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 $\{0, 1, \ldots, p-1\}$. Let $\beta_1, \ldots, \beta_r \in \mathbb{F}_q$ 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 $n \in \{0, 1, \ldots, q-1\}$ let

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

if

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

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

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

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

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

Let $d_1, \ldots, d_k$ 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 $\mathbb{F}_q$

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

* 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/

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 $a = a_1 + a_2p + \cdots + a_rp^{r-1}$ 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 $S(\eta_n, N)$.