Available online at www.sciencedirect.com
ScienceDirect
Information Sciences 178 (2008) 807–815
INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL
www.elsevier.com/locate/ins

The linear complexity of new generalized cyclotomic binary sequences of order four ☆

Tongjiang Yan [a,b,*], Li Hong [c], Guozhen Xiao [b]

[a] College of Mathematics and Computational Science, China University of Petroleum, Dongying 257061, China
[b] ISN National Key Laboratory, Xidian University, Xi'an 710071, China
[c] College of Computer and Communication Engineering, China University of Petroleum, Dongying 257061, China

Received 17 May 2006; received in revised form 12 September 2007; accepted 14 September 2007

Abstract

Whiteman generalized cyclotomic sequences are proven to exhibit a number of good randomness properties. In this paper we determine the linear complexity of some newly generalized cyclotomic sequences, of order four with period pq which are defined by Ding and Helleseth. The results show that all of these sequences have high linear complexity.

Keywords: Stream ciphers; Sequences; Generalized cyclotomy; Linear complexity; Minimal polynomial

1. Introduction

Pseudo-random sequences with certain unpredictable properties are widely used in simulation, software testing, ranging systems, global positioning systems, code-division multiple-access systems, radar systems, spread-spectrum communication systems and especially in stream ciphers [14,16]. Linear complexity, $L(s^\infty)$, is one of the important characteristics that indicates the unpredictability of the sequence, s^∞, and is the length of the shortest linear feedback shift register (LFSR) that can generate this sequence [9]. In practice, if $L(s^\infty) \geqslant N/2$ (where N denotes the period of the sequence), then one needs the complete sequence to deduce the feedback function; thus it might be said that a good sequence has $L(s^\infty) \geqslant N/2$ [12].

As we all know, certain cyclotomic sequences, such as Legendre sequences and Hall's sextic residue sequences, possess good linear complexity and autocorrelation properties [8,10,11,13]. In [3–5,7,8], Ding defined a new generalized cyclotomic sequence (W-GCS$_{2k}$, where $2k$ is the order, $k = 1, 2, \ldots$) from the Whiteman generalized cyclotomy and determined the linear complexity and autocorrelation of W-GCS$_2$. The linear complexity of W-GCS$_4$ was calculated by E. Bai et al. [1]. In [6], Ding and Helleseth defined a new generalized

☆ The National Natural Science Foundations of China (No. 60473028) and (No. 60503009).
* Corresponding author. Address: College of Mathematics and Computational Science, China University of Petroleum, Dongying 257061, China.
E-mail address: yantoji@163.com (T. Yan).

0020-0255/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2007.09.012

cyclotomic sequence (D-GCS$_{2k}$, where $2k$ is the order) from a new generalized cyclotomy, and predicted that it may find some applications in cryptography and coding. Later, the D-GCS$_2$ with period pq (where p and q are distinct odd primes) was proven to have high linear complexity [2]. This paper contributes to this line of research by calculating the linear complexity of the D-GCS$_4$ with period pq.

Let p and q ($p < q$) be two odd primes with $\gcd(p-1, q-1) = 4$. Define $N = pq$, $e = (p-1)(q-1)/4$. 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 $x \equiv g(\mathrm{mod}p)$, and $x \equiv 1(\mathrm{mod}q)$. The existence and uniqueness of $x(\mathrm{mod}pq)$ are also guaranteed by the Chinese Remainder Theorem. Thus, we can get a subgroup of the residue ring, Z_N, with its multiplication [15], as the following:

$$Z_N^* = \{g^s x^i : s = 0, 1, \ldots, e-1;\ i = 0, 1, 2, 3\}.$$

A Ding generalized cyclotomic class of order four (D-GC$_4$) with respect to p and q is defined as

$$D_i = \left\{ g^{4t+i} x^j : t = 0, 1, \ldots, \frac{e}{4} - 1,\ j = 0, 1, 2, 3 \right\},$$

where $i = 0, 1, 2, 3$ [6,2]. Then $Z_N^* = \cup_{i=0}^{3} D_i$, $D_i \cap D_j = \emptyset$ for $i \neq j$, where $\emptyset$ denotes the empty set.

If we define

$$D_i^{(p)} = \left\{ g^{4t+i} : t = 0, 1, \ldots, \frac{p-5}{4} \right\}, \quad D_i^{(q)} = \left\{ g^{4t+i} : t = 0, 1, \ldots, \frac{q-5}{4} \right\},$$

then $gD_i^{(p)} = D_{i+1}^{(p)}$, $gD_i^{(q)} = D_{i+1}^{(q)}$, $i = 0, 1, 2, 3$.

Let

$$P = \{p, 2p, \ldots, (q-1)p\}, \quad Q = \{q, 2q, \ldots, (p-1)q\}, R = \{0\},$$
$$P_i = pD_i^{(q)}, Q_i = qD_i^{(p)}, \quad C_1 = Q_2 \cup Q_3 \cup P_2 \cup P_3 \cup D_2 \cup D_3.$$

Ding generalized cyclotomic sequence of order four (D-GCS$_4$, with $s^\infty = \{s_0, s_1, \ldots, s_i, \ldots\}$) is defined as

$$s_i = \begin{cases} 1 & \text{if } i(\mathrm{mod}N) \in C_1, \\ 0 & \text{otherwise.} \end{cases}$$

Then s^∞ possesses the minimum period pq, and the balance of the symbols 1s and 0s.

2. Linear complexity and minimal polynomial of the D-GCS$_4$

For a binary sequence, s^∞, with period N, if $S^N(x) = s_0 + s_1 x + \cdots + s_{N-1}x^{N-1}$, its minimal polynomial and linear complexity can be calculated by the following equations [5]:

$$1.\ m(x) = (x^N - 1)/\gcd(x^N - 1, S^N(x)), \tag{1}$$
$$2.\ L(s^\infty) = N - \deg(\gcd(x^N - 1, S^N(x))). \tag{2}$$

Let α be a primitive Nth root of unity over the field $\mathbf{GF}(2^m)$ that is the splitting field of $x^N - 1$. Then, by Eq. (2), we have

$$L(s^\infty) = N - |\{j : S(\alpha^j) = 0, 0 \leqslant j \leqslant N-1\}|, \tag{3}$$

where $S(x)$ is defined by

$$S(x) = \left(\sum_{i \in 2} + \sum_{i \in Q_3} + \sum_{i \in P_2} + \sum_{i \in P_3} + \sum_{i \in D_2} + \sum_{i \in D_3} \right) x^i \in \mathbf{GF}(2)[x].$$

Note that

$$S(1) = S(\alpha^0) = \left(\sum_{i \in Q_2} + \sum_{i \in Q_3} + \sum_{i \in P_2} + \sum_{i \in P_3} + \sum_{i \in D_2} + \sum_{i \in D_3} \right) 1 = \frac{p-1}{2} + \frac{q-1}{2} + \frac{(p-1)(q-1)}{2} = 0(\mathrm{mod}\,2). \tag{4}$$