MATHEMATICS OF COMPUTATION
Volume 79, Number 269, January 2010, Pages 501–511
S 0025-5718(09)02271-6
Article electronically published on July 7, 2009

ON THE DEGREE GROWTH IN SOME POLYNOMIAL DYNAMICAL SYSTEMS AND NONLINEAR PSEUDORANDOM NUMBER GENERATORS

ALINA OSTAFE AND IGOR E. SHPARLINSKI

Abstract. In this paper we study a class of dynamical systems generated by iterations of multivariate polynomials and estimate the degree growth of these iterations. We use these estimates to bound exponential sums along the orbits of these dynamical systems and show that they admit much stronger estimates than in the general case and thus can be of use for pseudorandom number generation.

1. Introduction

Given a system of r polynomials $\mathcal{F} = \{f_0, \ldots, f_{r-1}\}$ in r variables over a ring $\mathcal{R}$, one can naturally define a dynamical system generated by its iterations:

$$f_i^{(0)} = f_i, \qquad f_i^{(k)} = f_i^{(k-1)}(f_0, \ldots, f_{r-1}), \qquad k = 0, 1, \ldots ,$$

for each $i = 0, \ldots, r-1$; see [1, 2, 3, 7, 9, 10, 14, 15, 26, 33, 42, 43, 44] and references therein for various aspects of such dynamical systems. It is also natural to consider the orbits obtained by such iterations evaluated at a certain initial value $(u_{k,0}, \ldots, u_{k,r-1})$.

In the special case of one linear univariate polynomial over a residue ring or a finite field, such iterations, known as linear congruential generators, have been successully used for decades in the theory of quasi-Monte Carlo methods; see [35, 36].

Unfortunately, in cryptographic settings, such linear generators have been successfully attacked [11, 19, 27, 29, 31] and thus deemed unusable for cryptograpic purposes. It should be noted that nonlinear generators have also been attacked [4, 5, 21, 24], but the attacks are much weaker and do not rule out their use for cryptographic purposes (provided reasonable precautions are made). Although linear congruential generators have been used quite sucessfully for quasi-Monte Carlo methods, their linear structure shows in these applications too and often limits their applicability; see [35, 36].

Motivated by these potential applications, the statistical uniformity of the distribution (measured by the discrepancy) of one and multidimensional nonlinear polynomial generators have been studied in [20, 22, 37, 40, 41, 45]. However, all previously known results are nontrivial only for those polynomial generators that produce sequences of extremely large period, which could be hard to achieve in

Received by the editor February 23, 2009 and, in revised form, March 9, 2009.
2000 *Mathematics Subject Classification.* Primary 11K45, 11T23, 37A45, 37F10.

practice. The reason behind this is that typically the degree of iterated polynomial systems grows exponentially, and that in all previous results, the saving over the trivial bound has been logarithmic. Furthermore, it is easy to see that in the one-dimensional case (that is, for $r = 1$) the exponential growth of the degree of iterations of a nonlinear polynomial is unavoidable. One also expects the same behaviour in the mulitidimensional case for "random" polynomials $f_0, \ldots, f_{r-1}$. However, for some specially selected polynomials $f_0, \ldots, f_{r-1}$, the degree may grow significantly slower.

Indeed, here we describe a rather wide class of polynomial systems with polynomial growth of the degree of their iterations. As a result we obtain much better estimates of exponential sums, and thus of discrepancy, for vectors generated by these iterations, with a saving over the trivial bound being a power of p. Our construction resembles that of *triangular maps* of [33] but behaves quite differently; for example, triangular maps in [33] have the fastest possible degree growth.

We remark that, in the case of the so-called *inversive generator*, rather strong estimates are also available [38, 39], but this generator involves a modular inversion at each step, which is a computationally expensive operation. Another alternative where stronger than general bounds are known is the power generator, which essentially consists of iterating a monomial map $X \to X^e$; see [8, 16, 17, 18, 34, 46] and especially the recent result of J. Bourgain [6] on the joint distribution of consecutive terms of this generator. Similar results also hold for pseudorandom number generators obtained by iterating *Dickson polynomials* [23] and *Redei functions* [25].

Finally, we note that we also hope that our results may be of use for some applications in polynomial dynamical systems.

2. Polynomial dynamical system with slow degree growth

2.1. **Construction.** Let $\mathbb{F}$ be an arbitrary field and let $\mathcal{F} = \{f_0, \ldots, f_m\}$ be a system of $m+1$ polynomials in $\mathbb{F}[X_0, \ldots, X_m]$ defined in the following way:

$$\begin{aligned} f_0(X_0, \ldots, X_m) &= X_0 g_0(X_1, \ldots, X_m) + h_0(X_1, \ldots, X_m), \\ f_1(X_0, \ldots, X_m) &= X_1 g_1(X_2, \ldots, X_m) + h_1(X_2, \ldots, X_m), \\ &\ldots \\ f_{m-1}(X_0, \ldots, X_m) &= X_{m-1} g_{m-1}(X_m) + h_{m-1}(X_m), \\ f_m(X_0, \ldots, X_m) &= aX_m + b, \end{aligned} \tag{1}$$

where

$$a, b \in \mathbb{F}, \quad a \neq 0, \quad g_i, h_i \in \mathbb{F}[X_{i+1}, \ldots, X_m], \quad i = 0, \ldots, m-1.$$

We also impose the condition that each polynomial g_i has a *unique leading monomial* $X_{i+1}^{s_{i,i+1}} \ldots X_m^{s_{i,m}}$, that is,

$$g_i(X_{i+1}, \ldots, X_m) = X_{i+1}^{s_{i,i+1}} \ldots X_m^{s_{i,m}} + \widetilde{g}_i(X_{i+1}, \ldots, X_m), \tag{2}$$

where

$$\deg \widetilde{g}_i < \deg g_i = s_{i,i+1} + \cdots + s_{i,m} \tag{3}$$

and

$$\deg h_i \le \deg g_i \tag{4}$$

for $i = 0, \ldots, m-1$.

For each $i = 0, \dots, m$ we define the k-th iteration of the polynomials f_i by the recurrence relation

$$f_i^{(0)} = f_i, \qquad f_i^{(k)} = f_i^{(k-1)}(f_0, \dots, f_m), \qquad k = 0, 1, \dots . \tag{5}$$

2.2. **Degree growth.** We denote by $d_{k,i}$ the degree of the polynomial $f_i^{(k)}$, $i = 0, \dots, m$. We also consider the vector of degrees of the iterations

$$\mathbf{d}_k = (d_{k,0} \dots, d_{k,m}),$$

and the upper triangular matrix

$$S = \begin{pmatrix} 1 & s_{0,1} & s_{0,2} & \dots & s_{0,m} \\ 0 & 1 & s_{1,2} & \dots & s_{1,m} \\ & & \dots & & \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

given by the exponents of the leading monomials in f_i, $i = 0, \dots, m$. We observe that under iterations we have

$$\begin{aligned} f_i^{(k)} &= f_i^{(k-1)} g_i(f_{i+1}^{(k-1)}, \dots, f_m^{(k-1)}) + h_i(f_{i+1}^{(k-1)}, \dots, f_m^{(k-1)}), \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad i = 0, \dots, m-1, \\ f_m^{(k)} &= a f_m^{(k-1)} + b, \end{aligned}$$

and using the conditions on the degrees of the polynomials g_i and h_i we get

$$\begin{aligned} d_{k,i} &= d_{k-1,i} + s_{i,i+1} d_{k-1,i+1} + \dots + s_{i,m} d_{k-1,m}, \qquad i = 0, \dots, m-1, \\ d_{k,m} &= 1. \end{aligned}$$

Using the above notation, the degrees of the iterations satisfy the relation

$$\mathbf{d}_k = S \mathbf{d}_{k-1}, \qquad k \geq 0 \qquad \text{and} \qquad \mathbf{d}_{-1} = (1, \dots, 1)^t,$$

which is equivalent to writing

$$\mathbf{d}_k = S^{k+1} (1, \dots, 1)^t, \qquad k \geq 0. \tag{6}$$

We now show that the degrees of the iterations of $\mathcal{F}$ grow polynomially.

Lemma 1. *Let $f_0, \dots, f_m \in \mathbb{F}[X_0, \dots, X_m]$ be as in (1), satisfying the conditions (2), (3) and (4). Then the degrees of the iterations of $\mathcal{F} = \{f_0, \dots, f_m\}$ grow as follows:*

$$\begin{aligned} d_{k,i} &= \frac{1}{(m-i)!} k^{m-i} s_{i,i+1} \dots s_{m-1,m} + \psi_i(k), \qquad i = 0, \dots, m-1, \\ d_{k,m} &= 1, \end{aligned}$$

where $\psi_i(T) \in \mathbb{Q}[T]$ is a polynomial of degree $\deg \psi_i < m - i$.

Proof. We use induction on m. For $m = 1$ one can easily see that we get

$$d_{k,0} = k s_{0,1} + s_{0,1} + 1 \qquad \text{and} \qquad d_{k,1} = 1.$$

We assume the result is true for m indeterminates. Let S be the matrix of exponents of the leading monomials in $\mathcal{F}$ as above. We write S in the following way:

$$S = \begin{pmatrix} R & \mathbf{s} \\ 0 & 1 \end{pmatrix},$$

where R is the matrix given by the exponents of the first m indeterminates in the leading monomials of f_i, $i = 0, \dots, m-1$, and $\mathbf{s} = (s_{0,m}, \dots, s_{m-1,m})$. For a vector

$\mathbf{v} \in \mathbb{F}^m$ we use $\mathbf{v}^t$ and $\mathbf{v}_i$ to denote the transpose and the ith component of $\mathbf{v}$, respectively. We also denote by $\mathbf{e}$ the unit vector $\mathbf{e} = (1, \ldots, 1) \in \mathbb{F}^m$. Using this notation and recalling (6), we obtain

$$\mathbf{d}_k = S^{k+1}\mathbf{e}^t = \begin{pmatrix} R^{k+1} & (R^k + \cdots + R + I)\mathbf{s}^t \\ 0 & 1 \end{pmatrix} \mathbf{e}^t.$$

Componentwise, we have

$$\begin{aligned} d_{k,i} &= \left(R^{k+1}\mathbf{e}^t\right)_i + \left((R^k + \cdots + R + I)\mathbf{s}^t\right)_i, \qquad i = 0, \ldots, m-1, \\ d_{k,m} &= 1. \end{aligned}$$

It is easy to note that the maximal degree of the kth iteration of polynomials f_i for any i is given by the last position in each row of S^{k+1}. Using this remark and the induction hypothesis we get

$$(R^j\mathbf{s}^t)_i = \frac{1}{(m-1-i)!} j^{m-1-i} s_{i,i+1} \ldots s_{m-2,m-1} s_{m-1,m} + \varphi_i(j),$$

for some polynomials $\varphi_i(Z) \in \mathbb{Q}[Z]$ of degree $\deg \varphi_i < m - 1 - i$. Then

$$\sum_{j=0}^{k} (R^j\mathbf{s}^t)_i = \frac{1}{(m-1-i)!} s_{i,i+1} \ldots s_{m-1,m} \sum_{j=0}^{k} j^{m-1-i} + \widetilde{\varphi}_i(k),$$

for some polynomials $\widetilde{\varphi}_i(Z) \in \mathbb{Q}[Z]$ of degree $\deg \widetilde{\varphi}_i < m - i$. As

$$\sum_{j=0}^{k} j^{m-1-i} = \frac{1}{m-i}(B_{m-i}(k+1) - B_{m-i}(0)),$$

where B_{m-i} is the Bernoulli polynomial of degree $m - i$ (which has the leading coefficient equal to 1), we finally obtain the desired result. □

Corollary 2. *Let $f_0, \ldots, f_m \in \mathbb{F}[X_0, \ldots, X_m]$ be as in (1), satisfying the conditions (2), (3) and (4). If $s_{0,1} \ldots s_{m-1,m} \neq 0$, then for any integer $\nu \geq 1$ there is a constant k_0 depending only on the matrix S and ν such that for any integers $k_1, \ell_1, \ldots, k_\nu, \ell_\nu \geq k_0$ and any nonzero $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}^m$,*

$$F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu} = \sum_{i=0}^{m-1} a_i \sum_{j=1}^{\nu} \left(f_i^{(k_j)} - f_i^{(\ell_j)}\right)$$

is a nonconstant polynomial of degree

$$\deg F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu} = O(k^m),$$

where

$$k = \max\{k_1, \ell_1, \ldots, k_\nu, \ell_\nu\}$$

unless the components of the vectors

$$(k_1, \ldots, k_\nu) \qquad \text{and} \qquad (\ell_1, \ldots, \ell_\nu)$$

are permutations of each other.

Proof. Let i_0 be the smallest integer with $a_{i_0} \neq 0$. Performing all trivial cancellations, without loss of generality we can also assume that the vectors $(k_1, \ldots, k_\nu)$ and $(\ell_1, \ldots, \ell_\nu)$ have no common elements. Thus the largest element amongst them, k, is unique. It is now clear from Lemma 1 that the leading term of $f_{i_0}^{(k)}$ is present in $F_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu}$. □

3. Polynomial pseudorandom number generators

3.1. **Construction.** Let $\mathcal{F} = \{f_0, \dots, f_m\}$ be a list of $m+1$ polynomials in $\mathbb{F}_p[X_0, \dots, X_m]$ defined as in section 2. We consider the sequence defined by a recurrence congruence modulo a prime p of the form

$$u_{n+1,i} \equiv f_i(u_{n,0}, \dots, u_{n,m}) \pmod{p}, \qquad n = 0, 1, \dots, \tag{7}$$

with some *initial values* $u_{0,0}, \dots, u_{0,m}$. We also assume that $0 \le u_{n,i} < p$, $i = 0, \dots, m$, $n = 0, 1, \dots$. Using the following vector notation:

$$\mathbf{w}_n = (u_{n,0}, \dots, u_{n,m})$$

and

$$\mathcal{F} = (f_0(X_0, \dots, X_m), \dots, f_m(X_0, \dots, X_m)),$$

we have the recurrence relation

$$\mathbf{w}_{n+1} = \mathcal{F}(\mathbf{w}_n).$$

In particular, for any $n, k \ge 0$ and $i = 0, \dots, m$ we have

$$u_{n+k,i} = f_i^{(k)}(u_{n,0}, \dots, u_{n,m})$$

or

$$\mathbf{w}_{n+k} = \mathcal{F}^{(k)}(\mathbf{w}_n).$$

Clearly the sequence of vectors $\mathbf{w}_n$ is eventually periodic with some period $T \le p^{m+1}$. Without loss of generality we assume that it is

$$\mathbf{w}_{n+T} = \mathbf{w}_n, \qquad n = 0, 1, \dots .$$

In our construction of pseudorandom sequences, we discard the last component in the vectors $\mathbf{w}_n$ and denote

$$\mathbf{u}_n = (u_{n,0}, \dots, u_{n,m-1}),$$

which we show to be rather uniformly distributed provided T is large enough.

3.2. **Exponential sums.** We put

$$\mathbf{e}(z) = \exp(2\pi i z/p).$$

Our second main tool is the Weil bound on exponential sums (see [32, Chapter 5]), which we present in the following slightly generalized form.

Lemma 3. *For any nonconstant polynomial $F \in \mathbb{F}_p[X_0, \dots, X_m]$ of total degree D, we have the bound*

$$\left| \sum_{x_0, \dots, x_m = 1}^{p} \mathbf{e}\left(F(x_0, \dots, x_m)\right) \right| < Dp^{m+1/2}.$$

We follow the scheme previously introduced in [37, 38]. Furthermore, as has been suggested in [41, 45], we work with higher moments of the corresponding exponential sums. However the polynomial growth of the degree allows us a much more favorable choice of parameters and thus leads to a better estimate than in previous works.

Assume that the sequence $\{\mathbf{u}_n\}$ generated by (7) is purely periodic with an arbitrary period T. For an integer vector $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{Z}^m$ we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i u_{n,i}\right).$$

Theorem 4. *Let the sequence $\{\mathbf{u}_n\}$ be given by (7), where the family of $m+1$ polynomials $\mathcal{F} = \{f_0, \ldots, f_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$ of total degree $d \geq 2$ is of the form (1), satisfying the conditions (2), (3) and (4), and such that $s_{0,1} \ldots s_{m-1,m} \neq 0$. Assume that $\{\mathbf{u}_n\}$ is purely periodic with period T. Then for any fixed integer $\nu \geq 1$, and any positive integer $N \leq T$, the bound*

$$\max_{\gcd(a_0,\ldots,a_{m-1},p)=1} |S_{\mathbf{a}}(N)| = O\left(p^{\alpha_{m,\nu}} N^{1-\beta_{m,\nu}}\right)$$

holds, where

$$\alpha_{m,\nu} = \frac{2m^2 + 2m\nu + 2m + \nu}{4\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d, m and ν.

Proof. Select any $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{Z}^m$ with $\gcd(a_0, \ldots, a_{m-1}, p) = 1$. It is obvious that for any integer $k \geq 1$ we have

$$\left|S_{\mathbf{a}}(N) - \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i u_{n+k,i}\right)\right| \leq 2k.$$

Let k_0 be the same as in Corollary 2. Therefore, for any integer $K \geq k_0$,

$$(K - k_0 + 1)|S_{\mathbf{a}}(N)| \leq W + K^2, \tag{8}$$

where

$$W = \left|\sum_{n=0}^{N-1} \sum_{k=k_0}^{K} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i u_{n+k,i}\right)\right| \leq \sum_{n=0}^{N-1} \left|\sum_{k=k_0}^{K} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i u_{n+k,i}\right)\right|.$$

As before, we define the sequence of polynomials

$$f_i^{(k)}(X_0, \ldots, X_m) \in \mathbb{F}_p[X_0, \ldots, X_m]$$

by (5). Then

$$\begin{aligned}
W^{2\nu} &\leq N^{2\nu-1} \sum_{n=0}^{N-1} \left|\sum_{k=k_0}^{K} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i f_i^{(k)}(\mathbf{u_n})\right)\right|^{2\nu} \\
&\leq N^{2\nu-1} \sum_{w_0,\ldots,w_m \in \mathbb{F}_p} \left|\sum_{k=k_0}^{K} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i f_i^{(k)}(w_0, \ldots, w_m)\right)\right|^{2\nu} \\
&= N^{2\nu-1} \sum_{k_1,\ell_1,\ldots,k_\nu,\ell_\nu=k_0}^{K} \sum_{\mathbf{w} \in \mathbb{F}_p^{m+1}} \mathbf{e}\left(\sum_{i=0}^{m-1} a_i \sum_{j=1}^{\nu} \left(f_i^{(k_j)}(\mathbf{w}) - f_i^{(\ell_j)}(\mathbf{w})\right)\right).
\end{aligned}$$

For $O(K^\nu)$ vectors

$$(k_1, \ldots, k_\nu) \qquad \text{and} \qquad (\ell_1, \ldots, \ell_\nu),$$

which are permutations of each other, we estimate the inner sum trivially as p^{m+1}.

For the other $O(K^{2\nu})$ vectors, we combine Corollary 2 with Lemma 3 getting the upper bound $K^m p^{m+1/2}$ for the inner sum for at most K^2 sums. Hence,

$$W^{2\nu} \le K^\nu N^{2\nu-1} p^{m+1} + K^{m+2\nu} N^{2\nu-1} p^{m+1/2}.$$

Inserting this bound in (8), we derive

$$S_{\mathbf{a}}(N) = O\left(K^{-1/2} N^{1-1/2\nu} p^{(m+1)/2\nu} + K^{m/2\nu} N^{1-1/2\nu} p^{(2m+1)/4\nu} + K\right).$$

Choosing

$$K = \left\lceil p^{1/2(m+\nu)} \right\rceil$$

(and assuming that p is large enough, so $K \ge k_0$), after simple calculations we obtain the desired result. □

Since

$$\lim_{\nu\to\infty} \alpha_{m,\nu}/\beta_{m,\nu} = m + 1/2,$$

we see from Theorem 4 that for any fixed $\varepsilon > 0$ there is a $\delta > 0$ such that if $T \ge N \ge p^{m+1/2+\varepsilon}$, then

$$\max_{\gcd(a_0,\ldots,a_{m-1},p)=1} |S_{\mathbf{a}}(N)| = O\left(N^{1-\delta}\right)$$

(to see this, it is enough to choose a sufficiently large ν). On the other hand, when T and N are close to their largest possible value p^{m+1}, that is, if

$$T \ge N \ge p^{m+1+o(1)},$$

then Theorem 4 applied with $\nu = 1$ gives the estimate

$$\max_{\gcd(a_0,\ldots,a_{m-1},p)=1} |S_{\mathbf{a}}(N)| \le N^{1-1/4(m+1)^2+o(1)}.$$

3.3. **Discrepancy.** Given a sequence Γ of N points,

$$\Gamma = \left\{(\gamma_{n,0}, \ldots, \gamma_{n,m-1})_{n=0}^{N-1}\right\} \tag{9}$$

in the m-dimensional unit cube $[0,1)^m$, it is natural to measure the level of its statistical uniformity in terms of the *discrepancy* $\Delta(\Gamma)$. More precisely,

$$\Delta(\Gamma) = \sup_{B\subseteq[0,1)^m} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of Γ inside the box

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_m, \beta_m) \subseteq [0,1)^m$$

and the supremum is taken over all such boxes; see [13, 30].

We recall that the discrepancy is a widely accepted quantitative measure of uniformity of distribution of sequences, and thus good pseudorandom sequences should (after an appropriate scaling) have a small discrepancy; see [35, 36].

Typically the bounds on the discrepancy of a sequence are derived from bounds of exponential sums with elements of this sequence. The relation is made explicit in the celebrated *Koksma–Szüsz inequality*, see [13, Theorem 1.21], which we present in the following form.

Lemma 5. *For any integer $L > 1$ and any sequence Γ of N points (9) the discrepancy $\Delta(\Gamma)$ satisfies the following bound:*

$$\Delta(\Gamma) < O\left(\frac{1}{L} + \frac{1}{N} \sum_{\substack{|a_0|,\ldots,|a_{m-1}| \le L \\ a_0^2+\cdots+a_{m-1}^2>0}} \prod_{j=0}^{m-1} \frac{1}{|a_j|+1} \left| \sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=0}^{m-1} a_j \gamma_{j,n}\right)\right|\right).$$

Now, combining Lemma 5 with the bound obtained in Theorem 4 and taking $L = p - 1$, we obtain:

Theorem 6. *Let the sequence $\{\mathbf{u}_n\}$ be given by (7), where the family of $m+1$ polynomials $\mathcal{F} = \{f_0, \ldots, f_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$ of total degree $d \ge 2$ is of the form (1), satisfying the conditions (2), (3) and (4), and such that $s_{0,1} \ldots s_{m-1,m} \ne 0$. Assume that $\{\mathbf{u}_n\}$ is purely periodic with period T. Then for any fixed integer $\nu \ge 1$, and any positive integer $N \le T$, the discrepancy D_N of the sequence*

$$\left(\frac{u_{n,0}}{p}, \ldots, \frac{u_{n,m-1}}{p}\right), \qquad n = 0, \ldots, N-1,$$

satisfies the bound

$$D_N = O\left(p^{\alpha_{m,\nu}} N^{-\beta_{m,\nu}} (\log p)^m\right),$$

where

$$\alpha_{m,\nu} = \frac{2m^2 + 2m\nu + 2m + \nu}{4\nu(m+\nu)} \qquad \text{and} \qquad \beta_{m,\nu} = \frac{1}{2\nu}$$

and the implied constant depends only on d, m and ν.

We remark that the same comments at the end of Section 3.2 also apply to Theorem 6.

4. Remarks and open questions

We recall that the dynamical degree $\operatorname{dyndeg} \mathcal{F}$ of the polynomial system $\mathcal{F}$ and of the associated affine map $\mathcal{F} : \mathbb{F}^r \to \mathbb{F}^r$ is defined as

$$\operatorname{dyndeg} \mathcal{F} = \lim_{k \to \infty} \left(\deg \mathcal{F}^{(k)}\right)^{1/k},$$

where $\mathcal{F}^{(k)}$ is the kth iteration of $\mathcal{F}$ (and $\deg \mathcal{F}^{(k)}$ is the largest degree of its components); see [43, Section 7.1.3]. We note that the polynomial systems $\mathcal{F}$ which we have constructed in (1) satisfy $\operatorname{dyndeg} \mathcal{F} = 1$ under the conditions (2), (3) and (4). Furthermore, for any nonlinear polynomial system $\mathcal{F}$ with $\operatorname{dyndeg} \mathcal{F} = 1$, one can obtain an improvement of the generic bounds on the corresponding exponential sums and the discrepancy of the generated sequences. However the actual improvement depends on the speed of the convergence.

One of the attractive choices of polynomials (1), which leads to a very fast pseudorandom number generator, is

$$g_i(X_{i+1}, \ldots, X_m) = X_{i+1} \qquad \text{and} \qquad h_i(X_{i+1}, \ldots, X_m) = a_i$$

for some constants $a_i \in \mathbb{F}_p$, $i = 0, \ldots, m-1$. The corresponding sequence of vectors is generated at the cost of one multiplication per component. This naturally leads to a question of studying the periods of such sequences generated by such polynomial dynamical systems.

We also note that it is natural to consider the joint distribution of several consecutive vectors

$$(\mathbf{u}_n, \ldots, \mathbf{u}_{n+s-1}), \qquad n = 0, 1, \ldots,$$

in the sm-dimensional space. It seems that our method (with some minor adjustments) can be applied to derive an appropriate variant of Corollary 2 which is needed for such a result.

One of the possible ways to improve our results is to construct special polynomials $\mathcal{F} = \{f_0, \ldots, f_{r-1}\}$ such that linear combinations of their iterations, of the type which appear in the proof of Theorem 4, satisfy the condition of the Deligne bound [12], that is, have a nonsingular highest form. In fact, even some partial control over the dimension of the singularity locus of this highest form may already lead to better estimates via results of Katz [28].

Finally, obtaining stronger results "on average" over all initial values $\mathbf{w_0} \in \mathbb{F}_p^{m+1}$ is an interesting and challenging question. It is possible that some of the arguments of [39] may be applied to this problem.

Acknowledgement

The authors would like to thank Markus Brodmann, Joachim Rosenthal, Joe Silverman and Arne Winterhof for valuable comments and providing additional references.

During the preparation of this paper, A. O. was supported in part by the Swiss National Science Foundation Grant 121874 and I. S. by the Australian Research Council Grant DP0556431.

References

[1] V. I. Arnold, 'The Fermat-Euler dynamical system and the statistics of the arithmetic of geometric progressions', *Funct. Analysis Appl.*, **37** (2003), 1–15. MR1988005 (2004k:11005)

[2] V. I. Arnold, 'Number-theoretic turbulence in Fermat-Euler arithmetics and large Young diagrams geometry statistics', *J. Math. Fluid Mech.*, **7** (2005), S4–S50. MR2126128 (2006g:11199)

[3] V. I. Arnold, 'Ergodic and arithmetical properties of geometrical progression's dynamics and of its orbits', *Moscow Math. J.*, **5** (2005), 5–22. MR2153464 (2006g:11200)

[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting the inversive generator', *Lect. Notes in Comput. Sci.*, Springer-Verlag, Berlin, **2898** (2003), 264–275. MR2090938 (2005e:94096)

[5] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Predicting nonlinear pseudorandom number generators', *Math. Comp.*, **74** (2005), 1471–1494. MR2137013 (2005m:11142)

[6] J. Bourgain, 'Mordell's exponential sum estimate revisited', *J. Amer. Math. Soc.*, **18** (2005), 477–499. MR2137982 (2006b:11099)

[7] M.-C. Chang, 'On a problem of Arnold on uniform distribution', *J. Funcional Analysis*, **242** (2007), 272–280. MR2274023 (2007j:37007)

[8] W.-S. Chou and I. E. Shparlinski, 'On the cycle structure of repeated exponentiation modulo a prime', *J. Number Theory*, **107** (2004), 345–356. MR2072394 (2005e:11118)

[9] S. D. Cohen and D. Hachenberger, 'The dynamics of linearized polynomials', *Proc. Edinburgh Math. Soc.*, **43** (2000), 113–128. MR1744703 (2001a:11195)

[10] O. Colón-Reyes, A. S. Jarrah, R. Laubenbacher and B. Sturmfels, 'Monomial dynamical systems over finite fields', *Complex Systems*, **16** (2006), 333–342. MR2293353 (2007m:37041)

[11] S. Contini and I. E. Shparlinski, 'On Stern's attack against secret truncated linear congruential generators', *Lect. Notes in Comput. Sci.*, Springer-Verlag, Berlin, **3574** (2005), 52–60.

[12] P. Deligne, 'Applications de la formule des traces aux sommes trigonométriques', *Lect. Notes in Mathematics*, Springer-Verlag, Berlin, **569** (1977), 168–232.

[13] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Lect. Notes in Math. **1651**, Springer-Verlag, Berlin, 1997. MR1470456 (98j:11057)
[14] G. R. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag, London, 1999. MR1700272 (2000e:11087)
[15] S. Fomin and A. Zelevinsky, 'The Laurent phenomenon', *Adv. in Appl. Math.*, **28** (2002), 119–144. MR1888840 (2002m:05013)
[16] J. B. Friedlander, J. Hansen and I. E. Shparlinski, 'On character sums with exponential functions', *Mathematika*, **47** (2000), 75–85. MR1924489 (2003g:11089)
[17] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, 'Period of the power generator and small values of Carmichael's function', *Math. Comp.*, **70** (2001), 1591–1605. MR1836921 (2002g:11112)
[18] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, **70** (2001), 1575–1589. MR1836920 (2002f:11107)
[19] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias and A. Shamir, 'Reconstructing truncated integer variables satisfying linear congruences', *SIAM J. Comp.*, **17** (1988), 262–280. MR935340 (89d:11115)
[20] F. Griffin, H. Niederreiter and I. E. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', *Lect. Notes in Comput. Sci.*, Springer-Verlag, Berlin, **1719** (1999), 87–93. MR1846485 (2002j:94038)
[21] D. Gomez-Perez, J. Gutierrez and Á. Ibeas, 'Attacking the Pollard generator', *IEEE Trans. Inform. Theory*, **52** (2006), 5518–5523. MR2300710 (2007m:94160)
[22] J. Gutierrez and D. Gomez-Perez, 'Iterations of multivariate polynomials and discrepancy of pseudorandom numbers', *Lect. Notes in Comput. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 192–199. MR1913465
[23] D. Gomez-Perez, J. Gutierrez and I. E, Shparlinski, 'Exponential sums with Dickson polynomials', *Finite Fields Appl.*, **12** (2006), 16–25. MR2190184 (2006i:11144)
[24] J. Gutierrez and Á. Ibeas, 'Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits', *Designs, Codes and Cryptography*, **41** (2007), 199–212. MR2341883 (2008g:11204)
[25] J. Gutierrez and A. Winterhof, 'Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions', *Finite Fields Appl.*, **14** (2008), 410–416. MR2401984 (2009b:11218)
[26] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.*, **78** (2008), 523–544. MR2439638
[27] A. Joux and J. Stern, 'Lattice reduction: A toolbox for the cryptanalyst', *J. Cryptology*, **11** (1998), 161–185. MR1633944 (99c:94031)
[28] N. Katz, 'Estimates for "singular" exponential sums', *International Mathematics Research Notices*, **16** (1999), 875–899. MR1715519 (2001d:11084)
[29] H. Krawczyk, 'How to predict congruential generators', *J. Algorithms*, **13** (1992), 527–545. MR1187200 (93g:65013)
[30] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience, New York-London-Sydney, 1974. MR0419394 (54:7415)
[31] J. C. Lagarias, 'Pseudorandom number generators in cryptography and number theory', *Proc. Symp. in Appl. Math.*, Amer. Math. Soc., Providence, RI, **42** (1990), 115–143. MR1095554 (92f:11109)
[32] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997. MR1429394 (97i:11115)
[33] S. Marcello, 'Sur la dynamique arithmétique des automorphismes de l'espace affine', *Bull. Soc. Math. France*, **131** (2003), 229–257. MR1988948 (2004d:11053)
[34] G. Martin and C. Pomerance, 'The iterated Carmichael λ-function and the number of cycles of the power generator', *Acta Arith.*, **118** (2005), 305–335. MR2165548 (2006h:11119)
[35] H. Niederreiter, 'Quasi-Monte Carlo methods and pseudo-random numbers', *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041. MR508447 (80d:65016)
[36] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, SIAM Press, 1992. MR1172997 (93h:65008)
[37] H. Niederreiter and I. E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields and Their Appl.*, **5** (1999), 246–253. MR1702905 (2000i:11126)

[38] H. Niederreiter and I. E. Shparlinski, 'On the distribution of inversive congruential pseudorandom numbers in parts of the period', *Math. Comp.*, **70** (2001), 1569–1574. MR1836919 (2002e:11104)
[39] H. Niederreiter and I. E. Shparlinski, 'On the average distribution of inversive pseudorandom numbers', *Finite Fields and Their Appl.*, **8** (2002), 491–503. MR1933620 (2003g:11085)
[40] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comput. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17. MR2042407 (2005a:94047)
[41] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64. MR2381476 (2008m:11166)
[42] I. E. Shparlinski, 'On some dynamical systems in finite fields and residue rings', *Discr. and Cont. Dynam. Syst., Ser.A*, **17** (2007), 901–917. MR2276481 (2007j:11098)
[43] J. H. Silverman, *The arithmetic of dynamical systems*, Grad. Texts in Math. **241**, Springer, New York, 2007. MR2316407 (2008c:11002)
[44] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616. MR2448661
[45] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006, 135–166. MR2278037 (2007m:11106)
[46] T. Vasiga and J. O. Shallit, 'On the iteration of certain quadratic maps over GF(p)', *Discr. Math.*, **277** (2004), 219–240. MR2033734 (2004k:05104)

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190 CH-8057, Zürich, Switzerland
E-mail address: alina.ostafe@math.uzh.ch

Department of Computing, Macquarie University, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au