = 0, \end{cases} \quad 0 \leq n < q.$$

They proved that if $f(X) \in \mathbb{F}_q[X]$ has no multiple zero, and if either

(i) $k = 2$ and $\deg f < p$

or

(ii) $4^{r(k+\deg f)} < p$,

then

$$C_k(L_q) = O(2^{(r-1)k} r 2^r k \deg f q^{1/2} (\log p)^r),$$

By applying Corollary 1, we get in the same way as in [11] that the correlation measure satisfies

$$C_k(L_q) = O((k+1)^{r-1} k \deg f q^{1/2} (\log p)^r)$$

under the same conditions (i) and (ii).

Moreover, if $f(X)$ is a linear polynomial, then we get

$$C_k(L_q) = O((k+1)^{r-1} k q^{1/2} (\log p)^r)$$

without conditions on k of type (i) or (ii). Therefore by [2, Theorem 1] we get a non-trivial lower bound on the linear complexity profile of the sequence $S_q = (s_0, s_1, \dots, s_{q-1}) \in \{0,1\}^q$ defined by $s_n = (l_n + 1)/2$

$$L(S_q, N) = \Omega\left(\frac{N^{1/r}}{p^{1/2}\log p}\right), \quad 2 \le N < q.$$

2.3. On the linear complexity profile of the threshold sequence for digital explicit inversive pseudorandom numbers

Let (γ_n) be a sequence of digital explicit inversive pseudorandom numbers defined by (4). If

$$\gamma_n = c_{n,1}\beta_1 + c_{n,2}\beta_2 + \dots + c_{n,r}\beta_r$$

with $0 \le c_{n,i} < p$ (for all i, j), we define *digital explicit inversive pseudorandom numbers* of period q in the interval $[0, 1)$ by defining

$$y_n = \sum_{j=1}^{r} c_{n,j} p^{-j}, \quad n = 0, 1, \dots$$

We here derive a bound on the correlation measure of order k of the binary sequences $E_q = (e_0, e_1, \dots, e_{q-1})$ defined by

$$e_n = \begin{cases} 1 & \text{if } 0 \le y_n < \dfrac{1}{2}, \\ -1 & \text{if } \dfrac{1}{2} \le y_n < 1, \end{cases} \quad n = 0, 1, \dots, q-1,$$

and also the linear complexity profile of the associated bit sequence $R_q = (r_0, r_1, \dots, r_{q-1}) \in \{0,1\}^q$, where $r_n := (e_n + 1)/2$.

Chen, Gomez, and Winterhof [3] studied the correlation measure of digital explicit inversive pseudorandom numbers and their linear complexity profile. They use the upper bound $r2^r 2^{k(r-1)}$ on the number of possible boxes (3), and obtain that

$$C_k(E_q) = O\Big(r2^r 2^{k(r-1)} k q^{1/2} (\log q)^k (1 + \log p)^r\Big)$$

and

$$L(R_q, N) = \Omega\left(\frac{\log(Nq^{-1/2} 2^{-r} r^{-1} (1+\log p)^{-r})}{r + \log\log q}\right), \quad 2 \le N < q.$$

Using Corollary 1 in the proof of [3] gives the improved bound:

$$C_k(E_q) = O\Big((k+1)^r q^{1/2} (\log q)^k (1 + \log p)^r\Big)$$

and by [2, Theorem 1]:

$$L(R_q, N) = \Omega\left(\frac{\log\big(Nq^{-1/2}(1+\log p)^{-r}(\log q^{1/2})^{-r}(\log\log q)^r\big)}{\log\log q}\right),$$

for $2 \le N < q$.

3. Proofs

Proof of Theorem 1. We can assume that $r \ge 2$ since otherwise the theorem is obvious. Let $L_{i,1}$ and $L_{i,2}$ be integers as follows:

$$L_{i,1} = \max\{0, pw_{1,i+1} - d_{1,i} - w_{1,i}, \dots, pw_{k,i+1} - d_{k,i} - w_{k,i}\}$$

and

$$L_{i,2} = \min\{p, pw_{1,i+1} - d_{1,i} - w_{1,i} + p, \dots, pw_{k,i+1} - d_{k,i} - w_{k,i} + p\}$$

for $i \in \{1, 2, \dots, r-1\}$, where $0 \le d_1 < \dots < d_k < q$ and $\omega_1, \dots, \omega_k \in \mathcal{W}$ such that $d_j = \sum_{i=1}^{r} d_{j,i} p^{i-1}$, $0 \le d_{j,i} < p$ and $\omega_j = w_{j,2}\beta_2 + \dots + w_{j,r}\beta_r$. We also define $L_{r,1} = 0$ and $L_{r,2} = p$.

Then clearly

$$S_{d_1,\omega_1} \cap \ldots \cap S_{d_k,\omega_k} = \{\ell_1\beta_1 + \dots + \ell_r\beta_r : L_{i,1} \le \ell_i < L_{i,2}, i = 1, 2, \dots, r\}$$

is a box or empty.

In order to prove the bound on the number of nonempty sets having the form (2), we write (2) as an intersection of decreasing boxes, when the k-tuple $(d_1, \dots, d_k)$ is fixed.

First, let $\overline{\omega}_t \in \{0, 1\}^k$ (for $t = 1, \dots, r$) be a tuple of the tth coordinates of $\omega_1, \dots, \omega_k$: $\overline{\omega}_t = (w_{1,t}, \dots, w_{k,t})$. In particular, $\overline{\omega}_1$ is the zero vector. For a $\overline{\omega}_2 \in \{0, 1\}^k$ we define $H^1(\overline{\omega}_2)$ as follows:

$$H^1(\overline{\omega}_2) = \{a \in \mathbb{F}_p : L_{1,1} \le a < L_{1,2}\}.$$

It is clear that the sets in $\{H^1(\overline{\omega}_2) : \overline{\omega}_2 \in \{0, 1\}^k\}$ split $\mathbb{F}_p$:

(i) $H^1(\overline{\omega}_2) \subset \mathbb{F}_p$,
(ii) $H^1(\overline{\omega}_2) \cap H^1(\overline{\omega}_2') = \emptyset$, for $\overline{\omega}_2 \neq \overline{\omega}_2'$,
(iii) $\bigcup_{\overline{\omega}_2 \in \{0,1\}^k} H^1(\overline{\omega}_2) = \mathbb{F}_p$.

Moreover, there are at most $k + 1$ nonempty sets among them. Indeed, for an $a \in \mathbb{F}_p$ we have

$$a \ge p - d_{j,1} \Leftrightarrow w_{j,2} = 1, \quad \text{for } j = 1, 2, \dots, k,$$

which means that there is a unique vector $\overline{\omega}_2 \in \{0, 1\}^k$ such that $a \in H^1(\overline{\omega}_2)$. Let σ be a permutation of $\{1, \dots, k\}$ such that

$$d_{\sigma(1),1} \le \dots \le d_{\sigma(k),1}.$$

Then, the possible sets of $H^1(\overline{\omega}_2)$ are

(i) $[0, p - d_{\sigma(k),1}) \cap \mathbb{N}$,
(ii) $[p - d_{\sigma(i),1}, p - d_{\sigma(i-1),1}) \cap \mathbb{N}$, for $i = 2, 3, \dots, k$,
(iii) $[p - d_{\sigma(1),1}, p) \cap \mathbb{N}$

and the empty set.

Let

$$\begin{aligned} C^1(\overline{\omega}_2) &= H^1(\overline{\omega}_2) \times \mathbb{F}_p^{r-1} \\ &= \{\ell_1\beta_1 + \ell_2\beta_2 + \dots + \ell_r\beta_r : \ell_1 \in H^1(\overline{\omega}_2), \ell_2, \dots, \ell_r \in \mathbb{F}_p\}. \end{aligned}$$

By recursion we split a non-empty set $C^{t-1}(\overline{\omega}_2, \dots, \overline{\omega}_t)$ $(t = 2, 3, \dots, r - 1)$ as a disjoint union

$$C^{t-1}(\overline{\omega}_2, \dots, \overline{\omega}_t) = \bigcup_{\overline{\omega}_{t+1} \in \{0,1\}^k} C^t(\overline{\omega}_2, \dots, \overline{\omega}_t, \overline{\omega}_{t+1})$$

such that there are at most $k + 1$-many non-empty sets $C^t(\overline{\omega}_2, \dots, \overline{\omega}_t, \overline{\omega}_{t+1})$ when $\overline{\omega}_{t+1}$ runs in $\{0, 1\}^k$.

Assume that $C^{t-1}(\overline{\omega}_2, \dots, \overline{\omega}_t)$ is defined for $2 \le t < r - 1$ and the k-tuples $\overline{\omega}_2, \dots, \overline{\omega}_t$ are fixed. Define the sets $H^t(\overline{\omega}_{t+1})$ as

$$H^t(\overline{\omega}_{t+1}) = \{a \in \mathbb{F}_p : L_{t,1} \le a < L_{t,2}\}.$$

The sets in $\{H^t(\overline{\omega}_{t+1}) : \overline{\omega}_{t+1} \in \{0, 1\}^k\}$ split $\mathbb{F}_p$:

(i) $H^t(\overline{\omega}_{t+1}) \subset \mathbb{F}_p$,
(ii) $H^t(\overline{\omega}_{t+1}) \cap H^t(\overline{\omega}_{t+1}') = \emptyset$, for $\overline{\omega}_{t+1} \neq \overline{\omega}_{t+1}'$,
(iii) $\bigcup_{\overline{\omega}_{t+1} \in \{0,1\}^k} H^t(\overline{\omega}_{t+1}) = \mathbb{F}_p$.

Similar to the case $t = 1$, there are at most $k + 1$ nonempty sets among them. Indeed, for an integer $a \in \mathbb{F}_p$ we have

$$a \ge p - d_{j,t} - w_{j,t} \Leftrightarrow w_{j,t+1} = 1, \quad \text{for } j = 1, \dots, k.$$

Then we define $C^t(\overline{\omega}_2, \dots, \overline{\omega}_t, \overline{\omega}_{t+1})$ as

$$C^t(\overline{\omega}_2, \dots, \overline{\omega}_t, \overline{\omega}_{t+1}) = \{\ell_1\beta_1 + \ell_2\beta_2 + \dots + \ell_r\beta_r \in C^{t-1}(\overline{\omega}_2, \dots, \overline{\omega}_t) : \ell_t \in H^t(\overline{\omega}_{t+1})\}.$$

We finish the proof of Theorem 1 by observing that

$$S_{d_1,\omega_1} \cap \dots \cap S_{d_k,\omega_k} = C^{r-1}(\overline{\omega}_2, \dots, \overline{\omega}_r).$$

Proof of Corollary 1. Let $M \in \{0, 1, \dots, q - 1\}$ and $d_1, \dots, d_k < q$ with $0 \le d_1 < \dots < d_k < q$ be given integers. We look for the intersection of $S_{d_1,\omega_1} \cap \dots \cap S_{d_k,\omega_k}$ and the set $\mathcal{E} = \{\xi_0, \dots, \xi_{M-1}\} \subseteq \mathbb{F}_q$ for tuples $(\omega_1, \dots, \omega_k) \in \mathcal{W}^k$. This intersection has at most r boxes for only the tuple $(\omega_1^0, \dots, \omega_k^0) \in \mathcal{W}^k$ where $\xi_{M-1} \in S_{d_1,\omega_1^0} \cap \dots \cap S_{d_k,\omega_k^0}$. Moreover, there are $(k + 1)$ tuples for which the intersection consists of at most $(r - 1)$ boxes. By Theorem 1 we know that we have at most $(k + 1)^{r-1}$ tuples for which $S_{d_1,\omega_1} \cap \dots \cap S_{d_k,\omega_k}$ is nonempty. Therefore, in the final step there are $(k + 1)^{r-1}$ tuples whose intersection with $\{\xi_0, \xi_2, \dots, \xi_{M-1}\}$ consists of at most one box. If we sum them up we obtain that

$$\sum_{i=0}^{r-1} (r - i)(k + 1)^i = \frac{(k + 1)^{r+1} - (r + 1)k - 1}{k^2} = O((k + 1)^{r-1}).$$

Acknowledgments

The authors thank Arne Winterhof for useful suggestions. This paper was prepared when the second author visited Johann Radon Institute for Computational and Applied Mathematics (RICAM), Linz. He was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant No. 2219. The hospitality of RICAM is gratefully acknowledged. The first author was partially supported by Hungarian National Foundation for Scientific Research, Grant No. K100291 and by the Austrian Science Fund (FWF): Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

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. (3) 95 (3) (2007) 778–812.

[2] N. Brandstätter, A. Winterhof, Linear complexity profile of binary sequences with small correlation measure, Period. Math. Hungar. 52 (2) (2006) 1–8.

[3] Z. Chen, D. Gomez, A. Winterhof, Distribution of digital explicit inversive pseudorandom numbers and their binary threshold sequence, in: Monte Carlo and quasi-Monte Carlo Methods 2008, Springer, Berlin, 2009, pp. 249–258.

[4] D. Gómez-Pérez, A. Gómez, On the lattice structure of inverse PRNG via the additive order, in: Sequences and Their Applications—SETA 2014, in: Lecture Notes in Comput. Sci., vol. 8865, Springer, Berlin, 2014, pp. 212–219.

[5] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol, Acta Arith. 82 (4) (1997) 365–377.

[6] W. Meidl, A. Winterhof, On the autocorrelation of cyclotomic generators, in: Finite Fields and Applications, in: Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 1–11.

[7] H. Niederreiter, A. Winterhof, Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators, Acta Arith. 93 (4) (2000) 387–399.

[8] H. Niederreiter, A. Winterhof, On the lattice structure of pseudorandom numbers generated over arbitrary finite fields, Appl. Algebra Engrg. Comm. Comput. 12 (3) (2001) 265–272.

[9] H. Niederreiter, A. Winterhof, On the structure of inversive pseudorandom number generators, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, in: Lecture Notes in Comput. Sci., vol. 4851, Springer, Berlin, 2007, pp. 208–216.

[10] G. Pirsic, A. Winterhof, On the structure of digital explicit nonlinear and inversive pseudorandom number generators, J. Complexity 26 (1) (2010) 43–50.

[11] A. Sárközy, A. Winterhof, Measures of pseudorandomness for binary sequences constructed using finite fields, Discrete Math. 309 (6) (2009) 1327–1333.