SEQUENCES WITH HIGH NONLINEAR COMPLEXITY

HARALD NIEDERREITER AND CHAOPING XING

Abstract. We improve lower bounds on the kth-order nonlinear complexity of pseudorandom sequences over finite fields and we establish a probabilistic result on the behavior of the kth-order nonlinear complexity of random sequences over finite fields.

1. Introduction

Pseudorandom sequences over large finite fields are of interest for simulation methods since such sequences can be transformed easily into sequences of uniform pseudorandom numbers in the unit interval $[0, 1]$ (see [17, Chapter 8]). Another area of applications is cryptography. In order to assess the suitability of a pseudorandom sequence, complexity-theoretic and statistical requirements have to be tested. In practice, both categories of tests—complexity-theoretic and statistical—should be carried out since these two categories are in a sense independent (see e.g. the recent paper [19]). A classical survey article on the testing of pseudorandom sequences in a cryptographic context is [21].

In this paper we focus on the complexity-theoretic analysis of pseudorandom sequences over finite fields. A variety of complexity measures for such sequences is available in the literature. The most common approach is to measure complexity by the shortest length of a feedback shift register that can generate the given sequence. The basic concept of this type is the *linear complexity* (also called the *linear span*) where only linear feedback shift registers are considered (see also Remark 3 below). There is a considerable amount of literature on the linear complexity which is surveyed in [18], [23], [25], and the recent handbook article [15]. Far less work has been done on complexity measures referring to feedback shift registers with feedback functions of higher algebraic degree (we may call them "nonlinear complexities"). A complexity measure of this type which has received some attention is the *maximum-order complexity* due to Jansen [4], [5] (see Remark 2 below). There are also complexity measures for sequences based on pattern counting, such as the *Lempel-Ziv complexity* (see [7] for the definition and [16] for cryptographic applications). The well-known *Kolmogorov complexity* is not of practical relevance since it cannot be computed in general for sequences of large length.

This paper contributes to the theory of nonlinear complexities by improving lower bounds on nonlinear complexities of interesting pseudorandom sequences and by establishing a probabilistic result on the behavior of nonlinear complexities of random sequences. In Section 2 we collect the basic definitions. In Sections 3 and 4 we establish complexity bounds for certain explicit inversive sequences and for newly constructed sequences from Hermitian function fields, respectively. Finally, in Section 5 we present the mentioned probabilistic result.

2. Definitions

We write $\mathbb{F}_q$ for the finite field with q elements, where q is an arbitrary prime power. For any positive integer m, let $\mathbb{F}_q[x_1, \ldots, x_m]$ be the ring of polynomials over $\mathbb{F}_q$ in the m

Date: October 12, 2018.

1991 *Mathematics Subject Classification.* 11K45, 68Q30, 94A55, 94A60.

Key words and phrases. Linear complexity, nonlinear complexity, maximum-order complexity, pseudorandom sequence.

variables $x_1, \ldots, x_m$. Furthermore, we denote the set of positive integers by $\mathbb{N}$. Now we define nonlinear complexities for sequences of finite length over $\mathbb{F}_q$.

Definition 1. Let $\mathbf{s} = (s_i)_{i=1}^n$ be a sequence of length $n \geq 1$ over the finite field $\mathbb{F}_q$ and let $k \in \mathbb{N}$. If $s_i = 0$ for $1 \leq i \leq n$, then we define the *kth-order nonlinear complexity* $N^{(k)}(\mathbf{s})$ to be 0. Otherwise, let $N^{(k)}(\mathbf{s})$ be the smallest $m \in \mathbb{N}$ for which there exists a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ of degree at most k in each variable such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \qquad \text{for } 1 \leq i \leq n-m. \tag{1}$$

Remark 1. For $n = 1$ we have $N^{(k)}(\mathbf{s}) = 0$ or 1. For $n \geq 2$ we always have $0 \leq N^{(k)}(\mathbf{s}) \leq n-1$, where the upper bound holds since (1) is satisfied for $m = n-1$ and f being the constant polynomial s_n. Both extreme values 0 and $n-1$ can occur. This is trivial for 0 by Definition 1. Furthermore, if $\mathbf{s} = (s_i)_{i=1}^n$ with $s_i = 0$ for $1 \leq i \leq n-1$ and $s_n = 1$, then $N^{(k)}(\mathbf{s}) = n-1$, since the assumption $N^{(k)}(\mathbf{s}) \leq n-2$ easily leads to a contradiction.

Remark 2. In Definition 1 it suffices to consider $1 \leq k \leq q-1$. This follows from the well-known fact that, as a map, any polynomial $f : \mathbb{F}_q^m \to \mathbb{F}_q$ can be represented by a polynomial over $\mathbb{F}_q$ in m variables of degree at most $q-1$ in each variable (see [8, pp. 368–369]). For $k \geq q-1$ all nonlinear complexities $N^{(k)}(\mathbf{s})$ of a fixed $\mathbf{s}$ are the same and equal to the *maximum-order complexity* $M(\mathbf{s}) = N^{(q-1)}(\mathbf{s})$ introduced by Jansen [4], [5]. Connections between the Lempel-Ziv complexity and the maximum-order complexity were studied in [4], [9], [10].

Remark 3. One may also consider the nonlinear complexity $L^{(k)}(\mathbf{s})$ where in Definition 1 we replace "of degree at most k in each variable" by "of total degree at most k". It is then trivial that $L^{(k)}(\mathbf{s}) \geq N^{(k)}(\mathbf{s})$ for any k and $\mathbf{s}$. Note that $L^{(1)}(\mathbf{s})$ is not quite the same as the linear complexity $L(\mathbf{s})$ of $\mathbf{s}$, since in the definition of $L(\mathbf{s})$ we accept only homogeneous linear polynomials $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ as feedback functions in (1), whereas in the definition of $L^{(1)}(\mathbf{s})$ we accept also linear polynomials with constant term. We have $L(\mathbf{s}) \geq L^{(1)}(\mathbf{s}) \geq L(\mathbf{s}) - 1$ for any $\mathbf{s}$, where the first inequality is trivial and the second inequality follows from a remark in [8, p. 401]. In particular, any lower bound on $L^{(1)}(\mathbf{s})$, like in Corollaries 1 and 2 and in Theorem 4 below, is also a lower bound on the linear complexity $L(\mathbf{s})$.

In order to define nonlinear complexities for infinite sequences, we proceed in analogy to the step from the linear complexity to the linear complexity profile (see [15]), namely by considering nonlinear complexities of finite-length initial segments of a given infinite sequence.

Definition 2. Let $S = (s_i)_{i=1}^\infty$ be an infinite sequence over $\mathbb{F}_q$. Then for any $k \in \mathbb{N}$ and $n \in \mathbb{N}$, we define $N_n^{(k)}(S) = N^{(k)}(\mathbf{s}_n)$ and $L_n^{(k)}(S) = L^{(k)}(\mathbf{s}_n)$, where $\mathbf{s}_n = (s_i)_{i=1}^n$.

3. Complexity bounds for explicit inversive sequences

We first consider sequences of finite length that belong to the family of *explicit inversive pseudorandom sequences* introduced in [13]. Let e be a primitive element of $\mathbb{F}_q$, i.e., a generator of the cyclic multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$, and choose an element $a \in \mathbb{F}_q^*$. Let $\mathbf{s} = (s_i)_{i=1}^{q-2}$ be the sequence over $\mathbb{F}_q$ defined by

$$s_i = (ae^i - a)^{-1} \qquad \text{for } 1 \leq i \leq q-2. \tag{2}$$

Theorem 1. *Let $\mathbf{s} = (s_i)_{i=1}^{q-2}$ be the sequence over $\mathbb{F}_q$ defined by (2). Then for any integer k with $1 \leq k \leq q-1$ we have*

$$N^{(k)}(\mathbf{s}_n) \geq (n-1)/(k+1) \qquad \textit{for } 1 \leq n \leq q-2,$$

where $\mathbf{s}_n = (s_i)_{i=1}^n$.

Proof. Since the kth-order nonlinear complexity is invariant under the termwise multiplication of a sequence by an element from $\mathbb{F}_q^*$, we can assume that $a = 1$. The result is trivial for $n = 1$, and so we can also assume that $2 \le n \le q-2$. Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ with $1 \le m \le n-1$ is a polynomial of degree at most k in each variable such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \qquad \text{for } 1 \le i \le n-m.$$

Thus, we have

$$-\frac{1}{e^{i+m}-1} + f\left(\frac{1}{e^i-1}, \frac{1}{e^{i+1}-1}, \ldots, \frac{1}{e^{i+m-1}-1}\right) = 0 \qquad \text{for } 1 \le i \le n-m. \tag{3}$$

Consider the rational function

$$R(z) = -\frac{1}{e^m z - 1} + f\left(\frac{1}{z-1}, \frac{1}{ez-1}, \ldots, \frac{1}{e^{m-1}z-1}\right) \in \mathbb{F}_q(z). \tag{4}$$

Since $1 \le m < q-1$, we have $e^m \ne e^i$ for $0 \le i \le m-1$. Therefore e^{-m} is not a pole of $f(1/(z-1), 1/(ez-1), \ldots, 1/(e^{m-1}z-1))$, and so $R(z) \ne 0 \in \mathbb{F}_q(z)$. Write $R(z)$ in reduced form as $R(z) = v(z)/w(z)$ with $v(z), w(z) \in \mathbb{F}_q[z]$, $v(z) \ne 0$, $w(z) \ne 0$, and $\gcd(v(z), w(z)) = 1$. From (3) we get $R(e^i) = 0$ for $1 \le i \le n-m$. Therefore $v(z)$ has at least $n-m$ zeros, and so $\deg(v(z)) \ge n-m$. On the other hand, the definition of $R(z)$ in (4) implies that $\deg(v(z)) \le \deg(w(z)) \le km+1$, and so $km+1 \ge n-m$. This yields $m \ge (n-1)/(k+1)$, which is the desired bound. □

Corollary 1. *Let $\mathbf{s} = (s_i)_{i=1}^{q-2}$ be the sequence over $\mathbb{F}_q$ defined by (2). Then for any integer k with $1 \le k \le q-1$ we have*

$$L^{(k)}(\mathbf{s}_n) \ge (n-1)/(k+1) \qquad \textit{for } 1 \le n \le q-2,$$

where $\mathbf{s}_n = (s_i)_{i=1}^n$.

Proof. This follows from Theorem 1 and Remark 3. □

For $k = 1$, it follows from Corollary 1 and an inequality in Remark 3 that for the linear complexity $L(\mathbf{s}_n)$ of the initial segment $\mathbf{s}_n = (s_i)_{i=1}^n$ in Corollary 1 we have $L(\mathbf{s}_n) \ge (n-1)/2$ for $1 \le n \le q-2$. This improves on the lower bound $L(\mathbf{s}_n) \ge (n-1)/3$ shown in [13, Theorem 1].

Now we consider infinite periodic sequences belonging to the family of explicit inversive pseudorandom sequences introduced in [13]. Let d be a positive divisor of $q-1$ with $d < q-1$ and let u be an element of order d of the multiplicative group $\mathbb{F}_q^*$. Such an element can be obtained as $u = e^{(q-1)/d}$, where e is a primitive element of $\mathbb{F}_q$. Furthermore, choose $b, c \in \mathbb{F}_q^*$ such that cb^{-1} does not belong to the cyclic subgroup of $\mathbb{F}_q^*$ generated by u. Then we define the sequence $S = (s_i)_{i=1}^\infty$ by

$$s_i = (bu^i - c)^{-1} \qquad \text{for all } i \ge 1. \tag{5}$$

Note that the sequence S is periodic with least period d.

Theorem 2. *Let $S = (s_i)_{i=1}^\infty$ be the sequence over $\mathbb{F}_q$ defined by (5). Then for any integer k with $1 \le k \le q-1$ we have*

$$N_n^{(k)}(S) \ge \min\{(n-1)/(k+1), (d-1)/k\} \qquad \textit{for all } n \ge 1.$$

Proof. Since the kth-order nonlinear complexity is invariant under the termwise multiplication of a sequence by an element from $\mathbb{F}_q^*$, we can assume that $b = 1$ and that c does not belong to the cyclic subgroup of $\mathbb{F}_q^*$ generated by u. We can also assume that $n \ge 2$ and $N_n^{(k)}(S) < (d-1)/k$, for otherwise the result is trivial. Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ with $1 \le m \le n-1$ and $m < (d-1)/k$ is a polynomial of degree at most k in each variable such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \qquad \text{for } 1 \le i \le n-m.$$

Thus, we have

$$-\frac{1}{u^{i+m}-c}+f\left(\frac{1}{u^i-c},\frac{1}{u^{i+1}-c},\ldots,\frac{1}{u^{i+m-1}-c}\right)=0 \qquad \text{for } 1\le i\le n-m. \tag{6}$$

Consider the rational function

$$R(z)=-\frac{1}{u^m z-c}+f\left(\frac{1}{z-c},\frac{1}{uz-c},\ldots,\frac{1}{u^{m-1}z-c}\right)\in \mathbb{F}_q(z). \tag{7}$$

Since $1\le m<(d-1)/k\le d-1$, we have $u^m\ne u^i$ for $0\le i\le m-1$. Therefore cu^{-m} is not a pole of $f(1/(z-c),1/(uz-c),\ldots,1/(u^{m-1}z-c))$, and so $R(z)\ne 0\in\mathbb{F}_q(z)$. Write $R(z)$ in reduced form as $R(z)=v(z)/w(z)$ with $v(z),w(z)\in\mathbb{F}_q[z]$, $v(z)\ne 0$, $w(z)\ne 0$, and $\gcd(v(z),w(z))=1$. From (6) we get $R(u^i)=0$ for $1\le i\le n-m$. Therefore $v(z)$ has at least $\min\{n-m,d\}$ zeros, and so $\deg(v(z))\ge\min\{n-m,d\}$. On the other hand, the definition of $R(z)$ in (7) implies that $\deg(v(z))\le\deg(w(z))\le km+1$, and so

$$km+1\ge\min\{n-m,d\}.$$

Now $m<(d-1)/k$ yields $km+1<d$, and so we must have $\min\{n-m,d\}=n-m$. Therefore $km+1\ge n-m$, hence $m\ge(n-1)/(k+1)$, and the proof is complete. □

Corollary 2. *Let $S=(s_i)_{i=1}^{\infty}$ be the sequence over $\mathbb{F}_q$ defined by (5). Then for any integer k with $1\le k\le q-1$ we have*

$$L_n^{(k)}(S)\ge\min\{(n-1)/(k+1),(d-1)/k\} \qquad \textit{for all } n\ge 1.$$

Proof. This follows from Theorem 2 and Remark 3. □

The lower bounds on nonlinear complexities in Theorem 2 and Corollary 2 are better than those for the periodic sequences over $\mathbb{F}_q$ (inversive generators, quadratic exponential generators, general nonlinear generators) shown in [3] and [12]. The exact value of the linear complexity of any finite-length initial segment of the sequence defined by (5) is known from [14, Corollary 7]. Distribution properties and structural properties of this sequence were investigated in [24].

4. Sequences obtained from Hermitian function fields

The length of the sequence (2) over $\mathbb{F}_q$ has order of magnitude q and the period length of the sequence (5) over $\mathbb{F}_q$ has an order of magnitude at most q. In this section, we construct finite-length sequences over $\mathbb{F}_q$ with high nonlinear complexity for which the length has an order of magnitude larger than q. This new construction of sequences uses the theory of global function fields. We follow the monographs [20] and [22] with regard to the notation and terminology for global function fields.

Let $F/\mathbb{F}_q$ be a global function field with full constant field $\mathbb{F}_q$. We write $\mathbb{P}_F$ for the set of places of F. Let $\deg(P)$ denote the degree of the place $P\in\mathbb{P}_F$. If $\deg(P)=1$, then we speak of a *rational place* of F. Let ν_P be the normalized discrete valuation corresponding to $P\in\mathbb{P}_F$. For a divisor D of F, let $\mathcal{L}(D)$ be the Riemann-Roch space associated with D. We note that $\mathcal{L}(D)$ is a finite-dimensional vector space over $\mathbb{F}_q$. Let $\deg(D)$ denote the degree of the divisor D. By the Riemann-Roch theorem [22, Theorem 1.5.17] we have

$$\dim(\mathcal{L}(D))=\deg(D)+1-g \quad \text{whenever } \deg(D)\ge 2g-1, \tag{8}$$

where g is the genus of F. For $P\in\mathbb{P}_F$ and $h\in F$ with $\nu_P(h)\ge 0$, we write $h(P)$ for the residue class of h modulo P (see [22, p. 6]). If P is a rational place, then $h(P)\in\mathbb{F}_q$.

Now let $H/\mathbb{F}_q$ be the Hermitian function field over $\mathbb{F}_q$ which exists whenever q is a square, say $q=\ell^2$ with a prime power ℓ. The Hermitian function field $H/\mathbb{F}_q$ can be defined explicitly by $H=\mathbb{F}_q(x,y)$ with $y^\ell+y=x^{\ell+1}$. The function field $H/\mathbb{F}_q$ has exactly ℓ^3+1 rational places and genus $g=\ell(\ell-1)/2$. A summary of the properties of $H/\mathbb{F}_q$ can be found in [22,

Lemma 6.4.4]. We single out the rational place $P_\infty \in \mathbb{P}_H$ which is defined as the unique pole of x.

Let $\mathcal{G} = \mathrm{Aut}(H/\mathbb{F}_q)$ be the group of field automorphisms of the Hermitian function field $H/\mathbb{F}_q$ that fix the elements of $\mathbb{F}_q$. We refer to [26, Section II] for a summary of the properties of the group $\mathcal{G}$. If $\sigma \in \mathcal{G}$ and $P \in \mathbb{P}_H$, then the set $\sigma(P) := \{\sigma(h) : h \in P\}$ is again a place of H. We have the following simple facts (see [22, Section 8.2] and [26, Lemma 2.1]).

Lemma 1. *For any $\sigma \in \mathcal{G} = \mathrm{Aut}(H/\mathbb{F}_q)$, $P \in \mathbb{P}_H$, and $h \in H$ we have:*
(i) $\deg(\sigma(P)) = \deg(P)$;
(ii) $\nu_{\sigma(P)}(\sigma(h)) = \nu_P(h)$;
(iii) $\sigma(h)(\sigma(P)) = h(P)$ *if* $\nu_P(h) \geq 0$.

Now, using the same notation as in [26, Lemma 2.2], let ϕ be the element of $\mathcal{G}$ determined by

$$\phi(x) = ex, \quad \phi(y) = e^{\ell+1}y,$$

where e is a primitive element of $\mathbb{F}_q$. Then according to [26, Lemma 2.2], the rational place P_∞ of H satisfies $\phi(P_\infty) = P_\infty$, and under the action of ϕ on $\mathbb{P}_H$ there are ℓ orbits each containing exactly $q-1$ distinct rational places of H. We denote these $(q-1)\ell$ distinct rational places of H occurring altogether in these ℓ orbits by

$$Q, \phi(Q), \ldots, \phi^{q-2}(Q), P_1, \phi(P_1), \ldots, \phi^{q-2}(P_1), \ldots, P_{\ell-1}, \phi(P_{\ell-1}), \ldots, \phi^{q-2}(P_{\ell-1}).$$

By (8) we have $\dim(\mathcal{L}((2g-1)P_\infty + Q)) = g+1$ and $\dim(\mathcal{L}((2g-1)P_\infty)) = g$, and so we can choose an element $h \in \mathcal{L}((2g-1)P_\infty + Q) \setminus \mathcal{L}((2g-1)P_\infty)$. Then we consider the sequence $\mathbf{s} = (s_i)_{i=1}^M$ over $\mathbb{F}_q$ of length $M := (q-1)(\ell-1)$ given by

$$\mathbf{s} = \big(h(P_1), h(\phi(P_1)), \ldots, h(\phi^{q-2}(P_1)), \ldots, h(P_{\ell-1}), h(\phi(P_{\ell-1})), \ldots, h(\phi^{q-2}(P_{\ell-1}))\big). \tag{9}$$

The choice of h guarantees that all terms of the sequence $\mathbf{s}$ are well defined. Note that the length M of $\mathbf{s}$ has order of magnitude $q^{3/2}$.

Theorem 3. *Let $H/\mathbb{F}_q$ be the Hermitian function field over $\mathbb{F}_q$ with $q = \ell^2$ for some prime power ℓ. Let $\mathbf{s} = (s_i)_{i=1}^M$ with $M = (q-1)(\ell-1)$ be the sequence over $\mathbb{F}_q$ defined by* (9)*. Then for any integer k with $1 \leq k \leq q-1$ we have*

$$N^{(k)}(\mathbf{s}_n) \geq \frac{(q-1)\lfloor n/(q-1)\rfloor - 1}{\ell(\ell-1)k + \lfloor n/(q-1)\rfloor} \qquad \text{for } 1 \leq n \leq M,$$

where $\mathbf{s}_n = (s_i)_{i=1}^n$.

Proof. The result is trivial for $n < q-1$, and so we can assume that $n \geq q-1$. Since $N^{(k)}(\mathbf{s}_n)$ is a nondecreasing function of n, we can also assume that n is a multiple of $q-1$, say $n = (q-1)r$ with $r \in \mathbb{N}$ and $r \leq \ell - 1$. Now we fix such an n. We claim that $\mathbf{s}_n$ is not the zero sequence. For otherwise there exist n rational places $Q_1, \ldots, Q_n$ of H different from P_∞ and Q that are zeros of h. This implies that $h \in \mathcal{L}(D)$ with

$$D := (2g-1)P_\infty + Q - Q_1 - \cdots - Q_n.$$

But

$$\deg(D) = 2g - n = \ell(\ell-1) - n \leq \ell(\ell-1) - (q-1) = -\ell + 1 < 0,$$

and so $h = 0$ by [20, Corollary 3.4.4]. This is a contradiction to the fact that $h \notin \mathcal{L}((2g-1)P_\infty)$ by the choice of h.

Thus we have $N^{(k)}(\mathbf{s}_n) \geq 1$. If $N^{(k)}(\mathbf{s}_n) \geq q-1$, then the lower bound in the theorem holds trivially. Hence we can assume that $N^{(k)}(\mathbf{s}_n) \leq q-2$. Suppose that $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ with $1 \leq m \leq q-2 \leq n-1$ is a polynomial of degree at most k in each variable such that

$$s_{i+m} = f(s_i, s_{i+1}, \ldots, s_{i+m-1}) \qquad \text{for } 1 \leq i \leq n-m. \tag{10}$$

By applying (10) only for $i = (q-1)(j-1)+t+1$ with $j = 1, \ldots, r$ and $t = 0, 1, \ldots, q-m-2$, we obtain

$$-h(\phi^{t+m}(P_j)) + f\left(h(\phi^t(P_j)), h(\phi^{t+1}(P_j)), \ldots, h(\phi^{t+m-1}(P_j))\right) = 0$$

for $1 \le j \le r$ and $0 \le t \le q-m-2$. Lemma 1(iii) yields

$$h(\phi^{t+b}(P_j)) = h(\phi^b(\phi^t(P_j))) = \phi^{-b}(h)(\phi^t(P_j))$$

for $1 \le j \le r$ and all integers $t \ge 0$ and $b \ge 0$, and so

$$-\phi^{-m}(h)(\phi^t(P_j)) + f\left(h(\phi^t(P_j)), \phi^{-1}(h)(\phi^t(P_j)), \ldots, \phi^{-(m-1)}(h)(\phi^t(P_j))\right) = 0 \tag{11}$$

for $1 \le j \le r$ and $0 \le t \le q-m-2$.

Consider the element

$$w = -\phi^{-m}(h) + f\left(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)\right) \in H.$$

We have $\nu_Q(h) = -1$ by the choice of h, hence $\nu_{\phi^{-m}(Q)}(\phi^{-m}(h)) = -1$ by Lemma 1(ii), and so the place $\phi^{-m}(Q)$ is a pole of $\phi^{-m}(h)$. On the other hand, for $b = 0, 1, \ldots, m-1$, the place $\phi^{-m}(Q)$ is not a pole of $\phi^{-b}(h)$ (use again Lemma 1(ii) and the choice of h), and so $\phi^{-m}(Q)$ is not a pole of $f\left(h, \phi^{-1}(h), \ldots, \phi^{-(m-1)}(h)\right)$. Hence we must have $w \ne 0$.

Now we study the zeros and poles of w. First of all, it follows from (11) that all the $(q-m-1)r$ distinct places $\phi^t(P_j)$, $1 \le j \le r$, $0 \le t \le q-m-2$, are zeros of w. Therefore the degree of the zero divisor $(w)_0$ of w satisfies

$$\deg((w)_0) \ge (q-m-1)r.$$

By the choice of h and Lemma 1(ii), the only possible poles of w are the rational places $P_\infty, Q, \phi(Q), \ldots, \phi^{q-2}(Q)$. Note that $\nu_{P_\infty}(h) \ge -(2g-1)$. Since P_∞ is invariant under ϕ, Lemma 1(ii) shows that $\nu_{P_\infty}(\phi^{-b}(h)) \ge -(2g-1)$ for any integer $b \ge 0$. It follows that $\nu_{P_\infty}(w) \ge -(2g-1)km$. Now we determine the possible poles of w in the set $\mathcal{Q} = \{Q, \phi(Q), \ldots, \phi^{q-2}(Q)\}$ of rational places. The only pole of h in $\mathcal{Q}$ is Q and its pole order is 1. Furthermore, for any integer b with $1 \le b \le m \le q-2$, Lemma 1(ii) shows that the only pole of $\phi^{-b}(h)$ in $\mathcal{Q}$ is $\phi^{-b}(Q) = \phi^{q-1-b}(Q)$ and its pole order is 1. Altogether, the degree of the pole divisor $(w)_\infty$ of w satisfies

$$\deg((w)_\infty) \le (2g-1)km + km + 1 = 2gkm + 1.$$

Now $\deg((w)_\infty) = \deg((w)_0)$ by a fundamental identity for algebraic function fields (see [22, Theorem 1.4.11]), and so

$$2gkm + 1 \ge \deg((w)_\infty) = \deg((w)_0) \ge (q-m-1)r.$$

It follows that

$$m \ge \frac{(q-1)r - 1}{2gk + r},$$

which completes the proof of the theorem (recall that we assumed without loss of generality that $n = (q-1)r$). □

Note that the lower bound on $N^{(k)}(\mathbf{s}_n)$ in Theorem 3 is of order of magnitude $n/(qk)$. If n is of the maximal order of magnitude $q^{3/2}$, then the lower bound is of order of magnitude $q^{1/2}/k$. In contrast to Section 3, we can obtain a better lower bound for the nonlinear complexity $L^{(k)}$ (see Remark 3) of the sequence (9) than that implied by Theorem 3.

Theorem 4. *Let $H/\mathbb{F}_q$ be the Hermitian function field over $\mathbb{F}_q$ with $q = \ell^2$ for some prime power ℓ. Let $\mathbf{s} = (s_i)_{i=1}^M$ with $M = (q-1)(\ell-1)$ be the sequence over $\mathbb{F}_q$ defined by (9). Then for any integer $k \ge 1$ we have*

$$L^{(k)}(\mathbf{s}_n) \ge \frac{(q-1)\lfloor n/(q-1)\rfloor - (\ell^2-\ell-1)k - 1}{k + \lfloor n/(q-1)\rfloor} \qquad \text{for } 1 \le n \le M,$$

where $\mathbf{s}_n = (s_i)_{i=1}^n$.

Proof. We proceed exactly as in the proof of Theorem 3. The only difference is that now $\nu_{P_\infty}(w) \geq -(2g-1)k$ since the polynomial f has *total degree* at most k. Therefore

$$\deg((w)_\infty) \leq (2g-1)k + km + 1,$$

and this yields the desired result. □

For small k and for n of a larger order of magnitude than q, the lower bound on $L^{(k)}(\mathbf{s}_n)$ in Theorem 4 is of order of magnitude q.

5. A probabilistic result

Let μ_q be the uniform probability measure on $\mathbb{F}_q$ which assigns the measure $1/q$ to each element of $\mathbb{F}_q$. Let $\mathbb{F}_q^\infty$ be the sequence space over $\mathbb{F}_q$ and let μ_q^∞ be the complete product probability measure on $\mathbb{F}_q^\infty$ induced by μ_q. We say that a property of sequences $S \in \mathbb{F}_q^\infty$ holds μ_q^∞-*almost everywhere* if it holds for a set of sequences S of μ_q^∞-measure 1. We may view such a property as a typical property of a random sequence over $\mathbb{F}_q$.

Theorem 5. *Let k be an integer with $1 \leq k \leq q-1$. Then μ_q^∞-almost everywhere we have*

$$\liminf_{n\to\infty} \Big(N_n^{(k)}(S) - \frac{\log n}{\log(k+1)} \Big) \geq 0.$$

Proof. For $m, n \in \mathbb{N}$ with $m \leq n-1$, let $T_n^{(k)}(m)$ be the number of sequences $\mathbf{s}$ of length n over $\mathbb{F}_q$ with $N^{(k)}(\mathbf{s}) \leq m$. Each sequence $\mathbf{s} = (s_i)_{i=1}^n$ counted by $T_n^{(k)}(m)$ is (not necessarily uniquely) determined by a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ of degree at most k in each variable and by initial values $s_1, \ldots, s_m$ of the recursion (1). Since the number of possibilities for f is $q^{(k+1)^m}$, we have

$$T_n^{(k)}(m) \leq q^{(k+1)^m + m} \qquad \text{for } 1 \leq m \leq n-1. \tag{12}$$

Now fix $\varepsilon > 0$ and put

$$b_n = \frac{\log n}{\log(k+1)} - \varepsilon \qquad \text{for } n = 1, 2, \ldots$$

and

$$A_n = \{S \in \mathbb{F}_q^\infty : N_n^{(k)}(S) \leq b_n\} \qquad \text{for } n = 1, 2, \ldots.$$

Then $1 \leq \lfloor b_n \rfloor \leq n-1$ for sufficiently large n, and so (12) yields

$$\mu_q^\infty(A_n) = q^{-n} T_n^{(k)}(\lfloor b_n \rfloor) \leq q^{(k+1)^{b_n} + b_n - n}$$

for sufficiently large n. Now for some $0 < \delta < 1$ we have

$$(k+1)^{b_n} + b_n - n < n\Big(\frac{1}{(k+1)^\varepsilon} + \frac{\log n}{n \log(k+1)} - 1 \Big) < -\delta n$$

for sufficiently large n, and so $\sum_{n=1}^\infty \mu_q^\infty(A_n) < \infty$. Then the Borel-Cantelli lemma (see [1, Lemma 3.14] and [11, p. 228]) shows that the set of all $S \in \mathbb{F}_q^\infty$ for which $S \in A_n$ for infinitely many n has μ_q^∞-measure 0. In other words, μ_q^∞-almost everywhere we have $S \in A_n$ for at most finitely many n. It follows then from the definition of A_n that μ_q^∞-almost everywhere we have

$$N_n^{(k)}(S) > b_n = \frac{\log n}{\log(k+1)} - \varepsilon$$

for sufficiently large n. This means that μ_q^∞-almost everywhere we have

$$\liminf_{n\to\infty} \Big(N_n^{(k)}(S) - \frac{\log n}{\log(k+1)} \Big) \geq -\varepsilon.$$

By applying this for all $\varepsilon = 1/r$ with $r \in \mathbb{N}$ and noting that the intersection of countably many sets of μ_q^∞-measure 1 has again μ_q^∞-measure 1, we obtain the result of the theorem. □

Remark 4. For $k = q-1$, Theorem 5 says that μ_q^∞-almost everywhere the maximum-order complexity $N_n^{(q-1)}(S)$ (see Remark 2) grows at least like $(\log n)/(\log q)$ as $n \to \infty$. This is in good accordance with the result of Jansen [4] (see also [2] and [6]) that the expected value of $N_n^{(q-1)}(S)$ behaves asymptotically like $(\log n)/(\log q)$, up to an absolute constant. On the basis of these results, it may be conjectured that μ_q^∞-almost everywhere we have

$$\lim_{n\to\infty} \frac{N_n^{(q-1)}(S)}{\log n} = C_q$$

for some constant $C_q > 0$ depending only on q. A similar behavior may be conjectured for $N_n^{(k)}(S)$ with $1 \le k < q-1$, where C_q is replaced by a constant $C_{q,k} > 0$ depending only on q and k. In view of this heuristic that the expected order of magnitude of $N_n^{(k)}(S)$ for random sequences S is $\log n$, it is clear that the sequences considered in Sections 3 and 4 can be said to have high nonlinear complexity.

Acknowledgments

We are grateful to Arne Winterhof of the Austrian Academy of Sciences for very fruitful discussions on the topic of this paper. The first author enjoyed the hospitality of Nanyang Technological University in Singapore at the time when this project was initiated.

References

[1] L. Breiman, Probability, SIAM, Philadelphia, 1992.
[2] D. Erdmann and S. Murphy, An approximate distribution for the maximum order complexity, Designs Codes Cryptography 10, 325–339 (1997).
[3] J. Gutierrez, I.E. Shparlinski, and A. Winterhof, On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators, IEEE Trans. Inform. Theory 49, 60–64 (2003).
[4] C.J.A. Jansen, Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods, Ph.D. Thesis, TU Delft (Netherlands), 1989.
[5] C.J.A. Jansen, The maximum order complexity of sequence ensembles, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), pp. 153–159, Lecture Notes in Computer Science, Vol. 547, Springer, Berlin, 1991.
[6] C.J.A. Jansen and D.E. Boekee, The shortest feedback shift register that can generate a given sequence, Advances in Cryptology – CRYPTO '89 (G. Brassard, ed.), pp. 90–99, Lecture Notes in Computer Science, Vol. 435, Springer, Berlin, 1990.
[7] A. Lempel and J. Ziv, On the complexity of finite sequences, IEEE Trans. Inform. Theory 22, 75–81 (1976).
[8] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[9] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, Nonlinear complexity of binary sequences and connections with Lempel-Ziv compression, Sequences and Their Applications – SETA 2006 (G. Gong, T. Helleseth, H.-Y. Song, and K.C. Yang, eds.), pp. 168–179, Lecture Notes in Computer Science, Vol. 4086, Springer, Berlin, 2006.
[10] K. Limniotis, N. Kolokotronis, and N. Kalouptsidis, On the nonlinear complexity and Lempel-Ziv complexity of finite length sequences, IEEE Trans. Inform. Theory 53, 4293–4302 (2007).
[11] M. Loève, Probability Theory, 3rd ed., Van Nostrand Reinhold Co., New York, 1963.
[12] W. Meidl and A. Winterhof, On the linear complexity profile of explicit nonlinear pseudorandom numbers, Inform. Process. Letters 85, 13–18 (2003).
[13] W. Meidl and A. Winterhof, On the linear complexity profile of some new explicit inversive pseudorandom numbers, J. Complexity 20, 350–355 (2004).
[14] W. Meidl and A. Winterhof, On the joint linear complexity profile of explicit inversive multisequences, J. Complexity 21, 324–336 (2005).
[15] W. Meidl and A. Winterhof, Linear complexity of sequences and multisequences, Handbook of Finite Fields (G.L. Mullen and D. Panario, eds.), pp. 324–336, CRC Press, Boca Raton, FL, 2013.
[16] S. Mund, Ziv-Lempel complexity for periodic sequences and its cryptographic application, Advances in Cryptology – EUROCRYPT '91 (D.W. Davies, ed.), pp. 114–126, Lecture Notes in Computer Science, Vol. 547, Springer, Berlin, 1991.

[17] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, SIAM, Philadelphia, 1992.
[18] H. Niederreiter, Linear complexity and related complexity measures for sequences, Progress in Cryptology – INDOCRYPT 2003 (T. Johansson and S. Maitra, eds.), pp. 1–17, Lecture Notes in Computer Science, Vol. 2904, Springer, Berlin, 2003.
[19] H. Niederreiter, The independence of two randomness properties of sequences over finite fields, J. Complexity 28, 154–161 (2012).
[20] H. Niederreiter and C.P. Xing, Algebraic Geometry in Coding Theory and Cryptography, Princeton University Press, Princeton, NJ, 2009.
[21] R.A. Rueppel, Stream ciphers, Contemporary Cryptology: The Science of Information Integrity (G.J. Simmons, ed.), pp. 65–134, IEEE Press, Piscataway, NJ, 1992.
[22] H. Stichtenoth, Algebraic Function Fields and Codes, 2nd ed., Springer, Berlin, 2009.
[23] A. Topuzoğlu and A. Winterhof, Pseudorandom sequences, Topics in Geometry, Coding Theory and Cryptography (A. Garcia and H. Stichtenoth, eds.), pp. 135–166, Springer, Dordrecht, 2007.
[24] A. Winterhof, On the distribution of some new explicit inversive pseudorandom numbers and vectors, Monte Carlo and Quasi-Monte Carlo Methods 2004 (H. Niederreiter and D. Talay, eds.), pp. 487–499, Springer, Berlin, 2006.
[25] A. Winterhof, Linear complexity and related complexity measures, Selected Topics in Information and Coding Theory (I. Woungang, S. Misra, and S.C. Misra, eds.), pp. 3–40, World Scientific, Singapore, 2010.
[26] C.P. Xing and Y. Ding, Multisequences with large linear and k-error linear complexity from Hermitian function fields, IEEE Trans. Inform. Theory 55, 3858–3863 (2009).

Harald Niederreiter, Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstr. 69, A-4040 Linz, AUSTRIA, and Department of Mathematics, University of Salzburg, Hellbrunnerstr. 34, A-5020 Salzburg, AUSTRIA; Chaoping Xing, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371, REPUBLIC OF SINGAPORE

E-mail address: ghnied@gmail.com (H. Niederreiter), xingcp@ntu.edu.sg (Chaoping Xing)