3-adic complexity of ternary generalized cyclotomic sequences with period $p^n$

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

Abstract. In this paper, we study the ternary generalized cyclotomic sequences with a period equal to a power of an odd prime. Ding-Helleseth's generalized cyclotomic classes of order three are used for the definition of these sequences. We derive the symmetric 3-adic complexity of above mentioned sequences and obtain the estimate of symmetric 3-adic complexity of sequences. It is shown that 3-adic complexity of these sequences is large enough to resist the attack of the rational approximation algorithm for feedback with carry shift registers.

1. Introduction

A feedback with carry shift registers for design binary sequences was proposed in [1]. Later, the properties of this register over the ring of integers modulo $m$ were discussed in [2, 3] (see also references here). $m$-adic complexity of a sequence is defined as the length of the shortest feedback with carry shift registers which is able to construct this sequence. According to [3], the $m$-adic complexity is an important characteristic of a sequence. Thus, it is interesting to study the $m$-adic complexity of known sequences and to find families of sequences with high $m$-adic complexity and high linear complexity.

During the last decades, a lot of papers devoted to use of cyclotomic classes and generalized cyclotomic classes for design sequences were presented. In particular, the properties of Ding-Helleseth's generalized cyclotomic sequences such as the linear complexity and other are investigated in [4, 5, 6] (see also references here). Further, the 2-adic complexity of Ding-Helleseth binary sequences of order two with period $p^n$ were studied in [7, 8] (see also references here). Comparing with the 2-adic complexity, the $m$-adic complexity of generalized cyclotomic sequences has not been fully researched. The 4-adic complexity of quaternary sequences with period $2p$ was derived in [9] and the $p$-adic complexity of Ding-Helleseth-Martinsen's sequence also with period $2p$ was determined in [10]. Thus, it is important to continue to study $m$-adic complexity of Ding-Helleseth generalized cyclotomic sequences. In this paper we derive the 3-adic complexity of ternary sequences defined on generalized cyclotomic classes of order 3. According to [11] these sequences have large linear complexity. We show that these sequences have high symmetric $m$-adic complexity and it is large enough to resist the attack of the rational approximation algorithm for feedback with carry shift registers.

The rest of the paper is organized as follows. Some preliminaries and the definition of sequences are introduced in Section 2. In Section 3 we discuss some subsidiary statements and in Section 4 we prove our main result.
2. The definition of sequences

In this section, we recall the definitions of generalized cyclotomic classes of Ding-Helleseth of order three and ternary sequences for this case [4].

Let \( p \) be a prime, \( p \equiv 1(\mod 3) \) and let \( n \geq 1 \) be an integer. Throughout this paper, we will denote by \( \mathbb{Z}_p^n \) the ring of integers modulo \( p^n \), and by \( \mathbb{Z}_p^* \) the multiplicative group of \( \mathbb{Z}_p^n \). It is well known that there exists \( g \) a primitive root modulo \( p^n \) and an order \( g \) modulo \( p^n \) equals the value of the Euler’s totient function \( \varphi(p^n) = p^n - 1 \).

Define

\[
H_j^{(p^k)} = \{ g^{j+3t} \pmod{p^k} \mid 0 \leq t < p^{k-1}(p-1)/3 \}, \quad j = 0, 1, 2; \quad k = 1, 2, \ldots, n .
\]

The cosets \( H_j^{(p^k)} \), \( j = 0, 1, 2 \) are called Ding-Helleseth generalized cyclotomic classes of order three with respect to \( p^k \). By definition we see that \( |H_j^{(p^k)}| = p^{k-1}(p-1)/3 \). According to [4], we have the following partitions

\[
\mathbb{Z}_p^* = \bigcup_{j=0}^{2} H_j^{(p^k)} \text{ and } \mathbb{Z}_p^n = \bigcup_{k=1}^{n} \bigcup_{j=0}^{2} p^{n-k}H_j^{(p^k)} \cup \{0\}.
\]

Let \( C_0 = \bigcup_{k=1}^{n} p^{n-k}H_0^{(p^k)} \cup \{0\} \) and \( C_j = \bigcup_{k=1}^{n} p^{n-k}H_j^{(p^k)} \), \( j = 1, 2 \). It is obvious that

\[
\mathbb{Z}_p^n = \bigcup_{j=0}^{2} C_j.
\]

Then ternary generalized cyclotomic sequence \( s^\infty = (s_0, s_1, s_2, \ldots) \) with period \( p^n \) can be defined as

\[
s_i = \begin{cases} 
0, & \text{if } i \pmod{p^n} \in C_0, \\
1, & \text{if } i \pmod{p^n} \in C_1, \\
2, & \text{if } i \pmod{p^n} \in C_2.
\end{cases}
\] (1)

The linear complexity of these sequences was studied in [11]. Here we will derive the symmetric 3-adic complexity of sequences defined by (1).

In conclusion of Section 2, we recall one the method for computing 2-adic complexity. Let \( s^\infty = (s_0, s_1, \ldots, s_N-1) \) be a sequence with period \( N \). Denote by \( S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x] \) the generating polynomial of this sequence. Then, according to [3] the \( m \)-adic complexity of \( s^\infty \) can be defined as

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

where \( [x] \) is the greatest integer that is less than or equal to \( x \). Thus, it is enough to study \( \gcd(S(m), m^{N-1}) \).

According to [12], it is also interesting to study symmetric complexity sequence \( s^\infty \), i.e., \( \Phi(s^\infty) = \min(\Phi(s^\infty), \Phi(\bar{s}^\infty)) \), where \( \bar{s}^\infty = (s_{p-1}, s_{p-2}, \ldots, s_0) \) is the reciprocal sequence of \( s^\infty \). By [12] symmetric 2-adic complexity is better than 2-adic complexity in measuring the security of a binary periodic sequence.

Let \( \bar{S}(X) = \sum_{i=1}^{p} s_{p-i} X^{i-1} \) be the generating polynomial of reciprocal sequence. In the considered case, we see that

\[
3\bar{S}(3) = \sum_{i=1}^{p} s_{p-i} 3^i = \sum_{i=0}^{p-1} s_{p-i} 3^i + s_0 3^p - s_p .
\]

Hence,

\[
3\bar{S}(3) \equiv \sum_{i=0}^{p-1} s_{p-i} 3^i(\mod (3^p - 1)).
\]
Since \(-1\) belongs to \(C_0\), it follows that \(s_{p-i} = s_i\) for \(i = 0, 1, \ldots, p - 1\). Then \(3S(3) \equiv S(3)(\text{mod } (3^p - 1))\) and \(\Phi(s^\infty) = \Phi(s^\infty)\) for sequence \(s^\infty = (s_0, s_1, s_2, \ldots)\) with period \(p^n\) defined by (1). Thus, it is enough to consider only \(3\)-adic complexity of sequences. The obtained results also right for the symmetric \(3\)-adic complexity.

In the following section we will prove a few subsidiary statements about the properties of the generating polynomial of the sequence \(s^\infty\).

3. Properties of generating polynomial of sequence

Let \(Z_f(X) = \sum_{i \in H_f} X^i, \quad j = 0, 1, 2\) and \(c = 3^p k\) for some integer \(k: 0 \leq k < n\). Further the subscripts \(j\) in \(Z_f(X)\) are all taken modulo 3. For cyclotomic classes of order four the properties of \(Z_f(2)\) were studied in [13].

It is clear that

\[
Z_0(c) + Z_1(c) + Z_3(c) \equiv -1(\text{mod } (c^p - 1)/(c - 1)).
\]  

(2)

Denote by \((k, f)_3\), \(k, f \in \mathbb{Z}\) the cyclotomic numbers of order three. We have the following statement.

Lemma 1. Let \(k, l = 0, 1, 2\). Then

\[
Z_i(c) \cdot Z_{i+k}(c) \equiv \sum_{f=0}^3 (k, f)_3 Z_{f+i}(c) + \delta \mod (c^p - 1)/(c - 1),
\]

where \(\delta = \begin{cases} (p - 1)/3, & \text{if } k = 0, \\ 0, & \text{otherwise}. \end{cases}\)

We can prove Lemma 1 in the same way as for classical Gauss periods.

Now we define the subsidiary polynomials. Let \(U_0(X) = Z_1(X) + 2Z_3(X), \quad U_1(X) = Z_2(X) + 2Z_0(X)\) and \(U_2(X) = Z_0(X) + 2Z_1(X)\).

Since \(p \equiv 1(\text{mod } 3)\), it follows that \(4p\) we can write as sum of squares of two integers, i.e., \(4p = L^2 + 27M^2, \quad L \equiv 1(\text{mod } 3)\). According to [14] we have the following formulae for cyclotomic numbers of order three:

\[
(0, 0)_3 = (p - 8 + L)/9, \quad (0, 1)_3 = (2, 2)_3 = (2p - 4 - L - 9M)/18,
\]

\[
(0, 2)_3 = (1, 1)_3 = (2p - 4 - L + 9M)/18, \quad (1, 2)_3 = (p + 1 + L)/9.
\]

Here a sign of \(M\) depends on the choice of a primitive root.

Lemma 2. Let \(4p = L^2 + 27M^2, \quad L \equiv 1(\text{mod } 3)\). Then \(U_0(c), U_1(c)\) and \(U_2(c)\) are satisfying the congruence

\[
X^3 - 3X^2 + (3 - p)X - pM - p + 1 \equiv 0(\text{mod } (c^p - 1)/(c - 1)).
\]

Proof. For the proof of this lemma we consider the product

\[
(X - U_0(c))(X - U_1(c))(X - U_2(c)) = X^3 + uX^2 + vX + w.
\]

Obviously, \(u = U_0(c) + U_1(c) + U_2(c)\). Then by (2) and the definition of \(U_0(c), U_1(c), U_2(c)\) we have \(u \equiv -3(\text{mod } (c^p - 1)/(c - 1))\).

Further,

\[
v = U_0(c)U_1(c) + U_0(c)U_2(c) + U_1(c)U_2(c).
\]

Hence, we get

\[
v = 7(Z_0(c)Z_1(c) + Z_0(c)Z_2(c) + Z_1(c)Z_2(c)) + 2((Z_0(c))^2 + (Z_1(c))^2 + (Z_2(c))^2)
\]

or

\[
v = 3(Z_0(c)Z_1(c) + Z_0(c)Z_2(c) + Z_1(c)Z_2(c)) + 2.
\]
Using Lemma 1 and the formulae for cyclotomic numbers of order three we obtain
\[ Z_0(c)Z_1(c) + Z_0(c)Z_2(c) + Z_1(c)Z_2(c) \equiv -(p - 1)/3 (mod (c^p - 1)/(c - 1)). \]
Hence, \( v \equiv -p + 3 (mod (c^p - 1)/(c - 1)). \)
Similarly, we see that
\[ w = -U_0(c)U_1(c)U_2(c) = -(Z_1(c) + 2Z_2(c)(Z_2(c) + 2Z_0(c))Z_0(c) + 2Z_1(c)). \]
In the same way as for calculating \( v \) we can show that \( w \equiv -Mp - p + 1 (mod (c^p - 1)/(c - 1)). \)
This completes the proof of Lemma 2.

The properties of Ding-Helleseth generalized cyclotomic classes are well-known (see for example [5]). Using them we obtain the following conclusion.

**Lemma 4.** Let \( s^\infty \) be defined by (1) and let \( S(x) = \sum_{i=0}^{n-1} s_i x^i \) be the generating polynomial of \( s^\infty \). Then
\[ S(3) \left( (mod \frac{3^{p^{n+1}}-1}{3^n-1}) \right) = p^{n-m-1}U_0(3^{p^m}) + p^{n-m-1} - 1 \]
for \( m = 0, 1, \ldots, n - 1. \)

### 4. Symmetric 3-adic complexity of sequences

In this section we present the main results. To obtain the results of 3-adic complexity in this case it is necessary to study \( \frac{3^{n-1}}{gcd(S(3),3^n-1)} \). To this end, we will investigate \( gcd(S(3),3^n-1) \).

**Lemma 4.** Let \( n = 1 \) and let \( s^\infty \) be a sequence defined in (1). Then we have the following estimate for symmetric 2-adic complexity of \( s^\infty \)
\[ \Phi(s^\infty) > p - 1.5 \log_3 p - 1. \]

**Proof.** Since \( S(1) = p - 1 \), it follows that 2 divides \( gcd(S(3),3^p - 1) \) and it is clear that 4 does not divide \( 3^p - 1 \) in the considered case.

Let \( d > 2 \) be a divisor of \( gcd(S(3),3^p - 1) \). By the definition of the sequence and the subsidiary polynomial we see that \( S(3) = U_0(3) \). Then by Lemma 2 \( d \) divides \( pM + p - 1 \). It is clear that \( |pM + p - 1| < p\sqrt{p} \). Thus, \( gcd(S(3),3^p - 1) < 2p\sqrt{p} \). This completes this lemma.

According to Lemma 4 cyclotomic ternary sequences of order three have high symmetric 3-adic complexity.

**Remark.** We showed that \( Mp + p - 1 \equiv 0 (mod d) \). Let \( d \) be a prime. Since \( d \) is a prime, it follows that \( d = 1 + 2fp \), where \( f \) is a positive integer. Then \( 2fp \equiv -1 (mod d) \) and \( -M - 1 - 2f \equiv 0 (mod d) \), i.e., \( -M - 1 - 2f = l(1 + 2fp) \) for an integer \( l \). By the condition \( 4p = L^2 + 27M^2 \), hence \( 2f = -M - 1 \) and \( d^2 \) does not divide \( gcd(S(3),3^p - 1) \). Thus \( gcd(S(3),3^p - 1) \neq 2 \) iff \( d = 1 + (M - 1)p \) is a prime and \( d \) divides \( 3^p - 1 \). Otherwise \( gcd(S(3),3^p - 1) = 2 \).

Let \( p = 7 \). Then \( M = 1 \) and \( d = 13 \). But \( S(3)(mod 13) = 1 \) and \( \Phi(s^\infty) = 6 \).
Note that it is easy to see that for \( p = 7 \) we have \( gcd(S(3), 3^7 - 1) = gcd(612, 2186) = 2 \).

Our main result is the following statement.

**Theorem 5.** Let \( s^\infty \) be a ternary generalized cyclotomic sequence defined by (1) for \( n > 1 \) and let \( n_0 \) be the least integer that is equal or more than \( 3(n - 1)/4. \) Then
\[ \Phi(s^\infty) \geq p^n - n_0. \]

**Proof.** First, we will show that \( gcd(S(3),3^{n_0} - 1) \) divides \( gcd(S(3),3^{n_0} - 1) \). Suppose it isn’t. Then there exists \( d \) which is an odd prime divisor of \( gcd(S(3),3^{n_0} - 1)/(3^{n_0} - 1) \). In this case, there also exists \( m \geq n_0 \) such that \( d \) divides \( 3^{n_0} - 1 \). Since an order of 3 modulo \( d \) equals \( p^{m+1} \) we get \( d \equiv 1 (mod p^{m+1}) \). Further, by Lemma 3
Hence and . Here are the inverse elements to modulo .

We consider two cases for .

1). Suppose ; then . In this case, by Lemma 2 divides and for . It is impossible.

2) Let . Then, according to Lemma 2 here exists such that .

Since and , it follows that . Hence .

If then the left part of relation (3) is a positive integer and according to (3) since .

Hence . It is easy to check that . Since , it follows by (3) that .

So, divides . Hence

Then we see that

The statement of this theorem for can be easily obtained by the simple calculation which we omit here. Theorem 5 is proved.

It is clear that the 3-adic complexity of these sequences is more than one half of its period.

Theorem 5 shows that Ding-Helleseth generalized cyclotomic ternary sequences of order three with period have high symmetric 3-adic complexity. It is clear that the 3-adic complexity of these sequences is more than one half of its period.

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 T Helleseth and D Sarwate et al 3486 (Berlin: Springer-Verlag) pp 56–71

[3] Xu J and Klapper A 1999 feedback with carry shift registers over . In: Sequences and their Applications. Discrete Mathematics and Theoretical Computer Science ed C Ding and
T Helleseth et al (London: Springer) pp 379–92

[4] Ding C and Helleseth T 1998 New generalized cyclotomy and its applications Finite Fields Appl. 4 140–66

[5] Edemskiy V 2011 About computation of the linear complexity of generalized cyclotomic sequences with period $p^{n+1}$ Des Codes Cryptography 61 251–60

[6] Du X and Chen Z 2013 A generalization of the Hall's sextic residue sequences Information Sciences 222 784–94

[7] Xiao Z, Zeng X and Sun Z 2016 2-Adic complexity of two classes of generalized cyclotomic binary sequences International Journal of Foundations of Comput. Sci. 27 (7) 879–93

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

[9] 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

[10] 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

[11] Edemskiy V and Sokolovskiy N 2016 Linear complexity cubic sequences over finite fields. Proceeding of the 3rd International Conference on Mathematics and Computers in Sciences and Industry (MCSI 2016), Chania, Crete, Greece pp 57–60

[12] 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

[13] Zhang L, Zhang J, Yang M and Feng K 2020 On the2-adic complexity of the Ding-Helleseth-Martinsen binary sequences IEEE Trans Inf Theory 66 (7) 4613–20

[14] Hall M 1975 Combinatorial Theory (Wiley, New York)