On the Linear Complexity Over F_p of M-ary Sidel'nikov Sequences

Young-Sik Kim, Jung-Soo Chung, and Jong-Seon No
School of Electrical Engineering and Computer Science,
Seoul National University,
Seoul 151-744, Korea
Email: {kingsi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
School of Electronics and Electrical Engineering,
Hong-Ik University,
Seoul 121-791, Korea
Email: habchung@hongik.ac.kr

***Abstract*— In this paper, we derive linear complexity over F_p of the M-ary Sidel'nikov sequences using discrete Fourier transform. As an example, we represent the linear complexity of the ternary Sidel'nikov sequences. It turned out that the ternary Sidel'nikov sequences have the linear complexity nearly close to their periods.**

I. Introduction

Linear complexity of a sequences is one of the important properties of the sequences used in the secure communication and cryptography. A sequence having a large linear complexity implies the difficulty in the analysis of the sequence.

For a positive integer m such that $M|p^m-1$, Sidel'nikov [8] constructed M-ary sequences (called *Sidel'nikov sequences*) of period p^m-1, the out-of-phase autocorrelation magnitude of which is upper bounded by 4 [8]. Later, Lempel, Cohn, and Eastman [7] independently introduced the binary Sidel'nikov sequences of period p^m-1. These binary sequences have near-ideal autocorrelation property which, under the condition of balancedness, is optimal.

Helleseth and Yang [5] studied the linear complexity over F_2 of the binary Sidel'nikov sequences. And Kyureghyan and Pott [6] extended their results using cyclotomic numbers. But these results are limited only to some special cases.

There is another approach to the study of the linear complexity of the binary Sidel'nikov sequences. Since Sidel'nikov sequences are constructed based on the finite field F_{p^m}, Helleseth, Kim, and No [3] introduced the linear complexity over F_p of the binary Sidel'nikov sequences. But they showed only for small primes p such as $p = 3, 5$, and 7. Recently, Helleseth, Maas, Mathiassen, and Segers [4] derived the linear complexity over F_p of the binary Sidel'nikov sequences for a general prime p.

In this paper, we derive the linear complexity over F_p of the M-ary Sidel'nikov sequences using discrete Fourier transform. As an example, we represent the linear complexity of the ternary Sidel'nikov sequences. It turned out that the ternary Sidel'nikov sequences have the linear complexity nearly close to their periods.

II. Preliminaries

For a sequence $s(t)$ of period $n = p^m - 1$, the discrete Fourier transform is given by

$$A_i = \frac{1}{n}\sum_{t=0}^{n-1} s(t)\alpha^{-it}$$

and its inverse Fourier transform is given by

$$s(t) = \sum_{i=0}^{n-1} A_i \alpha^{it}$$

where α is a primitive element of the finite field F_{p^m}.

The M-ary Sidel'nikov sequence is defined as follows:

Definition 1: Let α be a primitive element of F_{p^m}. For $k = 0, 1, \cdots, M-1$, define

$$S_k = \left\{ \alpha^{Ml+k} - 1 \;\middle|\; 0 \le l \le \frac{p^m-1}{M} - 1 \right\}.$$

Then M-ary Sidel'nikov sequence $s(t)$ is defined as follows

$$s(t) = \begin{cases} k, & \alpha^t \in S_k, \\ k_0, & \alpha^t = -1. \end{cases}$$

□

When $k_0 = 0$, the Sidel'nikov sequence is balanced. In the following discussion, we will only consider the case of $k_0 = 0$.

The following theorem shows some combinatorial relation between a number and its p-adic expansion.

Theorem 2: [Lucas' Theorem] [1] If p is a prime and $N = \sum_{i=0}^{I} N_i p^i$, $0 \le N_i < p$, $K = \sum_{i=0}^{I} K_i p^i$, $0 \le K_i < p$, then

$$\binom{N}{K} \equiv \prod_{i=0}^{I} \binom{N_i}{K_i} \bmod p. \tag{1}$$

□

In this paper, we will call each $\binom{N_i}{K_i}$ in (1) by a Lucas factor of $\binom{N}{K}$.

III. Linear Complexity of M-ary Sidel'nikov Sequences

From the Blahut's theorem, the linear complexity of periodic sequences can be determined by computing the Hamming weight of their Fourier transform.

We will compute the Fourier transform of M-ary Sidel'nikov sequences for a general alphabet size M.

Theorem 3: Let $L = \frac{p^m-1}{M}$, $n = p^m - 1$, and $p > M$. For $k_0 = 0$, the Fourier transform of an M-ary Sidel'nikov sequence is derived as

$$nA_{-i} = \frac{n(M-1)}{2}(-1)^i - n(-1)^i \sum_{v=1}^{M-1} \frac{B_v(i)}{1-\alpha^{vL}}$$

where $B_v(i) = \binom{i}{vL}(-1)^{-vL}$.

Proof: By Definition 1, Fourier transform of $s(t)$ is written as

$$\begin{aligned} nA_{-i} &= \sum_{t=0}^{n-1} s(t)\alpha^{it} \\ &= k_0(-1)^i + \sum_{\alpha^t \in S_0 \setminus \{0\}} 0 \cdot \alpha^{it} + \sum_{\alpha^t \in S_1} \alpha^{it} \\ &\quad + \cdots + \sum_{\alpha^t \in S_{M-1}} (M-1)\alpha^{it}. \end{aligned}$$

Since $k_0 = 0$, we have

$$\begin{aligned} nA_{-i} &= \sum_{u=1}^{M-1}\sum_{l=0}^{L-1} u(\alpha^{Ml+u} - 1)^i \\ &= \sum_{u=1}^{M-1} u \sum_{l=0}^{L-1}\sum_{r=0}^{i} \binom{i}{r}(-1)^{i-r}\alpha^{(Ml+u)r} \\ &= \sum_{u=1}^{M-1} u \sum_{r=0}^{i} \binom{i}{r}(-1)^{i-r}\alpha^{ur} \sum_{l=0}^{L-1} \alpha^{Mlr}. \end{aligned}$$

The innermost summation $\sum_{l=0}^{L-1} \alpha^{Mlr}$ is equal to L for $r = 0, L, \cdots, (M-1)L$, and it is equal to zero, otherwise. Therefore, we have

$$\begin{aligned} nA_{-i} &= \sum_{v=0}^{M-1}\sum_{u=1}^{M-1} Lu\binom{i}{vL}(-1)^{i-vL}\alpha^{uvL} \\ &= \sum_{v=0}^{M-1} L\binom{i}{vL}(-1)^{i-vL} \sum_{u=1}^{M-1} u\alpha^{uvL}. \end{aligned}$$

When $v = 0$, we have

$$\sum_{u=1}^{M-1} \frac{un}{M}\binom{i}{0}(-1)^i = \frac{n}{M}(-1)^i \sum_{u=1}^{M-1} u = \frac{n(M-1)}{2}(-1)^i.$$

Thus we have

$$\begin{aligned} nA_{-i} =& \frac{n(M-1)}{2}(-1)^i \\ &+ \sum_{v=1}^{M-1} L\binom{i}{vL}(-1)^{i-vL} \sum_{u=1}^{M-1} u\alpha^{uvL}. \end{aligned}$$

Since

$$\sum_{u=1}^{M-1} u\alpha^{uvL} = \frac{-M}{1-\alpha^{vL}}, \quad \text{for } 1 \le v \le M-1,$$

we have

$$\begin{aligned} nA_{-i} &= \frac{n(M-1)}{2}(-1)^i - M\sum_{v=1}^{M-1} \frac{L\binom{i}{vL}(-1)^{i-vL}}{1-\alpha^{vL}} \\ &= \frac{n(M-1)}{2}(-1)^i - n(-1)^i \sum_{v=1}^{M-1} \frac{\binom{i}{vL}(-1)^{-vL}}{1-\alpha^{vL}}. \end{aligned}$$

From $B_v(i) = \binom{i}{vL}(-1)^{-vL}$, we have

$$nA_{-i} = \frac{n(M-1)}{2}(-1)^i - n(-1)^i \sum_{v=1}^{M-1} \frac{B_v(i)}{1-\alpha^{vL}}.$$

□

Theorem 4: Let D be the number of integers i, $0 \le i \le p^m - 2$ satisfying the relation

$$\frac{(M-1)}{2} = \sum_{v=1}^{M-1} \frac{B_v(i)}{1-\alpha^{vL}}.$$

Then the linear complexity over F_p of the M-ary Sidel'nikov sequences of period $n = p^m - 1$ equals

$$L_M = n - D.$$

□

And the following lemma can be used in the calculation of combinations which are included in $B_v(i)$.

Lemma 5: For $p = Md + 1$ and $1 \le j \le d$, we have

$$\binom{(M-1)d-j}{d-j} = \binom{(M-1)d+j}{d+j} \bmod p.$$

Proof: We will show that

$$\frac{d-i}{(M-1)d-i} = \frac{(M-1)d+i+1}{d+i+1} \bmod p. \tag{2}$$

From this equation, we have

$$(d-i)(d+i+1) = ((M-1)d+i+1)((M-1)d-i) \bmod p.$$

The left hand side (LHS) and the right hand side (RHS) are

$$LHS = d^2 + id + d - id - i^2 - i = d^2 + d - i^2 - i$$

$$\begin{aligned} RHS &= (M-1)^2d^2 + (M-1)id + (M-1)d \\ &\quad - (M-1)id - i^2 - i \\ &= Md(Md+1) - 2d(Md+1) \\ &\quad + d^2 + d - i^2 - i \\ &= d^2 + d - i^2 - i \bmod p. \end{aligned}$$

Thus (2) is proved. Since $\binom{(M-1)d-j}{d-j} \bmod p$ and $\binom{(M-1)d+j}{d+j} \bmod p$ are obtained by multiplying $\frac{d-i}{(M-1)d-i}$ and $\frac{(M-1)d+i+1}{d+i+1}$, $i = 0, 1, \cdots, j-1$, to $\binom{(M-1)d}{d} \bmod p$, respectively. Thus we have $\binom{(M-1)d-j}{d-j} = \binom{(M-1)d+j}{d+j} \bmod p$. □

IV. Linear Complexity of Ternary Sidel'nikov Sequences

Let β be a primitive element of F_p. From Theorem 4, we have to count the number of nonzero A_{-i}'s for $M = 3$.

Corollary 6: For $M = 3$, we have

$$3 = \Big(\binom{i}{L} - \binom{i}{2L}\Big)\alpha^L + 2\binom{i}{L} + \binom{i}{2L}. \quad (3)$$

Proof: For $M = 3$, L is even. From Theorem 4, we have

$$\begin{aligned} 1 &= \sum_{v=1}^{2} \frac{B_v(i)}{1-\alpha^{vL}} = \frac{\binom{i}{L}}{1-\alpha^L} + \frac{\binom{i}{2L}}{1-\alpha^{2L}} \\ &= \frac{\binom{i}{L}(1-\alpha^{2L}) + \binom{i}{2L}(1-\alpha^L)}{1-\alpha^L-\alpha^{2L}+\alpha^{3L}}. \end{aligned}$$

Since $1 + \alpha^L + \alpha^{2L} = 0$, we have

$$3 = \Big(\binom{i}{L} - \binom{i}{2L}\Big)\alpha^L + 2\binom{i}{L} + \binom{i}{2L}.$$

□

Then we can obtain the linear complexity of the ternary Sidel'nikov sequences as in the following theorem.

Theorem 7: For $p \equiv 2 \bmod 3$, the linear complexity of ternary Sidel'nikov sequences is given as

$$L_1 = p^m - C_1'$$

where

$$\begin{aligned} C_1' = \sum_{\substack{\sum_{i=2d+1}^{p-1} v_i = \frac{m}{2}, \sum_{i=2d+1}^{p-1} u_i = \frac{m}{2} \\ U=0 \bmod p-1, V=0 \bmod p-1}} \Big[(v_{2d+1}, \cdots, v_{p-1})! \\ \times (u_{2d+1}, \cdots, u_{p-1})!\Big], \end{aligned}$$

$p = 3d + 2$, $\beta^{f_k} = \binom{k}{d} \bmod p$, $\beta^{g_k} = \binom{k}{2d+1} \bmod p$, v_k is the number of $\binom{k}{d}$ among the Lucas factors of $\binom{i}{L}$, u_k is the number of $\binom{k}{2d+1}$ among the Lucas factors of $\binom{i}{L}$, $U = \sum_{i=2d+1}^{p-1}(v_i f_i + u_i g_i)$, and $V = \sum_{i=2d+1}^{p-1}(v_i g_i + u_i f_i)$.

Proof: There are three cases.

Case 1. $0 \le i < L$

In this case, $\binom{i}{L} = 0$ and $\binom{i}{2L} = 0$. Then (3) cannot be achieved. Therefore, $A_{-i} \neq 0$ for all i, $0 \le i < L$.

Case 2. $L \le i < 2L$

In this case, $\binom{i}{2L} = 0$. Then we have

$$\binom{i}{L}\alpha^L = 3 - 2\binom{i}{L}. \quad (4)$$

Since $p \equiv 2 \bmod 3$, we have $(\alpha^L)^{p-1} \neq 1$. Therefore, $\alpha^L \notin F_p$. In (4), while left hand side is not an element of F_p, right hand side is an element of F_p. It is a contradiction. Therefore, $A_{-i} \neq 0$.

Case 3. $2L \le i < 3L$

In this case, from (3), if $\binom{i}{L} - \binom{i}{2L} \neq 0$, $A_{-i} \neq 0$ since $\alpha^L \notin F_p$ but $\binom{i}{L}$ and $\binom{i}{2L}$ are elements of F_p. If $\binom{i}{L} - \binom{i}{2L} = 0$, we have $\binom{i}{L} = \binom{i}{2L} = 1 \bmod p$.

In order to apply Lucas Theorem, we need to expand L as follows

$$L = \frac{p^m - 1}{3} = \frac{p^2 - 1}{3}(p^{m-2} + p^{m-4} + \cdots + 1).$$

Since $p = 3d + 2$, we have

$$\frac{p^2-1}{3} = 3d^2 + 4d + 1 = d(3d+2) + 2d + 1 = dp + (2d+1).$$

Then we have

$$\begin{aligned} L =& dp^{m-1} + (2d+1)p^{m-2} + dp^{m-3} + (2d+1)p^{m-4} \\ &+ \cdots + dp + (2d+1). \end{aligned}$$

Let $i = \sum_{a=0}^{m-1} i_a p^a$. By Lucas theorem, we have

$$\begin{aligned} \binom{i}{L} &= \binom{i_{m-1}}{d}\binom{i_{m-2}}{2d+1}\cdots\binom{i_1}{d}\binom{i_0}{2d+1} \\ &= 1 \bmod p. \end{aligned} \quad (5)$$

Similarly,

$$\begin{aligned} 2L =& (2d+1)p^{m-1} + dp^{m-2} + (2d+1)p^{m-3} + dp^{m-4} \\ &+ \cdots + (2d+1)p + d. \end{aligned}$$

Then we have

$$\begin{aligned} \binom{i}{2L} =& \binom{i_{m-1}}{2d+1}\binom{i_{m-2}}{d}\cdots\binom{i_1}{2d+1}\binom{i_0}{d} \\ =& 1 \bmod p. \end{aligned} \quad (6)$$

Since β is a primitive element of F_p, $\beta^{f_k} = \binom{k}{d} \bmod p$, and $\beta^{g_k} = \binom{k}{2d+1} \bmod p$, we can represent (5) and (6) as follows

$$\binom{i}{L} = \beta^{f_{i_{m-1}}}\beta^{g_{i_{m-2}}}\cdots\beta^{f_{i_1}}\beta^{g_{i_0}} = \beta^0 \bmod p \quad (7)$$

$$\binom{i}{2L} = \beta^{g_{i_{m-1}}}\beta^{f_{i_{m-2}}}\cdots\beta^{g_{i_1}}\beta^{f_{i_0}} = \beta^0 \bmod p. \quad (8)$$

Since v_k is the number of $\binom{k}{d}$ among the factors of $\binom{i}{L}$ in (5) and u_k is the number of $\binom{k}{2d+1}$ among the factors of $\binom{i}{L}$ in (6), we have $\sum_{i=2d+1}^{p-1} v_i = \frac{m}{2}$ and $\sum_{i=2d+1}^{p-1} u_i = \frac{m}{2}$. Since all of the Lucas factors of $\binom{i}{L}$ and $\binom{i}{2L}$ are not equal to zero, from (7) and (8), we have $U = \sum_{i=2d+1}^{p-1}(v_i f_i + u_i g_i) \equiv 0 \bmod p-1$ and $V = \sum_{i=2d+1}^{p-1}(v_i g_i + u_i f_i) \equiv 0 \bmod p-1$.

To count the number of i satisfying $\binom{i}{L} = 1$ and $\binom{i}{2L} = 1$, we have to count the number of selection of v_j and u_j, $2d+1 \le j \le p-1$, in (7) and (8). This can be done by the following multinomial

$$\begin{aligned} C_1' = \sum_{\substack{\sum_{i=2d+1}^{p-1} v_i = \frac{m}{2}, \sum_{i=2d+1}^{p-1} u_i = \frac{m}{2} \\ U=0 \bmod p-1, V=0 \bmod p-1}} \Big[(v_{2d+1}, \cdots, v_{p-1})! \\ \times (u_{2d+1}, \cdots, u_{p-1})!\Big] \end{aligned}$$

where

$$(v_{2d+1}, \cdots, v_{p-1})! = \frac{(v_{2d+1} + \cdots + v_{p-1})!}{(v_{2d+1})! \cdots (v_{p-1})!}.$$

We must rule out the case, $i_m = \cdots = i_0 = p-1$. Then the linear complexity of ternary Sidel'nikov sequences is given as

$$L_1 = p^m - C_1'.$$

□

Example 8: For $M = 3$, m is even for $p \equiv 2 \bmod 3$. For $p = 5$ and $\beta = 3$, we have

$$v_3 f_3 + v_4 f_4 + u_3 g_3 + u_4 g_4 = 0 \bmod 4$$
$$v_3 g_3 + v_4 g_4 + u_3 f_3 + u_4 f_4 = 0 \bmod 4.$$

Since $f_3 = 1$, $f_4 = 2$, $g_3 = 0$, and $g_4 = 2$,

$$v_3 + 2v_4 + 2u_4 = 0 \bmod 4$$
$$2v_4 + u_3 + 2u_4 = 0 \bmod 4.$$

Therefore, v_3 and u_3 are multiples of 4 and $v_4 + u_4$ is a multiple of 2. And $v_3 + v_4 = \frac{m}{2}$ and $u_3 + u_4 = \frac{m}{2}$. Then the linear complexity of ternary Sidel'nikov sequences is written as

$$\begin{aligned} L_1 &= p^m - \sum_{\substack{v_3+v_4=\frac{m}{2}, u_3+u_4=\frac{m}{2} \\ v_3+2v_4+2u_4=0 \bmod 4, \\ 2v_4+u_3+2u_4=0 \bmod 4}} (v_3, v_4)!(u_3, u_4)! \\ &= p^m - \left\{ \sum_{j=0}^{\lfloor \frac{m}{8} \rfloor} \binom{\frac{m}{2}}{4j} \right\}^2. \end{aligned}$$

□

From Lemma 5, we can easily obtain the following corollary.

Corollary 9: For $p = 3d+1$ and $1 \le j \le d$, we have

$$\binom{2d-j}{d} = \binom{2d+j}{d} \bmod p.$$

□

Lemma 10: For $p \equiv 1 \bmod 3$ and $L \le i < 3L$, the number of i satisfying $\binom{i}{2L} = 0$ and $\binom{i}{L} = \frac{3}{\gamma+2} \bmod p$ is given as

$$E(d) - E(2d)$$

where

$$E(k) = \sum_{\substack{\sum_{j=k}^{p-1} v_j = m \\ \sum_{j=k}^{p-1} v_j f_j = f' \bmod p-1}} (v_k, \cdots, v_{p-1})!,$$

$\gamma = \alpha^L$, $\beta^{f'} = \frac{3}{\gamma+2}$, $\binom{k}{d} = \beta^{f_k}$, and v_k is the number of $\binom{k}{d}$ among the Lucas factors of $\binom{i}{L}$.

Proof: By Lucas theorem, we have

$$\binom{i}{L} = \prod_{a=0}^{m-1} \binom{i_a}{d} = \beta^{f_{i_0}} \beta^{f_{i_1}} \cdots \beta^{f_{i_{m-1}}} = \beta^{f'} \bmod p.$$

Since v_k is the number of $\binom{k}{d}$ among the Lucas factors of $\binom{i}{L}$, we have

$$v_d + \cdots + v_{p-1} = m.$$

Then we have

$$E(d) = \sum_{\substack{\sum_{j=d}^{p-1} v_j = m \\ \sum_{j=d}^{p-1} v_j f_j = f' \bmod p-1}} (v_d, \cdots, v_{p-1})!.$$

If there exists the case that all i_a, $0 \le a \le m-1$, are equal to $p-1$, then we have $v_{p-1} = m$ and $m f_{p-1} = f' \bmod p-1$. From Lemma 9, we have $\binom{3d}{d} = \binom{d}{d} = 1 \bmod p$. Therefore, $f_{p-1} = 0$. But if $f' = 0 \bmod p-1$, then we have $\frac{3}{\gamma+2} = 1$ and $\gamma = 1$, which is a contradiction since the order of γ is 3. Therefore, there is no case that all i_a, $0 \le a \le m-1$, are equal to $p-1$.

Since $\binom{i}{2L} = 0$, we need to rule out the cases, $\binom{i}{2L} \ne 0$ from $E(d)$. $E(2d)$ is the number of i such that all the coefficients i_a, $0 \le a \le m-1$, of its p-adic expansion are contained in the range $2d \le i_a < p-1$, which corresponds to $\binom{i}{2L} \ne 0$ and $\binom{i}{L} = \frac{3}{\gamma+2} \bmod p$. Thus, we must subtract $E(2d)$ from $E(d)$.

□

Similarly, we can obtain the following lemma.

Lemma 11: For $p \equiv 1 \bmod 3$ and $2L \le i < 3L$, the number of i satisfying $\binom{i}{L} = c_1 \ne 0$ and $\binom{i}{2L} = c_2 \ne 0$ is given as

$$F_{c_1,c_2} = \sum_{\substack{\sum_{j=2d}^{p-1} v_j f_j = f' \bmod p-1 \\ \sum_{j=2d}^{p-1} v_j g_j = g' \bmod p-1 \\ v_{2d} + \cdots + v_{p-1} = m}} (v_{2d}, \cdots, v_{p-1})!$$

where $c_1 = \beta^{f'}$, $c_2 = \beta^{g'}$, $\binom{k}{d} = \beta^{f_k}$, and $\binom{k}{2d} = \beta^{g_k}$.

□

Theorem 12: For $p \equiv 1 \bmod 3$, the linear complexity of ternary Sidel'nikov sequences is given as

$$L_2 = p^m - E(d) + E(2d) - \sum_{(\gamma+2)c_1 - (\gamma-1)c_2 = 3} F_{c_1,c_2}.$$

Proof: Since $(\alpha^L)^{p-1} = (\alpha^d)^{p^m-1} = 1$, $\alpha^L \in F_p$. Let $\alpha^L = \gamma$. Then γ is an element of F_p with order 3. Equation (3) can be represented as

$$3 = (\gamma+2)\binom{i}{L} - (\gamma-1)\binom{i}{2L}. \tag{9}$$

There are two cases.

Case 1) $0 \le i < L$

Since $\binom{i}{L} = 0$ and $\binom{i}{2L} = 0$, (9) cannot be achieved.

Case 2) $L \le i < 3L$

There are two cases satisfying (9):

(a) $\binom{i}{2L} = 0$ and $\binom{i}{L} = \frac{3}{\gamma+2} \bmod p$.

(b) $\binom{i}{L} = c_1$ and $\binom{i}{2L} = c_2$.

In this case, c_1 and c_2 have the same order. Then $c_1 = 1$ and $c_2 = 1$ are always valid. When $i_a = p-1$, $0 \le a \le p-1$, from Corollary 9, we have $f_{p-1} = 0$, $g_{p-1} = 0$, and $v_{p-1} = m$. Thus $F_{1,1}$ contains the case for $i_a = p-1$, $0 \le a \le p-1$.

From Lemma 10, we have the number of i satisfying (a). And from Lemma 11, we also have the number of i satisfying

(b). And we must remove the case when all i_a's are equal to $p-1$.

Therefore, the linear complexity of ternary Sidel'nikov sequences for $p \equiv 1 \bmod 3$ is given as

$$L_2 = p^m - E(d) + E(2d) - \sum_{(\gamma+2)c_1-(\gamma-1)c_2=3} F_{c_1,c_2}.$$

□

Example 13: For $p=7$, $\beta=3$, and $\gamma=2$, we have

$$f_2=0, f_3=1, f_4=3, f_5=1, f_6=0$$
$$g_4=0, g_5=5, g_6=0.$$

Then we have

$$E(d) = \sum_{\substack{v_2+\cdots+v6=m \\ v_3+3v_4+v_5=3 \bmod 6}} (v_2,\cdots,v_6)!$$

and

$$E(2d) = \sum_{\substack{v_4+v_5+v_6=m \\ 3v_4+v_5=3 \bmod 6}} (v_4,v_5,v_6)!.$$

We can calculate the numbers c_1 and c_2 satisfying (9) and having the same order. As a result, we have $(c_1,c_2)=(1,1)$ and $(5,3)$. Then we have

$$F_{1,1} = \sum_{\substack{v_4+v_5+v_6=m \\ 3v_4+v_5=0 \bmod 6, 5v_5=0 \bmod 6}} (v_4,v_5,v_6)!$$

and

$$F_{5,3} = \sum_{\substack{v_4+v_5+v_6=m \\ 3v_4+v_5=5 \bmod 6, 5v_5=1 \bmod 6}} (v_4,v_5,v_6)!.$$

Finally, we have

$$L_2 = p^m - E(d) + E(2d) - F_{1,1} - F_{5,3}.$$

TABLE I

LINEAR COMPLEXITIES OF TERNARY SIDEL'NIKOV SEQUENCES FOR $p=7$

m	Period	$\gamma=2$	$\gamma=4$
3	342	325	315
4	2400	2344	2346
5	16806	16727	16692

Table I lists the linear complexities of some ternary Sidel'nikov sequences for $p=7$. □

ACKNOWLEDGMENT

This work was supported by University IT Research Center Project.

REFERENCES

[1] Elwyn R. Berlekamp, *Algebraic Coding Theory*, revised ed., Laguna Hills, CA: Aegean Park Press, 1987.

[2] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Devel.*, vol. 63, pp. 550–560, 1979.

[3] Tor Helleseth, Sang-Hyo Kim, and Jong-Seon No, "Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Inform. Theory*, vol. 49, no. 6, pp. 1548–1552, June 2003.

[4] Tor Helleseth, Martijn Maas, John Erik Mathiassen, and Toon Segers, "Linear compelxity over F_p of Sidel'nikov sequences," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2468–2472, Oct. 2004.

[5] T. Helleseth and K. Yang, "On binary sequences of period $n=p^m-1$ with optimal autocorrelation," in *Proc. 2001 Conf. SETA 2001*, 2001, pp. 29-30.

[6] Gohar M. Kyureghyan and Alexander Pott, "On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Design, Codes and Cryptography*, vol. 29, pp. 149–164, 2003.

[7] A. Lempel, M. Cohn, and W. L. Eastman, "A Class of Balanced Binary Sequences with Optimal Autocorrelation Properties," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 38–42, Jan. 1977.

[8] V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12–16, 1969.