Uniform Distribution Theory **5** (2010), no.1, 79–93

EXPONENTIAL SUMS AND LINEAR COMPLEXITY OF NONLINEAR PSEUDORANDOM NUMBER GENERATORS WITH POLYNOMIALS OF SMALL p-WEIGHT DEGREE

Álvar Ibeas — Arne Winterhof

ABSTRACT. For a class of polynomials $f(X)$ of small p-weight degree over a finite field of characteristic p we improve the general bounds on exponential sums and linear complexity of nonlinear pseudorandom number generators defined by $\mu_{n+1} = f(\mu_n)$, $n = 0, 1, \dots$ with some initial value μ_0. This extends the class of polynomials where a nontrivial exponential sum bound is known. From the bound on exponential sums we derive discrepancy bounds for nonlinear pseudorandom vectors.

Communicated by Shu Tezuka

Dedicated to the memory of Professor Edmund Hlawka

1. Introduction

Let p be a prime, r a positive integer, $q = p^r$ and denote by $\mathbb{F}_q$ the finite field of q elements. Given a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $d \geq 2$, we define the *nonlinear pseudorandom number generator* (μ_n) of elements of $\mathbb{F}_q$ by the recurrence relation

$$\mu_{n+1} = f(\mu_n), \qquad n = 0, 1, \dots \tag{1}$$

with some *initial value* $\mu_0 \in \mathbb{F}_q$. This sequence is eventually periodic with some period $T \leq q$. We assume that the sequence (μ_n) is purely periodic.

2010 Mathematics Subject Classification: 11K45, 11T23, 11K31, 11K38.
Keywords: Finite fields, pseudorandom numbers, discrepancy, exponential sums.
This paper was partly funded by the Austrian Science Fund (FWF) under the grant P-19004 N18.

In [20, 25] a method has been presented to study the exponential sums

$$S_{\mathbf{a},N}(f)=\sum_{n=0}^{N-1}\chi\left(\sum_{j=0}^{s-1}\alpha_j\mu_{n+j}\right),\quad 1\le N\le T,$$

and thus the distribution of such sequences for arbitrary polynomials $f(X)$, where χ is a nontrivial additive character of $\mathbb{F}_q$ and $\mathbf{a}=(\alpha_0,\dots,\alpha_{s-1})\in\mathbb{F}_q^s\setminus\mathbf{0}$, see also the recent surveys [17, 23, 24, 30]. Unfortunately, in general this method leads only to a nontrivial bound if $d=q^{o(1)}$. More precisely, under some necessary restrictions, say $\gcd(d,p)=1$, we can prove:

$$S_{\mathbf{a},N}(f)\ll N\left(\log\frac{2q}{N}\right)^{1/2}(\log d)^{1/2}/(\log q)^{1/2},\quad 1\le N\le T, \tag{2}$$

where $A\ll B$ is equivalent to the assertion that the inequality $|A|\le cB$ holds for some constant $c>0$ depending only on s.

However, in the special case of *inversive generators* this method leads to much stronger bounds [10, 19, 21, 22]. For other special classes of polynomials, namely for *monomials* and *Dickson polynomials*, an alternative approach, producing much stronger bounds has been proposed in [3, 4, 6]. Related results for sequences produced by *Rédei functions* are obtained in [12]. Moreover, we mention that certain multivariate polynomial systems with slow degree growth [26] admit stronger exponential sum bounds than in the general case of higher order nonlinear recurrences [8, 9].

For a nonnegative integer n, we define its *p-weight* as the sum of the coefficients in its p-adic expansion:

$$\sigma_p\left(\sum_{i=0}^{l}n_ip^i\right)=\sum_{i=0}^{l}n_i\quad\text{if}\quad 0\le n_i<p\,.$$

Let $0\le e_1<e_2<\dots<e_l$ be integers and $f(X)=\sum_{i=1}^{l}\gamma_iX^{e_i}\in\mathbb{F}_q[X]$ be a nonzero polynomial over a finite field $\mathbb{F}_q$, with $\gamma_i\ne 0$, $i=1,\dots,l$. We define its *p-weight degree* as

$$w_p(f)=\max\{\sigma_p(e_i)\mid 1\le i\le l\}.$$

Therefore, $w_p(f)\le\deg(f)$. Our first result is the following complement of (2) in the case that

$$f(X)=\alpha X^d+\tilde{f}(X)\in\mathbb{F}_q[X]\quad\text{with}\quad\alpha\ne 0,\quad w_p\left(\tilde{f}\right)<\sigma_p(d),\quad d\ge 2, \tag{3}$$

and

$$\gcd\left(d,\frac{q-1}{p-1}\right)\le\sigma_p(d)^r. \tag{4}$$

Theorem 1. *If the sequence* (μ_n) *given by* (1) *with a polynomial* $f(X) \in \mathbb{F}_q[X]$ *of the form* (3) *satisfying* (4) *is purely periodic with period* T*, then*

$$S_{\mathbf{a},N}(f) \ll N \left(\log \frac{2q}{N}\right)^{1/2} (\log w)^{1/2} / (\log p)^{1/2}, \quad 1 \le N \le T, \quad \mathbf{a} \neq \mathbf{0},$$

where $w = \sigma_p(d) > 1$ *is the* p*-weight degree of* $f(X)$ *and the implied constant depends only on* s.

This result is proved in Section 3 with a weaker condition than (4). Theorem 1 improves (2) for polynomials satisfying (3) and (4) if and only if $w^r < \deg(f)$.

We derive from the sequence (μ_n) defined by (1) a nonlinear method for pseudorandom vector generation defined as follows.
Let $\{\beta_1, \dots, \beta_r\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and identify $\mathbb{F}_p$ with the set of integers $\{0, 1, \dots, p-1\}$. If

$$\mu_n = u_{n,1}\beta_1 + \dots + u_{n,r}\beta_r, \quad \text{with} \quad u_{n,i} \in \mathbb{F}_p,$$

then we derive *digital nonlinear pseudorandom vectors* by

$$\mathbf{z}_n = \frac{1}{p}(u_{n,1}, \dots, u_{n,r}) \in [0,1)^r. \tag{5}$$

In Section 4 we derive from Theorem 1 results on the distribution of sequences of digital nonlinear pseudorandom vectors in terms of a discrepancy bound.

We can also derive from the sequence (μ_n) defined by (1) a nonlinear method for pseudorandom number generation. We derive *digital nonlinear pseudorandom numbers* in the unit interval $[0,1)$ by putting

$$y_n = \sum_{j=1}^{r} u_{n,j} p^{-j}.$$

However, we are not aware of a suitable general discrepancy bound which reduces the discrepancy to the exponential sums studied in this paper which is strong enough to obtain a nontrivial discrepancy bound. For example, the bound of [16, Theorem 3.12], see also [13], is too weak.

We also use the p-weight to bound the *Nth linear complexity* of the sequence defined in (1). For $N \ge 1$ the Nth linear complexity of a sequence is the smallest possible order of a linear feedback shift register (LFSR) that generates the first N sequence elements. More explicitly, for a sequence (μ_n) over $\mathbb{F}_q$, its Nth linear complexity $\mathcal{L}(\mu_n, N)$ over $\mathbb{F}_q$ is the smallest integer L such that there exist $\alpha_0, \dots, \alpha_{L-1} \in \mathbb{F}_q$ such that

$$\mu_{n+L} = \alpha_{L-1}\mu_{n+L-1} + \dots + \alpha_0\mu_n \quad \text{for} \quad 0 \le n < N - L$$

with the conventions that

$$\mathcal{L}(\mu_n, N) = 0 \quad \text{if} \quad \mu_0 = \cdots = \mu_{N-1} = 0 \quad \text{and} \quad \mathcal{L}(\mu_n, N) = N$$
$$\text{if} \quad \mu_0 = \cdots = \mu_{N-2} = 0 \quad \text{but} \quad \mu_{N-1} \neq 0.$$

Its *linear complexity* is $\mathcal{L}(\mu_n) = \sup_{N\geq 1} \mathcal{L}(\mu_n, N)$. Note that for a T-periodic sequence we have $\mathcal{L}(\mu_n) \leq T$. The linear complexity is a measure for the unpredictability and thus suitability in cryptography. For recent surveys on linear complexity and related measures see [18, 32].

For the sequence (μ_n) defined in (1) we know the lower bound

$$\mathcal{L}(\mu_n, N) \geq \frac{\min\{\log(N - \log N/\log d), \log T\}}{\log d}, \qquad N \geq 1$$

of [11, Theorem 4]. Specially tailored results have been proved for the inversive generator [11], power generator [7, 28], Dickson generator [1] and Rédei generator [15]. The linear complexities of nonlinear pseudorandom number generators of higher order and with multivariate polynomial systems have been analyzed in [29] and [27].

In Section 5 we prove the following improvement in a slightly more general form.

Theorem 2. *If the sequence* (μ_n) *given by* (1) *with a polynomial* $f(X) \in \mathbb{F}_q[X]$ *of the form* (3) *satisfying*

$$\gcd\left(d, \frac{q-1}{p-1}\right) \leq \sigma_p(d)^{r/2}, \tag{6}$$

with p-weight degree $w = \sigma_p(d) > 1$ is purely periodic with period T, then for $N \geq 2p^{r-1}\log p/\log w$,

$$\mathcal{L}(\mu_n, N) \geq \frac{\log(\min\{N, T\}/p^{r-1}) - 1}{\log w}.$$

Note that this result is only an improvement of the result of [11] if

$$w_p(f) < \deg(f)^{1/r}.$$

2. Basics

In this section we fix some notation and collect some results on the p-weight degree of a polynomial.

If $g(X) \in \mathbb{F}_q[X]$ and $\{\beta_1, \ldots, \beta_r\}$ is a fixed ordered $\mathbb{F}_p$-basis of $\mathbb{F}_q$, we define

$$G(X_1, \ldots, X_r) = \mathrm{Tr}\big(g(X_1\beta_1 + \ldots + X_r\beta_r)\big),$$

where $\mathrm{Tr}(X) = X + X^p + \ldots + X^{p^{r-1}}$ is the absolute trace function of $\mathbb{F}_q$. Then the *transformed polynomial* $G_R(X_1, \ldots, X_r)$ of $g(X)$ is the unique polynomial with all local degrees smaller than p such that $G_R(x_1, \ldots, x_r) = G(x_1, \ldots, x_r)$ for all $x_1, \ldots, x_r \in \mathbb{F}_p$ or equivalently

$$G_R(X_1, \ldots, X_r) \equiv G(X_1, \ldots, X_r) \mod (X_1^p - X_1, \ldots, X_r^p - X_r).$$

The interest of this construction relies on the fact that, under certain assumptions, the total degree of $G_R(X_1, \ldots, X_r)$ coincides with the p-weight degree of $g(X)$.

We consider the following property of a positive integer $D < q = p^r$:

$$\text{For all } \ t \mid r \ \text{ with } \ t < r \ \text{ we have } \ \frac{q-1}{p^t - 1} \nmid D. \tag{7}$$

Note that (7) is equivalent to $\mathbb{F}_q = \mathbb{F}_p\left(\gamma^D\right)$ for some $\gamma \in \mathbb{F}_q$, see, for example, [31].

In particular,

$$\gcd\left(D, \frac{q-1}{p-1}\right) \le q^{1/2}$$

implies (7). We will use the following result, which is proved in [5] in a slightly weaker form. We add its proof for the convenience of the reader.

Lemma 3. *Let $f(X) \in \mathbb{F}_q[X]$ be of the form* (3) *with $D = d < q$ satisfying* (7)*. Then the degree of the transformed polynomial $F_R(X_1, \ldots, X_r)$ equals $w_p(f)$.*

Proof. First we show that (7) implies the existence of $\xi \in \mathbb{F}_q$ with $\mathrm{Tr}(\alpha\xi^d) \ne 0$. If

$$Tr(\alpha\xi^d) = 0 \quad \text{for all} \qquad \xi \in \mathbb{F}_q,$$

we have

$$\mathrm{Tr}\Big(\alpha\big(j_1\xi_1^d + \ldots + j_r\xi_r^d\big)\Big) = 0 \quad \text{for all} \quad j_1, \ldots, j_r \in \mathbb{F}_p,\ \xi_1, \ldots, \ \xi_r \in \mathbb{F}_q.$$

Since $\mathrm{Tr}(X)$ has exactly q/p zeros and $\alpha \ne 0$, there is no $\mathbb{F}_p$-basis of $\mathbb{F}_q$ consisting of dth powers and thus $\mathbb{F}_p(\xi^d) \ne \mathbb{F}_q$ for all $\xi \in \mathbb{F}_q$ in contradiction to (7).

Next we show that either the total degree of $f(X_1,\dots,X_r)\equiv \mathrm{Tr}(\alpha(X_1\beta_1+\dots$ $\dots+X_r\beta_r)^d) \bmod (X_1^p-1,\dots,X_r^p-1)$ is $\sigma_p(d)$ or $f(X_1,\dots,X_r)$ is identically zero. For $d=d_1+d_2p+\dots+d_rp^{r-1}$ with $0\le d_1,\dots,d_r<p$ we have

$$\begin{aligned}
&f(X_1,\dots,X_r)\\
&\equiv \mathrm{Tr}\left(\alpha(X_1\beta_1+\dots+X_r\beta_r)^{d_1}\cdots\left(X_1\beta_1^{p^{r-1}}+\dots+X_r\beta_r^{p^{r-1}}\right)^{d_r}\right)\\
&\equiv \sum_{\substack{i_{1,j}+\dots+i_{r,j}=d_j\\ j=1,\dots,r}}\left(\prod_{j=1}^{r}\binom{d_j}{i_{1,j},\dots,i_{r,j}}\right)X_1^{i_{1,1}+\dots+i_{1,r}}\cdots X_r^{i_{r,1}+\dots+i_{r,r}}\\
&\quad \mathrm{Tr}\left(\alpha\prod_{j=1}^{r}\beta_j^{i_{j,1}+i_{j,2}p+\dots+i_{j,r}p^{r-1}}\right) \bmod (X_1^p-X_1,\dots,X_r^p-X_r).
\end{aligned}$$

This polynomial is either identical zero or homogeneous of total degree $d_1+\dots$ $\dots+d_r=\sigma_p(d)$. Since $\mathrm{Tr}(\alpha X^d)$ is not identically zero by (7) its degree is $\sigma_p(d)=w_p(f)$. □

Note that condition (7) is the weakest possible restriction which depends only on d and not on α. If (7) is not satisfied, all dth powers fall into a proper subfield $\mathbb{F}_{p^s}$ of $\mathbb{F}_q$. If the relative trace from $\mathbb{F}_q$ to $\mathbb{F}_{p^s}$ of α is zero, then $\mathrm{Tr}(\alpha X^d)$ is identically zero.

We also need a result derived from the multivariate Weil bound on exponential sums.

Lemma 4. *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and $f(X)\in\mathbb{F}_q[X]$ be of the form* (3) *satisfying* (7) *for $D=d<q$. Then,*

$$\left|\sum_{\xi\in\mathbb{F}_q}\chi\big(f(\xi)\big)\right|\le\big(w_p(f)-1\big)p^{r-1/2}.$$

P r o o f. By (7) the transformed polynomial $F_R(X_1,\dots,X_r)$ of $f(X)$ is not constant and has degree $w_p(f)$. Hence, we get for some nontrivial additive character χ_1 of $\mathbb{F}_p$

$$\left|\sum_{\xi\in\mathbb{F}_q}\chi\big(f(\xi)\big)\right|=\left|\sum_{x_1,\dots,x_r\in\mathbb{F}_p}\chi_1\big(F_R(x_1,\dots,x_r)\big)\right|\le\big(w_p(f)-1\big)p^{r-1/2}$$

by the multivariate Weil-bound. □

It is easy to check that, as the usual degree function, the p-weight degree satisfies

$$w_p(f+g) \le \max\{w_p(f), w_p(g)\}. \tag{8}$$

For the product and composition, however, we only have:

Lemma 5. *For $f, g \in \mathbb{F}_q[X]$ we have*

$$w_p(fg \bmod X^q - X) \le w_p(fg) \le w_p(f) + w_p(g)$$

and

$$w_p(f \circ g \bmod X^q - X) \le w_p(f \circ g) \le w_p(f)\, w_p(g).$$

Proof. Note that $w_p(f \bmod X^q - X) \le w_p(f)$.

The first statement derives from $\sigma_p(n+m) \le \sigma_p(n) + \sigma_p(m)$.

For the second one we may assume $f(X) = X^d$ by (8) with $d = d_0 + d_1 p + \ldots + d_l p^l$, $0 \le d_0, \ldots, d_l < p$. Then we have

$$f \circ g = \prod_{j=0}^{l} \left(g^{p^j}\right)^{d_j}$$

and

$$w_p(f \circ g) \le \sum_{j=0}^{l} d_j w_p\left(g^{p^j}\right) = \sum_{j=0}^{l} d_j w_p(g) = w_p(f)\, w_p(g)$$

which completes the proof. □

For a given polynomial $f(X) \in \mathbb{F}_q[X]$ we define the sequence of polynomials $f_k(X) \in \mathbb{F}_q[X]$ by

$$f_0(X) = X, \quad f_k(X) \equiv f(f_{k-1}(X)) \bmod X^q - X, \quad k = 1, 2, \ldots,$$

where $\deg(f_k) < q$.

Lemma 6. *Let $f(X) \in \mathbb{F}_q[X]$ be of the form (3). If $\sigma_p(d)^k < p$, then we have*

$$f_k(X) = \alpha^{(d^k-1)/(d-1)} X^{d^k \bmod (q-1)} + \widetilde{f}_k(X)$$

with

$$w_p\left(\widetilde{f}_k\right) < w_p(f_k) = \sigma_p(d)^k \quad \text{and} \quad \deg\left(\widetilde{f}_k\right) < q,$$

where $d^k \bmod (q-1)$ denotes the unique integer $0 \le z < q-1$ such that $q-1$ divides $d^k - z$.

Proof. Let $d = d_0 + d_1 p + \ldots + d_l p^l$ with $0 \le d_i < p$. The inequality

$$\sum_{v_1+\ldots+v_l=k} \binom{k}{v_1, \ldots, v_l} d_0^{v_1} \cdots d_l^{v_l} = \sigma_p(d)^k < p$$

implies $\sigma_p\left(d^k\right) = \sigma_p\left(d\right)^k$. The result is trivial for $k = 0$ and by induction we see

$$f_k(X) \equiv \alpha\left(\alpha^{(d^{k-1}-1)/(d-1)}X^{d^{k-1}} + \widetilde{f}_{k-1}(X)\right)^d + \widetilde{f}(f_{k-1}(X)) \bmod X^q - X.$$

By Lemma 5 we have $w_p\left(\widetilde{f} \circ f_{k-1}\right) < \sigma_p\left(d\right)\sigma_p\left(d^{k-1}\right) = \sigma_p\left(d\right)^k$. The first summand is of the form

$$\alpha^{(d^k-1)/(d-1)}X^{d^k} + \sum_{j=1}^{d}\binom{d}{j}\left(AX^{d^{k-1}}\right)^{d-j}\widetilde{f}_{k-1}(X)^j.$$

If $j = j_0 + j_1 p + \ldots + j_l p^l$ with $0 \le j_i < p$, by Lucas congruence

$$\binom{d}{j} \equiv \binom{d_0}{j_0}\cdots\binom{d_l}{j_l} \bmod p\,,$$

we have $\binom{d}{j} \equiv 0 \bmod p$ if $j_i > d_i$ for some $0 \le i \le l$. In the remaining cases we have $\sigma_p\left(d-j\right) = d_0 - j_0 + \ldots + d_l - j_l$ and thus

$$w_p\left(\left(AX^{d^{k-1}}\right)^{d-j}\widetilde{f}_{k-1}(X)^j\right) \le \sigma_p\left(d-j\right)\sigma_p\left(d^{k-1}\right) + w_p\left(\widetilde{f}_{k-1}\right)\sigma_p\left(j\right) < \sigma_p\left(d\right)^k$$

by Lemma 5 again. □

3. Exponential sums

In this section we prove Theorem 1. Indeed, condition (4) can be substituted by (7) on a certain power of the degree.

Theorem 7. *Let $K_0 \ge s-1$ be the largest integer such that $D = d^{K_0}$ satisfies (7). If the sequence (μ_n) given by (1) with a polynomial $f(X) \in \mathbb{F}_q[X]$ of the form (3) is purely periodic with period (T), then for any $\mathbf{a} \in \mathbb{F}_q^s\backslash\{0\}$ and $1 \le N \le T$,*

$$S_{\mathbf{a},N}(f) \ll N\left(\log\frac{2q}{N}\right)^{1/2}\max\left\{(\log w)^{1/2}/(\log p)^{1/2}, 1/K_0^{1/2}\right\},$$

where $w = \sigma_p\left(d\right) > 1$ is the p-weight degree of $f(X)$ and the implied constant depends only on s.

Proof. We proceed as in [25]. We have, for every $k \ge 0$

$$\left|S_{\mathbf{a},N}(f) - \sum_{n=0}^{N-1}\chi\left(\sum_{j=0}^{s-1}\alpha_j\mu_{n+k+j}\right)\right| \le 2k.$$

Therefore, setting

$$W = \left| \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} \chi \left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+k+j} \right) \right|,$$

we have $K|S| \le W + K^2$. Now, using the Hölder inequality and the notation

$$F_{k_1,\dots,k_{2\nu}} = \sum_{j=0}^{s-1} \alpha_j \left(f_{k_1+j} + \dots + f_{k_\nu+j} - f_{k_{\nu+1}+j} - \dots - f_{k_{2\nu}+j} \right),$$

we get

$$\begin{aligned} W^{2\nu} &\le N^{2\nu-1} \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi \left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+k+j} \right) \right|^{2\nu} \\ &\le N^{2\nu-1} \sum_{x \in \mathbb{F}_q} \left| \sum_{k=0}^{K-1} \chi \left(\sum_{j=0}^{s-1} \alpha_j f_{k+j}(x) \right) \right|^{2\nu} \\ &= N^{2\nu-1} \sum_{k_1,\dots,k_{2\nu}=0}^{K-1} \sum_{x \in \mathbb{F}_q} \chi\big(F_{k_1,\dots,k_{2\nu}}(x)\big). \end{aligned} \tag{9}$$

If the multisets (sets where elements are counted with multiplicity)

$$\{k_1, \dots, k_\nu\} \quad \text{and} \quad \{k_{\nu+1}, \dots, k_{2\nu}\}$$

coincide, the sum over $\mathbb{F}_q$ in (9) equals q. This happens in at most $\nu! K^\nu \le (\nu K)^\nu$ choices of indices $k_1, \dots, k_{2\nu}$. For the remaining at most $K^{2\nu}$ choices of $\{k_1, \dots, k_{2\nu}\}$ by Lemma 6 every polynomial $f_{k+j}(X)$ is of the form (3) with degree

$$d^{k+j} \bmod q-1 \quad \text{and} \quad w_p\left(f_{k+j}\right) = w^{k+j}.$$

Moreover, as $w^{K+s-2} < p$ if p is sufficiently large, $F_{k_1+j,\dots,k_{2\nu}+j}$ is of the form (3) and its degree satisfies (7) as well. Using Lemma 4, the character sum of (9) is bounded by $w^{K+s-2}p^{r-1/2}$ and we get

$$W^{2\nu} \le \nu^\nu K^\nu q N^{2\nu-1} + K^{2\nu} N^{2\nu-1} w^{K+s-2} p^{r-1/2}.$$

Choosing

$$K = \min\left\{ \left\lceil 0.4 \frac{\log p}{\log w} \right\rceil, \left\lfloor \nu p^{1/(11\nu)} \right\rfloor, K_0 - s - 2 \right\},$$

the first term dominates the second and we get

$$S_{\mathbf{a},N}(f) \ll \nu^{1/2} K^{-1/2} N (q/N)^{1/2\nu}.$$

With

$$\nu = \left\lfloor \log \frac{q}{N} \right\rfloor + 1$$

we get $(q/N)^{1/2\nu} = O(1)$ and $\nu p^{1/(11\nu)} \gg \log p$ and the result follows. □

For the choice

$$K_0 = \lceil 0.4 \log p / \log w \rceil + s - 2$$

note that (4) implies for sufficiently large p,

$$\gcd\left(d, \frac{q-1}{p-1}\right)^{K_0} \leq \gcd\left(d, \frac{q-1}{p-1}\right)^{0.5 \log p/\log w} \leq q^{1/2}$$

and $D = d^{K_0}$ satisfies (7).

4. Discrepancy bound

We measure the distribution or statistical independence properties of pseudorandom vectors in terms of the discrepancy. Given a sequence $(\mathbf{z}_n)$ of digital nonlinear pseudorandom vectors defined by (5) and an integer $s \geq 1$, we consider the rs-dimensional points

$$\mathbf{v}_n = (\mathbf{z}_n, \mathbf{z}_{n+1}, \dots, \mathbf{z}_{n+s-1}) \in [0,1)^{rs}, \quad n = 0, 1, \dots \tag{10}$$

Then for any N with $1 \leq N \leq T$ we define the *discrepancy*

$$D_{rs}(N) = \sup_{B \subseteq [0,1)^{rs}} \left| \frac{N(B)}{N} - V(B) \right|,$$

where $N(B)$ denotes the number of points $\mathbf{v}_n$ with $0 \leq n \leq N-1$ which hit the box

$$B = [a_1, b_1) \times \cdots \times [a_{rs}, b_{rs}) \subseteq [0,1)^{rs},$$

taking the supremum over all such boxes, and $V(B)$ is the volume of B.

Theorem 8. *Let the sequence (μ_n) given by (1) with a polynomial $f(X) \in \mathbb{F}_q[X]$ of the form (3) satisfying (4) of weighted degree $w = \sigma_p(d) > 1$ be purely periodic with period T.*
For any sequence of rs-dimensional digital nonlinear vectors $\mathbf{v}_n$ defined by (10) and (5), for any $s \geq 1$, and for any $1 \leq N \leq T$ the discrepancy $D_{rs}(N)$ satisfies

$$D_{rs}(N) \ll \left(\frac{3}{2}\right)^{rs} \left(\log \frac{2q}{N}\right)^{1/2} (\log w)^{1/2} (\log\log p)^{rs} / (\log p)^{1/2},$$

where the implied constant depends only on s.

Proof. Using the Erdős-Turán-Koksma inequality, see [2, Theorem 1.21], we get for $1 < H < p$,

$$D_{rs}(N) \ll \left(\frac{3}{2}\right)^{rs} \left(\frac{1}{H} + (\log H)^{rs} \max_{\mathbf{a}\neq\mathbf{0}} \left|S_N(\mathbf{a})\right|\right),$$

where

$$S_N(\mathbf{a}) = \sum_{n=0}^{N-1} \exp(2\pi i \mathbf{a} \cdot \mathbf{v_n})$$

and the dot denotes the standard inner product. For fixed $\mathbf{a} \neq \mathbf{0}$ we write $\mathbf{a} = (\mathbf{a}_0, \ldots, \mathbf{a}_{s-1})$ with $\mathbf{a}_i \in \mathbb{F}_q$ for $0 \leq i \leq s-1$, where not all $\mathbf{a}_i$ are $\mathbf{0}$. Then we have

$$S_N(\mathbf{a}) = \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i}{p} \sum_{i=0}^{s-1} \sum_{j=1}^{r} a_{ij} u_{n+i,j}\right),$$

where $\mathbf{a}_i = (a_{i1}, \ldots, a_{ir})$ for $0 \leq i \leq s-1$ and $a_{ij} \in \mathbb{F}_p$.
Let $\{\delta_1, \ldots, \delta_r\}$ be the dual basis of the given ordered basis $\{\beta_1, \ldots, \beta_r\}$. Then we have (see [14, p. 55]),

$$u_{n,j} = \mathrm{Tr}(\delta_j \mu_n), \quad 1 \leq j \leq r, \; n = 0, 1, \ldots$$

Therefore,

$$\begin{aligned} S_N(\mathbf{a}) &= \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i}{p} \sum_{i=0}^{s-1} \sum_{j=1}^{r} a_{ij} \mathrm{Tr}(\delta_j \mu_{n+i})\right) \\ & \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i}{p} \mathrm{Tr}\left(\sum_{i=0}^{s-1} \sum_{j=1}^{r} a_{ij} \delta_j \mu_{n+i}\right)\right) \\ &= \sum_{n=0}^{N-1} \chi\left(\sum_{i=0}^{s-1} \alpha_i \mu_{n+i}\right), \end{aligned}$$

where χ is the additive canonical character of $\mathbb{F}_q$ and $\alpha_i = \sum_{j=1}^{r} a_{ij} \delta_j$. Since not all $\mathbf{a}_i$ are zero and $\{\delta_1, \ldots, \delta_r\}$ is a basis, it follows that not all α_i are 0. Hence we may apply Theorem 1. Choosing

$$H = \left\lceil \left(\frac{\log p}{\log(2q/N)}\right)^{1/2} \right\rceil$$

we get the result. □

5. Linear complexity

In this section we use the transformed polynomial considered in Section 2 to prove a general bound for the linear complexity of (1).

Theorem 9. *Let $L_0 \geq 1$ be the largest integer such that $D = d^{L_0-1}$ satisfies* (7)*. If the sequence (μ_n) given by* (1) *with a polynomial $f(X) \in \mathbb{F}_q[X]$ of the form* (3) *and with p-weight degree $w = \sigma_p(d) > 1$, is purely periodic with period T, then for $N \geq 2p^{r-1}\log p/\log w$,*

$$\mathcal{L}(\mu_n, N) \geq \min\left\{\frac{\log\left(\min\{N,T\}/p^{r-1}\right) - 1}{\log w}, L_0\right\}.$$

P r o o f. Put $L = \mathcal{L}(\mu_n, N)$. Since otherwise the result is trivial, we may assume $L < L_0$ and

$$L < \frac{\log p}{\log w}.$$

Then we have $w^L < p$ and $\sigma_p(d^l) = w^l$ for $l = 0, \dots, L$ and thus $w_p(f_l) = w^l$, by Lemma 6. Let

$$\sum_{l=0}^{L} \alpha_l \mu_{n+l} = 0 \quad \text{for} \quad 0 \leq n < N - L,$$

be the shortest recurrence relation for the first N sequence elements of (μ_n) with $\alpha_0, \dots, \alpha_{L-1} \in \mathbb{F}_q$ and $\alpha_L = -1$. Then, the polynomial $F(X) = \sum_{l=0}^{L} \alpha_l f_l(X)$ is of the form (3) by Lemma 6 and has at least $\min\{T, N - L\}$ distinct roots over $\mathbb{F}_q$. On the other hand, by Lemma 3, $F_R(X_1, \dots, X_r)$ has degree w^L and at least $\min\{T, N - L\}$ distinct roots. Therefore, $p^{r-1}w^L \geq \min\{T, N - L\}$ and the result follows. □

Note that for $L_0 = \lceil \log p/\log w \rceil$ condition (6) implies

$$\gcd\left(d, \frac{q-1}{p-1}\right)^{L_0-1} \leq q^{1/2}$$

and $D = d^{L_0-1}$ satisfies (7).

Acknowledgement. The authors wish to thank Igor Shparlinski for pointing to this way to improve the exponential sum bound and useful discussions. They also wish to thank the anonymous referee for several valuable suggestions.

REFERENCES

[1] ALY, H. – WINTERHOF, A.: *On the linear complexity profile of nonlinear congruential pseudorandom number generators with Dickson polynomials*, Des. Codes Cryptogr. **39** 2006, no. 2, 155–162.

[2] DRMOTA, M. – TICHY, R. F.: *Sequences, discrepancies and applications*, in: Lecture Notes in Math., Vol. **1651**, Springer-Verlag, Berlin, 1997.

[3] FRIEDLANDER, J. B. – HANSEN, J. – SHPARLINSKI, I. E.: *Character sums with exponential functions*, Mathematika **47** (2000), no. 1–2, 75–85.

[4] FRIEDLANDER, J. B. – SHPARLINSKI, I. E.: *On the distribution of the power generator*, Math. Comp. **70** (2001), no. 236, 1575–1589 (electronic).

[5] GILLOT, V.: *Bounds for exponential sums over finite fields*, Finite Fields Appl. **1** (1995), no. 4, 421–436.

[6] GOMEZ-PEREZ, D. – GUTIERREZ, J. – SHPARLINSKI, I. E. : *Exponential sums with Dickson polynomials*, Finite Fields Appl. **12** (2006), no. 1, 16–25.

[7] GRIFFIN, F. – SHPARLINSKI, I. E.: *On the linear complexity profile of the power generator*, IEEE Trans. Inform. Theory, **46** 2000, no. 6, 2159–2162.

[8] GRIFFIN, F. – NIEDERREITER, H. – SHPARLINSKI, I. E.: *On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Honolulu, HI, 1999)*, Lecture Notes in Comput. Sci., Vol. **1719**, Springer, Berlin, 1999, pp. 87–93.

[9] GUTIERREZ, J. – GOMEZ-PEREZ, D.: *Iterations of multivariate polynomials and discrepancy of pseudorandom numbers*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001)*, Lecture Notes in Comput. Sci., Vol. **2227**, Springer, Berlin, 2001, pp. 192–199.

[10] GUTIERREZ, J. – NIEDERREITER, H. – SHPARLINSKI, I. E.: *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math. **129** (2000), no. 1, 31–36.

[11] GUTIERREZ, J. – SHPARLINSKI, I. E. – WINTERHOF, A.: *On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators*, IEEE Trans. Inform. Theory, **49** (2003), no. 1, 60–64.

[12] GUTIERREZ, J. – WINTERHOF, A.: *Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions*, Finite Fields Appl. **14** (2008), no. 2, 410–416.

[13] HELLEKALEK, P.: *General discrepancy estimates: the Walsh function system*, Acta Arith. **67** (1994), no. 3, 209–218.

[14] LIDL, R. – NIEDERREITER, H.: *Introduction to Finite Fields and Their Applications*. Revision of the 1986 first edition. Cambridge University Press, Cambridge, 1994.

[15] MEIDL, W. – WINTERHOF, A.: *On the linear complexity profile of nonlinear congruential pseudorandom number generators with Rédei functions*, Finite Fields Appl. **13** (2007), no. 3, 628–634.

[16] NIEDERREITER, H.: *Random Number Generation and Quasi-Monte Carlo Methods*, in: *CBMS-NSF Regional Conference Series in Applied Mathematics*, Vol. **63**, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992.

[17] NIEDERREITER, H.: *Design and analysis of nonlinear pseudorandom number generators*, in: *Monte Carlo Simulation*, A. A. Balkema Publishers, Rotterdam, 2001, pp. 3–9.

[18] NIEDERREITER, H.: *Linear complexity and related complexity measures for sequences*, in: *Progress in Cryptology–INDOCRYPT 2003*, Lecture Notes in Comput. Sci., Vol. **2904**, Springer, Berlin, 2003, pp. 1–17.

[19] NIEDERREITER, H. – RIVAT, J.: *On the correlation of pseudorandom numbers generated by inversive methods*, Monatsh. Math. **153** (2008), no. 3, 251–264.

[20] NIEDERREITER, H. – SHPARLINSKI, I. E.: *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. **5** (1999), no. 3, 246–253.

[21] NIEDERREITER, H. – SHPARLINSKI, I. E.: *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 3, 189–202.

[22] NIEDERREITER, H. – SHPARLINSKI, I. E.: *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp. **70** (2001), no. 236, 1569–1574 (electronic).

[23] NIEDERREITER, H. – SHPARLINSKI, I. E.: *Recent advances in the theory of nonlinear pseudorandom number generators*, in: *Monte Carlo and Quasi-Monte Carlo Methods, 2000 (Hong Kong)*, Springer, Berlin, 2002, pp. 86–102.

[24] NIEDERREITER, H. – SHPARLINSKI, I. E.: *Dynamical systems generated by rational functions*, in: *Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Toulouse, 2003)*, Lecture Notes in Comput. Sci. Vol. 2643, Springer, Berlin, 2003, pp. 6–17.

[25] NIEDERREITER, H. – WINTERHOF, A.: *Exponential sums for nonlinear recurring sequences*, Finite Fields Appl. 14 (2008), no. 1, 59–64.

[26] OSTAFE, A. – SHPARLINSKI, I. E.: *On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators*, Math. Comp. **79** (2010), no. 269, 501–511.

[27] OSTAFE, A. – SHPARLINSKI, I. E. – WINTERHOF, A.: *On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences*, Adv. Math. Commun. (to appear).

[28] SHPARLINSKI, I. E.: *On the linear complexity of the power generator*, Des. Codes Cryptogr. **23** (2001), no. 1, 5–10.

[29] TOPUZOĞLU, A. – WINTERHOF, A.: *On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders*, Appl. Algebra Engrg. Comm. Comput. **16** (2005), no. 4, 219–228.

[30] TOPUZOĞLU, A. – WINTERHOF, A.: *Pseudorandom sequences*, in: *Topics in Geometry, Coding Theory and Cryptography*, Algebr. Appl. Vol. **6**, Springer, Dordrecht, 2007, pp. 135–166.

[31] WINTERHOF, A.: *On Waring's problem in finite fields*, Acta Arith. **87** (1998), no. 2, 171–177.

[32] WINTERHOF, A.: *Linear complexity and related complexity measures*, in: *Selected Topics in Information and Coding Theory*, World Scientific, 2010, pp. 3–40.

Received December 17, 2009
Accepted March 10, 2010

Álvar Ibeas
University of Cantabria
E-39071 Santander,
SPAIN
E-mail: alvar.ibeas@unican.es

Arne Winterhof
Johann Radon Institute for
Computational and Appl. Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
AT-4040 Linz
AUSTRIA
E-mail: arne.winterhof@oeaw.ac.at