Designs, Codes and Cryptography (2019) 87:2585–2596
https://doi.org/10.1007/s10623-019-00638-5

Linear complexity of generalized cyclotomic sequences of period $2p^m$

Yi Ouyang[1] · Xianhong Xie[2]

Received: 6 September 2018 / Revised: 17 April 2019 / Accepted: 25 April 2019 / Published online: 4 May 2019

Abstract
In this paper, we construct two generalized cyclotomic binary sequences of period $2p^m$ based on the generalized cyclotomy and compute their linear complexity, showing that they are of high linear complexity when $m \geq 2$.

Keywords Binary sequence · Linear complexity · Cyclotomy · Generalized cyclotomic sequence

Mathematics Subject Classification 11B50 · 94A55 · 94A60

1 Introduction

A sequence $\mathbf{s}^\infty = \{s_0, s_1, s_2, \ldots\}$ is called a binary sequence of period N if $s_i \in \mathbb{F}_2$ and $s_i = s_{i+N}$ for all $i \geq 0$. The linear complexity (LC) of a periodic binary sequence $\mathbf{s}^\infty$, denoted by $\mathrm{LC}(\mathbf{s}^\infty)$, is the length of shortest linear feedback shift register (LFSR) that generates the sequence [10], i.e., the smallest positive integer l such that $s_i = c_l s_{i-l} + \cdots + c_2 s_{i-2} + c_1 s_{i-1}$ for $i \geq l$ and constants $c_0 = 1, c_1, \ldots, c_l \in \mathbb{F}_2$. For $\mathbf{s}^\infty$ a sequence of period N, the characteristic power series/polynomial of $\mathbf{s}^\infty$ and $\mathbf{s}^N = \{s_0, s_1, \ldots, s_{N-1}\}$ are defined respectively as $c^\infty(x) = s_0 + s_1 x + \cdots$ and $c^N(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$, the

Communicated by T. Helleseth.

Partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and NSFC (Grant No. 11571328).

✉ Xianhong Xie
xianhxie@mail.ustc.edu.cn

Yi Ouyang
yiouyang@ustc.edu.cn

1 Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei 230026, Anhui, China

2 Key Laboratory of Electromagnetic Space Information, CAS, University of Science and Technology of China, Hefei 230027, Anhui, China

minimal polynomial [3] of $\mathbf{s}^\infty$ is

$$m(x) = (x^N - 1)/\gcd\left(c^N(x), x^N - 1\right).$$

Then we have the following classical relation

$$\mathrm{LC}(\mathbf{s}^\infty) = \deg(m(x)) = N - \deg\left(\gcd\left(x^N - 1, c^N(x)\right)\right). \tag{1}$$

The linear complexity of a sequence is an important criteria of its quality. As we all know, sequences with high linear complexity (such that $\mathrm{LC}(\mathbf{s}^\infty) > \frac{N}{2}$) have important applications in cryptography.

Cyclotomic generators based on cyclotomy can generate sequences with large linear complexity. Generalized cyclotomic classes with respect to pq and p^2 were introduced by Whiteman and Ding for the purposes of searching for residue difference sets [19] and cryptography [4] respectively. Based on Whiteman's generalized cyclotomy of order 2, Ding [5] constructed a class of generalized cyclotomic sequences of period pq and determined their linear complexity. Autocorrelation and linear complexity of period p^2 and p^3 were studied in [18,22]. The linear complexity of generalized cyclotomic sequences of period p^m were investigated in [14,15]. In addition, the generalized cyclotomy of order 2 was extended to the case of period $p_1^{e_1}\cdots p_m^{e_m}$, which is not consistent with the classical cyclotomy [7]. Subsequently, new generalized cyclotomic sequences of period $p_1^{e_1}\cdots p_m^{e_m}$ that include the classical ones as special cases were presented in [6], and the linear complexity of such sequences of period pq were calculated in [1]. Furthermore, new classes of generalized cyclotomic sequences of period $2p^m$ were proposed in [8], which included the sequence presented in [12] as a special case, and they were shown to have high linear complexity. For recent development of the linear complexity of generalized cyclotomic sequences with different periods, the reader is referred to [2,11–13,16,17,21,23].

In this paper, we construct two new classes of generalized cyclotomic binary sequences of period $2p^m$ and compute their linear complexity, showing that they are of high linear complexity when $m \geq 2$.

2 Generalized binary cyclotomic sequences of period $2p^m$

Let p be an odd prime and g be a primitive root module p^m. Replace g by $g + p^m$ if necessary, without loss of generality, we may assume that g is an odd integer, and thus g is a common primitive root module p^j and $2p^j$ for all $1 \leq j \leq m$. For a decomposition $p - 1 = ef$, write $d_j = \frac{\varphi(p^j)}{e} = p^{j-1}f$ for each j where $\varphi(\cdot)$ is Euler's totient function. For $i \in \mathbb{Z}$, $s = p^j$ or $2p^j$, define

$$D_i^{(s)} := \left\{g^{i+d_j t} \pmod{s} :\ 0 \leq t < e\right\} = g^i D_0^{(s)}. \tag{2}$$

One can see immediately $D_i^{(s)}$ depends only on the congruence class $i \pmod{d_j}$. By abuse of notation we say an integer $n \in D_i^{(s)}$ if $n \pmod{s} \in D_i^{(s)}$.

For $(s, a) = (p^j, p^{m-j})$, $(p^j, 2p^{m-j})$ or $(2p^j, p^{m-j})$, we define

$$aD_i^{(s)} := \left\{ag^{i+d_j t} \pmod{as} :\ 0 \leq t < e\right\}. \tag{3}$$

It is well known that $\left\{D_0^{(p^j)}, D_1^{(p^j)}, \ldots, D_{d_j-1}^{(p^j)}\right\}$ forms a partition of $\mathbb{Z}_{p^j}^*$ (see [24]), which we call the generalized cyclotomic class of order d_j with respect to p^j, and

$$\mathbb{Z}_{p^m} = \bigcup_{j=1}^{m} \bigcup_{i=0}^{d_j-1} p^{m-j} D_i^{(p^j)} \cup \{0\}, \tag{4}$$

$$\mathbb{Z}_{2p^m} = \bigcup_{j=1}^{m} \bigcup_{i=0}^{d_j-1} p^{m-j} \left(2D_i^{(p^j)} \cup D_i^{(2p^j)}\right) \cup \{0, p^m\}. \tag{5}$$

From now on, take

$$f = 2^r \ (r \geq 1),\ b \in \mathbb{Z},\ \delta_j = \frac{d_j}{2} = \frac{p^{j-1} f}{2}.$$

In the following we define two families of generalized cyclotomic sequences of period $2p^m$. The ideal of construction comes from Xiao et al. [20], where generalized cyclotomic sequences of period p^m were constructed and studied.

(i) The generalized cyclotomic binary sequence of period $2p^m$ is defined as $\mathbf{s}^\infty = \{s_i\}_{i\geq 0}$ with

$$s_i = \begin{cases} 1, & \text{if } i \pmod{2p^m} \in C_1, \\ 0, & \text{if } i \pmod{2p^m} \in C_0, \end{cases} \tag{6}$$

where

$$C_0 = \bigcup_{j=1}^{m} \bigcup_{i=\delta_j}^{d_j-1} p^{m-j} \left(2D_{i+b}^{(p^j)} \cup D_{i+b}^{(2p^j)}\right) \cup \{p^m\},$$

$$C_1 = \bigcup_{j=1}^{m} \bigcup_{i=0}^{\delta_j-1} p^{m-j} \left(2D_{i+b}^{(p^j)} \cup D_{i+b}^{(2p^j)}\right) \cup \{0\}.$$

For the above sequence $\mathbf{s}^\infty$, the following theorem holds.

Theorem 1 *For the generalized cyclotomic sequence defined by (6) of period $2p^m$,*

(1) *if $2^e \not\equiv \pm 1 \pmod{p}$ or $2^e \equiv 1 \pmod{p}$ but $2^e \not\equiv 1 \pmod{p^2}$, then $\mathrm{LC}(\mathbf{s}^\infty) = 2p^m$;*
(2) *if $2^e \equiv -1 \pmod{p}$ but $2^e \not\equiv -1 \pmod{p^2}$, then $2p^m - 2(p-1) \leq \mathrm{LC}(\mathbf{s}^\infty) \leq 2p^m - (p-1)$.*

(ii) The modified generalized cyclotomic binary sequence of period $2p^m$ is defined as $\widetilde{\mathbf{s}}^\infty = \{\widetilde{s}_i\}_{i\geq 0}$ with

$$\widetilde{s}_i = \begin{cases} 1, & \text{if } i \pmod{2p^m} \in \widetilde{C}_1, \\ 0, & \text{if } i \pmod{2p^m} \in \widetilde{C}_0, \end{cases} \tag{7}$$

where

$$\widetilde{C}_0 = \bigcup_{j=1}^{m} p^{m-j} \left(\bigcup_{i=0}^{\delta_j-1} 2D_{i+b}^{(p^j)} \bigcup_{i=\delta_j}^{d_j-1} D_{i+b}^{(2p^j)} \right) \cup \{p^m\},$$

$$\widetilde{C}_1 = \bigcup_{j=1}^{m} p^{m-j} \left(\bigcup_{i=\delta_j}^{d_j-1} 2D_{i+b}^{(p^j)} \bigcup_{i=0}^{\delta_j-1} D_{i+b}^{(2p^j)} \right) \cup \{0\}.$$

For the above sequence $\widetilde{\mathbf{s}}^\infty$, the following theorem holds.

Theorem 2 *For the modified generalized cyclotomic sequence defined by* (7) *of period* $2p^m$,

(1) *if* $2^e \not\equiv 1 \pmod{p}$, *then* $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 2p^m$;
(2) *if* $2^e \equiv 1 \pmod{p}$ *but* $2^e \not\equiv 1 \pmod{p^2}$, *then* $2p^m - 2(p-1) \le \mathrm{LC}(\widetilde{\mathbf{s}}^\infty) \le 2p^m - (p-1)$.

We give two remarks about our main results.

Remark (1) The two theorems covers all non-Wieferich primes, as in this case, $2^{p-1} \not\equiv 1 \pmod{p^2}$ implies $2^e \not\equiv \pm 1 \pmod{p^2}$. Consequently the case that $2^e \equiv \pm 1 \pmod{p^a}$ but $\not\equiv \pm 1 \pmod{p^{a+1}}$ for $a > 1$ is rare.
(2) A key argument of our computation follows from the work of Edemskiy et al. [9]. Based on our computation, a new (but essentially the same) proof of the conjecture by Xiao et al. in [20] can be achieved.

The inequalities in Theorems 1(2) and 2(2), arising from the inseparability of the polynomial $x^{2p^m} - 1$ over $\mathbb{F}_2$, are strong enough to deduce that the two generalized sequences are of high linear complexity if $m \ge 2$. For the exact values there, based on numerical evidence, we have the following conjecture:

Conjecture *If* $2^e \equiv -1 \pmod{p}$ *but* $2^e \not\equiv -1 \pmod{p^2}$, *then* $\mathrm{LC}(\boldsymbol{s}^\infty) = 2p^m - (p-1)$.

Remark If $2^e \equiv 1 \pmod{p}$ but $2^e \not\equiv 1 \pmod{p^2}$, we expected that $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 2p^m - (p-1) - e$ and checked many examples. However, as pointed out by the referee, if $p = 73$, $m = 1$ and $f = 4$, then $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 38 \ne p + 1 - e = 56$. So the prediction is false and we now expect $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) \le 2p^m - (p-1) - e$.

3 Proof of the main results

Let $\beta = \beta_m$ be a fixed primitive p^m-th root of unity, then the field $\mathbb{F}_2(\beta) = \mathbb{F}_{2^n}$ where n is the order of 2 module p^m. For $j < m$, $\beta_j = \beta_m^{p^{m-j}}$ is a primitive p^j-th root of unity.

We fix the decomposition $p-1 = ef$, $f = 2^r$ for $r \ge 1$, $\delta_j = \frac{d_j}{2} = \frac{p^{j-1}f}{2}$ for $1 \le j \le m$ and $b \in \mathbb{Z}$. Note that $\delta_1 = \frac{f}{2}$ and $d_1 = f$. For $v \in \mathbb{Z}$, set

$$\mathbf{H}_{m,v}^{(p^j)} := \bigcup_{i=0}^{\delta_j - 1} p^{m-j} D_{i+v}^{(p^j)}, \quad H_{m,v}^{(p^j)} := 2\mathbf{H}_{m,v}^{(p^j)}, \quad H_{m,v}^{(2p^j)} := \bigcup_{i=0}^{\delta_j - 1} p^{m-j} D_{i+v}^{(2p^j)}$$

and

$$\mathbf{H}_{m,v}^{(p^j)}(x) := \sum_{t \in \mathbf{H}_{m,v}^{(p^j)}} x^t, \quad H_{m,v}^{(p^j)}(x) := \sum_{t \in H_{m,v}^{(p^j)}} x^t = \mathbf{H}_{m,v}^{(p^j)}(x^2), \quad H_{m,v}^{(2p^j)}(x) := \sum_{t \in H_{m,v}^{(2p^j)}} x^t.$$

The characteristic polynomials of $\mathbf{s}^\infty$ and $\widetilde{\mathbf{s}}^\infty$ are

$$s(x) := \sum_{t \in C_1} x^t = 1 + \sum_{j=1}^{m} \left(H_{m,b}^{(p^j)}(x) + H_{m,b}^{(2p^j)}(x) \right),$$

$$\widetilde{s}(x) := \sum_{t \in \widetilde{C}_1} x^t = 1 + \sum_{j=1}^{m} \left(H_{m,b+\delta_j}^{(p^j)}(x) + H_{m,b}^{(2p^j)}(x) \right).$$

To study the linear complexity of $\mathbf{s}^\infty$ and $\widetilde{\mathbf{s}}^\infty$, note that there is some subtlety here: the polynomial $x^{2p^m}-1$ is inseparable, each root β^a ($a \in \mathbb{Z}_{p^m}$) is of multiplicity 2, so by Eq. (1), we have the inequalities

$$2p^m - 2|\{a \in \mathbb{Z}_{p^m} \mid s(\beta^a)=0\}| \le \mathrm{LC}(\mathbf{s}^\infty) \le 2p^m - |\{a \in \mathbb{Z}_{p^m} \mid s(\beta^a)=0\}|, \tag{8}$$

$$2p^m - 2|\{a \in \mathbb{Z}_{p^m} \mid \widetilde{s}(\beta^a)=0\}| \le \mathrm{LC}(\widetilde{\mathbf{s}}^\infty) \le 2p^m - |\{a \in \mathbb{Z}_{p^m} \mid \widetilde{s}(\beta^a)=0\}|. \tag{9}$$

Since the polynomial is valued over a field of characteristic 2, for $v \in \mathbb{Z}$, we have

$$H_{m,v}^{(p^j)}(\beta^a) = \mathbf{H}_{m,v}^{(p^j)}(\beta^{2a}) = a(\mathbf{H}_{m,v}^{(p^j)}(\beta^a)a)^2, \tag{10}$$

$$H_{m,v}^{(2p^j)}(\beta^a) = \mathbf{H}_{m,v}^{(p^j)}(\beta^a). \tag{11}$$

To study $s(\beta^a)$ and $\widetilde{s}(\beta^a)$, it suffices to evaluate $\mathbf{H}_{m,b}^{(p^j)}(\beta^a)$ for each $j \le m$.

Lemma 1 ([20], Lemma 4) *For $v \in \mathbb{Z}$, we have*

$$\mathbf{H}_{m,v}^{(p)}(\beta) + \mathbf{H}_{m,v+\frac{f}{2}}^{(p)}(\beta) = \sum_{t \in p^{m-1}\mathbb{Z}_p^*} \beta^t = 1, \tag{12}$$

$$\mathbf{H}_{m,v}^{(p^j)}(\beta) + \mathbf{H}_{m,v+\delta_j}^{(p^j)}(\beta) = \sum_{t \in p^{m-j}\mathbb{Z}_{p^j}^*} \beta^t = 0 \text{ if } 2 \le j \le m. \tag{13}$$

Lemma 2 *Let $a = p^l u \in p^l D_k^{(p^{m-l})}$ where $0 \le l \le m-1$. Then for $j = 1, 2, \cdots, m$,*

(1) *if $j \le l$, $\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \frac{p^{j-1}(p-1)}{2}$;*
(2) *if $j = l+1$, $\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \frac{p^l-1}{2} + \mathbf{H}_{m,b+k}^{(p)}(\beta)$;*
(3) *if $j > l+1$, $\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \mathbf{H}_{b+k}^{(p^{j-l})}(\beta)$.*

Proof First note the computation here is carried out in $\mathbb{F}_2(\beta)$. By definition,

$$\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \sum_{t \in \mathbf{H}_{m,b}^{(p^j)}} \beta^{at} = \sum_{i=0}^{\delta_j-1} \sum_{t \in p^{m-j}D_{i+b}^{(p^j)}} \beta^{tp^l u} = \sum_{i=0}^{\delta_j-1} \sum_{t \in p^{m+l-j}D_{i+b}^{(p^j)}} \beta^{tu}. \tag{14}$$

If $j \le l$, each term in $\mathbf{H}_{m,b}^{(p^j)}(\beta^a)$ defined in (14) equals to 1, hence

$$\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \delta_j \cdot |D_{i+b}^{(p^j)}| = \delta_j p^{j-1}\frac{p-1}{p^{j-1}f} = \frac{p^{j-1}(p-1)}{2}.$$

If $j > l$, let $s = j - l$, then

$$\mathbf{H}_{m,b}^{(p^j)}(\beta^a) = \sum_{i=0}^{\delta_j-1} \sum_{t \in p^{m+l-j}D_{i+b}^{(p^j)}} \beta^{tu} = \sum_{i=0}^{\delta_j-1} \sum_{t \in D_{i+b}^{(p^j)}} \beta^{p^{m-s}tu}. \tag{15}$$

Note that when i passes through $\{0, 1, \ldots, \delta_j - 1\}$, $i \pmod{d_s}$ takes value $\frac{p^l-1}{2}$ times on each element in $\{0, 1, \ldots, d_s - 1\}$ and one additional time on elements in $\{0, 1, \ldots, \delta_s - 1\}$. Hence the multiset

$$\left\{tu \pmod{p^s} \mid t \in D_{i+b}^{(p^j)},\ 0 \le i \le \delta_j - 1\right\}$$

passes $\frac{p^l-1}{2}$ times through $\mathbb{Z}_{p^s}^*$, and one additional time over the union of $D_{i+k+b}^{(p^s)}$ for $0 \le i \le \delta_s - 1$. Since $\beta^{p^{m-s}}$ is a primitive p^s-th root of unity, by (15), we have

$$\mathbf{H}_{m,b}^{(p^{l+1})}(\beta^a) = \frac{p^l-1}{2} \sum_{a \in \mathbb{Z}_{p^s}^*} \beta^{p^{m-s}a} + \mathbf{H}_{m,b+k}^{(p^s)}(\beta),$$

which is $\frac{p^l-1}{2} + \mathbf{H}_{m,b+k}^{(p)}(\beta)$ if $s = 1$ and $\mathbf{H}_{m,b+k}^{(p^s)}(\beta)$ if $s \ge 2$ by Lemma 1. □

For $1 \le j \le m$ and $v \in \mathbb{Z}$, set

$$A_{m,j,v}(x) := \sum_{s=1}^{j} \mathbf{H}_{m,v}^{(p^s)}(x). \tag{16}$$

Note that $\mathbf{H}_{m,v}^{(p^s)}(\beta_m) = \mathbf{H}_{j,v}^{(p^s)}(\beta_j)$ for $s \le j$, then

$$A_{m,j,v}(\beta_m) = \sum_{s=1}^{j} \mathbf{H}_{m,v}^{(p^s)}(\beta_m) = \sum_{s=1}^{j} \mathbf{H}_{j,v}^{(p^s)}(\beta_j) = A_{j,j,v}(\beta_j).$$

Set

$$A_{j,v} := A_{j,j,v}(\beta_j) \in \mathbb{F}_2(\beta_j). \tag{17}$$

By Lemma 2 and Eqs. (10)–(11), for $a \in p^l D_k^{(p^{m-l})}$, $0 \le l < m$, let $t = m - l$, then

$$s(\beta^a) = 1 + A_{t,b+k} + A_{t,b+k}^2, \quad \widetilde{s}(\beta^a) = 1 + A_{t,b+k+\delta_t} + A_{t,b+k}^2.$$

By Lemma 1, $1 + A_{t,b+k+\delta_t} = A_{t,b+k}$. In conclusion, then we have:

Proposition 1 *For $a = 0$, one has $s(1) = \widetilde{s}(1) = 1$. For $a \in p^l D_k^{(p^{m-l})}$, $0 \le l < m$, let $t = m - l$, then*

$$s(\beta^a) = 1 + A_{t,b+k} + A_{t,b+k}^2, \tag{18}$$
$$\widetilde{s}(\beta^a) = A_{t,b+k} + A_{t,b+k}^2. \tag{19}$$

It now suffices to study the values of $A_{j,v}$ for $j \ge 1$ and $v \in \mathbb{Z}$. We first list three key identities about $A_{j,v}$:

Lemma 3 *For each $j \ge 1$ and $v \in \mathbb{Z}$, one has*

(1) $A_{j,v} = A_{j,v+d_j}$.
(2) $A_{j,v} + A_{j,v+\delta_j} = 1$.
(3) *If $2 \in D_h^{(p^j)}$, then $A_{j,v}^2 = A_{j,v+h}$.*

Proof (1) is trivial. (2) follows immediately from Lemma 1.

For (3), if $2 \in D_h^{(p^j)}$, then $2 \in D_h^{(p^s)}$ for all $s \le j$. For any i, we have $\{2t \mid t \in D_i^{(p^s)}\} = D_{i+h}^{(p^s)}$, hence $\mathbf{H}_{j,v}^{(p^s)}(\beta_j)^2 = \mathbf{H}_{j,v}^{(p^s)}(\beta_j^2) = \mathbf{H}_{j,v+h}^{(p^s)}(\beta_j)$ and (3) follows. □

Following the proof of [9, Proposition 2], we have the following essential result.

Lemma 4 *Suppose* $[\mathbb{F}_2(\beta_j):\mathbb{F}_2(\beta_{j-1})]=p$. *Then* $A_{j,v}+A_{j,v+f/2}\notin\mathbb{F}_2(\beta_{j-1})$. *In particular, for* $0<t<j$, *set*

$$A^{[t]}_{j,v}:=A_{j,v}-A_{t,v}=\sum_{s=t+1}^{j}\mathbf{H}^{(p^s)}_{j,v}(\beta_j).$$

Then $A^{[t]}_{j,v}+A^{[t]}_{j,v+f/2}\notin\mathbb{F}_2(\beta_{j-1})$, *and consequently,* $A^{[t]}_{j,v}\neq A^{[t]}_{j,v+f/2}$.

Proof Note that in our case $j\geq 2$ as $[\mathbb{F}_2(\beta_1):\mathbb{F}_2(\beta_0)]\leq p-1<p$. Let $\xi=\mathbf{H}^{(p^j)}_{j,v}(\beta_j)+\mathbf{H}^{(p^j)}_{j,v+f/2}(\beta_j)$. If $A_{j,v}+A_{j,v+f/2}\in\mathbb{F}_2(\beta_{j-1})$, then

$$\xi=(A_{j,v}+A_{j,v+f/2})-(A_{j-1,v}+A_{j-1,v+f/2})\in\mathbb{F}_2(\beta_{j-1}).$$

On the other hand, by definition we have $\xi=\sum_{k\in\mathscr{D}}\beta_j^k$, where

$$\mathscr{D}=\bigcup_{i=0}^{f/2-1}\left(D^{(p^j)}_{i+v}\cup D^{(p^j)}_{i+\delta_j+v}\right)$$

is the same $\mathscr{D}$ (with translation by v) in the proof of [9, Proposition 2]. Note that if $k_1\neq k_2\in\mathscr{D}$, then $k_1\pmod p\neq k_2\pmod p$, and the set $\mathscr{D}\mod p$ is nothing but the set $\mathbb{Z}_p^*$. We have

$$\xi=\sum_{i=1}^{p-1}c_i\beta_j^i,\quad 0\neq c_i\in\mathbb{F}_2(\beta_{j-1}).$$

Thus the minimal polynomial of β_j over $\mathbb{F}_2(\beta_{j-1})$ is of degree $[\mathbb{F}_2(\beta_j):\mathbb{F}_2(\beta_{j-1})]<p$, which leads to a contradiction. □

Lemma 5 *For* $j\geq 1$, *suppose* $2\in D^{(p^j)}_h$. *Then one of the following holds:*

(1) $2^e\not\equiv\pm 1\pmod p$, *equivalently,* $\delta_1=\frac{f}{2}\nmid h$.
(2) $2^e\equiv 1\pmod{p^a}$ *and* $2^e\not\equiv 1\pmod{p^{a+1}}$, *equivalently,* $2\in D^{(p^j)}_0$ *for* $j\leq a$ *and* $2\notin D^{(p^j)}_0$ *for* $j>a$.
(3) $2^e\equiv -1\pmod{p^a}$ *and* $2^e\not\equiv -1\pmod{p^{a+1}}$, *equivalently,* $2\in D^{(p^j)}_{\delta_j}$ *for* $j\leq a$ *and* $2\notin D^{(p^j)}_{\delta_j}$ *for* $j>a$.

Furthermore,
(4) *If* (2) *holds, then* $\mathbb{F}_2(\beta_1)=\mathbb{F}_2(\beta_a)$ *and* $[\mathbb{F}_2(\beta_j):\mathbb{F}_2(\beta_{j-1})]=p$ *for* $j>a$.
(5) *If* (3) *holds, then* $\mathbb{F}_2(\beta_1)=\mathbb{F}_2(\beta_a)$ *and* $[\mathbb{F}_2(\beta_j):\mathbb{F}_2(\beta_{j-1})]=p$ *for* $j>a$.

Proof The equivalence of different descriptions of each condition is easy to get. (4) and (5) can be proved in the same way. We only show (5) here.

Let τ_j be the order of $2\mod p^j$ and $\tau=\tau_1$. It is well-known $\mathbb{F}_2(\beta_j)=\mathbb{F}_{2^{\tau_j}}$. It suffices to show $\tau_a=\tau$ and $\tau_j=\tau p^{j-a}$ for $j>a$.

On one hand $\tau_j\mid\tau_{j+1}$. On the other hand, $2^{\tau_j}\equiv 1\mod p^j$, then $2^{\tau_j p^k}\equiv 1\mod p^{j+k}$, hence $\tau_{j+k}\mid\tau_j p^k$. The condition (3) means τ_j is a factor of $2e$ for $j\leq a$, thus $\tau_a\mid\gcd(\tau p^{a-1},2e)=\tau$, and $\mathbb{F}_2(\beta_a)=\mathbb{F}_2(\beta_1)$.

Now we have $2^\tau \equiv 1 \bmod p^a$ and $2^\tau \not\equiv 1 \bmod p^{a+1}$ (otherwise $2^{2e} \equiv 1 \bmod p^{a+1}$ and $2^e \equiv -1 \bmod p^{a+1}$). Write $2^\tau = 1 + \lambda p^a$, then $p \nmid \lambda$. For $j > a$,

$$2^{\tau p^{j-a-1}} = (1+\lambda p^a)^{p^{j-a-1}} \equiv 1 + \lambda p^{j-1} \not\equiv 1 \pmod{p^j}.$$

Hence $\tau_j \nmid \tau p^{j-a-1}$. Along with $\tau \mid \tau_j \mid \tau p^{j-a}$, one must have $\tau_j = \tau p^{j-a}$. □

Proposition 2 *For any $v \in \mathbb{Z}$, we have*

(1) *If $2^e \equiv 1 \pmod{p^j}$, then $A_{j,v} \in \mathbb{F}_2$. If $2^e \not\equiv 1 \pmod{p}$, then $A_{j,v} \notin \mathbb{F}_2$ for $j \geq 1$.*
(2) *If $2^e \equiv 1 \pmod{p}$ but $2^e \not\equiv 1 \pmod{p^2}$, then $A_{1,v} \in \mathbb{F}_2$ and $A_{j,v} \notin \mathbb{F}_4$ for $j \geq 2$.*
(3) *If $2^e \equiv -1 \pmod{p}$ but $2^e \not\equiv -1 \pmod{p^2}$, then $A_{1,v} \in \mathbb{F}_4 - \mathbb{F}_2$ and $A_{j,v} \notin \mathbb{F}_4$ for $j \geq 2$.*
(4) *If $2^e \not\equiv \pm 1 \pmod{p}$, then $A_{j,v} \notin \mathbb{F}_4$ for any $j \geq 1$.*

Proof Suppose $2 \in D_h^{(p^j)}$. We may assume $0 \leq h < d_j$.

(1) The condition $2^e \equiv 1 \pmod{p^j}$ means $h = 0$. Then Lemma 3(3) implies $A_v^2 = A_v$, hence $A_v \in \mathbb{F}_2$.

The condition $2^e \not\equiv 1 \pmod{p}$ means $2 \notin D_0^{(p)}$, hence $f \nmid h$, there exists $x_1 > 0$ such that $hx_1 \equiv \delta_j \pmod{d_j}$. By Lemma 3(2), we have

$$A_{j,v+hx_1} = A_{j,v+\delta_j} = A_{j,v} + 1.$$

On the other hand, if $A_v \in \mathbb{F}_2$, by Lemma 3(3), for all $n \in \mathbb{Z}$, we have

$$A_{j,v} = A_{j,v\pm h} = \cdots = A_{j,v+nh} \in \mathbb{F}_2.$$

This is a contradiction.

(2) The condition means $2 \in D_0^{(p)}$ but $2 \notin D_0^{(p^2)}$. That $A_{1,v} \in \mathbb{F}_2$ follows from (1). For $j \geq 2$, the assumption means $\gcd(h, d_j) = d_1 = f$ and hence $\gcd(h, \delta_j) = \delta_1 = f/2$. For $A_{j,v}^{[1]} = A_{j,v} - A_{1,v}$, by Lemma 3(2),

$$A_{j,v}^{[1]} = A_{j,v\pm\delta_j}^{[1]} = \cdots = A_{j,v+n\delta_j}^{[1]},\ n \in \mathbb{Z}.$$

If $A_{j,v} \in \mathbb{F}_2$, then $A_{j,v}^{[1]} \in \mathbb{F}_2$, and for $n \in \mathbb{Z}$,

$$A_{j,v}^{[1]} = A_{j,v\pm h}^{[1]} = \cdots = A_{j,v+nh}^{[1]} \in \mathbb{F}_2.$$

Hence $A_{j,v}^{[1]} = A_{j,v+n_1h+n_2\delta_j}^{[1]}$ for any $n_1,\ n_2 \in \mathbb{Z}$, and $A_{j,v}^{[1]} = A_{j,v+n\delta_1}^{[1]}$ for $n \in \mathbb{Z}$. In particular, $A_{j,v}^{[1]} = A_{j,v+\delta_1}^{[1]} = A_{j,v+f/2}^{[1]}$. By Lemma 5(4), $[\mathbb{F}_2(\beta_j) : \mathbb{F}_2(\beta_{j-1})] = p$ for $j \geq 2$. Then Lemma 4 implies $A_{j,v}^{[1]} \neq A_{j,v+f/2}^{[1]}$, a contradiction. Hence $A_{j,v} \notin \mathbb{F}_2$.

If $A_{j,v} \in \mathbb{F}_4 - \mathbb{F}_2$, then $A_{j,v}^{[1]} \in \mathbb{F}_4 - \mathbb{F}_2$, we have $A_{j,v+h}^{[1]} = (A_{j,v}^{[1]})^2 = A_{j,v}^{[1]} + 1$ and $A_{j,v+2h}^{[1]} = A_{j,v}^{[1]}$; and $(A_{j,v-h}^{[1]})^2 = A_{j,v}^{[1]} = (A_{j,v}^{[1]} + 1)^2$, $A_{j,v-h}^{[1]} = A_{j,v}^{[1]} + 1$ and $A_{j,v-2h}^{[1]} = A_{j,v}^{[1]}$. Again we get $A_{j,v}^{[1]} = A_{j,v+n\delta_1}^{[1]}$, which is impossible by Lemma 4.

(3) The condition means $2 \in D_{\delta_1}^{(p)}$ but $2 \notin D_{\delta_2}^{(p^2)}$. Hence

$$A_{1,v}^2 = A_{1,v+\delta_1} = A_{1,v} + 1$$

and $A_{1,v} \in \mathbb{F}_4$. For $j \geq 2$, then $(A_{j,v}^{[1]})^2 = A_{j,v+h}^{[1]}$. If $A_{j,v}^{[1]} \in \mathbb{F}_2$, we have $A_{j,v+h}^{[1]} = A_{j,v}^{[1]}$, If $A_{j,v}^{[1]} \in \mathbb{F}_4 - \mathbb{F}_2$, we have $A_{j,v\pm 2h}^{[1]} = A_{j,v}^{[1]}$. Since by assumption, $\gcd(h, \delta_j) = \gcd(2h, \delta_j) =$

δ_1, we get $A_{j,v}^{[1]} = A_{j,v+n\delta_1}^{[1]}$. By Lemma 5(5), $[\mathbb{F}_2(\beta_j) : \mathbb{F}_2(\beta_{j-1})] = p$, and by Lemma 4, $A_{j,v}^{[1]} \neq A_{j,v+\delta_1}^{[1]}$. We get a contradiction.

(4) The condition means $\frac{f}{2} \nmid h$, in particular $\frac{f}{2} = 2^{r-1}$ is even and there exists an even integer $x_1 > 0$ such that $hx_1 \equiv \frac{f}{2} \pmod{f}$. If $A_{j,v} \in \mathbb{F}_4$, by the proof of (1), we may assume $A_{j,v} = \epsilon_0 \notin \mathbb{F}_2$, thus $\epsilon_0^2 + \epsilon_0 + 1 = 0$. By Lemma 3(2),

$$\epsilon_{p^{j-1}hx_1} := A_{j,v+p^{j-1}hx_1} = A_{j,v+\delta_j} = A_{j,v} + 1 = \epsilon_0 + 1.$$

By Lemma 3(3), we have $\epsilon_1 = A_{j,v+h} = \epsilon_0^2 = \epsilon_0 + 1$, $\epsilon_2 = A_{j,v+2h} = \epsilon_1^2 = \epsilon_0$, hence $\epsilon_0 = \epsilon_2 = \cdots = \epsilon_{p^{j-1}hx_1}$. This is a contradiction. $\square$

Remark For the case $2^e \equiv \pm 1 \pmod{p^a}$ but $\not\equiv \pm 1 \pmod{p^{a+1}}$ for $a > 1$, if $j \geq 2a$, we can imitate the proof of Lemma 4 and Proposition 2 (i.e., the method in the proof of [9, Proposition 2]) to show $A_{j,v} \notin \mathbb{F}_4$. However, we don't know how to treat the case $a < j < 2a$.

We are now ready to prove our main results by applying Propositions 1 and 2.

Proof of Theorem 1 If $2^e \equiv 1 \pmod{p}$ but $2^e \not\equiv 1 \pmod{p^2}$, then $A_{1,v} \in \mathbb{F}_2$ and $A_{j,v} \notin \mathbb{F}_4$ for $j \geq 2$, in both cases, $s(\beta^a) = 1 \neq 0$. If $2^e \not\equiv \pm 1 \pmod{p}$, then $\delta_1 \nmid h$ and $A_{j,v} \notin \mathbb{F}_4$, hence $s(\beta^a) \neq 0$. Therefore $\mathrm{LC}(\mathbf{s}^\infty) = 2p^m$.

If $2^e \equiv -1 \pmod{p}$ but $2^e \not\equiv -1 \pmod{p^2}$, then $A_{1,v} \in \mathbb{F}_4 - \mathbb{F}_2$ and $A_{j,v} \notin \mathbb{F}_4$ for $j \geq 2$. Hence $s(\beta^a) = 0$ for $a \in p^{m-1}\mathbb{Z}_p^*$ and $s(\beta^a) \neq 0$ for all other a's. Hence $2p^m - 2(p-1) \leq \mathrm{LC}(\mathbf{s}^\infty) \leq 2p^m - (p-1)$. $\square$

Proof of Theorem 2 If $2^e \not\equiv 1 \pmod{p}$, then $2 \notin D_0^{(p)}$. Hence $A_{j,v} \notin \mathbb{F}_2$ for all j and $\widetilde{s}(\beta^a) \neq 0$. Therefore $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 2p^m$.

If $2^e \equiv 1 \pmod{p}$ but $2^e \not\equiv 1 \pmod{p^2}$, then only $A_{1,v} \in \mathbb{F}_2$ and $\widetilde{s}(\beta^a) = 0$ for $a \in p^{m-1}\mathbb{Z}_p^*$. For all other a, $\widetilde{s}(\beta^a) \neq 0$. Hence $2p^m - 2(p-1) \leq \mathrm{LC}(\widetilde{\mathbf{s}}^\infty) \leq 2p^m - (p-1)$. $\square$

4 Numerical evidence

By using Magma, we compute the following examples to check our results.

Example 1 Let $p = 7$, $m = 2$ and $g = 3$. Take $f = 2$ and $e = 3$, then $2^3 \equiv 1 \pmod{p}$ and $2^3 \not\equiv 1 \pmod{p^2}$. For $b = 0$,

$$\begin{aligned} \mathbf{s}^\infty =& \dot{1}110111011001110010000000111111010001101010101010 \\ & 010101010101001110100000001111110110001100100010\dot{0}, \\ \widetilde{\mathbf{s}}^\infty =& \dot{1}101110111001101100010101101010000100111111111111 \\ & 000000000000011011110101001010111001001100010001\dot{0}. \end{aligned}$$

Then $\mathrm{LC}(\mathbf{s}^\infty) = 98 = 2p^m$ and $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 89 = 2p^m - (p-1) - e$, consistent with Theorems 1(1) and 2(2).

Example 2 Let $p = 5$, $m = 2$ and $g = 3$. Then f can be taken either 2 or 4.

Table 1 $\mathrm{LC}(\mathbf{s}^\infty)$ for $2^e \equiv -1 \bmod p$ but $\not\equiv -1 \pmod{p^2}$

p	m	e	g	b	$\mathrm{LC}(\mathbf{s}^\infty)$	$2p^m-(p-1)$
5	2	2	3	0, 1, 3	46	46
	3				246	246
	4				1246	1246
11	2	5	7	2, 19	232	232
13	2	6	7	6, 11	326	326
			11	5, 12		
	3		7	5, 12	4382	4382
			11			
17	1	4	3	0, 3	18	18
			5			
	2		3	0, 2	562	562
			5	0, 7		
19	2	9	3	1, 6	704	704
			13	3, 22		

(i) If one takes $f = 2$, then $e = 2$, $2^2 \equiv -1 \pmod{p}$ and $2^2 \not\equiv -1 \pmod{p^2}$. For $b = 0$,

$$\mathbf{s}^\infty = \dot{1}11111100110100000011000100010001100000010110011111\dot{1},$$
$$\widetilde{\mathbf{s}}^\infty = \dot{1}10101001100000101101101110111011000001000001100101 0\dot{1}.$$

Then $\mathrm{LC}(\mathbf{s}^\infty) = 46 = 2p^m - (p-1)$ and $\mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 50 = 2p^m$, consistent with Theorems 1(2) and 2(1).

(ii) If one takes $f = 4$, then $e = 1$, $2 \not\equiv 1 \pmod{p}$. For $b = 0$,

$$\mathbf{s}^\infty = \dot{1}11111101111100110100010100101110100110000010000 0\dot{0},$$
$$\widetilde{\mathbf{s}}^\infty = \dot{1}10101000101001100001000001110111100110101110101\dot{0}.$$

Then $\mathrm{LC}(\mathbf{s}^\infty) = \mathrm{LC}(\widetilde{\mathbf{s}}^\infty) = 50 = 2p^m$, consistent with Theorems 1(1) and 2(1) respectively.

Example 3 Let $p = 31$, $m = 1$, $g = 3$ and $e = 15$. Then $2^{15} \equiv 1 \pmod{31}$ and $2^{15} \not\equiv 1 \pmod{31^2}$. For $b = 0$,

$$\mathbf{s}^\infty = \dot{1}110110111100010101110000100100011011011110001010111000010010\dot{0},$$
$$\widetilde{\mathbf{s}}^\infty = \dot{1}100011101001000000100101110001001110001011011111101101000111\dot{0}.$$

Then $\mathrm{LC}(\mathbf{s}^\infty) = 62 = 2p$ and $\mathrm{LC}(\mathbf{s}^\infty) = 17 = 2p - (p-1) - e$, consistent with Theorems 1(1) and 2(2).

Because of the above examples, we form our conjecture and try more examples in Table 1.

5 Conclusion

In this paper, we introduced two generalized cyclotomic binary sequences of period $2p^m$, which include the sequences in [13,25] as special cases. We computed their linear complexity in most cases (all cases for p a non-Wieferich odd prime) and showed each of our sequences is of high linear complexity if $m \geq 2$.

Acknowledgements Y. O. would like to thank the Morningside Center of Mathematics for hospitality where part of this paper was written. We thank the referees for many helpful comments, especially for providing a counterexample for a previous conjecture about the linear complexity of sequences in the second class.

References

1. Bai E., Liu X., Xiao G.: Linear complexity of new generalized cyclotomic sequences of order two of length pq. IEEE Trans. Inf. Theory **51**(5), 1849–1853 (2005).
2. Chang Z., Li D.: On the linear complexity of generalized cyclotomic binary sequence of length $2pq$. Concurr. Comput. Pract. Exp. **26**(8), 1520–1530 (2014).
3. Cusick T., Ding C., Renvall A.: Stream Ciphers and Number Theory. North-Holland Mathematical Library, vol. 55, pp. 198–212. Elsevier, Amsterdam (1998).
4. Ding C.: Binary cyclotomic generators. Fast Software Encryption. LNCS, vol. 1008, pp. 29–60. Springer, Leuven (1995).
5. Ding C.: Linear complexity of generalized cyclotomic binary sequences of order 2. Finite Fields Appl. **3**, 159–174 (1997).
6. Ding C., Helleseth T.: New generalized cyclotomy and its applications. Finite Fields Appl. **4**, 140–166 (1998).
7. Ding C., Helleseth T.: Generalized cyclotomy codes of length $p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}$. IEEE Trans. Inf. Theory **45**(2), 467–474 (1999).
8. Edemskiy V.: About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. Des. Codes Cryptogr. **61**, 251–260 (2011).
9. Edemskiy V., Li C., Zeng X., Helleseth T.: The linear complexity of generalized cyclotomic binary cyclotomic sequences of period p^n. Des. Codes Cryptogr. (2018). https://doi.org/10.1007/s10623-018-0513-2.
10. Golomb S.W.: Shift register sequence. Holden Day, San Francisco (1967).
11. Hu H.G., Gong G.: New sets of zeros or low correlation zone sequences via interleaving technique. IEEE Trans. Inf. Theory **56**, 1702–1713 (2010).
12. Hu L., Yue Q., Wang M.: The linear complexity of Whiteman's generalized cyclotomic sequences of period $p^{m+1}q^{n+1}$. IEEE Trans. Inf. Theory **58**, 5534–5543 (2012).
13. Ke P.H., Zhang J., Zhang S.Y.: On the of linear complexity and the autocorrelation of generalized cyclotomic binary sequences with the period $2p^m$. Des. Codes Cryptogr. **67**(3), 325–339 (2013).
14. Kim Y. J., Song H. Y.: Linear complexity of prime n-square sequences. In: IEEE International Symposium on Information Theory, Toronto, Canada, pp. 2405–2408 (2008).
15. Kim Y.J., Jin S.Y., Song H.Y.: Linear complexity and autocorrelation of prime cube sequences. LNCS, vol. 4851, pp. 188–197. Springer, Berlin (2007).
16. Li D.D., Wen Q.Y.: Linear complexity of generalized cyclotomic binary sequences with period $2p^{m+1}q^{n+1}$. IEICE Trans. Fund. Electron. E **98A**, 1244–1254 (2015).
17. Liu F., Peng D.Y., Tang X.H.: On the autocorrelation and the linear complexity of q-ary prime n-square sequence. Sequences and Their Applications. LNCS, vol. 6338, pp. 139–150. Springer, Berlin (2010).
18. Park Y.H., Hong D., Chun E.: On the linear complexity of some generalized cyclotomic sequences. Int. J. Algebra Comput. **14**(4), 431–439 (2004).
19. Whiteman A.L.: A family of difference sets. Illionis J. Math. **6**(1), 107–121 (1962).
20. Xiao Z.B., Zeng X.Y., Li C.L., Helleseth T.: New generalized cyclotomic binary sequences of period p^2. Des. Codes Cryptogr. **86**, 1483–1497 (2018).
21. Yan T.: Some notes on the generalized cyclotomic binary sequences of length $2p^m$ and p^m. IEICE Trans. Fund. **E96–A 10**, 2049–2051 (2013).
22. Yan T., Sun R., Xiao G.: Autocorrelation and linear complexity of the new generalized cyclotomic sequences. IEICE Trans. Fund. Electron. **E90–A**, 857–864 (2007).
23. Ye Z.F., Ke P.H., Wu C.H.: A further study on the linear complexity of new binary cyclotomic sequence of length p^r. arXiv:1712.08886V2 [cs.CR] 15 Mar 2018.
24. Zeng X., Cai H., Tang X., Yang Y.: Optimal frequency hopping sequences of odd length. IEEE Trans. Inf. Theory **59**(5), 3237–3248 (2013).

25. Zhang J.W., Zhao C.A., Ma X.: Linear complexity of generalized cyclotomic binary sequences of length $2p^m$. Applicable Algebra in Engineering, Communication and Computing, vol. 21, pp. 93–108. Springer, Berlin (2010).