Information Processing Letters 112 (2012) 646–650

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

# New classes of quaternary cyclotomic sequence of length $2p^m$ with high linear complexity

Pinhui Ke *, Shengyuan Zhang

*Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou 350007, PR China*

ARTICLE INFO

*Article history:*
Received 2 February 2012
Received in revised form 27 May 2012
Accepted 31 May 2012
Available online 4 June 2012
Communicated by D. Pointcheval

*Keywords:*
Cryptography
Linear complexity
Quaternary sequence
Generalized cyclotomic sequence

ABSTRACT

In this paper, we introduce a new class of quaternary cyclotomic sequence over $\mathbb{F}_4$ with period $2p^m$. We prove that the constructed sequences possess high linear complexity.



## 1. Introduction

The linear complexity of a sequence is defined as the length of the shortest linear feedback shift register that can generate the sequence. By the Berlekamp–Massey algorithm [10], for a sequence with least period $N$, if its linear complexity is larger than $\frac{N}{2}$, then it is considered good with respect to its linear complexity. Pseudo-random sequences are required to have high linear complexity for cryptographic applications [2,3,6].

Different classes of cyclotomic sequences have been reported to possess good linear complexity. For the binary cyclotomic sequence, readers may refer to [2–4,7,8,13,14] and the references therein. Recently, a new class of almost quaternary cyclotomic sequences with ideal autocorrelation property was reported in [12]. However, compared to the quaternary sequences over $\mathbb{Z}_4$, there are sporadic results on the quaternary sequences over $\mathbb{F}_4$. In [5], a class of quaternary sequence of length $2p$ over $\mathbb{F}_4$ was defined and showed to have good linear complexity. For the application of quaternary sequences over $\mathbb{F}_4$, see [9], for instance.

In this paper, we construct a new class of quaternary sequences over $\mathbb{F}_4$ with length $2p^m$ by using generalized cyclotomic classes. The new constructed sequences are proved to be balanced and possess high linear complexity.

## 2. Preliminaries

Let $p$ be an odd prime and $g$ be a primitive root of $\mathbb{Z}_{p^2}^*$, where $\mathbb{Z}_n^*$ denotes the set of all invertible elements of $\mathbb{Z}_n$. Then it is known that $g$ is also a primitive root of $\mathbb{Z}_{p^m}^*$ for $m \geqslant 1$ [1]. Since either $g$ or $g + p^m$ is odd modulo $2p^m$ and both of them are primitive roots modulo $p^m$, we assume that $g$ is an odd integer without loss of generality. It is known that $g$ is also a primitive root of $\mathbb{Z}_{2p^m}^*$ [11]. Furthermore, $g$ is a common primitive root of $\mathbb{Z}_{p^j}^*$ and $\mathbb{Z}_{2p^j}^*$ for all $1 \leqslant j \leqslant m$.

Define

$$D_0^{(p^j)} = \langle g^2 \rangle \pmod{p^j},$$
$$D_0^{(2p^j)} = \langle g^2 \rangle \pmod{2p^j},$$
$$D_1^{(p^j)} = g D_0^{(p^j)} \pmod{p^j},$$
$$D_1^{(2p^j)} = g D_0^{(2p^j)} \pmod{2p^j},$$

* Corresponding author.
*E-mail addresses:* keph@fjnu.edu.cn (P. Ke), syzhang@fjnu.edu.cn (S. Zhang).

0020-0190/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ipl.2012.05.011

where $D_0^{(n)}$ and $D_1^{(n)}$ denote the generalized cyclotomic classes of order two with respect to $n$ [4]. It is well known that

$$\left|D_i^{(p^j)}\right| = \left|D_i^{(2p^j)}\right| = \frac{\varphi(p^j)}{2}, \quad i \in \{0,1\},$$

where $\varphi(\cdot)$ is the Euler function. Obviously, for $1 \leqslant j \leqslant m$, we have

$$\mathbb{Z}_{p^j}^* = D_0^{(p^j)} \cup D_1^{(p^j)}, \qquad \mathbb{Z}_{2p^j}^* = D_0^{(2p^j)} \cup D_1^{(2p^j)},$$

and

$$\begin{aligned}\mathbb{Z}_{2p^m} &= \bigcup_{j=1}^{m} p^{m-j}\left(\mathbb{Z}_{2p^j}^* \cup 2\mathbb{Z}_{p^j}^*\right) \cup \{0, p^m\},\\ &= \bigcup_{j=1}^{m}\left(p^{m-j}D_0^{(2p^j)} \cup p^{m-j}D_1^{(2p^j)} \cup 2p^{m-j}D_0^{(p^j)}\right.\\ &\quad \left.\cup\, 2p^{m-j}D_1^{(p^j)}\right) \cup \{0, p^m\}.\end{aligned}$$

For abbreviation, we define

$$H_i^{(p^j)} = p^{m-j}D_i^{(p^j)} \quad \text{and} \quad H_i^{(2p^j)} = p^{m-j}D_i^{(2p^j)},$$

for $i = 0, 1$. The partition of $\mathbb{Z}_{2p^m}$ described above can be depicted as the following table intuitively.

| | | | | | | |
|---|---|---|---|---|---|---|
| $H_0^{(2p^m)}$ | $2H_0^{(p^m)}$ | $\cdots$ | $\cdots$ | $H_0^{(2p)}$ | $2H_0^{(p)}$ | 0 |
| $H_1^{(2p^m)}$ | $2H_1^{(p^m)}$ | $\cdots$ | $\cdots$ | $H_1^{(2p)}$ | $2H_1^{(p)}$ | $p^m$ |

Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ be a finite field of order 4, where $\alpha$ satisfies $\alpha^2 = 1 + \alpha$. By assigning the elements of $\mathbb{F}_4$ to each generalized cyclotomic classes with respect to $\mathbb{Z}_{2p^m}$, one obtains a quaternary sequence of length $2p^m$ naturally. However, in order to guarantee that the constructed sequences have high linear complexity, one should do it technically.

Let $\Omega$ be a set of four tuple over $\mathbb{F}_4$ such that the elements in each tuple are pairwise distinct. We call each four tuple in $\Omega$ a *defining vector*. Assume $\mathrm{I} = (a, b, c, d) \in \Omega$, we construct a quaternary sequence with the first $2p^m$ terms of sequence $\{s_t\}$ defined as

$$s_t = \begin{cases} 0, & \text{if } t = 0;\\ e, & \text{if } t = p^m;\\ a, & \text{if } t \in \bigcup_{i=1}^m H_0^{(2p^i)};\\ b, & \text{if } t \in \bigcup_{i=1}^m H_1^{(2p^i)};\\ c, & \text{if } t \in \bigcup_{i=1}^m 2H_0^{(p^i)};\\ d, & \text{if } t \in \bigcup_{i=1}^m 2H_1^{(p^i)}, \end{cases} \tag{1}$$

where $e \neq b + d \in \mathbb{F}_4^*$ if $p \equiv \pm 1 \pmod 8$ and $e \neq b + c \in \mathbb{F}_4^*$ if $p \equiv \pm 3 \pmod 8$.

**Remark 1.** A quaternary sequence $\{a_i\}_{i=0}^{N-1}$ over $\mathbb{F}_4$ is called balanced if

$$\max_{i \in \mathbb{F}_4}\left|\{t \mid 0 \leqslant t \leqslant N-1,\ a_t = i\}\right| - \min_{i \in \mathbb{F}_4}\left|\{t \mid 0 \leqslant t \leqslant N-1,\ a_t = i\}\right| \leqslant 1.$$

The quaternary cyclotomic sequence defined in (1) is then obviously balanced.

**Remark 2.** If $p \equiv \pm 3 \pmod 8$, a class of quaternary sequence with length $2p$ was constructed in [5] and was shown to have linear complexity $2p$ (Theorem 1 in [5]). It can be regarded as a special case of our construction by taking $m = 1$ and $\mathrm{I} = (0, 1, \alpha^2, \alpha)$. If $p \equiv \pm 1 \pmod 8$, the quaternary sequence constructed in [5], which has linear complexity $p + 1$, is the same with our construction in (1) by taking $m = 1$ and $\mathrm{I} = (0, 1, \alpha^2, \alpha)$ except when $t = p^m$. However, as we will show in the next section, even a little modification of sequence $S$ will result in a great improvement with respect to the linear complexity.

## 3. Linear complexity of the constructed sequences

Let $\mathbb{F}_q$ be the finite field with $q$ element. Let $S = \{s_i\}$ be an $N$-periodic sequence over $\mathbb{F}_q$. The monic polynomial $f(x) = x^L + a_{L-1}x^{L-1} + \cdots + a_1x + a_0 \in \mathbb{F}_q[x]$ is called the *characteristic polynomial* of $S$, if

$$s_{L+t} + a_{L-1}s_{L-1+t} + \cdots + a_1s_{t+1} + a_0s_t = 0$$

holds for any $t \geqslant 0$. The characteristic polynomial $m(x) \in \mathbb{F}_q[x]$ with least degree is called the *minimal polynomial* of $S$. For a binary sequence, its minimal polynomial exists uniquely [6]. Furthermore, $\deg(m(x))$, denoted as $L(S)$, is called the linear complexity of $S$. The *generating polynomial* of the sequence $S$ is defined by

$$S(x) = s_0 + s_1x + \cdots + s_{N-1}x^{N-1} \in F_q[x].$$

It is well known that [2,6]

$$m(x) = \frac{x^N - 1}{\gcd(x^N - 1, S(x))}.$$

And the linear complexity of $S$ is then given by

$$L(S) = N - \deg\left(\gcd\left(x^N - 1, S(x)\right)\right). \tag{2}$$

By definition, the generating polynomials of the sequences in (1) is

$$S(x) = ex^{p^m} + a\sum_{i=1}^m S_i^{(0)}(x) + b\sum_{i=1}^m S_i^{(1)}(x) + c\sum_{i=1}^m S_i^{(2)}(x) + d\sum_{i=1}^m S_i^{(3)}(x),$$

where

$$S_i^{(0)}(x) = \sum_{t \in H_0^{(2p^i)}} x^t, \qquad S_i^{(1)}(x) = \sum_{t \in H_1^{(2p^i)}} x^t,$$

$$S_i^{(2)}(x) = \sum_{t \in 2H_0^{(p^i)}} x^t, \qquad S_i^{(3)}(x) = \sum_{t \in 2H_1^{(p^i)}} x^t.$$

Let $d$ be the order of 4 modulo $p^m$, namely, $d$ is the least positive integer satisfying $4^d \equiv 1 \pmod{p^m}$. Assume