AIMS Mathematics, 7(4): 5821–5829.
DOI:10.3934/math.2022322
Received: 31 October 2021
Revised: 23 December 2021
Accepted: 28 December 2021
Published: 11 January 2022

http://www.aimspress.com/journal/Math

Letter

On the 1-error linear complexity of two-prime generator

Tongjiang Yan*, Pazilaiti Ainiwaer and Lianbo Du

College of Science, China University of Petroleum, Qingdao 266580, China

* **Correspondence:** Email: yantoji@163.com; Tel: +8618366269028.

Abstract: Jing et al. dealed with all possible Whiteman generalized cyclotomic binary sequences $s(a, b, c)$ with period $N = pq$, where $(a, b, c) \in \{0, 1\}^3$ and p, q are distinct odd primes (Jing et al. arXiv:2105.10947v1, 2021). They have determined the autocorrelation distribution and the 2-adic complexity of these sequences in a unified way by using group ring language and a version of quadratic Gauss sums. In this paper, we determine the linear complexity and the 1-error linear complexity of $s(a, b, c)$ in details by using the discrete Fourier transform (DFT). The results indicate that the linear complexity of $s(a, b, c)$ is large enough and stable in most cases.

Keywords: linear complexity; generalized cyclotomic sequence; k-error linear complexity; discrete Fourier transform
Mathematics Subject Classification: 11T22, 94A60

1. Introduction

The linear complexity and the k-error linear complexity are important cryptographic characteristics of stream cipher sequences. The linear complexity of an N-periodic sequence $s = \{s_u\}_{u=0}^{\infty}$, denoted by $LC(s)$, is defined as the length of the shortest linear feedback shift register (LFSR) that generates it [1]. With the Berlekamp-Massey (B-M) algorithm [2], if $LC(s) \geq N/2$, then s is regarded as a good sequence with respect to its linear complexity. For an integer $k \geq 0$, the k-error linear complexity $LC_k(s)$ is the smallest linear complexity that can be obtained by changing at most k terms of s in the first period and periodically continued [3]. The cryptographic background of the k-error linear complexity is that some key streams with large linear complexity can be approximated by some sequences with much lower linear complexity [2]. For a sequence to be cryptographically strong, its linear complexity should be large enough, and its k-error linear complexity should be close to the linear complexity.

The relationship between the linear complexity and the DFT of the sequence was given by Blahut in [4]. Let m be the order of 2 modulo an odd number N. For a primitive N-th root $\beta \in \mathbb{F}_{2^m}$ of unity,

the DFT of s is defined by

$$\rho_i = \sum_{u=0}^{N-1} s_u \beta^{-iu}, 0 \le i \le N-1. \tag{1.1}$$

Then

$$LC(s) = W_H(\rho_0,\ \rho_1,\ \cdots,\ \rho_{N-1}), \tag{1.2}$$

where $W_H(A)$ is the hamming weight of the sequence A. The polynomial

$$G(X) = \sum_{i=0}^{N-1} \rho_i X^i \in \mathbb{F}_{2^m}[X] \tag{1.3}$$

is called the Mattson-Solomon polynomial (M-S polynomial) of s [5]. It can be deduced from Eqs (1.2)and (1.3) that the linear complexity of s is equal to the number of the nonzero terms of $G(X)$, namely

$$LC(s) = |G(X)|. \tag{1.4}$$

By the inverse DFT,

$$s_u = \sum_{i=0}^{N-1} \rho_i \beta^{iu} = G(\beta^u), 0 \le u \le N-1. \tag{1.5}$$

There are many studies about two-prime generators. In 1997–1998, Ding calculated the linear complexity and the autocorrelation values of binary Whiteman generalized cyclotomic sequences of order two [6, 7]. In 2013, Li defined a new generalized cyclotomic sequence of order two of length pq, which is based on Whiteman generalized cyclotomic classes, and calculated its linear complexity [8]. In 2015, Wei determined the k-error linear complexity of Legendre sequences for $k = 1, 2$ [9]. In 2018, Hofer and Winterhof studied the 2-adic complexity of the two-prime generator of period pq [10]. Alecu and Sălăgean transformed the optimisation problem of finding the k-error linear complexity of a sequence into an optimisation problem in the DFT domain, by using Blahut's theorem in the same year [11]. In 2019, in terms of the DFT, Chen and Wu discussed the k-error linear complexity for Legendre, Ding-Helleseth-Lam, and Hall's sextic residue sequences of odd prime period p [12]. In 2020, Zhou and Liu presented a type of binary sequences based on a general two-prime generalized cyclotomy, and derived their minimal polynomial and linear complexity [13]. In 2021, the autocorrelation distribution and the 2-adic complexity of generalized cyclotomic binary sequences of order 2 with period pq were determined by Jing [14].

This paper is organized as follows. Firstly, we present some preliminaries about Whiteman generalized cyclotomic classes and the linear complexity in Section 2. In Section 3, we give main results about the linear complexity of Whiteman generalized cyclotomic sequences of order two. In Section 4, we give the 1-error linear complexity of these sequences. At last, we conclude this paper in Section 5.

2. Preliminaries

Let p and q be two distinct odd primes with $\gcd(p-1, q-1) = 2$, and $N = pq$, $e = (p-1)(q-1)/2$. By the Chinese Remainder Theorem, there is a fixed common primitive root g of both p and q such

that $\mathrm{ord}_N(g) = e$. Let x be an integer satisfying

$$x = g(\mathrm{mod}\, p),\ x = 1(\mathrm{mod} q).$$

Then the set

$$D_i = \{g^s x^j \bmod N : s = 0, 1, \cdots, e-1\}$$

for $i = 0, 1$ is called a Whiteman generalized cyclotomic class of order two [15].

As pointed out in [14], the unit group of the ring Z_N is

$$\begin{aligned} Z_N^* &= \{a(\mathrm{mod}\ N) : \gcd(a, N) = 1\} \\ &= \{ip + jq(\mathrm{mod}\ N) : 1 \le i \le q-1, 1 \le j \le p-1\}. \end{aligned}$$

Let $P = \{p, 2p, \cdots, (q-1)p\}$, $Q = \{q, 2q, \cdots, (p-1)q\}$ and $R = \{0\}$. Then $Z_N = Z_N^* \cup P \cup Q \cup R$. The sequence $s(a, b, c) = \{s_u\}_{u=0}^{\infty}$ over $\mathbb{F}_2$ is defined by

$$s_u = \begin{cases} c, & \text{if } u = 0, \\ a, & \text{if } u \in P, \\ b, & \text{if } u \in Q, \\ \frac{1}{2}(1 - (\frac{u}{p})(\frac{u}{q})), & \text{if } u \in Z_N^*, \end{cases}$$

where $(\frac{\cdot}{\cdot})$ denotes the Legendre symbol and $a, b, c \in \mathbb{F}_2$ [14].

Lemma 2.1. *[7] $-1 \in D_1$, if $|p-q|/2$ is odd; and $-1 \in D_0$, if $|p-q|/2$ is even.*

Lemma 2.2. *[6]*

(1) If $p \equiv \pm 1(\mathrm{mod}8)$, $q \equiv \pm 1(\mathrm{mod}8)$ or $p \equiv \pm 3(\mathrm{mod}8)$, $q \equiv \pm 3(\mathrm{mod}8)$, then $2 \in D_0$.
(2) If $p \equiv \pm 1(\mathrm{mod}8)$, $q \equiv \pm 3(\mathrm{mod}8)$ or $p \equiv \pm 3(\mathrm{mod}8)$, $q \equiv \pm 1(\mathrm{mod}8)$, then $2 \in D_1$.

Lemma 2.3. *[6] (1) If $a \in P$, then $aP = P$ and $aQ = R$.*
(2) If $a \in Q$, then $aP = R$ and $aQ = Q$.
(3) If $a \in D_i$, then $aP = P$, $aQ = Q$, and $aD_j = D_{(i+j) \bmod 2}$, where $i, j = 0, 1$.

It was shown in [6] that, for a primitive N-th root $\beta \in \mathbb{F}_{2^m}$ of unity, we have

$$\sum_{i \in P} \beta^i = 1,\ \sum_{i \in Q} \beta^i = 1,$$

and

$$\sum_{i \in D_0} \beta^i + \sum_{i \in D_1} \beta^i + \sum_{i \in P} \beta^i + \sum_{i \in Q} \beta^i = 1. \tag{2.1}$$

Lemma 2.4. *[6]*

$$\sum_{u \in D_j} \beta^{iu} = \begin{cases} \frac{p-1}{2}(\mathrm{mod}2), & \text{if } i \in P, \\ \frac{q-1}{2}(\mathrm{mod}2), & \text{if } i \in Q. \end{cases}$$

Actually, if $p \equiv -1(\mathrm{mod}8)$ or $p \equiv 3(\mathrm{mod}8)$, then $(p-1)/2 = 1$; if $p \equiv 1(\mathrm{mod}8)$ or $p \equiv -3(\mathrm{mod}8)$, then $(p-1)/2 = 0$. By symmetry, if $q \equiv -1(\mathrm{mod}8)$ or $q \equiv 3(\mathrm{mod}8)$, then $(q-1)/2 = 1$; if $q \equiv 1(\mathrm{mod}8)$ or $q \equiv -3(\mathrm{mod}8)$, then $(q-1)/2 = 0$.

Lemma 2.5. *Define*

$$D_i(X) = \sum_{u \in D_i} X^u \in \mathbb{F}_2[X],\ i = 0, 1.$$

Then for β, we have $D_0(\beta) = 0$ and $D_1(\beta) = 1$ if $2 \in D_0$; $D_0(\beta) = \omega$ and $D_1(\beta) = 1 + \omega$ if $2 \in D_1$, where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$.

Proof. (1) If $2 \in D_0$, by Lemma 2.3 we have

$$[D_i(\beta)]^2 = D_i(\beta^2) = \sum_{2u \in D_i} \beta^{2u} = D_i(\beta) \in \mathbb{F}_2.$$

(2) If $2 \in D_1$, by Lemma 2.3 we have

$$[D_i(\beta)]^2 = D_i(\beta^2) = \sum_{2u \in D_{i+1}} \beta^{2u} = D_{i+1}(\beta),$$
$$[D_i(\beta)]^4 = [D_i(\beta)^2]^2 = [D_{i+1}(\beta)]^2 = D_{i+1}(\beta^2) = \sum_{2u \in D_i} \beta^{2u} = D_i(\beta).$$

Hence $D_i(\beta) \in \mathbb{F}_4 \setminus \mathbb{F}_2$.

And by Eq (2.1), we have $D_0(\beta) \neq D_1(\beta)$ and $D_0(\beta) + D_1(\beta) = 1$. Assume that $D_0(\beta) = 0$, $D_1(\beta) = 1$ for $2 \in D_0$, and $D_0(\beta) = \omega$, $D_1(\beta) = 1 + \omega$ for $2 \in D_1$, where $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$. □

3. The linear complexity of $s(a, b, c)$

Let $LC(s(a, b, c))$ be the linear complexity of $s(a, b, c)$, and the other symbols be the same as before.

Theorem 3.1. *Let $p \equiv v(\mathrm{mod}8)$ and $q \equiv w(\mathrm{mod}8)$, where $v, w = \pm 1, \pm 3$. Then the linear complexity of $s(a, b, c)$ respect to different values of p and q is as shown as Table 1.*

Table 1. The linear complexity of $s(a, b, c)$.

(v, w) \ $s(a,b,c)$	$s(0,0,0)$	$s(0,0,1)$	$s(0,1,0)$	$s(0,1,1)$	$s(1,0,0)$	$s(1,0,1)$	$s(1,1,0))$	$s(1,1,1)$
$(-1,-3)$ or $(3,1)$	$pq-p$	$pq-q+1$	$pq-1$	$pq-p-q+2$	$pq-p-q+1$	pq	$pq-q$	$pq-p+1$
$(-1,3)$ or $(3,-1)$	$pq-1$	$pq-p-q+2$	$pq-p$	$pq-q+1$	$pq-q$	$pq-p+1$	$pq-p-q+1$	pq
$(-1,1)$ or $(3,-3)$	$\frac{pq-p+q-1}{2}$	$\frac{pq+p-q+1}{2}$	$\frac{pq+p+q-3}{2}$	$\frac{pq-p-q+3}{2}$	$\frac{pq-p-q+1}{2}$	$\frac{pq+p+q-1}{2}$	$\frac{pq+p-q-1}{2}$	$\frac{pq-p+q+1}{2}$
$(-1,-1)$ or $(3,3)$	$\frac{pq+p+q-3}{2}$	$\frac{pq-p-q+3}{2}$	$\frac{pq-p+q-1}{2}$	$\frac{pq+p-q+1}{2}$	$\frac{pq+p-q-1}{2}$	$\frac{pq-p+q+1}{2}$	$\frac{pq-p-q+1}{2}$	$\frac{pq+p+q-1}{2}$
$(-3,-1)$ or $(1,3)$	$pq-q$	$pq-p+1$	$pq-p-q+1$	pq	$pq-1$	$pq-p-q+2$	$pq-p$	$pq-q+1$
$(1,-1)$ or $(-3,3)$	$\frac{pq+p-q-1}{2}$	$\frac{pq-p+q+1}{2}$	$\frac{pq-p-q+1}{2}$	$\frac{pq+p+q-1}{2}$	$\frac{pq+p+q-3}{2}$	$\frac{pq-p-q+3}{2}$	$\frac{pq-p+q-1}{2}$	$\frac{pq+p-q+1}{2}$

Proof. We provide the process of calculating $LC(s(0,0,0))$ when $v = -1$ and $w = -3$, and can prove other cases in a similar way.

By Lemmas 2.1–2.3 and Eq (1.1), we have $-1 \in D_1$, $2 \in D_1$, then

$$\rho_i = \sum_{u=0}^{N-1} s_u \beta^{-iu} = \sum_{u \in D_1} \beta^{-iu} = \sum_{u \in D_0} \beta^{iu},$$

and $\rho_0 = 0$. By Eq (1.3), we have

$$\begin{aligned} G(X) &= \sum_{i=0}^{N-1} \rho_i X^i = \sum_{i \in D_0} \rho_i X^i + \sum_{i \in D_1} \rho_i X^i + \sum_{i \in P} \rho_i X^i + \sum_{i \in Q} \rho_i X^i + \rho_0 \\ &= \sum_{i \in D_0} \sum_{u \in D_0} \beta^{iu} X^i + \sum_{i \in D_1} \sum_{u \in D_0} \beta^{iu} X^i + \sum_{i \in P} \sum_{u \in D_0} \beta^{iu} X^i + \sum_{i \in Q} \sum_{u \in D_0} \beta^{iu} X^i. \end{aligned}$$

Let $t = iu$. Then by Lemmas 2.3–2.5, we have

$$\begin{aligned} G(X) &= \sum_{i \in D_0} \sum_{t \in D_0} \beta^t X^i + \sum_{i \in D_1} \sum_{t \in D_1} \beta^t X^i + \sum_{i \in P} \frac{p-1}{2} X^i + \sum_{i \in Q} \frac{q-1}{2} X^i \\ &= D_0(\beta) D_0(X) + D_1(\beta) D_1(X) + \sum_{i \in P} X^i \\ &= \omega D_0(X) + (1+\omega) D_1(X) + \sum_{i \in P} X^i. \end{aligned}$$

By Eq (1.4) we can get the linear complexity of $s(0,0,0)$ as

$$LC(s(0,0,0)) = |G(X)| = pq - p.$$

□

Actually, the linear complexity of $s(1,0,0)$ was studied by Ding in [6] with its minimal polynomial.

4. The 1-error linear complexity of $s(a,b,c)$

Let $LC_k(s(a,b,c))$ be the k-error linear complexity of $s(a,b,c)$, $\tilde{s} = \{\tilde{s}_u\}_{u=0}^{\infty}$ be the new sequence obtained by changing at most k terms of s, that $\tilde{s} = s + e$, where $e = \{e_u\}_{u=0}^{\infty}$ is an error sequence of period N. Ding has provided in [2] that, the k-error linear complexity of a sequence can be expressed as

$$LC_k(s) = \min_{W_H(e) \le k} \{LC(s+e)\}. \tag{4.1}$$

It is clearly that $LC_0(s) = LC(s)$ and

$$N \ge LC_0(s) \ge LC_1(s) \ge \cdots \ge LC_l(s) = 0,$$

where $l = W_H(s)$.

Let $G(X)$, $G_k(X)$ and $\tilde{G}(X)$ be the M-S polynomials of s, e and $\tilde{s}$ respectively. Note that

$$G(X) = \sum_{i=0}^{N-1} \rho_i X^i,\ G_k(X) = \sum_{i=0}^{N-1} \eta_i X^i,\ \tilde{G}(X) = \sum_{i=0}^{N-1} \xi_i X^i, \tag{4.2}$$

where ρ_i, η_i and ξ_i are the DFTs of s, e and $\tilde{s}$ respectively. By Eqs (1.5), (4.1) and (4.2), we have $\tilde{G}(X) = G(X) + G_k(X)$, then

$$\xi_i = \rho_i + \eta_i. \tag{4.3}$$

Assume that $e_{u_0} = 1$ for $0 \le u_0 \le N-1$ and $e_u = 0$ for $u \ne u_0$ in the first period of e. Then the DFT of e is

$$\eta_i = \sum_{u=0}^{N-1} e_u \beta^{-iu} = \beta^{-iu_0},\ 0 \le i \le N-1.$$

Specially, if $u_0 = 0$, then $\eta_i = 1$ for all $0 \le i \le N-1$; otherwise, $\eta_0 = 1$ and the order of η_i is N for $1 \le i \le N-1$.

Theorem 4.1. *Let $p \equiv v (\mathrm{mod} 8)$ and $q \equiv w (\mathrm{mod} 8)$, where $v, w = \pm 1, \pm 3$, and the other symbols be the same as before. Then the 1-error linear complexity of $s(a, b, c)$ is as shown as Table 2.*

Table 2. The 1-error linear complexity of $s(a, b, c)$.

$s(a,b,c)$ / (v,w)	$s(0,0,0)$ and $s(0,0,1)$	$s(0,1,0)$ and $s(0,1,1)$	$s(1,0,0)$ and $s(1,0,1)$	$s(1,1,0))$ and $s(1,1,1)$
$(-1,-3)$ or $(3,1)$	(1) $pq-p$, if $p>q$; (2) $pq-q+1$, if $p<q$.	$pq-p-q+2$	$pq-p-q+1$	(1) $pq-p+1$, if $p>q$; (2) $pq-q$, if $p<q$.
$(-1,3)$ or $(3,-1)$	$pq-p-q+2$	(1) $pq-p$, if $p>q$; (2) $pq-q+1$, if $p<q$.	(1) $pq-p+1$, if $p>q$; (2) $pq-q$, if $p<q$.	$pq-p-q+1$
$(-1,1)$ or $(3,-3)$	(1) $\frac{pq-p+q-1}{2}$, if $p>q$; (2) $\frac{pq+p-q+1}{2}$, if $p<q$.	$\frac{pq-p-q+3}{2}$	$\frac{pq-p-q+1}{2}$	(1) $\frac{pq-p+q+1}{2}$, if $p>q$; (2) $\frac{pq+p-q-1}{2}$, if $p<q$.
$(-1,-1)$ or $(3,3)$	$\frac{pq-p-q+3}{2}$	(1) $\frac{pq-p+q-1}{2}$, if $p>q$; (2) $\frac{pq+p-q+1}{2}$, if $p<q$.	(1) $\frac{pq-p+q+1}{2}$, if $p>q$; (2) $\frac{pq+p-q-1}{2}$, if $p<q$.	$\frac{pq-p-q+1}{2}$
$(-3,-1)$ or $(1,3)$	(1) $pq-p+1$, if $p>q$; (2) $pq-q$, if $p<q$.	$pq-p-q+1$	$pq-p-q+2$	(1) $pq-p$, if $p>q$; (2) $pq-q+1$, if $p<q$.
$(1,-1)$ or $(-3,3)$	(1) $\frac{pq-p+q+1}{2}$, if $p>q$; (2) $\frac{pq+p-q-1}{2}$, if $p<q$.	$\frac{pq-p-q+1}{2}$	$\frac{pq-p-q+3}{2}$	(1) $\frac{pq-p+q-1}{2}$, if $p>q$; (2) $\frac{pq+p-q+1}{2}$, if $p<q$.

Proof. We consider the case $v = -1, w = -3$ for $LC_1(s(0,0,0))$. By Lemmas 2.1–2.5 and Eq (1.1), we have $-1 \in D_1$, $2 \in D_1$ and

$$\xi_i = \rho_i + \eta_i = \sum_{u \in D_0} \beta^{iu} + \beta^{-iu_0} = \begin{cases} \omega + \beta^{-iu_0}, & \text{if } i \in D_0, \\ 1 + \omega + \beta^{-iu_0}, & \text{if } i \in D_1, \\ 1 + \beta^{-iu_0}, & \text{if } i \in P, \\ \beta^{-iu_0}, & \text{if } i \in Q, \\ 1, & \text{if } i = 0. \end{cases}$$

Then by Eq (4.2), we can get

$$\tilde{G}(X) = \sum_{i=0}^{N-1} \xi_i X^i = \sum_{i \in D_0} \left(\omega + \beta^{-iu_0}\right) X^i + \sum_{i \in D_1} \left(1 + \omega + \beta^{-iu_0}\right) X^i + \sum_{i \in P} \left(1 + \beta^{-iu_0}\right) X^i + \sum_{i \in Q} \beta^{-iu_0} X^i + 1.$$

According to Lemma 2.3, we can get the following results.
(1) If $u_0 = 0$, then

$$\tilde{G}(X) = \sum_{i\in D_0} (\omega + 1) X^i + \sum_{i\in D_1} \omega X^i + \sum_{i\in Q} X^i + 1,$$
$$|\tilde{G}(X)| = pq - q + 1.$$

(2) If $u_0 \in Q$, then

$$\tilde{G}(X) = \sum_{i\in D_0} \left(\omega + \beta^{-iu_0}\right) X^i + \sum_{i\in D_1} \left(1 + \omega + \beta^{-iu_0}\right) X^i + \sum_{i\in Q} \beta^{-iu_0} X^i + 1,$$
$$|\tilde{G}(X)| = pq - q + 1.$$

(3) If $u_0 \in D_0$ or $u_0 \in D_1$ or $u_0 \in P$, then

$$\tilde{G}(X) = \sum_{i\in D_0} \left(\omega + \beta^{-iu_0}\right) X^i + \sum_{i\in D_1} \left(1 + \omega + \beta^{-iu_0}\right) X^i + \sum_{i\in P} \left(1 + \beta^{-iu_0}\right) X^i + \sum_{i\in Q} \beta^{-iu_0} X^i + 1,$$
$$|\tilde{G}(X)| = pq.$$

Compare the results of Cases (1)–(3) with $LC(s(0,0,0)) = pq - p$. If $p > q$, then $pq - p < pq - q + 1 < pq$; if $p < q$, then $pq - q + 1 < pq - p < pq$. Hence

$$LC_1(s(0,0,0)) = \begin{cases} pq - p, & \text{if } p > q, \\ pq - q + 1, & \text{if } p < q. \end{cases}$$

Similarly we can prove the other cases for $LC_1(s(a,b,c))$. □

All results of $LC(s(a,b,c))$ and $LC_1(s(a,b,c))$ in Sections 3 and 4 have been tested by MAGMA program.

5. Conclusions

The purpose of this paper is to determine the linear complexity and the 1-error linear complexity of $s(a,b,c)$. In most of the cases, $s(a,b,c)$ possesses high linear complexity, namely $LC(s(a,b,c)) > N/2$, consequently has decent stability against 1-bit error. Notice that the linear complexity of some of the sequences above is close to $N/2$. Then the sequences can be selected to construct cyclic codes by their minimal generating polynomials with the method introduced by Ding [16].

Acknowledgments

This work was supported by Fundamental Research Funds for the Central Universities (No. 20CX05012A), the Major Scientific and Technological Projects of CNPC under Grant (No. ZD2019-183-008), the National Natural Science Foundation of China (Nos. 61902429, 11775306) and Shandong Provincial Natural Science Foundation of China (ZR2019MF070).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. T. Cusick, C. Ding, A. Renvall, *Stream ciphers and number theory*, Amsterdam: Elsevier, 2004.
2. C. Ding, G. Xiao, W. Shan, *The stability theory of stream ciphers*, Berlin: Springer, 1991. http://dx.doi.org/10.1007/3-540-54973-0
3. M. Stamp, C. Martin, An algorithm for the k-error linear complexity of binary sequences with period 2^n, *IEEE Trans. Inform. Theory*, **39** (1993), 1398–1401. http://dx.doi.org/10.1109/18.243455
4. R. Blahut, Transform techniques for error control codes, *IBM J. Res. Dev.*, **23** (1979), 299–315. http://dx.doi.org/10.1147/rd.233.0299
5. F. MacWilliams, N. Sloane, *The theory of error-correcting codes*, Amsterdam: Elsevier, 1977.
6. C. Ding, Linear complexity of generalized cyclotomic binary sequences of order 2, *Finite Fields Th. Appl.*, **3** (1997), 159–174. http://dx.doi.org/10.1006/ffta.1997.0181
7. C. Ding, Autocorrelation values of generalized cyclotomic sequences of order two, *IEEE Trans. Inform. Theory*, **44** (1998), 1699–1702. http://dx.doi.org/10.1109/18.681354
8. X. Li, W. Ma, T. Yan, X. Zhao, Linear complexity of a new generalized cyclotomic sequence of order two of length pq, *IEICE Trans. Fund. Elect.*, **96** (2013), 1001–1005. http://dx.doi.org/10.1587/transfun.E96.A.1001
9. Y. Wei, 1,2-error linear complexity of Legendre sequences (Chinese), Master's Thesis, Hubei University, 2015.
10. R. Hofer, A. Winterhof, On the 2-adic complexity of the two-prime generator, *IEEE Trans. Inform. Theory*, **64** (2018), 5957–5960. http://dx.doi.org/10.1109/TIT.2018.2811507
11. A. Alecu, A. Sălăgean, An approximation algorithm for computing the k-error linear complexity of sequences using the discrete fourier transform, Proceedings of *IEEE International Symposium on Information Theory*, 2008, 2414–2418. http://dx.doi.org/10.1109/ISIT.2008.4595424
12. Z. Chen, C. Wu, K-error linear complexity of binary cyclotomic generators, *Journal on Communications*, **40** (2019), 197–206. http://dx.doi.org/10.11959/j.issn.1000-436x.2019034
13. X. Zhou, Cyclic codes via the general two-prime generalized cyclotomic sequence of order two, *J. Math.*, **2020** (2020), 6625652. http://dx.doi.org/10.1155/2020/6625652
14. X. Jing, S. Qing, M. Yang, K. Feng, Determination of the autocorrelation distribution and 2-adic complexity of generalized cyclotomic binary sequences of order 2 with period pq, arXiv:2105.10947.
15. A. Whiteman, A family of defference sets, *Illinois J. Math.*, **6** (1962), 107–121. http://dx.doi.org/10.1215/ijm/1255631810

16. C. Ding, Cyclotomic constructions of cyclic codes with length being the product of two primes, *IEEE Trans. Inform. Theory*, **58** (2012), 2231–2236. http://dx.doi.org/10.1109/TIT.2011.2176915

AIMS Press