On the calculation of the linear complexity of periodic sequences

Hassan Aly, Radwa Marzouk, and Wilfried Meidl

Abstract. Based on a result of Hao Chen in 2006 we present a general procedure how to reduce the determination of the linear complexity of a sequence over a finite field $\mathbb{F}_q$ of period un to the determination of the linear complexities of u sequences over $\mathbb{F}_q$ of period n. We apply this procedure to some classes of periodic sequences over a finite field $\mathbb{F}_q$ obtaining efficient algorithms to determine the linear complexity.

1. Introduction

Let $S = s_0, s_1, s_2, \cdots$ be a sequence with terms in the finite field $\mathbb{F}_q$ of q elements. For a positive integer N, the sequence S is said to be N-periodic if $s_{i+N} = s_i$ for all $i \geq 0$. Since an N-periodic sequence is determined by the terms of one period, we can use the notation $S^N = (s_0, s_1, \cdots, s_{N-1})^\infty$ to completely describe S. An N-periodic sequence over $\mathbb{F}_q$ satisfies a linear recursion given by

$$s_{i+d} + c_1 s_{i+d-1} + \cdots + c_d s_i = 0, \quad i = 0, 1, \ldots \tag{1}$$

where $c_t \in \mathbb{F}_q$ for $t = 1, \ldots, d$ and $c_d \neq 0$. The positive integer d is called the order of the linear recursion in (1), the corresponding polynomial

$$f(X) = X^d + c_1 X^{d-1} + \cdots + c_{d-1} X + c_d \in \mathbb{F}_q[X]$$

is called a *characteristic polynomial* of S. The *linear complexity* $L(S)$ of the sequence S is the smallest order among all linear recursions for S, the corresponding characteristic polynomial is called the *minimal polynomial* of S.

The linear complexity of a periodic sequence is considered as a primary measure of its randomness and plays an important role in applications of the sequence in cryptography and communication. The *generating polynomial* corresponding to the N-periodic sequence S is defined as

$$S(X) = s_0 + s_1 X + s_2 X^2 + \cdots + s_{N-1} X^{N-1}.$$

It is well-known (see [**5**, Lemma 8.2.1]) that then the minimal polynomial of S is $(X^N - 1)/\gcd(S(X), X^N - 1)$, and the linear complexity $L(S)$ of S is given by

$$L(S) = N - \deg(\gcd(S(X), X^N - 1)), \tag{2}$$

where $\deg(f(X))$ is the degree of the polynomial $f(X)$.

The linear complexity of an N-periodic sequence S can be determined by the well-known Berlekamp-Massey algorithm [**8**] in $O(N^2)$ elementary operations,

where only $2L$ consecutive terms of the sequence are needed if $L(S) = L$. For various classes of period length N faster algorithms have been presented in the literature that determine the linear complexity of N-periodic sequences. Games and Chan [**6**] presented a fast algorithm to determine the linear complexity of a periodic binary sequence of period $N = 2^v$. Ding [**3**] generalized this algorithm to p^v-periodic sequences over the finite field $\mathbb{F}_{p^m}$ for a prime p. Blackburn [**1**] presented a method for up^v-periodic sequences over a finite field $\mathbb{F}_{p^m}$, p prime, which can be seen as a generalization of both, the Games-Chan algorithm and the discrete Fourier transform (see [**7**, Sect. 6.8], [**16**]). In [**19**] a fast algorithm for q^v-periodic sequences over $\mathbb{F}_p$ for two primes p, q such that p is a primitive root modulo q^2 was introduced. In [**18**] this algorithm has been generalized to an algorithm for $p^w q^v$-periodic sequences over $\mathbb{F}_p$ for two primes p, q such that p is a primitive root modulo q^2.

In [**2**] Chen showed how to reduce the calculation of the linear complexity of a un-periodic sequence over a finite field $\mathbb{F}_{p^m}$ to the calculation of the linear complexities of u sequences over $\mathbb{F}_{p^m}$ with period n under the condition that $u|(p^m - 1)$ and $\gcd(n, p^m - 1) = 1$. With a slight generalization of Chen's main theorem and using the concept of multisequences we are able to drop the condition that $u|(p^m - 1)$, i.e. we will show how to determine the linear complexity of un-periodic sequences over $\mathbb{F}_p$ from the linear complexities of u sequences over $\mathbb{F}_p$ with period n without the condition that u divides $p - 1$. This result can then be used to generate algorithms to determine the linear complexity of sequences over a finite field $\mathbb{F}_p$ for several classes of period length. As examples we discuss the construction of algorithms for $u2^v$-periodic binary sequences, u odd, and uq^v-periodic sequences over $\mathbb{F}_p$ for two primes p, q such that p is a primitive root modulo q^2. The algorithms for $u2^v$-periodic binary sequences improve the algorithms presented in [**11**].

2. Reducing period un to period n

In this section we present the theoretical background for establishing procedures to determine the linear complexity of un-periodic sequences over a finite field $\mathbb{F}_p$ when u and n are integers with $\gcd(u, p) = 1$. We remark that p need not necessarily be a prime, but the case of sequences over prime fields - e.g. binary sequences - is most interesting in applications. We will use the following lemmas.

LEMMA 2.1. *([**11**, Proposition 2]) Let S be a periodic sequence over the finite field $\mathbb{F}_{p^m}$ and suppose that all terms of S are in the subfield $\mathbb{F}_p$. If S satisfies a linear recurrence relation with coefficients in $\mathbb{F}_{p^m}$ and length L, then S also satisfies a linear recurrence relation of length at most L and coefficients exclusively in the subfield $\mathbb{F}_p$.*

LEMMA 2.2. *Let $f(X) \in \mathbb{F}_p[X]$ and b_s, b_t be two elements of an extension field $\mathbb{F}_{p^m}$ with the same minimal polynomial over $\mathbb{F}_p$. Then*

$$\deg(\gcd(f(X), 1 - (b_s^{-1}X)^n)) = \deg(\gcd(f(X), 1 - (b_t^{-1}X)^n)),$$

where the greatest common divisor is calculated in $\mathbb{F}_{p^m}[X]$.

PROOF. If b_s, b_t have the same minimal polynomial of degree $d \leq m$ over $\mathbb{F}_p$, then $b_t = b_s^{p^j}$ for some $0 \leq j \leq d - 1$. Thus the automorphism σ of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ given by $\sigma(z) = z^{p^j}$ maps b_s to b_t, and with the obvious extension of σ to the polynomial rings we have $\sigma(f(X)) = f(X)$ and $\sigma(1 - (b_s^{-1}X)^n) = 1 - (b_t^{-1}X)^n$.

The lemma follows then from the fact that $\sigma(h(X))|\sigma(k(X))$ if $h(X)|k(X)$ for two polynomials $h(X), k(X) \in \mathbb{F}_{p^m}[X]$. □

Let

$$1 - X^u = (1 - X)g_1 g_2 \cdots g_{r-1} \tag{3}$$

be the canonical factorization of $1 - X^u$ into irreducibles over the finite field $\mathbb{F}_p$, and suppose that the order m of p modulo u, i.e. the smallest integer such that $u|(p^m - 1)$, satisfies $\gcd(n, p^m - 1) = 1$. Then $\mathbb{F}_{p^m}$ contains all u distinct uth roots of unity $x_0 = 1, x_1, \ldots, x_{r-1}, x_r, \ldots x_{u-1}$, where we suppose that x_i is a root of g_i for $1 \le i \le r-1$, and since $\gcd(n, p^m - 1) = 1$ we can find a unique $b_i \in \mathbb{F}_{p^m}$ such that $b_i^n = x_i$ for all $i = 0, 1, \ldots, u-1$. We remark that also b_i is a uth root of unity. The following proposition is a generalization of the main theorem in Chen [**2**]. The proof closely follows the proof in [**2**].

PROPOSITION 2.3. *Suppose $p, u, n, m, g_1, \ldots, g_{r-1}, b_0, \ldots, b_{r-1}, b_r, \ldots, b_{u-1}$ are given as above. Let $S = (s_0, s_1, \ldots, s_{un-1})^\infty$ be a un-periodic sequence over the finite field $\mathbb{F}_p$. For $i = 0, 1, \ldots, r-1$ let $S^{(i)} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{n-1}^{(i)})^\infty$ be the n-periodic sequence over $\mathbb{F}_{p^m}$ with kth term*

$$s_k^{(i)} = s_k b_i^k + s_{n+k} b_i^{n+k} + \cdots + s_{(u-1)n+k} b_i^{(u-1)n+k}, \quad 0 \le k \le n-1.$$

The linear complexity $L(S)$ of S is then given by

$$L(S) = L(S^{(0)}) + \deg(g_1)L(S^{(1)}) + \cdots + \deg(g_{r-1})L(S^{(r-1)}).$$

PROOF. We can interpret the sequence S as a sequence over the extension field $\mathbb{F}_{p^m}$ and determine the linear complexity of S over $\mathbb{F}_{p^m}$, which by Lemma 2.1 equals its linear complexity over $\mathbb{F}_p$. In order to obtain $\gcd(S(X), X^{un} - 1)$, with $S(X) = \sum_{i=0}^{un-1} s_i X^i$, we observe that with the above notations

$$1 - X^{un} = \prod_{i=0}^{u-1} (x_i - X^n) = x_1 \cdots x_{u-1}(1 - X^n) \prod_{i=1}^{u-1} (1 - (b_i^{-1}X)^n),$$

where any two distinct polynomials among the u polynomials $1 - X^n, 1 - (b_1^{-1}X)^n, \ldots, 1 - (b_{u-1}^{-1}X)^n$ are coprime in $\mathbb{F}_{p^m}[X]$. Thus

$$\gcd(S(X), 1 - X^{un}) = \gcd(S(X), 1 - X^n) \prod_{i=1}^{u-1} \gcd(S(X), (1 - (b_i^{-1}X)^n)).$$

Then by equation (2) the linear complexity of S is given by

$$\begin{aligned} L(S) &= nu - \deg(\gcd(S(X), 1 - X^n)) - \deg(\gcd(S(X), (1 - (b_1^{-1}X)^n))) - \cdots \\ &\quad - \deg(\gcd(S(X), (1 - (b_{u-1}^{-1}X)^n))) \\ &= n - \deg(\gcd(S(X), 1 - X^n)) + \\ &\quad \deg(g_1)(n - \deg(\gcd(S(X), (1 - (b_1^{-1}X)^n)))) + \ldots \\ &\quad + \deg(g_{r-1})(n - \deg(\gcd(S(X), (1 - (b_{r-1}^{-1}X)^n)))), \end{aligned}$$

where in the last step we apply Lemma 2.2.
First with $\gcd(S(X), 1 - X^n) = \gcd(S^{(0)}(X), 1 - X^n)$, where

$$S^{(0)}(X) = \textstyle\sum_{k=0}^{n-1} (s_k + s_{n+k} + \cdots + s_{(u-1)n+k}) X^k$$

we obtain that

$$n - \deg(\gcd(S(X), 1 - X^n)) = L(S^{(0)}).$$

Then for $1 \le i \le r-1$ we set

$$\gcd(S(X), 1-(b_i^{-1}X)^n) = k_i(X) \quad \text{and} \quad \gcd(S(b_iY), 1-Y^n) = h_i(Y),$$

thus $k_i(X) = h_i(b_i^{-1}X)$. With $h_i(Y) = \gcd(S^{(i)}(Y), 1-Y^n)$, where

$$S^{(i)}(Y) = \sum_{k=0}^{n-1}(s_k b_i^k + s_{n+k}b_i^{n+k} + \cdots + s_{(u-1)n+k}b_i^{(u-1)n+k})Y^k$$

we get that

$$n - \deg(\gcd(S(X), 1-(b_i^{-1}X)^n)) = L(S^{(i)}),$$

which completes the proof. □

REMARK 2.4. *If $m = 1$, then Proposition 2.3 reduces to the main theorem in* [**2**].

By the proof of Proposition 2.3 it is natural to construct the sequences $S^{(i)}$, $0 \le i \le r-1$, using the nth roots b_i of x_i. The following proposition permits to construct the sequences $S^{(i)}$ directly with the roots x_i of g_i. This will be of particular advantage in the construction of algorithms for the linear complexity.

PROPOSITION 2.5. *Let $1-X^u = (1-X)g_1g_2\cdots g_{r-1}$ be the canonical factorization of $1-X^u$ into irreducibles over the finite field $\mathbb{F}_p$, let $x_0 = 1$ and $x_i \in \mathbb{F}_{p^m}$, $1 \le i \le r-1$, be a root of the polynomial g_i, let m be the order of p modulo u, and let n be an integer such that $\gcd(n, p^m-1) = 1$. Then also the set $\{x_0^n = 1, x_1^n, \ldots, x_{r-1}^n\}$ contains one root for each polynomial $(1-X), g_1, g_2, \ldots, g_{r-1}$. Moreover if x_i is a root of g_i and x_i^n is a root of g_j, then $\deg(g_j) = \deg(g_i)$.*

PROOF. First we remark that $gcd(n, p^m-1) = 1$ implies that x_i and x_i^n have the same order in $\mathbb{F}_{p^m}$, in particular both are uth roots of unity, hence a solution of a polynomial in (3). For an i, $1 \le i \le r-1$, let d be the degree of g_i and x_i be a root of g_i. Then all distinct roots of g_i are given by $x_i, x_i^p, \ldots, x_i^{p^{d-1}}$. Since the nth roots are unique in $\mathbb{F}_{p^m}$ the conjugates $x_i^n, (x_i^p)^n, \ldots, (x_i^{p^{d-1}})^n$ are distinct and $x_i^{p^d} = x_i$ implies $(x_i^{p^d})^n = x_i^n$. Consequently the minimal polynomials of x_i and x_i^n have the same degree, and if the two uth roots of unity x_i and x_l have different minimal polynomials, i.e. x_l is not a conjugate of x_i, then the minimal polynomials of x_i^n and x_l^n are different. This completes the proof. □

By Proposition 2.5 choosing a set $\{x_0, x_1, \ldots, x_{r-1}\}$ of solutions of the polynomials $X-1, g_1, \ldots, g_{r-1}$ and choosing a set of nth roots of solutions of the polynomials $X-1, g_1, \ldots, g_{r-1}$ is equivalent. The subsequent theorem is an immediate consequence.

THEOREM 2.6. *Suppose $p, u, n, m, g_1, \ldots, g_{r-1}, x_0, \ldots, x_{r-1}$ are given as above, and let $d_0 = 1$ and $d_i = \deg(g_i)$, $1 \le i \le r-1$. Let $S = (s_0, s_1, \ldots, s_{un-1})^\infty$ be a un-periodic sequence over the finite field $\mathbb{F}_p$. For $i = 0, 1, \ldots, r-1$ let $S^{(i)} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{n-1}^{(i)})^\infty$ be the n-periodic sequence over $\mathbb{F}_{p^{d_i}}$ with kth term*

$$s_k^{(i)} = s_k x_i^k + s_{n+k}x_i^{n+k} + \cdots + s_{(u-1)n+k}x_i^{(u-1)n+k}, \quad 0 \le k \le n-1.$$

The linear complexity $L(S)$ of S is then given by

$$L(S) = L(S^{(0)}) + \deg(g_1)L(S^{(1)}) + \cdots + \deg(g_{r-1})L(S^{(r-1)}).$$

EXAMPLE 2.7. *Let S be the 63-periodic binary sequence with generating polynomial $1+X+X^6+X^9+X^{10}+X^{15}=(X^6+X+1)(X^9+1)$. With equation (2) we see that $L(S)=48$. The factorization of X^7-1 over $\mathbb{F}_2$ is $X^7-1=(X+1)(X^3+X+1)(X^3+X^2+1)=g_0g_1g_2$. Straightforwardly one obtains the all zero sequence for $S^{(0)}$, thus $\deg(\gcd(S^{(0)},X^9-1))=9$. If $\alpha:=x_1$ is a root of g_1, then $\alpha+1:=x_2$ is a root of g_2. The generating polynomials of $S^{(1)}$ and $S^{(2)}$ are $S^{(1)}(X)=(\alpha^2+\alpha+1)X^6+X+\alpha^2+1$ and $S^{(2)}(X)=(\alpha^2+1)X^6+(\alpha^2+\alpha+1)X+\alpha^2$. With $\gcd(X^9-1,S^{(1)}(X))=1$ and $\deg(\gcd(X^9-1,S^{(2)}(X)))=\deg((\alpha^2+\alpha)X^2+(\alpha^2+\alpha+1)X+\alpha^2+\alpha)=2$ by Theorem 2.6 we in fact obtain $L(S)=1\cdot 0+3\cdot 9+3\cdot 7=48$.*

An obvious drawback in the application of Theorem 2.6 is that the calculations have to be shifted into a (probably large) extension field of $\mathbb{F}_p$. Following the ideas in [**11**] we may overcome this disadvantage by considering multisequences.

Consider m periodic sequences $S_1,S_2,\ldots,S_m$ over a finite field $\mathbb{F}_p$ and assume w.l.o.g. that they have common period N. The *joint linear complexity* $L(S_1,S_2,\ldots,S_m)$ of $S_1,S_2,\ldots,S_m$ is the least order of a linear recurrence relation with coefficients in $\mathbb{F}_p$ that $S_1,S_2,\ldots,S_m$ satisfy simultaneously. Similarly the *joint minimal polynomial* of $S_1,S_2,\ldots,S_m$ is the unique monic polynomial of minimal degree which is a characteristic polynomial of $S_1,S_2,\ldots,S_m$ simultaneously. Clearly, if $f_1(X),f_2(X),\ldots,f_m(X)$ are the minimal polynomials of the sequences $S_1,S_2,\ldots,S_m$, respectively, then the joint minimal polynomial $f(X)$ of $S_1,S_2,\ldots,S_m$ is given by

$$f(X)=\operatorname{lcm}(f_1(X),f_2(X),\ldots,f_m(X)). \tag{4}$$

Since the $\mathbb{F}_p$-linear spaces $\mathbb{F}_p^m$ and $\mathbb{F}_{p^m}$ are isomorphic, an m-fold multisequence can also be identified with a single sequence $\mathcal{S}$ having its terms in the extension field $\mathbb{F}_{p^m}$. If $s_k^{(r)}\in\mathbb{F}_p$ denotes the kth term of the rth sequence S_r, $1\le r\le m$, and $\{\beta_1,\beta_2,\ldots,\beta_m\}$ is a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$, then the kth term of $\mathcal{S}$ is given by $\sigma_k=\sum_{r=1}^m\beta_r s_k^{(r)}$. In this interpretation we call S_r the *component sequence of $\mathcal{S}$ to the basis element β_r*.

The joint linear complexity of m N-periodic sequences over $\mathbb{F}_p$ can also be interpreted as the $\mathbb{F}_p$-linear complexity of the corresponding N-periodic sequence $\mathcal{S}$ over $\mathbb{F}_{p^m}$, which is the least order of a linear recurrence relation with coefficients in $\mathbb{F}_p$ that $\mathcal{S}$ satisfies (cf. [**5**, pp. 27], [**4**, pp. 83–85]).
In some cases the conventional linear complexity of $\mathcal{S}$ is significantly smaller than the $\mathbb{F}_p$-linear complexity of $\mathcal{S}$. For a comparison of conventional linear complexity and $\mathbb{F}_p$-linear complexity of sequences over $\mathbb{F}_{p^m}$ we refer to [**10, 13, 14**]. The next proposition [**12**, Proposition 2] provides a condition when we have always equality.

PROPOSITION 2.8. *Let $N=c^vn$ with $c=char(\mathbb{F}_p)$, $v\ge 0$, and $\gcd(n,p)=1$, and let l be the multiplicative order of p in $\mathbb{Z}_n^*$, the reduced residue class group modulo n. Then the $\mathbb{F}_p$-linear complexity and the conventional linear complexity of any N-periodic sequence $\mathcal{S}$ with terms in $\mathbb{F}_{p^m}$ are the same if and only if $\gcd(l,m)=1$.*

We will now use the concept of multisequences to show how to determine the linear complexity of a un-periodic sequence over $\mathbb{F}_p$ from the linear complexities of u sequences over $\mathbb{F}_p$ of period n. Differently to the result of Hao Chen [**2**] the

condition that $u|(p-1)$ is not needed. The theorem will then be utilized to construct efficient procedures for determining the linear complexity.

THEOREM 2.9. *Let p be a prime power, u, n be two integers, let $n = c^v n_1, c = \mathrm{char}(\mathbb{F}_p)$, $\gcd(p, n_1) = 1$, let m be the order of p modulo u and l be the order of p modulo n_1, and suppose that $1 - X^u = (1 - X)g_1 g_2 \cdots g_{r-1}$ is the canonical factorization of $1 - X^u$ into irreducibles over the finite field $\mathbb{F}_p$ with $\deg(g_0) = \deg(1 - X) = 1$ and $\deg(g_i) = d_i$, $1 \le i \le r - 1$. Let $S = (s_0, s_1, \ldots, s_{un-1})^\infty$ be a un-periodic sequence over the finite field $\mathbb{F}_p$, assume that $\gcd(n, p^m - 1) = 1$ and $\gcd(l, m) = 1$. For $x_0 = 1$ and a root $x_i \in \mathbb{F}_{p^{d_i}}$ of g_i, $1 \le i \le r - 1$, let $S^{(i)} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{n-1}^{(i)})^\infty$ be the n-periodic sequence over $\mathbb{F}_{p^{d^i}}$ with kth term*

$$s_k^{(i)} = s_k x_i^k + s_{n+k} x_i^{n+k} + \cdots + s_{(u-1)n+k} x_i^{(u-1)n+k}, \quad 0 \le k \le n - 1. \tag{5}$$

For a given basis $\{\beta_1, \beta_2, \ldots, \beta_{d_i}\}$ of $\mathbb{F}_{p^{d_i}}$ over $\mathbb{F}_p$ let $S_j^{(i)}$, $0 \le i \le r - 1$ and $1 \le j \le d_i$, denote the component sequence of $S^{(i)}$ to the basis element β_j. The linear complexity $L(S)$ of S is then given by

$$L(S) = \sum_{i=0}^{r-1} \deg(g_i) L(S_1^{(i)}, S_2^{(i)}, \ldots, S_{d_i}^{(i)}). \tag{6}$$

PROOF. By Theorem 2.6 the linear complexity of S is given by

$$L(S) = L(S^{(0)}) + \deg(g_1) L(S^{(1)}) + \cdots + \deg(g_{r-1}) L(S^{(r-1)}),$$

where the sequences $S^{(i)}$, $0 \le i \le r - 1$, are determined as in equation (5). Since we suppose that $\gcd(l, m) = 1$ by Proposition 2.8 we know that for $0 \le i \le r - 1$ the $\mathbb{F}_p$-linear complexity and the $\mathbb{F}_{p^{d_i}}$-linear complexity of the sequence $S^{(i)}$ are the same. Equivalently the linear complexity of $S^{(i)}$, $0 \le i \le r - 1$, equals the joint linear complexity of the component sequences $S_1^{(i)}, S_2^{(i)}, \ldots, S_{d_i}^{(i)}$. □

REMARK 2.10. *If the condition $\gcd(l, m) = 1$ in Theorem 2.9 is not satisfied, then equation (6) does not always give the correct value of the linear complexity. For the 63-periodic binary sequence in Example 2.7 equation (6) gives 54 whereas the linear complexity is 48. The reason behind is the fact that $\gcd(X^9 - 1, S^{(2)}(X))$ over the finite field $\mathbb{F}_8$ has degree 2 and thus the sequences $S^{(2)}$ over $\mathbb{F}_8$ has linear complexity 7. Over the finite field $\mathbb{F}_2$ the polynomials $X^9 - 1$ and $S^{(2)}(X)$ are relatively prime and thus the $\mathbb{F}_2$-linear complexity, i.e. the joint linear complexity of the corresponding component sequences is 9.*

3. Construction of linear complexity algorithms

In this section we will show how to utilize Theorem 2.9 to establish efficient algorithms for determining the linear complexity. In the first subsection we will discuss how to set up component sequences for a given integer u. The construction of algorithms will be presented in the second subsection.

3.1. Obtaining the component sequences. In order to be able to apply Theorem 2.9 we need a procedure to find the component sequences $S_j^{(i)}$, $0 \le i \le r - 1, 1 \le j \le d_i$, given the sequence S. As we will see, the procedure only depends on u (and the field) and not on n, but for every u the set of component sequences looks different. Therefore the procedure has to be performed once for every u. We

describe the procedure at the cases $u = 3, 5$ for binary sequences and $u = 13$ for ternary sequences. At first we have to fix some notations where we restrict ourselves to the case that $\mathbb{F}_p$ is a prime field. The general case is analogous.

Let $S = (s_0, s_1, \ldots, s_{un-1})^\infty$ be a un-periodic sequence over the prime field $\mathbb{F}_p$, then we define the n-periodic sequence $T = (t_0, t_1, \ldots, t_{n-1})^\infty$ by

$$t_k = s_k + s_{k+n} + s_{k+2\cdot n} + \cdots + s_{k+(u-1)n},\ 0 \le k \le n-1. \tag{7}$$

For a divisor d of u and a set $\Omega = \{\Omega_1, \ldots, \Omega_{p-1}\}$ of distinct subsets of $\{0, 1, \ldots, d-1\}$ (some of the subsets may be the empty set), we define the un-periodic sequence $S_\Omega^{[d]} = (s_0^\Omega, s_1^\Omega, \ldots, s_{un-1}^\Omega)^\infty$ over $\mathbb{F}_p$ by

$$s_k^\Omega = \begin{cases} cs_k & : \ k \bmod d \in \Omega_c, \\ 0 & : \ k \bmod d \notin \Omega_c \text{ for all } 1 \le c \le p-1. \end{cases}$$

We then define the n-periodic p-ary sequence $T_\Omega^{[d]} = (t_0^\Omega, t_1^\Omega, \ldots, t_{n-1}^\Omega)^\infty$ by

$$t_k^\Omega = s_k^\Omega + s_{k+n}^\Omega + s_{k+2\cdot n}^\Omega + \cdots + s_{k+(u-1)n}^\Omega,\ 0 \le k \le n-1.$$

3n-periodic binary sequences: With the notation above we have $m = 2$, $g_1 = X^2 + X + 1$, $x_0 = 1$ and $x_1 = \alpha$ is a root of g_1. As basis of $\mathbb{F}_4$ over $\mathbb{F}_2$ we may take the set $\{\beta_1 = 1 = x_0, \beta_2 = \alpha = x_1\}$.
Since $d_0 = 1$ and $x_0 = 1$, the sequence $S^{(0)}$ defined as in Theorem 2.3 is binary, and precisely the n-periodic binary sequence T described in (7) (in the notation of Theorem 2.9 the sequence T is also the component sequence $S_1^{(0)}$ of $S^{(0)}$ to $\beta_1 = 1$). Since $d_2 = 2$ the sequence $S^{(1)}$ has terms in $\mathbb{F}_4$. In order to identify the component sequences of $S^{(1)}$ to the basis elements 1 and α we observe that $x_1^k = 1$ if $k \equiv 0 \bmod 3$, $x_1^k = \alpha$ if $k \equiv 1 \bmod 3$ and $x_1^k = \alpha + 1$ if $k \equiv 2 \bmod 3$. Consequently the terms s_k of S with $k \equiv 1 \bmod 3$ do not contribute to the component sequence of $S^{(1)}$ to the basis element 1, and the terms s_k with $k \equiv 0 \bmod 3$ do not contribute to the component sequence of $S^{(1)}$ to the basis element α. Therefore we obtain the sequences

$$T_{\Omega(1)} \text{ and } T_{\Omega(\alpha)} \text{ with } \Omega(1) = \{\{0, 2\}\} \text{ and } \Omega(\alpha) = \{\{1, 2\}\}$$

for the component sequences of $S^{(1)}$ to the basis elements 1 and α, respectively.

7n-periodic binary sequences: In this case $m = 3$, $X^7 - 1 = g_0 g_1 g_2 = (X - 1)(X^3 + X + 1)(X^3 + X^2 + 1)$, $d_0 = 1, d_1 = d_2 = 3$, and the set $\{1, \alpha, \alpha^2\}$, where α is a root of g_1 is a basis of $\mathbb{F}_8$ over $\mathbb{F}_2$. We can choose the roots α of g_1 and $\alpha^3 = \alpha + 1$ of g_2 for x_1 and x_2, respectively, both having multiplicative order 7. With $x_0 = 1$ we obtain the sequence T as before with equation (7). Since $x_1^0 = 1, x_1^1 = \alpha, x_1^2 = \alpha^2, x_1^3 = \alpha + 1, x_1^4 = \alpha^2 + \alpha, x_1^5 = \alpha^2 + \alpha + 1, x_1^6 = \alpha^2 + 1$, the component sequences $T_{\Omega^{(1)}(1)}^{[7]}$, $T_{\Omega^{(1)}(\alpha)}^{[7]}$, $T_{\Omega^{(1)}(\alpha^2)}^{[7]}$ of $S^{(1)}$ to the basis elements $1, \alpha, \alpha^2$ are described by the sets

$$\Omega^{(1)}(1) = \{\{0, 3, 5, 6\}\}, \Omega^{(1)}(\alpha) = \{\{1, 3, 4, 5\}\} \text{ and } \Omega^{(1)}(\alpha^2) = \{\{2, 4, 5, 6\}\}.$$

With $x_2^0 = 1, x_2^1 = \alpha + 1, x_2^2 = \alpha^2 + 1, x_2^3 = \alpha^2, x_2^4 = \alpha^2 + \alpha + 1, x_2^5 = \alpha, x_2^6 = \alpha^2 + \alpha$ we obtain $T_{\Omega^{(2)}(1)}^{[7]}$, $T_{\Omega^{(2)}(\alpha)}^{[7]}$, $T_{\Omega^{(2)}(\alpha^2)}^{[7]}$ with

$$\Omega^{(2)}(1) = \{\{0, 1, 2, 4\}\}, \Omega^{(2)}(\alpha) = \{\{1, 4, 5, 6\}\} \text{ and } \Omega^{(2)}(\alpha^2) = \{\{2, 3, 4, 6\}\}$$

for the component sequences of $S^{(2)}$ to the basis elements $1, \alpha$ and α^2, respectively.

13n-periodic ternary sequences: In this case $m = 3$ and $X^{13}-1 = g_0g_1g_2g_3g_4 = (X-1)(X^3+2X+2)(X^3+X^2+X+2)(X^3+X^2+2)(X^3+2X^2+2X+2)$, $d_0 = 1, d_i = 3, 1 \le i \le 4$. Let α be a root of $g_1 = X^3+2X+2$, then $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbb{F}_{27}$ over $\mathbb{F}_3$, and $\alpha^2, \alpha^4 = \alpha^2+\alpha, \alpha^7 = 2\alpha^2+2\alpha+1$ are roots of g_2, g_3 and g_4, respectively. Thus we can choose $x_1 = \alpha, x_2 = \alpha^2, x_3 = \alpha^4$ and $x_4 = \alpha^7$, all having multiplicative order 13.
With $x_1^0 = 1, x_1^1 = \alpha, x_1^2 = \alpha^2, x_1^3 = \alpha+1, x_1^4 = \alpha^2+\alpha, x_1^5 = \alpha^2+\alpha+1, x_1^6 = \alpha^2+2\alpha+1, x_1^7 = 2\alpha^2+2\alpha+1, x_1^8 = 2\alpha^2+2, x_1^9 = \alpha+2, x_1^{10} = \alpha^2+2\alpha, x_1^{11} = 2\alpha^2+\alpha+1, x_1^{12} = \alpha^2+2$ we obtain $T^{[13]}_{\Omega^{(1)}(1)}$, $T^{[13]}_{\Omega^{(1)}(\alpha)}$, $T^{[13]}_{\Omega^{(1)}(\alpha^2)}$ with

$$\begin{aligned}\Omega^{(1)}(1) &= \{\{0,3,5,6,7,11\},\{8,9,12\}\},\\ \Omega^{(1)}(\alpha) &= \{\{1,3,4,5,9,11\},\{6,7,10\}\},\\ \Omega^{(1)}(\alpha^2) &= \{\{2,4,5,6,10,12\},\{7,8,11\}\}\end{aligned}$$

for the component sequences of $S^{(1)}$ to the basis elements $1, \alpha$ and α^2, respectively. Similarly the component sequences of $S^{(2)}$ are determined by the sets

$$\begin{aligned}\Omega^{(2)}(1) &= \{\{0,3,8,9,10,12\},\{4,6,11\}\},\\ \Omega^{(2)}(\alpha) &= \{\{2,7,8,9,11,12\},\{3,5,10\}\},\\ \Omega^{(2)}(\alpha^2) &= \{\{1,2,3,5,6,9\},\{4,10,12\}\},\end{aligned}$$

the component sequences of $S^{(3)}$ are determined by the sets

$$\begin{aligned}\Omega^{(3)}(1) &= \{\{0,4,5,6,8,11\},\{2,3,12\}\},\\ \Omega^{(3)}(\alpha) &= \{\{1,4,6,10,11,12\},\{5,8,9\}\},\\ \Omega^{(3)}(\alpha^2) &= \{\{1,3,7,8,9,11\},\{2,5,6\}\},\end{aligned}$$

and finally the component sequences of $S^{(4)}$ are determined by the sets

$$\begin{aligned}\Omega^{(4)}(1) &= \{\{0,1,6,9,10,12\},\{3,5,11\}\},\\ \Omega^{(4)}(\alpha) &= \{\{2,5,6,8,9,10\},\{1,7,12\}\},\\ \Omega^{(4)}(\alpha^2) &= \{\{4,7,8,10,11,12\},\{1,3,9\}\}.\end{aligned}$$

3.2. Determining the linear complexity. Theorem 2.9 shows how to reduce the determination of the linear complexity of a *un*-periodic sequence over a finite field $\mathbb{F}_p$ to the determination of the linear complexities of u sequences over $\mathbb{F}_p$ with period n. In principal n, u can be any integers satisfying the conditions of Theorem 2.9. For some classes of period length n, linear complexity algorithms are known that are much faster than the Berlekamp-Massey algorithm that works for arbitrary period lengths. In this section we point out how to obtain algorithms for determining the linear complexity by combining Theorem 2.9 with the Games-Chan algorithm [**6**], and with the algorithm by Xiao et *al.* in [**19**].

u2^v-periodic binary sequences: It is obvious that for any odd u and $n = 2^v$, $v \ge 1$, the conditions of Theorem 2.9 are satisfied. As observed in [**11**, Proposition 4] the joint linear complexity $L(S_1, S_2, \ldots, S_m)$ of m parallel 2^v-periodic binary sequences $S_1, S_2, \ldots, S_m$ is given by $\max(L(S_1), L(S_2), \ldots, L(S_m))$. Therefore with Theorem 2.9 we obtain the following corollary.

COROLLARY 3.1. *For an odd integer u let m be the order of 2 modulo u, let $1-X^u = (1-X)g_1g_2\cdots g_{r-1}$ be the canonical factorization of $1-X^u$ into irreducibles*

over $\mathbb{F}_2$ *with* $d_0 = 1$ *and* $d_i = \deg(g_i)$, $1 \le i \le r-1$, *and let* $x_0 = 1$ *and* x_i, $1 \le i \le r-1$, *be roots of the polynomials* g_i, $1 \le i \le r-1$, *respectively. For a* $u2^v$*-periodic binary sequence* $S = (s_0, s_1, \ldots, s_{u2^v-1})^\infty$ *and* $0 \le i \le r-1$ *let* $S^{(i)} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{2^v-1}^{(i)})^\infty$ *be the* 2^v*-periodic sequence over* $\mathbb{F}_{2^{d_i}}$ *with* k*th term*

$$s_k^{(i)} = s_k x_i^k + s_{2^v+k} x_i^{2^v+k} + \cdots + s_{(u-1)2^v+k} x_i^{(u-1)2^v+k}, \quad 0 \le k \le 2^v - 1,$$

and for a given basis $\{\beta_1, \beta_2, \ldots, \beta_{d_i}\}$ *of* $\mathbb{F}_{2^{d_i}}$ *over* $\mathbb{F}_2$ *let* $T_j^{(i)}$, $0 \le i \le r-1$ *and* $1 \le j \le d_i$, *denote the component sequence of* $S^{(i)}$ *to the basis element* β_j. *Then the linear complexity* $L(S)$ *of* S *is given by*

$$L(S) = \sum_{i=0}^{r-1} \deg(g_i) \max(L(T_1^{(i)}), L(T_2^{(i)}), \ldots, L(T_{d_i}^{(i)})).$$

Example $u = 3$*:*
Using Corollary 3.1 and the result on component sequences in Section 3.1, with the notation introduced above we obtain

$$L(S) = L(T) + 2\max(L(T^{[3]}_{\{\{0,2\}\}}), L(T^{[3]}_{\{\{1,2\}\}}))$$

for the linear complexity $L(S)$ of a $3 \cdot 2^v$-periodic binary sequence S. Thus the determination of the linear complexity of S is reduced to applying the Games-Chan algorithm to $u = 3$ easy to generate 2^v-periodic binary sequences.

Example $u = 7$*:*
With Corollary 3.1 and our results on component sequences in Section 3.1, the linear complexity $L(S)$ of a $7 \cdot 2^v$-periodic binary sequence S can be determined as

$$\begin{aligned} L(S) \quad = \quad & L(T) + 3\max(L(T^{[7]}_{\{\{0,3,5,6\}\}}), L(T^{[7]}_{\{\{1,3,4,5\}\}}), L(T^{[5]}_{\{\{2,4,5,6\}\}})) \\ & +3\max(L(T^{[7]}_{\{\{0,1,2,4\}\}}), L(T^{[7]}_{\{\{1,4,5,6\}\}}), L(T^{[5]}_{\{\{2,3,4,6\}\}})) \end{aligned}$$

by applying the Games-Chan algorithm to $u = 7$ easy to generate 2^v-periodic binary sequences.

Example $u = 5$*:*
With the same arguments and notations as before, the linear complexity $L(S)$ of a $5 \cdot 2^v$-periodic binary sequence S is given by

$$L(S) = L(T) + 4\max(L(T^{[5]}_{\{\{0,4\}\}}), L(T^{[5]}_{\{\{3,4\}\}}), L(T^{[5]}_{\{\{2,4\}\}}), L(T^{[5]}_{\{\{1,2,3,4\}\}})).$$

REMARK 3.2. *Our results improve the algorithms in* [**11**] *where the linear complexity of* $3 \cdot 2^v$*-periodic binary sequences is determined from four* 2^v*-periodic binary sequences, the linear complexity of* $5 \cdot 2^v$*-periodic binary sequences is determined from ten* 2^v*-periodic binary sequences, and the linear complexity of* $7 \cdot 2^v$*-periodic binary sequences is determined from nine* 2^v*-periodic binary sequences.*

uq^v-periodic sequences over $\mathbb{F}_p$:

For a prime p let Q_p be the set of all odd primes q for which p is a primitive root modulo q^2 (and thus p is a primitive root modulo q^n for all $n \ge 1$). Then the factorization of $X^{q^v} - 1$ in $\mathbb{F}_p[X]$ into irreducible polynomials is given by (see [**15, 19**])

$$X^{q^v} - 1 = (X-1) \prod_{n=1}^{v} \Phi_{q^n},$$

where Φ_{q^n} is the q^nth cyclotomic polynomial. The minimal polynomial of a q^v-periodic sequence S over $\mathbb{F}_p$ is then of the form (cf. [**5**, Lemma 8.2.1])

$$m(X) = (X-1)^{\delta_0} \prod_{n=1}^{v} \Phi_{q^n}^{\delta_n}, \quad \delta_n \in \{0,1\} \text{ for } n = 0,1,\ldots,v, \tag{8}$$

and thus the linear complexity of S is of the form (see also [**9**])

$$L(S) = \epsilon + (p-1)\sum_{t\in R} p^{t-1}, \quad R \subseteq \{1,2,\ldots,v\}, \epsilon \in \{0,1\}. \tag{9}$$

Note that the value of $L(S)$ uniquely determines the minimal polynomial, i.e. the subset R of $\{1,2,\ldots,v\}$ and ϵ, as the sequence of integers $1, p, p^2, \ldots, p^{v-1}$ is super-increasing. From the above considerations and equations (4), (8) and (9), the joint linear complexity of an m-fold q^v-periodic multisequence $(S_1, S_2, \ldots, S_m)$ over $\mathbb{F}_p$ can easily be obtained from the linear complexities of the sequences $S_1, S_2, \ldots, S_m$ (see also [**17**]):
Let $\mathbf{S} = (S_1, S_2, \cdots, S_m)$ be an m-fold q^v-periodic multisequence over $\mathbb{F}_p$, where $q \in Q_p$. Suppose that the linear complexity of S_i, $1 \le i \le m$, is given by

$$L(S_i) = \epsilon_i + (p-1)\sum_{t\in R_i} p^{t-1}, \quad R_i \subseteq \{1,2,\ldots,v\}, \epsilon_i \in \{0,1\}.$$

Then the joint linear complexity of $S_1, S_2, \cdots, S_m$ is given by

$$L(S_1, S_2, \cdots, S_m) = \epsilon + (p-1)\sum_{t\in R} p^{t-1},$$

where $\epsilon = \max(\epsilon_1, \ldots, \epsilon_m)$ and $R = \bigcup_{i=1}^{m} R_i$.

With Theorem 2.9 we then obtain the following corollary by which we can reduce the determination of the linear complexity of uq^v-periodic sequences over $\mathbb{F}_p$, $q \in Q_p$, to the application of the algorithm in [**19**] to u sequences over $\mathbb{F}_p$ of period q^v. We note that the conditions $\gcd(n, p^m - 1) = 1$ and $\gcd(l, m) = 1$ in Theorem 2.9 in this case reduce to $\gcd(q, p^m - 1) = 1$ and $\gcd(q(q-1), m) = 1$.

COROLLARY 3.3. *For an integer u relatively prime to p let m be the order of p modulo u, let $1 - X^u = (1-X)g_1 g_2 \cdots g_{r-1}$ be the canonical factorization of $1 - X^u$ into irreducibles over $\mathbb{F}_p$ with $d_0 = 1, d_i = \deg(g_i)$, $1 \le i \le r-1$, and let $x_0 = 1$ and x_i, $1 \le i \le r-1$, be roots of the polynomials g_i, $1 \le i \le r-1$, respectively. Suppose that $q \in Q_p$, $\gcd(q, p^m - 1) = 1$ and $\gcd(q(q-1), m) = 1$. For a uq^v-periodic sequence $S = (s_0, s_1, \ldots, s_{uq^v-1})^\infty$ over $\mathbb{F}_p$ and $0 \le i \le r-1$ let $S^{(i)} = (s_0^{(i)}, s_1^{(i)}, \ldots, s_{q^v-1}^{(i)})^\infty$ be the q^v-periodic sequence over $\mathbb{F}_{p^{d_i}}$ with kth term*

$$s_k^{(i)} = s_k x_i^k + s_{q^v+k} x_i^{q^v+k} + \cdots + s_{(u-1)q^v+k} x_i^{(u-1)q^v+k}, \quad 0 \le k \le q^v - 1,$$

and for a given basis $\{\beta_1, \beta_2, \ldots, \beta_{d_i}\}$ of $\mathbb{F}_{p^{d_i}}$ over $\mathbb{F}_p$ let $T_j^{(i)}$, $0 \le i \le r-1$ and $1 \le j \le d_i$, denote the component sequence of $S^{(i)}$ to the basis element β_j, and let the linear complexity of $T_j^{(i)}$ be given by

$$L(T_j^{(i)}) = \epsilon_{i_j} + (p-1)\sum_{t\in R_{i_j}} p^{t-1}, \quad R_{i_j} \subset \{1,2,\ldots,v\}, \epsilon_{i_j} \in \{0,1\}.$$

Then the linear complexity $L(S)$ of S is given by

$$L(S) = \sum_{i=0}^{r-1} \deg(g_i) \left(\epsilon_i + (p-1) \sum_{n \in R_i} p^{n-1} \right),$$

with $\epsilon_i = \max(\epsilon_{i_1}, \ldots, \epsilon_{i_{d_i}})$ *and* $R_i = \bigcup_{j=1}^{d_i} R_{i_j}$ *for* $i = 0, 1, \ldots, r-1$.

4. Final remarks

In this paper we showed how to reduce the calculation of the linear complexity of a *un*-periodic sequence over a finite field $\mathbb{F}_p$ to the calculation of the linear complexities of u sequences over $\mathbb{F}_p$ of period n, under the conditions that

(i) $\gcd(p^m - 1, n) = 1$ if m is the order of p modulo u,
(ii) $\gcd(l, m) = 1$ if l is the order of p modulo n_1, where $n = c^k n_1$, $c = char(\mathbb{F}_p), k \geq 0$, $\gcd(p, n_1) = 1$.

As fast algorithms for the linear complexity are known for several period lengths, our result can be used to construct fast algorithms for the linear complexity for further classes of period length. We note that as in our procedure we determine the linear complexity of a *un*-periodic sequence by applying u times an algorithm for the linear complexity of an n-periodic sequence, the performance of the procedure depends on the performance of the algorithm for n-periodic sequences. We explicitly described the construction of algorithms for binary $u2^v$-periodic sequences, u odd, and uq^v-periodic sequences over $\mathbb{F}_p$ where p and q are primes such that $q \in Q_p$. In both cases each of the algorithms work for a fixed constant u and variable v, by u times applying the known algorithms for binary 2^v-periodic sequences and q^v-periodic sequences over $\mathbb{F}_p$, respectively. As these algorithms evaluate the linear complexity in $O(n)$ operations, where $n = 2^v$ and $n = q^v$, respectively, so do our procedures.
Combining our results with the algorithm in [**3**] yields in the same way efficient algorithms for sequences over $\mathbb{F}_p$ with period up^v, $\gcd(u, p) = 1$.
With the algorithm in [**18**] for p-ary sequences of period $p^w q^v$, $v \geq 1, w \geq 0$, $q \in Q_p$, one obtains efficient algorithms for p-ary sequences with period $up^w q^v$, $v \geq 1, w \geq 0$, $q \in Q_p$, $\gcd(p^m - 1, q) = 1$, $\gcd(m, q(q-1)) = 1$, where m is the order of p modulo u. Some possible choices for p and u are then for instance $p = 2, u = 7$; $p = 3, u = 2, 11, 13, 22, \ldots$; $p = 5, u = 2, 4, 11, \ldots$; or $p = 7, u = 2, 3, 6, 9, 18, 19, \ldots$.

References

[1] Blackburn, S. R.: *A generalization of the discrete Fourier transform: Determining the minimal polynomial of a period sequence*, IEEE Transaction on Information Theory **40** (1994), no. 9, 1702–1704.

[2] Chen, H.: *A fast algorithm for determining the linear complexity of sequences over* $\mathrm{GF(p^m)}$ *with period* $2^t n$, IEEE Transaction on Information Theory **51** (2005), no. 5, 1854–1856.

[3] Ding, C.: *A fast algorithm for the determination of the linear complexity of sequences over* $\mathrm{GF(p^m)}$ *with period* p^n, in: The Stability Theory of Stream Ciphers, Lecture Notes in Computer Science **561**, Springer-Verlag, Berlin-Heidelberg, New York, 1991.

[4] Ding, C., Xiao, G., Shan, W.: *The Stability Theory of Stream Ciphers*, Lecture Notes in Computer Science **561**, Springer-Verlag, Berlin-Heidelberg, New York, 1991.

[5] Cusick, T., Ding, C., Renvall,A.: *Stream Ciphers and Number Theory*, North-Holland Mathematical Library, Elsevier, Amserdam, 2004.

[6] Games, R., Chan, A.: *A fast algorithm for determining the complexity of a binary sequence with period* 2^n, IEEE Transaction on Information Theory **29** (1983), no. 1, 144–146.

[7] Jungnickel, D.: *Finite Fields: Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.
[8] Massey, J.: *Shift-register synthesis and BCH decoding*, IEEE Transaction on Information Theory **15** (1969), no. 1, 122–127.
[9] Meidl, W.: *Linear complexity and k-error linear complexity for p^n-periodic sequences*, Coding, Cryptography and Combinatorics, Eds.: Feng, K. Q., Niederreiter, H., Xing, C. P., Birkhäuser, Basel, 2004, 227–236.
[10] Meidl, W.: *Discrete Fourier transform, joint linear complexity and generalized joint linear complexity of multisequences*, Proceedings of SETA'04, Eds.: Helleseth, T., et al., Lecture Notes in Computer Science **3486** (2005), Springer-Verlag, Berlin-Heidelberg, 101–112.
[11] Meidl, W.: *Reducing the calculation of the linear complexity of $u2^v$-periodic binary sequences to Games-Chan algorithm*, Designs, Codes and Cryptography **46** (2007), 57–65.
[12] Meidl, W., Niederreiter, H.: *The expected value of the joint linear complexity of periodic multisequences*, Journal of Complexity **19** (2003), 61–72.
[13] Meidl, W., Özbudak, F.: *Generalized joint linear complexity of linear recurring sequences*, Proceedings of SETA'08, Eds.: Golomb, S., Pott, A., Parker, M., Winterhof, A., Lecture Notes in Computer Science **5203** (2008), Springer-Verlag, Berlin-Heidelberg, 266–277.
[14] Meidl, W., Özbudak, F.: *Linear complexity over $\mathbb{F}_q$ and over $\mathbb{F}_{q^m}$ for linear recurring sequences*, Finite Fields and their Applications **15** (2009), 110–124.
[15] Rosen, H. K.: *Elementary Number Theory and its Applications*, Addison-Wesley, Reading, MA, 1988.
[16] Rueppel, R. A.: *Stream ciphers*, Contemporary Cryptology: The Science of Information Integrity, Ed.: Simmons, G. J., IEEE Press, New York, 1992, 65–134.
[17] Venkateswarlu, A.: *Studies on Error Linear Complexity Mesures for Multisequences*, Ph.D. Dissertation, National University of Singapore, 2007.
[18] Xiao, G., Wei, S.: *Fast algorithms for determining the linear complexity of period sequences*, INDOCRYPT 2002, Eds.: Menezes, A., Sarkar, P., Lecture Notes in Computer Science **2551** (2002), Springer-Verlag, Berlin-Heidelberg, 12–21.
[19] Xiao, G., Wei, S., Lam, K., Imamura, K.: *A fast algorithm for determining the linear complexity of a sequence with period p^n over* GF(q), IEEE Transaction on Information Theory **46** (2000), no. 6, 2203–2206.

Dept. of Mathematics, Faculty of Science, Cairo University, Giza 12632, Egypt

Dept. of Mathematics, Faculty of Science, Cairo University, Giza 12632, Egypt

MDBF, Sabanci University, Orhanli, Tuzla, 34956 Istanbul, Turkey