On the Carlitz rank of permutations of $\mathbb{F}_q$ and pseudorandom sequences

Domingo Gómez-Pérez[a], Alina Ostafe[b], Alev Topuzoğlu[c,*]

[a]*Faculty of Science, University of Cantabria, E-39071 Santander, Spain*
[b]*School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia*
[c]*Sabanci University, MDBF, Orhanli 34956 Tuzla, Istanbul, Turkey, Tel:+90 2164839500*

Abstract

L. Carlitz proved that any permutation polynomial f over a finite field $\mathbb{F}_q$ is a composition of linear polynomials and inversions. Accordingly, the minimum number of inversions needed to obtain f is defined to be the Carlitz rank of f by Aksoy et al. The relation of the Carlitz rank of f to other invariants of the polynomial is of interest. Here we give a new lower bound for the Carlitz rank of f in terms of the number of nonzero coefficients of f which holds over any finite field. We also show that this complexity measure can be used to study classes of permutations with uniformly distributed orbits, which, for simplicity, we consider only over prime fields. This new approach enables us to analyze the properties of sequences generated by a large class of permutations of $\mathbb{F}_p$, with the advantage that our bounds for the discrepancy and linear complexity depend on the Carlitz rank, not on the degree. Hence, the problem of the degree growth under iterations, which is the main drawback in all previous approaches, can be avoided.

Keywords: Permutation polynomials over finite fields, Carlitz rank, Pseudorandom number generators
2010 MSC: 11T06, 11K38, 12Y05

*Corresponding Author
Email addresses: domingo.gomez@unican.es (Domingo Gómez-Pérez), alina.ostafe@unsw.edu.au (Alina Ostafe), alev@sabanciuniv.edu (Alev Topuzoğlu)

1. Introduction and Preliminaries

Let $\mathbb{F}_q$ be the finite field with $q = p^s$ elements for a prime p and $s \geq 1$. As usual, $\mathbb{F}_q^*$ denotes the set of nonzero elements. It is well known that any self map f of $\mathbb{F}_q$ can be represented uniquely by a polynomial $f \in \mathbb{F}_q[X]$ of degree less than q.

A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if it induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$, that is, if all elements $f(a)$, $a \in \mathbb{F}_q$, are distinct. See [17] for a detailed exposition of permutation polynomials of $\mathbb{F}_q$.

Carlitz [5] proved the following classical result:

Lemma 1. *For $q > 2$, all permutation polynomials over $\mathbb{F}_q$ can be generated by the following two classes of permutation polynomials,*

$$aX + b, \quad a, b \in \mathbb{F}_q,\ a \neq 0,\ \textit{and}\ X^{q-2}.$$

Thus, by Lemma 1, every permutation polynomial of $\mathbb{F}_q$ can be represented by

$$P_k(X) = \Big(\ldots\big((a_0X + a_1)^{q-2} + a_2\big)^{q-2} + \ldots + a_k\Big)^{q-2} + a_{k+1}, \quad k \geq 0,$$

where $a_1, a_{k+1} \in \mathbb{F}_q$, $a_i \in \mathbb{F}_q^*$, $i = 0, 2, \ldots, k$. See [7] for more details. We denote by $\deg f$ the degree of a permutation f seen as a polynomial over $\mathbb{F}_q$.

The authors of [1] define the *Carlitz rank* of a permutation polynomial f over $\mathbb{F}_q$ to be the smallest positive integer k satisfying $f = P_k$ for a permutation P_k of the above form, and denote it by $Crk(f)$. In other words, $Crk(f) = k$ if f is a composition of at least k inversions X^{q-2} and k (or $k + 1$) linear polynomials.

Various problems concerning this complexity measure are tackled in [1, 7, 8]. For instance, the cycle structure of polynomials of a given Carlitz rank, the enumeration of polynomials with small Carlitz rank and of particular cycle structure, or of permutations of a fixed Carlitz rank are studied.

The relation between invariants of a polynomial f and $Crk(f)$ are of interest. A lower bound for $Crk(f)$ in terms of the degree of f, $\deg f$, can be found in [1], which shows that polynomials of small degree have large Carlitz rank. Here we give a similar bound in terms of the weight of f, i.e., the number of nonzero coefficients, which we denote by $\omega(f)$. Our bound is better than the one concerning $\deg f$, when $\deg f \geq q - q/(\omega(f) + 2)$.

The classification of permutations with respect to their Carlitz ranks has already found applications, see [8] for instance. A potential utilization in symmetric cryptography is mentioned in Section 2.

In this work we shall focus on another application, namely on studying the distribution of elements in orbits of permutation polynomials, and in particular on the analysis of pseudorandom sequences. Let f be a permutation of $\mathbb{F}_p$, and consider the sequence $\{u_n\}_{n\geq 0}$ generated by the recurrence relation

$$u_{n+1} = f(u_n), \quad n = 0, 1, \ldots, \tag{1}$$

where $u_0 \in \mathbb{F}_p$ is a random value, called the seed. Equivalently, one can define $\{u_n\}$ by $u_{n+l} = f^{(l)}(u_n)$, where

$$f^{(l+1)}(X) = f^{(l)}(f(X)), \quad f^{(0)}(X) = X, \quad l = 0, 1, \ldots.$$

In the special case of linear polynomials over a residue ring or a finite field, such iterations have been in use for decades.

When $\deg f \geq 2$, one talks about nonlinear generators. We refer the reader to the monograph [20], and recent surveys [24, 28, 29] for a detailed analysis of randomness of widely-used sequences in the context of pseudorandom number generators.

We note that sequences generated by permutations with Carlitz rank zero are well-known to be unfavorable for many applications, in particular for use in cryptography, see for example [9, 15, 16]. We therefore assume $Crk(f) \geq 1$ ($\deg f \geq 2$) for f in (1).

One should note that nonlinear generators are also vulnerable against attacks [3, 4, 11, 12] but these attacks are not strong enough to rule out their use for cryptographic purposes (provided reasonable precautions are made).

Here we focus on two important measures: the distribution of the sequences (1) and their predictability. The first is particularly relevant for applications in simulations and the latter in cryptography. The tools we use, namely discrepancy and linear complexity (profile) have been widely studied for pseudorandom sequences, see [21, 24, 25, 28], and references therein.

Although "good" upper bounds are available for the discrepancy of sequences defined by some special classes of polynomials, results concerning sequences using arbitrary nonlinear f in (1) are not only weak, but also nontrivial only when the sequences have extremely large periods, a property difficult to achieve in practice. This is because, under iterations, the degree of nonlinear polynomials or rational functions grows exponentially in the

number of iterates, and thus, the saving over the trivial discrepancy bound has been only logarithmic.

One can avoid this problem for large classes of permutations, since a permutation can essentially be approximated by a fractional linear transformation in case its Carlitz rank is small relative to the field size. Indeed, our new approach of using the Carlitz rank enables us to obtain nontrivial estimates with a saving of a power of the field size. Moreover, methods of constructing polynomials of any Carlitz rank, yielding sequences with maximum possible period p are available, see Remark 2 below.

We note that the use of sequences generated by permutation polynomials of a given Carlitz rank k as pseudorandom sequences is particularly interesting for certain choices of k. For fixed k and sufficiently large p, the trajectory is obtained by gluing at most k trajectories of inversive generators, hence one can obtain randomness properties from those of the inversive generator, see [23]. For $k = p^{\varepsilon}$ for some $\varepsilon > 0$, generating such sequences does not seem to be possible in polynomial time, thus these generators are not feasible for such applications. However, if $k = (\log p)^c$, for some $c > 0$, then one can generate the sequence in polynomial time and the result of Theorem 8 will give a stronger bound for the discrepancy than the one obtained by gluing trajectories of inversive generators together.

We remark that our study of sequences generated by permutations of a given Carlitz rank yields a large class of permutations with uniformly distributed orbits, which are described in a natural way. Hence, most of this work is of independent interest also, regardless of its applications concerning pseudorandom sequences.

The following lemma is the main tool of our approach and results.

Lemma 2. *Let f be a permutation of $\mathbb{F}_q$, represented as*

$$f(X) = P_k(X) = \Big(\ldots\big((a_0X + a_1)^{q-2} + a_2\big)^{q-2} + \ldots + a_k\Big)^{q-2} + a_{k+1},$$

for some $k \geq 0$. Put

$$R_k(X) = \frac{\alpha_{k+1}X + \beta_{k+1}}{\alpha_k X + \beta_k}, \tag{2}$$

where

$$\alpha_n = a_n\alpha_{n-1} + \alpha_{n-2} \quad \text{and} \quad \beta_n = a_n\beta_{n-1} + \beta_{n-2}, \tag{3}$$

for $n \geq 2$ and $\alpha_0 = 0, \alpha_1 = a_0, \beta_0 = 1, \beta_1 = a_1$.

Then $f(u) = R_k(u)$ for all $u \in \mathcal{K}$, where $\mathcal{K}$ is a subset of $\mathbb{F}_q$ of cardinality at least $q - k$.

The proof of Lemma 2 can be found in [7].

Remark 1. *For any representation P_k of a permutation f, the elements $\alpha_n, \alpha_{n+1}, \beta_n, \beta_{n+1}$ in the above lemma satisfy $\alpha_{n+1}\beta_n - \alpha_n\beta_{n+1} \neq 0$. The string $\mathbf{O}_k = \{X_i : X_i = \frac{-\beta_i}{\alpha_i}, i = 1, \ldots, k\} \subset \mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ is naturally called the string of poles. With this notation, $\mathcal{K} = \mathbb{F}_q \setminus \mathbf{O}_k$. Note that R_k is linear when the pole X_k is at infinity or $\alpha_k = 0$. Any three consecutive elements of $\mathbf{O}_k$ are distinct, and if $Crk(f) = 1$ or 2, the corresponding fractional transformations R_1, R_2 are not linear. For further details we refer to [7, 27].*

The rest of the paper is structured as follows. Section 2 gives a new bound for the Carlitz rank of a permutation polynomial in terms of its weight, and briefly discusses the range of applicability of this result. In Section 3 we study the distribution of sequences defined by (1) by estimating exponential sums and thus obtaining an upper bound for the discrepancy, based on the Carlitz rank of f. We conclude the paper with lower bounds for the linear complexity profile of sequences (1).

2. Carlitz rank and weight of a polynomial

In this section we give a lower bound for the Carlitz rank of a permutation polynomial f, which depends on $\omega(f)$, the number of its nonzero coefficients. Before presenting our bound, we start by stating a result relating $\omega(f)$ to the number of zeros of f. This lemma and its proof can be found in [26, Lemma 2.5].

Lemma 3. *Let $f \in \mathbb{F}_q[X]$ be a nonzero polynomial of degree at most $q - 2$ with N zeros in $\mathbb{F}_q^*$. Then, we have*

$$\omega(f) \geq \frac{q-1}{q-1-N}.$$

We recall that if f is a permutation polynomial, then $\deg f \leq q-2$, see [2, Theorem 11]. Now, we present the main result of this section.

Theorem 4. *Let $f \in \mathbb{F}_q[X]$ be a permutation polynomial,* $\deg f \geq 2$,

$$f(X) = \sum_{i=1}^{\omega(f)} a_i X^{e_i}, \quad \textit{and} \quad f(X) \neq c_1 + c_2 X^{q-2},$$

for $c_1, c_2 \in \mathbb{F}_q,\ c_2 \neq 0$. Then,

$$Crk(f) > \frac{q}{\omega(f)+2} - 1.$$

Proof. Put $Crk(f) = k$. By Lemma 2 there exists a non-constant rational function R_k defined by (2), satisfying $f(u) = R_k(u)$ for $u \in \mathcal{K}$, where $\mathcal{K}$ is a subset of $\mathbb{F}_q$ of cardinality at least $q - k$.

We first assume that $R_k(X)$ is not a linear polynomial, hence there exist $b_1, b_2, b_3, b_4 \in \mathbb{F}_q,\ b_3 \neq 0$ such that

$$f(u) = b_1 + \frac{b_2}{b_3 u + b_4}, \quad u \in \mathcal{K}.$$

We divide the proof of this case into two parts depending on b_4 being zero or not. If $b_4 \neq 0$, for $\alpha u \in \mathcal{K}$, $b_3 \alpha u + b_4 \neq 0$, we have

$$\sum_{i=1}^{\omega(f)} a_i (\alpha u)^{e_i} = \sum_{i=1}^{\omega(f)} a_i \alpha^{e_i} u^{e_i} = b_1 + \frac{b_2}{\alpha b_3 u + b_4},$$

where for the rest of the proof we put $\omega = \omega(f)$. We can now select $\omega + 1$ different values $\alpha_1, \ldots, \alpha_{\omega+1} \in \mathbb{F}_q$ such that

$$a_1 \alpha_i^{e_1} u^{e_1} + \cdots + a_\omega \alpha_i^{e_\omega} u^{e_\omega} = b_1 + \frac{b_2}{\alpha_i b_3 u + b_4}, \quad i = 1, \ldots, \omega + 1,$$

for at least $q - k(\omega + 1)$ different values of u. Let the vectors $\vec{v}_1, \ldots, \vec{v}_{\omega+1}$ be defined by

$$\vec{v}_i = (a_1 \alpha_i^{e_1}, \ldots, a_\omega \alpha_i^{e_\omega}), \quad i = 1, \ldots, \omega + 1.$$

Since these $\omega + 1$ vectors are in $\mathbb{F}_q^\omega$, they are linearly dependent, hence there are $c_1, \ldots, c_{\omega+1}$ in $\mathbb{F}_q$, not all zero, satisfying

$$c_1 \left(b_1 + \frac{b_2}{\alpha_1 b_3 u + b_4} \right) + \ldots + c_{\omega+1} \left(b_1 + \frac{b_2}{\alpha_{\omega+1} b_3 u + b_4} \right) = 0.$$

Equivalently, the polynomial

$$F(X) = b_1(c_1 + \ldots + c_{\omega+1}) \prod_{i=1}^{\omega+1} (\alpha_i b_3 X + b_4) + b_2 \sum_{i=1}^{\omega+1} c_i \prod_{j=1, j\neq i}^{\omega+1} (\alpha_j b_3 X + b_4)$$

has at least $q - k(\omega + 1)$ zeros. On the other hand, if w. l. o. g. $\alpha_1 c_1 \neq 0$,

$$F(-b_4(\alpha_1 b_3)^{-1}) = c_1 b_2 \prod_{j=2}^{\omega+1} (b_4(1 - \alpha_j \alpha_1^{-1})) \neq 0,$$

hence F is not the zero polynomial. Note that we can suppose that $\alpha_1 c_1 \neq 0$ because the values $\alpha_1, \ldots, \alpha_{\omega+1}$ are distinct and at least two of $c_1, \ldots, c_{\omega+1}$ must be nonzero.

Summing up, we get

$$\omega + 1 \geq \deg F \geq q - k(\omega + 1),$$

which implies the desired result.

If $b_4 = 0$, we have

$$\sum_{i=1}^{\omega} a_i u^{e_i} - b_1 - b_2 b_3^{q-2} u^{q-2} = 0, \quad \text{for } u \in \mathcal{K}.$$

Note that the number of nonzero coefficients of $f(X) - b_1 - b_2 b_3^{q-2} X^{q-2}$ is at most $\omega + 2$, it is not the zero polynomial and the number of elements in $\mathcal{K}$ is at least $q - k$. Now, we study two different cases:

- If $0 \notin \mathcal{K}$, then using Lemma 3, we get the result.
- If $0 \in \mathcal{K}$, then $f(0) = b_1$, so $f(X) - b_1$ is a permutation polynomial of weight $\omega - 1$ and its Carlitz rank is the same as the Carlitz rank of $f(X)$. Applying Lemma 3, we get the result.

The case $f(u) = au + b, u \in \mathcal{K}$, follows by the same argument. □

This bound shows that the complexity of permutations with respect to weight and Carlitz rank do not match, i. e. permutations with low weight have large Carlitz rank and those with small Carlitz rank have large weight. Our result is particularly interesting for permutations f such that $Crk(f) = k$

is small and the corresponding R_k is linear. Such polynomials are linear except for very few elements in $\mathbb{F}_q$, but have many nonzero coefficients.

We remark that the bound is tight for permutations of the form $P_1(X) = (a_0X + a_1)^{q-2} - a_1^{q-2}$,with $a_0, a_1 \in \mathbb{F}_q^*$. Then we obtain $Crk(P_1) = 1 > 0$.

We also note that a lower bound for the Carlitz rank in terms of the degree of f was given in [1, Theorem 4]: $Crk(f) \geq q - \deg f - 1$. Our bound is better when $q \leq q/(\omega(f) + 2) + \deg f$.

A recent result in [8] shows that permutations with small Carlitz rank have low differential uniformity. Hence, such permutations can have potential use in symmetric cryptography, since they are easy to implement, although they have large degree and many nonzero coefficients.

3. Exponential sums and discrepancy

In this and next sections we analyze pseudorandom sequences $\{u_n\}$, $n \geq 1$, generated by (1), where $f \in \mathbb{F}_p[X]$ is a permutation polynomial with $\deg f \geq 2$, and of Carlitz rank $k \geq 1$. For simplicity we restrict ourselves to sequences over the prime field $\mathbb{F}_p$. As usual, we identify $\mathbb{F}_p$ by the set $\{0, \ldots, p-1\}$. Obviously the sequence $\{u_n\}$ is eventually periodic, and we assume it to be purely periodic.

This section focuses on finding an upper bound for the discrepancy of the sequence

$$\left\{ \left(\frac{u_{n+1}}{p}, \ldots, \frac{u_{n+m}}{p} \right) \in [0,1)^m, \ n = 0, \ldots, N-1 \right\}. \tag{4}$$

Before presenting the main results of this section, we introduce some notation and terminology. We will extensively use the symbols $A = O(B)$ and $A \ll B$, which are equivalent to $|A| \leq c|B|$ for some positive constant c. Unless it is explicitly specified, this constant is absolute.

Let Γ be a sequence of N points

$$\Gamma = \left\{ (\gamma_{n,1}, \ldots, \gamma_{n,m})_{n=0}^{N-1} \right\} \tag{5}$$

in the m-dimensional unit cube $[0,1)^m$. The *discrepancy* $\Delta_N(\Gamma)$ is defined as

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

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

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

$|B|$ represents the volume of the box B, and the supremum is taken over all such boxes, see [10].

The law of the iterated logarithm asserts that the order of magnitude of the discrepancy of N independent and uniformly distributed random points in $[0, 1)^m$ should be around $N^{-1/2}$, up to some power of $\log N$. Accordingly, for a given sequence in $[0, 1)$, one investigates the discrepancy of m-tuples of its consecutive terms, see [20].

Typically, the bounds for the discrepancy of sequences are derived from bounds of exponential sums. The relation is made explicit in the celebrated *Koksma–Szüsz inequality*, see [20, Corollary 3.11], which we present in the following form. Before stating the lemma, we introduce the following notation,

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

Lemma 5. *Suppose that the sequence* (5) *consists of points with rational coordinates, which have common denominator p, and that there is a real number B such that*

$$\left| \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{j=1}^{m} a_j \gamma_{n,j} \right) \right| \leq B,$$

for any nonzero vector $(a_1, \ldots, a_m) \in \mathbb{Z}^m$ with $-p/2 < a_j \leq p/2$, $j = 1, \ldots, m$. Then, the discrepancy $\Delta(\Gamma)$ of the sequence (5) *satisfies*

$$\Delta_N(\Gamma) \ll \frac{1}{p} + \frac{B(\log p)^m}{N},$$

where the implied constant depends only on m.

We now study exponential sums involving the sequence $\{u_n\}$ defined by (1), assuming it is purely periodic with an arbitrary period T. For a positive integer $N \leq T$ and a vector $\vec{a} = (a_1, \ldots, a_m) \in \mathbb{Z}^m$, we introduce the exponential sum

$$S_{\vec{a}}(N) = \sum_{n=0}^{N-1} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n+i} \right). \tag{6}$$

Our second tool is the Bombieri-Weil bound for exponential sums involving rational functions, which we present in the improved form given in [18].

Lemma 6. *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*

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

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 $\rho = 0$.

Now, we are ready to estimate the exponential sum defined in (6).

Theorem 7. *Let $\{u_n\}$ be the sequence defined by (1) with $Crk(f) = k$. Suppose that $\{u_n\}$ is purely periodic with period T and that f has a representation P_k such that α_k in (2) is not zero. Then, for any $\vec{a} = (a_1, \dots, a_m) \in \mathbb{Z}^m$, with $\gcd(a_1, \dots, a_m, p) = 1$, and any integers $\nu \ge 1$ and $1 \le N \le T$, we have*

$$S_{\vec{a}}(N) \ll \left(k^{1/2(\nu+1)}p^{1/2\nu(\nu+1)} + p^{1/4\nu}\right) N^{1-1/2\nu},$$

The implied constant depends on m and ν.

Proof. Since $Crk(f) = k$, Lemma 2 implies that there exists a rational function R_k defined by (2), satisfying $f(u) = R_k(u)$ for $u \in \mathcal{K}$, where $\mathcal{K}$ is a subset of $\mathbb{F}_p$ of cardinality at least $p-k$. Since $\alpha_k \neq 0$, the rational function R_k is not a linear polynomial. Then there exist $b_1, b_2, b_3, b_4 \in \mathbb{F}_p,\ b_2b_3 - b_1b_4 \neq 0,\ b_3 \neq 0$ such that

$$f(u) = \frac{b_1u + b_2}{b_3u + b_4}, \quad u \in \mathcal{K}.$$

Moreover, at the l-th iteration we have,

$$f^{(l)}(u) = \frac{\ell_{1,l}(u)}{\ell_{2,l}(u)}, \tag{7}$$

where $\ell_{1,l}, \ell_{2,l}$ are linear polynomials with $u \in \mathcal{K}_l$ and $\mathcal{K}_l$ a subset of $\mathbb{F}_p$ of cardinality at least $p - lk$.

We may also define a sequence of rational functions $R^{(l)}$, as follows

$$R^{(1)}(X) = \frac{b_1X + b_2}{b_3X + b_4}, \quad R^{(l+1)}(X) = R^{(l)}(R^{(1)}(X)),$$

for $l = 1, \ldots$. Hence the equation (7) can be rewritten as,

$$f^{(l)}(u) = R^{(l)}(u), \quad \text{for } u \in \mathcal{K}_l. \tag{8}$$

From this point, the proof is similar to the one in [23, Theorem 1] so we omit some details. For a sufficiently large integer $T \geq L \geq 1$, we have

$$S_{\vec{a}}(N) \ll WL^{-1} + L, \tag{9}$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{l=0}^{L} \mathbf{e}\left(\sum_{i=1}^{m} a_i u_{n+l+i} \right) \right| = \sum_{n=0}^{N-1} \left| \sum_{l=0}^{L} \mathbf{e}\left(\sum_{i=1}^{m} a_i f^{(l+i)}(u_n) \right) \right|.$$

By the Hölder inequality we obtain,

$$W^{2\nu} \leq N^{2\nu-1} \sum_{n=0}^{N-1} \left| \sum_{l=0}^{L} \mathbf{e}\left(\sum_{i=1}^{m} a_i f^{(l+i)}(u_n) \right) \right|^{2\nu}$$
$$\leq N^{2\nu-1} \sum_{x \in \mathbb{F}_p} \sum_{l_1,\ldots,l_{2\nu}=0}^{L} \mathbf{e}\left(\sum_{i=1}^{m} a_i \left(f_{l_1,\ldots,l_{2\nu}}(f^{(i)}(x)) \right) \right),$$

where

$$f_{l_1,\ldots,l_{2\nu}}(X) = f^{(l_1)}(X) + \ldots + f^{(l_\nu)}(X) - f^{(l_{\nu+1})}(X) - \ldots - f^{(l_{2\nu})}(X).$$

If $\{l_1, \ldots, l_\nu\} = \{l_{\nu+1}, \ldots, l_{2\nu}\}$ as multisets, then $f_{l_1,\ldots,l_{2\nu}}$ is constant and the inner sum is trivially equal to p.

Since (8) holds for all but $O(kL)$ elements $x \in \mathbb{F}_p$, we get

$$\frac{W^{2\nu}}{N^{2\nu-1}} \ll L^\nu p + kL^{2\nu+1} + \sum_{l_1,\ldots,l_{2\nu}=0}^{L} {\sum_{x \in \mathbb{F}_p}}^{*} \mathbf{e}\left(\sum_{i=1}^{m} a_i \left(R_{l_1,\ldots,l_{2\nu}}(R^{(i)}(x)) \right) \right),$$

where Σ^* indicates that the poles are excluded from the summation,

$$R_{l_1,\ldots,l_{2\nu}}(X) = R^{(l_1)}(X) + \ldots + R^{(l_\nu)}(X) - R^{(l_{\nu+1})}(X) - \ldots - R^{(l_{2\nu})}(X), \tag{10}$$

with $l_1, \ldots, l_{2\nu}$ ranging over all $\{l_1, \ldots, l_\nu\} \neq \{l_{\nu+1}, \ldots, l_{2\nu}\}$. We note that, by [22, Lemma 2], $R^{(t)}$ has different poles for $1 \leq t \leq T$, and thus $R_{l_1,\ldots,l_{2\nu}}$

is a nonconstant rational function. Indeed, if $R_{l_1,\ldots,l_{2\nu}}(X) = c \in \mathbb{F}_q$, then eliminating the linear denominators in (10) and applying the obtained polynomial equation in one of the poles of any of R_{l_i} for some $i = 1, \ldots, 2\nu$, we immediately get a contradiction with the fact that $R^{(t)}$ has different poles for $1 \le t \le T$.

Now, applying Lemma 6, we get

$$W^{2\nu} \ll (kL^{2\nu+1} + L^{2\nu}p^{1/2} + L^{\nu}p)N^{2\nu-1},$$

which implies

$$S_{\vec{a}}(N) \ll (k^{1/2\nu}L^{1/2\nu} + p^{1/4\nu} + L^{-1/2}p^{1/2\nu})N^{1-1/2\nu} + L.$$

Finally, selecting $L = \lceil k^{-1/(\nu+1)}p^{1/(\nu+1)} \rceil$, we obtain,

$$S_{\vec{a}}(N) \quad \ll \quad \left(k^{1/2(\nu+1)}p^{1/2\nu(\nu+1)} + p^{1/4\nu}\right) N^{1-1/2\nu} \quad + \quad k^{-1/(\nu+1)}p^{1/(\nu+1)}.$$

Assuming that

$$k^{-1/(\nu+1)}p^{1/(\nu+1)} < k^{1/2(\nu+1)}p^{1/2\nu(\nu+1)}N^{1-1/2\nu},$$

as otherwise the estimate is trivial, we get the desired result. □

Now we can apply Lemma 5 to obtain the following bound for the discrepancy.

Corollary 8. *Let $\{u_n\}$ be the sequence defined by (1), where $Crk(f) = k$ and f has a representation P_k such that α_k in (2) is not zero. Suppose $\{u_n\}$ is purely periodic with an arbitrary period T and Γ is the sequence defined by (4). Then, for any fixed integer $\nu \ge 1$, and any positive integer $N \le T$, the discrepancy of the sequence Γ with $N \le T$ satisfies*

$$\Delta_N(\Gamma) = O\left(\left(k^{1/2(\nu+1)}p^{1/2\nu(\nu+1)} + p^{1/4\nu}\right) N^{-1/2\nu}(\log p)^m\right), \qquad (11)$$

when f has a representation P_k such that α_k in (2) is not zero. The implied constant depends only on m and ν.

The bound (11) is nontrivial in a rather wide range (provided that $k < p(\log p)^{-2(\nu+1)m-\varepsilon}$),

$$p \ge T \ge N \gg \max\left(p^{1/(\nu+1)}k^{\nu/(\nu+1)}, p^{1/2}\right)(\log p)^{2\nu m+\epsilon} \qquad (12)$$

for a fixed $\epsilon > 0$.

We remark that for $k \le p^{1/2-\varepsilon}$, taking a sufficiently large ν in (12), we get a nontrivial bound on the discrepancy provided that $N \gg p^{1/2}(\log p)^c$, where c depends only on ε. We also note that in [1, Theorem 5] a formula for the number of such permutations is given.

When R_k is linear the proof above is not valid, as one would expect. In case $m = 1$, one can use the estimates from [19, Theorem 9.1] to obtain a similar bound. When $m > 1$, the distribution of the sequence $\{u_n\}$ depends on the element α_{k+1}/β_k in (2) since techniques for linear congruential generators apply, see [19] or [20, Theorem 7.3].

When $f = aX^{p-2} + b$ with $Crk(f) = 1$, the sequence generated by (1) is the so-called *inversive* pseudorandom sequence. In this case, the discrepancy bound for Γ defined by (4) has been obtained in [13]:

$$\Delta_N(\Gamma) = O(N^{-1/2}p^{1/4}(\log p)^m), \tag{13}$$

for $p \ge T \ge N$.

Our result generalizes (13) and improves the previously known estimate for the discrepancy of (4) generated by an arbitrary nonlinear polynomial f, which is

$$\Delta_N(\Gamma) = O\left(\left(\frac{\log(2p/N)}{\log p}\right)^{1/2}\left(\log\frac{\log p}{\log(2p/N)}\right)^m\right), \tag{14}$$

where the implied constant depends on m, and the degree of the polynomial f in (1), see [25, Theorem 2]. It is interesting to compare the range (12) with the considerably shorter range corresponding to (14), see [25, Corollary 2].

Remark 2. *Methods of construction of permutations P_k of $\mathbb{F}_p$ for any $k \ge 1$, consisting of one full cycle of length p are given in [7]. When $k = 2l$, it is shown in [6] that any permutation which has a representation of the form*

$$P_k(X) = (\ldots(X + a_1)^{p-2} + a_2)^{p-2} + \ldots + a_{l+1})^{p-2} - a_l)^{p-2} - \ldots - a_2)^{p-2} - a_1$$

is a full cycle. For permutations with Carlitz rank $1, 2$ and 3, conditions for them to have full cycles are also known, see [7]. Therefore, one can construct sequences $\{u_n\}$ as in (1), with largest possible period p, generated by $f = P_k$. For such sequences one has $Crk(f) \le k$, and the upper bound

in (11) *applies, if the corresponding* α_k *is non-zero. For practical purposes one would of course choose small* k *so that the generation of* $\{u_n\}$ *is not slow, which in this case can be done in polynomial time in* k*. Note that for any small* $k > 1$ *we obtain very good alternatives to the inversive generator.*

Theorem 7, together with Remark 2, enables the construction of many new pseudorandom sequences with full period and good distribution behavior. These sequences can be chosen to have large linear complexity also as we show in the next section.

4. Linear Complexity Profile

The linear complexity profile is a widely used measure for predictability of a sequence of elements of $\mathbb{F}_p$. We recall that the *linear complexity profile* of a sequence $\{u_n\}$, $n = 0, \ldots, N-1$, is the order L of the shortest linear recurrence which generates the first N elements of the sequence, i. e.

$$u_{n+L} = c_{L-1}u_{n+L-1} + \cdots + c_1 u_{n+1} + c_0 u_n, \quad n = 0, \ldots, N-L-1.$$

We denote this quantity by $L(u_n, N)$. Here, we give a lower bound for $L(u_n, N)$ defined by a permutation f with Carlitz rank k. The proof follows the same ideas as in [14, Theorem 1].

Theorem 9. *Let* f *be a permutation with* $Crk(f) = k$*, which has a representation* P_k *such that* α_k *in* (2) *is not zero. Suppose the sequence* $\{u_n\}$ *is defined by* (1) *and has period* T*. Then the linear complexity profile* $L(u_n, N)$ *satisfies*

$$L(u_n, N) \geq \min\left\{\frac{N-2}{k+2}, \frac{T-2}{k+2}\right\}.$$

Proof. Suppose $\{u_n\}$ satisfies a linear recurrence relation of length L,

$$u_{n+L} = c_{L-1}u_{n+L-1} + \cdots + c_1 u_{n+1} + c_0 u_n, \qquad n = 0, \ldots, N-L-1,$$

with $c_0, \ldots, c_{L-1} \in \mathbb{F}_p$. We may assume $L \leq p-1$.

Recall that $f(u) = R_k(u)$ for $u \in \mathcal{K}$, where R_k is defined by (2) and $\mathcal{K}$ is a subset of $\mathbb{F}_p$ of cardinality at least $p-k$. Also, $\mathcal{K}_l$ is the set of elements $u \in \mathbb{F}_p$ such that

$$f^{(l)}(u) = \frac{\ell_{1,l}(u)}{\ell_{2,l}(u)}, \tag{15}$$

where $\ell_{i,l}$, $i = 1, 2$, are linear polynomials, and the cardinality of $\mathcal{K}_l$ is at least $p - kl$. The bound for the cardinality of $\mathcal{K}_l$ comes from two simple facts: if $u, f(u), \ldots, f^{(l)}(u) \in \mathcal{K}$, then $u \in \mathcal{K}_l$, and f is a permutation.

As the rational function R_k in (2) is not linear since $\alpha_k \neq 0$, we note that $\ell_{2,l}$ is a nonconstant linear polynomial for every $\ell \geq 1$.

Putting $c_L = -1$, we define the following rational function

$$c_L \frac{\ell_{1,L}(X)}{\ell_{2,L}(X)} + c_{L-1} \frac{\ell_{1,L-1}(X)}{\ell_{2,L-1}(X)} + \ldots + c_1 \frac{\ell_{1,1}(X)}{\ell_{2,1}(X)} + c_0 X,$$

and getting rid of the denominators, which are all distinct, we arrive at a nonconstant polynomial F of degree at most $L + 1$ defined by

$$F(X) = c_0 X \prod_{i=1}^{L} \ell_{2,i}(X) + \sum_{j=1}^{L} c_j \ell_{1,j}(X) \prod_{i=1, i \neq j}^{L} \ell_{2,i}(X),$$

which has at least $N - Lk - L$ zeros corresponding to $u_0, \ldots, u_{N-L-1}$ for which (15) holds for $l = 0, \ldots, L$. Since all, but at most kL elements u of $\mathbb{F}_p$ satisfy $u, f(u), \ldots, f^{(L)}(u) \in \mathcal{K}$, the polynomial F has at least $N - Lk - L$ zeros.

The degree of F gives an upper bound on the number of roots, so

$$L + 1 \geq \deg F \geq \min\{N - Lk, T - Lk\} - L$$

and the result follows. □

Acknowledgements

The authors would like to thank to Igor Shparlinski for valuable discussions and comments which have improved the presentation of the paper. D. G.-P. was supported in part by the Spanish Government Projects MTM2011-24678 and TIN2011-27479-C04-04. A. O. was partially supported by the Swiss National Science Foundation Grant PA00P2–139679. A. T. was partially supported by TUBITAK grant 111T234.

References

[1] E. Aksoy, A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 2009. On the Carlitz rank of permutation polynomials, Finite Fields Appl., 15, 428–440.

[2] S. Blackburn, T. Etzion, and K. Paterson, 1996. Permutation polynomials, de Bruijn sequences, and linear complexity, J. Comb. Theory, Ser. A, 76(1), 55–82.

[3] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 2003. Predicting the inversive generator, Lect. Notes in Comp. Sci. Springer-Verlag, Berlin, 2898, 264–275.

[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez and I. E. Shparlinski, 2005. Predicting nonlinear pseudorandom number generators, Math. Comp., 74, 1471–1494.

[5] L. Carlitz, 1953. Permutations in a finite field, Proc. Amer. Math. Soc., 4, 538.

[6] A. Çeşmelioğlu, 2012. On permutations with full cycle, preprint.

[7] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 2008. On the cycle structure of permutation polynomials, Finite Fields Appl., 14, 593–614.

[8] A. Çeşmelioğlu, W. Meidl and A. Topuzoğlu, 2013. Permutations of finite fields with prescribed properties, J. Comput. Appl. Math., article in press, http://dx.doi.ors/10.1016/j.cam.2013.07.036

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

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

[11] D. Gomez-Perez, J. Gutierrez and Á. Ibeas, 2006. Attacking the Pollard generator, IEEE Trans. Inform. Theory, 52 5518–5523.

[12] J. Gutierrez and Á. Ibeas, 2007. Inferring sequences produced by a linear congruential generator on elliptic curves missing high-order bits, Designs, Codes and Cryptography, 41, 199–212.

[13] J. Gutierrez, H. Niederreiter, I. Shparlinski, 2000. On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period, Monatsh. Math., 129, 31-36

[14] J. Gutierrez, I. Shparlinski and A. Winterhof, 2003. On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators, IEEE Trans. Inform. Theory, 49, 60–64.

[15] H. Krawczyk, 1992. How to predict congruential generators, J. Algorithms, 13, 527–545.

[16] J. C. Lagarias, 1990. Pseudorandom number generators in cryptography and number theory, in: Proc. Symp. in Appl. Math., Amer. Math. Soc., Providence, RI, 42, 115–143.

[17] R. Lidl and H. Niederreiter, 1997. Finite fields, second ed, Cambridge University Press, Cambridge.

[18] C. J. Moreno and O. Moreno, 1991. Exponential sums and Goppa codes, 1, Proc. Amer. Math. Soc., 111, 523–531.

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

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

[21] H. Niederreiter and I. E. Shparlinski, 1999. 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', Finite Fields Appl., 5, 246–253.

[22] H. Niederreiter and I. E. Shparlinski, 2000. On the Distribution of Pseudorandom Numbers and Vectors Generated by Inversive Methods, AAECC, 10(3), 189–202.

[23] H. Niederreiter and I. Shparlinski, 2001. On the distribution of inversive congruential pseudorandom numbers in parts of the period, Math. Comp., 70, 1569–1574.

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

[25] H. Niederreiter and A. Winterhof, 2008. Exponential sums for nonlinear recurring sequences, Finite Fields Appl., 14, 59–64.

[26] I. E. Shparlinski, 2003. Cryptographic applications of analytic number theory: complexity lower bounds and pseudorandomness, Birkhäuser Verlag.

[27] A. Topuzoğlu, 2013. The Carlitz rank of permutations of finite fields: A survey, to appear in J. Symbolic Computation.

[28] A. Topuzoğlu and A. Winterhof, 2006. Pseudorandom sequences, in: A. Garcia, H. Stichtenoth (Eds.), Topics in Geometry, Coding Theory and Cryptography, Springer-Verlag, 135–166.

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