A general approach to construction and determination of the linear complexity of sequences based on cosets

Ayça Çeşmelioğlu and Wilfried Meidl

Faculty of Engineering and Natural Sciences,
Sabancı University, Tuzla, 34956, İstanbul, Turkey

Abstract. We give a general approach to N-periodic sequences over a finite field $\mathbb{F}_q$ constructed via a subgroup D of the group of invertible elements modulo N. Well known examples are Legendre sequences or the two-prime generator. For some generalizations of sequences considered in the literature and for some new examples of sequence constructions we determine the linear complexity.

1 Introduction

A sequence $S = s_0, s_1, \ldots$ with terms in a finite field $\mathbb{F}_d$ with d elements is said to be N-*periodic* if $s_i = s_{i+N}$ for all $i \geq 0$. The *linear complexity* $L(S)$ of an N-periodic sequence S over $\mathbb{F}_d$ is the smallest nonnegative integer L for which there exist coefficients $c_1, c_2, \ldots, c_L$ in $\mathbb{F}_d$ such that S satisfies the linear recurrence relation $s_i + c_1 s_{i-1} + \cdots + c_L s_{i-L} = 0$ for all $i \geq L$. If d and N are relatively prime and θ is a primitive Nth root of unity in some extension field of $\mathbb{F}_d$, and $S(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$ then

$$L(S) = N - |\{a \ : \ S(\theta^a) = 0, 0 \leq a \leq N-1\}|. \tag{1}$$

The linear complexity is considered as a primary quality measure for periodic sequences and plays an important role in applications of sequences in cryptography and communication (see for instance [13] and the references therein).

In this paper we point to a general approach to N-periodic sequences over a finite field $\mathbb{F}_d$ defined via a subgroup D of the group $\mathbb{Z}_N^*$ of the invertible elements modulo N. Well-known basic examples are the Legendre sequences and its generalizations and the two-prime generator. We describe a uniform approach to obtain results on the linear complexity for such sequence constructions that comprise also the known proofs [3–7] for the above mentioned examples. We apply this approach to some further examples of sequences and determine their linear complexity. The first example can be seen as a natural generalization of earlier constructions, the further examples are different, some - otherwise than the sequences mentioned above - are based on subgroups D of $\mathbb{Z}_N^*$ for which the factor group $\mathbb{Z}_N^*/D$ is not cyclic.

2 A general construction of sequences based on cosets

Let N be an odd integer, Δ be a divisor of $\varphi(N)$, where φ denotes Euler's totient function, and let $D = D_0$ be a subgroup of index Δ of $\mathbb{Z}_N^*$, the group of invertible elements modulo N. Denote the elements of the factor group $G = \mathbb{Z}_N^*/D_0$ by $\{D_0, D_1, \ldots, D_{\Delta-1}\}$. Naturally this defines a partition of $\mathbb{Z}_N^*$, regarding to which we will write $n \in D_j$ if $nD_0 = D_j$ for an integer $n \in \mathbb{Z}_N^*$. An N-periodic sequence $S = s_0, s_1, \ldots$ over a finite field $\mathbb{F}_d$ satisfying

$$s_n = \xi_j \text{ whenever } n \bmod N \in D_j$$

is then called a *coset sequence*. We remark that the sequence terms s_n for $\gcd(n, N) \neq 1$ have to be defined separately.
In order to obtain (almost) balanced sequences over $\mathbb{F}_d$ one may prefer to consider subgroups D_0 of index d and to assign every field element $\xi_j \in \mathbb{F}_d$ to precisely one coset D_j.

If the period $N = p$ is prime and Δ is a divisor of $p-1$, then the (only) subgroup D_0 of index Δ of $\mathbb{Z}_N^*$ is the set of Δth powers

$$D_0 = \{g^{\Delta s} \ : \ s = 0, 1, \ldots, (p-1)/\Delta - 1\} \tag{2}$$

for a primitive element g modulo p. The cosets $D_j = g^j D_0$, $0 \leq j \leq \Delta - 1$, are then called the *cyclotomic classes* of order Δ. Trivially the factor group $\mathbb{Z}_N^*/D_0$ is then cyclic.

Some well-known examples of coset sequences are the following:

Legendre sequences and its generalizations: To describe this class of sequences in its most general form we have to fix an ordering of the elements of the finite field $\mathbb{F}_d$, $d = r^t$ for a prime r. Given a basis $\{\beta_0, \beta_1, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{r^t}$ over $\mathbb{F}_r$ we fix an ordering of the elements of $\mathbb{F}_{r^t}$ by

$$\xi_j = j_0\beta_0 + j_1\beta_1 + \cdots + j_{t-1}\beta_{t-1} \tag{3}$$

if $(j_0, j_1, \ldots, j_{t-1})_r$ is the r-ary representation of the integer j. If $t = 1$ this reduces to the conventional ordering $0, 1, \ldots, r-1$ of the prime field $\mathbb{F}_r$ (with $\beta_0 = 1$).

Let $N = p$ be a prime, $\Delta = d = r^t$ a prime power divisor of $p-1$ and D_0 be the group of the dth powers modulo p. The *generalized Legendre sequence* is then the N-periodic sequence over $\mathbb{F}_d$ defined by

$$s_n = \xi_j \text{ if } n \bmod p \in D_j, \quad \text{and} \quad s_n = 0 \text{ if } n \equiv 0 \bmod p. \tag{4}$$

For $d = 2$ the sequence (4) is known as the classical Legendre sequence, its linear complexity is determined in [5]. In [6] and [4] the linear complexity of (4) is presented for d prime and for $d = r^t$, r prime and $\gcd(t, r) = 1$.

Hall's sextic residue sequence: Let $N = p$ be prime congruent 1 modulo 6, $D_0, \ldots, D_5$ be the cyclotomic classes of order 6 defined as in (2). The N periodic binary coset sequence given by

$$s_n = \begin{cases} 1 & : \quad n \bmod N \in D_0 \cup D_1 \cup D_3, \\ 0 & : \quad \text{otherwise} \end{cases}$$

is called *Hall's sextic residue sequence* (see [10] for its linear complexity).

Two-prime generator: For two odd primes p and q let D_0 be the subgroup of index 2 of $\mathbb{Z}_{pq}^*$ consisting of the elements which are either squares or nonsquares modulo both primes p and q. Denoting the two elements of the corresponding factor group by D_0 and D_1, the *two-prime generator* is the binary pq-periodic sequence given by $s_{n+pq} = s_n$ and for $0 \le n < pq$

$$s_n = j \text{ if } n \in D_j,\ s_n = 0 \text{ if } n \in Q \cup \{0\} \text{ and } s_n = 1 \text{ if } n \in P,$$

where here and in the following $P = p\mathbb{Z}_q^* = \{p, 2p, \ldots, (q-1)p\}$ and $Q = q\mathbb{Z}_p^* = \{q, 2q, \ldots, (p-1)q\}$. The linear complexity of the two-prime generator has been determined in [7] for $\gcd(p-1, q-1) = 2$. In [9] the generalization to arbitrary prime fields has been analysed.

In [1, 15] the subgroup D of $\mathbb{Z}_{pq}^*$ which consists of all elements which are a square modulo q has been used to define a pq-periodic binary sequence. As pointed out in [12] where a generalization to arbitrary prime fields was considered, these sequences essentially are only concatenations of p Legendre sequences of period q. Similar constructions leading to binary sequences of period q^m and $2q^m$ with much similarity to concatenated Legendre sequences of period q have been considered recently in [14, 16].

3 Basic results

In what follows N will always be an odd integer, d a prime power divisor of $\varphi(N)$, D_0 a subgroup of $\mathbb{Z}_N^*$ of index d, and $D_0, D_1, \ldots, D_{d-1}$ denote the cosets of D_0. If $\mathbb{Z}_N^*/D_0$ is cyclic, which always applies when d is prime, then we can suppose that $D_iD_j = D_{i+j \bmod d}$.
Let S be a coset sequence of period N over $\mathbb{F}_d$ with $s_n = \xi_j$ if $n \in D_j$. (At this position ξ_j does not necessarily refer to the ordering in (3).) The polynomial $S(x)$ corresponding to S can then be written as $S(x) = U(x) + T(x)$ with

$$U(x) = \sum_{n \in \mathbb{Z}_N \setminus \mathbb{Z}_N^*} s_n x^n \text{ and } T(x) = \sum_{j=0}^{d-1} \xi_j f_j(x) \text{ where } f_j(x) = \sum_{i \in D_j} x^i. \quad (5)$$

We collect some simple basic properties which partly had been shown in the literature for different concrete examples of coset sequences (see e.g. [4–7]). In what follows we suppose that $d = r^t$, r prime, $\gcd(N, r) = 1$, and we let θ be a primitive Nth root of unity over $\mathbb{F}_d$.

Lemma 1. (i) *If $a, \bar{a} \in D_i$ for some $0 \le i \le d-1$ then $T(\theta^{\bar{a}}) = T(\theta^a)$.*
(ii) *For all $0 \le a \le N-1$ we have $f_j(\theta^a) \in \mathbb{F}_{r^d}$, $0 \le j \le d-1$. If $d \in D_0$ then $f_j(\theta^a) \in \mathbb{F}_d$, $0 \le j \le d-1$, and $T(\theta^a) \in \mathbb{F}_d$ for all $0 \le a \le N-1$. If also $r \in D_0$ then $f_j(\theta^a) \in \mathbb{F}_r$, $0 \le j \le d-1$, for all $0 \le a \le N-1$.*

(iii) *If* $a \in D_k$ *then* $T(\theta^a) = \sum_{j=0}^{d-1} \xi_{j\ominus k} f_j(\theta)$ *where* $j \ominus k = l$ *if* $D_j = D_k D_l$ *in* $\mathbb{Z}_N^*/D_0$.
(iv) $\sum_{j=0}^{d-1} f_j(\theta) = \mu(N)$, *where* μ *denotes the Möbius function.*

Proof. (i),(ii) are straightforward, we also may refer to [4].
(iii) $T(\theta^a) = \sum_{j=0}^{d-1} \xi_j \sum_{i\in D_j} \theta^{ai} = \sum_{j=0}^{d-1} \xi_j \sum_{i\in aD_j} \theta^{i} = \sum_{j=0}^{d-1} \xi_j f_{j\oplus k}(\theta) = \sum_{j=0}^{d-1} \xi_{j\ominus k} f_j(\theta)$.
(iv) Observe that $\sum_{j=0}^{d-1} f_j(\theta) = \sum_{k\in\mathbb{Z}_N^*} \theta^k$ is the negative of the coefficient of $x^{\varphi(N)-1}$ in the Nth cyclotomic polynomial $\mathcal{Q}_N$. With $\mathcal{Q}_N = \prod_{c|N}(x^{N/c}-1)^{\mu(c)}$ (see [11, Theorem 3.27]) we obtain

$$\mathcal{Q}_N = \frac{(x^{a_1}-1)\cdots(x^{a_1}-1)}{(x^{b_1}-1)\cdots(x^{b_s}-1)} = (x^A - x^{A-a_1} + \cdots \pm 1) \ : \ (x^B - x^{B-b_1} + \cdots \pm 1),$$

where a_i, b_j run through the divisors c of N for which N/c is squarefree, we choose a_1 and b_1 to be the minimum of the a_i and b_j, respectively, and put $A = a_1 + \cdots + a_r$ and $B = b_1 + \cdots + b_s$. As obvious, $A - B = \varphi(N)$. Performing the division we then get

$$\mathcal{Q}_N = x^{\varphi(N)} \pm x^{\varphi(N)-\min(a_1,b_1)} \pm \cdots + 1,$$

where the coefficient of $x^{\varphi(N)-\min(a_1,b_1)}$ is "1" if $a_1 > b_1$ and "-1" if $a_1 < b_1$. As $\mu(N) = 0$ implies $\min(a_1, b_1) > 1$, the coefficient of $x^{\varphi(N)-1}$ in $\mathcal{Q}_N$ is zero in this case. If $\mu(N) = 1$ then $\min(a_1, b_1) = a_1 = 1$, if $\mu(N) = -1$ then $\min(a_1, b_1) = b_1 = 1$, which completes the proof. □

As generally known the possible values for the linear complexity of an N-periodic sequence over $\mathbb{F}_d$ depend on the degrees of the polynomials in the canonical factorization of $x^N - 1$ over $\mathbb{F}_d$. The following proposition indicates that for many classes of coset sequences the order of the coset D_j which contains d in the factor group $\mathbb{Z}_N^*/D_0$ decides on the possible values for the linear complexity

Proposition 1. *Let* D_0 *be a subgroup of* $\mathbb{Z}_N^*$, $G = \mathbb{Z}_N^*/D_0$, $d \in D_j$ *and let* $B = \langle D_j \rangle$ *be the subgroup of* G *generated by* D_j. *For a corresponding coset sequence over* $\mathbb{F}_d$ *let* $T(x)$ *be defined as in* (5). *If* $T(\theta^a) = 0$ *for* $a \in D_k$ *then* $T(\theta^b) = 0$ *for all* $b \in BD_k$.

Proof. Let s be the order of d modulo N, then the minimal polynomial of θ^a over $\mathbb{F}_d$ is given by $m(x) = \prod_{l=0}^{s-1}(x - \theta^{ad^l})$. Consequently if $T(\theta^a) = 0$ then $T(\theta^{ad^l}) = 0$ for $0 \le l \le s-1$. Since $B = \langle D_j \rangle = \{D_0, dD_0 = D_j, \ldots, d^{s-1}D_0\}$ (depending on the order of D_j in G elements in this set repeat), with Lemma 1(i) we have $T(\theta^b) = 0$ for all $b \in BD_k$. □

Remark 1. If $U(\theta^a) = c \in \mathbb{F}_d$ is constant for all $a \in \mathbb{Z}_N^*$ then Lemma 1(i) and consequently Proposition 1 also holds for $S(x)$.

If $\mathbb{Z}_N^*/D_0$ is cyclic (as in the sequence constructions in the literature , see [1, 4–7, 12, 15]) then we can naturally employ the ordering defined as in (3) to define

a coset sequence. Following the objective of the paper to give a general approach to N-periodic sequences constructed via subgroups D_0 of $\mathbb{Z}_N^*$ we consider further classes of factor groups that are not cyclic. We concentrate hereby on factor groups whose order is a prime power.
For an odd integer N and a prime r let D_0 be a subgroup of $\mathbb{Z}_N^*$ such that $\mathbb{Z}_N^*/D_0$ is isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$ (with the componentwise addition) for some positive integers t_i, $1 \le i \le w$. The cardinality of $\mathbb{Z}_N^*/D_0$ is then $d = r^t$ with $t = t_1 + t_2 + \ldots + t_w$, and we can easily define an N-periodic coset sequence over $\mathbb{F}_d$ which is close to be balanced.

Example. Let $N = pq$ for two odd primes p and q, let $D_0^{(p)}$ and $D_0^{(q)}$ denote the set of squares modulo p and q, and consider

$$D_0 = \{j \mid 1 \le j \le pq-1, j \bmod p \in D_0^{(p)}, j \bmod q \in D_0^{(q)}\},$$

As obvious D_0 is a subgroup of $\mathbb{Z}_{pq}^*$ with $\mathbb{Z}_{pq}^*/D_0$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

For the definition of a sequence we again employ the ordering (3) of the elements of $\mathbb{F}_{r^t}$. In order to assign the elements of $\mathbb{F}_{r^t}$ to the r^t cosets of D_0 we also need an ordering of the elements of $\mathbb{Z}_N^*/D_0$. We put $\rho_0 = 0, \rho_1 = t_1, \rho_2 = t_1 + t_2, \ldots, \rho_w = \sum_{i=1}^{w} t_i = t$, and let Ψ be the isomorphism from $\mathbb{Z}_N^*/D_0$ to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$. For $0 \le j \le r^t - 1$ we then denote the coset D of D_0 by D_j for which

$$\Psi(D) = (J_1, J_2, \ldots, J_w) \text{ with } J_1 + J_2 r^{\rho_1} + J_3 r^{\rho_2} + \cdots + J_w r^{\rho_{w-1}} = j. \quad (6)$$

Based on the orderings (3), (6), N-periodic coset sequences over $\mathbb{F}_{r^t}$ with

$$s_n = \xi_j \text{ if } n \in D_j$$

can be defined. We remark that $D_k D_l = D_{k \oplus l}$ when we define

$$k \oplus l = h \text{ if } k = \sum_{i=1}^{w} K_i r^{\rho_i}, l = \sum_{i=1}^{w} L_i r^{\rho_i} \text{ and } h = \sum_{i=1}^{w} (K_i + L_i \bmod r^{t_i}) r^{\rho_i}, \quad (7)$$

according to the operation in $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$.

The following Lemma generalizes [4, Lemma 10] shown for the generalized Legendre sequence (4).

Lemma 2. *Let N be squarefree, D_0 a subgroup of $\mathbb{Z}_N^*$, $d = r^t$ a prime power with $\gcd(r, t) = 1$, and let*

1. *$\mathbb{Z}_N^*/D_0$ be a cyclic group of order d, or*
2. *$\mathbb{Z}_N^*/D_0$ be isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$ with $t_1 + \cdots + t_w = t$.*

Consider a coset sequence over $\mathbb{F}_d$ satisfying $s_n = \xi_j$ if $n \in D_j$, where ξ_j refers to the ordering (3) of the elements of $\mathbb{F}_d$, the cosets D_j are naturally ordered in case 1 and ordered as in (6) in case 2. Then $T(\theta^{a'}) \ne T(\theta^a)$ if $a' \not\equiv a \bmod D_0$.

Proof. For this proof we denote by $k \oplus l$ the addition modulo d in case 1 and the addition (7) in case 2. Let $a \in D_k$ and $a' \in D_{k'}$, let $k \ominus k' = \delta$ and suppose

that $0 \le v \le t-1$ is the smallest index in the r-ary representation of the integer $\delta = \sum_{i=0}^{t-1} \delta_i r^i$ of δ with $\delta_v \neq 0$. (We remark that in case 2 if $k = \sum_{i=1}^{w} K_i r^{\rho_i}$, $k' = \sum_{i=1}^{w} K_i' r^{\rho_i}$ and $\rho_{c-1} \le v < \rho_c$, then $K_i' = K_i$, $1 \le i < c$, but $K_c' \neq K_c$.)
Let $\xi_l = \sum_{i=0}^{t-1} l_i\beta_i$ and $\xi_{l\oplus\delta} = \sum_{i=0}^{t-1} l_i'\beta_i$. Then using the ordering of the elements of $\mathbb{F}_{r^t}$ and the property of v we get $l + \delta \equiv l \oplus \delta \equiv \sum_{i=0}^{v} l_i r^i + \delta_v r^v \bmod r^{v+1}$, thus $l_i' = l_i$ for $0 \le i \le v-1$ and $l_v' \equiv l_v + \delta_v \bmod r$.
For $0 \le j \le d-1$ we set $\xi_{j\ominus k} = \sum_{i=0}^{t-1} j_i\beta_i$ and $\xi_{j\ominus k'} = \sum_{i=0}^{t-1} j_i'\beta_i$. With Lemma 1(iii) we then obtain

$$T(\theta^{a'}) - T(\theta^a) = \sum_{j=0}^{d-1} (\xi_{j\ominus k'} - \xi_{j\ominus k}) f_j(\theta) = \sum_{j=0}^{d-1} (\xi_{j\ominus k\oplus\delta)} - \xi_{j\ominus k}) f_j(\theta)$$

$$= \sum_{j=0}^{d-1} \left(\delta_v\beta_v + \sum_{i=v+1}^{t-1} (j_i' - j_i)\beta_i \right) f_j(\theta)$$

$$= \delta_v\beta_v \sum_{j=0}^{d-1} f_j(\theta) + \sum_{j=0}^{d-1} \sum_{i=v+1}^{t-1} (j_i' - j_i)\beta_i f_j(\theta) = \mu(N)\delta_v\beta_v + \sum_{i=v+1}^{t-1} \beta_i \sum_{j=0}^{d-1} (j_i' - j_i) f_j(\theta)$$

$$= \mu(N)\delta_v\beta_v + \sum_{i=v+1}^{t-1} \Lambda_i\beta_i. \tag{8}$$

Since N is squarefree, (8) is a nontrivial linear combination of β_i, $0 \le i \le t-1$, and by Lemma 1(ii) its coefficients are in $\mathbb{F}_{r^d}$. As $\gcd(t, r) = 1$ the basis $\{\beta_0, \ldots, \beta_{t-1}\}$ of $\mathbb{F}_{r^t}$ over $\mathbb{F}_r$ is also a basis of $\mathbb{F}_{r^{td}}$ over $\mathbb{F}_{r^d}$, thus (8) is not 0. □

Corollary 1. *Let D_0 be a subgroup of prime power index $d = r^t$ of $\mathbb{Z}_N^*$, let $\mathbb{Z}_N^*/D_0$ be cyclic or isomorphic to $\mathbb{Z}_{r^{t_1}} \times \mathbb{Z}_{r^{t_2}} \times \cdots \times \mathbb{Z}_{r^{t_w}}$. Let S be a coset sequence with $s_n = \xi_j$ if $n \in D_j$ for the ordering* (3) *of the elements in $\mathbb{F}_d$, the obvious ordering of $\mathbb{Z}_N^*/D_0$ in the cyclic case, else for the ordering defined in* (6)*. If $d \in D_0$ then $T(\theta^a) = 0$ for $\varphi(N)/d$ values of $a \in \mathbb{Z}_N^*$. If $d \notin D_0$ then $T(\theta^a) \neq 0$ for all $a \in \mathbb{Z}_N^*$.*

Proof. By Lemma 2, $T(\theta^a) \neq T(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$. If $d \in D_0$ then by Lemma 1(ii), $T(\theta^a) \in \mathbb{F}_d$ for all $a \in \mathbb{Z}_N^*$, thus for exactly one integer j, $0 \le j \le d-1$, we have $T(\theta^a) = 0$ if $a \in D_j$. If $d \in D_j \neq D_0$ then the order of D_j in $\mathbb{Z}_N^*/D_0$ is greater than 1, and with Proposition 1, $T(\theta^a) = 0$ for $a \in D_k$ implies that $T(\theta^b) = 0$ for all $b \in \langle D_j\rangle D_K$ which contradicts Lemma 2. □

We remark that Corollary 1 also holds for $S(x)$ if $U(\theta^a) = c \in \mathbb{F}_d$ for all $a \in \mathbb{Z}_N^*$.

4 Examples of sequence constructions

Let $N = pq$ for two odd primes p and q. As easily seen $aP = P$ if $a \in \mathbb{Z}_{pq}^*$ or $a \in P$ (where the calculation is performed modulo N), which will be used several times in the following.

On the basis of the previous section we firstly consider two constructions of pq-periodic sequences over an arbitrary finite field $\mathbb{F}_d$.

Construction 1: Let $d = r^t$ be a power of the prime r dividing $\gcd(p-1, q-1)$, then we can consider the cyclotomic classes (2) of order d, $D_j^{(p)}$ and $D_j^{(q)}$, $0 \le j \le d-1$, for both primes p, q, respectively. We define a subgroup D_0 by

$$D_0 = \{n \ : \ n \bmod p \in D_k^{(p)} \text{ and } n \bmod q \in D_l^{(q)} \text{ for some } k, l \text{ with } k + l \equiv 0 \bmod d\}. \tag{9}$$

For simplicity we will write $n \in D_k^{(p)} \sqcap D_l^{(q)}$ if $n \bmod p \in D_k^{(p)}$ and $n \bmod q \in D_l^{(q)}$. As obvious, the factor group $\mathbb{Z}_N^*/D_0$ is cyclic, its elements D_j, $0 \le j \le d-1$, are given by

$$D_j = \bigcup_{k+l \equiv j \bmod d} (D_k^{(p)} \sqcap D_l^{(q)}). \tag{10}$$

Note that $D_i D_j = D_{i+j \bmod d}$.
For $d = 2$, this construction reduces to the classical two-prime generator, thus we may call this construction the *generalized two-prime generator*. For d being an odd prime the generalized two-prime generator was analysed in [9].

Construction 2: Let $d = r^t$ be a power of the prime r, let t_1, t_2 be integers such that $t_1 + t_2 = t$, and let p and q be primes such that $d_1 = r^{t_1}$ divides $p-1$ and $d_2 = r^{t_2}$ divides $q-1$. (To keep the contribution of p and q to the behaviour of the sequence equal, one may prefer to choose d_1, d_2 close to each other, if possible $d_1 = r^{\lfloor t/2 \rfloor}$, $d_2 = r^{\lceil t/2 \rceil}$.) We consider the cyclotomic classes of order d_1 modulo p and order d_2 modulo q, and choose D_0 as

$$D_0 = \{n \mid 1 \le n \le pq-1, n \in D_0^{(p)} \sqcap D_0^{(q)}\}, \tag{11}$$

which is a subgroup of $\mathbb{Z}_{pq}^*$. The index of D_0 is $d = r^t$ and $\mathbb{Z}_{pq}^*/D_0$ is isomorphic to $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$. We then can employ the ordering (6) for the cosets of D_0.

For both subgroups, (9) and (11), we can utilize the ordering (3) of the elements of $\mathbb{F}_d$ and define a pq-periodic sequence $S = s_0, s_1, \ldots$ over $\mathbb{F}_d$ by

$$s_n = \begin{cases} \xi_j & : \quad n \in D_j, \\ 0 & : \quad n \in Q \cup \{0\}, \\ 1 & : \quad n \in P. \end{cases} \tag{12}$$

4.1 The case $\gcd(r, t) = 1$

In the next theorem we determine the linear complexity of sequences obtained by both, Construction 1 and Construction 2. In order to be able to apply Lemma 2 and the subsequent Corollary 1 we need the condition $\gcd(r, t) = 1$.

Theorem 1. *For two odd primes p and q, and a power $d = r^t$ of the prime r with $\gcd(r, t) = 1$ let*

1. *d divide* $\gcd(p-1,q-1)$*, suppose* $d \neq 2$ *and let* D_0 *be the subgroup* (9) *of* $\mathbb{Z}_{pq}^*$*, or*
2. $d_1 = r^{t_1}$ *divide* $p-1$*,* $d_2 = r^{t_2}$ *divide* $q-1$ *for two positive integers* t_1, t_2 *with* $t = t_1 + t_2$*, suppose that* $r > 2$ *or* $t_i \geq 2$*,* $i = 1, 2$*, and let* D_0 *be the subgroup* (11) *of* $\mathbb{Z}_{pq}^*$*.*

Then the linear complexity L *of the sequence* (12) *is given by*

$$L = \begin{cases} pq - p - \frac{(p-1)(q-1)}{d} & : \quad d \in D_0 \\ pq - p & : \quad d \notin D_0. \end{cases}$$

Proof. Following (1) we have to determine the number of integers a, $0 \leq a \leq pq-1$ for which $S(\theta^a) = U(\theta^a) + T(\theta^a) = 0$ where $U(x), T(x)$ are defined as in (5), and θ is a primitive pqth root of unity in an extension field of $\mathbb{F}_d$.
We first observe that with $aP = P$ if $a \in \mathbb{Z}_{pq}^*$, we obtain $U(\theta^a) = \sum_{n \in P} \theta^{an} = \sum_{n \in P} \theta^n = U(\theta) = -1$. As a consequence, by Corollary 1 and the remark thereafter we have $S(\theta^a) \neq 0$ for all $a \in \mathbb{Z}_{pq}^*$ if $d \notin D_0$, and if $d \in D_0$ then $S(\theta^a) = 0$ for exactly $(p-1)(q-1)/d$ values for $a \in \mathbb{Z}_{pq}^*$. Hence it suffices to evaluate $S(\theta^a)$ for $a \in \mathbb{Z}_{pq} \setminus \mathbb{Z}_{pq}^*$.
First of all we see that

$$S(1) = \sum_{n \in P} 1 + \sum_{j=0}^{d-1} \xi_j \sum_{i \in D_j} 1 = (q-1) + \frac{(p-1)(q-1)}{d} \sum_{j=0}^{d-1} \xi_j = 0.$$

We finish the proof showing that $S(\theta^a) = -1$ if $a \in P$ and $S(\theta^a) = 0$ if $a \in Q$. With $aP = P$ if $a \in P$ we obtain $U(\theta^a) = -1$ as above, and $a \in Q$ implies $U(\theta^a) = \sum_{n \in P} \theta^{an} = \sum_{n \in P} 1 = q - 1 = 0$. Consequently it remains to be shown that $T(\theta^a) = \sum_{j=0}^{d-1} \xi_j f_j(\theta^a) = 0$ if $a \in P \cup Q$, where we have to distinguish between the two constructions.

Construction 1. Suppose that $b \in \mathbb{Z}_q^*$ is an element of $D_l^{(q)}$ and let $0 \leq k \leq d-1$ be the unique integer with $k + l \equiv j \bmod d$. By the Chinese remainder theorem for each of the $(p-1)/d$ elements c_i of $D_k^{(p)}$ there exists a unique integer n, $1 \leq n \leq pq-1$, with $n \equiv c_i \bmod p$, $n \equiv b \bmod q$, and by definition $n \in D_j$. Therefore if $a \in P$, then aD_j (modulo pq) runs $(p-1)/d$ times through $P = p\mathbb{Z}_q^*$. Consequently

$$f_j(\theta^a) = \sum_{i \in D_j} \theta^{ai} = \frac{p-1}{d} \sum_{n \in P} \theta^n = -\frac{p-1}{d},$$

hence $a \in P$ implies

$$T(\theta^a) = \sum_{j=0}^{d-1} \xi_j f_j(\theta^a) = -\frac{p-1}{d} \sum_{j=0}^{d-1} \xi_j. \tag{13}$$

For $a \in Q$ we similarly obtain $T(\theta^a) = -\frac{q-1}{d} \sum_{j=0}^{d-1} \xi_j$. With the assumption $d \neq 2$, the sum $\sum_{j=0}^{d-1} \xi_j$ of the elements of $\mathbb{F}_d$ vanishes, thus $T(\theta^a) = 0$ for

$a \in P \cup Q$.

Construction 2. Let $j = r^{t_1}k+\ell$ with $k = 0, 1, \cdots, r^{t_2}-1$ and $\ell = 0, 1, \cdots, r^{t_1}-1$, then

$$D_j = \{n \mid 1 \le n \le pq-1, n \in D_l^{(p)} \sqcap D_k^{(q)}\}$$

by definition. Consequently if the set D_j is reduced modulo p every element of $D_l^{(p)}$ is taken on precisely $(q-1)/r^{t_2}$ times and vice versa in D_j reduced modulo q every element of $D_k^{(q)}$ appears $(p-1)/r^{t_1}$ times. For $a \in P$ we therefore get

$$f_j(\theta^a) = \sum_{i \in D_j} \theta^{ai} = \frac{p-1}{r^{t_1}} \sum_{i \in pD_k^{(q)}} \theta^i$$

and subsequently

$$\begin{aligned} T(\theta^a) &= \sum_{k=0}^{r^{t_2}-1} \sum_{\ell=0}^{r^{t_1}-1} \frac{p-1}{r^{t_1}} \sum_{i \in pD_k^{(q)}} \theta^i \xi_{r^{t_1}k+\ell} \qquad (14) \\ &= \frac{p-1}{r^{t_1}} \sum_{k=0}^{r^{t_2}-1} \sum_{i \in pD_k^{(q)}} \theta^i \sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k+\ell}. \end{aligned}$$

Since $\xi_{r^{t_1}k+\ell} = \xi_{r^{t_1}k} + \xi_\ell$ for all $k \in \{0, 1, \cdots, r^{t_2}-1\}, \ell \in \{0, 1, \cdots, r^{t_1}-1\}$, we can write

$$\sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k+\ell} = \sum_{\ell=0}^{r^{t_1}-1} \xi_{r^{t_1}k} + \xi_\ell = \sum_{\ell=0}^{r^{t_1}-1} \xi_\ell = 0, \qquad (15)$$

where in the last step we used $r \neq 2$ or $r = 2$ and $t_1 > 1$. Hence $T(\theta^a) = 0$ for all $a \in P$.

For $a \in Q$ we obtain $T(\theta^a) = 0$ similarly if $r \neq 2$ or $r = 2$ and $t_2 > 1$. □

Remark 2. For $d = 2$ equation (13) yields $T(\theta^a) = (p-1)/2$ if $a \in P$ and similarly one then gets $T(\theta^a) = (q-1)/2$ if $a \in Q$. This leads to the formula presented in [7] for the linear complexity of the binary two-prime generator.

We observe that for Construction 2, in Theorem 1 we had to suppose that $r > 2$ or $t_i \ge 2$, $i = 1, 2$, which was used to show equation (15). However, to obtain a sequence over $\mathbb{F}_8$ with Construction 2 we have to choose $t_1 = 1$ (and $t_2 = 2$). Consequently sequences over $\mathbb{F}_8$ for Construction 2 are not covered by Theorem 1, thus have to be dealt with separately. This is accomplished in the next theorem. As basis of $\mathbb{F}_8$ over $\mathbb{F}_2$ we may choose the polynomial basis $\{1, \beta, \beta^2\}$, where β can be taken as a root of $x^3 + x + 1$.

Theorem 2. *The linear complexity of the sequence over $\mathbb{F}_8$ obtained by Construction 2 with $t_1 = 1, t_2 = 2$ and the polynomial basis $\{1, \beta, \beta^2\}$ of $\mathbb{F}_8$ over $\mathbb{F}_2$ is given by*

$$L(S) = \begin{cases} pq - p - \frac{(p-1)(q-1)}{8} & : \quad p \equiv 1 \mod 4,\ 2 \in D_0, \\ pq - p - q + 1 - \frac{(p-1)(q-1)}{8} & : \quad p \equiv 3 \mod 4,\ 2 \in D_0, \\ pq - p & : \quad p \equiv 1 \mod 4,\ 2 \notin D_0, \\ pq - p - q + 1 & : \quad p \equiv 3 \mod 4,\ 2 \notin D_0. \end{cases}$$

Proof. Since $r = 2$ and $t_1 = 1$ equation (15) now attains the value 1. Thus for equation (14) we obtain

$$T(\theta^a) = \frac{p-1}{2} \sum_{k=0}^{2^{t_2}-1} \sum_{i \in pD_k^{(q)}} \theta^i = \frac{p-1}{2} \sum_{i \in P} \theta^i = \frac{p-1}{2}.$$

As we had $U(\theta^a) = -1$ if $a \in P$ we therefore get $S(\theta^a) = (p+1)/2$ for all $a \in P$. With the observation that $8 \in D_0$ if and only if $2 \in D_0$, we obtain the assertion of the theorem. □

Remark 3. By definition of D_0 we have $2 \in D_0$ if and only if 2 is a quadratic residue modulo p and a quartic residue modulo q, or equivalently $p \equiv \pm 1 \bmod 8$ and $q \equiv -1 \bmod 8$ or $q \equiv 1 \bmod 8$ and $q = x^2 + 64y^2$ for some integers x, y. Thus one may write the statement of Theorem 2 entirely in terms of p and q.

4.2 Quaternary sequences

If $\gcd(r, t) \neq 1$ then Lemma 2 cannot be applied and the values of $S(\theta^a)$ for $a \in \mathbb{Z}_{pq}^*$ have to be determined individually. We present the results for the linear complexity of sequences defined via the subgroups (9) and (11) for the important case $d = 4$. As we will see, for the subgroup (9) the linear complexity does not rely on a predefined ordering of the elements of $\mathbb{F}_4$, whereas for the subgroup (11) it does.

Theorem 3. *Let $\eta_0, \eta_1, \eta_2, \eta_3$ be the elements of $\mathbb{F}_4$, let D_j be defined as in* (10) *for two primes $p \equiv q \equiv 1 \bmod 4$ and $d = 4$, and let S be the pq-periodic sequence over $\mathbb{F}_4$ defined by*

$$s_n = \begin{cases} \eta_j & : \quad n \in D_j, \\ 0 & : \quad n \in Q \cup \{0\}, \\ 1 & : \quad n \in P. \end{cases}$$

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

$$L(S) = \begin{cases} pq - p - \frac{(p-1)(q-1)}{4} & : \quad p \equiv q \equiv 1 \bmod 8 \text{ or } p \equiv q \equiv 5 \bmod 8, \\ pq - p & : \quad p \equiv 1 \bmod 8, q \equiv 5 \bmod 8 \text{ or} \\ & \quad\ \ p \equiv 5 \bmod 8, q \equiv 1 \bmod 8. \end{cases}$$

Proof. With Lemma 1(i) and $aP = P$ for $a \in \mathbb{Z}_{pq}^*$ we have $S(\theta^a) = S(\theta)$ for all $a \in D_0$. Defining $U(x), T(x)$ as in equation (5) we observe that again $U(\theta^a) = U(\theta) = 1$ if $a \in \mathbb{Z}_{pq}^* \cup P$ and $U(\theta^a) = 0$ if $a \in Q$. We hence restrict ourselves to the determination of $T(\theta^a)$. From $\mathbb{Z}_{pq}^*/D_0$ being cyclic we get for $a \in D_1$

$$\begin{aligned} T(\theta^a) &= \sum_{j=0}^{3} \eta_j f_j(\theta^a) = \eta_3 f_0(\theta) + \eta_0 f_1(\theta) + \eta_1 f_2(\theta) + \eta_2 f_3(\theta) \\ &= T(\theta) + (\eta_0 + \eta_3) f_0(\theta) + (\eta_0 + \eta_1) f_1(\theta) + (\eta_1 + \eta_2) f_2(\theta) + (\eta_2 + \eta_3) f_3(\theta) \\ &= T(\theta) + (\eta_0 + \eta_3)(f_0(\theta) + f_2(\theta)) + (\eta_0 + \eta_1)(f_1(\theta) + f_3(\theta)), \end{aligned}$$

since $\sum_{j=0}^{3} \eta_j = 0$. With Lemma 1(iv) we then obtain

$$T(\theta^a) = T(\theta) + \eta_0 + \eta_1 + (\eta_1 + \eta_3)(f_0(\theta) + f_2(\theta)).$$

With similar arguments one gets $T(\theta^a) = T(\theta) + \eta_0 + \eta_2$ if $a \in D_2$, and $T(\theta^a) = T(\theta) + \eta_0 + \eta_3 + (\eta_1 + \eta_3)(f_0(\theta) + f_2(\theta))$ if $a \in D_3$.
$T(\theta^a) = 0$ if $a \in P \cup Q$, thus $S(\theta^a) = 1$ if $a \in P$ and $S(\theta^a) = 0$ if $a \in Q$, follows with the proof of Theorem 1 for the general case. We distinguish two cases.
First suppose that $2 \in D_0 \cup D_2$, or equivalently $p \equiv q \bmod 8$, then $4 \in D_0$ and thus $S(\theta) \in \mathbb{F}_4$. Furthermore observe that $2 \in D_0 \cup D_2$ also implies $f_0(\theta) + f_2(\theta) \in \mathbb{F}_2$. As easily seen we then have $S(\theta^a) \neq S(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$ and we obtain the proclaimed value for the linear complexity with the usual conclusion.
Secondly suppose that $2 \in D_1 \cup D_3$, hence $4 \in D_2$. Then $S(\theta)^4 = S(\theta^4) = S(\theta) + \eta_0 + \eta_2 \neq S(\theta)$, and consequently $S(\theta) \notin \mathbb{F}_4$. On the other hand again $4 \in D_2$ implies $f_0(\theta) + f_2(\theta) \in \mathbb{F}_4$ and thus $S(\theta^a) \notin \mathbb{F}_4$ for all $a \in \mathbb{Z}_{pq}^*$, which yields the proclaimed linear complexity. □

Theorem 4. *Let $\eta_0, \eta_1, \eta_2, \eta_3$ be the elements of $\mathbb{F}_4$ and for two odd primes p, q let $D_0^{(p)}$ and $D_1^{(p)}$ ($D_0^{(q)}$, $D_1^{(q)}$) be the set of squares and nonsquares modulo p (modulo q), respectively. Let S be the pq-periodic sequence over $\mathbb{F}_4$ defined by*

$$s_n = \begin{cases} \eta_{l+2k} & : \quad n \in D_l^{(p)} \sqcap D_k^{(q)}, \\ 0 & : \quad n \in Q \cup \{0\}, \\ 1 & : \quad n \in P. \end{cases}$$

The linear complexity of S is then

$$L(S) = \begin{cases} pq - 1 - \frac{(p-1)(q-1)}{4} & : \ q \equiv 3 \bmod 4 \text{ and } p \equiv 1 \bmod 4 \text{ or} \\ & \quad p \equiv 3 \bmod 4, \eta_2 \neq \eta_0 + 1, \\ pq - p - \frac{(p-1)(q-1)}{4} & : \ q \equiv 1 \bmod 4 \text{ and } p \equiv 1 \bmod 4 \text{ or} \\ & \quad p \equiv 3 \bmod 4, \eta_2 \neq \eta_0 + 1, \\ pq - q - \frac{(p-1)(q-1)}{4} & : \ q \equiv 3 \bmod 4, p \equiv 3 \bmod 4, \eta_2 = \eta_0 + 1, \\ pq - p - q + 1 - \frac{(p-1)(q-1)}{4} & : \ q \equiv 1 \bmod 4, p \equiv 3 \bmod 4, \eta_2 = \eta_0 + 1. \end{cases}$$

Proof. With Lemma 1(i) and $aP = P$ for $a \in \mathbb{Z}_{pq}^*$ we have $S(\theta^a) = S(\theta)$ for all $a \in D_0$. From $\mathbb{Z}_{pq}^*/D_0 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, for $a \in D_1$ we obtain

$$\begin{aligned} S(\theta^a) &= \sum_{n \in P} \theta^n + \eta_0 f_1(\theta) + \eta_1 f_0(\theta) + \eta_2 f_3(\theta) + \eta_3 f_2(\theta) = S(\theta) + \eta_0(f_0(\theta) + f_1(\theta)) \\ &\quad + \eta_1(f_0(\theta) + f_1(\theta)) + \eta_2(f_2(\theta) + f_3(\theta)) + \eta_3(f_2(\theta) + f_3(\theta)) \\ &= S(\theta) + (\eta_0 + \eta_1)(f_0(\theta) + f_1(\theta)) + (\eta_2 + \eta_3)(f_2(\theta) + f_3(\theta)) \\ &= S(\theta) + (\eta_0 + \eta_1) \sum_{j=0}^{3} f_j(\theta) = S(\theta) + \eta_0 + \eta_1. \end{aligned}$$

Similarly we get $S(\theta^a) = S(\theta) + \eta_0 + \eta_2$ for $a \in D_2$ and $S(\theta^a) = S(\theta) + \eta_0 + \eta_3$ for $a \in D_3$. Hence $S(\theta^a) \neq S(\theta^{a'})$ if $a \not\equiv a' \bmod D_0$. Since $4 \in D_0$ and $U(x)$

is as in the proof of Theorem 3, with Lemma 1(ii) we have $S(\theta^a) \in \mathbb{F}_4$ when $a \in D_j, j = 0, 1, 2, 3$.
Employing that the sets D_0 and D_2 (D_1 and D_3) reduced modulo q are equal for $a \in P$ we get

$$\begin{aligned} S(\theta^a) &= \sum_{n\in P} \theta^n + (\eta_0+\eta_2) \sum_{n\in D_0} \theta^{an} + (\eta_1+\eta_3) \sum_{n\in D_1} \theta^{an} \\ &= 1 + (\eta_0+\eta_2) \sum_{n\in D_0\cup D_1} \theta^{an} = 1 + (\eta_0+\eta_2)\frac{p-1}{2} \sum_{n\in P} \theta^n \\ &= 1 + (\eta_0+\eta_2)\frac{p-1}{2}. \end{aligned}$$

In the penultimate step we used that the set $D_0 \cup D_1$ reduced modulo q contains all elements of $\mathbb{Z}_q^*$ and each element is taken on $(p-1)/2$ times.
In an analog way we obtain $S(\theta^a) = (\eta_0+\eta_1)\frac{q-1}{2}$ if $a \in Q$. The simple observation that $S(1) = 0$ completes the proof. □

We complete this section pointing out that the generalized two-prime generator (Construction 1) has favourable autocorrelation properties when d is prime (or likewise if one defines the sequence as a d-ary sequence for an arbitrary module d in an analog way, as autocorrelation is then also defined). For $d = 2$ this was shown in [8], an alternative proof using characters was presented in [2]. The methods of [2] can be applied to the case of arbitrary modules d. As far as we are aware, autocorrelation results for arbitrary modules d have not been presented, thus we give the result but omit the proof. In the following we put $\varepsilon_d = e^{2\pi\sqrt{-1}/d}$, and $\chi^{(p)}$ ($\chi^{(q)}$) shall denote the multiplicative character of order d of $\mathbb{F}_p$ ($\mathbb{F}_q$) given by $\chi^{(p)}(g^k) = \varepsilon_d^k$ if g is a primitive element of $\mathbb{F}_p$ ($\mathbb{F}_q$).

Theorem 5. *The autocorrelation of the generalized two-prime generator S with prime d is given by*

$$A(S,t) = \begin{cases} p-q+1 & : \quad t \in q\mathbb{Z}_p^*, \\ \varepsilon_d + \overline{\varepsilon_d} + q - p - 1 & : \quad t \in p\mathbb{Z}_q^*, \\ 1 + (1 - \bar{\varepsilon}\chi^{(p)}(-t)\chi^{(q)}(-t)) & : \quad t \in \mathbb{Z}_{pq}^*. \\ \quad +(1 - \varepsilon\overline{\chi^{(p)}}(t)\overline{\chi^{(q)}}(t)) & \end{cases}$$

5 Final Remarks

We consider N-periodic sequences over finite fields that are constant on the cosets of a subgroup of $\mathbb{Z}_N^*$, which can be seen as a general approach to classes of N-periodic sequences that contain well known constructions as the Legendre sequences and the two-prime generator. With this general approach one may construct and analyse various classes of sequences. We give examples of pq-periodic sequences over arbitrary finite fields and determine their linear complexity. Similar constructions can be considered and analysed (using tools from Section 2)

for other (squarefree) periods. One may use subgroups D of $\mathbb{Z}_N^*$ with index not a prime power as in the following example: For an odd prime p and a prime $q \equiv 1 \bmod 3$ we consider the cyclotomic classes of order 2 and 3, respectively, and the subgroup $D_0 = D_0^{(q)} \sqcap D_0^{(p)}$ of index 6. We define a corresponding ternary sequence S by $s_n = l + 2k \bmod 3$ if $n \in D_l^{(p)} \sqcap D_k^{(q)}$, $s_n = 0$ if $n \in Q \cup \{0\}$ and $s_n = 1$ if $n \in P$. With the above used techniques and using Proposition 1 one obtains that $L(S) = pq - p - (p-1)(q-1)/3$ if $p \equiv \pm 1 \bmod 12$ and $q = 3a^2 + b^2$ with $9|a$ or $9|(a \pm b)$, if $q = 3a^2 + b^2$ with $9 \not| a$ and $9 \not| (a \pm b)$ then $L(S) = pq - p$. This pq-periodic ternary sequence is certainly different from the ternary version of the two-prime generator and the ternary sequence constructed as in [12]. An analysis of the autocorrelation of such coset sequences, which differently to the sequences in [1, 12, 14–16] are not similar to a concatenation of Legendre sequences, may be worthwhile. There, an adaptation of the method in [8] with an adequate generalization of cyclotomic numbers seems promising. In this connection it may also be of interest to use the above considered factor group of $\mathbb{Z}_{pq}^*$ isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ to define quaternary sequences.

References

1. E. Bai, X. Liu, and G. Xiao, Linear complexity of new generalized cyclotomic sequences of order two of length pq, IEEE Trans. Inform. Theory 51 (2005), 1849–1853.
2. N. Brandstätter, A. Winterhof, Some notes on the two-prime generator of order 2, IEEE Trans. Inform. Theory 51 (2005), 3654–3657.
3. T. W. Cusick, C. Ding, and A. Renvall, Stream Ciphers and Number Theory, North-Holland Publishing Co., Amsterdam (1998).
4. Z. Dai, J. Yang, G. Gong, P. Wang, On the linear complexity of generalized Legendre sequences, Sequences and their applications (Bergen, 2001), 145–153, Discrete Math. Theor. Comput. Sci. (Lond.), Springer, London, 2002.
5. C. Ding, T. Helleseth, W. Shan, On the linear complexity of Legendre sequences, IEEE Trans. Inform. Theory 44 (1998), 1276–1278.
6. C. Ding, T. Helleseth, On cyclotomic generator of order r, Inform. Process. Letters 66 (1998), 21–25.
7. C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl. 3 (1997), 159–174.
8. C. Ding, Autocorrelation values of generalized cyclotomic sequences of order two, IEEE Trans. Inform. Theory 44 (1998), 1699–1702.
9. D. Green, L. Garcia-Perera, The linear complexity of related prime sequences, Proc. R. Soc. Lond. A 460 (2004), 487–498.
10. J.-H. Kim, H.-Y. Song, On the linear complexity of Hall's sextic residue sequences, IEEE Trans. Inform. Theory 47 (2001), 2094–2096.
11. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, Cambridge, 1986.
12. W. Meidl, Remarks on a cyclotomic sequence, Designs, Codes and Cryptography 51 (2009), 33–43.
13. H. Niederreiter, Linear complexity and related complexity measures for sequences, Progress in Cryptology - Proceedings of INDOCRYPT 2003 (T. Johansson and S. Maitra, eds.), LNCS 2904 (2003), Springer-Verlag, Berlin, pp. 1–17.

14. T. Yan, S. Li, and G. Xiao, On the linear complexity of generalized cyclotomic sequences with the period p^m, Appl. Math. Lett. 21 (2008), 187–193.
15. T. Yan, Z. Chen, and G. Xiao, Linear complexity of Ding generalized cyclotomic sequences, Journal of Shanghai University (English Edition) 11 (2007), 22–26.
16. J. Zhang, C.A. Zhao, X. Ma, Linear complexity of generalized cyclotomic sequences with length $2p^m$, AAECC 21 (2010), 93–108.