Symmetric 2-Adic Complexity of Generalized Cyclotomic Sequences with Period $2p^n$

VALDIMIR EDEMSKIY[1], XIANGYONG ZENG[2], ZHIMIN SUN[3], YUAN CHEN[2]
[1]Department of Applied Mathematics and Information Science,
Yaroslav-the-Wise Novgorod State University,
Veliky Novgorod,
RUSSIA

[2]Faculty of Mathematics and Statistics,
Hubei Key Laboratory of Applied Mathematics,
Hubei University,
Wuhan, Hubei,
CHINA

[3]School of Cyber Science and Technology,
Hubei Key Laboratory of Applied Mathematics,
Hubei University,
Wuhan, Hubei,
CHINA

Abstract: - Using the cyclotomic classes and generalized cyclotomic classes for sequence design is a well known method. In this paper, we study the symmetric 2-adic complexity of sequences based on generalized cyclotomic classes of order two. These sequences with period $2p^n$ have high linear complexity. We show that the 2-adic complexity of these sequences is good enough to resist the attack of the rational approximation algorithm. The 2-adic complexity is the measure of the predictability of a sequence which is important for cryptographic applications. Our method of studying 2-adic complexity is based on using the generalized "Gauss periods".

Key-Words: - Binary Sequence, 2-Adic Complexity, Cyclotomy, Generalized Cyclotomic Sequence, Gauss Period, Symmetric 2-Adic Complexity.

Received: October 11, 2024. Revised: January 27, 2025. Accepted: February 26, 2025. Published: April 17, 2025.

1 Introduction

Pseudo-random sequences are widely used in secure and reliable communications. They have a lot of characteristics like period, auto-correlation, and complexity of sequences. Any binary periodic pseudo-random sequences can be generated by linear feedback shift registers (LFSRs) or feedback with carry shift registers (FCSRs). The rational approximation algorithm (resp. Berlekamp-Massey algorithm) showed that any binary periodic sequence having 2-adic complexity m (resp. linear complexity l) can be completely determined by its $2m$ (resp. $2l$) consecutive bits, where the 2-adic complexity (resp. linear complexity) is defined as the length of the shortest FCSRs (resp. LFSRs) that can generate the sequence.

Using the cyclotomic classes and generalized cyclotomic classes is a well known method of designing sequences with high linear complexity, [1], [2], [3], [4], [5]. The 2-adic complexity is another important measure of the predictability of a sequence. Thus, it is useful to study the 2-adic complexity of binary sequences with large linear complexity.

2-adic complexity of sequences with ideal two-level auto-correlation was completely determined by computing the determinant of a circulant matrix and the greatest common divisor of two numbers, which are associated with the corresponding sequences, [6]. This method was further used to study the 2-adic complexity of interleaved sequences, [7]. Furthermore, applying the property of ideal two-level auto-correlation, a simple method was

proposed to show that ideal two-level auto-correlation periodic sequences have the optimal 2-adic complexity, [8]. This approach was extended to study the 2-adic complexity of the two-prime generator [9] and binary sequences with period $4N$ and optimal auto-correlation magnitude, [10]. Among the ideal two-level auto-correlation periodic sequences mentioned above, Legendre sequences were constructed based on the classical cyclotomy of order two, and their 2-adic complexities are optimal, [6], [8], [9]. For other binary cyclotomic sequences of order two having large linear complexity, by the method in [6], the 2-adic complexity of Ding-Helleseth binary sequences with period p^2 was proved to attain the maximal value [10] and a lower bound on 2-adic complexity of Ding-Helleseth binary sequences with period p^n was given, which is larger than $\frac{p^n+1}{2}$, [11]. Other issue for studying of 2-adic complexity was propose in [12], where using generalized "Gauss periods" for derivate of 2-adic complexity of Ding-Helleseth-Martinsen binary sequences with a period $2p$. Further, according to [13], the symmetric 2-adic complexity is better than the 2-adic complexity in measuring the security of a binary periodic sequence.

In this paper, we study the symmetric 2-adic complexity of sequences are based on generalized cyclotomic classes of order two. These generalized binary cyclotomic sequences with period $2p^n$ were proposed in [3] and according to [3] they have high linear complexity. For any of these sequences, to determine its 2-adic complexity, it suffices to find the greatest common divisor $S(2)$ and $2^{2p^n}-1$, where $S(x)$ is the generating polynomial of the sequence. To do this, we will use generalized "Gauss periods" proposed in [12]. Consequently, it is proved that the 2-adic complexity of these sequences is optimal. Our results show that the symmetric 2-adic complexity of these sequences is large enough to resist the attack of the rational approximation algorithm.

The remainder of this paper is organized as follows. In Section 2, we introduce some basic concepts and the main result. In Section 3, the properties of generalized polynomials of sequences and subsidiary Lemmas are given. Section 4 gives the proof of the main result and completely determines the symmetric 2-adic complexity of sequences.

2 Preliminaries

Throughout this paper, we will denote by $\mathbb{Z}_N$ the residue class ring modulo N for a positive integer N, and by $\mathbb{Z}_N^*$ the multiplicative group of $\mathbb{Z}_N$.

2.1 Generalized Cyclotomic Sequences

Let p be an odd prime and n be a positive integer. Assume that g is an odd primitive root modulo p^n. Then g is also a primitive root modulo $2p^n$, [14]. Below we recall the notation of Ding-Helleseth generalized cyclotomic classes of order two [15] and the definition of generalized cyclotomic sequences proposed in [3].

For $j = 1,2,\cdots,n$ and $i = 0,1$, we put:

$$D_i^{(p^j)}=\{g^{i+2t}(\mathrm{mod}\ p^j) \mid 0\le t<p^{j-1}(p-1)/2\};$$
$$D_i^{(2p^j)}=\{g^{i+2t}(\mathrm{mod}\ 2p^j) \mid 0\le t<p^{j-1}(p-1)/2\}. \quad (1)$$

Here and hereafter a mod q denotes the least nonnegative integer that is congruent to a modulo q. The cosets $D_i^{(p^j)}$, $i = 0,1$ are called Ding-Helleseth generalized cyclotomic classes of order 2 with respect to p^j. By the definition, we have that $|D_i^{(p^j)}| = |D_i^{(2p^j)}| = p^{j-1}(p-1)/2$ for $i = 0,1$. It is obvious that $\left\{D_0^{(2p^j)}, D_1^{(2p^j)}\right\}$ forms a partition of $\mathbb{Z}_{2p^j}^*$ and

$$\mathbb{Z}_{2p^n} = \bigcup_{j=1}^{n} p^{n-j}(D_0^{(2p^j)} \cup D_1^{(2p^j)} \cup 2D_0^{(p^j)} \cup 2D_1^{(p^j)}) \cup \{0, p^n\}.$$

As in [3], let $H_i^{(p^j)} = p^{n-j}D_i^{(p^j)}$ and $H_i^{(2p^j)} = p^{n-j}D_i^{(2p^j)}$ for $i = 0,1$. Throughout this paper, the subscripts in $D_i^{(p^j)}$, $D_i^{(2p^j)}$, $H_i^{(p^j)}$ and $H_i^{(2p^j)}$ are computed modulo 2. Set

$$C_1 = \bigcup_{j=1}^{n} \left(H_{i_j}^{(2p^j)} \cup 2H_{i_j}^{(p^j)}\right) \cup \{0\}$$

and $C_0 = \mathbb{Z}_{2p^n} \backslash C_1$, where $(i_1, i_2, \dots, i_n) \in \square_2^n$ is a defining vector and

$$\tilde{\imath}_j = \begin{cases} i_j, & \text{if } p \equiv \pm 1(\mathrm{mod}\ 8), \\ i_j + 1(\mathrm{mod}2), & \text{if } p \equiv \pm 3(\mathrm{mod}\ 8). \end{cases} \quad (2)$$

Then generalized cyclotomic sequences $u^\infty = (u_0, u_1, u_2, \dots)$ with period $2p^n$ can be defined as

$$u_i = \begin{cases} 0, & \text{if } i(\mathrm{mod}\ 2p^n) \in C_0, \\ 1, & \text{if } i(\mathrm{mod}\ 2p^n) \in C_1. \end{cases} \quad (3)$$

Example. Let $n = 2, (i_1, i_2) = (0,1)$. Suppose $p = 5$. Then $D_0^{(p)} = \{1,4\}$, $D_1^{(p)} = \{2,3\}$, $D_0^{(2p)} = \{1,9\}$,

$D_1^{(2p)} = \{3,7\}$, $D_0^{(p^2)} = \{1,4,6,9,11,14,16,19,21,24\}$, $D_1^{(p^2)} = \{2,3,7,8,12,13,17,18,22,23\}$, $D_0^{(2p^2)} = \{1,9,11,19,21,29,31,39,41,49\}$, $D_1^{(2p^2)} = \{3,7,13,17,23,27,33,37,43,47\}$, and $(\tilde{\imath}_0, \tilde{\imath}_1) = (1,0)$. Thus, $C_0 = D_1^{(2p^2)} \cup D_0^{(p)} \cup 2D_0^{(p^2)} \cup pD_1^{(p)}$.

2.2 Adic Complexity

The linear complexity and auto-correlation of these sequences were studied in [3]. In this paper, we will consider the 2-adic complexity of these sequences.

The 2-adic complexity was first studied in [16], [17]. Below we recall the definition of the 2-adic complexity of a sequence in [16].

Let $s^\infty = (s_0, s_1, \dots, s_N)^\infty$ be a binary sequence with period N, where N is a positive integer. Its generating polynomial is $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$. Then the 2-adic complexity of s^∞ can be defined as

$$\Phi(s^\infty) = \left\lfloor \log_2 \left(\frac{2^N - 1}{\gcd(S(2), 2^N - 1)} + 1 \right) \right\rfloor, \quad (4)$$

where $\lfloor x \rfloor$ is the greatest integer that is no more than x, and $\gcd(a, b)$ denotes the greatest common divisor of two integers a and b. Particularly, $\Phi(s^\infty) = N$ if and only if $\gcd(S(2), 2^N - 1) = 1$. In this case, the 2-adic complexity of the binary periodic sequence reaches the maximal value.

3 Main Result

Using the generalized "Gauss periods" to compute $\gcd(S(2), 2^N - 1)$, we get the main result of this paper as below.

Theorem 3.1 Let u^∞ be the generalized cyclotomic sequence defined by (3). Then $\Phi(u^\infty) = 2p^n$.

3.1 The Properties of $S(2)$

In this section, we give some subsidiary lemmas on the basis of the properties of generalized cyclotomic classes and present the definition and the property of "Gauss periods", which will be used to compute the 2-adic complexity of u^∞ defined in (3). By (4), we need to study the greatest common divisor of $S(2)$ and $2^{2p^n} - 1$. In this section we study $S(2) (\mathrm{mod} \frac{2^{p^{m+1}} \pm 1}{2^{p^m} \pm 1})$, since

$$2^{p^n} \pm 1 = \frac{2^{p^n} \pm 1}{2^{p^{n-1}} \pm 1} \cdot \frac{2^{p^{n-1}} \pm 1}{2^{p^{n-2}} \pm 1} \cdot \dots \cdot (2^p \pm 1).$$

We also show how these residues are connected with Gauss periods. First, we investigate the properties of generalized cyclotomic classes.

3.2 The Properties of Generalized Cyclotomic Classes

The properties of generalized cyclotomic classes are well-known. Here we only list some necessary properties for further use in the following lemma.

Lemma 3.1 With the notations as above, let l and k be two integers with $1 \le l < k \le n$. For $i = 0,1$, we have:

(i) $D_i^{(p^k)} (\mathrm{mod} p^l) = D_i^{(p^l)}$ and $D_i^{(2p^k)} (\mathrm{mod} 2p^l) = D_i^{(2p^l)}$;

(ii) if $b \in 2D_i^{(p^l)}$, then $(b + 2tp^l) (\mathrm{mod} 2p^k) \in 2D_i^{(p^k)}$; and if $b \in D_i^{(2p^l)}$, then $(b + 2tp^l) (\mathrm{mod} 2p^k) \in D_i^{(2p^k)}$ for any $t \in \mathbb{Z}_N$;

(iii) $2D_i^{(p^k)} = \{b, b + 2p^l, \dots, b + 2(p^{k-l} - 1)p^l \mid b \in 2D_i^{(p^l)}\}$ and $D_i^{(2p^k)} = \{b, b + 2p^l, \dots, b + 2(p^{k-l} - 1)p^l \mid b \in D_i^{(2p^l)}\}$.

Proof: (i) The statements can be obtained by (1).

(ii) Note that g is an odd primitive root modulo both p^n and $2p^n$, from the definitions of $D_i^{(p^l)}$ and $D_i^{(2p^l)}$, we have $2D_i^{(p^l)} \subset 2D_i^{(p^k)}$ and $D_i^{(2p^l)} \subset D_i^{(2p^k)}$ for $i = 0,1$. Since $b + 2tp^l \equiv b (\mathrm{mod} 2p^l)$, the second conclusion follows from (1).

(iii) Let $H \triangleq \{b, b + 2p^l, \dots, b + 2(p^{k-l} - 1)p^l \mid b \in 2D_i^{p^l}\}$. For any element $x \in H$, we have $x \in 2D_i^{(p^k)}$ by (1) and (2). Hence $H \subseteq 2D_i^{(p^k)}$. On the other hand, the order of $|H| = \left|2D_i^{(p^l)}\right| \cdot p^{k-l} = \frac{p^{l-1}(p-1)}{2} \cdot p^{k-l} = \frac{p^{k-1}(p-1)}{2}$. Then $|H| = |2D_i^{(p^k)}|$ by (1). Therefore, we have $H = 2D_i^{(p^k)}$.

Similarly, we get $D_i^{(2p^k)} = \{b, b + 2p^l, \dots, b + 2(p^{k-l} - 1)p^l \mid b \in D_i^{(2p^l)}\}$.

3.3 Subsidiary Lemmas

Now, we derive $S(2) (\mathrm{mod} \frac{2^{p^{m+1}} \pm 1}{2^{p^m} \pm 1})$ in this subsection.

Lemma 3.2 Let $m = 0,1, \dots, n-1$ and $k = 1,2, \dots, n$. For $i = 0,1$, we have

$$\sum_{f\in p^{n-k}D_i^{(2p^k)}} 2^f \pmod{\frac{2^{2p^{m+1}}-1}{2^{2p^m}-1}}$$
$$= \begin{cases} 2^{p^{n-k}}p^{k-1}(p-1)/2, & \text{if } k<n-m, \\ p^{n-m-1}\sum_{f\in D_i^{(2p)}} 2^{fp^m}, & \text{if } k=n-m, \\ 0, & \text{otherwise} \end{cases}$$

and

$$\sum_{f\in 2p^{n-k}D_i^{(p^k)}} 2^f \pmod{\frac{2^{2p^{m+1}-1}}{2^{2p^m}-1}}$$
$$= \begin{cases} p^{k-1}(p-1)/2, & \text{if } k<n-m, \\ p^{n-m-1}\sum_{f\in 2D_i^{(p)}} 2^{fp^m}, & \text{if } k=n-m, \\ 0, & \text{otherwise} \end{cases}$$

Proof: Since the second statement can be proved by the same method as the first one, its proof is omitted here. Next, we prove the first statement.

According to the value of k, we consider the three cases.

(i) Let $k<n-m$. Then $n-k>m$ and $2^f \equiv 2^{p^{n-k}} (\mathrm{mod} 2^{2p^{m+1}}-1)$ for $f\in p^{n-k}D_i^{(2p^k)}$. Thus, we get

$$\sum_{f\in p^{n-k}D_i^{(2p^k)}} 2^f \pmod{\frac{2^{2p^{m+1}}-1}{2^{2p^m}-1}} = 2^{p^{n-k}}p^{k-1}(p-1)/2.$$

(ii) Suppose $k=n-m$, then $n-k=m$. By Lemma 3.1 (iii), for $l=1$, we get $p^m D_i^{(2p^k)} = p^m\{b, b+2p, \dots, b+2(p^{k-1}-1)p \mid b\in D_i^{(2p)}\}$.

Hence $\sum_{f\in p^m D_i^{(2p^k)}} 2^f \pmod{\frac{2^{2p^{m+1}-1}}{2^{2p^m}-1}} = p^{k-1}\sum_{f\in D_i^{(2p)}} 2^{fp^m}$.

(ii) Let $k>n-m$. It follows$m-n+k>0$.

According to Lemma 3.1 (iii), we have $p^{n-k}D_i^{(2p^k)} = \{bp^{n-k}, bp^{n-k}+2p^m, \dots, bp^{n-k}+2(p^{n-m}-1)p^m \mid b\in D_i^{(2p^{m-n+k})}\}$.

Since

$$2^{bp^{n-k}} + 2^{bp^{n-k}+2p^m} + \cdots + 2^{bp^{n-k}+2(p^{n-m}-1)p^m} = 2^{bp^{n-k}}\frac{2^{2p^n}-1}{2^{2p^m}-1}$$

and $\frac{2^{2p^{m+1}}-1}{2^{2p^m}-1}$ divides $\frac{2^{2p^n}-1}{2^{2p^m}-1}$, it follows that

$$\sum_{f\in p^{n-k}D_i^{(2p^k)}} 2^f \pmod{\frac{2^{2p^{m+1}-1}}{2^{2p^m}-1}} = 0$$

in this case.

The following lemmas will be heavily used to investigate the 2-adic complexity of u^∞ in Section 4.

Lemma 3.3 Let u^∞ be defined by (3) and $S(x)=\sum_{i=0}^{2p^n-1} u_i x^i$ be its generating polynomial. Then

(i) $S(2)(\mathrm{mod}\frac{2^{p^{m+1}}-1}{2^{p^m}-1}) = p^{n-m-1}\left(\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m}\right) + p^{n-m-1}$;

(ii) $S(2)(\mathrm{mod}\frac{2^{p^{m+1}}+1}{2^{p^m}+1}) = p^{n-m-1}\left(\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m}\right) + 1$.

Proof: By definitions of the sequence u^∞ and $S(x)$, we have $S(2) = 1+\sum_{k=1}^{n}\sum_{i\in H_{i_k}^{(2p^k)}\cup 2H_{i_k}^{(p^k)}} 2^i = 1+\sum_{k=1}^{n-m-1}\left(\sum_{i\in p^{n-k}D_{i_k}^{(2p^k)}} 2^i + \sum_{i\in 2p^{n-k}D_{i_k}^{(p^k)}} 2^i\right) + \sum_{k=n-m+1}^{n}\sum_{i\in p^{n-k}(D_{i_k}^{(2p^k)}\cup 2D_{i_k}^{(p^k)})} 2^i + \sum_{i\in p^m D_{i_{n-m}}^{(2p^{n-m})}} 2^i + \sum_{i\in 2p^m D_{i_{n-m}}^{(p^{n-m})}} 2^i$.

According to Lemma 3.2, we get $S(2)\left(\mathrm{mod}\ \frac{2^{2p^{m+1}}-1}{2^{2p^m}-1}\right) p^{n-m-1}\sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m} + 1 + \frac{p-1}{2}\sum_{k=1}^{n-m-1}\left(2^{p^{n-k}}+1\right)p^{k-1} + p^{n-m-1}\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m}$. (5)

Let $A=\frac{p-1}{2}\sum_{k=1}^{n-m-1}(2^{p^{n-k}}+1)p^{k-1}$ and consider it in two cases.

(i) Since $2^{p^{n-k}}\equiv 1(\mathrm{mod} 2^{p^{m+1}}-1)$ for $k\le n-m-1$, it follows that

$$A \equiv \sum_{k=1}^{n-m-1} p^{k-1}(p-1)(\mathrm{mod}\ 2^{p^{m+1}}-1).$$

Hence $A\equiv p^{n-m-1}-1(\mathrm{mod}\ 2^{p^{m+1}}-1)$. Thus, the first statement of this lemma follows from (5).

(ii) Here we observe that $2^{p^{n-k}}\equiv -1(\mathrm{mod}\ 2^{p^{m+1}}+1)$ for $k\le n-m-1$, then $A\equiv 0(\mathrm{mod}\ 2^{p^{m+1}}+1)$. Hence, we also obtain (ii) from (5).

Lemma 3.4 With the notations as above, we have

(i) $\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m} \equiv 2\sum_{f\in D_{i_{n-m}}^{(p)}} 2^{fp^m} (\mathrm{mod}\ 2^{p^{m+1}}-1)$;

(ii) $\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m} \equiv 0 (\mathrm{mod}\ 2^{p^{m+1}}+1)$.

Proof: It is well known that $2 \in D_0^{(p)}$ when $p \equiv \pm 1(\mathrm{mod}\ 8)$ and $2 \in D_1^{(p)}$ when $p \equiv \pm 3(\mathrm{mod}\ 8)$.

Hence, if $h \in D_i^{(p)}$ with $i = 0,1$, then $2h(\mathrm{mod}\ p) \in D_i^{(p)}$ for $p \equiv \pm 1(\mathrm{mod}\ 8)$ and $2h(\mathrm{mod}\ p) \in D_{i+1}^{(p)}$ for $p \equiv \pm 3(\mathrm{mod}\ 8)$. Based on this, the statements (i) and (ii) will be proved as below.

(i) If $f \in D_{i_{n-m}}^{(2p)}$, then $f(\mathrm{mod} p) \in D_{i_{n-m}}^{(p)}$ by (1).

Furthermore, we get that $f(\mathrm{mod} p) \in D_{i_{n-m}}^{(p)}$ by (2) if $f \in 2D_{i_{n-m}}^{(p)}$. This completes the proof of (i).

(ii) If $f \in D_{i_{n-m}}^{(2p)}$, then $f(\mathrm{mod} p) \in D_{i_{n-m}}^{(p)}$ and f is odd. Hence $f + p = 2l$. It follows $f \equiv 2l(\mathrm{mod} p)$. By (2) and the above analysis, we get $l(\mathrm{mod} p) \in D_{i_{n-m}}^{(p)}$. From (1), we have that $(f+p)(\mathrm{mod} p) = 2l(\mathrm{mod} p) \in 2D_{i_{n-m}}^{(p)}$. Note that $2^{fp^m} \equiv -2^{(f+p)p^m} (\mathrm{mod}\ 2^{p^{m+1}}+1)$, then

$$\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m} \equiv 0 (\mathrm{mod}\ 2^{p^{m+1}}+1).$$

This completes the proof of Lemma 3.4.

According to Lemma 3.4, to determine the $\gcd(S(2), 2^{2p^n}-1)$, it suffices to study the sums obtained.

3.4 Generalized "Gauss Periods"

To compute the 2-adic complexity of sequences defined by (3), we generalize the notion of "Gauss periods" presented in [12] to determine the greatest common divisor of two integers $S(2)$ and $2^{2p^n}-1$. In this subsection, we introduce the definition and properties of the generalized "Gauss periods".

Let $a = 2^{p^m}$. The generalized "Gauss periods" is defined as:

$$\eta_i(a) = \sum_{j\in D_i^{(p)}} a^j, \qquad i = 0,1.$$

By Lemma 3.4, we have $\sum_{f\in D_i^{(p)}} 2^{fp^m} = \eta_i(2^{fp^m})$. Thus, the values $S(2)(\mathrm{mod}\frac{2^{p^{m+1}}\pm 1}{2^{p^m}\pm 1})$ are determined by the generalized "Gauss periods". In conclusion of Subsection 3.3 we recall some of their properties.

It is clear that $\eta_i(a^b) \equiv \eta_i(a)(\mathrm{mod} a^p - 1)$ for $b \in D_0^{(p)}$ and

$$\eta_0(a) + \eta_1(a) = \frac{a^p-1}{a-1} - 1. \qquad (6)$$

The following property of "Gauss periods" was discussed in [18].

Lemma 3.5 With the notations as above, we have

$$\eta_0(a)\cdot\eta_1(a) \equiv \mp(p \mp 1)/4(\mathrm{mod}\ (a^p-1)/(\mathrm{a}-1)), \text{ if } p \equiv \pm 1(\mathrm{mod}\ 4).$$

4 Proof of the Main Result

Proof of Theorem 3.1: According to (4), to prove Theorem 3.1, it suffices to prove $\gcd(S(2), 2^{2p^n}-1) = 1$. We will proveit by contradiction here.

Let d be a prime divisor of $\gcd(S(2), 2^{2p^n}-1)$. Then $d \neq 2$ and d divides $2^{p^n}-1$ or $2^{p^n}+1$.

Since $2^k \equiv 1(\mathrm{mod}\ 3)$ when $k \in H_i^{(2p^j)}$ and $2^k \equiv -1(\mathrm{mod}\ 3)$ if $k \in H_i^{(p^j)}$, it follows by (3) that $S(2) \equiv 1(\mathrm{mod}\ 3)$. Hence $d \neq 3$. As notedbefore

$$2^{p^n} \pm 1 = \frac{2^{p^n}\pm 1}{2^{p^{n-1}}\pm 1}\cdot\frac{2^{p^{n-1}}\pm 1}{2^{p^{n-2}}\pm 1}\cdot\cdots\cdot(2^p \pm 1),$$

hence there exists an integer m such that d divides $(2^{p^{m+1}}\pm 1)/(2^{p^m}\pm 1)$ with $0 \le m \le n-1$.

We consider the following two cases.

(i) Let d be a prime divisor of $\gcd(S(2), \frac{2^{p^{m+1}}-1}{2^{p^m}-1})$ for some $m \in \{0,1,\dots,n-1\}$. First of all, we note that $d \neq p$. In fact, assume that $d = p$, then p divides $\frac{2^{p^{m+1}}-1}{2^{p^m}-1}$ and $2^{p^{m+1}} \equiv 1(\mathrm{mod}\ p)$. It is impossible, since $2^{p-1} \equiv 1(\mathrm{mod}\ p)$ by Fermat's little theorem.

Further, from Lemma 3.2, we get $S(2) \equiv p^{n-m-1}\left(\sum_{f\in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f\in 2D_{i_{n-m}}^{(p)}} 2^{fp^m} + 1\right)(\mathrm{mod}\ d)$ and we see by Lemma 3.4 that

$$S(2) \equiv p^{n-m-1}\left(2\sum_{f\in D_{i_{n-m}}^{(p)}} 2^{fp^m} + 1\right)(\mathrm{mod}\ d).$$

According to the definition of the generalized "Gauss periods" introduced in Subsection 3.3, we obtain

$$S(2) \equiv p^{n-m-1}(2\eta_{i_{n-m}}(2^{p^m}) + 1) \equiv 0 (\mathrm{mod}\ d).$$

Since $\gcd(2, d) = 1$ and, it follows that $\eta_{i_{n-m}}(2^{p^m}) \equiv -1/2 (\mathrm{mod}\ d)$. By (6), we also have $\eta_{i_{n-m+1}}(2^{p^m}) \equiv -1/2 (\mathrm{mod}\ d)$. Then from Lemma 3.3 we get $(\pm p + 1)/4 \equiv 1/4 (\mathrm{mod}\ d)$. Hence, $p \equiv 0 (\mathrm{mod}\ d)$, which leads to a contradiction.

(ii) Let d divide $\gcd(S(2), (2^{p^{m+1}} + 1)/(2^{p^m} + 1))$ for certain integer m with $0 \le m \le n-1$.

Applying Lemma 3.2 again, we get:

$$S(2) \equiv p^{n-m-1}\left(\sum_{f \in D_{i_{n-m}}^{(2p)}} 2^{fp^m} + \sum_{f \in 2D_{i_{n-m}}^{(p)}} 2^{fp^m}\right) + 1 (\mathrm{mod}\ d).$$

By Lemma 3.4, we have that $S(2) \equiv 1 (\mathrm{mod}\ d)$in this case. This is impossible since d divides $S(2)$. The proof of Theorem 3.1 is completed.

Theorem 3.1 shows that the 2-adic complexity of these sequences is good enough to resist the attack of the rational approximation algorithm.

Remark. As to note before, for measuring the security of a binary periodic sequence, the symmetric 2-adic complexity is a finer measure than the 2-adic complexity, [13]. The symmetric 2-adic complexity is defined as

$$\bar{\Phi}(s^\infty) = \min(\Phi(s^\infty), \Phi(\tilde{s}^\infty)),$$

where $\tilde{s}^\infty$is the reciprocal sequence of s^∞.

Let $\tilde{S}(x)$ be the generating polynomial of $\tilde{u}^\infty$. Then $\tilde{S}(x) = \sum_{t=1}^{N} u_{N-t} x^{t-1}$.

Hence

$$2\tilde{S}(2) = \sum_{t=1}^{N} u_{N-t} 2^t = \sum_{t=0}^{N-1} u_{-t} 2^t + u_0 2^N - u_0.$$

So $2\tilde{S}(2) \equiv \sum_{t=0}^{N-1} u_{-t} 2^t (\mathrm{mod}\ 2^N - 1)$. It is clear that $-t \in p^{n-k} D_i^{(p^k)}$ or $-t \in p^{n-k} D_{i+1}^{(p^k)}$ if $t \in p^{n-k} D_i^{(p^k)}$. Hence, the sequence $(u_0, u_{-1}, u_{-2}, \dots, u_{-N+1})$ can be defined by (3) too.

Therefore, by Theorem 3.1, we have $\bar{\Phi}(u^\infty) = \Phi(u^\infty) = 2p^n$.

That is to say, the 2-adic complexity and the symmetric 2-adic complexity of sequences defined by (3) are optimal.

Numerical experiments have been done for $5 \le p \le 1000, n = 1,2$ and $5 \le p \le 100, n = 3$ in accordance with statements of Theorem 3.1 and Remark.

5 Conclusion

We developed the method for analyzing 2-adic complexity proposed in [12] for sequences with period $2p$. We prove that the 2-adic complexity and symmetric 2-adic complexity of considered sequences attains the maximal value. The approach of this article can also be used to study the 2-adic complexity of other generalized cyclotomic sequences. Moreover, with this method we can study the *m*-adic complexity of series of cyclotomic sequences.

References:

[1] C. Ding, T. Helleseth and W. Shan. On the linear complexity of Legendre sequences. *IEEE Trans. Inf. Theory*, Vol.44, 1998, pp. 1276-1278. https://doi.org/10.1109/18.669398.

[2] V. Edemskiy. About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1}. *Des. Codes Cryptogr.*, Vol.61, 2011, pp. 251-260. https://doi.org/10.1007/s10623-010-9474-9.

[3] P. Ke, J. Zhang and S. Zhang. On the linear complexity and the autocorrelation of generalized cyclotomic binary sequences of length $2p^m$. Des. Codes Cryptogr., Vol.67, 2013, pp. 325-339. https://doi.org/10.1007/s10623-012-9610-9.

[4] W. Meidl and A. Winterhof . Some Notes on the Linear Complexity of Sidelnikov-Lempel-Cohn-Eastman Sequences. *Des. Codes Cryptogr.*, Vol.38, 2006, pp. 159-178. https://doi.org/10.1007/s10623-005-6340-2.

[5] T. Yan, S. Li and G. Xiao. On the linear complexity of generalized cyclotomic sequences with the period p^m. *Appl. Math. Lett.*, Vol.21, 2008, pp. 187-193. https://doi.org/10.1016/j.aml.2007.03.011.

[6] Xiong, L. Qu and C. Li. A new method to compute the 2-adic complexity of binary sequences. *IEEE Trans. Inf. Theory,* Vol.60, 2014, pp. 2399-2406. https://doi.org/10.1109/TIT.2014.2304451.

[7] H. Xiong, L. Qu and C. Li. 2-Adic complexity of binary sequences with interleaved structure.

Finite Fields Appl., Vol.33, 2005, pp. 14-28. https://doi.org/10.1016/j.ffa.2014.09.009.

[8] H. Hu. Comments on "A new method to compute the 2-adic complexity of binary sequences". *IEEE Trans. Inf. Theory*, Vol.60, 2014, pp. 5803-5804. https://doi.org/10.1016/j.ffa.2014.09.009.

[9] R. Hofer and A. Winterhof. On the 2-adic complexity of the two-prime generator. *IEEE Trans. Inf. Theory*, Vol.64, 2018, pp. 5957-5960. https://doi.org/10.1109/TIT.2018.2811507.

[10] Z. Xiao, X. Zeng and Z. Sun. 2-Adic complexity of two classes of generalized cyclotomic binary sequences, *Int. J. Found. Comput. Sci.*, Vol.27, 2016, pp. 879–893. https://doi.org/10.1142/S0129054116500350.

[11] Y. Sun, Q. Wang, T. Yan and C. Zhao. A lower bound on the 2-adic complexity of Ding-Helleseth generalized cyclotomic sequence of period p^n. 2017, Preprint arXiv:1704.05544.

[12] L. Zhang, J. Zhang, M. Yang and K. Feng. On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences. *IEEE Trans. Inf. Theory*, Vol.66, 2020, pp. 4613-4620. https://doi.org/10.1109/TIT.2020.2964171.

[13] H. Hu and D. Feng. On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences. *IEEE Trans. Inf. Theory*, Vol.54, 2008, pp. 874-883. https://doi.org/10.1109/TIT.2007.913238.

[14] K. Ireland and M. Rosen (1990). *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics, Springer.

[15] C. Ding and T. Helleseth. New generalized cyclotomy and its applications. *Finite Fields Appl.*, Vol.4, 1998, pp. 140-166. https://doi.org/10.1006/ffta.1998.0207.

[16] A. Klapper and M. Goresky. Cryptanalysis based on 2-adic rational approximation. In: *CRYPTO 1995, LNCS*, Vol.963, 1995, pp. 262-273. https://doi.org/10.1007/3-540-44750-4_21.

[17] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. *J. Cryptol.*, Vol.10, 1997, pp. 111-147. https://doi.org/10.1007/s001459900024.

[18] F. Sun, Q. Yue Q. and X. Li.. On the 2-Adic Complexity of Cyclotomic Binary Sequences with Period p^2 and $2p^2$. In: Mesnager, S., Zhou, Z. (eds) Arithmetic of Finite Fields. *WAIFI 2022. LNCS*, Vol. 13638, 2022, pp 334–347. https://doi.org/10.1007/978-3-031-22944-2_22.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

- Vladimir Edemskiy: Project administration; Supervision; Investigation; Writing —original draft.
- Xiangyong Zeng: Investigation; Writing—review & editing.
- Zhimin Sun: Investigation; Writing—review & editing.
- Yuan Chen: Resources; Software; Validation.

Sources of Funding for Research Presented in a Scientific Article

V. Edemskiy was supported by Russian Science Foundation according to the research project under Grant 24–21–00442. The work of X. Zeng was supported by the National Nature Science Foundation of China (NSFC) under Grant 62072161 and the innovation group project of the natural science foundation of Hubei Province of China (No. 2003AFA021).

The work of Z. Sun was supported by National Nature Science Foundation of China (NSFC) under Grant 12371520.The work of Y. Chen was partly supported by Hubei Provincial Department of Education under Grant D20191003.

Conflict of Interest

The authors have no conflicts of interest to declare.