Iterations of Multivariate Polynomials and Discrepancy of Pseudorandom Numbers

Jaime Gutierrez and Domingo Gomez-Perez

Department of Mathematics and Computing,
Faculty of Science, University of Cantabria,
Santander E–39071, Spain
e-mail:{jaime, domingo}@matesco.unican.es

Abstract. In this paper we present an extension of a result in [2] about a discrepancy bound for sequences of s-tuples of successive nonlinear multiple recursive congruential pseudorandom numbers of higher orders. The key of this note is based on linear properties of the iterations of multivariate polynomials.

1 Introduction

The paper [2] studies the distribution of pseudorandom number generators defined by a recurrence congruence modulo a prime p of the form

$$u_{n+1} \equiv f(u_n, \dots, u_{n-m+1}) \pmod{p}, \qquad n = m-1, m, \dots, \tag{1}$$

with some *initial values* $u_0, \dots, u_{m-1}$, where $f(X_1, \dots, X_m)$ is a polynomial of m variables over the field $\mathbb{F}_p$ of p elements. These nonlinear congruential generators provide a very attractive alternative to linear congruential generators and, especially in the case $m = 1$, have been extensively studied in the literature, see [1] for a survey.

When $m = 1$, for sequences of the largest possible period $t = p$, a number of results about the distribution of the fractions u_n/p in the interval $[0, 1)$ and, more generally, about the distribution of the points

$$\left(\frac{u_n}{p}, \dots, \frac{u_{n+s-1}}{p}\right) \tag{2}$$

in the s-dimensional unit cube $[0, 1)^s$ have been obtained, see the recent series of papers [3, 5–8] for more details. In the paper [2], the same method for nonlinear generators of arbitrary order $m > 1$ is presented. In particular, the paper [2] gives a nontrivial upper bound on exponential sums and the discrepancy of corresponding sequences for polynomials of total degree $d > 1$ which have a *dominating term* (see Theorem 1 and Theorem 2 in that paper). As in [2], we say that a polynomial $f(X_1, \dots, X_m) \in \mathbb{F}_p[X_1, \dots, X_m]$ has a *dominating term* if it is of the form

$$f(X_1, \dots, X_m) = a_{d_1 \dots d_m} X_1^{d_1} \cdots X_m^{d_m} + \sum_{i_1=0}^{d_1-1} \cdots \sum_{i_m=0}^{d_m-1} a_{i_1 \dots i_m} X_1^{i_1} \cdots X_m^{i_m}$$

with some integers $d_1 \geq 1, d_2 \geq 0, \ldots, d_m \geq 0$ and coefficients $a_{i_1 \ldots i_m} \in \mathbb{F}_p$ with $a_{d_1 \ldots d_m} \neq 0$. We denote by $\mathcal{DT}$ the class of polynomials having a dominating term.

In this paper we extend Theorem 1 and Theorem 2 of [2] to a very large class of polynomials, including arbitrary polynomials of degree greater than one with respect to the variable X_m, that is, polynomials f with $\deg_{X_m}(f) > 1$. This question appears in [2] as an important open problem. This note is based on properties about composition of multivariate polynomials which could be of independent interest.

The paper is divided into three sections. In Section 2 we study the behaviour of the polynomials under composition. Then Section 3 we extend the result of [2]. Finally, in Section 4 we pose some open problems.

2 Iterations of Multivariate Polynomials

Let $\mathbb{K}$ be an arbitrary field and let f be a polynomial in $\mathbb{K}[X_1, \ldots, X_m]$. As in the paper [2], we consider, for $k = 1, 2, \ldots$, the sequence of polynomials $f_k(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$ by the recurrence relation

$$f_k(X_1, \ldots, X_m) = f(f_{k-1}(X_1, \ldots, X_m), \ldots, f_{k-m}(X_1, \ldots, X_m)),$$

where $f_k(X_1, \ldots, X_m) = X_{1-k}$, for $k = -m+1, \ldots, 0$.

In this section we will give sufficient conditions for the polynomial f such that the polynomial sequence $f_k, k = -m+1, \ldots,$ is linearly independent. In order to prove this we can suppose, without loss of generality, that $\mathbb{K}$ is an algebraically closed field. A central tool to study this sequence of polynomials is the following ring homomorphism :

$$\phi : \mathbb{K}[X_1, \ldots, X_m] \to \mathbb{K}[X_1, \ldots, X_m]$$

defined as: $\phi(X_1) = f$ and $\phi(X_k) = X_{k-1}$, for $k = 2, \ldots, m$.

Lemma 1. *With the above notations, we have the following:*

- $\phi^j(f_k) = f_{k+j}$, *for* $j > 0$ *and* $k = -m+1, \ldots, 0, 1, 2, \ldots$.
- *The polynomial* f *has degree greater than zero with respect to the variable* X_m *if and only if* ϕ^j *is an injective map, for every* $j \geq 1$. *In particular, the* $\{f_r, f_{r+1}, \ldots, f_{r+m-1}\}$ *are algebraically independent, for all* $r \geq -m+1$.

Proof. The proof of the first part it is trivial by the definition of the rinh homorphism ϕ.

On the other hand, we have that ϕ is injective map if and only if its kernel is trivial, that is, ϕ is injective if and only if

$$\{p \in \mathbb{K}[X_1, \ldots, X_m], \quad \phi(p) = 0\} = \{0\}.$$

If $p \in \mathbb{K}[X_1, \dots, X_m]$, then $\phi(p) = p(f, X_1, \dots, X_{m-1})$; so $p = 0$ if and only if $\{X_{m-1}, \dots, X_1, f\}$ are algebraically independent. If $\deg_{X_m}(f) > 0$ then X_m is algebraically dependent over $\mathbb{K}(f, X_1, \dots, X_{m-1})$. Consequently $\{X_{m-1}, \dots, X_1, f\}$ are algebraically independent over $\mathbb{K}$ if and only if we have $\deg_{X_m}(f) > 0$.

Finally, by the first part, we see that $\phi^{r+m}(X_{m-j}) = f_{r+j}$, for $j = 0, \dots, m-1$. Now, the claim follows by induction on r. □

We say that a multivariate polynomial $f(X_1, \dots, X_m) \in \mathbb{K}[X_1, \dots, X_m]$ is *quasi-linear* in X_m if it is of the form $f = aX_m + g$ where $0 \neq a \in \mathbb{K}$ and $g \in \mathbb{K}[X_1, \dots, X_{m-1}]$. We denote by $\mathcal{NL}$ the class of *non quasi-linear* in X_m polynomials of degree greater than zero with respect to the variable X_m. So, the class $\mathcal{NL}$ is the set of all polynomials except the polynomials which do not depend on X_m and the *quasi-linear* polynomials.

Lemma 2. *Let f be an element of $\mathcal{NL}$. Then any finite family of the polynomials f_k, $k = -m+1, \dots, 0, 1, \dots$, is linearly independent.*

Proof. We prove it by induction on m. For $m = 1$ it is obvious, because the degree is multiplicative with respect to polynomial composition. Now, we assume that $\deg_{X_m}(f) > 0$ and we suppose that we have a nonzero linear combination:

$$a_r f_r + a_{r+1} f_{r+1} + \cdots + a_{r+s} f_{r+s} = 0, \tag{3}$$

where $a_j \in \mathbb{K}$ and $a_r \neq 0$. We claim that $X_m \in \mathcal{I}$, where $\mathcal{I}$ is the ideal in the polynomial ring $\mathbb{K}[X_1, \dots, X_m]$, generated by:

$$\mathcal{I} = (X_1, \dots, X_{m-1}, \bar{f}),$$

with $\bar{f} = f - f(0, \dots, 0)$.

By Lemma 1, ϕ^{r+m-1} is an injective map and

$$\phi^{r+m-1}(f_{-m+1}) = \phi^{r+m-1}(X_m) = f_r.$$

Applying the inverse of ϕ^{r+m-1} to equation (3), we obtain:

$$a_r X_m + a_{r+1} X_{m-1} + \cdots + a_{r+s} f_{s-m+1} = 0. \tag{4}$$

We show that $\bar{f}_t = f_t - f_t^0 \in \mathcal{I}$, where $f_t^0 = f_t(0, \dots, 0)$. By the uniqueness of the classical euclidean division

$$f = (X_1 - f_{t-1}^0) g_1 + r_1(X_2, \dots, X_m)$$

and

$$r_1(X_2, \cdots, X_m) = (X_2 - f_{t-2}^0) g_2 + r_2(X_3, \dots, X_m).$$

Now, by recurrence, we have:

$$f = (X_1 - f_{t-1}^0) g_1 + \cdots + (X_{m-1} - f_{t-m+1}^0) g_{m-1} + (X_m - f_{t-m}^0) g_m + g_0,$$

where $g_i \in \mathbb{K}[X_i, \dots, X_m]$, $i = 0, \dots, m$.

Since, $f_t = f(f_{t-1}, \ldots, f_{t-m})$ we have that $g_0 = f_t^0$. Now, by induction on t, we will show that $\bar{f}_t \in \mathcal{I}$, for $t > 0$. In order to see that, we observe that

$$f_t = f(f_{t-1}, \ldots, f_{t-m})) =$$

$$= \bar{f}_{t-1} g_1(f_{t-1}, \ldots, f_{t-m})) + \cdots + \bar{f}_{t-m} g_m(f_{t-1}, \ldots, f_{t-m})) + g_0.$$

Then, $\bar{f}_t = f_t - g_0 \in \mathcal{I}$.

Using the equation (4), we have:

$$a_r X_m = -a_r^{-1}(a_{r+1} X_{m-1} + \cdots + a_{r+s} f_{s-m+1}).$$

And have just proved that $X_m \in \mathcal{I}$. So, there exist polynomials $w_i \in \mathbb{K}[X_1, \ldots, X_m]$, $i = 1, \ldots, m$, such that

$$X_m = X_1 w_1 + \cdots + X_{m-1} w_{m-1} + \bar{f} w_m,$$

then $X_m = \bar{f}(0, \ldots, 0, X_m) w_m(0, \ldots, 0, X_m)$. As consequence, we can write f as follows:

$$f = X_1 h_1 + \cdots + X_{m-1} h_{m-1} + \alpha X_m + \beta, \quad (5)$$

where $h_i \in \mathbb{K}[X_i, \ldots, X_m]$, $(i = 1, \ldots, m-1)$, $\alpha, \beta \in \mathbb{K}$ and $\alpha \neq 0$. Now, we consider the polynomial

$$H = f(X_1, \ldots, X_{m-1}, Y) - f(X_1, \ldots, X_{m-1}, Z) \in \mathbb{K}[X_1, \ldots, X_{m-1}, Y, Z].$$

We claim there exists a zero $(\alpha_{0,1}, \ldots, \alpha_{0,m-1}, \beta_0, \gamma_0) \in \mathbb{K}^{m+1}$ of the polynomial H, with $\beta_0 \neq \gamma_0$. In order to prove this last claim, we write the polynomial f as univariate polynomial in the variable X_m with coefficients b_j in the polynomial ring $\mathbb{K}[X_1, \ldots, X_{m-1}]$, for $j = 0, \ldots, s$, that is, $f = b_s X_m^s + \cdots + b_1 X_m + b_0$, for $j = 0, \ldots, s$ and $b_s \neq 0$. So,

$$H = b_s(Y^s - Z^s) + \cdots + b_1(Y - Z).$$

If a such zero does not exist, then the zero set of h coincides with the zero set of the polynomial $Y - Z$. Since $Y - Z$ is an irreducible polynomial in $\mathbb{K}[X_1, \ldots, X_{m-1}, Y, Z]$, then by the Nullstellensatz theorem, (see for instance [4]) H is a power of $Y - Z$, i.e., there exists a positive natural number t such that $H = \gamma(Y - Z)^t$, where $0 \neq \gamma \in \mathbb{K}$. We have the following:

$$b_s(Y^s - Z^s) + \cdots + b_1(Y - Z) = \gamma(Y - Z)^t.$$

From this polynomial equality, we obtain that $s = t$. Since $\gamma(Y - Z)^s$ is a homogenous polynomial, then $b_s(Y^s - Z^s) = \gamma(Y - Z)^s$. Now, from (5), we get that $s = 1$ and f must be $b_1 X_m + b_0$, that is, f is a quasi-linear polynomial in X_m. By the assumption $f \in \mathcal{NL}$, this is a contradiction.

Finally, we evaluate the left hand of the polynomial equality (4) in the point $P_0 = (\alpha_{0,1}, \ldots, \alpha_{0,m-1}, \beta_0)$, we obtain:

$$a_r \beta_0 + \ldots + a_{r+m-1} \alpha_{0,1} + a_{r+m} f(P_0) + \cdots + a_{r+s} f_{r+s-m}(P_0) = 0. \quad (6)$$

We also evaluate (4) in the point $Q_0 = (\alpha_{0,1}, \ldots, \alpha_{0,m-1}, \gamma_0)$ and we obtain:

$$a_r\gamma_0 + \cdots + a_{r+m-1}\alpha_{0,1} + a_{r+m}f(Q_0) + \cdots + a_{r+s}f_{r+s-m}(Q_0) = 0. \qquad (7)$$

We observe that $f_k(P_0) = f_k(Q_0)$ for all $k \geq 0$. Thus, subtracting the equation (7) from the equation (6), we get $a_r(\beta_0 - \gamma_0) = 0$. Again, this is a contradiction and, the result follows. □

We can also extend the above result to another class of polynomials. We say that a multivariate polynomial $f(X_1, \ldots, X_m) \in \mathbb{K}[X_1, \ldots, X_m]$ of total degree d, has the *dominating variable* X_1 if it is of the form

$$f = a_d X_1^d + a_{d-1}X_1^{d-1} + \cdots + a_0$$

where $d > 0$ and $a_i \in \mathbb{K}[X_2, \ldots, X_m]$, with $a_d \neq 0$. We denote by $\mathcal{DV}$ the class of polynomials having the dominating variable X_1.

Lemma 3. *With the above notations, for polynomial $f \in \mathcal{DV}$ the total degree of the polynomial f_k is d^k, $k = 1, 2, \ldots$. In particular, if $d > 1$, any finite family of the polynomials f_k, $k = -m+1, \ldots, 0, 1, \ldots$, is linearly independent.*

Proof. We prove this statement by induction on k. For $k = 1$ it is obvious.

Now we assume that $k \geq 2$. We have

$$f_k = a_d f_{k-1}^d + a_{d-1}(f_{k-2}, \ldots, f_{k-(m-1)})f_{k-1}^{d-1} + \cdots + a_0(f_{k-2}, \ldots, f_{k-(m-1)})$$

We remark that for all

$$\deg(a_{d-i}) \leq i, \qquad i = 0, \ldots, d,$$

because $\deg f = d$. Using the induction assumption we obtain

$$\begin{aligned}&\deg(a_{d-i}(f_{k-2}, \ldots, f_{k-(m-1)})f_{k-1}^{d-i}) \\ &= \deg(a_{d-i}(f_{k-2}, \ldots, f_{k-(m-1)})) + \deg(f_{k-1}^{d-i}) \leq id^{k-2} + (d-i)d^{k-1},\end{aligned}$$

for all $i = 1, \ldots, d$. On the other hand

$$\deg(a_d f_{k-1}^d) \geq \deg(f_{k-1}^d) = d^k.$$

Finally, we observe that $d^k > id^{k-2} + (d-i)d^{k-1}$ for all $i = 1, \ldots, d$. □

We have the following corollary:

Corollary 1. *If f is a polynomial in $\mathbb{K}[X_1, X_2]$ of total degree greater than one, then any finite family of the polynomials f_k, $k = -m+1, \ldots, 0, 1, \ldots$, is linearly independent.*

Proof. It is an immediate consequence of Lemmas 2 and 3 □

We observe that any polynomial in the class $\mathcal{NL}$ has total degree greater than one. On the other hand, if f is a linear polynomial, the sequence f_k, $k = 1, \ldots$, is obviously linearly dependent.

The following examples illustrate that we have three different classes of multivariate polynomial in m variables. The polynomial $f = X_1^2 + X_2 X_1$ has dominating variable X_1, that is, $f \in \mathcal{DV}$, but it has not a dominating term, $f \notin \mathcal{DT}$. We also have, that f is not a quasi-linear polynomial in X_2. Conversely, $g = X_1 X_2 + 1 \in \mathcal{DT} \bigcap \mathcal{NL}$, but $f \notin \mathcal{DV}$. Finally, $h = X_1^2 + X_2 \in \mathcal{DT} \bigcap \mathcal{DV}$, but $h \notin \mathcal{NL}$.

3 Discrepancy Bound

We denote by $\mathcal{T}$ the union of the three classes $\mathcal{T} = \mathcal{DV} \bigcup \mathcal{DT} \bigcup \mathcal{NL}$.

Following the proof of Theorem 1 in [2], we note that the only condition that they require is the statement of the above results. So, as a consequence of Lemma 2 and 3 and Corollary 1 we have Theorem 1 and Theorem 2 of [2] for polynomials $f(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_m]$ with $f \in \mathcal{T}$ if $m > 2$ and for any non-linear polynomial f if $m = 2$.

As in the paper [2], let the sequence (u_n) generated by (1) be purely periodic with an arbitrary period $t \leq p^m$. For an integer vector $\mathbf{a} = (a_0, \ldots, a_{s-1}) \in Z^s$, we introduce the exponential sum

$$S_{\mathbf{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{j=0}^{s-1} a_j u_{n+j}\right),$$

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

Theorem 1. *Suppose that the sequence (u_n), given by (1) generated by a polynomial $f(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_m]$ of the total degree $d \geq 2$ is purely periodic with period t and $t \geq N \geq 1$. If $m = 2$ or $f \in \mathcal{T}$, then the bound*

$$\max_{\gcd(a_0, \ldots, a_{s-1}, p) = 1} \mid S_{\mathbf{a}}(N) \mid \ = O\left(N^{1/2} p^{m/2} \log^{-1/2} p\right)$$

holds, where the implied constant depends only on d and s.

As in the paper [2], for a sequence of N points

$$\Gamma = (\gamma_{1,n}, \ldots, \gamma_{s,n})_{n=1}^{N}$$

of the half-open interval $[0, 1)^s$, denote by Δ_Γ its discrepancy, that is,

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

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

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

and the supremun is taken over all such boxes.

Let $D_s(N)$ denote the discrepancy of the points (2) for $n = 0, \ldots, N-1$.

Theorem 2. *Suppose that the sequence (u_n), given by (1) generated by a polynomial $f(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_m]$ of the total degree $d \geq 2$ is purely periodic with period t and $t \geq N \geq 1$. If $m = 2$ or $f \in \mathcal{T}$, then the bound*

$$D_s(N) = O\left(N^{1/2} p^{m/2} \log^{-1/2} p (\log\log p)^s\right)$$

holds, where the implied constant depends only on d and s.

In particular, Theorems 1 and 2 apply to any *non-linear* with respect to X_1 polynomial. Thus these are direct generalizations of the results of [5].

4 Remarks

We have extended the results of [2] to a very large class of polynomials, including multivariate polynomials f such that $\deg_{X_m}(f) > 1$. The only remain open problem is for a subclass of polynomials of the form $g(X_1, \ldots, X_{m-1}) + aX_m$, where $a \in \mathbb{K}^{\times}$.

On the other hand, it would be very interesting to extend these results to the case of generators defined by a list of m polynomials of $\mathbb{F}_p[X_1, \ldots, X_m]$:

$$\mathbf{F} = (f_1(X_1, \ldots, X_m), \ldots, f_m((X_1, \ldots, X_m))$$

For each $i = 1, \ldots, m$ we define the sequence of polynomials $f_i^{(k)}(X_1, \ldots, X_m) \in \mathbb{F}_p[X_1, \ldots, X_m]$ by the recurrence relation

$$f_i^{(0)} = f_i, \quad f_i^{(k)}(X_1, \ldots, X_m) = f_i^{(k-1)}(f_1, \ldots, f_m), \qquad k = 0, 1, \ldots .$$

So, for very k, we have the following list of m multivariate polynomials:

$$\mathbf{F^k} = (f_1^k(X_1, \ldots, X_m), \ldots, f_m^k(X_1, \ldots, X_m)).$$

Now, the question is for what general families of polynomials $\mathbf{F}$, for any two numbers r and s with $0 \leq r < s$ the polynomials $f_i^r - f_i^s$, $i = 1, ..., m$, are linearly independent.

Acknowledgments

This research is partially supported by the National Spanish project PB97-0346.

References

1. J. Eichenauer-Herrmann, E. Herrmann and S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, Lect. Notes in Statistics, Springer-Verlag, Berlin, **127** (1998), 66–97.
2. F. Griffin, H. Niederreiter and I. Shparlinski, *On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders,* Proc. the 13th Symp. on Appl. Algebra, Algebraic Algorithms, and Error-Correcting Codes, Hawaii, 1999, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 1999, **1719** , 87–93.

3. J. Gutierrez, H. Niederreiter and I. Shparlinski, *On the multidimensional distribution of nonlinear congruential pseudorandom numbers in parts of the period,* Monatsh. Math., **129**, (2000) 31–36.
4. M. Nagata, *Theory of commutative fields,* Translations of Mathematical Monograph, vol. **125**, Amer. Math. Soc., Providence, R.IU., 1993.
5. H. Niederreiter and I. Shparlinski, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers,* Finite Fields and Their Applications, **5** (1999), 246–253.
6. H. Niederreiter and I. Shparlinski, *On the distribution of inversive congruential pseudorandom numbers modulo a prime power*, Acta Arithm., **92**, (2000), 89–98.
7. H. Niederreiter and I. Shparlinski, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra in Engin., Commun. and Computing, **10**, (2000) 189–202.
8. H. Niederreiter and I. E. Shparlinski, 'On the distribution of inversive congruential pseudorandom numbers in parts of the period', *Math. Comp.* (to appear).