Distribution of Digital Explicit Inversive Pseudorandom Numbers and Their Binary Threshold Sequence

Zhixiong Chen, Domingo Gomez and Arne Winterhof

[1] Zhixiong Chen 1. Key Laboratory of Applied Mathematics, Putian University, Putian, Fujian 351100, P.R.China; 2. Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian 350007, P.R.China. e-mail: ptczx@126.com.
[2] Domingo Gomez Faculty of Sciences, University of Cantabria, 39071 Santander, Spain, `http://personales.unican.es/gomezd/.` e-mail: domingo.gomez@unican.es.
[3] Arne Winterhof Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria, `http://www.ricam.oeaw.ac.at/people/page.cgi?firstn=Arne;lastn=Winterhof.` e-mail: arne.winterhof@oeaw.ac.at.

In memory of Edmund Hlawka

Summary. * We study the distribution of s-dimensional points of digital explicit inversive pseudorandom numbers with arbitrary lags. We prove a discrepancy bound and derive results on the pseudorandomness of the binary threshold sequence derived from digital explicit inversive pseudorandom numbers in terms of bounds on the correlation measure of order k and the linear complexity profile. The proofs are based on bounds on exponential sums and earlier relations of Mauduit, Niederreiter and Sárközy between discrepancy and correlation measure of order k and of Brandstätter and the third author between correlation measure of order k and linear complexity profile, respectively.

Summary. We study the distribution of s-dimensional points of digital explicit inversive pseudorandom numbers with arbitrary lags. We prove a discrepancy bound and derive results on the pseudorandomness of the binary threshold sequence derived from digital explicit inversive pseudorandom numbers in terms of bounds on the correlation measure of order k and the linear complexity profile. The proofs are based on bounds on exponential sums and earlier relations of Mauduit, Niederreiter and Sárközy between discrepancy and correlation measure of order k and of Brandstätter and the third author between correlation measure of order k and linear complexity profile, respectively.

1 Introduction

Inversive methods are attractive alternatives to the linear method for generating pseudorandom numbers, see the recent surveys [11, 12, 17]. In this paper we analyze the distribution of *digital explicit inversive pseudorandom numbers* introduced in [13] and further analyzed in [6, 13, 14, 15, 16].

Let $q = p^r$ be a prime power and $\mathbb{F}_q$ the finite field of order q. Let

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

We order the elements of $\mathbb{F}_q = \{\xi_0, \xi_1, \dots, \xi_{q-1}\}$ using an ordered basis $\{\gamma_1, \dots, \gamma_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ for $0 \le n < q$,

$$\xi_n = n_1\gamma_1 + n_2\gamma_2 + \dots + n_r\gamma_r,$$

if

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

For $n \ge 0$ we define $\xi_{n+q} = \xi_n$. Then the *digital explicit inversive pseudorandom number generator* of period q is defined by

$$\rho_n = \overline{\alpha\xi_n + \beta},\ n = 0, 1, \dots$$

for some $\alpha, \beta \in \mathbb{F}_q$ with $\alpha \ne 0$.

If

$$\rho_n = c_{n,1}\gamma_1 + c_{n,2}\gamma_2 + \dots + c_{n,r}\gamma_r$$

with all $c_{n,i} \in \mathbb{F}_p$, we derive *digital explicit inversive pseudorandom numbers of period q* in the interval $[0,1)$ by defining

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

For $s \ge 1$ the distribution of points $(y_n, y_{n\oplus 1}, \dots, y_{n\oplus(s-1)})$, where $n \oplus k = d$ if $\xi_n + \xi_k = \xi_d$, $0 \le n, k, d < q$, was studied in [13]. Here we study the distribution of the points $(y_{n+d_1}, \dots, y_{n+d_s})$ for any integers $0 \le d_1 < \dots < d_s < q$ and the integer addition $+$. We prove a discrepancy bound which is based on estimates for exponential sums generalizing the earlier result of the first author [3] for $s = 2$ using some additional ideas.

As applications we use some results of [4] and [1] to derive bounds on the *correlation measure of order k* and *linear complexity profile* of the binary sequences $\mathscr{R}_q = (r_0, r_1, \dots, r_{q-1})$ defined by

$$r_n = \begin{cases} 0, & \text{if } 0 \le y_n < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \le y_n < 1, \end{cases} \quad 0 \le n < q. \tag{2}$$

Note that for such applications a discrepancy bound with arbitrary lags $0 \le d_1 < \dots < d_s < q$ is needed. Most known discrepancy bounds on nonlinear pseudorandom numbers found in the literature consider only the special lags $d_i = i - 1$ for $i = 1, \dots, s$. In many cases the analysis of the discrepancy becomes much more intricate for arbitrary lags, see for example [10].

We recall that the correlation measure of order k, introduced by Mauduit and Sárközy in [5], is an important measure of pseudorandomness for finite binary sequences. For a finite binary sequence

$$\mathscr{S}_N = \{s_0, s_1, \dots, s_{N-1}\} \in \{0,1\}^N,$$

the *correlation measure of order k* of $\mathscr{S}_N$ is defined as

$$C_k(\mathscr{S}_N) = \max_{M,D} \left| \sum_{n=1}^{M} (-1)^{s_{n+d_1}+s_{n+d_2}+\cdots+s_{n+d_k}} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ with non-negative integers $0 \le d_1 < \cdots < d_k$ and M such that $M + d_k \le N - 1$. For a "good" pseudorandom sequence $\mathscr{S}_N$, $C_k(\mathscr{S}_N)$ (for "small" k) is small and is ideally greater than $N^{1/2}$ only by at most a power of $\log N$, see [2].

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

For a T-periodic binary sequence $\mathscr{S}_T = (s_0, s_1, \ldots, s_{T-1})$ over $\mathbb{F}_2$, the *linear complexity profile* $L(\mathscr{S}_T, N)$ is the function which is defined as the shortest length L of a linear recurrence relation over $\mathbb{F}_2$ for $N > 1$

$$s_{n+L} = c_{L-1}s_{n+L-1} + \cdots + c_0 s_n, \ 0 \le n \le N - L - 1,$$

which is satisfied by this sequence.

The discrepancy bound is proved in Section 2, and the bounds on the correlation measure of order k and the linear complexity profile are given in Sections 3 and 4.

2 Discrepancy Bound

In this section we estimate the discrepancy of the points

$$\mathbf{Y}_n = (y_{n+d_1}, \ldots, y_{n+d_s}) \in [0,1)^s, \ n = 0, 1, \ldots, N-1,$$

for any non-negative integers $d_1, \ldots, d_s$ with $0 \le d_1 < \cdots < d_s < q$ and $1 \le N \le q$. We recall that the *discrepancy* of the points $\mathbf{Y}_0, \ldots, \mathbf{Y}_{N-1}$, denoted by $\mathscr{D}_N(d_1, \ldots, d_s)$, is defined by

$$\mathscr{D}_N(d_1, \ldots, d_s) = \sup_{J \subseteq [0,1)^s} \left| \frac{A(J,N)}{N} - |J| \right|,$$

where $A(J,N)$ is the number of points $\mathbf{Y}_0, \ldots, \mathbf{Y}_{N-1}$ which hit the box $J = [\alpha_1, \beta_1) \times \cdots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$, the volume $|J|$ of an interval J is given by $\prod_{i=1}^{s}(\beta_i - \alpha_i)$ and the supremum is taken over all such boxes, see e.g. [9].

Theorem 1. *Let $y_0, y_1, \ldots$ be the sequence defined by (1). For any non-negative integers $d_1, \ldots, d_s$ with $d_1 < \cdots < d_s < q$ and $1 \le N \le q$, the discrepancy $\mathscr{D}_N(d_1, \ldots, d_s)$ of the points*

$$\mathbf{Y}_n = (y_{n+d_1}, \ldots, y_{n+d_s}) \in [0,1)^s, \ n = 0, 1, \ldots, N-1,$$

satisfies

$$\mathscr{D}_N(d_1, \ldots, d_s) = O(N^{-1} 2^{r+rs} rs q^{1/2} (\log q)^s (1 + \log p)^r),$$

where the implied constant is absolute.

Proof. Let $\lambda_{ij} \in \mathbb{F}_p$ $(1 \le i \le s, 1 \le j \le r)$ be not all zero and put $e_p(x) = \exp(2\pi\sqrt{-1}x/p)$ and

$$S_N = S_N(\lambda_{11}, \dots, \lambda_{sr}) = \sum_{n=0}^{N-1} e_p\left(\sum_{i=1}^{s}\sum_{j=1}^{r} \lambda_{ij} c_{n+d_i,j}\right),$$

where the $c_{i,j}$ are defined in (1). According to [9, Proposition 2.4, Theorem 3.12 and Lemma 3.13] we have

$$\mathscr{D}_N(d_1, \dots, d_s) \ll 2^s (\log q)^s \frac{1}{N} \max_{\lambda_{11},\dots,\lambda_{sr}} |S_N(\lambda_{11}, \dots, \lambda_{sr})|, \tag{3}$$

where the maximum is taken over all nonzero vectors $(\lambda_{11}, \dots, \lambda_{sr}) \in \mathbb{F}_p^{sr} \setminus \{(0, \dots, 0)\}$. Hence it suffices to estimate S_N above.

Let $\{\gamma_1', \dots, \gamma_r'\}$ be the dual basis of the ordered basis $\{\gamma_1, \dots, \gamma_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then we have

$$\begin{aligned} S_N &= \sum_{n=0}^{N-1} e_p\left(\sum_{i=1}^{s}\sum_{j=1}^{r} \lambda_{ij} \mathrm{Tr}(\gamma_j' \rho_{n+d_i})\right) \\ &= \sum_{n=0}^{N-1} e_p\left(\mathrm{Tr}\left(\sum_{i=1}^{s}\sum_{j=1}^{r} \lambda_{ij} \gamma_j' \rho_{n+d_i}\right)\right) \\ &= \sum_{n=0}^{N-1} \psi\left(\sum_{i=1}^{s} \mu_i \rho_{n+d_i}\right), \end{aligned}$$

where Tr denotes the absolute trace of $\mathbb{F}_q$, ψ is the additive canonical character of $\mathbb{F}_q$ and

$$\mu_i = \sum_{j=1}^{r} \lambda_{ij} \gamma_j', \;\; i = 1, \dots, s.$$

Since $\lambda_{ij} \in \mathbb{F}_p$ $(1 \le i \le s, 1 \le j \le r)$ are not all zero and $\{\gamma_1', \dots, \gamma_r'\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, it follows that $\mu_1, \dots, \mu_s$ are not all zero.

First we present three auxiliary steps for the proof.

(i). We call a set of the form $\{\delta + n_1\gamma_1 + \cdots + n_r\gamma_r : 0 \le n_i < N_i, i = 1, \dots, r\}$ for some integers $0 \le N_1, \dots, N_r \le p$ and $\delta \in \mathbb{F}_q$ a *box*. Note that the empty set is also a box and that the intersection of a family of boxes is the union of at most 2^r boxes. (For $r = 1$ this is trivial and in general each r-dimensional box is the direct product of r one-dimensional boxes.)

As in the proof of [7, Theorem 2], it can be verified that for $0 \le \tau, m < q$ there are only 2^{r-1} different $\omega \in \mathbb{F}_q$, namely,

$$\omega = w_2\gamma_2 + \cdots + w_r\gamma_r, \quad w_2, \dots, w_r \in \{0, 1\}, \tag{4}$$

such that

$$\xi_{m+\tau} = \xi_m + \xi_\tau + \omega,$$

where we used the definition $\xi_{m+q} = \xi_m$, $m = 0, \dots, q-1$. We are going to prove that the sets

$$S_{\tau,\omega} = \{\xi_m : 0 \le m < q, \; \xi_{m+\tau} = \xi_m + \xi_\tau + \omega\}$$

are boxes. For $0 \le \tau, m < q$, let

$$\tau = \tau_1 + \tau_2 p + \cdots + \tau_r p^{r-1}, \;\; 0 \le \tau_1, \tau_2, \dots, \tau_r < p$$

and

$$m = m_1 + m_2 p + \cdots + m_r p^{r-1}, \;\; 0 \le m_1, m_2, \ldots, m_r < p.$$

Put

$$w_1 = 0, \;\; w_{i+1} = \begin{cases} 1, \text{ if } m_i + \tau_i + w_i \ge p, \\ 0, \text{ otherwise}, \end{cases}$$

for $i = 1, 2, \ldots, r$. We get

$$m + \tau = z_1 + z_2 p + \cdots + z_r p^{r-1}, \;\; 0 \le z_1, z_2, \ldots, z_r < p$$

where

$$z_i = m_i + \tau_i + w_i - w_{i+1} p, \;\; 1 \le i \le r.$$

Then we get

$$\xi_{m+\tau} = \xi_m + \xi_\tau + \omega,$$

where

$$\omega = w_2 \gamma_2 + \cdots + w_r \gamma_r.$$

Note that for fixed τ and ω the sets $S_{\tau,\omega}$ define a partition of $\mathbb{F}_q$ and we have

$$S_{\tau,\omega} = \{\delta + u_1 \gamma_1 + \cdots + u_r \gamma_r : 0 \le u_j < k_j, j = 1, \ldots, r\},$$

where

$$\delta = \sum_{\substack{j=1 \\ w_{j+1}=1}}^{r-1} (p - \tau_j - w_j)\gamma_j$$

and

$$k_j = \begin{cases} p - \tau_j - w_j, & \text{if } w_{j+1} = 0, 1 \le j < r, \\ \tau_j + w_j, & \text{if } w_{j+1} = 1, 1 \le j < r, \\ p, & \text{if } j = r. \end{cases}$$

So the sets $S_{\tau,\omega}$ are all boxes.

(*ii*). For $0 \le d_1 < d_2 < \cdots < d_s < q$ and $\omega_1, \ldots, \omega_s \in \mathbb{F}_q$ of the form (4) the sets

$$S_{d_1,\omega_1} \cap \cdots \cap S_{d_s,\omega_s} = \{\xi_n : 0 \le n < q, \xi_{n+d_i} = \xi_n + \xi_{d_i} + \omega_i, i = 1, \ldots, s\}$$

are unions of at most 2^r boxes. As in the proof of [7, Theorem 4] for $1 \le N \le q$, below we verify that the intersection of a box B with $\{\xi_0, \ldots, \xi_{N-1}\}$ is a union of r boxes. Write $B' = B \cap \{\xi_0, \ldots, \xi_{N-1}\}$.

Let $l = \left\lfloor \frac{\log N}{\log p} \right\rfloor + 1$, we write

$$N = v_1 + v_2 p + \cdots + v_l p^{l-1}, \;\; 0 \le v_1, v_2, \ldots, v_l < p.$$

We give a partition for B' by defining

$$\begin{aligned} &V_{2,\omega} = \{\xi_m \in B | m_1 \le v_1, m_2 = v_2, \ldots, m_l = v_l\}, \\ &V_{j,\omega} = \{\xi_m \in B | 0 \le m_1, \ldots, m_{j-2} < p, \\ &\qquad\qquad m_{j-1} \le v_{j-1} - 1, m_j = v_j, \ldots, m_l = v_l\}, \\ &\text{where } j = 3, 4, \ldots, l, \text{ and} \\ &V_{1,\omega} = \{\xi_m \in B | 0 \le m_1, \ldots, m_{l-1} < p, \; m_l \le v_l - 1\}. \end{aligned}$$

It is easy to see that each $V_{j,\omega}$ is a box since on the coefficients of the ξ_m only possibly more constraints are added.

In summary, there are $2^{(r-1)s}$ possible choices for $\omega_1,\dots,\omega_s \in \mathbb{F}_q$. For fixed $\omega_1,\dots,\omega_s \in \mathbb{F}_q$, $S_{d_1,\omega_1}\cap\cdots\cap S_{d_s,\omega_s}$ is a union of at most 2^r boxes B, while $B\cap\{\xi_0,\dots,\xi_{N-1}\}$ is a union of r boxes $V_{j,\omega}$.

(iii). Let $B=\{\delta+n_1\gamma_1+\cdots+n_r\gamma_r : 0\le n_i<N_i, i=1,\dots,r\}$ with $0\le N_1,\dots,N_r\le p$ and $\delta\in\mathbb{F}_q$ be a box. By [18, Lemma 6], we have

$$\sum_{\varsigma\in\mathbb{F}_q^*}\left|\sum_{\xi\in B}\psi(\varsigma\xi)\right| < q(1+\log p)^r.$$

Now we continue the proof. Let

$$\mathbf{I}(\omega_1,\dots,\omega_s)=S_{d_1,\omega_1}\cap\cdots\cap S_{d_s,\omega_s}\cap\{\xi_0,\dots,\xi_{N-1}\}.$$

We note that if $\xi_{d_i}+\omega_i=\xi_{d_j}+\omega_j$ for $i<j$, then there is no n with $0\le n<q$ such that

$$\xi_{n+d_i}=\xi_n+\xi_{d_i}+\omega_i \quad \text{and} \quad \xi_{n+d_j}=\xi_n+\xi_{d_j}+\omega_j.$$

Otherwise, suppose n_0 is such a value then $\xi_{n_0+d_i}=\xi_{n_0+d_j}$, which leads to $d_i\equiv d_j \pmod q$, a contradiction. So for ω_i,ω_j with $\xi_{d_i}+\omega_i=\xi_{d_j}+\omega_j$,

$$S_{d_i,\omega_i}\cap S_{d_j,\omega_j}=\emptyset,$$

which leads to

$$\mathbf{I}(\omega_1,\dots,\omega_s)=\emptyset.$$

In such case $|\mathbf{I}(\omega_1,\dots,\omega_s)|=0$. Hence we obtain

$$\begin{aligned}
S_N &= \sum_{n=0}^{N-1}\psi\left(\sum_{i=1}^{s}\mu_i\rho_{n+d_i}\right)\\
&= \sum_{n=0}^{N-1}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha\xi_{n+d_i}+\beta}\right)\\
&= \sum_{\omega_1,\dots,\omega_s}\sum_{\xi\in\mathbf{I}(\omega_1,\dots,\omega_s)}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha(\xi+\xi_{d_i}+\omega_i)+\beta}\right)\\
&= \sum_{\omega_1,\dots,\omega_s}\sum_{x\in\mathbb{F}_q}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha(x+\xi_{d_i}+\omega_i)+\beta}\right)\\
&\qquad \sum_{\xi\in\mathbf{I}(\omega_1,\dots,\omega_s)}\frac{1}{q}\sum_{\varsigma\in\mathbb{F}_q}\psi(\varsigma(x-\xi))\\
&= \frac{1}{q}\sum_{\omega_1,\dots,\omega_s}\sum_{\varsigma\in\mathbb{F}_q}\sum_{\xi\in\mathbf{I}(\omega_1,\dots,\omega_s)}\psi(-\varsigma\xi)\\
&\qquad \sum_{x\in\mathbb{F}_q}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha(x+\xi_{d_i}+\omega_i)+\beta}+\varsigma x\right)\\
&= \sum_{\omega_1,\dots,\omega_s}\frac{|\mathbf{I}(\omega_1,\dots,\omega_s)|}{q}\sum_{x\in\mathbb{F}_q}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha(x+\xi_{d_i}+\omega_i)+\beta}\right)\\
&\quad +\frac{1}{q}\sum_{\omega_1,\dots,\omega_s}\sum_{\varsigma\in\mathbb{F}_q^*}\sum_{\xi\in\mathbf{I}(\omega_1,\dots,\omega_s)}\psi(-\varsigma\xi)\\
&\qquad \sum_{x\in\mathbb{F}_q}\psi\left(\sum_{i=1}^{s}\mu_i\overline{\alpha(x+\xi_{d_i}+\omega_i)+\beta}+\varsigma x\right).
\end{aligned}$$

By [8, Theorem 2] (see also [19, Lemma 1] or [13, Lemma 1]) the sum over x has absolute value $O(sq^{1/2})$ if the rational functions in the argument are not of the form A^p-A. This implies

$$S_N \ll 2^{(r-1)s} s q^{1/2} + 2^{(r-1)s} \cdot s q^{1/2} \cdot \frac{1}{q} \sum_{\varsigma \in \mathbb{F}_q^*} \left| \sum_{\xi \in \mathbf{I}(\omega_1,\dots,\omega_s)} \psi(\varsigma\xi) \right|.$$

In fact in the proof above we only consider the case when $\mathbf{I}(\omega_1,\dots,\omega_s) \neq \emptyset$, which leads to $\xi_{d_i} + \omega_i \neq \xi_{d_j} + \omega_j$ for all $i \neq j$. So both rational functions

$$\sum_{i=1}^{s} \mu_i(\alpha(X + \xi_{d_i} + \omega_i) + \beta)^{-1}$$

and

$$\sum_{i=1}^{s} \mu_i(\alpha(X + \xi_{d_i} + \omega_i) + \beta)^{-1} + \varsigma X$$

are not of the form $A^p - A$, where A is a rational function over $\overline{\mathbb{F}}_q$, by [19, Lemma 2] or [13, Lemma 2].

Now according to Steps (*ii*) and (*iii*) above, we have

$$\begin{aligned}
\sum_{\varsigma \in \mathbb{F}_q^*} \left| \sum_{\xi \in \mathbf{I}(\omega_1,\dots,\omega_s)} \psi(\varsigma\xi) \right| &\leq 2^r \sum_{\varsigma \in \mathbb{F}_q^*} \left| \sum_{j=1}^{l} \sum_{\xi \in V_{j,\omega}} \psi(\varsigma\xi) \right| \\
&\leq 2^r \sum_{j=1}^{l} \sum_{\varsigma \in \mathbb{F}_q^*} \left| \sum_{\xi \in V_{j,\omega}} \psi(\varsigma\xi) \right| \\
&\ll 2^r l q (1 + \log p)^r \leq 2^r r q (1 + \log p)^r.
\end{aligned}$$

Putting everything together, we obtain

$$S_N = O\left(2^{(r-1)s} 2^r r s q^{1/2} (1 + \log p)^r\right).$$

Now (3) yields the theorem. □

Note that the bound converges slowly if s is large.

3 Correlation Measure of Order k

The correlation measure of order $k = 2$ of $\mathscr{R}_q$ satisfies

$$C_2(\mathscr{R}_q) = O(q^{1/2} (\log q)^2 (1 + \log p)^r)$$

with implied constant depending on r, see [3]. In this paper, we now extend this result to the case of $k > 2$.

Theorem 2. *The correlation measure of order k of $\mathscr{R}_q$ defined by (2) satisfies*

$$C_k(\mathscr{R}_q) = O(2^r 2^{(r+1)k} r k q^{1/2} (\log q)^k (1 + \log p)^r).$$

Proof. By [4, Theorem 1] and Theorem 1, we have

$$\begin{aligned}
\left| \sum_{n=1}^{M} (-1)^{r_{n+d_1} + \cdots + r_{n+d_k}} \right| &\leq 2^k M \mathscr{D}_{M+d_k}(d_1,\dots,d_k) \\
&= O(2^r 2^{(r+1)k} r k q^{1/2} (\log q)^k (1 + \log p)^r)
\end{aligned}$$

and the result follows. □

Note that the result is only nontrivial if p is large enough.

4 Linear Complexity Profile

In [1, Theorem 1], Brandstätter and the third author used the correlation measure of order k to estimate the linear complexity profile for some related binary sequence $\mathscr{S}_T$:

$$L(\mathscr{S}_T, N) \geq N - \max_{1 \leq k \leq L(\mathscr{S}_T, N)+1} C_k(\mathscr{S}_T) \tag{5}$$

where $2 \leq N \leq T-1$.

Combining (5) and Theorem 2 we get a lower bound on the linear complexity profile of $\mathscr{R}_q$ after simple calculations.

Corollary 1. *The linear complexity profile of* $\mathscr{R}_q$ *defined by* (2) *satisfies*

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

Acknowledgement. Z.X.C. was partially supported by the Open Funds of Key Lab of Fujian Province University Network Security and Cryptology under grant 07B005, the Funds of the Education Department of Fujian Province under grant JA07164 and the Natural Science Foundation of Fujian Province of China under grant 2007F3086.

D.G. was partially supported by the Spanish Ministry of Education and Science grant MTM2007-67088.

A.W. was partially supported by the Austrian Science Fund (FWF) under research grant P-19004-N18.

The authors thank Harald Niederreiter for useful suggestions.

References

1. Brandstätter, N., Winterhof, A.: Linear complexity profile of binary sequences with small correlation measure. Periodica Mathematica Hungarica 52(2), 1–8 (2006)
2. Cassaigne, J., Mauduit, C. Sárközy, A.: On finite pseudorandom binary sequences, VII: the measures of pseudorandomness. Acta Arithmetica 103(2), 97–118 (2002)
3. Chen, Z.: Finite binary sequences constructed by explicit inversive methods. Finite Fields and Their Applications 14(3), 579–592 (2008)
4. Mauduit, C., Niederreiter, H., Sárközy, A.: On pseudorandom $[0,1)$ and binary sequences. Publicationes Mathematicae Debrecen 71(3-4), 305–324 (2007)
5. Mauduit, C., Sárközy, A.: On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol. Acta Arithmetica 82, 365–377 (1997)
6. Meidl, W., Winterhof, A.: On the linear complexity profile of explicit nonlinear pseudorandom numbers. Information Processing Letters 85(1), 13–18 (2003)
7. Meidl, W., Winterhof, A.: On the autocorrelation of cyclotomic generator. In : Fq7, Lecture Notes in Computer Science, vol. 2948, pp.1–11. Springer, Berlin Heidelberg (2003)
8. Moreno, C.J., Moreno, O.: Exponential sums and Goppa codes: I. Proceedings of the American Mathematical Society 111, 523–531 (1991)
9. Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods. SIAM CBMSNSF Regional Conference Series in Applied Mathematics, vol. 63. SIAM, Philadelphia, PA (1992)

10. Niederreiter, H., Rivat, J.: On the correlation of pseudorandom numbers generated by inversive methods. Monatshefte für Mathematik 153(3), 251–264 (2008)
11. Niederreiter, H., Shparlinski, I.E.: Recent advances in the theory of nonlinear pseudorandom number generators. In: Monte Carlo and quasi-Monte Carlo methods 2000, pp.86–102, Springer, Berlin Heidelberg (2002)
12. Niederreiter, H., Shparlinski, I.E.: Dynamical systems generated by rational functions. In: AAECC, Lecture Notes in Computer Science, vol.2643, pp.6–17. Springer-Verlag, Berlin Heidelberg (2003)
13. Niederreiter, H., Winterhof, A.: Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. Acta Arithmetica 93, 387–399 (2000)
14. Niederreiter, H., Winterhof, A.: On a new class of inversive pseudorandom numbers for parallelized simulation methods. Periodica Mathematica Hungarica 42(1), 77–87 (2001)
15. Niederreiter, H., Winterhof, A.: On the lattice structure of pseudorandom numbers generated over arbitrary finite fields. Applicable Algebra in Engineering, Communication and Computing 12(3), 265–272 (2001)
16. Pirsic, G., Winterhof, A.: On the structure of digital explicit nonlinear and inversive pseudorandom number generators. Preprint 2009.
17. Topuzoğlu, A., Winterhof, A.: Pseudorandom sequences. In: Topics in Geometry, Coding Theory and Cryptography. Algebra and Applications, vol.6, pp.135–166, Springer, Dordrecht (2007)
18. Winterhof, A.: Some estimates for character sums and applications. Designs, Codes and Cryptography 22(2), 123–131 (2001)
19. Winterhof, A.: On the distribution of some new explicit inversive pseudorandom numbers and vectors. In: Monte Carlo and Quasi-Monte Carlo Methods 2004, pp. 487–499, Springer, Berlin Heidelberg (2006)