ACADEMIC PRESS

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Complexity 19 (2003) 61–72

Journal of COMPLEXITY

http://www.elsevier.com/locate/jco

The expected value of the joint linear complexity of periodic multisequences ☆

Wilfried Meidl[a] and Harald Niederreiter[b,*]

[a] *Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria*

[b] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Singapore*

Received 14 May 2002; accepted 12 September 2002

Abstract

Complexity measures for sequences of elements of a finite field, such as the linear complexity, play an important role in cryptology. Recent developments in stream ciphers point towards an interest in word-based (or vectorized) stream ciphers, which require the study of the complexity of multisequences. We extend a well-known relationship between the linear complexity of an N-periodic sequence and the (generalized) discrete Fourier transform of N-tuples to the case of multisequences. Using the concept of the generalized discrete Fourier transform for multisequences, we compute the expected value of the joint linear complexity of random periodic multisequences, and for some types of period lengths N we determine the number $\mathcal{N}_N^t(c)$ of t N-periodic sequences with given joint linear complexity c.

Keywords: Multisequences; Linear complexity; Stream ciphers; Generalized discrete Fourier transform

1. Introduction

The linear complexity of sequences with terms in a finite field is a fundamental concept for the assessment of keystreams in stream ciphers (cf. [11]). A lot of research has been done on the linear complexity and related complexity measures for sequences; see [9] for a recent survey. This body of research has concentrated,

☆ Research partially supported by the Austrian Science Fund (FWF) under the project S8306-MAT.
*Corresponding author.
E-mail addresses: wilfried.meidl@oeaw.ac.at (W. Meidl), nied@math.nus.edu.sg (H. Niederreiter).

0885-064X/02/$ - see front matter
PII: S0885-064X(02)00009-2

however, on single sequences. Recent developments in stream ciphers point towards an interest in word-based (or vectorized) stream ciphers. The theory of such stream ciphers requires the study of the complexity of multisequences, i.e., of parallel streams of finitely many sequences. Not much work has been carried out in this direction. However, we can refer to investigations on the synthesis of multisequences (see e.g. [1, Appendix A];[12]) and on the linear complexity profile of multisequences (cf. [13]). In the present paper we study the (joint) linear complexity of periodic multisequences. For the necessary background on linear recurring sequences we refer to [4, Chapter 8].

Throughout this paper, F_q denotes the finite field of order q. The *linear complexity* $L(S)$ of a periodic sequence $S = s_0, s_1, s_2, \ldots$ with terms in F_q is the smallest nonnegative integer c for which there exist coefficients $d_1, d_2, \ldots, d_c \in F_q$ such that

$$s_j + d_1 s_{j-1} + \cdots + d_c s_{j-c} = 0 \quad \text{for all } j \geqslant c.$$

In other words, $L(S)$ is the least order of a linear recurrence relation that S satisfies. If $c = L(S)$, then the coefficients $d_1, \ldots, d_c$ of the above linear recurrence relation for the sequence S give rise to the *minimal feedback polynomial* $f(x) = 1 + d_1 x + \cdots + d_c x^c \in F_q[x]$ of S. Thus, the linear complexity $L(S)$ is equal to the degree of $f(x)$.

If for a positive integer N the terms $s_0, s_1, \ldots \in F_q$ of the sequences S satisfy $s_{i+N} = s_i$ for all $i \geqslant 0$, then we say that S is *N-periodic*. For an N-periodic sequence $S = s_0, s_1, \ldots$ the minimal feedback polynomial $f(x)$ is, up to a nonzero multiplicative constant, given by

$$f(x) = \frac{x^N - 1}{\gcd(x^N - 1, S^N(x))}, \tag{1}$$

where $S^N(x) := s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$.

If $N = p^v n$ with $\gcd(n, p) = 1$, p denotes the characteristic of F_q, and α is a primitive nth root of unity in some extension field of F_q, then it follows from (1) that the degree of $f(x)$ is given by $N - \sum_{i=0}^{n-1} v_i$, where v_i is the minimum of p^v and the multiplicity of α^i as a root of $S^N(x)$. This correspondence is summarized in the Günther–Blahut Theorem (cf. [6]). To present the Günther–Blahut Theorem, we need the following definition.

Definition 1. The Günther weight of a matrix is the number of its entries that are nonzero or that lie below a nonzero entry.

Proposition 1 (Günther–Blahut Theorem). *Let S be an N-periodic sequence with terms in the finite field F_q, $N = p^v n$, $\gcd(n, p) = 1$. Then the linear complexity of S is the Günther weight of the $p^v \times n$ matrix*

$$\begin{pmatrix} S^N(1) & S^N(\alpha) & \ldots & S^N(\alpha^{n-1}) \\ (S^N)^{[1]}(1) & (S^N)^{[1]}(\alpha) & \ldots & (S^N)^{[1]}(\alpha^{n-1}) \\ \vdots & & & \\ (S^N)^{[p^v-1]}(1) & (S^N)^{[p^v-1]}(\alpha) & \ldots & (S^N)^{[p^v-1]}(\alpha^{n-1}) \end{pmatrix},$$

where $S^N(x)$ is the polynomial corresponding to the sequence S, $(S^N)^{[k]}(x)$ denotes the kth Hasse derivative (cf. [2]) of $S^N(x)$, and α is any primitive nth root of unity in some extension field of F_q.

Remark 1. The kth Hasse derivative of a polynomial has the advantage that it does not vanish identically if $k \geqslant p$, the characteristic of F_q. Thus, it can be used to derive the multiplicity v of a root of a polynomial even if $v \geqslant p$ (cf. [4, Lemma 6.51] where Hasse derivatives are called hyperderivatives).

The matrix in Proposition 1 is called the *generalized discrete Fourier transform* (GDFT) of the N-tuple $S^N := (s_0, s_1, \ldots, s_{N-1})$ corresponding to the N-periodic sequence S (see [6]). The GDFT is an important tool in the paper [8] of the authors in which the expected value of the linear complexity of random N-periodic sequences is determined. By shifting this problem from the time domain to the frequency domain via the GDFT, the problem becomes more manageable, so that in particular a conjecture of Rueppel [10, p. 52] on this expected value can be settled. One of the principal aims of the present paper is to extend this result in [8] to multisequences (see Theorem 1).

For an integer $0 \leqslant j \leqslant n-1$, let the integer $0 \leqslant d \leqslant n-1$ be an element of the cyclotomic coset C_j of j modulo n, where here and in the following cyclotomic cosets will be considered relative to powers of q, unless stated explicitly otherwise. This is equivalent to $d \equiv jq^b \bmod n$ for some integer $b \geqslant 0$. Then it can easily be seen that

$$(S^N)^{[k]}(\alpha^d) = ((S^N)^{[k]}(\alpha^j))^{q^b}.$$

Consequently, if we have h different cyclotomic cosets modulo n, then the GDFT is uniquely determined by h columns, one column for each cyclotomic coset. Furthermore, if c_j is the cardinality of the cyclotomic coset of j, then the entries in the column of α^j are elements of the extension field $F_{q^{c_j}}$ (cf. [8]). Hence the GDFT of an arbitrary N-tuple has a specific form, which we will call *GDFT form*. As pointed out in [8], there is a bijective correspondence between the matrices in GDFT form and the N-periodic sequences.

2. The linear complexity and the generalized discrete Fourier transform for multisequences

Consider t periodic sequences $S_1, S_2, \ldots, S_t$ with terms in F_q, i.e., a multisequence. We can assume w.l.o.g. that they have the common period N. The *joint linear complexity* $L(S_1, S_2, \ldots, S_t)$ is the least order of a linear recurrence relation that $S_1, S_2, \ldots, S_t$ satisfy simultaneously. Clearly $L(S_1, S_2, \ldots, S_t) \leqslant N$. Since the F_q-linear spaces F_q^t and F_{q^t} are isomorphic, the given multisequence can also be identified with a single sequence having its terms in the extension field F_{q^t}.

The joint linear complexity of t N-periodic sequences with terms in F_q can also be interpreted as the F_q-linear complexity of a corresponding N-periodic sequence $\mathscr{S}$

with terms in F_{q^t}, which is the least order of a linear recurrence relation in F_q that $\mathscr{S}$ satisfies (cf. [1, pp. 83–85]). For $N = p^v n$ with $\gcd(n,p) = 1$ we have $x^N - 1 = (x^n - 1)^{p^v}$, and the canonical factorization of $x^n - 1$ in $F_q[x]$ is given by

$$x^n - 1 = \prod_{r=1}^{h} f_r(x) \quad \text{with} \quad f_r(x) = \prod_{j \in D_r} (x - \alpha^j), \tag{2}$$

where $D_1, \ldots, D_h$ are the different cyclotomic cosets modulo n relative to powers of q and α is a primitive nth root of unity in some extension field of F_q. If the partition of the residue class ring modulo n into cyclotomic cosets modulo n relative to powers of q^t is the same, then the canonical factorization of $x^n - 1$ in $F_{q^t}[x]$ is again given by (2). Due to Eq. (1) and the subsequent considerations, in this case, the F_q-linear complexity and the conventional linear complexity of a sequence $\mathscr{S}$ with terms in F_{q^t} are the same, and the joint linear complexity of t N-periodic sequences $S_1, S_2, \ldots, S_t$ with terms in F_q is just the linear complexity of the corresponding sequence $\mathscr{S}$ with terms in F_{q^t}.

Proposition 2. *Let $N = p^v n$ with $p = \operatorname{char} F_q$, $v \geqslant 0$, and $\gcd(n,p) = 1$, and let l be the multiplicative order of q in $\mathbf{Z}_n^*$, the reduced residue class group modulo n. Then the F_q-linear complexity and the conventional linear complexity of an N-periodic sequence $\mathscr{S}$ with terms in F_{q^t} are the same if and only if $\gcd(l,t) = 1$.*

Proof. If $\gcd(l,t) \neq 1$, then the multiplicative order of q^t in $\mathbf{Z}_n^*$, which is the maximal cardinality of a cyclotomic coset modulo n relative to powers of q^t, is smaller than the multiplicative order of q in $\mathbf{Z}_n^*$. Let conversely $\gcd(l,t) = 1$. We have to show that for any integer $0 < j < n$ the cardinality of the cyclotomic coset of $j \bmod n$ relative to powers of q is equal to the cardinality of the cyclotomic coset of j modulo n relative to powers of q^t. Suppose l_1 and l_2 are the least positive integers such that $jq^{l_1} \equiv j \bmod n$ and $jq^{tl_2} \equiv j \bmod n$. Obviously, l_1 divides l and since $jq^{tl_1} \equiv j \bmod n$, we have $l_2 \leqslant l_1$. On the other hand, l_1 divides tl_2, and since $\gcd(l_1, t) = 1$, this implies that l_1 divides l_2. Hence we have $l_2 = l_1$. □

In the following, we generalize the concept of the GDFT to the case of t N-periodic sequences. We will need the GDFT for multisequences in order to extend the proof technique in [8] to multisequences. The use of the GDFT is crucial in the proof of the main result of the present paper, namely Theorem 1. Let $S_i^N(x)$ be the polynomial corresponding to the sequence S_i, $1 \leqslant i \leqslant t$, and let $f_i(x)$ be the minimal feedback polynomial of S_i. Then up to a nonzero multiplicative constant,

$$f_i(x) = \frac{x^N - 1}{\gcd(x^N - 1, S_i^N(x))}.$$

The common minimal feedback polynomial $f(x)$ of $S_1, \ldots, S_t$ is, again up to a nonzero multiplicative constant, given by

$$\begin{aligned} f(x) &= \operatorname{lcm}(f_1(x), \ldots, f_t(x)) \\ &= \operatorname{lcm}\left(\frac{x^N-1}{\gcd(x^N-1, S_1^N(x))}, \ldots, \frac{x^N-1}{\gcd(x^N-1, S_t^N(x))}\right) \\ &= \frac{x^N-1}{\gcd(x^N-1, S_1^N(x), \ldots, S_t^N(x))}. \end{aligned}$$

Therefore

$$L(S_1, \ldots, S_t) = N - \deg(\gcd(x^N-1, S_1^N(x), \ldots, S_t^N(x))).$$

To obtain the degree of $\gcd(x^N-1, S_1^N(x), \ldots, S_t^N(x))$, we consider the GDFT for all t N-tuples S_i^N corresponding to the sequences $S_i, 1 \leqslant i \leqslant t$. This leads to the following definition.

Definition 2. The generalized discrete Fourier transform of the t N-tuples $S_1^N, \ldots, S_t^N$ with elements in the finite field F_q, $N = p^v n$, $\gcd(n,p) = 1$, is defined to be the $p^v \times n$ matrix

$$\operatorname{GDFT}(S_1^N, \ldots, S_t^N) = \begin{pmatrix} S^N(1)^{\rightarrow} & S^N(\alpha)^{\rightarrow} & \ldots & S^N(\alpha^{n-1})^{\rightarrow} \\ (S^N)^{[1]}(1)^{\rightarrow} & (S^N)^{[1]}(\alpha)^{\rightarrow} & \ldots & (S^N)^{[1]}(\alpha^{n-1})^{\rightarrow} \\ \vdots & & & \\ (S^N)^{[p^v-1]}(1)^{\rightarrow} & (S^N)^{[p^v-1]}(\alpha)^{\rightarrow} & \ldots & (S^N)^{[p^v-1]}(\alpha^{n-1})^{\rightarrow} \end{pmatrix}$$

of t-tuples $(S^N)^{[k]}(\alpha^j)^{\rightarrow} := ((S_1^N)^{[k]}(\alpha^j), \ldots, (S_t^N)^{[k]}(\alpha^j))$ of Hasse derivatives, where α is any primitive nth root of unity in some extension field of F_q and $S_i^N(x)$ is the polynomial corresponding to the sequence S_i.

We adapt the concept of the Günther weight to matrices of t-tuples.

Definition 3. The Günther weight of a matrix of t-tuples is the number of its t-tuples that are nonzero or that lie below a nonzero t-tuple.

With Definitions 2 and 3 the following analog of the Günther–Blahut Theorem is evident.

Proposition 3. *The joint linear complexity $L(S_1, \ldots, S_t)$ of the N-periodic sequences $S_1, \ldots, S_t$ with terms in the finite field F_q of characteristic p, where $N = p^v n$ and $\gcd(n,p) = 1$, is the Günther weight of the GDFT of the t N-tuples $S_1^N, \ldots, S_t^N$ corresponding to the sequences $S_1, \ldots, S_t$.*

Remark 2. If $\gcd(N,p)=1$, then the GDFT of t N-tuples reduces to an N-tuple of t-tuples, which we can treat as a $t\times N$ matrix. In analogy with the case of a single sequence (cf. [3,5,11]) we will call this matrix the *discrete Fourier transform* (DFT) of t N-tuples. It is of the form

$$\mathrm{DFT}(S_1^N,S_2^N,\ldots,S_t^N)=\begin{pmatrix} S_1^N(1) & S_1^N(\alpha) & \ldots & S_1^N(\alpha^{N-1})\\ S_2^N(1) & S_2^N(\alpha) & \ldots & S_2^N(\alpha^{N-1})\\ \vdots & & & \\ S_t^N(1) & S_t^N(\alpha) & \ldots & S_t^N(\alpha^{N-1}) \end{pmatrix}.$$

Evidently, in this case the Günther weight is just the number of nonzero columns in this matrix.

It is obvious that the GDFT of t N-tuples again has a specific form and that there is a bijective correspondence between the GDFT of t N-tuples and t N-periodic sequences with terms in F_q.

3. The expected value of the joint linear complexity and the counting function $\mathcal{N}_N^t(c)$

In this section we present results on the expected value of the joint linear complexity of t random N-periodic sequences and on the counting function $\mathcal{N}_N^t(c)$, the number of t N-periodic sequences with given joint linear complexity c.

Using the relationship between the Günther weight of the GDFT for multi-sequences and the joint linear complexity (see Proposition 3), we can determine the expected value of the joint linear complexity of t random N-periodic sequences in terms of the cardinalities of the cyclotomic cosets modulo n in an analogous way as it was done for a single sequence in [8]. The underlying stochastic model is that of each t-tuple of N-periodic sequences with terms in F_q having the same probability q^{-tN}.

Theorem 1. *Let $N=p^v n$ with $p=\mathrm{char}\,F_q$, $v\geqslant 0$, and $\gcd(n,p)=1$. Let $l_1,\ldots,l_s$ be the different cardinalities of the cyclotomic cosets modulo n and ϕ_i, $1\leqslant i\leqslant s$, denote the total number of integers modulo n belonging to cyclotomic cosets modulo n with cardinality l_i. Then the expected value E_N^t of the joint linear complexity of t random N-periodic sequences with terms in F_q is given by*

$$E_N^t=N-\sum_{i=1}^{s}\frac{\phi_i(1-q^{-l_i t p^v})}{q^{l_i t}-1}.$$

Proof. Let $D_1,\ldots,D_h$ be the different cyclotomic cosets modulo n and put $m_r=|D_r|$ for $1\leqslant r\leqslant h$. By the previous discussion, E_N^t is equal to the expected value of the Günther weight $g(M)$ of a $p^v\times n$ matrix M of t-tuples in GDFT form. Furthermore, it suffices to consider the set $\mathcal{K}$ of $p^v\times h$ matrices K of t-tuples with columns $\mathbf{k}_1,\ldots,\mathbf{k}_h$, such that, for $1\leqslant r\leqslant h$, the entries of $\mathbf{k}_r$ are in $F_{q^{m_r}}^t$. For a nonzero column

$\mathbf{k}_r$ we let $u(\mathbf{k}_r)$ denote the least positive integer u such that the uth entry of $\mathbf{k}_r$ is a nonzero t-tuple. Then we have

$$g(M) = \sum_{\substack{r=1 \\ \mathbf{k}_r \neq \mathbf{0}}}^{h} m_r(p^v - u(\mathbf{k}_r) + 1).$$

Hence

$$\begin{aligned} E_N^t &= \frac{1}{q^{tN}} \sum_{K \in \mathscr{K}} \sum_{\substack{r=1 \\ \mathbf{k}_r \neq \mathbf{0}}}^{h} m_r(p^v - u(\mathbf{k}_r) + 1) \\ &= \frac{1}{q^{tN}} \sum_{r=1}^{h} \sum_{\substack{K \in \mathscr{K} \\ \mathbf{k}_r \neq \mathbf{0}}} m_r(p^v - u(\mathbf{k}_r) + 1) \\ &= \frac{p^v}{q^{tN}} \sum_{r=1}^{h} m_r \sum_{\substack{K \in \mathscr{K} \\ \mathbf{k}_r \neq \mathbf{0}}} 1 - \frac{1}{q^{tN}} \sum_{r=1}^{h} m_r \sum_{\substack{K \in \mathscr{K} \\ \mathbf{k}_r \neq \mathbf{0}}} (u(\mathbf{k}_r) - 1) =: T_1 - T_2. \end{aligned}$$

For the first term T_1 we get

$$\begin{aligned} T_1 &= \frac{p^v}{q^{tN}} \sum_{r=1}^{h} m_r(q^{m_r p^v t} - 1) q^{Nt - p^v t m_r} \\ &= p^v \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{p^v t m_r}}\right) = p^v \sum_{r=1}^{h} m_r - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v t m_r}} \\ &= N - p^v \sum_{r=1}^{h} \frac{m_r}{q^{p^v t m_r}}, \end{aligned}$$

where we used $\sum_{r=1}^{h} m_r = n$ in the last step. For the second term T_2 we have

$$\begin{aligned} T_2 &= \frac{1}{q^{tN}} \sum_{r=1}^{h} m_r \sum_{u=1}^{p^v} (u-1) \sum_{\substack{K \in \mathscr{K} \\ u(\mathbf{k}_r) = u}} 1 \\ &= \frac{1}{q^{tN}} \sum_{r=1}^{h} m_r \sum_{u=1}^{p^v} (u-1)(q^{m_r t} - 1) q^{m_r(p^v - u)t} q^{Nt - m_r t p^v} \\ &= \sum_{r=1}^{h} m_r \sum_{u=1}^{p^v} (u-1)(q^{m_r t} - 1) q^{m_r(p^v - u)t} q^{-m_r t p^v} \end{aligned}$$

$$= \sum_{r=1}^{h} m_r(q^{m_r t} - 1) \sum_{u=1}^{p^v} (u-1)(q^{-m_r t})^u$$
$$= \sum_{r=1}^{h} m_r(q^{m_r t} - 1) q^{-m_r t} \sum_{u=1}^{p^v} (u-1)(q^{-m_r t})^{u-1}$$
$$= \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{m_r t}}\right) \sum_{u=0}^{p^v-1} u(q^{-m_r t})^u.$$

By using the identity

$$\sum_{u=0}^{p^v-1} uz^u = \frac{z - p^v z^{p^v} + (p^v - 1)z^{p^v+1}}{(z-1)^2}$$

for any real number $z \neq 1$, we obtain

$$T_2 = \sum_{r=1}^{h} m_r \left(1 - \frac{1}{q^{m_r t}}\right) \frac{q^{-m_r t} - p^v q^{-m_r t p^v} + (p^v - 1)q^{-m_r t(p^v+1)}}{(q^{-m_r t} - 1)^2}$$
$$= \sum_{r=1}^{h} \frac{m_r}{q^{m_r t} - 1} (1 - p^v q^{-m_r t(p^v-1)} + (p^v - 1)q^{-m_r t p^v})$$
$$= \sum_{r=1}^{h} \frac{m_r(1 - q^{-m_r t p^v})}{q^{m_r t} - 1} - p^v \sum_{r=1}^{h} \frac{m_r}{q^{m_r t p^v}}.$$

By combining the formulas for T_1 and T_2, we get

$$E_N^t = N - \sum_{r=1}^{h} \frac{m_r(1 - q^{-m_r t p^v})}{q^{m_r t} - 1},$$

which immediately yields the desired result. □

For the case where $\gcd(N, p) = 1$, i.e., $v = 0$, the formula in Theorem 1 reduces to the following form.

Corollary 1. *Let* $\gcd(N, p) = 1$, *let* $l_1, \ldots, l_s$ *be the different cardinalities of the cyclotomic cosets modulo* N, *and let* ϕ_i, $1 \leqslant i \leqslant s$, *denote the total number of integers modulo* N *belonging to cyclotomic cosets modulo* N *with cardinality* l_i. *Then the expected value* E_N^t *of the joint linear complexity of* t *random* N*-periodic sequences with terms in* F_q *is given by*

$$E_N^t = N - \sum_{i=1}^{s} \frac{\phi_i}{q^{l_i t}}.$$

Remark 3. The formulas in Theorem 1 and Corollary 1 are of the same form as the formulas in [8] for the expected value of the linear complexity of a single random N-periodic sequence over the extension field F_{q^t}. But in the latter case the values of ϕ_i

and l_i result from the cyclotomic cosets modulo n relative to powers of q^t. In general, the cyclotomic cosets modulo n are different if we consider them relative to powers of q, respectively q^t. As pointed out in Proposition 2, we have equality if and only if $\gcd(l,t)=1$, where l is the multiplicative order of q in the reduced residue class group $\mathbf{Z}_n^*$.

The following lower bounds on E_N^t are easily derived from the above formulas for E_N^t. These lower bounds show clearly that E_N^t is, in general, very close to N (note that it is trivial that $E_N^t \leqslant N$). Thus, for multisequences we also have the phenomenon conjectured by Rueppel [10, p. 52] for single sequences, namely that E_N^t tends to be close to N.

Corollary 2. *If $N=p^v n$ with $p=\operatorname{char} F_q$, $v\geqslant 0$, and $\gcd(n,p)=1$, then the expected value E_N^t of the joint linear complexity of t random N-periodic sequences with terms in F_q satisfies*

$$E_N^t > N - \frac{n}{q^t-1}.$$

For $v=0$ we get the improved bound

$$E_N^t \geqslant \left(1-\frac{1}{q^t}\right)N.$$

Proof. With the notation in Theorem 1, we have

$$\sum_{i=1}^{s}\frac{\phi_i(1-q^{-l_i t p^v})}{q^{l_i t}-1} < \sum_{i=1}^{s}\frac{\phi_i}{q^{l_i t}-1} \leqslant \frac{1}{q^t-1}\sum_{i=1}^{s}\phi_i = \frac{n}{q^t-1}.$$

Thus, the first lower bound on E_N^t follows from Theorem 1. If $v=0$, then

$$\sum_{i=1}^{s}\frac{\phi_i}{q^{l_i t}} \leqslant \frac{1}{q^t}\sum_{i=1}^{s}\phi_i = \frac{N}{q^t},$$

and so the second lower bound follows from Corollary 1. □

For several families of integers n we are able to specify the cardinalities of the cyclotomic cosets modulo n. Thus, for certain types of period lengths N we can determine the expected value E_N^t of the joint linear complexity of t random N-periodic sequences with terms in F_q as an explicit function of N, t, and q by means of Theorem 1 and Corollary 1. Furthermore, using the concept of GDFT, in some of those cases the determination of the counting function $\mathcal{N}_N^t(c)$ reduces to an easy combinatorial problem. In the remainder of this section we will give some examples.

N prime, different from p:

Suppose $l\geqslant 2$ is the multiplicative order of q in the prime field F_N. Then besides the coset $\{0\}$ we have $(N-1)/l$ cyclotomic cosets modulo N of cardinality l. Due to

Corollary 1 the expected value E_N^t is given by

$$E_N^t = N - \frac{N-1}{q^{lt}} - \frac{1}{q^t}.$$

Furthermore, each DFT is uniquely determined by $(N-1)/l+1$ columns, one column for each cyclotomic coset, and the Günther weight $g(M)$ of a matrix M in DFT form is of the form

$$g(M) = rl + i, \quad 0 \leqslant r \leqslant (N-1)/l \quad \text{and} \quad i \in \{0,1\}.$$

Using the equivalence between $\mathcal{N}_N^t(c)$ and the number of matrices in DFT form with given Günther weight c, we can determine the counting function $\mathcal{N}_N^t(c)$ by combinatorial arguments (see [7] for the case of a single N-periodic sequence).

Corollary 3. *Let N be a prime with $\gcd(N,q)=1$ and let $l \geqslant 2$ be the multiplicative order of q in the finite field F_N. Then the number $\mathcal{N}_N^t(c)$ of t N-periodic sequences with terms in F_q and joint linear complexity c is given by*

$$\mathcal{N}_N^t(rl+i) = (q^t-1)^i \binom{(N-1)/l}{r} (q^{lt}-1)^r, \quad i \in \{0,1\},\ 0 \leqslant r \leqslant \frac{N-1}{l}.$$

In all other cases we have $\mathcal{N}_N^t(c) = 0$.

For some further cases in which we know the cardinalities of the cyclotomic cosets, the expected value of the joint linear complexity of t random N-periodic sequences immediately follows from Theorem 1, respectively Corollary 1. Moreover, with similar combinatorial arguments as in the previously considered case we get analogous results on the counting function $\mathcal{N}_N^t(c)$ for some of these further cases. Since the calculations are analogous to the case of a single N-periodic sequence (see [8]), we just present the results on the expected value E_N^t and the counting function $\mathcal{N}_N^t(c)$.

$N = p^v$:

Corollary 4. *Let $N = p^v$, $p = \operatorname{char} F_q$. Then the expected value E_N^t of the joint linear complexity of t random N-periodic sequences with terms in F_q is given by*

$$E_N^t = N - \frac{1}{q^t-1}\left(1 - \frac{1}{q^{tN}}\right).$$

For the counting function $\mathcal{N}_N^t(c)$ we have

$$\mathcal{N}_N^t(0) = 1 \quad \textit{and} \quad \mathcal{N}_N^t(c) = (q^t-1)q^{t(c-1)} \textit{ for } 1 \leqslant c \leqslant N.$$

Moreover, in this case the factorization of $x^N - 1$ is given by $(x-1)^{p^v}$ over any extension field F_{q^t}, $t \geqslant 1$. Thus, the F_q-linear complexity of an N-periodic sequence $\mathcal{S}$

with terms in F_{q^t} is just its conventional linear complexity.

$q = 2, N = 2^n - 1, n$ prime:

Corollary 5. *Suppose $N = 2^n - 1, n$ prime. Then the expected value E_N^t of the joint linear complexity of t random N-periodic binary sequences is given by*

$$E_N^t = (N-1)\left(1 - \frac{1}{2^{nt}}\right) + \frac{2^t - 1}{2^t}.$$

For the number $\mathcal{N}_N^t(c)$ of t N-periodic binary sequences with joint linear complexity c we have

$$\mathcal{N}_N^t(a_0 + a_1 n) = (2^t - 1)^{a_0} \binom{(N-1)/n}{a_1} (2^{tn} - 1)^{a_1}$$

$$\text{for } a_0 \in \{0, 1\} \quad \text{and} \quad 0 \leqslant a_1 \leqslant (N-1)/n.$$

In all other cases we have $\mathcal{N}_N^t(c) = 0$.

Since the order n of 2 in $\mathbf{Z}_N^*$, the reduced residue class group modulo N, is prime, the conventional linear complexity of an N-periodic sequence $\mathcal{S}$ with terms in F_{q^t} equals its F_q-linear complexity if and only if the degree t of the extension field is not a multiple of n (see Proposition 2).

$N = p^v n, n$ prime different from p:

Corollary 6. *Let $N = p^v n$, $p = \operatorname{char} F_q$, n a prime different from p. Let l be the multiplicative order of q in the prime field F_n. Then the expected value E_N^t of the joint linear complexity of t random N-periodic sequences with terms in F_q is given by*

$$E_N^t = N - \frac{1}{q^t - 1}\left(1 - \frac{1}{q^{tp^v}}\right) - \frac{n-1}{q^{tl} - 1}\left(1 - \frac{1}{q^{tlp^v}}\right).$$

We consider $\mathcal{N}_N^t(c)$ just for the case where q generates the multiplicative group of the prime field F_n, and additionally we suppose that $p^v < n - 1$.

Corollary 7. *Let $N = p^v n$, n prime, and let q be a primitive element of the finite field F_n. If $p^v < n - 1$, then the number $\mathcal{N}_N^t(c)$ of t N-periodic sequences $S_1, \ldots, S_t$ with terms in F_q and $L(S_1, \ldots, S_t) = c$ is given by*

$$\mathcal{N}_N^t(r(n-1)) = (q^{t(n-1)} - 1) q^{t(n-1)(r-1)} \text{ for all } r \text{ with } 1 \leqslant r \leqslant p^v,$$

$$\mathcal{N}_N^t(0) = 1$$

and

$$\mathcal{N}_N^t(r(n-1) + s) = (q^t - 1) q^{t(s-1)} \mathcal{N}_N^t(r(n-1)) \quad \text{for } 1 \leqslant r, s \leqslant p^v.$$

In all other cases we have $\mathcal{N}_N^t(c) = 0$.

Acknowledgments

This research was initiated during a visit of the first author to the National University of Singapore. He wishes to thank the Institute for Mathematical Sciences for hospitality and financial support.

References

[1] C. Ding, G. Xiao, W. Shan, The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science, Vol. 561, Springer, Berlin, 1991.
[2] H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, J. Reine Angew. Math. 175 (1936) 50–54.
[3] D. Jungnickel, Finite Fields: Structure and Arithmetics, Bibliographisches Institut, Mannheim, 1993.
[4] R. Lidl, H. Niederreiter, Finite Fields, Addison-Wesley, Reading, MA, 1983.
[5] J.L. Massey, S. Serconek, A Fourier transform approach to the linear complexity of nonlinearly filtered sequences, in: Y.G. Desmedt (Ed.), Advances in Cryptology—Crypto '94, Lecture Notes in Computer Science, Vol. 839, Springer, Berlin, 1994, pp. 332–340.
[6] J.L. Massey, S. Serconek, Linear complexity of periodic sequences: a general theory, in: N. Koblitz (Ed.), Advances in Cryptology—CRYPTO '96, Lecture Notes in Computer Science, Vol. 1109, Springer, Berlin, 1996, pp. 358–371.
[7] W. Meidl, H. Niederreiter, Linear complexity, k-error linear complexity, and the discrete Fourier transform, J. Complexity 18 (2002) 87–103.
[8] W. Meidl, H. Niederreiter, On the expected value of the linear complexity and the k-error linear complexity of periodic sequences, IEEE Trans. Inform. Theory 48 (2002) 2817–2825.
[9] H. Niederreiter, Some computable complexity measures for binary sequences, in: C. Ding, T. Helleseth, H. Niederreiter (Eds.), Sequences and their Applications, Springer, London, 1999, pp. 67–78.
[10] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.
[11] R.A. Rueppel, Stream ciphers, in: G.J. Simmons (Ed.), Contemporary Cryptology: The Science of Information Integrity, IEEE Press, New York, 1992, pp. 65–134.
[12] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, Inform. and Comput. 84 (1990) 207–239.
[13] C.P. Xing, Multi-sequences with almost perfect linear complexity profile and function fields over finite fields, J. Complexity 16 (2000) 661–675.