Multivariate permutation polynomial systems and nonlinear pseudorandom number generators

Ostafe, A

DOI: https://doi.org/10.1016/j.ffa.2009.12.003

MULTIVARIATE PERMUTATION POLYNOMIAL SYSTEMS AND NONLINEAR PSEUDORANDOM NUMBER GENERATORS

ALINA OSTAFE

ABSTRACT. In this paper we study a class of dynamical systems generated by iterations of multivariate permutation polynomial systems which lead to polynomial growth of the degrees of these iterations. Using these estimates and the same techniques studied previously for inversive generators, we bound exponential sums along the orbits of these dynamical systems and show that they admit much stronger estimates "on average" over all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ than in the general case and thus can be of use for pseudorandom number generation.

1. INTRODUCTION

Let $\mathcal{F} = \{f_0, \ldots, f_m\}$ be a system of $m+1$ polynomials in $m+1$ variables over an arbitrary field. One can naturally define a dynamical system generated by its iterations, see [3, 21] and references therein for various aspects of such dynamical systems, and consider the orbits obtained by such iterations evaluated at a certain initial value $(v_0, \ldots, v_m)$. The statistical uniformity of the distribution (measured by the discrepancy) of one and multidimensional nonlinear polynomial generators over a finite field have been studied in [6, 7, 17, 18, 22]. However, almost 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 practice (the only known exceptions are generators from inversions [16], power functions [4], Dickson polynomials [5] and Redei functions [8]). 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 $m = 0$) the exponential growth of the degree of iterations of a nonlinear polynomial is unavoidable. One also expects the same behaviour in the multidimensional case for "random" polynomials $f_0, \ldots, f_m$. However, as we saw in [19], for some specially selected polynomials $f_0, \ldots, f_m$ the degree may grow significantly slower.

In [19] 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 the discrepancy, for vectors generated by these iterations (after scaling them to the unit cube), with a saving over the trivial bound being a power of p.

Obtaining stronger results "on average" over all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ is an interesting and challenging question. We remark that in the case of the so-called inversive generator rather stronger estimates "on average" are available (see [16])

Key words and phrases. Pseudorandom number generators, permutation polynomials, discrepancy.

and also estimates for the average distribution of powers and primitive elements of the inversive generators are considered in [1]. In this paper we study this problem by following the same arguments introduced for the inversive generator in [16]. For this we define a special family of multivariate polynomial systems of [19], which beside the polynomial degree growth also leads to *permutation polynomial systems*. In turn this allows us to use the approach of [16] to obtain a stronger bound on the discrepancy "on average" over initial values.

Furthermore, here we exploit the special structure of iterations of the polynomial systems of [19] that allows us to replace the use of the Weil bound (see [12, Chapter 5]) by a more elementary and stronger estimate on the corresponding exponential sums which in turn leads to a better final result and for more general systems of congruences. In fact, since our construction can easily be extended to polynomials over commutative rings, the new estimate can also be used to study polynomials maps over residue rings (while the Weil bound does not apply there). This estimate can also be used to improve and generalise the main result of [19].

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

Throughout the paper, the implied constants in the symbols 'O' and '$\ll$' may occasionally, where obvious, depend on some integer parameter $s \geq 1$ and are absolute otherwise. We recall that the notations $A = O(B)$ and $A \ll B$ are all equivalent to the assertion that the inequality $|A| \leq c|B|$ holds for some constant $c > 0$.

2. Permutation Polynomial Dynamical System with Slow Degree Growth

2.1. **General construction.** We recall and modify the construction of [19] of multivariate polynomial systems with slow degree growth. Let $\mathbb{F}$ be an arbitrary field and let the polynomials $g_i, h_i \in \mathbb{F}[X_{i+1}, \ldots, X_m]$, $i = 0, \cdots, m-1$, satisfying the following conditions: each polynomial g_i has a *unique leading monomial* $X_{i+1}^{s_{i,i+1}} \ldots X_m^{s_{i,m}}$, that is,

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

where

$$\deg_{X_j} \widetilde{g}_i < s_{i,j}, \qquad \deg_{X_j} h_i \leq s_{i,j}, \tag{2}$$

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

Throughout, we use deg to denote the total degree of a multivariate polynomial.

We construct now a system $\mathcal{F} = \{f_0, \dots, f_m\}$ of $m+1$ polynomials in the ring $\mathbb{F}[X_0, \dots, X_m]$ defined in the following way:

$$\begin{aligned} f_0(X_0, \dots, X_m) &= X_0 g_0(X_1, \dots, X_m) + h_0(X_1, \dots, X_m), \\ f_1(X_0, \dots, X_m) &= X_1 g_1(X_2, \dots, X_m) + h_1(X_2, \dots, X_m), \\ &\dots \\ f_{m-1}(X_0, \dots, X_m) &= X_{m-1} g_{m-1}(X_m) + h_{m-1}(X_m), \\ f_m(X_0, \dots, X_m) &= aX_m + b, \end{aligned} \tag{3}$$

where

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

are defined as above.

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

$$f_i^{(0)} = X_i, \qquad f_i^{(k)} = f_i(f_0^{(k-1)}, \dots, f_m^{(k-1)}), \qquad k = 0, 1, \dots . \tag{4}$$

The following result shows the exact form of the polynomials $f_i^{(k)}$ and also the polynomial growth of the degrees of the polynomials $X_i g_i$, $i = 0, \dots, m$, under iterations.

Lemma 1. *Let $f_0, \dots, f_m \in \mathbb{F}[X_0, \dots, X_m]$ be as in (3), satisfying the conditions (1) and (2). Then for the polynomials $f_i^{(k)}$, $k = 1, 2, \dots$, given by (4) we have*

$$f_i^{(k)} = X_i g_{i,k}(X_{i+1}, \dots, X_m) + h_{i,k}(X_{i+1}, \dots, X_m)$$

where $g_{i,k}, h_{i,k} \in \mathbb{F}[X_{i+1}, \dots, X_m]$ and

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

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

Proof. We have

$$f_i^{(k)} = f_i^{(k-1)} g_i\left(f_{i+1}^{(k-1)}, \dots, f_m^{(k-1)}\right) + h_i\left(f_{i+1}^{(k-1)}, \dots, f_m^{(k-1)}\right).$$

Thus an easy inductive argument implies that

$$f_i^{(k)} = X_i g_{i,k}(X_{i+1}, \dots, X_m) + h_{i,k}(X_{i+1}, \dots, X_m)$$

for some polynomials $g_{i,k}, h_{i,k} \in \mathbb{F}[X_{i+1}, \dots, X_m]$, with $\deg g_{i,k} \geq \deg h_{i,k}$, where $i = 0, \dots, m$, $k = 1, 2, \dots$.

For the asymptotic formulas for the degrees of the polynomials $g_{i,k}$ see [19, Lemma 1] where it is given in the equivalent form for $\deg f_i^{(k)} = \deg g_{i,k} + 1$. □

2.2. **Permutation polynomial systems.** In order to be able to apply the technique introduced in [16] for inversive pseudorandom number generators, we need to work with systems of multivariate polynomials in $\mathbb{F}_p[X_0, \ldots, X_m]$ which induce maps that permute the elements of $\mathbb{F}_p^{m+1}$. Lidl and Niederreiter [12, 13] call such systems *orthogonal polynomial systems*, but we here refer to them as *permutation polynomial systems*.

Let the polynomial system $\mathcal{F} = \{f_0, \ldots, f_m\}$, $m \geq 1$, be defined by (3) and satisfy the conditions (1) and (2). It is obvious that this system is a permutation system if and only if the polynomials g_i, $i = 0, \ldots, m$, do not have zeros over $\mathbb{F}_p$.

We note that a "typical" absolute irreducible polynomial in $m \geq 2$ variables over $\mathbb{F}_p$ always has lots of zeros. By a special case of the Lang-Weil theorem [11] a polynomial F in $m \geq 2$ variables over $\mathbb{F}_p$ always has $rp^{m-1} + O(p^{m-3/2})$ zeros where r is the number of absolutely irreducible factors of F (with the implied constant depending only on $\deg F$), see also [20]. That is why we seek "atypical" polynomials, as the example below shows.

One of the attractive choices of polynomials which would lead to a fast PRNG is

$$g_i(X_{i+1}, \ldots, X_m) = \prod_{j=1}^{m-i} (X_{i+j}^2 - a_{i,j})$$

and

$$h_i(X_{i+1}, \ldots, X_m) = b_i$$

where $a_{i,j}$ are quadratic nonresidues and b_i are any constants in $\mathbb{F}_p$.

Even simpler, one can take

$$g_i(X_{i+1}, \ldots, X_m) = (X_{i+1}^2 - a_i)$$

where a_i are quadratic nonresidues.

3. Polynomial Pseudorandom Number Generators

3.1. **Construction.** Let $\mathcal{F} = \{f_0, \ldots, f_m\}$ be a permutation polynomial system in $\mathbb{F}_p[X_0, \ldots, X_m]$ defined as in Section 2. We fix a vector $\mathbf{v} \in \mathbb{F}_p^{m+1}$ and consider the sequence defined by a recurrence congruence modulo a prime p of the form

$$u_{n+1,i} \equiv f_i(u_{n,0}, \ldots, u_{n,m}) \pmod{p}, \qquad n = 0, 1, \ldots, \tag{5}$$

with the *initial values* $(u_{0,0}, \ldots, u_{0,m}) = \mathbf{v}$. We also assume that $0 \leq u_{n,i} < p$, $i = 0, \ldots, m$, $n = 0, 1, \ldots$.

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

$$u_{n+k,i}(\mathbf{v}) = f_i^{(k)}(u_{n,0}(\mathbf{v}), \ldots, u_{n,m}(\mathbf{v})). \tag{6}$$

Using the following vector notation

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

we have the recurrence relation

$$\mathbf{u}_{n+k}(\mathbf{v}) = (f_0^{(k)}(u_{n,0}(\mathbf{v}), \ldots, u_{n,m}(\mathbf{v})), \ldots, f_{m-1}^{(k)}(u_{n,0}(\mathbf{v}), \ldots, u_{n,m}(\mathbf{v}))).$$

We show that for almost all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$, the sequence

$$\left(\frac{u_{n,0}(\mathbf{v})}{p}, \ldots, \frac{u_{n,m-1}(\mathbf{v})}{p}\right), \qquad n = 0, \ldots, N-1, \tag{7}$$

is uniformly distributed for all $N \ge (\log p)^{2+\varepsilon}$, any fixed $\varepsilon > 0$ and sufficiently large p.

3.2. **Exponential Sums.** We put

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

Our second main tool is the following bound on exponential sums which is stronger than the one immediately implied by the Weil bound (see [12, Chapter 5]).

Lemma 2. *Let $f_0, \ldots, f_m \in \mathbb{F}_p[X_0, \ldots, X_m]$ be as in (3), satisfying the conditions (1) and (2). If $s_{0,1} \ldots s_{m-1,m} \ne 0$, then there is a positive integer k_0 depending only on the degrees of the polynomials in $\mathcal{F}$ such that for any integers $k > l \ge k_0$ and any nonzero $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p^m$, for the polynomial*

$$F_{\mathbf{a},k,l} = \sum_{i=0}^{m-1} a_i \left(f_i^{(k)} - f_i^{(l)}\right),$$

we have

$$\left| \sum_{x_0,\ldots,x_m=1}^{p} \mathbf{e}_p\left(F_{\mathbf{a},k,l}(x_0, \ldots, x_m)\right) \right| \ll k^m p^m.$$

Proof. Let $s \le m-1$ be the smallest integer such that $a_s \ne 0$. By Lemma 1 we have

$$\begin{aligned}
&\sum_{x_0,\ldots,x_m=1}^{p} \mathbf{e}_p\left(F_{\mathbf{a},k,l}(x_0, \ldots, x_m)\right) \\
&\quad = \sum_{x_0,\ldots,x_m=1}^{p} \mathbf{e}_p\left(\sum_{i=0}^{m-1} a_i \left(x_i(g_{i,k} - g_{i,l}) + (h_{i,k} - h_{i,l})\right)\right) \\
&\quad = p^s \sum_{x_s,\ldots,x_m=1}^{p} \mathbf{e}_p\left(\sum_{i=s}^{m-1} a_i \left(x_i(g_{i,k} - g_{i,l}) + (h_{i,k} - h_{i,l})\right)\right) \\
&\quad = p^s \sum_{x_{s+1},\ldots,x_m=1}^{p} \mathbf{e}_p\left(h_{s,k} - h_{s,l} + \sum_{i=s+1}^{m-1} a_i \left(x_i(g_{i,k} - g_{i,l}) + (h_{i,k} - h_{i,l})\right)\right) \\
&\qquad\qquad \sum_{x_s=1}^{p} \mathbf{e}_p\left(a_s x_s (g_{s,k} - g_{s,l})\right).
\end{aligned}$$

Then the sum over the variable x_s is nonzero only if its coefficient

$$g_{s,k}(x_{s+1}, \ldots, x_m) - g_{s,l}(x_{s+1}, \ldots, x_m) \equiv 0 \pmod p,$$

see [13, Equation (5.9)].

We see from Lemma 1 that if $k > l \geq k_0$ for a sufficiently large k_0 then $g_{s,k} - g_{s,l}$ is a nontrivial polynomial modulo p of degree $O(k^{m-s}) = O(k^m)$. A simple inductive argument shows that a nontrivial modulo p polynomial in r variables of degree D may have only $O(Dp^{r-1})$ zeros modulo p, which concludes the proof. □

We note that we do not include the linear polynomials $f_m^{(k)}$ and $f_m^{(l)}$ in $F_{\mathbf{a},k,l}$ as generally speaking in this case such a linear combination may vanish even for nontrivial coefficients (note that it is possible that $f_m^{(k)} = f_m^{(l)}$ for $k \neq l$).

We follow the scheme previously introduced in [16] for estimating the exponential sum introduced below, and thus the discrepancy of a sequence of points.

For a vector $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p^m$ and integers c, M, N with $M \geq 1$ and $N \geq 1$, we introduce

$$V_{\mathbf{a},c}(M,N) = \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j f_j^{(n)}(v_0, \ldots, v_m) \right) \mathbf{e}_M(cn) \right|^2.$$

Note that as in Lemma 2 we do not include polynomials $f_m^{(n)}$ in the above exponential sum.

Lemma 3. *Let the permutation polynomial system of $m+1$ polynomials $\mathcal{F} = \{f_0, \ldots, f_m\} \in \mathbb{F}_p[X_0, \ldots, X_m]$ of total degree $d \geq 2$ of the form (3), satisfying the conditions (1) and (2). Then for any positive integers c, M, N and any nonzero vector $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathbb{F}_p^m$ we have*

$$V_{\mathbf{a},c}(M,N) \ll A(N,p),$$

where

$$A(N,p) = \begin{cases} Np^{m+1} & \text{if } N \leq p^{1/(m+1)}, \\ N^2 p^{m(m+2)/(m+1)} & \text{if } N > p^{1/(m+1)}. \end{cases}$$

Proof. We have

$$\begin{aligned} V_{\mathbf{a},c}(M,N) &= \sum_{k,l=0}^{N-1} \mathbf{e}_M(c(k-l)) \\ &\qquad \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j \left(f_j^{(k)}(v_0, \ldots, v_m) - f_j^{(l)}(v_0, \ldots, v_m) \right) \right) \\ &\leq \sum_{k,l=0}^{N-1} \left| \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j \left(f_j^{(k)}(v_0, \ldots, v_m) - f_j^{(l)}(v_0, \ldots, v_m) \right) \right) \right|. \end{aligned}$$

For $O(N)$ values of k and l which are equal, we estimate the inner sum trivially by p^{m+1}.

For the other values, by Lemma 2 getting the upper bound $O(N^m p^m)$ for the inner sum for at most N^2 sums. Hence,

$$V_{\mathbf{a},c}(M,N) \ll Np^{m+1} + N^{m+2}p^m. \tag{8}$$

Because $\mathcal{F}$ is a permutation polynomial system and using (6), for any integer L we obtain

$$\begin{aligned}
&\sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=L}^{L+N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j f_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_M(cn) \right|^2 \\
&\quad = \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \\
&\qquad \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j f_j^{(n)} \left(f_0^{(L)}(v_0,\ldots,v_m), \ldots, f_m^{(L)}(v_0,\ldots,v_m) \right) \right) \mathbf{e}_M(cn) \right|^2 \\
&\quad = \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j f_j^{(n)}(v_0,\ldots,v_m) \right) \mathbf{e}_M(cn) \right|^2 = V_{\mathbf{a},c}(M,N).
\end{aligned}$$

Therefore, for any positive integer $K \le N$, separating the inner sum into at most $N/K+1$ subsums of length at most K, and using (8), we derive

$$V_{\mathbf{a},c}(M,N) \ll (Kp^{m+1} + K^{m+2}p^m)N^2K^{-2} = N^2(K^{-1}p^{m+1} + K^m p^m).$$

Thus, selecting $K = \min\{N, \lfloor p^{1/(m+1)} \rfloor\}$ and taking into account that $N^{-1}p^{m+1} \ge N^m p^m$ for $N \le p^{1/(m+1)}$, we obtain the desired result. □

Note that the estimates for $V_{\mathbf{a},c}(M,N)$ work not only over prime fields, but also over any finite field.

We also need the identity (see [9])

$$\sum_{-(m-1)/2 \le a \le m/2} \mathbf{e}_m(ab) = \begin{cases} 0 & \text{if } b \not\equiv 0 \pmod m, \\ m & \text{if } b \equiv 0 \pmod m. \end{cases} \tag{9}$$

Then we have the following inequality

$$\sum_{r=L+1}^{L+Q} \mathbf{e}_m(cr) \ll \min\left\{Q, \frac{m}{|c|}\right\} \ll \min\left\{m, \frac{m}{|c|}\right\} \ll \frac{m}{|c|+1} \tag{10}$$

which holds for any integers c, Q and L with $|c| \le m/2$, and $m \ge Q \ge 1$, see [9, Bound (8.6)].

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

$$\Gamma = \left\{(\gamma_{n,0}, \ldots, \gamma_{n,s-1})_{n=0}^{N-1}\right\} \tag{11}$$

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

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

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

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes, see [2, 10].

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 [14, 15].

For an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{a}| = \max_{j=0,\ldots,s-1} |a_j|, \qquad r(\mathbf{a}) = \prod_{j=0}^{s-1} \max\{|a_j|, 1\}.$$

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 *Erdős-Turan-Koksma inequality*, see [2, Theorem 1.21], which we present in the following form.

Lemma 4. *For any integer $L > 1$ and any sequence Γ of N points* (11) *the discrepancy $\Delta(\Gamma)$ satisfies the following bound:*

$$\Delta(\Gamma) < O\left(\frac{1}{L} + \frac{1}{N} \sum_{0 < |\mathbf{a}| \le L} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=0}^{s-1} a_j \gamma_{n,j}\right) \right| \right).$$

Now, as in [16], combining Lemma 4 with the bound obtained in Lemma 3 we obtain stronger estimates for the discrepancy "on average" over all initial values.

Theorem 5. *Let $0 < \varepsilon < 1$ and let the sequence $\{\mathbf{u}_n\}$ be given by* (5)*, where the permutation system 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* (3)*, satisfying the conditions* (1) *and* (2)*, and such that $s_{0,1} \ldots s_{m-1,m} \ne 0$. Then for all initial values $\mathbf{v} \in \mathbb{F}_p^{m+1}$ except at most $O(\varepsilon p^{m+1})$ of them, and any positive integer $N \le p^{m+1}$, the discrepancy $D_N(\mathbf{v})$ of the sequence* (7) *satisfies the bound*

$$D_N(\mathbf{v}) \ll \varepsilon^{-1} B(N,p),$$

where

$$B(N,p) = \begin{cases} N^{-1/2} (\log N)^{m+1} \log p & \text{if } N \le p^{1/(m+1)}, \\ p^{-1/2(m+1)} (\log N)^{m+1} \log p & \text{if } N > p^{1/(m+1)}. \end{cases}$$

Proof. Without loss of generality we can assume that $N \ge 2$. From Lemma 4 with $G = \lfloor N/2 \rfloor$ we derive

$$D_N(\mathbf{v}) \ll \frac{1}{N} + \frac{1}{N} \sum_{0<|\mathbf{a}|\le N/2} \frac{1}{r(\mathbf{a})} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \right|.$$

Let $m_\nu = 2^\nu$, $\nu = 0, 1, \ldots$, and define $k \ge 1$ by the condition $m_{k-1} < N \le m_k$. From (9) we derive

$$\sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) = \frac{1}{m_k} \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \sum_{-(m_k-1)/2 \le c \le m_k/2} \sum_{r=0}^{N-1} \mathbf{e}_{m_k}(c(n-r)).$$

Since $m_k/2 = m_{k-1}$, from (10) we obtain

$$\left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \right| \ll \sum_{|c| \le m_{k-1}} \frac{1}{|c|+1} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \mathbf{e}_{m_k}(cn) \right|.$$

It follows that

$$D_N(\mathbf{v}) \ll \Delta_k(\mathbf{v}), \tag{12}$$

where

$$\Delta_k(\mathbf{v}) = \frac{1}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{|c| \le m_{k-1}} \frac{1}{|c|+1} \cdot \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j u_{n,j}(\mathbf{v}) \right) \mathbf{e}_{m_k}(cn) \right|.$$

Now

$$\sum_{\mathbf{v}=(v_0,\ldots,v_m) \in \mathbb{F}_p^{m+1}} \Delta_k(\mathbf{v}) = \frac{p^{m+1}}{N} + \frac{1}{m_k} \sum_{0<|\mathbf{a}|\le m_{k-1}} \frac{1}{r(\mathbf{a})} \sum_{|c| \le m_{k-1}} \frac{1}{|c|+1} \cdot \sum_{v_0,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{m_k-1} \mathbf{e}_p \left(\sum_{j=0}^{m-1} a_j f_j^{(n)}(v_0, \ldots, v_m) \right) \mathbf{e}_{m_k}(cn) \right|.$$

Applying the Cauchy inequality, from Lemma 3 we derive

$$\sum_{v_0,\ldots,v_m\in\mathbb{F}_p}\left|\sum_{n=0}^{m_k-1}\mathbf{e}_p\left(\sum_{j=0}^{m-1}a_jf_j^{(n)}(v_0,\ldots,v_m)\right)\mathbf{e}_{m_k}(cn)\right|\ll p^{(m+1)/2}A(m_k,p)^{1/2}.$$

Therefore

$$\begin{aligned}\sum_{v_0,\ldots,v_m\in\mathbb{F}_p}\Delta_k(\mathbf{v})&\ll\frac{p^{m+1}}{N}+\frac{p^{(m+1)/2}A(m_k,p)^{1/2}}{m_k}\sum_{0<|\mathbf{a}|\le m_{k-1}}\frac{1}{r(\mathbf{a})}\sum_{|c|<m_{k-1}}\frac{1}{|c|+1}\\&\ll\frac{p^{(m+1)/2}A(m_k,p)^{1/2}(\log m_k)^{m+1}}{m_k},\end{aligned}$$

where we used the standard bound for partial sums of the harmonic series in the last step. Thus, for each $k=1,\ldots,\lceil\log(p^{m+1})\rceil$, the inequality

$$\Delta_k(\mathbf{v})\ge\frac{A(m_k,p)^{1/2}(\log m_k)^{m+1}\log p}{\varepsilon m_kp^{(m+1)/2}}=\varepsilon^{-1}B(m_k,p)\tag{13}$$

can hold for at most $O(\varepsilon p^{m+1}/\log p)$ values of $v_0,\ldots,v_m\in\mathbb{F}_p$. Therefore the number of $v_0,\ldots,v_m\in\mathbb{F}_p$ for which (13) holds for at least one $k=1,\ldots,\lceil\log(p^{m+1})\rceil$ is $O(\varepsilon p^{m+1})$. For all other $v_0,\ldots,v_m$, we get from (12),

$$D_N(\mathbf{v})\ll\Delta_k(\mathbf{v})<\varepsilon^{-1}B(m_k,p)\ll\varepsilon^{-1}B(N,p)$$

for $1\le N\le p^{m+1}$, where we used $m_k=2m_{k-1}<2N$ in the last step. □

4. Remarks and Open Questions

As we have mentioned, one of the attractive choices of polynomials (3), which leads to a very fast pseudorandom number generator is

$$g_i(X_{i+1},\ldots,X_m)=X_{i+1}^2-a_i\qquad\text{and}\qquad h_i(X_{i+1},\ldots,X_m)=b_i$$

for some quadratic nonresidues a_i and any constants b_i, $i=0,\ldots,m-1$. The corresponding sequence of vectors is generated at the cost of two multiplications per component. This naturally leads to a question of studying in what cases the periods of such sequences generated by such polynomial dynamical systems are maximal.

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

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

in the sm-dimensional space. It seems that the scheme used in [19] can be also applied to derive such a result.

Acknowledgement

The author would like to thank Igor Shparlinski for introducing the idea of using permutation polynomial systems in order to obtain better results and also Markus Brodmann, Joachim Rosenthal, Arne Winterhof and the anonymous referee for valuable comments and providing additional references.

The idea of this work appeared during the "Cryptography Retrospective Meeting" at the Fields Institute, May, 2009, which hospitality and financial support is gratefully appreciated.

During the preparation of this paper, the author was also supported in part by the Swiss National Science Foundation Grant 121874.

References

[1] A. Çeşmelioğlu and A. Winterhof, 'On the average distribution of power residues and primitive elements in inversive and nonlinear recurring sequences ', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **5203** (2008), 60–70.

[2] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[3] G. R. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag, London, 1999.

[4] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, **70** (2001), 1575–1589.

[5] D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 'Exponential sums with Dickson polynomials', *Finite Fields Appl.*, **12** (2006), 16–25.

[6] F. Griffin, H. Niederreiter and I. E. Shparlinski, 'On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1719** (1999), 87–93.

[7] J. Gutierrez and D. Gomez-Perez, 'Iterations of multivariate polynomials and discrepancy of pseudorandom numbers', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2227** (2001), 192–199.

[8] J. Gutierrez and A. Winterhof, 'Exponential sums of nonlinear congruential pseudorandom number generators with Redei functions', *Finite Fields Appl.*, **14** (2008), 410–416.

[9] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[10] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Intersci., New York-London-Sydney, 1974.

[11] S. Lang and A. Weil, 'Number of points of varieties in finite fields', *Amer. J. Math.*, **76** (1954), 819–827.

[12] R. Lidl and H. Niederreiter, 'On orthogonal systems and permutation polynomials in several variables', *Acta Arith.*, **22** (1973), 257–265.

[13] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[14] H. Niederreiter, 'Quasi-Monte Carlo methods and pseudo-random numbers', *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.

[15] H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods*, SIAM Press, 1992.

[16] H. Niederreiter and I. E. Shparlinski, 'On the average distribution of inversive pseudorandom numbers', *Finite Fields and Their Appl.*, **8** (2002), 491–503.

[17] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17.

[18] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64.
[19] A. Ostafe and I. E. Shparlinski, 'On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators', *Math. Comp.* 79 (2010) 501-511.
[20] W. M. Schmidt, 'A lower bound for the number of solutions of equations over finite fields', *J. Number Theory*, **6** (1974), 448–480.
[21] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York, 2007.
[22] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006, 135–166.

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190 CH-8057, Zürich, Switzerland

E-mail address: alina.ostafe@math.uzh.ch