Some Notes on Prime-Square Sequences

En-Jian Bai¹,² (白恩健) and Xiao-Juan Liu³ (刘晓娟)

¹School of Information Science and Technology, Donghua University, Shanghai 201620, China
²State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences
Beijing 100039, China
³Department of Information and Computing Science, Shanghai University of Electric Power, Shanghai 200090, China

E-mail: baiej@dhu.edu.cn; liuxiaojuan428@sina.com

Received November 2, 2005; revised December 8, 2006.

Abstract The well-known binary Legendre sequences possess good autocorrelation functions and high linear complexity, and are just special cases of much larger families of cyclotomic sequences. Prime-square sequences are the generalization of these Legendre sequences, but the ratio of the linear complexity to the least period of these sequences approximates to zero if the prime is infinite. However, a relatively straightforward modification can radically improve this situation. The structure and properties, including linear complexity, minimal polynomial, and autocorrelation function, of these modified prime-square sequences are investigated. The hardware implementation is also considered.

Keywords cyclotomy, autocorrelation, linear complexity, sequence

1 Introduction

Balanced binary sequences with optimal randomness properties, especially those with large linear complexity, are widely used in cryptosystems. They can be implemented as key stream in stream cipher models, session key and pseudo-random number in digital signature standard, and multi-media encryption, etc. A sequence of length $L$ is said to have the "good" linear complexity property if its linear complexity $C_L$ satisfies $C_L > L/2$. In practice, if $C_L > L/2$, then one needs to have the complete sequence to deduce its minimal polynomial[1].

Binary Legendre sequences are the well-known classes of sequences with good autocorrelation functions[2]. If $L \equiv 3 \mod 4$, the out-of-phase correlation values are all $-1$. If $L \equiv 1 \mod 4$, the out-of-phase correlation values are $-1$ or $3$. It has also been shown that these sequences also have good linear complexity with $(L-1)/2 \leq C_L \leq L$, depending on the residue $L \mod 8$[3].

Define a sequence $s$ of length $L$ by the following sequence generator,

$$s(i_0)_i = F_C(i_0 + i \mod L), \ i \geq 0$$ (1)

where $F_C(x)$ denotes the complement of $F_C(x)$, $0 \leq i_0 < L$ is the key of this generator, and

$$F_C(x) = \begin{cases} 0, & \text{for } x \in R, \\ \left(\frac{x^{\varphi(L)}}{2}\right) \mod 2, & \text{otherwise,} \end{cases}$$ (2)

where $\varphi(\cdot)$ is Euler function, and $R$ is defined depending on the length $L$.

Define $L = p$, where $p$ is a prime and $R = \{0\}$. A binary Legendre sequence can be constructed by using (1) and (2). If, take $L = p^2$, where $p$ is a prime, then $\varphi(p^2) = p(p-1)$. Define $R = \{0, p, 2p, \ldots, (p-1)p\}$.

The sequence defined by (1) and (2) is just the prime-square sequence[4], so the sequence is the generalization of Legendre sequence. The autocorrelation functions of prime-square sequence can be deduced from Legendre sequence easily. If $p \equiv 3 \mod 4$, the autocorrelation values are taken from $\{p^2, -p\}$, and if $p \equiv 1 \mod 4$, they are taken from $\{p^2, p, -3p\}$. The linear complexity of prime-square sequence has also been studied, the results are as follows[5]:

$$C_L = \begin{cases} (p+1)/2, & \text{if } p \equiv 1 \mod 8, \\ p-1, & \text{if } p \equiv 3 \mod 8, \\ p, & \text{if } p \equiv 5 \mod 8, \\ (p-1)/2, & \text{if } p \equiv 7 \mod 8. \end{cases}$$ (3)

Therefore, the maximum ratio of the linear complexity to the length of this sequence (linear complexity per symbol) is $1/p$, which is much smaller than $1/2$ if $p$ is a large prime.

The reason that prime-square sequences do not exhibit "good" randomness property may be their imbalance, which is defined as the difference between the number of 1s and the number of 0s. A prime-square sequence of length $p^2$ contains $p(p+1)/2$ 1s and $p(p-1)/2$ 0s, therefore, it has an imbalance $p$. However, a relatively straightforward modification can radically improve this situation. The modified prime-square sequences of length $p^2$ can be defined as (1) and the following:

$$R = \{0, p, 2p, \ldots, (p-1)\}$$

$$F_C(x) = \begin{cases} 0, & \text{for } x = 0 \\ \left(\frac{x^{\varphi(p)}}{p}\right) \mod p, & \text{for } x \in R', \\ \left(\frac{x^{\varphi(p)}}{p}\right) \mod p, & \text{otherwise,} \end{cases}$$ (4)

Short Paper

This work is supported by the National Natural Science Foundation of China under Grant No. 60503009.
where \( R' = R \setminus \{0\} \). Evidently, a modified prime-square sequence of length \( p^2 \) contains \((p + 1)(p - 1)/2 + 1\) 1s and \((p + 1)(p - 1)/2\) 0s, therefore, it has an imbalance 1 since \( p^2 \) is odd. In the following sections the randomness properties will be determined.

2 Modified Prime-Square Sequences

There are several kinds of cyclotomic sequences. They have a number of good randomness properties\(^{[6,7]}\). Binary Legendre sequences are just cyclotomic sequences of order 2 with respect to \( p \). The prime-square sequences\(^{[4,5]}\) and modified prime-square sequences also can be described by using the cyclotomic classes of order 2 with respect to \( p^2 \).

Let \( g \) be a primitive root of \( p^2 \), \( g \) is also a primitive root of \( p \). Define

\[
\begin{align*}
D_0^{(p)} &= (g^2), \\
D_1^{(p)} &= gD_0^{(p)}, \\
D_0^{(p^2)} &= (g^2), \\
D_1^{(p^2)} &= gD_0^{(p^2)},
\end{align*}
\]

where \((g^2)\) denotes the subgroup of \( \mathbb{Z}_p \) and \( \mathbb{Z}_{p^2} \) respectively generated by \( g^2 \). \( D_i^{(p^2)} \) is called the generalized cyclotomic classes of order 2 with respect to \( p^2 \). \( D_i^{(p)} \) is called the cyclotomic classes of order 2 with respect to \( p \). The corresponding generalized cyclotomic numbers of order 2 with respect to \( p^2 \) and cyclotomic numbers of order 2 with respect to \( p \) are defined by

\[
(i,j)^{(p^2)} = |(D_i^{(p^2)} + 1) \cap D_j^{(p^2)}|,
\]

\[
(i,j)^{(p)} = |(D_i^{(p)} + 1) \cap D_j^{(p)}|
\]

for all \( i, j = 0, 1 \).

Define

\[
\begin{align*}
C_0 &= pD_0^{(p)} \cup D_0^{(p^2)}, \\
C_1 &= \{0\} \cup pD_1^{(p)} \cup D_1^{(p^2)}.
\end{align*}
\]

By definition, the order of \( g \) modulo \( p \) is \( p - 1 \), and the order of \( g \) modulo \( p^2 \) is \( p(p - 1) \). Hence,

\[
C_0 \cup C_1 = \mathbb{Z}_{p^2}, \quad C_0 \cap C_1 = \emptyset.
\]

Then the modified prime-square sequence concerned in this paper is a shifted version of the following sequence defined by

\[
s_i = \begin{cases} 0, & \text{if } (i \mod p^2) \in C_0, \\ 1, & \text{if } (i \mod p^2) \in C_1. \end{cases}
\]

So, we need only to determine the randomness properties of this sequence. We have the following results.

3 Linear Complexity and Minimal Polynomial

Let \( s^\infty = s_0 s_1 \cdots s_{l-1} \cdots \) be a sequence of period \( L \) over a field \( F \). The linear complexity of \( s^\infty \) is defined as the least positive integer \( l \) such that there are constants \( c_0 = 1, c_1, \ldots, c_l \in F \) satisfying

\[
-s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_l s_{i-l}, \quad \text{for all } l \leq i < L.
\]

The polynomial \( c(x) = c_0 + c_1 x + \cdots + c_l x^l \) is called a minimal polynomial of \( s^\infty \). The linear complexity and minimal polynomial of periodic sequences can be expressed simply as follows.

Let \( s^\infty \) be a sequence of period \( L \) over a field \( F \), and \( s(x) = s_0 + s_1 x + \cdots + s_{L-1} x^{L-1} \). It is well known that\(^{[8]}\):

1) The minimal polynomial of \( s^\infty \) is given by

\[
c(x) = (x^L - 1)/\gcd(x^L - 1, s(x)).
\]

2) The linear complexity of \( s^\infty \) is given by

\[
C_L = L - \deg(\gcd(x^L - 1, s(x))).
\]

Define \( P_0 = pD_0^{(p)}, P_1 = pD_1^{(p)}, D_0 = D_0^{(p^2)}, \) and \( D_1 = D_1^{(p^2)} \). Let \( m \) be the order of 2 modulo \( p^2 \), then there is a primitive \( p^2 \)-th root of unity \( \theta \) over \( F_{2^m} \). Define

\[
s(x) = \sum_{i \in \mathbb{F}_1} x^i
\]

\[
= 1 + \sum_{i \in P_1} x^i + \sum_{i \in D_1} x^i \in F_2[x].
\]

By (10), we now compute \( \gcd(x^{p^2} - 1, s(x)) \). Note that

\[
0 = \theta^{p^2} - 1 = (\theta^p)^p - 1
\]

\[
= (\theta^{p - 1})(1 + \theta^p + \theta^{2p} + \cdots + \theta^{(p - 1)p}).
\]

It follows that

\[
1 + \theta^p + \theta^{2p} + \cdots + \theta^{(p - 1)p} = \sum_{i \in R} \theta^i = 0.
\]

Since

\[
\left( \sum_{i \in R} + \sum_{i \in D_0} + \sum_{i \in D_1} \right) \theta^i = \sum_{i = 0}^{p^2 - 1} \theta^i = 0,
\]

by (13) we obtain

\[
\sum_{i \in D_0} \theta^i = \sum_{i \in D_1} \theta^i.
\]

Let \( \eta = \theta^p \) be a primitive \( p \)-th root of unity over the field \( F_{2^r} \) that is the splitting field of \( x^p - 1 \). Define \( t(\eta) = \sum_{i \in D_1^\infty} \eta^i \).

Lemma 1. Let the symbols be the same as before:

\[
s(\theta^a) = \begin{cases} s(\theta), & a \in D_0, \\ s(\theta + 1), & a \in D_1. \end{cases}
\]

Proof. If \( a \in D_0 \), by definition, there is an integer \( s \) and \( a = g^{2s} \). It follows that

\[
aD_1 = \{ g^{2s + 2t + 1} : t = 0, 1, \ldots, p(p - 1) - 1 \} = D_1,
\]

\[
aP_1 = p\{ g^{2s + 2t + 1} : t = 0, 1, \ldots, p - 1 \} = P_1.
\]