On the linear complexity of a new class of binary cyclotomic sequences having order $2^l t$

Debashis Ghosh[1], Pranab Goswami[2], Tauseef Khan[3]

[1]School of Applied Science and Humanities, Haldia Institute of Technology, Haldia,
West Bengal, India
E-mail: ghoshdebashis10@gmail.com

[2] Department of Information Technology, Haldia Institute of Technology, Haldia,
West Bengal, India
Email: pranab.goswami07@gmail.com

[3] Department of Information Technology, Haldia Institute of Technology, Haldia,
West Bengal, India
E-mail: tauseef.hit2013@gmail.com

Abstract

Several reasonably cyclotomic sequences are constructed by cyclotomic classes with good pseudo-randomness property. During this paper, we derive the linear complexity of a new binary cyclotomic sequences of order $2^l t$ over finite field having period pq. Our result shows that these sequences have high linear complexity, which can resist linear attack.

Keywords. Generalised cyclotomy,linear complexity, pseudo random sequence, stream cipher.

Subject class [2010]Primary: 11T71, 94A60.

I. Introduction

Now-a-days utilisation of networks and its security aspects are growing at a rapid rate. Users often reveal critical information like account numbers, bank passwords, personal and financial details, important transaction details etc., over the internet. Apart from its legitimate use, vulnerabilities like password theft, virus attacks, spoofing, message confidentiality threats, message integrity threats etc. are found, causing potential loss of the users' private information. Hence it is important to make a secure system, providing an ideal balance of confidentiality, integrity and availability of user's private data. These security parameters are provided by a mechanism of key generation (public and private keys), random password generation, one-time password generation, strong authentication in wireless communication, radar application and so on [1, 2]. Implementation of these mechanisms is done through generation of unpredictable sets of random numbers having high uncertainty, called pseudo-random numbers. Hence, pseudo-random numbers are at the core in providing security to network applications. On the other hand, if there is a flaw or the Pseudo-Random Number Generator produces predictable sets of random numbers, then the entire application would be vulnerable to attacks. Therefore, development of a generic framework for generating strong sets of pseudo-random numbers, employing a co-simulation of hardware and software is proposed. The proposal aims to build a framework and a unified model for enhanced security specifically for LFSR [3, 4].

The cyclotomic sequence of order pq was introduced by Whiteman [5]. This has been shown later, that the randomness properties of such sequence behave same as Legendre sequence in many formulation [6]. A series of papers have been described those sequences over finite field and computed its linear complexity [7, 8, 9, 10]. from the last two decades.

The sequences of period pq, for two odd primes p and q on generalised cyclotomic sequences become the eminent subject of research in cryptographic point of view[11, 12, 13]. Works has been executed on the linear complexity of generalised cyclotomic sequences of order 2 [11] and 4 [14] and 2^k[15] over Z_{pq}. In this correspondence, we explore the linear complexity over GF (2) of generalised cyclotomic sequence of order $2^l t$ of length pq.

Rest of the paper is organized as follows. In sec I, we recall the relevant definitions and results of generalised cyclotomic sequences as Technical Preliminaries. The linear complexity of the defined sequences is being executed in Sec III. Our results show that such sequences have high linear complexity and may have some application in security system. In the final section a conclusion on further work prosperity is given in section IV.

II. Technical Preliminaries

Let p and q be two odd primes with $\gcd(p-1, q-1) = d$. Define $N = pq$ and $e = \frac{(p-1)(q-1)}{d}$. From Chinese Remainder Theorem, there is a common primitive root g for both of p and q, with order e modulo N. Then for any integer solution x has following assertion,

$x \equiv g \pmod p$ and $x \equiv 1 \pmod q$.

Being primitive root of both p and q is g, again by Chinese Remainder Theorem,

$$\mathrm{ord}_N(g) = \mathrm{lcm}\left(\mathrm{ord}_p(g), \mathrm{ord}_q(g)\right) = \mathrm{lcm}(p-1, q-1) = e, \quad (2.1)$$

where $\mathrm{ord}_N(g)$ denotes the multiplicative order of g modulo N.

For any subset G of Z_N and let h be an element of Z_N. Define,

$$G + h = \{g + h: g \in G\} \text{and } h.\, G = \{hg: g \in G\}.$$

Whiteman [5], proved that

$$Z_N^* = \{g^s x^i : s = 0, 1, \ldots, e-1;\ i = 0, 1, \ldots, d-1\}, \quad (2.2)$$

where Z_N^* denotes the set of all invertible elements of the residue class ringZ_N. The generalised cyclotomic classes $D_i$of order dwith respect to p and q are defined by,

$$D_i = \{g^s x^i : s = 0, 1, \ldots, e-1;\ i = 0, 1, \ldots, d-1\}. \quad (2.3)$$

It has been proved in [6], from (2.2) and (2.3) that

$$Z_N^* = Z_{pq}^* = \cup_{i=0}^{d-1} D_i,$$
$$D_i \cap D_j = \emptyset, \text{ for } i \neq j.$$

Let P= {p, 2p, ..., (q – 1)p} and Q = {q, 2q, ..., (p – 1)q} and R = {0}. We consider here the case for $d = \gcd(p-1, q-1) = 2^l t$, for some positive integer l and t.

Let $\lambda = \max\{2^l, t\}$ and $\mu = \min\{2^l, t\}$.

Then we can define, $C_0 = \cup_{i=0}^{\lambda-1} D_i$and $C_k = \cup_{i=k\lambda}^{(k+1)\lambda-1} D_i$, where $k = 1, 2, 3, \ldots (\mu - 1)$ (2.4)

$B_0 = R \cup Q \cup C_0$ and $B_k = P \cup C_k, k = 1, 2, 3, \ldots.(\mu - 1)$. Thus the B_i's have the properties as $Z_{pq} = B_0 \cup B_1 \cup \dots \cup B_{(\mu-1)}$with $B_i \cap B_j = \emptyset$, for $i \neq j$.

The sequences$^{\infty} = (s_0, s_1, s_2, \dots)$ satisfies$s_j = c_1 s_{j-1} + \dots + c_L s_{j-L} = 0$, where $j \geq L$, L is a positive integer $c_1, c_2, \dots, c_L \in$ GF(M), where GF(M) denote the Galois Field of order M. The smallest value of L is called the **linear complexity** of the sequence s^{∞}, denoted by $L(s^{\infty})$ which gives the length of the shortest LFSR that can generate such sequence. By the Berlekamp–Massey algorithm [4], if $L(s^{\infty}) > \frac{N}{2}$, Then s^{∞} is considered to be a good sequence with respect to its linear complexity. Characteristic polynomials of the sequences $s^{\infty} = (s_0, s_1, s_2, \dots)$ and $s_N = (s_0, s_1, s_2, \dots, s_{N-1})$ are defined as $S(x) = s_0 + s_1 x + s_2 x^2 + \cdots$and $S^N(x) = s_0 + s_1 x + s_2 x^2 + \dots + s_{N-1} x^{N-1}$, respectively. If N is a period of s^{∞}, then $m(x) = (1 - S^N)/\gcd(S^N(x), 1 - x^N))$ is called the minimal polynomial of s^{∞}[16]. Therefore,

$L(s^{\infty}) = N - deg\,(gcd\,(x^N - 1, S^N(x)))$.

For further details, we refer the readers to [1].

The generalised cyclotomic binary sequences s^{∞} of order $2^l t$ with respect to prime p and q is defined as

$$s(u) = \begin{cases} 0 & if\ (u\ mod\ N) \in B_0, \\ 1, & if\ (u\ mod\ N) \in B_k,\ k \neq 0, \end{cases} \text{for all } u \geq 0.$$

Many generalised cyclotomic sequences are investigated, and in most of the cases result shows that generalised cyclotomic sequences possess attractive cryptographic properties, one of which is large linear complexity with low autocorrelation. Now we calculate the linear complexity of the sequences of order $2^l t$.

III. Linear complexity of generalised cyclotomic sequences of order $2^l t$.

Following lemmas are required to establish our result. Some of its proofs are given.

Lemma3.1 [11]

(1) $ord_N(g)$= e, where $ord_N(g)$ denotes the order of g modulo N.

(2) $D_0$is subgroup of Z_N^*.

Proof. Every notation has their usual meaning for (1).For (2), the result hold good from the construction D_0 and the equation (2.3) and (2.4).

Lemma3.2 [11]

For each $w \in D_0,\ wD_j = D_{i+j}\ (\,mod\ 2^l t)$, where $i, j = 0, 1, 2, \dots, (2^l t - 1)$.

Proof. Define $J_i = \bigcup_{(2^{l-1}t-1)-i}^{2^l t+i} D_i$.

We have, from (2.4), $J_0 = C_1$, $J_2 = C_0$ and also, $wJ_i = J_{i+j}$ for each $w \in D_j$.

Let α be a primitive N$^{\text{th}}$root of unity in the extension of GF(ζ), where $\zeta = 2^{\theta}$for some positive number θ, which is the splitting field of$x^N - 1$. Then from the definition of minimal polynomial and linear complexity of the sequence$S_i(x)$, for all i, defined by $S_i(x) = \sum_{j\, \in J_i\, \cup P} x^j$, is the same as to find the zeros in $S^N(x)$in the set $\{\alpha^w, w = 0, 1, 2, \dots, N - 1\}$ and their multiplicity.

Lemma3.3 [11]

If α be the primitive N$^{\text{th}}$root of unity, then

$$\sum_{w \in P} \alpha^w = \sum_{w \in Q} \alpha^w = 1.$$

$$S_i(\alpha) + S_{2^{(l-1)}t+i}(\alpha) = 1$$

$$\sum_{i \in D_j} S_i\left(\alpha^{wi}\right) = \begin{cases} \frac{p-1}{2^l\ t} & if\ w\ \in P \\ \frac{q-1}{2^l\ t} & if\ w\ \in Q \end{cases} \qquad (3.1)$$

Where, $j = 0, 1, 2, \ldots, 2^l t - 1$.

In particular, $\sum_{i \in C_j} \alpha^{wi} = 0$, for each $w \in P \cup Q$.

Lemma. 3.4

Let $S_0(x)$denote the generating polynomial of the binary sequence s^∞, then

$$S_0(\alpha^w) \begin{cases} S_i(\alpha), & w \in D_i \\ 0, & w \in Q \\ 1, & w \in P \end{cases}$$

(3.2)

Lemma 3.5 [16]

The residue equation $ax \equiv b\ (mod\ m), ax \neq 0\ (mod\ m)$, having solution if and only if $gcd(a, m)\ |b$.

In particular, if $gcd(a, m) = 1$, it has a unique solution.

From the above two results, we have the following useful lemma.

Lemma 3.6

The residue equation $ux \equiv d/2$ (mod d) have a solution, for all u, $0 \le u \le (d-1)$ be such that

$gcd(u, d-1) = 1$, for d = $2^l t$.

Proof:

Proof follows from the Lemma (3.5).

Lemma 3.7 [1]

$2 \in D_0$ if and only if $S_0(\alpha) \in \{0, 1\}$

From the definition of $\alpha, P, Q\ and\ R$, we have

$$x^p - 1 = \prod_{i \in Q\ \cup R} (x - \alpha^i)(x^q - 1)$$

$$= \prod_{i \in P\ \cup R}(x - \alpha^i).$$

Let f(x) = $\prod_{i \in C_0 \cup C_k}(x - \alpha^i)$,

Then, $x^{pq} - 1 = \prod_{i=0}^{pq-1}(x - \alpha^i) = \frac{(x^p-1)(x^q-1)}{x-1}$ f(x), where $f(x) \in GF(2)[x]$.

Now from the above Lemma (3.2), $2 \in D_0$, gives rises to an integer s $\le (e-1)$be such that$g^s = (2\ mod\ N)$i.e. the index of 2(mod N) base g is s. Again, from the property of greatest common divisor, $gcd\{\frac{(p-1)}{2^l t}, \frac{(q-1)}{2^l t}\}$= 1. On the otherhand, when $g^s \le 2\ (mod\ N)$ and $2 \notin D_0$ and by Lemma (3.4) gives $S_0(\alpha^w) = 0$ if and only if $w = 0$, or $w \in Q, from$ (3.2).

Therefore $gcd(x^{pq} - 1, S_0(x))$ = $x^p - 1$.

The minimal characteristic polynomial will have the expression

$$m(x) = \frac{x^{pq} - 1}{gcd\{(x^{pq} - 1), S_0(x)\}}$$

$$= \frac{x^{pq} - 1}{x^p - 1}$$

$$L(s^\infty) = deg(m(x)) = pq - p$$

$$= (q - 1)p$$

- this gives the linear complexity under certain conditions.

Define a function $f_j(x) = \prod_{i \in D_j}(x - \alpha^i)$, $j = 0, 1, 2, \ldots, \mu - 1$.

Again, lemma(3.3) gives us 2 $D_0 = D_0$.

And $f_0 have\ the\ property\ that f_0^2(x) = f_0(x)$. Thus we have

$$x^{pq} - 1 = \frac{(x^p - 1)(x^q - 1)\prod_{i=1}^{\mu-1} f_i\ (x)}{x - 1}$$

where the polynomials $f_i\ (x)$depending upon the choice of α.

The lemma (3.7) says that there are exactly 2^{l-1}tnumber of S $_i$for whichS$_i$ (α)= 0.

Lastly, we define a set

$\beta = \{i_j\ |S_{i_j}(\alpha) = 0, j = 0, 1, 2, \ldots, \mu - 1\} \subseteq \{0, 1, 2, \ldots, 2^l t - 1\} = I$

But this gives either w $\in \bigcup_{i \in \beta} D_i$ or w $\in$ Q.So, gcd((x^N– 1), S$_0$(x))= (x^q– 1)$\prod_{I=1}^{\mu-1}$ f$_i$(x).

Hence the characteristic polynomial of the sequence is

$$m(x) = \frac{x^N - 1}{\gcd(x^N - 1, S_0(x))} = \frac{x^{pq} - 1}{(x^p - 1)\prod_{i \in \beta} f_i(x)}$$

Again $L(s^\infty) = \deg(m(x)) = N - p - \mu e = \frac{(p+1)(q-1)}{2}$. Therefore, from the above two results, we have the following conclusions.

Theorem. 3.1

For a positive integer s, such that $g^s = 2(\bmod pq)$, then the linear complexity of sequence s^∞ of order $2^l t$, is given by $L(s^\infty) =$

$pq - p - \min(2^l, t)\,\mathrm{lcm}(p-1, q-1)$.

Proof. The result follows from the lemma 3.4, lemma 3.6 and lemma 3.7.

Theorem 3.2

If there exist s, such that $g^s \neq 2(\bmod pq)$, then the linear complexity of sequence s^∞ of order $2^l t$ will be $L(s^\infty) = p(q-1)$.

Corollary 3.3

In particular, if t = 1, then the order of the sequence become2^l. In that case$L(s^\infty) = \frac{(p+1)(q-1)}{2}$.

IV. Conclusion.

In this work, we have studied an extension of the binary generalised cyclotomic sequence, which has been widely considered in the literature. More exactly, we have investigated the linear complexity of a binary sequence having period pq and order $2^l t$, for any integer$t \geq 1$. These sequences with higher linear complexity are significant for additive stream ciphering. Being of this large linear complexity, the above sequence is a valid one, from linear complexity point of view and that could resist linear attack betterly.

Reference

[1] Cusick, T. W., Ding C., and Renvall, A., Stream Ciphers and Number Theory, Elsevier, Amsterdam, (1998).

[2] Ghosh, D. and Pal, J., New Approach of Deterministic Key Pre-distribution Scheme Using Triangle Free Quasi Symmetric Designs, Appli., Applied Maths 14(1) (2019) 188--198.

[3] Herlestam, T., On the complexity of functions of linear shift registers, in Advances in Cryptology, Lecture Notes in Computer Science, vol. 219. Heidelberg, Germany: Springer, (1988) 119–129.

[4] Massey, J. L., Shift register synthesis and BCH decoding, IEEE Trans. Inf. Theory 15(1) (1969) 122--127.

[5] Whiteman, A., L., A family of difference set, Illinois J. Math., 6 (1962) 107--121.

[6] Ding, C., Helleseth, T., and Shan, W. On the linear complexity of Legendre sequences, IEEE Trans. Inf. Theory 44(3) (1998) 1276–1278.

[7] Cao, J., Yue, Q., and Hu, L., Whiteman's generalized cyclotomic numbers with respect to t primes, Finite Fields Appl. 18(3) (2012) 634–644.

[8] Ding, C., Cyclic codes from the two primes sequences, IEEE Trans. Inf. Theory 58(6) (2012) 3881–3891.

[9] Edemskii, V. A., On the linear complexity of binary sequences on the basis of biquadratic and sextic residue classes. Discrete. Math. Appl., 2010, 20(1) (2010) 75--84.

[10] Edemskii, V., Ivanov, A., The linear complexity of balanced quaternary sequences with optimal autocorrelation value. Cryptography and Communications, 7(4) (2015) 485-496.

[11] Ding, C, Linear complexity of generalized cyclotomic binary sequences of order 2, Finite Fields Appl. 3, (1997) 159–-174.

[12] Ding, C., Cyclic codes from cyclotomic sequences of order four, Finite Fields Appl. 23(1) (2013) 8–34.

[13] Edemskii, V, The linear complexity and autocorrelation of quaternary Whiteman's Sequences,Applied Mathematics, Electronics and Computers, 1(4), (2013), 7--11.

[14] 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) (2005) 1849–1854.

[15] Yan, T., Du X., Xiao G., and Huang, X., Linear complexity of binary Whiteman generalized cyclotomic sequences of order z^k, Inf. Sci. 179(7) (2009) 1019–1023.

[16] Lidl, N. and Niederreiter, H., Finite Fields: Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, (1984).