International Symposium on Information Theory and its Applications, ISITA2006
Seoul, Korea, October 29–November 1, 2006

On the Relationship of Sidel'nikov Sequences

Tae-Hyung Lim†, Young-Sik Kim†, Jung-Soo Chung†, and Jong-Seon No†

† School of Electrical Engineering and Computer Science,
Seoul National University
Seoul 151-744, Korea
E-mail: {jayel, kingsi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr

Abstract

In this paper, the relationship among M-ary Sidel'nikov sequences generated by different primitive elements and decimation are studied. Their autocorrelation function and autocorrelation distribution are derived. It is proved that Sidel'nikov sequences for a given period are equivalent under the decimation, cyclic shift, and scalar multiplication of the sequence.

1. INTRODUCTION

For the high-speed data communications, which usually use M-ary modulation schemes as a transmission standard, it becomes more important to fine M-ary codes with good error correctability and M-ary sequence with good correlation property.

For a prime p, positive integers n and M such that $M|p^n-1$, Sidel'nikov introduced M-ary sequences of period p^n-1. The out-of-phase autocorrelation magnitudes of the Sidel'nikov sequences are upper bounded by 4 [1]–[4].

In this paper, the relationship among M-ary Sidel'nikov sequences generated by different primitive elements and decimation are studied. Their autocorrelation function and autocorrelation distribution are derived. It is proved that Sidel'nikov sequences for a given period are equivalent under the decimation, cyclic shift, and scalar multiplication of the sequence.

2. PRELIMINARIES

Let $s(t)$ be an M-ary sequence of period N and ω_M a complex M-th root of unity, $\omega_M = e^{j\frac{2\pi}{M}}$. The autocorrelation function of $s(t)$ is defined as

$$R(\tau) = \sum_{t=0}^{N-1} \omega_M^{s(t)-s(t+\tau)}$$

where $0 \le \tau \le N-1$.

Sidel'nikov [1] introduced M-ary sequences as follows.

Definition 1 Let p be a prime and α a primitive element of the finite field F_{p^n} with p^n elements. Let $Mf = p^n - 1$. Let $\mathcal{S}_k$, $k = 0, 1, \cdots, M-1$, be the disjoint subsets of F_{p^n} defined as

$$\mathcal{S}_k = \{\alpha^{Mi+k} - 1 \mid 0 \le i \le f-1\}.$$

The M-ary Sidel'nikov sequence $s_o(t)$ of period p^n-1 is defined as

$$s_o(t) = \begin{cases} k, & \text{if } \alpha^t \in \mathcal{S}_k, 0 \le k \le M-1 \\ k_0, & \text{if } t = \frac{p^n-1}{2} \end{cases}$$

where k_0 is some integer modulo M. □

Note that $\alpha^{\frac{p^n-1}{2}} = -1$, $\bigcup_{k=0}^{M-1} \mathcal{S}_k = F_{p^n} \backslash \{-1\}$, and $0 \in \mathcal{S}_0$. It is clear that the M-ary Sidel'nikov sequences with $k_0 = 0$ are balanced.

We can represent the M-ary Sidel'nikov sequences using the indicator function and the multiplicative character of F_{p^n}.

Definition 2 The indicator function is defined as

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \ne 0. \end{cases}$$

□

And the multiplicative character is defined as follows [5].

Definition 3 A multiplicative character of order M of F_{p^n} is defined as

$$\psi_M(\alpha^t) = e^{j\frac{2\pi t}{M}}, \quad \text{if } \alpha^t \in F_{p^n}^*$$

and $\psi_M(0) = 0$, where α is a primitive element of F_{p^n}, $M|p^n-1$, and $0 \le t \le p^n-2$. □

This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Lab. of Excellency.

Then the M-ary Sidel'nikov sequence can be expressed as

$$\omega_M^{s_o(t)} = \omega_M^{k_0} I(\alpha^t + 1) + \psi_M(\alpha^t + 1).$$

We can also represent the M-ary Sidel'nikov sequences using the indicator function and the index function of F_{p^n}. Index function is defined as follows.

Definition 4 If x is a nonzero element of F_{p^n}, then the unique integer i such that

$$x = \alpha^i, \quad 0 \le i \le p^n - 2$$

is called the *index* of x with respect to the primitive element α, and is denoted by $\mathrm{ind}_\alpha x$. □

Indices play a role similar to logarithms. Then the M-ary Sidel'nikov sequence can be expressed as

$$s_o(t) = k_0 I(\alpha^t + 1) + \mathrm{ind}_\alpha(\alpha^t + 1)\bar{I}(\alpha^t + 1) \qquad (1)$$

where $\bar{I}(x) = 1 - I(x)$.

Let M be an integer with $M > 1$ and let $p^n = Mf+1$. Then cyclotomic numbers are defined as below.

Definition 5 The cyclotomic classes C_i, $0 \le i \le M - 1$, in F_{p^n} are defined as

$$C_i = \{\alpha^{Ms+i} | s = 0, 1, \cdots, f - 1\}.$$

For fixed positive integers u and v, not necessarily distinct, the cyclotomic number $(u, v)_M$ is defined as the number of elements $z_u \in C_u$ such that $1 + z_u \in C_v$. □

The elementary relationships between the cyclotomic numbers can be found in [6] and [7].

3. PROPERTIES OF THE SIDEL'NIKOV SEQUENCES

In this section, we investigate the relationship among those sequences. We first consider the generation of sequences by changing primitive element and decimation.

3.1. Changing Primitive Elements and Decimation

The relationship among M-ary Sidel'nikov sequences generated by different primitive elements and decimation are considered. It means that α is replaced by α^c such that $(c, p^n - 1) = 1$ in Definition 1. Then Definition 1 can be changed as follows.

Let $M|p^n - 1$ and $p^n - 1 = Mf$. Then we can construct Sidel'nikov sequences $s_o(t)$ by using Definition 1. If we replace α by α^c, the definition of $\mathcal{S}_k$ is changed as follows.

$$\mathcal{S}'_k = \{\alpha^{cMi+ck} - 1 \mid 0 \le i \le f - 1\}.$$

M-ary Sidel'nikov sequence generated by changing primitive elements is given as

$$s^{(c)}(t) = \begin{cases} k, & \text{if } \alpha^{ct} \in \mathcal{S}'_k, 0 \le k \le M-1 \\ k_0, & \text{if } ct = \frac{p^n-1}{2} \end{cases}$$

where k_0 is some integer modulo M. From the definition of Sidel'nikov sequences, $s^{(c)}(t)$ is also Sidel'nikov sequence. But $s^{(c)}(t)$ shows different properties from the original sequence $s_o(t)$. Later, we look into the relationship among those sequences.

Next, we consider the Sidel'nikov sequences generated by decimation, which is denoted by $s(dt)$. In this paper, we use the decimation factor d such that $(d, p^n - 1) = 1$. It doesn't change the definition of $\mathcal{S}_k$. But the construction method of sequences can be modified as

$$s(dt) = \begin{cases} k, & \text{if } \alpha^{dt} \in \mathcal{S}_k, 0 \le k \le M-1 \\ k_0, & \text{if } dt = \frac{p^n-1}{2} \end{cases}$$

where k_0 is some integer modulo M. Definition of $s(dt)$ is different from that of Sidel'nikov sequences. Therefore, it cannot be considered as a Sidel'nikov sequence.

Now we consider both changing primitive element and decimation. Let $s(t)$ be the sequence decimated by d and replaced by α^c from Sidel'nikov sequence $u(t)$. A sequence $s(t)$ can be represented as

$$\omega_M^{s(t)} = \omega_M^{k_0} I(\alpha^{cdt} + 1) + \psi_M^{c^{-1}}(\alpha^{cdt} + 1). \qquad (2)$$

3.2. Autocorrelation Function

In this section, we look into the autocorrelation function of the sequences defined in (2). Using the properties of the character, the autocorrelation function can be derived as in the following theorem [4].

Theorem 6 Let $s(t)$ be the sequence defined in (2). Then the nontrivial (that is, $\tau \not\equiv 0 \bmod q-1$) autocorrelation function of $s(t)$ is given as

$$R(\tau) = \omega_M^{k_0} \overline{\psi}_M^{c^{-1}}(1 - \alpha^{cd\tau}) + \omega_M^{-k_0} \psi_M^{c^{-1}}(1 - \alpha^{-cd\tau}) - \psi_M^{c^{-1}}(\alpha^{-cd\tau}) - 1.$$

□

According to the above theorem, we know that the sequence defined in (2) has the out-of-phase autocorrelation magnitudes of which are upper bounded by 4 as Sidel'nikov sequences.