Des. Codes Cryptogr.
DOI 10.1007/s10623-008-9241-3

Remarks on a cyclotomic sequence

Wilfried Meidl

Received: 10 March 2008 / Revised: 2 September 2008 / Accepted: 2 September 2008

Abstract We analyse a binary cyclotomic sequence constructed via generalized cyclotomic classes by Bai et al. (IEEE Trans Inforem Theory 51: 1849–1853, 2005). First we determine the linear complexity of a natural generalization of this binary sequence to arbitrary prime fields. Secondly we consider k-error linear complexity and autocorrelation of these sequences and point out certain drawbacks of this construction. The results show that the parameters for the sequence construction must be carefully chosen in view of the respective application.

Keywords Cyclotomic sequence · Linear complexity · Autocorrelation · Generalized cyclotomic classes · Stream cipher

Mathematics Subject Classifications (2000) 94A55 · 94A60 · 11B50

1 Introduction

A sequence $S = s_0, s_1, \ldots$ with terms in a finite field $\mathbb{F}_d$ with d elements (or over the finite field $\mathbb{F}_d$) 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

$$s_i + c_1 s_{i-1} + \cdots + c_L s_{i-L} = 0 \quad \text{for all } i \geq L.$$

It is clear that an N-periodic sequence has at most N as its linear complexity. The *k-error linear complexity* of an N-periodic sequence is the smallest linear complexity that can be

Communicated by T. Helleseth.

W. Meidl (✉)
Sabancı University, MDBF, Orhanlı, 34956 Tuzla, Istanbul, Turkey
e-mail: wmeidl@sabanciuniv.edu

obtained by changing at most k terms of the sequence per period (see [15], and for the related even earlier defined *sphere complexity* see [9]).

The *autocorrelation* of an N-periodic sequence S over $\mathbb{F}_d$ is the complex-valued function defined by

$$A(S,t) = \sum_{n=0}^{N-1} \varepsilon_d^{s_{n+t}-s_n}, \quad 1 \le t \le N-1 \tag{1}$$

where $\varepsilon_d = e^{2\pi\sqrt{-1}/d}$. The autocorrelation measures the amount of similarity between the sequence S and a shift of S by t positions. Large linear complexity and k-error linear complexity, and small autocorrelation for all t, $1 \le t \le N-1$, are desirable features for sequences used in applications like cryptology and Quasi Monte Carlo methods (see [13,14,16]).

In [1] Bai et al. defined a binary sequence constructed via *generalized cyclotomic classes* (cf. [7]). The binary sequence considered in [18] is a modification of the sequence in [1] which permits a natural generalization to sequences over arbitrary prime fields:
Let p, q be two odd primes with $p < q$, $\gcd(p-1, q-1) = 2n$ and $e = (p-1)(q-1)/(2n)$. Let g be a common primitive root of p and q, and x an integer that satisfies $x \equiv g \bmod p$ and $x \equiv 1 \bmod q$. As shown in [17]

$$\mathbb{Z}_{pq}^* = \{g^s x^i \ : \ s = 0, 1, \ldots, e-1; i = 0, 1, \ldots, 2n-1\}$$

where $\mathbb{Z}_{pq}^*$ is the multiplicative group of the invertible elements modulo pq.

Let d be a divisor of $2n$, then we can define a partition of $\mathbb{Z}_{pq}^*$ by

$$D_0 = \{g^{dt}x^i \ : \ t = 0, 1, \ldots, e/d-1; i = 0, 1, \ldots, 2n-1\} \quad \text{and}$$
$$D_j = g^j D_0, \ 1 \le j \le d-1$$

where the multiplication is that of $\mathbb{Z}_{pq}$. In accordance with [7] we call D_j, $0 \le j \le d-1$, *generalized cyclotomic classes of order d*.

We recall that the conventional cyclotomic classes of order d modulo p and q are given by

$$D_0^{(p)} = \{g^{dt} \bmod p \ : \ t = 0, 1, \ldots, (p-1)/d-1\} \quad \text{and} \quad D_j^{(p)} = g^j D_0^{(p)}$$

for $1 \le j \le d-1$, and

$$D_0^{(q)} = \{g^{dt} \bmod q \ : \ t = 0, 1, \ldots, (q-1)/d-1\} \quad \text{and} \quad D_j^{(q)} = g^j D_0^{(q)}$$

for $1 \le j \le d-1$, respectively.
Let $R = \{0\}$, $P = \{p, 2p, \ldots, (q-1)p\}$ and $Q = \{q, 2q, \ldots, (p-1)q\}$, then we define

$$P_j = pD_j^{(q)} \quad \text{and} \quad Q_j = qD_j^{(p)}, \quad 0 \le j \le d-1,$$

and obtain a partition of $\mathbb{Z}_{pq}$ given by

$$C_0 = R \cup P_0 \cup Q_0 \cup D_0 \quad \text{and} \quad C_j = P_j \cup Q_j \cup D_j, \quad 1 \le j \le d-1.$$

For an element $k \in \mathbb{F}_p^*$ ($\mathbb{F}_q^*$) we denote by $ind_{g,d}^{(p)}(k)$ ($ind_{g,d}^{(q)}(k)$) the discrete logarithm of k in $\mathbb{F}_p^*$ ($\mathbb{F}_q^*$) modulo d relative to the basis g, i.e. $ind_{g,d}^{(p)}(k) = j$ if $(k \bmod p) \in D_j^{(p)}$. With the above definitions we can generalize the concept of discrete logarithm modulo d to the residue class ring $\mathbb{Z}_{pq}$. Let $k \in \mathbb{Z}_{pq} \backslash \{0\}$ then we define the index of k by

$$ind_{g,d}(k) = j \quad \text{if} \quad k \in C_j.$$

If the divisor d of $\gcd(p-1, q-1)$ is a prime then we can define a pq-periodic sequence $S = s_0, s_1, \ldots$ with terms in $\mathbb{F}_d$ by

$$s_i = \begin{cases} ind_{g,d}(k) & : \ i \equiv k \bmod pq \text{ for } 0 \neq k \in \mathbb{Z}_{pq} \\ 0 & : \ i \equiv 0 \bmod pq. \end{cases} \tag{2}$$

For $d = 2$ the sequence (2) coincides with the sequence considered in [18].

In this contribution we confirm a high linear complexity for the sequence (2) over arbitrary prime fields $\mathbb{F}_d$, but we also point out certain deficiencies of the construction of [1,18] when we consider k-error linear complexity and autocorrelation.

2 Linear complexity and k-error linear complexity

Let $S = s_0, s_1, \ldots$ be the pq-periodic sequence over $\mathbb{F}_d$ defined by (2), and α a primitive pqth root of unity in an extension field of $\mathbb{F}_d$. Then by Blahut's theorem (see [14, p. 77])

$$L(S) = pq - |\{j \ : \ s(\alpha^j) = 0, \ 0 \leq j \leq pq-1\}| \tag{3}$$

where

$$s(x) = s_0 + s_1 x + \cdots + s_{pq-1} x^{pq-1}. \tag{4}$$

Our first goal is to generalize the results on the linear complexity given in [18] for the binary sequence (2) to arbitrary prime fields. We start with collecting some simple facts on the above defined partition of $\mathbb{Z}_{pq}$. Some of these facts can be seen as generalizations of Lemmas 1 and 2 in [18].

Lemma 1 *(i) If $a \in D_j$ for some j, $0 \leq j \leq d-1$, then $aD_i = D_{i+j \bmod d}$, $aP = P$, $aP_i = P_{i+j \bmod d}$ and $aQ = Q$.*
(ii) If $a \in P_j$ for some j, $0 \leq j \leq d-1$, then $aP = P$, $aP_i = P_{i+j \bmod d}$ and $aQ = R$. If $a \in Q_j$ for some j, $0 \leq j \leq d-1$, then $aQ = Q$, $aQ_i = Q_{i+j \bmod d}$ and $aP = R$.
(iii) If $a \bmod p \in D_j^{(p)}$ then $aQ_i = Q_{j+i \bmod d}$.

From now on all calculations are performed in an appropriate extension field of $\mathbb{F}_d$ containing the pqth primitive root of unity α. The following lemma is straightforward.

Lemma 2 $\sum_{j \in P} \alpha^j = \sum_{j \in Q} \alpha^j = -1$, $\sum_{j \in \mathbb{Z}_{pq}^*} \alpha^j = 1$.

The next lemma generalizes [1, Lemma 2] and [18, Lemma 4]. The proof is similar as in [1]. We present the proof for the convenience of the reader.

Lemma 3 *For $j = 0, 1, \ldots, d-1$ we have*

$$\sum_{i \in D_j} \alpha^{ki} = \begin{cases} 0 & \text{if } k \in P, \\ -\frac{q-1}{d} \bmod d & \text{if } k \in Q. \end{cases}$$

Proof Since g is a primitive root modulo q and $x \equiv 1 \bmod q$ the set $D_j \bmod q$ equals the set $D_j^{(q)}$. When t ranges over $\{0, 1, \ldots, e/d-1\}$ and i ranges over $\{0, 1, \ldots, 2n-1\}$ each element of $D_j^{(q)}$ is taken on exactly $p-1$ times in $D_j \bmod q$. If $k \in P$ then $ki \equiv k(i \bmod q) \bmod pq$ and thus with $d|(p-1)$

$$\sum_{i \in D_j} \alpha^{ki} = (p-1) \sum_{i \in D_j^{(q)}} \alpha^{ki} = 0.$$

With the definition of g and x we observe that the set $D_j \bmod p$ equals the set $\{1, 2, \ldots, p-1\}$, where each element of $\{1, 2, \ldots, p-1\}$ is taken on exactly $(q-1)/d$ times in $D_j \bmod p$ when t ranges over $\{0, 1, \ldots, e/d-1\}$ and i ranges over $\{0, 1, \ldots, 2n-1\}$. If $k \in Q$ then $ki \equiv k(i \bmod p) \bmod pq$. Thus

$$\sum_{i \in D_j} \alpha^{ki} = \frac{q-1}{d} \sum_{i=1}^{p-1} \alpha^{ki} = \frac{q-1}{d} \sum_{i \in Q} \alpha^i = -\frac{q-1}{d}.$$

□

Lemma 4 *Let $s(x)$ be the polynomial defined in (4) and let α be a primitive pqth root of unity in an extension field of $\mathbb{F}_d$, then*

$$s(\alpha^k) = \begin{cases} s(\alpha) + ind_{g,d}^{(p)}(k) & \text{if } k \in \mathbb{Z}_{pq}^*, \\ \frac{(p-1)(d-1)}{2} + \sum_{i \in P} ind_{g,d}(i)\alpha^{ki} & \text{if } k \in P, \\ \sum_{i \in Q} ind_{g,d}(i)\alpha^{ki} & \text{if } k \in Q. \end{cases}$$

Proof By the definition of $s(x)$ we have

$$\begin{aligned} s(\alpha^k) &= \sum_{i=0}^{pq-1} ind_{g,d}(i)\alpha^{ki} = \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^{ki} + \sum_{i \in P} ind_{g,d}(i)\alpha^{ki} + \sum_{i \in Q} ind_{g,d}(i)\alpha^{ki} \\ &:= T_1 + T_2 + T_3. \end{aligned}$$

If $k \in \mathbb{Z}_{pq}^*$ with Lemma 1(i),(iii) we obtain $ind_{g,d}(ki) = ind_{g,d}(i) + ind_{g,d}(k)$ if $i \in \mathbb{Z}_{pq}^* \cup P$ and $ind_{g,d}(ki) = ind_{g,d}(i) + ind_{g,d}^{(p)}(k)$ if $i \in Q$. Hence with Lemma 2 we obtain for T_1

$$\begin{aligned} T_1 &= \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^{ki} = \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(ik^{-1})\alpha^i = \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^i + ind_{g,d}(k^{-1}) \sum_{i \in \mathbb{Z}_{pq}^*} \alpha^i \\ &= \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^i - ind_{g,d}(k), \quad \text{similarly for } T_2 \end{aligned}$$

$$T_2 = \sum_{i \in P} ind_{g,d}(i)\alpha^i + ind_{g,d}(k^{-1}) \sum_{i \in P} \alpha^i = \sum_{i \in P} ind_{g,d}(i)\alpha^i + ind_{g,d}(k),$$

and finally for T_3

$$T_3 = \sum_{i \in Q} ind_{g,d}(i)\alpha^i + ind_{g,d}^{(p)}(k^{-1}) \sum_{i \in P} \alpha^i = \sum_{i \in P} ind_{g,d}(i)\alpha^i + ind_{g,d}^{(p)}(k),$$

which proves the lemma for $k \in \mathbb{Z}_{pq}^*$. If $k \in P$ then

$$T_1 = \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^{ki} = \sum_{r=0}^{d-1} r \sum_{i \in D_r} \alpha^{ki} = 0 \quad \text{by Lemma 3. For } T_3 \text{ we get}$$

$$T_3 = \sum_{i \in Q} ind_{g,d}(i)\alpha^{ki} = \sum_{r=0}^{d-1} r \sum_{i \in D_r^{(p)}} \alpha^{ki} = \sum_{r=0}^{d-1} r \sum_{i \in D_r^{(p)}} 1 = \frac{(p-1)(d-1)}{2},$$

which proves the lemma for $k \in P$. If $k \in Q$ then with Lemma 3

$$T_1 = \sum_{i \in \mathbb{Z}_{pq}^*} ind_{g,d}(i)\alpha^{ki} = \sum_{r=0}^{d-1} r \sum_{i \in D_r} \alpha^{ki} = -\frac{q-1}{d} \sum_{r=0}^{d-1} r = -\frac{(q-1)(d-1)}{2}.$$

Similarly as above for T_3 in the case $k \in P$ we now obtain $T_2 = (q-1)(d-1)/2$, which completes the proof. □

Lemma 5 *(i)* $s(\alpha) \in \mathbb{F}_d$ *if and only if* d *is a* d*th power in* $\mathbb{F}_p$*, i.e.* $d \in D_0^{(p)}$.
(ii) If $k \in P$ *then* $\sum_{i \in P} ind_{g,d}(i)\alpha^{ki} \in \mathbb{F}_d$ *if and only if* $d \in D_0^{(q)}$*, and if* $k \in Q$ *then* $\sum_{i \in Q} ind_{g,d}\alpha^{ki} \in \mathbb{F}_d$ *if and only if* $d \in D_0^{(p)}$.

Proof (i) Since $s(x) \in \mathbb{F}_d[x]$ we have $s(\alpha)^d = s(\alpha^d)$ which by Lemma 4 equals $s(\alpha)$ if and only if $d \in D_0^{(p)}$.
(ii) Let $k \in P$ and put $t(\alpha) = \sum_{i \in P} ind_{g,d}(i)\alpha^{ki}$, then

$$t(\alpha)^d = t(\alpha^d) = \sum_{i \in P} ind_{g,d}(i)\alpha^{dki} = \sum_{i \in P} ind_{g,d}(id^{-1})\alpha^{ki}$$
$$= \sum_{i \in P} ind_{g,d}(i)\alpha^{ki} - ind_{g,d}^{(q)}(d) \sum_{i \in P} \alpha^{ki} = t(\alpha) - ind_{g,d}^{(q)}(d) \sum_{i \in P} \alpha^i = t(\alpha) + ind_{g,d}^{(q)}(d)$$

by Lemma $1(ii)$ and Lemma 2. Therefore $t(\alpha) \in \mathbb{F}_d$ if and only if $d \in D_0^{(q)}$. The second statement of (ii) can be shown in the same way. □

Lemma 6 *(i) Suppose that* $d \in D_0^{(q)}$ *then there exists an integer* l, $0 \le l \le d-1$, *such that* $\sum_{i \in P} ind_{g,d}(i)\alpha^{ki} = 0$ *for all* $k \in P_l$ *and* $\sum_{i \in P} ind_{g,d}(i)\alpha^{ki} \neq 0$ *for all* $k \in P_j$, $j \neq l$.
(ii) Suppose that $d \in D_0^{(p)}$ *then there exists an integer* l, $0 \le l \le d-1$, *such that* $\sum_{i \in Q} ind_{g,d}(i)\alpha^{ki} = 0$ *for all* $k \in Q_l$ *and* $\sum_{i \in Q} ind_{g,d}(i)\alpha^{ki} \neq 0$ *for all* $k \in Q_j$, $j \neq l$.

Proof Let $\kappa \in P_0$ and $k \in P$, then $ind_{g,d}(\kappa i) = ind_{g,d}(i)$ and $ind_{g,d}(ki) = ind_{g,d}(i) + ind_{g,d}(k)$ for all $i \in P$. By Lemma 5 we have

$$\sum_{j \in P} ind_{g,d}(j)\alpha^{\kappa j} = r \in \mathbb{F}_d, \quad \text{and consequently}$$
$$\sum_{i \in P} ind_{g,d}(i)\alpha^{ki} = \sum_{i \in P} ind_{g,d}(i)\alpha^{k\kappa i} = \sum_{j \in P} (ind_{g,d}(j) - ind_{g,d}(k))\alpha^{\kappa j}$$
$$= \sum_{j \in P} ind_{g,d}(j)\alpha^{\kappa j} - ind_{g,d}(k) \sum_{j \in P} \alpha^{\kappa j} = r + ind_{g,d}(k) = 0$$

if and only if $k \in P_l$ with $l = d - r$. Part *(ii)* is proved in the same way. □

We can now determine the linear complexity $L(S)$ of the sequence S defined in (2).

Theorem 1 *I. If* $d \notin D_0^{(p)}$ *and* $d \notin D_0^{(q)}$ *then*

$$L(S) = pq \quad \text{if } (p+q)/2 - 1 \not\equiv 0 \bmod d \quad \text{and}$$
$$L(S) = pq - 1 \quad \text{if } (p+q)/2 - 1 \equiv 0 \bmod d.$$

II. If $d \notin D_0^{(p)}$ *and* $d \in D_0^{(q)}$ *then*

$$L(S) = pq - \frac{q-1}{d} \quad \text{if } (p+q)/2 - 1 \not\equiv 0 \bmod d \quad \text{and}$$
$$L(S) = pq - \frac{q-1}{d} - 1 \quad \text{if } (p+q)/2 - 1 \equiv 0 \bmod d.$$

III. If $d \in D_0^{(p)}$ *and* $d \notin D_0^{(q)}$ *then*

$$L(S) = pq - \frac{q(p-1)}{d} \quad \text{if } (p+q)/2 - 1 \not\equiv 0 \bmod d \quad \text{and}$$
$$L(S) = pq - \frac{q(p-1)}{d} - 1 \quad \text{if } (p+q)/2 - 1 \equiv 0 \bmod d.$$

IV. If $d \in D_0^{(p)}$ *and* $d \in D_0^{(q)}$ *then*

$$L(S) = pq - \frac{pq-1}{d} \quad \text{if } (p+q)/2 - 1 \not\equiv 0 \bmod d \quad \text{and}$$
$$L(S) = pq - \frac{pq-1}{d} - 1 \quad \text{if } (p+q)/2 - 1 \equiv 0 \bmod d.$$

Proof We will employ Eq. 3 to determine the linear complexity of S. First of all we note that $s(1) = ((p-1)/d + (q-1)/d + (q-1)(p-1)/d)(1+2+\cdots d-1) \equiv (p+q-2)/d \cdot d(d-1)/2 \bmod d$ which vanishes modulo d if and only if $(p+q)/2 - 1 \equiv 0 \bmod d$.

If $d \notin D_0^{(p)}$ then Lemmas 4 and 5 imply that $s(\alpha^k) \neq 0$ for $k \in \mathbb{Z}_{pq}^* \cup Q$. If $d \notin D_0^{(q)}$ then $s(\alpha^k) \neq 0$ for $k \in P$. Statement I immediately follows. If $d \in D_0^{(q)}$ then by Lemma 6 we have $s(\alpha^k) = 0$ for precisely $(q-1)/d$ integers of P. This shows statement II.

If $d \in D_0^{(p)}$ then by Lemma 6 we have $s(\alpha^k) = 0$ for precisely $(p-1)/d$ integers of Q, and by Lemmas 4 and 5 exactly $(p-1)(q-1)/d$ integers $k \in \mathbb{Z}_{pq}^*$ satisfy $s(\alpha^k) = 0$. This yields statements III and IV. □

We remark that for $d = 2$ Theorem 1 reduces to [18, Theorems 1–4]

For a finite field $\mathbb{F}_p$ let $\chi_d^{(p)}$ denote the nontrivial character in $\mathbb{F}_p$ given by $\chi_d^{(p)}(\beta^k) = e^{2\pi\sqrt{-1}k/d}$ for a primitive element β of $\mathbb{F}_p$. As easily seen we then can describe the sequence $S = s_0, s_1, \ldots$ defined in (2) by $s_n = 0$ if $n \equiv 0 \bmod pq$ and

$$\varepsilon_d^{s_n} = \begin{cases} \overline{\chi_d^{(q)}(n)} & \text{if } n \bmod pq \in \mathbb{Z}_{pq}^* \\ \overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(n) & \text{if } n \bmod pq \in P \\ \overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n) & \text{if } n \bmod pq \in Q \end{cases} \tag{5}$$

where $\varepsilon_d = e^{2\pi\sqrt{-1}/d}$. We immediately observe that for $(n \bmod pq) \in \mathbb{Z}_{pq}^*$ the sequence (2) coincides with the *cyclotomic generator* $C = c_0, c_1, \ldots$ of order d and period q, which is defined by $c_n = ind_{g,d}^{(q)}(n)$ if $n \not\equiv 0 \bmod q$ and $c_n = 0$ if $n \equiv 0 \bmod q$. (We refer to [2,6,12] for an analysis of the cyclotomic generator, and to [8] for an analysis of the *Legendre sequence*, i.e. the cyclotomic generator for $d = 2$.) If p is a dth power in $\mathbb{F}_q$ then we also have $s_n = c_n$ if $n \in P$. As easily seen we additionally have $\overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n) = 1$ and therefore $s_n = c_n$ for precisely $(p-1)/d$ elements $n \in Q$. Summarizing, if p is not a dth power in $\mathbb{F}_q$ we have $s_n \neq c_n$ for precisely $q - 1 + (d-1)(p-1)/d$ integers n, $0 \leq n < pq$,

if p is a dth power in $\mathbb{F}_q$ then $s_n \neq c_n$ for only $(d-1)(p-1)/d$ integers n, $0 \leq n < pq$, and thus the sequence (2) is essentially the cyclotomic generator with period q. With the definition of the k-error linear complexity we obtain the following theorem.

Theorem 2 *If p is a dth power in $\mathbb{F}_q$ then $L_k(S) \leq q$ for $k \geq (d-1)(p-1)/d$. If p is not a dth power in $\mathbb{F}_q$ then $L_k(S) \leq q$ for $k \geq q - 1 + (d-1)(p-1)/d$.*

Theorem 2 certainly reveals a drawback of the generator in [1,18] if p and q are arbitrarily chosen, and suggests to choose a large prime for q and a small prime for p which is not a dth power in $\mathbb{F}_q$.

3 Autocorrelation

With Eqs. 1 and 5 we can derive the autocorrelation $A(S,t)$ of S using character sums. First we note that

$$A(S,t) = \varepsilon_d^{s_t} + \varepsilon_d^{s_{-t}} + \sum_{\substack{n \in \mathbb{Z}_{pq} \\ n \neq 0,\, pq-t}} \varepsilon_d^{s_{n+t}-s_n}. \tag{6}$$

For the determination of

$$T = \sum_{\substack{n \in \mathbb{Z}_{pq} \\ n \neq 0,\, pq-t}} \varepsilon_d^{s_{n+t}-s_n}$$

we have to distinguish the cases $t \in \mathbb{Z}_{pq}^*$, $t \in P$ and $t \in Q$.

Case I $t \in \mathbb{Z}_{pq}^*$: In this case with the usual convention that $\chi_d^{(p)}(0) = \chi_d^{(q)}(0) = 0$ we get

$$\begin{aligned} T = & \sum_{\substack{n \in \mathbb{Z}_{pq}{}^* \\ n+t \in \mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n \in \mathbb{Z}_{pq}^* \\ n+t \in P}} \overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} \\ & + \sum_{\substack{n \in \mathbb{Z}_{pq}^* \\ n+t \in Q}} \overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n+t)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n \in P \\ n+t \in \mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\chi_d^{(q)}(p)\overline{\chi_d^{(q)}(n)} \\ & + \sum_{\substack{n \in Q \\ n+t \in \mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\chi_d^{(p)}(q)\overline{\chi_d^{(p)}(n)} + \overline{\chi_d^{(p)}(q)}\chi_d^{(q)}(p)\chi_d^{(p)}(t)\overline{\chi_d^{(q)}(-t)} \\ & + \chi_d^{(p)}(q)\overline{\chi_d^{(q)}(p)\chi_d^{(p)}(-t)}\chi_d^{(q)}(-t) \end{aligned}$$

where the last two summands result from the fact that the equation $rp + t = sq$ has a unique integer solution r, s with $1 \leq r \leq q-1$, $1 \leq s \leq p-1$. Using [10, Lemma 7.3.7] we obtain

$$\sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} = \sum_{r=0}^{p-1}\sum_{j=0}^{q-1} \chi^{(q)}(rq+j+t)\overline{\chi^{(q)}(rq+j)}$$
$$- \sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in P}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} - \sum_{\substack{n\in P\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)}$$
$$= \sum_{r=0}^{p-1}(-1) - (-1) - (-1) = -p+2,$$

and then with straightforward calculations for the total sum T

$$T = -p+2 - \overline{\chi_d^{(q)}(p)} - \chi_d^{(q)}(p) + \overline{\chi_d^{(p)}(q)}\chi_d^{(q)}(p)\chi_d^{(p)}(t)\overline{\chi_d^{(q)}(-t)}$$
$$+ \chi_d^{(p)}(q)\overline{\chi_d^{(q)}(p)\chi_d^{(p)}(-t)}\chi_d^{(q)}(t).$$

Case II $t \in P$: In this case we have

$$T = \sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n\in P\\ n+t\in P}} \overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(n+t)\chi_d^{(q)}(p)\overline{\chi_d^{(q)}(n)}$$
$$+ \sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in Q}} \overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n+t)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n\in Q\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\chi_d^{(p)}(q)\overline{\chi_d^{(p)}(n)}.$$

With straightforward calculations we see that the last two sums vanish and obtain -1 for the second sum. For the first sum we get

$$\sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} = \sum_{r=0}^{p-1}\sum_{j=0}^{q-1} \chi^{(q)}(j+t)\overline{\chi^{(q)}(j)} - \sum_{\substack{n\in P\\ n+t\in P}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)}$$
$$= -p+1.$$

Case III $t \in Q$: Now T is given by

$$T = \sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n\in Z_{pq}^*\\ n+t\in P}} \overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(n+t)\overline{\chi_d^{(q)}(n)}$$
$$+ \sum_{\substack{n\in P\\ n+t\in\mathbb{Z}_{pq}^*}} \chi_d^{(q)}(n+t)\chi_d^{(q)}(p)\overline{\chi_d^{(q)}(n)} + \sum_{\substack{n\in Q\\ n+t\in Q}} \overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n+t)\chi_d^{(p)}(q)\overline{\chi_d^{(p)}(n)}.$$

Since $t \in Q$ we have $\chi_d^{(q)}(n+t) = \chi_d^{(q)}(n)$ and consequently the first sum equals

$$\sum_{\substack{n\in\mathbb{Z}_{pq}^*\\ n+t\in\mathbb{Z}_{pq}^*}} 1 = (p-2)(q-1).$$

For the same reason the second sum is given by

$$\overline{\chi_d^{(q)}(p)} \sum_{r=1}^{q-1} 1 = (q-1)\overline{\chi_d^{(q)}(p)}$$

and similarly for the third sum we obtain $(q-1)\chi_d^{(q)}(p)$. With simple calculations and [10, Lemma 7.3.7] we see that the fourth sum equals -1.

Combining (6) with the above results for the term T we obtain the following theorem.

Theorem 3 *The autocorrelation $A(S,t)$ of the sequence S defined by (2) is given by*

$$\begin{aligned} A(S,t) = &-p+2+\chi_d^{(q)}(t)+\overline{\chi_d^{(q)}(t)}-\chi_d^{(q)}(p)-\overline{\chi_d^{(q)}(p)} \\ &+\overline{\chi_d^{(p)}(q)}\chi_d^{(q)}(p)\chi_d^{(p)}(t)\overline{\chi_d^{(q)}(-t)}+\chi_d^{(p)}(q)\overline{\chi_d^{(q)}(p)\chi_d^{(p)}(-t)}\chi_d^{(q)}(t) \end{aligned}$$

if $t \in \mathbb{Z}_{pq}^*$,

$$A(S,t) = -p+\overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(t)+\chi_d^{(q)}(p)\overline{\chi_d^{(q)}(-t)}$$

if $t \in P$, and

$$A(S,t) = (p-2+\overline{\chi_d^{(q)}(p)}+\chi_d^{(q)}(p))(q-1)-1+\overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(t)+\chi_d^{(p)}(q)\overline{\chi_d^{(p)}(-t)}$$

if $t \in Q$.

As a corollary one immediately obtains the autocorrelation for the binary sequence considered in [1,18]. We only present the case that $p \equiv 3 \bmod 4$, $q \equiv 1 \bmod 4$ and p is a nonsquare modulo q.

Corollary 1 *If $p \equiv 3 \bmod 4$, $q \equiv 1 \bmod 4$ and p is a nonsquare modulo q, then the autocorrelation $A(S,t)$ of the binary sequence S defined by (2) for $d=2$ is given by*

$$A(S,t) = \begin{cases} -p+4+2\chi_2^{(q)}(t) & : \ t \in \mathbb{Z}_{pq}^* \\ -p-2\chi_2^{(q)}(t) & : \ t \in P \\ (p-4)(q-1)-1 & : \ t \in Q \end{cases}.$$

Theorem 3 and Corollary 1 present another downside of the generator in [1,18]. In order to obtain small values for the autocorrelation at least for almost all values of t we again have to choose p small. The autocorrelation for $t \in Q$ will always be larger than one would expect the autocorrelation to be for a truly random sequence.

Example $d=2$: If $p=3$, $q \equiv 1 \bmod 4$ and $q \equiv 2 \bmod 3$ (i.e. 3 is a nonsquare modulo q), then $A(S,t) \in \{-5,-1,3\}$ for all $1 \le t < 3q$ and $t \ne q, 2q$. For $t = q, 2q$ we have $A(S,t) = -q$.

With Theorem 1 I,II we obtain $L(S) = 3q$ if 2 is not a square modulo q and $L(S) = 3q-1$ if 2 is a square modulo q. Since we chose q such that 3 is a nonsquare modulo q, the sequence S differs from the q-periodic Legendre sequence at q terms (among the first $3q$ terms), and can be seen as an alternative to the Legendre sequence which is well distinguishable from its shifts by t positions for $3(q-1)$ values for t, $0 \le t \le 3q-1$.

Example $d=3$: If $p=7$ and q is a prime such that 7 is not a third power modulo q, then $A(S,t)$ is small for all values of $1 \le t < 7q$ except for $t = rq, r = 1,2,\ldots,6$, we have $L(S) \ge 7q-3$ and S differs from the ternary cyclotomic generator with period q at $q+3$ terms (among the first $7q$ terms).

4 Conclusions

Our analysis of the generator introduced in [1,18] and its generalization to arbitrary prime fields shows a favourable behaviour regarding linear complexity but points out a drawback of the generator with arbitrary choice of the primes p, q when one considers k-error linear complexity and autocorrelation. In particular we see that the considered generator may be an attractive alternative to the cyclotomic generator only if q is chosen large, p small, and p is not a dth power modulo q.

Amongst the binary generators defined via generalized cyclotomy the two prime generator [4,5] and [2, Chapter 8.2] has still the best properties. If p, q are twin primes then the two prime generator has best possible autocorrelation properties [5] (for the trace representation of the binary two prime gernerator we refer to [3]). In [11] Li et al. determined the autocorrelation of the pq-periodic binary cyclotomic sequence T defined by $t_n = l_n$ if $n \in \mathbb{Z}_{pq}^*$, where l_n is the nth term of the q-periodic Legendre sequence, $t_n = 0$ for $n \in Q \cup R$ and $t_n = 1$ for $n \in P$. It turns out that $A(T, t)$ is not small for a large number of shifts t for all choices of the primes p, q. This suggests that the sequence in [11] is not attractive for several applications. A further possibility to define a cyclotomic sequence is given by $s_0 = 0$, $\varepsilon_d^{s_n} = \chi_d^{(q)}(n)\chi_d^{(p)}(n)$ if $n \bmod pq \in \mathbb{Z}_{pq}^*$, $\varepsilon_d^{sn} = \overline{\chi_d^{(q)}(p)}\chi_d^{(q)}(n)$ if $n \bmod pq \in P$ and $\varepsilon_d^{sn} = \overline{\chi_d^{(p)}(q)}\chi_d^{(p)}(n)$ if $n \bmod pq \in Q$, where again $\varepsilon_d = e^{2\pi\sqrt{-1}/d}$. Analysis via character sums show that also this sequence has not desirable autocorrelation properties for all choices of p, q.

References

1. Bai E., Liu X., Xiao G.: Linear complexity of new generalized cyclotomic sequences of order two of length pq. IEEE Trans. Inform. Theory **51**, 1849–1853 (2005).
2. Cusick T.W., Ding C., Renvall A.: Stream Ciphers and Number Theory. North-Holland Publishing Co., Amsterdam (1998).
3. Dai Z., Gong G., Song H.: Trace representation of binary Jacobi sequences. In: Proceedings of ISIT 2003, p. 379.
4. Ding C.: Linear complexity of generalized cyclotomic binary sequences of order 2. Finite Fields Appl. **3**, 159–174 (1997).
5. Ding C.: Autocorrelation values of generalized cyclotomic sequences of order two. IEEE Trans. Inform. Theory **44**, 1699–1702 (1998).
6. Ding C., Helleseth T.: On cyclotomic generator of order r. Inform. Process. Lett. **66**, 21–25 (1998).
7. Ding C., Helleseth T.: New generalized cyclotomy and its applications. Finite Fields Appl. **4**, 140–166 (1998).
8. Ding C., Helleseth T., Shan W.: On the linear complexity of Legendre sequences. IEEE Trans. Inform. Theory **44**, 1276–1278 (1998).
9. Ding C., Xiao G., Shan W.: The Stability Theory of Stream Ciphers. Lecture Notes in Computer Science, vol. 561. Springer-Verlag, Berlin (1991).
10. Jungnickel D.: Finite fields. In: Structure and Arithmetics. Bibliographisches Institut, Mannheim (1993).
11. Li S., Chen Z., Fu X., Xiao G.: Autocorrelation values of new generalized cyclotomic sequences of order two and length pq. J. Comput. Sci. Technol. **22**, 830–834 (2007).
12. Meidl W., Winterhof A.: On the autocorrelation of cyclotomic generators. In: Mullen G.L., Stichtenoth H., Tapia-Recillas H. (eds.) Proceedings of Finite Fields and Applications 6. Lecture Notes in Computer Science, vol. 2948, pp. 1–11. Springer-Verlag, Berlin (2004).
13. Niederreiter H.: Linear complexity and related complexity measures for sequences. In: Johansson T., Maitra S. (eds.) Progress in Cryptology – Proceedings of INDOCRYPT 2003. Lecture Notes in Computer Science, vol. 2904, pp. 1–17. Springer-Verlag, Berlin (2003).
14. Rueppel R.A.: Stream ciphers. In: Simmons G.J. (ed.) Contemporary Cryptology: The Science of Information Integrity, pp. 65–134. IEEE Press, New York (1992).
15. Stamp M., Martin C.F.: An algorithm for the k-error linear complexity of binary sequences with period 2^n. IEEE Trans. Inform. Theory **39**, 1398–1401 (1993).

16. Topuzoğlu A., Winterhof A.: Pseudorandom sequences. In: Garcia A., Stichtenoth H. (eds.) Topics in Geometry, Coding Theory and Cryptography, Algebra and Applications, vol. 6, pp. 135–166. Springer-Verlag, Berlin (2007).
17. Whiteman A.L.: A family of difference sets. Illinois J. Math. **6**, 107–121 (1962).
18. Yan T., Chen Z., Xiao G.: Linear complexity of Ding generalized cyclotomic sequences. J. Shanghai Univ. (English Edition) **11**, 22–26 (2007).