ALGEBRAIC ENTROPY, AUTOMORPHISMS AND SPARSITY OF ALGEBRAIC DYNAMICAL SYSTEMS AND PSEUDORANDOM NUMBER GENERATORS

DOMINGO GÓMEZ-PÉREZ, ALINA OSTAFE, AND IGOR SHPARLINSKI

Abstract. We present several general results that show how algebraic dynamical systems with a slow degree growth and also rational automorphisms can be used to construct stronger pseudorandom number generators. We then give several concrete constructions that illustrate the applicability of these general results.

1. Introduction

1.1. **Motivation.** It is well-known that most of the pseudorandom number generators used in Monte Carlo methods and cryptography are based on the iteration of rational functions, see [9, 18, 19, 22]. However, a "randomly" chosen system of such functions usually yields a rather poor generator, with a short cycle length. Here we discuss the properties of pseudorandom number generators based on the iteration of several special systems of rational functions that lead to better generators. Surprisingly, these constructions bring together several notions which have intrinsic interest in the theory of polynomial rings over finite fields, such as algebraic entropy and automorphisms. We also give new explicit constructions of rational functions that satisfy the desired conditions.

1.2. **Degree growth of algebraic dynamical systems.** Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ be a system of m rational functions in $\mathbb{F}_p(X_1, \ldots, X_m)$, where p is prime and $\mathbb{F}_p$ denotes the finite field of p elements and each element is represented by an integer in the range $\{0, \ldots, p-1\}$. For each $i = 1, \ldots, m$ we define the k-th iteration of the polynomial F_i, $i = 1, \ldots, m$, by the recurrence relation

$$F_i^{(0)} = X_i, \quad F_i^{(k)} = F_i^{(k-1)}(F_1, \ldots, F_m) = F_i^{(k-1)}(\mathcal{F}), \qquad k = 1, 2, \ldots.$$

2010 *Mathematics Subject Classification.* Primary 11K45, 37A45; Secondary 11T71, 65C10, 94A60.

Key words and phrases. Pseudoransdom numbers, polynomial iterations.

It is certainly natural to expect that the degrees of the iterations $F_i^{(k)}$, $i = 1, \ldots, m$, grow exponentially with k (which is always the case for iterations of nonlinear univariate polynomials). On the other hand, it has been shown in recent works [11, 12, 13, 14, 16, 17] that there are rich families of multivariate polynomial systems with much slower degree growth and that such families lead to better pseudorandom number generators.

We recall that the *algebraic entropy* of the dynamical system generated by $\mathcal{F} = \{F_1, \ldots, F_m\}$ is

$$\delta(\mathcal{F}) = \lim_{n\to\infty} \frac{\log D_n(\mathcal{F})}{n},$$

where $D_k(\mathcal{F})$ is the degree of $\mathcal{F}^{(k)}$, defined as the largest degree of the components $F_1^{(k)}, \ldots, F_m^{(k)}$, see [1, 20, 21] and references therein. We note that the existence of the above limit follows immediately from the inequality $D_{k+m}(\mathcal{F}) \le D_k(\mathcal{F})D_m(\mathcal{F})$.

In particular, the polynomial systems constructed in [11, 13, 14, 16] are of algebraic entropy zero. The degree growth of this class of systems is polynomial in the number of iterations and therefore, it satisfies a linear recurrence. This is in full agreement with [1, Conjecture 1], which asserts that the generating function of the degree sequence $D_n(\mathcal{F})$ is rational, that is,

$$\sum_{n=0}^{\infty} D_n(\mathcal{F}) Z^n \in \mathbb{Z}(Z),$$

where, as usual, $\mathbb{Z}$ denotes the ring of integers.

However, these constructions have two common features which may potentially lead to cryptographically weak pseudorandom number generators that are based on these systems. More precisely,

- the ith rational function F_i is linear in at least one variable;
- these systems are of triangular shape, that is, F_i depends only on $X_i, \ldots, X_m$.

Here we introduce a new approach, namely, we show how to use the *rational automorphisms* of $\mathbb{F}_p(X_1, \ldots, X_m)$ to overcome the above potential weaknesses, see Section 2.4 for a definition and some specific examples of automorphisms. This is the first step to study the distribution of vectors generated by systems of rational functions with zero algebraic entropy.

We present general results of this kind which we then apply to certain specific examples which lead to new families of pseudorandom number generators.

1.3. **Sparsity of polynomial systems.** Another class of algebraic dynamical systems which can be useful for designing good pseudorandom number generators is the class of polynomial systems such that their iterations have certain sparsity with respect to some variables (and with strictly positive algebraic entropy). For example, such are the polynomial systems constructed in [15], for which we have $F_i^{(k)} = (X_i - h_i)^{e_i^k} G_i + h_i$ for some integers e_i, elements $h_i \in \mathbb{F}_p$ and polynomials $G_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$, $i = 1, \ldots, m$. Here we give more examples of such systems and also show how to use polynomial automorphisms to expand the class of such systems.

1.4. **Pseudorandom number generators.** We consider the sequence of vectors defined by a recurrence relation over $\mathbb{F}_p$ of the form

$$u_{n+1,i} = F_i(u_{n,1}, \ldots, u_{n,m}), \qquad n = 0, 1, \ldots, \tag{1}$$

with some *initial values* $u_{0,1}, \ldots, u_{0,m}$. We also assume that, $0 \le u_{n,i} < p$, $i = 1, \ldots, m$, $n = 0, 1, \ldots$, and that if $(u_{n,1}, \ldots, u_{n,m})$ is a pole of F_i, then we set $F_i(u_{n,1}, \ldots, u_{n,m}) = 0$ (certainly there is nothing special in this choice and it can be set to any other fixed element from $\mathbb{F}_p$). Additionally, we need to suppose $m \ge 2$, due to the difference between the behaviour in the univariate and multivariate case. Using the following vector notation

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

we have the recurrence relation

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

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

$$u_{n+k,i} = F_i^{(k)}(u_{n,1}, \ldots, u_{n,m}) \quad \text{or} \quad \mathbf{u}_{n+k} = \mathcal{F}^{(k)}(\mathbf{u}_n).$$

We also set $0^{-1} = 0$ so that the relation (1) is always well-defined. Clearly the sequence of vectors $\{\mathbf{u}_n\}$ is eventually periodic with some period less than p^m.

Furthermore, for a sequence $\{\mathbf{u}_n\}$ generated by (1) we define the trajectory length as the smallest integer $T \ge 1$ such that $\mathbf{u}_T = \mathbf{u}_r$ for some $r < T$. Clearly all vectors $\mathbf{u}_0, \ldots, \mathbf{u}_{T-1}$ are pairwise distinct, so $T \le p^m$. Some constructions of systems for which T achieves its largest possible value p^m are given in [12, 16].

We note that there is little doubt that analogues of our results also hold over arbitrary finite fields, however some bounds of character sums require more care. For example, an analogue of Lemma 2 over a finite field of q elements of characteristic p requires an additional condition

$F/G \neq H^p - H$ for any rational function H over the algebraic closure of $\mathbb{F}_p$, that could be more difficult to verify.

1.5. **General notation.** As usual, $\mathbb{Z}_q$ denotes the ring of the integers modulo q and $\mathbb{Z}_q^*$ represents the set of multiplicative units of $\mathbb{Z}_q$.

The polynomials over $\mathbb{F}_p$ are usually denoted by capital letters and we omit the variables on which they depend if it is clear from the context.

We use $\#\mathcal{S}$ denotes the number of elements of a set $\mathcal{S}$.

We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the statement that $|U| \le cV$ holds with some constant $c > 0$. Throughout the paper, any implied constants in the symbols O, $\ll$ and $\gg$ may occasionally depend, where obvious, on the dimension of the points and some real positive parameters ε and δ, and are absolute otherwise.

The letters, m, n, r, s in lower case, always denote integer numbers.

2. Preliminaries

2.1. **Discrepancy and exponential sums.** For an integer $M \ge 2$, define the following sequence Γ of N points

$$(\gamma_{n,1}, \ldots, \gamma_{n,s}) \in [0,1)^s, \quad \gamma_{n,i} = y_{n,i}/M, \quad n = 0, \ldots, N-1, \tag{2}$$

where $y_{n,1}, \ldots, y_{n,s}$ are integers between 0 and $M-1$. It is natural to measure the level of its statistical uniformity in terms of the *discrepancy* $D_N(\Gamma)$. More precisely,

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

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

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

of volume $|\mathcal{B}| = (\beta_1 - \alpha_1) \ldots (\beta_s - \alpha_s)$ and the supremum is taken over all such boxes, see [2].

We study the discrepancy of the sequence in the m-dimensional unit interval,

$$\frac{1}{p}\mathbf{u}_n = \left(\frac{u_{n,1}}{p}, \ldots, \frac{u_{n,m}}{p} \right), \qquad n = 0, \ldots, N-1, \tag{3}$$

where $\{\mathbf{u}_n\}$ is defined by (1).

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 [5, 6].

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 [6, Corollary 3.11], which we present in the following form.

Lemma 1. *Suppose that for the sequence* (2) *there is a real number* B *such that*

$$\left|\sum_{n=0}^{N-1} \exp\left(2\pi i \sum_{j=1}^{s} a_j \gamma_{n,j}\right)\right| \le B,$$

o for any nonzero vector $(a_1, \ldots, a_s) \in \mathbb{Z}^s$ *with* $-M/2 < a_j \le M/2$, $j = 1, \ldots, s$. *Then, the discrepancy* $D_N(\Gamma)$ *of the sequence* (2) *satisfies*

$$D_N(\Gamma) \ll \frac{1}{M} + \frac{B(\log M)^s}{N},$$

where the implied constant depends only on s.

2.2. **Exponential sums and congruences.** For a positive integer r we denote

$$\mathbf{e}_r(z) = \exp(2\pi i z/r), \quad z \in \mathbb{Z}.$$

Notice that for a prime $r = p$, the function $\mathbf{e}_p(z)$ is an additive character of $\mathbb{F}_p$.

Lemma 1 shows the relationship between bounds on exponential sums and bounds on the discrepancy.

We derive bounds of exponential sums with elements of the sequence (3), which imply good distribution properties. Thus, quite naturally, one of our main tools is the following version of the Weil bound from [4]:

Lemma 2. *Let* F/G *be a non-constant univariate rational function over* $\mathbb{F}_p$ *and let* v *be the number of distinct roots of the polynomial* G *in the algebraic closure of* $\mathbb{F}_p$. *Then*

$$\left|\sum_{x\in\mathbb{F}_p}{}^{*} \mathbf{e}_p\left(\frac{F(x)}{G(x)}\right)\right| \le (\max(\deg F, \deg G) + v^* - 2)\ p^{1/2} + \rho,$$

where Σ^* *indicates that the poles of* F/G *are excluded from the summation,* $v^* = v$ *and* $\rho = 1$ *if* $\deg F \le \deg G$, *otherwise* $v^* = v + 1$ *and* $\rho = 0$.

We also need the following technical result [3, Lemma 2]:

Lemma 3. *Let* h *and* q *be positive integers with* $h \ge q^\delta$, *for some fixed* $\delta > 0$. *Then for any set* $\mathcal{K} \subseteq \mathbb{Z}_q^*$ *there exists* $r \in \mathbb{Z}_q^*$, *such that*

$$\#\{(x, y)\ :\ rx \equiv y \pmod q,\ x \in \mathcal{K},\ 0 \le y \le h-1\} \gg \#\mathcal{K}h/q.$$

2.3. **Exponential sums along the trajectories.** We see from Section 2.1 that in order to study the distribution of elements in orbits it is natural to consider the following exponential sums. For a set $\mathcal{I} \subseteq \{1, \ldots, m\}$ of cardinality s and a vector $\mathbf{a} = (a_i)_{i \in \mathcal{I}} \in \mathbb{F}_p^s$ we introduce the exponential sum

$$S_{\mathcal{I}}(\mathbf{a}; N) = \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{i \in \mathcal{I}} a_i u_{n,i} \right). \tag{4}$$

The most common choices of $\mathcal{I}$ are $\mathcal{I} = \{1\}$ (when only the first component of the vector $\mathbf{u}_n$ is studied) and $\mathcal{I} = \{1, \ldots, m\}$ (when the whole vector is studied). Furthermore, in [11, 13, 14] the case $\mathcal{I} = \{1, \ldots, m-1\}$ has been studied as well.

2.4. **Automorphisms.** We recall that a system of m rational functions $\mathcal{A} = \{A_1, \ldots, A_m\}$ in m variables is called a *rational automorphism* in $\mathbb{F}_p(X_1, \ldots, X_m)$ if there exists a system of rational functions $\mathcal{A}^{-1} = \{A_1^{-1}, \ldots, A_m^{-1}\}$ such that for their composition we have $\mathcal{A}^{-1} \circ \mathcal{A} = \{X_1, \ldots, X_m\}$. If all functions involved in $\mathcal{A}$ and $\mathcal{A}^{-1}$ are polynomials we say that $\mathcal{A}$ is a *polynomial automorphism*. Notice that a polynomial automorphism defines a bijection from $\mathbb{F}_p^m$ into itself.

As usual, we say that a monomial $X_1^{e_1} \cdots X_m^{e_m}$ is lexicographic higher than $X_1^{f_1} \cdots X_m^{f_m}$ if for some r we have $e_i = f_i$, $i = 1, \ldots, r-1$ and $e_r > f_r$. For $i = 1, \ldots, m$, let

$$j_i = \min\{j \ : \ f_{i,j} \neq 0, \ j = 1, \ldots, m\}, \tag{5}$$

where $X_1^{f_{i,1}} \ldots X_m^{f_{i,m}}$ is the lexicographically highest monomial of A_i.

The set $\mathcal{I} \subseteq \{1, \ldots, m\}$ with $j_i < m$ for $i \in \mathcal{I}$ is called the *support* of $\mathcal{A}$. We say that the automorphism $\mathcal{A}$ has *degree separation* if the pairs $(f_{i,j_i}, j_i)_{i \in \mathcal{I}}$, are pairwise distinct.

As an example, we introduce the *Henón map* and its inverse (see [1]),

$$\mathcal{H} = \{X_2 + 1 - aX_1^2, bX_1\}, \qquad \mathcal{H}^{-1} = \{b^{-1}X_2, X_1 + ab^{-2}X_2^2 - 1\}, \tag{6}$$

where $b \neq 0$. Following the equation (5), we have that the support of $\mathcal{H}$ is $\mathcal{I} = \{1, 2\}$ and

$$(f_{i,j_i}, j_i)_{i \in \mathcal{I}} = (2, 1), \ (1, 1)$$

so this system has degree separation. For $\mathcal{H}^{-1}$, we have the support $\mathcal{I} = \{2\}$ and

$$(f_{i,j_i}, j_i)_{i \in \mathcal{I}} = (1, 1)$$

so $\mathcal{H}^{-1}$ also has degree separation.

It is easy to check that if we define $\mathcal{G}$ as,

$$\mathcal{G} = \{X_1, X_2 - X_1\}, \qquad \mathcal{G}^{-1} = \{X_1, X_2 + X_1\},$$

then neither $\mathcal{G}$ nor $\mathcal{G}^{-1}$ has degree separation.

3. Algebraic Dynamical Systems with Slow Degree Growth

3.1. **Previous results.** One of our basic building blocks is the following construction from [13, 16]:

$$\begin{aligned} F_1(X_1, \ldots, X_m) &= X_1^{e_{1,1}} G_1(X_2, \ldots, X_m) + H_1(X_2, \ldots, X_m), \\ F_2(X_1, \ldots, X_m) &= X_2^{e_{2,2}} G_2(X_3, \ldots, X_m) + H_2(X_3, \ldots, X_m), \\ &\ldots \\ F_m(X_1, \ldots, X_m) &= g_m X_m^{e_{m,m}} + h_m, \end{aligned} \tag{7}$$

with $e_{1,1}, \ldots, e_{m,m} \in \{-1, 1\}$, $G_i, H_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$, for all $i = 1, \ldots, m-1$, and $g_m, h_m \in \mathbb{F}_p$, $g_m \neq 0$.

Furthermore, we always assume that a system (7) satisfies the following conditions for F_i for any $i = 1, \ldots, m$:

- if $e_{i,i} = 1$, as in [13, 14], we assume that the polynomial G_i has a unique leading monomial $X_{i+1}^{e_{i,i+1}} \ldots X_m^{e_{i,m}}$, that is
$$G_i = g_i X_{i+1}^{e_{i,i+1}} \ldots X_m^{e_{i,m}} + \widetilde{G}_i,$$
where $g_i \in \mathbb{F}_p^*$ and $\widetilde{G}_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$ with
$$\deg_{X_j} \widetilde{G}_i,\ \deg_{X_j} H_i < e_{i,j}, \quad j = i+1, \ldots, m; \tag{8}$$
- if $e_{i,i} = -1$, we assume that the polynomial H_i has a unique leading monomial $X_{i+1}^{e_{i,i+1}} \ldots X_m^{e_{i,m}}$, that is
$$H_i = h_i X_{i+1}^{e_{i,i+1}} \ldots X_m^{e_{i,m}} + \widetilde{H}_i,$$
where $h_i \in \mathbb{F}_p^*$, $\widetilde{H}_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m]$ and
$$\deg_{X_j} \widetilde{H}_i < e_{i,j}, \quad \deg_{X_j} G_i < 2e_{i,j}, \quad j = i+1, \ldots, m. \tag{9}$$

As in [13], we can describe explicitly the iterations of the rational functions F_i as follows. We define

$$\begin{aligned} G_i^{(\ell)}(X_{i+1}, \ldots, X_m) &= G_i\left(F_{i+1}^{(\ell-1)}, \ldots, F_m^{(\ell-1)}\right), \\ H_i^{(\ell)}(X_{i+1}, \ldots, X_m) &= H_i\left(F_{i+1}^{(\ell-1)}, \ldots, F_m^{(\ell-1)}\right). \end{aligned}$$

Lemma 4. *Let $\mathcal{F}$ be defined by* (7) *and satisfying the conditions* (8) *and* (9) *and such that $e_{j,j+1} \neq 0$, $j = 1, \ldots, m-1$. Then the degrees* *of the iterations of* $F_1, \ldots, F_m$ *grow as follows*

$$\deg F_i^{(k)} = \frac{1}{(m-i)!} k^{m-i} e_{i,i+1} \ldots e_{m-1,m} + \psi_i(k), \quad i = 1, \ldots, m-1,$$
$$\deg F_m^{(k)} = 1,$$

where $\psi_i(T)$ *is a polynomial of degree* $\deg \psi_i < m - i$ *with rational coefficients.*

Notice that the Henón map defined in (6) is similar to this class of systems, however, the algebraic entropy for the Henón map is positive.

3.2. **New constructions from automorphisms.** It is conceivable that the triangular shape and linearity of F_i in X_i of the systems (7) can be a weakness from the cryptographic point of view. We now suggest a way to overcome this potential weakness which is based on using rational automorphisms.

Let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be an arbitrary rational automorphism in $\mathbb{F}_p(X_1, \ldots, X_m)$.

We consider systems of the form

$$\mathcal{R} = \{R_1, \ldots, R_m\} = \mathcal{A} \circ \mathcal{F} \circ \mathcal{A}^{-1}, \tag{10}$$

where $\mathcal{F}$ is defined by (7). In particular, we note that

$$R_i = (\mathcal{A} \circ \mathcal{F} \circ \mathcal{A}^{-1})_i = A_i(\mathcal{F} \circ \mathcal{A}^{-1}), \qquad i = 1, \ldots, m.$$

It is easy to see that for every $k = 1, 2, \ldots$ we have

$$R_i^{(k)} = (\mathcal{A} \circ \mathcal{F}^{(k)} \circ \mathcal{A}^{-1})_i = A_i(\mathcal{F}^{(k)} \circ \mathcal{A}^{-1}), \qquad i = 1, \ldots, m.$$

In order to find bounds for the exponential sums with the elements of the sequence (3) we need to study the degree growth (which is immediate) and also the linear independence of iterations of $\mathcal{R}$.

We note that if the sequence $\{\mathbf{u}_n\}$ is entirely generated by iterations of the system $\mathcal{R}$ of the form (10) (that is, the convention $0^{-1} = 0$ has never been applied) then we have

$$\mathbf{u}_n = \mathcal{A}(\mathbf{v}_n), \tag{11}$$

where $\{\mathbf{v}_n\}$ is a sequence generated by the iterations of $\mathcal{F}$, that is,

$$\mathbf{v}_{n+1} = \mathcal{F}(\mathbf{v}_n), \tag{12}$$

starting with initial vector $\mathbf{u}_0 = \mathcal{A}(\mathbf{v}_0)$. In fact in this case $\mathcal{A}$ does not have to be an automorphism. However, keeping in mind potential cryptographic scenarios, where the systems $\mathcal{F}$ and the automorphism $\mathcal{A}$ may not be immediately available or found from $\mathcal{R}$, we consider and study the sequence $\{\mathbf{u}_n\}$ as generated by iterations of $\mathcal{R}$. We mention that most of the proofs can be adjusted (and slightly simplified) to study the distribution of sequences (11). Also, to generate that sequence, repeated applications of $\mathcal{A}^{-1}$ are not necessary, which reduces the time to generate the sequence.

Lemma 5. *Let $\mathcal{A} = \{A_1, \dots, A_m\}$ be an arbitrary polynomial automorphism in $\mathbb{F}_p(X_1, \dots, X_m)$ and let $\mathcal{F}$ be defined by (7), satisfying the conditions (8) and (9), such that $e_{j,j+1} \neq 0$, $j = 1, \dots, m-1$. If $X_1^{f_{i,1}} \dots X_m^{f_{i,m}}$ is the lexicographically highest monomial of A_i, then*

$$\deg\left(A_i \circ \mathcal{F}^{(k)}\right) = \sum_{j=1}^{m} f_{i,j} \left(\frac{1}{(m-j)!} e_{j,j+1} \dots e_{m-1,m} k^{m-j} + O(k^{m-1-j}) \right),$$

for $i = 1, \dots, m$.

Proof. Let $X_1^{l_1} \dots X_m^{l_m}$ be another monomial in A_i, that is,

$$f_{i,1} = l_1, \dots, f_{i,r-1} = l_{r-1} \qquad \text{and} \qquad f_{i,r} > l_r$$

for some $r \leq m$. Then, applying Lemma 4, we obtain

$$\begin{aligned} \sum_{j=1}^{m} f_{i,j} \deg F_j^{(k)} - \sum_{j=1}^{m} l_j \deg F_j^{(k)} &= \sum_{j=r}^{m} (f_{i,j} - l_j) \deg F_j^{(k)} \\ &\geq \deg F_r^{(k)} + O(k^{m-1-r}) \\ &= \frac{1}{(m-r)!} k^{m-r} e_{r,r+1} \dots e_{m-1,m} + O(k^{m-1-r}) > 0, \end{aligned}$$

provided that k is large enough. Thus $\deg A_i(\mathcal{F}^{(k)})$ is equal to the degree that appears in its lexicographically highest monomial after the substitution of $X_1, \dots, X_m$ with $\mathcal{F}^{(k)}$. $\square$

Lemma 5 shows that the system defined in (10) has algebraic entropy 0 and this is independent of $\mathcal{A}$. Also, it satisfies [1, Conjecture 1]. Using this fact, we prove the following bound on the discrepancy of the sequences we generate.

Theorem 6. *Let the sequence $\{\boldsymbol{u}_n\}$ be defined by (1) with the polynomial system (10), where $\mathcal{F}$ is defined by (7) and satisfies the conditions (8) and (9). Let $\mathcal{A}$ be a rational automorphism with the degree separation property and support $\mathcal{I}$ of cardinality $s = \#\mathcal{I}$. If $N \leq T$ where T is the trajectory length of the sequence $\{\boldsymbol{u}_n\}$, then, for any $\nu = 1, 2 \dots$, the discrepancy $D_N((u_{n,i}/p)_{i \in \mathcal{I}})$ satisfies*

$$D_N((u_{n,i}/p)_{i \in \mathcal{I}}) = O\left(p^{\alpha_{m,\nu}} N^{-\beta_{m,\nu}} (\log p)^s\right),$$

where

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

and the implied constant depends only on m, ν and the degrees of $\mathcal{F}$ and $\mathcal{A}$.

Proof. The initial part of the argument is essentially a repetition with some minor modification of the standard approach, see [7, 10, 13], so we suppress some details.

We consider the sum $S_{\mathcal{I}}(\mathbf{a}; N)$ defined by (4) and for a sufficiently large integer $K \geq 1$, we have

$$S_{\mathcal{I}}(\mathbf{a}; N) \ll WK^{-1} + K, \tag{13}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=K}^{2K} \mathbf{e}_p\left(\sum_{i \in \mathcal{I}} a_i u_{n+k,i} \right) \right|.$$

We use the Hölder inequality to obtain

$$\begin{aligned} W^{2\nu} &\leq N^{2\nu-1} \sum_{n=0}^{N-1} \left| \sum_{k=K}^{2K} \mathbf{e}_p\left(\sum_{i \in \mathcal{I}} a_i u_{n+k,i} \right) \right|^{2\nu} \\ &\leq N^{2\nu-1} \sum_{\mathbf{x} \in \mathbb{F}_p^m}{}^{*} \left| \sum_{k=K}^{2K} \mathbf{e}_p\left(\sum_{i \in \mathcal{I}} a_i R_i^{(k)}(\mathbf{x}) \right) \right|^{2\nu} + O(K^{2\nu+1} N^{2\nu-1} p^{m-1}), \end{aligned}$$

since for $N \leq T$ all vectors $\mathbf{u}_n$, $n = 0, \ldots, N-1$, are pairwise distinct (note that the term $O(K^{2\nu+1} N^{2\nu-1} p^{m-1})$ comes from at most sKp^{m-1} values of n for which at least one of the vectors $\mathbf{u}_{n+k}$, $K \leq k \leq 2K$, has been generated via an application of the 'special' convention $0^{-1} = 0$, thus they have at least one zero component).

We now remark that

$$\begin{aligned} W^{2\nu} \leq N^{2\nu-1} &\sum_{k_1, \ell_1, \ldots, k_\nu, \ell_\nu = K}^{2K} \\ &\sum_{\mathbf{x} \in \mathbb{F}_p^m}{}^{*} \mathbf{e}_p\left(\sum_{i \in \mathcal{I}} a_i \sum_{j=1}^{\nu} \left(R_i^{(k_j)}(\mathbf{x}) - R_i^{(\ell_j)}(\mathbf{x}) \right) \right) \\ &\qquad + O(K^{2\nu+1} N^{2\nu-1} p^{m-1}). \end{aligned} \tag{14}$$

Clearly $\mathcal{A}$ induces a permutation of $\mathbb{F}_p^m$. Hence

$$\begin{aligned}
&\sum_{\mathbf{x}\in\mathbb{F}_p^m}{}^{*}\, \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i \sum_{j=1}^{\nu}\left(R_i^{(k_j)}(\mathbf{x}) - R_i^{(\ell_j)}(\mathbf{x})\right)\right)\\
&\quad = \sum_{\mathbf{x}\in\mathbb{F}_p^m}{}^{*}\, \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i \sum_{j=1}^{\nu}\left(A_i\left(\mathcal{F}^{(k_j)}\left(\mathcal{A}^{-1}(\mathbf{x})\right)\right) - A_i\left(\mathcal{F}^{(\ell_j)}\left(\mathcal{A}^{-1}(\mathbf{x})\right)\right)\right)\right)\\
&\quad = \sum_{\mathbf{x}\in\mathbb{F}_p^m}{}^{*}\, \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i \sum_{j=1}^{\nu}\left(A_i\left(\mathcal{F}^{(k_j)}(\mathbf{x})\right) - A_i\left(\mathcal{F}^{(\ell_j)}(\mathbf{x})\right)\right)\right).
\end{aligned}$$

We now study how often the rational function

$$Q_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu} = \sum_{i\in\mathcal{I}} a_i \sum_{j=1}^{\nu}\left(A_i\circ\mathcal{F}^{(k_j)} - A_i\circ\mathcal{F}^{(\ell_j)}\right)$$

in the exponential sum is constant.

Assume that the components of the vectors

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

are not permutations of each other. After making trivial cancellations, without loss of generality we may assume that these two vectors have no common components. Then, Lemma 5 implies that if $\mathbf{a} = (a_i)_{i\in\mathcal{I}} \in \mathbb{F}_p^s$ is a nonzero vector, then $Q_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu}$ is a nontrivial linear combination of terms of degrees

$$\begin{aligned}
&\deg \sum_{j=1}^{\nu}\left(A_i\circ\mathcal{F}^{(k_j)} - A_i\circ\mathcal{F}^{(\ell_j)}\right)\\
&\qquad\qquad = f_{i,j_i}\frac{1}{(m-j_i)!}e_{j_i,j_i+1}\ldots e_{m-1,m}k^{m-j_i} + O(k^{m-1-j_i}),
\end{aligned}$$

where j_i is defined by (5) and

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

Note that, by Lemma 5, for a sufficiently large k these degrees are pairwise distinct (since $\mathcal{A}$ has a separation property) and positive (since $\mathcal{I}$ is the support of $\mathcal{A}$). Thus, we conclude that for $\mathbf{a}\neq\mathbf{0}$, the function $Q_{\mathbf{a},k_1,\ell_1,\ldots,k_\nu,\ell_\nu}$ is a non-constant rational function with respect to at least one variable. We now use Lemma 2 with respect to this variable to estimate the inner sums as $O(K^{m-1}p^{m-1/2})$ for $O(K^{2\nu})$ choices of $k_1,\ell_1,\ldots,k_\nu,\ell_\nu$ and otherwise trivially as $O(p^m)$ for $O(K^\nu)$ choices of

$k_1, \ell_1, \ldots, k_\nu, \ell_\nu$. Noticing that the term $O(K^{2\nu+1}N^{2\nu-1}p^{m-1})$ in (14) never dominates, we derive

$$W^{2\nu} \ll N^{2\nu-1}\left(K^{2\nu+m-1}p^{m-1/2} + K^\nu p^m\right).$$

Inserting this bound in (13) and choosing $K = \left\lceil p^{1/2(m+\nu-1)} \right\rceil$ we obtain

$$S_{\mathcal{I}}(\mathbf{a}; N) \ll p^{\alpha_{m,\nu}} N^{1-\beta_{m,\nu}}.$$

Recalling Lemma 1 we conclude the proof. □

It is easy to see that for any fixed ε and a sufficiently large ν, the bound of Theorem 6 is nontrivial provided that $T \geq N \geq p^{m-1/2+\varepsilon}$.

It is easy to see that the proof of Theorem 6 also works for the sequence $\{\mathbf{u}_n\}$ defined by (11) and (12). In fact it even shortens a little as some transformations become redundant.

In the case when the system $\mathcal{F} = \{F_1, \ldots, F_m\}$ induces a permutation of $\mathbb{F}_p^m$ we can obtain rather strong estimates of the discrepancy "on average" over the initial values. First we need the following estimate (which is also a simple unification of several previously known results, see [8, 11, 14]).

Given a system of rational functions $\mathcal{R} = \{R_1, \ldots, R_m\}$ as in the equation (10), for a vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{F}_p^m$ and integers c, M, N with $M \geq 1$ and $N \geq 1$, we introduce the sums

$$V_{\mathcal{I},\mathbf{a},c}(M, N) = \sum_{v_1,\ldots,v_m \in \mathbb{F}_p} \left| \sum_{n=0}^{N-1} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i R_i^{(n)}(v_1, \ldots, v_m)\right) \mathbf{e}_M(cn) \right|^2,$$

where $\mathcal{I}$ is the support of the automorphism $\mathcal{A}$ in the definition (10).

Lemma 7. *Assume that $\mathcal{F}$ is defined by* (7)*, satisfies the conditions* (8) *and* (9) *and also induces a permutation of $\mathbb{F}_p^m$. Let $\mathcal{A}$ be an automorphism with the degree separation property and with support $\mathcal{I}$ of cardinality $s = \#\mathcal{I}$. Then, for the polynomial system* (10)*, we have*

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

where

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

and the implied constant depends only on m and the degree of $\mathcal{A}$.

Proof. We have

$$\begin{aligned} V_{\mathcal{I},\mathbf{a},c}(M,K) &= \sum_{k,\ell=0}^{K-1} \mathbf{e}_M(c(k-\ell)) \sum_{\mathbf{v}\in\mathbb{F}_p^m} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i \left(R_i^{(k)}(\mathbf{v}) - R_i^{(\ell)}(\mathbf{v})\right)\right) \\ &\le \sum_{k,\ell=0}^{K-1} \left| \sum_{\mathbf{v}\in\mathbb{F}_p^m} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i \left(R_i^{(k)}(\mathbf{v}) - R_i^{(\ell)}(\mathbf{v})\right)\right)\right|. \end{aligned}$$

Thus as in the proof of Theorem 6, using that $\mathcal{A}$ induces a permutation of $\mathbb{F}_p^m$, we obtain

$$V_{\mathcal{I},\mathbf{a},c}(M,K) \le \sum_{k,\ell=0}^{K-1} \left| \sum_{\mathbf{v}\in\mathbb{F}_p^m} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} \left(A_i\left(\mathcal{F}^{(k)}(\mathbf{v})\right) - A_i\left(\mathcal{F}^{(\ell)}(\mathbf{v})\right)\right)\right)\right|.$$

We now use the trivial bound p^m on the inner sum if $k=\ell$ or if $\max\{k,\ell\}$ is not large enough to make the degree argument used in the proof of Theorem 6 work. For the other pairs (k,ℓ) we use Lemma 2. This leads to the bound

$$V_{\mathcal{I},\mathbf{a},c}(M,K) \ll Kp^m + K^{m+1}p^{m-1/2}. \tag{15}$$

For $N > p^{1/2m}$, since $\mathcal{R}$ is also permutation polynomial system on $\mathbb{F}_p^m$, for any integer L we obtain

$$\begin{aligned} &\sum_{\mathbf{v}\in\mathbb{F}_p^m} \left| \sum_{n=L}^{L+K-1} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i R_i^{(n)}(\mathbf{v})\right) \mathbf{e}_M(cn)\right|^2 \\ &\quad = \sum_{\mathbf{v}\in\mathbb{F}_p^m} \left| \sum_{n=0}^{K-1} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i R_i^{(n)}\left(R_1^{(L)}(\mathbf{v}),\ldots,R_m^{(L)}(\mathbf{v})\right)\right) \mathbf{e}_M(cn)\right|^2 \\ &\quad = \sum_{\mathbf{v}\in\mathbb{F}_p^m} \left| \sum_{n=0}^{K-1} \mathbf{e}_p\left(\sum_{i\in\mathcal{I}} a_i R_j^{(n)}(\mathbf{v})\right) \mathbf{e}_M(cn)\right|^2 = V_{\mathcal{I},\mathbf{a},c}(M,K). \end{aligned}$$

Therefore, for any positive integer $K \le N$, separating the inner sum into at most $N/K+1 \le 2N/K$ subsums of length at most K, and using (15), we derive

$$\begin{aligned} V_{\mathcal{I},\mathbf{a},c}(M,N) &\ll (Kp^m + K^{m+1}p^{m-1/2})N^2K^{-2} \\ &= N^2p^m(K^{-1} + K^{m-1}p^{-1/2}). \end{aligned}$$

Thus, selecting $K = \min\{N, \lfloor p^{1/2m}\rfloor\}$ and taking into account that $N^{-1}p^m \ge N^{m-1}p^{m-1/2}$ for $N \le p^{1/2m}$, we obtain the desired result. ☐

Combining Lemmas 1 and 7, we derive exactly as in [8, 11]:

Theorem 8. *Let $0 < \varepsilon < 1$. Assume that $\mathcal{F}$ is defined by (7), satisfies the conditions (8) and (9) and also induces a permutation of $\mathbb{F}_p^m$. Let $\mathcal{A}$ be an automorphism with the degree separation property and with the support $\mathcal{I}$ of cardinality $s = \#\mathcal{I}$. Then for all initial values $\mathbf{u}_0 \in \mathbb{F}_p^m$ except at most $O(\varepsilon p^m)$ of them, and any positive integer $N \le p^m$, the discrepancy $D_N((u_{n,i}/p)_{i\in\mathcal{I}})$ satisfies*

$$D_N((u_{n,i}/p)_{i\in\mathcal{I}}) \ll \varepsilon^{-1} B(N,p),$$

where

$$B(N,p) = \begin{cases} N^{-1/2}(\log N)^m \log p & \text{if } N \le p^{1/2m}, \\ p^{-1/4m}(\log N)^m \log p & \text{if } N > p^{1/2m}. \end{cases}$$

and the implied constant depends only on m, ν and the degrees of $\mathcal{F}$ and $\mathcal{A}$.

As after Theorem 6 we remark that Theorem 8 also applies to the sequence $\{\mathbf{u}_n\}$ defined by (11) and (12).

4. Multivariate Generalisations of the Power Generator

Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ be the polynomial system

$$F_i = (X_i - h_i)^{e_i} G_i + h_i, \qquad i = 1, \ldots, m. \tag{16}$$

where for $i = 1, \ldots, m$ we have

$$e_i \in \mathbb{N} \quad G_i \in \mathbb{F}_p[X_{i+1}, \ldots, X_m] \quad h_i \in \mathbb{F}_p, \tag{17}$$

and for some polynomials G_i that have no zeros over $\mathbb{F}_p$:

$$G_i(x_{i+1}, \ldots, x_m) \ne 0, \qquad x_{i+1}, \ldots, x_m \in \mathbb{F}_p, \tag{18}$$

(in particular $G_m = g_m \in \mathbb{F}_p^*$ is a nonzero constant). Polynomial systems of the form (16) have been introduced and studied in [15].

Here we consider more general systems of polynomials

$$\mathcal{R} = \{R_1, \ldots, R_m\} \in \mathbb{F}_p[X_1, \ldots, X_m],$$

defined by

$$\mathcal{R} = \mathcal{L} \circ \mathcal{F} \circ \mathcal{L}^{-1}, \tag{19}$$

where $\mathcal{F}$ is defined by (16) and

$$\mathcal{L}(\mathbf{X}) = A\mathbf{X}, \tag{20}$$

with $A \in \mathrm{GL}_m(\mathbb{F}_p)$ and $\mathbf{X} = (X_1, \ldots, X_m)$. In particular, we note that

$$R_i = L_i(\mathcal{F} \circ \mathcal{L}^{-1}),$$

where L_i is a linear function corresponding to the ith row of A in (20).

We recall the following result given in [15, Lemma 4], which can easily be shown by induction on k:

Lemma 9. *Let $F_1, \ldots, F_m \in \mathbb{F}_p[X_1, \ldots, X_m]$ be defined by* (16)*. Then, we have*

$$F_i^{(k)} = (X_i - h_i)^{e_i^k} G_{i,k} + h_i$$

where, for $i = 1, \ldots, m$ and $k = 1, 2, \ldots,$ we define

$$G_{i,k} = G_i^{e_i^{k-1}} \left(G_i^{(2)}\right)^{e_i^{k-2}} \cdots G_i^{(k)},$$

with

$$G_i^{(k)} \quad = \quad G_i \left(F_{i+1}^{(k-1)}, \ldots, F_m^{(k-1)}\right).$$

We note that the method of [15, Theorem 2], which works for $m = 1$, does not seem to apply to the more general systems (19) with $m \geq 2$. Hence, the proof of [15, Theorem 8], that applies to the systems (16) is based on different arguments. This same approach also works for the more general systems (19). However, here we use an alternative method to study the distribution of the corresponding sequences. This new method produces nontrivial results only for more restrictive sets of exponents $e_1, \ldots, e_m$, compared to that used in the proof of [15, Theorem 8], but typically leads to stronger bounds.

We note that the proof uses the fact that $m \geq 2$ in a substantial way (allowing us some extra flexibility in the choice of parameters), so the result is not analogous to those known for $m = 1$, see [15, Theorem 2].

For relatively prime integers e and $t \geq 1$ we use $\mathrm{ord}_t e$ to denote the multiplicative order of e modulo t. We are now ready to prove the main result of this section.

Theorem 10. *Let the sequence $\{\boldsymbol{u}_n\}$ be defined by* (1) *with the polynomial system* (19) *with $m \geq 2$ and satisfying* (16)*,* (17) *and* (18)*. Then, for any $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$ with*

$$\gcd(a_1, \ldots, a_m, p) = 1, \quad i = 1, \ldots, m,$$

for $N \leq T$, where T is the trajectory length of the sequence $\{\boldsymbol{u}_n\}$, we have the estimate

$$|S_{\mathbf{a}}(N)| \ll N^{1/2} p^{m/2+1/8} \tau^{-1/4},$$

where

$$\tau = \min\{\mathrm{ord}_{p-1} e_i \ : \ i = 1, \ldots, m\}$$

and the implied constant depends only on m.

Proof. Select any $\mathbf{a} = (a_1, \ldots, a_m)$ satisfying the conditions of the theorem. It is obvious that for any $k \geq 0$, we have

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

For any set of non-negative integers $\mathcal{K}$,

$$\#\mathcal{K}|S_{\mathbf{a}}(N)| \le W + \#\mathcal{K} \max_{k\in\mathcal{K}} k, \tag{21}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k\in\mathcal{K}} \mathbf{e}_p \left(\sum_{j=1}^{m} a_j u_{n+k,j} \right) \right|.$$

We use the Cauchy inequality, as in the proof of Theorem 6 (except that since $e_i \in \mathbb{N}$, $i = 1, \ldots, m$, the 'special' convention $0^{-1} = 0$ is never applied in this case). Hence, we obtain

$$\begin{aligned}
W^2 &\le N \sum_{n=0}^{N-1} \left| \sum_{k\in\mathcal{K}} \mathbf{e}_p \left(\sum_{j=1}^{m} a_j u_{n+k,j} \right) \right|^2 \\
&\le N \sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{x}\in\mathbb{F}_p^m} \mathbf{e}_p \left(\sum_{i=1}^{m} a_i \left(R_i^{(k)}(\mathbf{x}) - R_i^{(\ell)}(\mathbf{x}) \right) \right) \\
&= N \sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{x}\in\mathbb{F}_p^m} \mathbf{e}_p \left(\sum_{i=1}^{m} a_i \left(L_i \left(\mathcal{F}^{(k)}(\mathcal{L}^{-1}(\mathbf{x})) \right) - L_i \left(\mathcal{F}^{(\ell)}(\mathcal{L}^{-1}(\mathbf{x})) \right) \right) \right) \\
&= N \sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{x}\in\mathbb{F}_p^m} \mathbf{e}_p \left(\sum_{i=1}^{m} a_i \left(L_i \left(\mathcal{F}^{(k)}(\mathbf{x}) \right) - L_i \left(\mathcal{F}^{(\ell)}(\mathbf{x}) \right) \right) \right).
\end{aligned}$$

Since $\mathcal{L} \in \mathrm{GL}_m(\mathbb{F}_p)$, we see from Lemma 9 that

$$\begin{aligned}
\sum_{i=1}^{m} & a_i \left(L_i \left(\mathcal{F}^{(k)}(\mathbf{x}) \right) - L_i \left(\mathcal{F}^{(\ell)}(\mathbf{x}) \right) \right) \\
&= \sum_{i=1}^{m} c_i \left(F_i^{(k)}(\mathbf{x}) - F_i^{(\ell)}(\mathbf{x}) \right) \\
&= \sum_{i=1}^{m} c_i \left((x_i - h_i)^{e_i^k} G_{i,k}(\mathbf{x}) - (x_i - h_i)^{e_i^\ell} G_{i,\ell}(\mathbf{x}) \right)
\end{aligned}$$

for some nonzero vector $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{F}_p^m$.

For each vector $\mathbf{x} \in \mathbb{F}_p^m$ we change $x_i - h_i$ to x_i, $i = 1, \ldots, m$, in the inner sum and derive

$$W^2 \le N \sum_{k,\ell\in\mathcal{K}} \left| \sum_{\mathbf{x}\in\mathbb{F}_p^m} \mathbf{e}_p \left(\sum_{i=1}^{m} c_i \left(x_i^{e_i^k} G_{i,k}(\mathbf{x}) - x_i^{e_i^\ell} G_{i,\ell}(\mathbf{x}) \right) \right) \right|.$$

Let j be the smallest subscript with $c_j \neq 0$. Then

$$W^2 \le N \sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{y}\in\mathbb{F}_p^{m-1}} \left| \sum_{x\in\mathbb{F}_p} \mathbf{e}_p\left(c\left(x^{e^k}H_k(\mathbf{y}) - x^{e^\ell}H_\ell(\mathbf{y})\right)\right)\right|, \tag{22}$$

where $c = c_j$, $e = e_j$ and $H_n = G_{j,n}$.

Finally, let

$$t = \mathrm{ord}_{p-1}e_j = \mathrm{ord}_{p-1}e.$$

Taking $\mathcal{S} = \{e^u \pmod{p-1} \ : \ u = 0,\ldots,t-1\} \subseteq \mathbb{Z}_{p-1}$ and for

$$h = \lceil p^{3/4}t^{-1/2}\rceil \ge p^{1/4}$$

we select r as in Lemma 3. Thus $\mathcal{K}$ is the set of $s \in \mathcal{S}$ such that $rs \equiv y \pmod{p-1}$ for some nonnegative integer $y \le h-1$ of cardinality

$$\#\mathcal{K} \gg th/p. \tag{23}$$

We now make the change of variables $x \to x^r$ in the inner sum in (22) and derive

$$\begin{aligned}
&\sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{y}\in\mathbb{F}_p^{m-1}} \left| \sum_{x\in\mathbb{F}_p} \mathbf{e}_p\left(c\left(x^{e^k}H_k(\mathbf{y}) - x^{e^\ell}H_\ell(\mathbf{y})\right)\right)\right| \\
&\qquad = \sum_{k,\ell\in\mathcal{K}} \sum_{\mathbf{y}\in\mathbb{F}_p^{m-1}} \left| \sum_{x\in\mathbb{F}_p} \mathbf{e}_p\left(c\left(x^{h_k}H_k(\mathbf{y}) - x^{h_\ell}H_\ell(\mathbf{y})\right)\right)\right|,
\end{aligned}$$

with some positive integers $h_k, h_\ell \le h$ such that $h_k \neq h_\ell$ if $k \neq \ell$, $k,\ell \in \mathcal{K}$.

For $O(\#\mathcal{K})$ pairs (k,ℓ) with $k = \ell$, we estimate the inner sum in (22) trivially by p^m. For the other $O(\#\mathcal{K}^2)$ cases, we recall that

$$H_k(\mathbf{y})H_\ell(\mathbf{y}) = G_{j,k}(\mathbf{y})G_{j,\ell,}(\mathbf{y}) \neq 0$$

and apply Lemma 2. So we obtain:

$$W^2 = O\left(N\#\mathcal{K}p^m + Nh(\#\mathcal{K})^2p^{m-1/2}\right),$$

which, together with (21) and (23), implies

$$\begin{aligned}
|S_{\mathbf{a}}(N)| &\ll N^{1/2}\left((\#\mathcal{K})^{-1/2}p^{m/2} + h^{1/2}p^{m/2-1/4}\right) + t \\
&\ll N^{1/2}\left((th)^{-1/2}p^{(m+1)/2} + h^{1/2}p^{m/2-1/4}\right) + t.
\end{aligned}$$

Recalling the choice of h we derive

$$|S_{\mathbf{a}}(N)| \ll N^{1/2}p^{m/2+1/8}t^{-1/4} + t. \tag{24}$$

Clearly the bound is trivial if $N \le p^{m+1/4}t^{-1/2}$. On the other hand, for $N > p^{m+1/4}t^{-1/2}$ we have

$$N^{1/2}p^{m/2+1/8}t^{-1/4} \ge p^{m+1/4}t^{-1/2} \ge p^{m-1/4} \ge p \ge t$$

for $m \ge 2$. So the second term can be omitted in (24). Since $t \ge \tau$, the result now follows. □

Using Theorem 10 and Lemma 1, we obtain:

Corollary 11. *The discrepancy $D_N(\mathbf{u}_n/p)$ of the sequence* (3)*, defined by* (1) *with the polynomial system* (19) *satisfying* (16)*,* (17) *and* (18) *for $N \le T$, where T is the trajectory length of the sequence $\{\boldsymbol{u}_n\}$, satisfies*

$$D_N(u_n) \ll N^{-1/2}p^{m/2+1/8}\tau^{-1/4}(\log p)^m,$$

where

$$\tau = \min\{\mathrm{ord}_{p-1} e_i \ : \ i = 1, \ldots, m\}$$

and the implied constant depends only on m.

We note that in the most favourable case, when $N = p^{m+o(1)}$ and $\tau = p^{1+o(1)}$ the bound of Corollary 11 takes the form $O(p^{-1/8+o(1)})$ while the bound of [15, Corollary 9] gives only $O(p^{-3/184+o(1)})$. However, Corollary 11 is nontrivial only for $\tau > p^{1/2+\delta}$ for some fixed $\delta > 0$ which [15, Corollary 9] yields a meaningful estimate for a much wider class of the exponents $e_1, \ldots, e_m$.

Acknowledgment

The authors are very grateful to both referees for the very careful reading of the manuscript and very helpful comments.

During the preparation of this paper, D. G.-P. was supported in part by the Spanish Government Projects MTM2011-24678 and TIN2011-27479-C04-04, A. O. by the Swiss National Science Foundation Grant PA00P2–139679 and I. S. by the Australian Research Council Grant DP1092835.

References

[1] M. Bellon and C.-M. Viallet, 'Algebraic entropy', *Comm. Math. Phys.*, **2004** (1999), 425–437.

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

[3] J. B. Friedlander, J. Hansen and I. E. Shparlinski, 'On character sums with exponential functions', *Mathematika*, **47** (2000), 75–85.

[4] C. J. Moreno and O. Moreno, 'Exponential sums and Goppa codes, 1', *Proc. Amer. Math. Soc.*, **111** (1991), 523–531.

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

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

[7] 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.

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

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

[10] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64.

[11] A. Ostafe, 'Multivariate permutation polynomial systems and nonlinear pseudorandom number generators', *Finite Fields and Their Appl.*, **16** (2010), 144–154.

[12] A. Ostafe, 'Pseudorandom vector sequences of maximal period generated by polynomial dynamical systems', *Designs, Codes and Crypto.*, **63** (2012), 59–72.

[13] 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.

[14] A. Ostafe and I. E. Shparlinski, 'Pseudorandom numbers and hash functions from iterations of multivariate polynomials', *Cryptography and Communications*, **2** (2010), 49–67.

[15] A. Ostafe and I. E. Shparlinski, 'On the power generator of pseudorandom numbers and its multivariate analogue', *J. Complexity*, **28** (2012), 238–249.

[16] A. Ostafe and I. E. Shparlinski, 'Degree growth, linear independence and periods of a class of rational dynamical systems', *Arithmetic, Geometry, Cryptography and Coding Theory 2010*, Contemp. Math., (in press).

[17] A. Ostafe, I. E. Shparlinski and A. Winterhof, 'On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences', *Adv. in Math. of Comm.*, **4** (2010), v.4, 369–379.

[18] I. E. Shparlinski, 'On some dynamical systems in finite fields and residue rings', *Discr. and Cont. Dynam. Syst., Ser.A*, **17** (2007), 901–917.

[19] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2007, 135–166.

[20] T. T. Truong, 'Degree complexity of a family of birational maps. II. Exceptional cases', *Math. Phys. Anal. Geom.*, **12** (2009), 157–180.

[21] C.-M. Viallet, 'Algebraic dynamics and algebraic entropy', *Int. J. Geom. Methods Mod. Phys.*, **5** (2008), 1373–1391.

[22] A. Winterhof, 'Recent results on recursive nonlinear pseudorandom number generators', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **6338** (2010), 113–124.

Department of Mathematics, University of Cantabria, Santander 39005, Spain

E-mail address: domingo.gomez@unican.es

Department of Computing, Macquarie University, Sydney NSW 2109, Australia

E-mail address: alina.ostafe@mq.edu.au

Department of Computing, Macquarie University, Sydney NSW 2109, Australia

E-mail address: igor.shparlinski@mq.edu.au