Notes about symmetric $m$-adic complexity of generalized cyclotomic sequences of order two with period $pq$

V A Edemskiy and S V Garbar
Yaroslav-the-Wise Novgorod State University, Veliky Novgorod, Russian Federation
Vladimir.Edemsky@novsu.ru

Abstract. In this paper, we consider binary generalized cyclotomic sequences with period $pq$, where $p$ and $q$ are two distinct odd primes. These sequences derive from generalized cyclotomic classes of order two modulo $pq$. We investigate the generalized binary cyclotomic sequences as the sequences over the ring of integers modulo $m$ for a positive integer $m$ and study $m$-adic complexity of sequences. We show that they have high symmetric $m$-adic complexity. Our results generalize well-known statements about 2-adic complexity of these sequences.

1 Introduction
Pseudorandom binary sequences are widely used in many areas of communication and cryptography, and they can be efficiently generated by linear feedback shift registers (LFSRs) or by feedback with carry shift registers (FCSRs). The feedback with carry shift register for design binary sequences was introduced by Klapper and Goresky in [1]. The notation of 2-adic complexity was initially used by Klapper who showed this indicator to be important measure of pseudo-randomness. Later, the properties of this register over $\mathbb{Z}_m$ were discussed in [2, 3] (see also references here), where $\mathbb{Z}_m$ is the ring of integers modulo $m$ for a positive integer $m$. The $m$-adic complexity of a sequence is defined as the length of the shortest feedback with carry shift register, which is capable of generating a given sequence, and is viewed as one of the important security criteria of sequence. The sequences with low autocorrelation, high linear complexity and large $m$-adic complexity are widely used in many areas of communication and cryptography.

Using cyclotomic and generalized cyclotomic classes is an important method to design sequences. To search for residue difference sets, Whiteman introduced a generalized cyclotomy with respect to $pq$ [4]. There are lots of papers devoted to study of the autocorrelation and the linear complexity of generalized cyclotomic sequences with period $pq$. In particular, the autocorrelation and the linear complexity of binary generalized cyclotomic sequences of order two with period $pq$, where $p$ and $q$ are odd distinct primes, are studied in [5, 6]. Later, the 2-adic complexity of these sequences was investigated in [7-10]. A binary sequence can be considered to be a sequence over $\mathbb{Z}_m$. For every integer $m$ this gives a new measure of cryptographic security. Any sequence over \{0,1,\ldots, m \- 1\} is not secure for use in a stream cipher if its $m$-adic complexity is small [3]. In comparison with the linear complexity and the 2-adic complexity, the $m$-adic complexity of generalized cyclotomic sequences has not been fully researched. Very recently, the $p$-adic complexity of Ding-Helleseth-Martinsen’s sequence with period $2p$ was determined in [11] by using “Gauss periods” and 4-adic complexity of quaternary sequences also with period $2p$ was derived in [12]. Thus, it is important to
study \( m \)-adic complexity of the known sequences and find sequences with high linear complexity and large \( m \)-adic complexity.

In this paper, we study the symmetric \( m \)-adic complexity of binary sequences with period \( pq \), where \( m > 1 \) is a natural number. These sequences are derived from generalized Whiteman's cyclotomic classes of order two modulo \( pq \) and they have low autocorrelation, large linear complexity and high 2-adic complexity [4-8]. We show that considered sequences have high symmetric \( m \)-adic complexity. It is good enough to resist the attack by the rational approximation algorithm. We also generalize the results about 2-adic complexity from [7, 8] by another method.

2 Preliminary
Throughout this paper, we will denote by \( \mathbb{Z}_m \) the ring of integers modulo \( m \) for a positive integer \( m \) such that \( \gcd(pq,m) = 1 \).

Let \( s^{\infty} = (s_0, s_1, ..., s_{N-1}) \) be a sequence with period \( N \) over \( \mathbb{Z}_m \). Then the \( m \)-adic complexity of the sequence \( s^{\infty} \) can be defined as

\[
\Phi(s^{\infty}) = \left\lfloor \log_m \left( \frac{m^{N-1}}{\gcd(S(x), m^{N-1})} + 1 \right) \right\rfloor,
\]

where \( \lfloor x \rfloor \) is the greatest integer that is less than or equal to \( x \) and \( S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x] \) is the generating polynomial of this sequence.

Hu et al. proposed a new measure for binary sequences \( \tilde{\Phi}(s^{\infty}) = \min(\Phi(s^{\infty}), \Phi(s^{\infty})) \) called symmetric 2-adic complexity, where \( s^{\infty} = (s_{N-1}, s_{N-2}, ..., s_0) \) is the reciprocal sequence of \( s^{\infty} \) [13]. They also showed that symmetric 2-adic complexity is better than 2-adic complexity in measuring the security of a binary periodic sequence. Taking this into account, we will also study the symmetric \( m \)-adic complexity of sequences here.

2.1 The definition of sequences
We need some preliminary notations first. We recall the definitions of generalized cyclotomic classes of order two and sequences derived from these classes [4].

Let \( p \) and \( q \) be two distinct primes with \( \gcd(p-1, q-1) = 2 \) and \( e = (p-1)(q-1)/2 \). There exists a common primitive root \( g \) of both \( p \) and \( q \), and the multiplicative order of \( g \) modulo \( pq \) is \( e \). There also exists an integer \( h \) satisfying the following congruences \( h \equiv g(\operatorname{mod} p), h \equiv 1(\operatorname{mod} q) \) [4]. Then Whiteman's generalized cyclotomic classes of order two modulo \( pq \) is defined as

\[
D_i = \{g^ih^j; j = 0, 1, ..., e-1\}, \quad i = 0, 1.
\]

Also denote \( P = \{p, 2p, ..., (q-1)p\}, Q = \{q, 2q, ..., (p-1)q\}, \) and \( R = \{0\} \). According to [4] we have the partition

\[
\mathbb{Z}_{pq} = D_0 \cup D_1 \cup P \cup Q \cup R.
\]

It is clear that \( |D_i| = (p-1)(q-1)/2, \quad i = 0, 1, 2, 3. \)

Let \( C_0 = D_0 \cup Q \cup R \) and \( C_1 = D_1 \cup P \). The sequence \( s^{\infty} = (s_0, s_1, s_2, ...) \) with period \( pq \) can thus be defined as

\[
s_i = \begin{cases} 0, & \text{if } i \equiv \text{mod } pq \in C_0, \\ 1, & \text{if } i \equiv \text{mod } pq \in C_1. \end{cases}
\]  \tag{1}

As noted in Introduction, the different properties of these sequences were studied in [5-8]. In this paper, we derive the symmetric \( m \)-adic complexity of binary sequences over \( \mathbb{Z}_m \) by a method different from the one used in the above-mentioned papers.

2.2 Main Result
Our main result about the symmetric \( m \)-adic complexity of binary sequences of order two with period \( pq \) is the following statement.
Theorem 1. Let \( s^\infty \) be a binary sequence of period \( pq \) defined in (1) and \( \gcd(pq, m) = 1 \). Then for the symmetric \( m \)-adic complexity of \( s^\infty \) over \( \mathbb{Z}_m \) we have

\[
\Phi(s^\infty) = \left\lfloor \log_m \left( \frac{(m^p-1)r_5}{r_2} + 1 \right) \right\rfloor,
\]

where \( r_1 = \gcd((p+1)(q-1)/2, m^q - 1) \), \( r_2 = \gcd((p+1)(q-1)/2, m^p - 1) \) and \( r_3 = \gcd((p+1)(q-1)/2, m - 1) \).

According to Theorem 1 the above mentioned sequences have high symmetric \( m \)-adic complexity. It is clear that

\[
\Phi(s^\infty) > pq - p - q
\]

for any \( m: \gcd(pq, m) = 1 \). If \( m = 2 \) then these results are consistent with [7, 8].

We will use the generalized "Gauss periods" for the studying of symmetric \( m \)-adic complexity of above-mentioned sequences. We study their properties in the next section. Note that the method of autocorrelation function is used in [7], and the method of the determinant of a circulant matrix and Gauss periods is used in [8, 9].

3. Gauss periods

In this section, we consider the notation of generalized "Gauss periods" similarly to presented in [14] and study their properties. However, here we will employ them with values from \( \mathbb{Z}_{m^{pq-1}} \) and not from \( \mathbb{Z}_{2^{2q-1}} \) as it was done in [11] or in [8].

By definition put \( \eta_j(m) = \sum_{i \in D_j} m^i \), \( j = 0.1, m \in \mathbb{N}, \gcd(m, pq) = 1 \). The properties of \( \eta_j(m) \) defined for classical cyclotomic classes are considered in [8, 11, 14]. In these papers, the authors called these sums generalized Gauss periods.

Since

\[
\sum_{i=0}^{pq-1} m^i = \sum_{i=0}^{q-1} m^{ip} + \sum_{i=0}^{p-1} m^{iq} + \sum_{i \in D_0 \cup D_1} m^i - 1,
\]

it follows that

\[
\eta_0(m) + \eta_1(m) \equiv 1 \pmod{r}
\]

when \( r \) divides \( m^{pq} - 1 \) and \( r \) does not divide \( (m^p - 1)(m^q - 1) \).

Let \( S(x) = \sum_{i=0}^{q-1} s_i x^i \in \mathbb{Z}[x] \) be the generating polynomial of sequence defined by (1). According to (1) and the definition of generalized Gauss periods we get

\[
S(m) = \eta_1(m) + \sum_{i=1}^{q-1} m^{ip}.
\]

The following statement is well-known for Gauss periods, i.e. when instead of \( m \) we use a \( pq \)-th root of unity in an algebraic extension of finite field or a complex root \( pq \)-th root of unity. The proof of it with using of properties of generalized cyclotomic classes and cyclotomic numbers modulo \( pq \) for \( m \) is similar. We will only make short sketches here.

Lemma 1. Let \( r \) divide \( m^{pq} - 1 \) and \( r \) not divide \( (m^p - 1)(m^q - 1) \). Then

(i) \( \eta_0(m) \cdot \eta_1(m) \equiv (1 - pq)/4 \pmod{r} \), if \( (p - 1)(q - 1)/4 \) is odd.

(ii) \( \eta_0(m) \cdot \eta_1(m) \equiv (1 + pq)/4 \pmod{r} \), if \( (p - 1)(q - 1)/4 \) is even.

Proof. Let \( (p - 1)(q - 1)/4 \) be odd. In this case \( -1 \in D_0 \). Denote by \( (j, f)_2 \), \( j, f \in \mathbb{Z} \) the cyclotomic numbers of order two. Then \( \left((D_j + 1) \cap D_f\right) = (j, f)_2 \), \( j, f = 0, 1 \) and using Lemma 2 from [4] we get

\[
\eta_0(m) \cdot \eta_1(m) \equiv (1, 1)_{2} - 1 = (p - 1)(q - 1)/2 \pmod{r}.
\]

The formulae for these cyclotomic numbers are obtained in [4]. According to [4] we have

\[
(1, 1)_{2} = (p - 2)(q - 2)/2.
\]
Hence \( \eta_0(m) \cdot \eta_1(m) \equiv (1 - pq)/4 \pmod{r} \).

We can prove (ii) in the same way. Lemma 1 is obtained.

We finish the section with a remark about the greatest common divisor for two numbers. This lemma will be useful in the further.

**Lemma 2.** Let \( p \) and \( q \) be odd distinct primes. Then \( \gcd(m^p - 1, m^q - 1) = m - 1 \).

**Proof.** It is clear that \( m - 1 \) divides \( m^p - 1, m^q - 1 \).

Let \( d \) divide \( \gcd(m^p - 1, m^q - 1) \). Since \( \gcd(p, q) = 1 \) there exist \( k, l \in \mathbb{Z} \) such that \( kp + lq = 1 \) and \( m^{kp+\ell q} \equiv 1 \pmod{d} \), i.e., \( m \equiv 1 \pmod{d} \). Hence \( \gcd(m^p - 1, m^q - 1) \) divides \( m - 1 \). This completes the proof of this lemma.

4. **Symmetric \( m \)-adic complexity of binary cyclotomic sequences of order two**

First, we consider the generating polynomial of reciprocal sequence.

**Lemma 3.** Let \( s^\infty \) be defined in (1), \( S^\infty = (s_{pq-1}, ..., s_1, s_0) \) and let \( \hat{S}(x) = \sum_{i=1}^{pq} s_{pq-i} x^{i-1} \) be the generating polynomial of \( S^\infty \). Then

(i) \( m\hat{S}(m) \equiv S(m)(\text{mod } m^{pq} - 1) \) if \( (p - 1)(q - 1)/4 \) is odd;

(ii) \( m\hat{S}(m) \equiv \eta_0(m) + \sum_{i=1}^{q-1} m^{pi} \pmod{m^{pq} - 1} \) if \( (p - 1)(q - 1)/4 \) is even.

**Proof.** By definition of \( S^\infty \) we see that \( \hat{S}(m) = \sum_{i=1}^{pq} s_{pq-i} m^{i-1} \). Hence

\[
m\hat{S}(m) = \sum_{i=1}^{pq} s_{pq-i} m^i = \sum_{i=0}^{pq-1} s_{pq-i} m^i + s_0 m^{pq} - s_p.
\]

Thus,

\[
m\hat{S}(m) \equiv \sum_{i=0}^{pq-1} s_{-i} m^i \pmod{(m^{pq} - 1)}. \tag{2}
\]

It is clear that \( s_{-i} = s_i \) for \( i \in P \cup Q \cup R \).

Let \( i \in \mathbb{Z}_{pq} \). According to [4], we have \(-1 \in D_0\) for \( (p - 1)(q - 1)/4 \) is odd and \(-1 \in D_1\) for \( (p - 1)(q - 1)/4 \) is even. So, \( s_{-i} = s_i \) in the first case and \( m\hat{S}(m) \equiv S(m) \pmod{m^{pq} - 1} \). In the second case, \( s_{-i} = j \) iff \( i \in D_0 \) or \( D_1 \), i.e., \( s_{-i} = 1 \) if \( i \in D_0 \). Thus this statement follows from (2) and the definition of \( \eta_0(m) \).

4.1 **Proof of Theorem 1**

By definition (1) we see that

\[
S(m) = \eta_1(m) + \sum_{i=1}^{q-1} m^{pi} \pmod{(m^{pq} - 1)}. \tag{3}
\]

Further, we consider three cases.

1. Let \( d > 1 \) divide \( \gcd(S(m), m^{pq} - 1) \) and \( d \) not divide \( (m^p - 1)(m^q - 1) \). Since \( p \) and \( q \) are primes, it follows that the order of \( m \) modulo \( d \) equals \( pq \) and \( pq \) divides \( d - 1 \). Further, we get \( S(m) \equiv \eta_1(m) - 1 \pmod{d} \) by (3) and as noted above \( \eta_0(m) + \eta_1(m) \equiv 1 \pmod{d} \), hence we see that \( \eta_0(m) \equiv 0 \pmod{d} \). Then, according to Lemma 1 we see that \( d \) divides \( pq + 1 \) or \( pq - 1 \). It is impossible. We get a contradiction.

This statement is also true for \( \gcd(S(m), m^{pq} - 1) \) by Lemma 3.

2. Second, we study \( \gcd(S(m), m^q - 1) \). According to [15], Lemma 2 we have \( D_j \) mod \( q = \{1, 2, ..., q - 1\} \) and when \( s \) ranges over \{0.1, ..., e - 1\}, \( g^s h^l \text{mod} q \) takes on each element of \{1, 2, ..., q - 1\} \((p - 1)/2\) times, hence

\[
\eta_j(m) \equiv \frac{p-1}{2} (m + \cdots + m^{q-1}) \pmod{m^q - 1}.
\]

Hence, by (3) we have

\[
S(m) \equiv -(p + 1)/2 (\text{mod } (m^q - 1)/(m - 1))
\]

and
\[ S(m) \equiv (q - 1)(p + 1)/2(\text{mod } (m - 1)). \]

Thus, \( \gcd(S(m), m^q - 1) = \gcd(m^q - 1, (q - 1)(p + 1)/2) \), i.e., \( \gcd(S(m), m^q - 1) = r_1 \).

This statement is also true for \( \gcd(S(m), m^q - 1) \) by Lemma 3.

3. Now, we consider \( \gcd(S(m), m^p - 1) \). We can obtain in the same way that
\[ S(m) \equiv (q - 1)/2(\text{mod } (m^p - 1)/ (m - 1)) \]

and
\[ S(m) \equiv (q - 1)(p + 1)/2(\text{mod } (m - 1)). \]

Thus, \( \gcd(S(m), m^p - 1) = \gcd(m^p - 1, (q - 1)(p + 1)/2) \), i.e., \( \gcd(S(m), m^p - 1) = r_2 \). This statement is also true for \( \gcd(S(m), m^p - 1) \).

Further, if \( d \) divides \( r_1 \) and \( r_2 \) then according to Lemma 2 we see that \( d \) divides \( \gcd(S(m), m - 1) = \gcd(m - 1, (p + 1)(q - 1)/2) \). Thus, \( \gcd(S(m), m^{pq} - 1) = r_1r_2/r_3 \) and \( \gcd(S(m), m^{pq} - 1) = r_1r_2/r_3 \). This completes the proof of Theorem 1.

**Remark** The fraction \( \frac{r_1r_2}{r_3} \) is not equal to
\[ \frac{\gcd((p+1)/2,(m^{q-1})/(m-1))\gcd((q-1)/2,(m^p-1)/(m-1))}{\gcd((p+1)/(q-1)/2,m-1)}. \]

Sometimes, the divisor of \( m - 1 \) can divide \( (m^q - 1)/(m - 1) \). For example, if \( m = 4, q = 3 \) then \( 3 \) divides \( m - 1 \) and \( (m^q - 1)/(m - 1) \).

With the help of computer program, we verified the results of Theorem 1 for \( m = 3, \ldots, 16 \) and all primes \( p \) and \( q \) such that \( pq < 65933; p, q < 10000 \).

### 5. Conclusion

Sequences generated by FCSRs share many important properties of LFSR sequences. We estimated symmetric \( m \)-adic complexity of binary generalized cyclotomic sequences of order two with period \( pq \) for any odd distinct primes \( p, q \). Due to the effectiveness of rational approximation algorithm, \( m \)-adic complexity becomes a new security index of binary sequences. Our results showed that \( m \)-adic complexity of these sequences is good enough to resist the attack by the rational approximation algorithm.

### References

[1] Klapper A and Goresky M 1997 Feedback shift registers, 2-adic span, and combiners with memory *Journal of Cryptology* 10 111–47

[2] Klapper A 2005 A Survey of Feedback with Carry Shift Registers. In: *Sequences and Their Applications - SETA 2004* in: *LNCS* ed Helleseth T and Sarwate D et al 3486 (Berlin: Springer-Verlag) pp 56–71

[3] Xu J and Klapper A 1999 Feedback with Carry Shift Registers over \( \mathbb{Z}/(N) \). In: *Sequences and Their Applications: Discrete Mathematics and Theoretical Computer Science* ed Ding C and Helleseth T et al (London: Springer) pp 379–392

[4] Whiteman A L 1962 A family of difference sets *Illinois J. Math.* 6 107–21

[5] Ding C 1998 Autocorrelation values of generalized cyclotomic sequences of order two *IEEE Trans. Inf Theory* 44 (4) 1699–1702.

[6] Ding C 1997 Linear complexity of generalized cyclotomic binary sequences of order 2 *Finite Fields Appl* 3 159–74

[7] Hofer R and Winterhof A 2018 On the 2-adic complexity of the two-prime generator *IEEE Trans. Inf Theory* 64 (8) 5957–60

[8] Yang M and Feng K 2020 Determination of 2-Adic Complexity of Generalized Binary Sequences of Order 2 Preprint arXiv:2007.15327

[9] Sun Y, Wang Q and Yan T 2019 A lower bound on the 2-adic complexity of the modified...
Jacobi sequences *Cryptogr Commun* 11 337–49

[10] Zhao C, Sun Y and Yan T 2021 Further results on the 2-adic complexity of a class of balanced generalized cyclotomic sequences *Preprint* arXiv:2102.12098v1 [cs.IT] 24 Feb 2021

[11] Jing X, Xu Z, Yang M and Feng K 2021 On the $p$-Adic Complexity of the Ding-Helleseth-Martinsen Binary Sequences *Chinese Journal of Electronics* 30 64–71

[12] Qiang S, Li Y, Yang M and Feng K 2020 The 4-Adic Complexity of A Class of Quaternary Cyclotomic Sequences with Period $2p$ *Preprint* arXiv:2011.11875v1 [cs.IT] 24 Nov 2020

[13] Hu H and Feng D 2008 On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences *IEEE Trans. Inf. Theory* 54 (2) 874–83

[14] Zhang L, Zhang J, Yang M and Feng K 2020 On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences *IEEE Trans Inf Theory* 66 (7) 4613–20

[15] Chen Z. Linear complexity and trace representation of quaternary sequences over $\mathbb{Z}_4$ based on generalized cyclotomic classes modulo $pq$ *Cryptogr Commun* 9 445–58