Information Processing Letters 116 (2016) 153–156

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

The linear complexity of binary sequences of length $2p$ with optimal three-level autocorrelation

V. Edemskiy *, A. Palvinskiy

Department of Applied Mathematics and Informatics, Novgorod State University, Veliky Novgorod, Russia

ARTICLE INFO

Article history:
Received 1 March 2015
Received in revised form 10 August 2015
Accepted 15 September 2015
Available online 25 September 2015
Communicated by S.M. Yiu

Keywords:
Cryptography
Linear complexity
Binary sequences

ABSTRACT

In this paper we derive the linear complexity of binary sequences of length $2p$ with optimal three-level autocorrelation. These almost balanced and balanced sequences are constructed by cyclotomic classes of order four using a method presented by Ding et al. We investigate the linear complexity of above-mentioned sequences over the finite fields of different orders.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

Autocorrelation is an important measure of pseudo-random sequence for their application in code-division multiple access systems, spread spectrum communication systems, radar systems and so on [5]. An important problem in sequence design is to find sequences with optimal autocorrelation. In their paper, Ding et al. [3] give several new families of binary sequences of period $2p$ with optimal autocorrelation $\{-2, 2\}$. These sequences have also been referred to as generalized cyclotomic sequences.

The linear complexity is another important characteristic of pseudo-random sequence significant for cryptographic applications. It is defined as the length of the shortest linear feedback shift register that can generate the sequence [8]. The linear complexity of above-mentioned sequences over the finite field of order two was investigated in [11] (see also references therein). Also, the linear complexity of several cyclotomic sequences of length p was derived in [1,2] over the finite field $\mathbb{F}_p$ and Legendre sequences over $\mathbb{F}_q$ in [10].

In this paper we derive the linear complexity of binary sequences of length $2p$ from [3] over the finite field of odd characteristic q, $q = p$ in Section 3 and $q \neq p$ in Section 4. We show the linear complexity of these sequences to be high for any length.

2. The definition of sequences

First, we briefly repeat the basic definitions from [3].

Let p be a prime of the form $p \equiv 1 (\text{mod } 4)$, and let θ be a primitive root modulo p [7]. By definition, put $D_0 = \{\theta^{4s} \bmod p; s = 1, \dots, (p-1)/4\}$ and $D_n = \theta^n D_0$, $n = 1, 2, 3$. Then D_n are cyclotomic classes of order four [6].

The ring residue classes $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \times \mathbb{Z}_p$ relative to isomorphism $\phi(a) = (a \bmod 2, a \bmod p)$ [7]. Ding et al. considered sequences defined as

$$s_i = \begin{cases} 1, & \text{if } \; i \bmod 2p \in C; \\ 0, & \text{if } \; i \bmod 2p \notin C, \end{cases} \tag{1}$$

for $C = \phi^{-1}\left(\{0\} \times (D_k \cup D_j) \cup \{1\} \times (D_l \cup D_j)\right)$ where i, j, and l are pairwise distinct integers between 0 and 3, also for $C^{(0)} = C \cup \{0\}$ [3].

By [3], if $\{s_i\}$ have an optimal autocorrelation value then $p \equiv 5 (\text{mod } 8)$ and $p = 1 + 4y^2$ or $p = x^2 + 4$, $y = 1$.

* Corresponding author. Tel.: +78162629972; fax: 78162624110.
E-mail address: Vladimir.Edemsky@novsu.ru (V. Edemskiy).

http://dx.doi.org/10.1016/j.ipl.2015.09.007
0020-0190/© 2015 Elsevier B.V. All rights reserved.

Here x, y are integers and $x \equiv 1 (\text{mod } 4)$. In what follows, we will consider only these p.

To begin with, we give another definition of the sequence $\{s_i\}$. It is known that if g is an odd number in the pair θ, $\theta + p$, then g is a primitive root modulo $2p$ [7]. By definition, put $H_0 = \{g^{4s} \mod 2p; s = 1, \dots, (p-1)/4\}$. Denote by H_n a set $g^n H_0$, $n = 1, 2, 3$. Further, we will consider the indices of H_n modulo 4.

Since $p \equiv 5 (\text{mod} 8)$, it follows that $ind_\theta 2 \equiv 1 (\text{mod} 4)$ or $ind_\theta 2 \equiv 3 (\text{mod} 4)$ [7]. If $ind_\theta 2 \equiv 1 (\text{mod} 4)$ then $ind_{\theta^{-1}} 2 \equiv 3 (\text{mod} 4)$. Hence, without loss of generality, we can assume that $ind_\theta 2 \equiv 3 (\text{mod} 4)$. We choose $ind_\theta 2 \equiv 3 (\text{mod} 4)$ because below we will investigate the sequences for $y = 1$.

Lemma 1.

(i) $\phi^{-1}(\{0\} \times D_n) = 2H_{n-3}, n = 0, \dots, 3;$
(ii) $\phi^{-1}(\{1\} \times D_n) = H_n, n = 0, \dots, 3;$
(iii) $2H_{n-3} = H_n + p, n = 0, \dots, 3.$

Lemma 1 follows from our definitions.

So, if $\{s_i\}$ is defined by (1) then

$$s_i = \begin{cases} 1, & \text{if } \ i \mod 2p \in 2H_{k-3} \cup 2H_{j-3} \\ & \qquad\qquad \cup H_l \cup H_j; \\ 0, & \text{if } \ \text{else}. \end{cases} \tag{2}$$

3. The linear complexity of sequences over $\mathbb{F}_{p^r}$

First of all, we derive the linear complexity of $\{s_i\}$ for $q = p$. In this case we use Günther–Blahut theorem (see, for example [9]).

Lemma 2. *Let $0 \le m \le 3$ and $d = m(p-1)/4$. Then*

$$\sum_{i \in H_m} i^n = \begin{cases} 0, & \text{if } 1 \le n \le (p-5)/4, \\ g^d (p-1)/4, & \text{if } n = (p-1)/4. \end{cases}$$

Proof. By definition of H_m we have $\sum_{i \in H_m} i^{(p-1)/4} = g^d (p-1)/4$. Suppose $n < (p-1)/4$; denote $\sum_{i \in H_0} i^n$ by A. Since $\sum_{j=1}^{p-1} j^n = 0$, it follows that $0 = \sum_{t=0}^{3} \sum_{i \in H_t} i^n = A(g^{4n} - 1)/(g^n - 1)$. Hence, $A = 0$ and $\sum_{i \in H_m} i^n = 0$. $\square$

Let us introduce the auxiliary polynomials $F_m(x) = \sum_{i \in H_m} x^i$.

Lemma 3. *Let $F_m^{(n)}(x)$ be a formal derivative of order n of the polynomial $F_m(x)$. Then*

$$F_m^{(n)}(\pm 1) = \begin{cases} 0, & \text{if } 1 \le n \le (p-5)/4, \\ g^d (p-1)/4, & \text{if } n = (p-1)/4. \end{cases}$$

Proof. Let $T_1(x) = x F'_m(x)$ and $T_n(x) = x T'_{n-1}(x)$, $n = 2, 3, \dots$. Then $T_n(\pm 1) = \pm \sum_{i \in H_m} i^n$, $n = 1, 2, \dots$, and by Lemma 2 $T_n(\pm 1) = 0$ if $1 \le n \le (p-5)/4$; $T_{(p-1)/4}(\pm 1) = \pm g^d (p-1)/4$.

To conclude the proof, it remains to note that by definition $T_n(x) = \sum_{j=1}^{n-1} a_j(x) F_m^{(j)}(x) + x^n F_m^{(n)}(x)$, where $a_j(x)$ are polynomials. $\square$

Our first contribution in this paper is the following.

Theorem 4. *Let the almost balanced binary sequences $\{s_i\}$ be defined by (1) for $C = \phi^{-1}\big(\{0\} \times (D_k \cup D_j) \cup \{1\} \times (D_l \cup D_j)\big)$. Then $L = (7p+1)/4$.*

Proof. In this case, by Günther–Blahut theorem we have

$$\begin{aligned} L = 2p &- \min\{j : \ S^{(j)}(1) \ne 0\} \\ &- \min\{j : \ S^{(j)}(-1) \ne 0\} \end{aligned} \tag{3}$$

where $S(x) = \sum_{i=0}^{2p-1} s_i x^i$ is the polynomial of $\{s_i\}$.

By definition $S(1) = p - 1$. Further, by (2) and by Lemma 1 we obtain

$$\begin{aligned} S(x) \equiv (x^p + 1) \sum_{i \in H_j} x^i + x^p \sum_{i \in H_k} x^i \\ + \sum_{i \in H_l} x^i \big(\text{mod}\,(x^{2p} - 1)\big). \end{aligned} \tag{4}$$

Therefore, since $\left(\sum_{i \in H_m} x^i\right)^{(n)} = F_m^{(n)}(x)$ by definition of $F_m^{(n)}(x)$, it follows that

$$\begin{aligned} S^{(n)}(\pm 1) = \big((x^p + 1) F_j^{(n)}(x) + x^p F_k^{(n)}(x) \\ + F_l^{(n)}(x)\big)\big|_{x = \pm 1}. \end{aligned} \tag{5}$$

So, by Lemma 3 we see $S^{(n)}(-1) = 0$ if $0 \le n \le (p-5)/4$ and $S^{((p-1)/4)}(-1) \ne 0$. Then the conclusion of this theorem follows from (3). $\square$

Theorem 5. *Let the balanced binary sequences $\{s_i\}$ be defined by (1) for $C^{(0)} = C \cup \{0\}$. Then $L = (7p+1)/4$.*

Proof. Let $S_0(x)$ be the polynomial of $\{s_i\}$ defined by (1) for $C^{(0)} = C \cup \{0\}$. Then $S_0(x) = S(x) + 1$ where $S(x)$ satisfies (4). Therefore, using (5), we can write $S^{(n)}(1) = 0$ if $0 \le n \le (p-5)/4$, $S^{((p-1)/4)}(1) \ne 0$ and $S(-1) \ne 0$. Then the conclusion of this theorem follows from (3). $\square$

The results of computing the linear complexity by Berlekamp–Massey algorithm when $p = 5, 37, 101, 197, 677$ $(x = 1)$ and $p = 5, 13, 29, 53, 173, 229, 293$ $(y = 1)$ confirm Theorems 4 and 5.

4. The linear complexity of sequences over $\mathbb{F}_{q^r}$ for $q \ne p$

Now we derive the linear complexity of $\{s_i\}$ over $\mathbb{F}_{q^r}$ for $q \ne p$. Let α be a primitive $2p$-th root of unity in the extension of the field $\mathbb{F}_{q^r}$. Then by Blahut's theorem for the linear complexity L of the sequence $\{s_i\}$ we have

$$L = 2p - \left| \left\{ i \,\middle|\, S(\alpha^i) = 0, \ \ i = 0, 1, \dots, 2p-1 \right\} \right|. \tag{6}$$

Let us derive L using the procedure proposed in [4]. In the next subsections we consider the values $S(\alpha^i)$, $i = 0, 1, \dots, 2p-1$. But first we need to prove intermediate lemmas.

Download English Version:

https://daneshyari.com/en/article/10331040

Download Persian Version:

https://daneshyari.com/article/10331040

Daneshyari.com