Available online at www.sciencedirect.com
ScienceDirect
Applied Mathematics Letters 21 (2008) 187–193
Applied Mathematics Letters
www.elsevier.com/locate/aml

On the linear complexity of generalized cyclotomic sequences with the period p^m ☆

Tongjiang Yan[a,b,*], Shengqiang Li[b], Guozhen Xiao[b]

[a] *Institute of Mathematics and Computational Science, China University of Petroleum, Dongying 257061, China*
[b] *ISN National Key Laboratory, Xidian University, Xi'an 710071, China*

Received 9 December 2005; received in revised form 11 March 2007; accepted 13 March 2007

Abstract

This letter contributes to the investigation of the linear complexity of generalized cyclotomic sequences with the period p^m, which are contained by the sequences constructed by C. Ding and T. Helleseth in 1998, as a representative special case. The results obtained confirm that all of these sequences have high linear complexity.

Keywords: Stream ciphers; Sequences; Cyclotomy; Linear complexity; Minimal polynomials

1. Introduction

Pseudo-random sequences used for stream ciphers are required to have the properties of unpredictability. Balance and linear complexity are two main components that indicate this feature. If a sequence $s^\infty = (s_0, s_1, \ldots, s_i, \ldots)$ satisfies

$$s_j + c_1 s_{j-1} + \cdots + c_L s_{j-L} = 0, \quad j \geq L, \tag{1}$$

where L is a positive integer, $c_1, c_2, \ldots, c_L \in \mathrm{GF}(p^n)$, $\mathrm{GF}(p^n)$ denotes a Galois field of order p^n, then the least L is called the linear complexity of the sequence s^∞, denoted by $L(s^\infty)$. The Berlekamp–Massey algorithm [1] states that if $L(s^\infty) > N/2$ (N is the least period of s^∞), s^∞ is considered good with respect to its linear complexity. The characteristic polynomials of the sequences $s^\infty = (s_0, s_1, \ldots, s_i, \ldots)$ and $s^N = (s_0, s_1, \ldots, s_{N-1})$ are defined as $s(x) = s_0 + s_1 x + \cdots + s_i x^i + \cdots = \sum_{i=0}^{\infty} s_i x^i$ and $s^N(x) = s_0 + s_1 x + \cdots + s_{N-1} x^{N-1}$ 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 [2]

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

We refer readers to [3,4] for details.

☆ Project supported by the National Natural Science Foundations of China (No. 60473028).

* Corresponding author at: Institute of Mathematics and Computational Science, China University of Petroleum, Dongying 257061, China. Tel.: +86 5468391368.
E-mail address: yantoji@163.com (T. Yan).

0893-9659/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.aml.2007.03.011

In this work, $xA = \{xa | a \in A\}$, $x+A = \{x+a | a \in A\}$, $\mathrm{ord}_N(x)$ denotes the order of x modulo N, $\gcd(a(x), b(x))$ denotes the largest common factor of $a(x)$ and $b(x)$, and $\varphi(x)$ is the Euler function. If g is an element of a group G, then (g) denotes a subgroup generated by the element g in G.

2. Generalized cyclotomy and sequences

Here we introduce a fact which we use in the sequel:

Lemma 1 (*[5]*). *Let p be a prime; then the following three assertions are equivalent:*

1. *g is a primitive root of p and $g^{p-1} \not\equiv 1 \pmod{p^2}$.*
2. *g is a primitive root of p^2.*
3. *For every $e \geq 2$, g is a primitive root of p^e.*

Assume p to be an odd prime and m a natural number larger than 1. By Lemma 1, if g is a primitive root of p^2 and $g_n \equiv g \bmod p^n$, then g_n is a primitive root of p^n where $n = 1, 2, 3, \ldots, m$, and $g_2 = g$. Moreover, by the Chinese Remainder Theorem, $\mathrm{ord}_{p^n}(g_n) = \varphi(p^n) = p^{n-1}(p-1)$.

For each n, $n = 1, 2, 3, \ldots, m$, define $Z^*_{p^n} = (g_n)$, $D^{(n)}_0 = (g_n^2)$, $D^{(n)}_1 = gD^{(n)}_0$, $R^{(n)} = \{0, p, 2p, \ldots, (p^{n-1} - 1)p\} = pZ_{p^{n-1}}$; then $Z^*_{p^n}$ and $D^{(n)}_0$ are multiplicative groups and the residue class ring Z_{p^n} possesses the following partitions:

$$Z_{p^n} = D^{(n)}_0 \cup D^{(n)}_1 \cup R^{(n)} = Z^*_{p^n} \cup R^{(n)}. \tag{3}$$

For n_1, n_2 $(n_1 < n_2)$, it is easy to prove that $D^{(n_2)}_i \bmod p^{n_1} \equiv D^{(n_1)}_i$, $R^{(n_2)} \bmod p^{n_1} \equiv R^{(n_1)}$, $i = 0, 1$.

Thus we obtain the m partitions of the residue ring Z_{p^m}:

$$\begin{aligned} Z_{p^m} &= D^{(m)}_0 \cup D^{(m)}_1 \cup pZ_{p^{m-1}} \\ &= \left(D^{(m)}_0 \cup pD^{(m-1)}_0\right) \cup \left(D^{(m)}_1 \cup pD^{(m-1)}_1\right) \cup p^2 Z_{p^{m-2}} \\ &\cdots \\ &= \bigcup_{n=1}^{m} p^{m-n} D^{(n)}_0 \cup \bigcup_{n=1}^{m} p^{m-n} D^{(n)}_1 \cup \{0\}. \end{aligned} \tag{4}$$

If we assume that

$$C_0 = \bigcup_{n=1}^{m} p^{m-n} D^{(n)}_0, \quad C_1 = \bigcup_{n=1}^{m} p^{m-n} D^{(n)}_1 \cup \{0\}, \tag{5}$$

then $C_0 \cup C_1 = Z_{p^m}$, $C_0 \cap C_1 = \emptyset$, where $\emptyset$ denotes the empty set.

The binary generalized cyclotomic sequence $s^\infty = (s_0, s_1, \ldots, s_i, \ldots)$ of order 2 is defined as

$$s_i = \begin{cases} 0, & \text{if } i \bmod p^m \in C_0, \\ 1, & \text{if } i \bmod p^m \in C_1, \end{cases} \text{ for all } i \geq 0. \tag{6}$$

Its balance is guaranteed by the definition. Since p^n $(n < m)$ is not a period of s^∞, then it possesses the least period p^m. This sequence is introduced in [6] and can be considered as a representative special case of the sequences defined by Ding and Helleseth [7], of which the generalized cyclotomic sequence with the period pq is another representative special case, the linear complexity of which was determined by Bai et al. in 2005 [2].

3. Linear complexity of generalized cyclotomic sequences

Lemma 2 (*[7, Lemma 7]*). *If $a \in D^{(n)}_i$, then $aD^{(n)}_j = D^{(n)}_{(i+j) \bmod 2}$, $0 \leq i, j \leq 1$, $1 \leq n \leq m$.*

Let $k = \mathrm{ord}_{p^m} 2$ and θ_m be a p^mth primitive root of unity in $\mathrm{GF}(2^k)$. Assume $\theta_n = \theta^{m-n}$; then θ_n is a p^nth primitive root of unity in $\mathrm{GF}(2^k)$.