Information Sciences 179 (2009) 1019–1023

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k ☆

Tongjiang Yan [a,b,*], Xiaoni Du [b,c], Guozhen Xiao [b], Xiaolong Huang [d]

[a] College of Mathematics and Computational Science, China University of Petroleum, North 2, 271, Dongying 257061, China
[b] ISN National Key Laboratory, Xidian University, Xi'an 710071, China
[c] College of Mathematics and Information Technology, Northwest Normal University, Lanzhou 730070, China
[d] The First Recovey Team, Zhongyuan Petrochemical Co. Ltd., Sinopec. 457000, China

A R T I C L E I N F O

Article history:
Received 21 July 2007
Received in revised form 11 August 2008
Accepted 11 November 2008

Keywords:
Stream ciphers
Sequences
Cyclotomy
Linear complexity
Minimal polynomials

A B S T R A C T

In this correspondence, we obtain the linear complexity and minimal polynomials of binary Whiteman generalized cyclotomic sequences of order 2^k, where $k > 1$. Our result shows that all of these sequences possess large linear complexity.

1. Introduction

Pseudo-random sequences used for stream ciphers are required to have the properties of unpredictability. The linear complexity is one of the important components that indicate this feature. If a sequence $s^\infty = (s_0, s_1, s_2, \dots)$ satisfies $s_j + c_1 s_{j-1} + \cdots + c_L s_{j-L} = 0$, where $j \geqslant L$, L is a positive integer, $c_1, c_2, \dots, c_L \in \mathrm{GF}(M)$, $\mathrm{GF}(M)$ denotes a Galois field of order M, then the least L is called the linear complexity of the sequence s^∞, denoted by $L(s^\infty)$, which is the length of the shortest linear feedback shift register (LFSR) that can generate this sequence. By the Berlekamp–Massey algorithm [4], if $L(s^\infty) > N/2$ (N is the least period of s^∞), then s^∞ is considered good 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 $S(x) = s_0 + s_1 x + s_2 x^2 + \cdots = \sum_{i=0}^{\infty} s_i x^i$ and $S^N(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}$, respectively. If N is a period of s^∞, then $m(x) = (1 - x^N)/\gcd(s^N(x), 1 - x^N)$ is called the minimal polynomial of s^∞, yielding the classic equation

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

We refer readers to Cusick et al. [4] for details.

☆ Project supported by the China University of Petroleum Doctor Foundation (y080806) and the Science and Research Foundation (Y080803).

* Corresponding author. Address: College of Mathematics and Computational Science, China University of Petroleum, North 2, 271, Dongying 257061, China.
E-mail address: yantoji@163.com (T. Yan).

0020-0255/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2008.11.006

Let p and q be odd primes, $d = \gcd(p-1, q-1)$ and $e = (p-1)(q-1)/d$. The Chinese Remainder Theorem guarantees that there exists a common primitive root, g, of both p and q, and the order of g modulo N is e. Let x be an integer satisfying $x \equiv g(\bmod p)$, and $x \equiv 1(\bmod q)$. The existence and uniqueness of $x(\bmod pq)$ are also guaranteed by the Chinese Remainder Theorem. Thus, we can get a subgroup of the residue ring, Z_N, with its multiplication [12], as the following:

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

A Whiteman generalized cyclotomic class of order d with respect to p and q [4] is defined as

$$D_i = \{g^s x^i : s = 0, 1, \ldots, e-1\}, \quad \text{where } i = 0, 1, \ldots, d-1.$$

Let $P = \{p, 2p, \ldots, (q-1)p\}, Q = \{q, 2q, \ldots, (p-1)q\}$ and $R = \{0\}$. We consider the case $d = \gcd(p-1, q-1) = 2^k$. Let

$$C_0 = \bigcup_{i=0}^{2^{k-1}-1} D_i, C_1 = \bigcup_{i=2^{k-1}}^{2^k-1} D_i, \quad B_0 = R \cup Q \cup C_0, B_1 = P \cup C_1.$$

Then $B_0 \cup B_1 = Z_N, B_0 \cap B_1 = \emptyset$, where $\emptyset$ denotes the empty set.

A binary sequence $s = (s_0, s_1, \ldots)$ is defined by Ding and Helleseth as the generalized Whiteman cyclotomic sequence of order d as the following:

$$s_i = \begin{cases} 1, & \text{if } i(\bmod N) \in B_1, \\ 0, & \text{otherwise.} \end{cases}$$

Generalized Whiteman cyclotomic sequences behave like the twin-prime sequences and have several good randomness properties which are important in cryptography and coding [4,6,9]. These sequences of order 2 have been shown to possess high linear complexity [7] and low autocorrelation [3–5]. Then Bai et al. proved that the linear complexity of these sequences of order 4 is high enough [1]. Now we consider the linear complexity of these sequences of order 2^k, where $k > 1$.

Some new generalized cyclotomic sequences defined by Ding and Helleseth and their modified versions defined by Li et al. are based on a new generalized cyclotomy [8,10,11]. Although most of these new sequences have been proved to possess good linear complexity [2,10,11,13–16], but their properties of correlation are not good enough [14,16].

2. Linear complexity of binary Whiteman generalized cyclotomic sequences of order 2^k

In the following, we always assume k is larger than 1. The following Lemmas 1–6 are needed to prove Lemma 7.

Lemma 1 [4]. *Let the symbols be the same as before. Then*

(1) *$ord_N(g) = e$, where $ord_N(g)$ denotes the order of g modulo N.*
(2) *D_0 is a subgroup of Z_N^*.*

Lemma 2 [4]. *For all $a \in D_i$, $aD_j = D_{i+j}$.*

Define $J_i = \bigcup_{t=2^{k-1}+i}^{2^k-1+i} D_t$. Then Lemma 2 yields

Lemma 3. *$J_0 = C_1, J_{2^{k-1}} = C_0$ and $aJ_i = J_{i+j}$, for each $a \in D_j$.*

If we define $S_i(x) = \sum_{j \in J_i \cup P} x^j$, where $i = 0, 1, \ldots, 2^k - 1$, then $S_0(x) = \sum_{i \in B_1} x^i$ is the generating polynomial of the binary sequence s^∞. Let α be a primitive Nth root of unity over the field $GF(2^m)$ which is the splitting field of $x^N - 1$, where $m = ord_N(2)$.

Lemma 4. *Let the symbols be the same as before. Then*

(1) *$\sum_{j \in P} \alpha^j = \sum_{j \in Q} \alpha^j = 1$.*
(2) *$S_i(\alpha) + S_{2^{k-1}+i}(\alpha) = 1$.*

Proof. From the definition of α, we have

$$0 = \alpha^N - 1 = (\alpha^p)^q - 1 = (\alpha^p - 1)(1 + \alpha^p + \alpha^{2p} + \cdots + \alpha^{(q-1)p}).$$

Hence, $1 + \alpha^p + \alpha^{2p} + \cdots + \alpha^{(q-1)p} = 0$. By symmetry, we have

$$1 + \alpha^q + \alpha^{2q} + \cdots + \alpha^{(p-1)q} = 0. \tag{2}$$

So (1) of this lemma is proven.

From the definition of α, we have

$$0 = \alpha^N - 1 = (\alpha - 1)(1 + \alpha + \alpha^2 + \cdots + \alpha^{pq-1}). \tag{3}$$