Linear Complexity over F_p of Ternary Sidel'nikov Sequences*

Young-Sik Kim[1], Jung-Soo Chung[1], Jong-Seon No[1], and Habong Chung[2]

[1] School of Electrical Engineering and Computer Science and INMC, Seoul National University, Seoul 151-744, Korea
{kingsi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr
[2] School of Electronics and Electrical Engineering, Hongik University, Seoul 121-791, Korea
habchung@hongik.ac.kr

Abstract. In this paper, for positive integers m, M, and a prime p such that $M|p^m - 1$, we derive linear complexity over the prime field F_p of M-ary Sidel'nikov sequences of period $p^m - 1$ using discrete Fourier transform. As a special case, the linear complexity of the ternary Sidel'nikov sequence is presented. It turns out that the linear complexity of a ternary Sidel'nikov sequence with the symbol $k_0 \neq 1$ at the $(p^m - 1)/2$-th position is nearly close to the period of the sequence, while that with $k_0 = 1$ shows much lower value.

1 Introduction

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

For positive integers m, M, and a prime p, such that $M|p^m - 1$, Sidel'nikov [9] 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 [9]. Later, Lempel, Cohn, and Eastman [8] independently rediscovered 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 [7] extended their results using cyclotomic numbers. But these results are limited only to some special cases.

There has been 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,

* 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 Laboratory of Excellency.

G. Gong et al. (Eds.): SETA 2006, LNCS 4086, pp. 61–73, 2006.

and Segers [4] derived the linear complexity over the prime field F_p of the binary Sidel'nikov sequences for a prime p. For the balanced Sidel'nikov sequences, Kim, Chung, No, and Chung present the linear complexity over F_p of M-ary Sidel'nikov sequences using discrete Fourier transform [6].

In this paper, the derivation [6] of the linear complexity over F_p of M-ary Sidel'nikov sequences is extended to the general case including unbalanced sequences. It turns out that the linear complexity of a ternary Sidel'nikov sequence with the symbol $k_0 \neq 1$ at the $(p^m-1)/2$-th position is nearly close to the period of the sequence, while that with $k_0 = 1$ shows much lower value.

2 Preliminaries

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

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

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

where α is a primitive element of the finite field F_{p^m} with p^m elements. An M-ary sequence $s(t)$ of period n, $M|n$, is said to be balanced if each element occurs exactly n/M times in a period.

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

Definition 1. Let m and M be positive integers, and p a prime such that $M|p^m - 1$. 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 the M-ary Sidel'nikov sequence $s(t)$ is defined as

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

□

When $k_0 = 0$, the Sidel'nikov sequence is balanced. The following theorem shows some combinatorial relation between a number and its p-ary expansion.

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

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

□

In this paper, we will call $\binom{N_i}{K_i}$ Lucas factor of $\binom{N}{K}$.

3 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, that is, the number of nonzero values of their Fourier transform.

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

Theorem 2. Let $L = (p^m - 1)/M$, $n = p^m - 1$, and $p > M$. The Fourier transform of an M-ary Sidel'nikov sequence is derived as

$$A_{-i} \equiv \Big(\frac{(M-1)}{2} - k_0\Big)(-1)^i - (-1)^i \sum_{v=1}^{M-1} \frac{B_v(i)(-1)^{-vL}}{1-\alpha^{vL}} \bmod p \qquad (1)$$

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

Proof. From Definition 1, the Fourier transform of $s(t)$ is written as

$$\begin{aligned} nA_{-i} &= k_0(-1)^i + \sum_{\alpha^t \in S_0 \setminus \{0\}} 0 \cdot \alpha^{it} + \sum_{\alpha^t \in S_1} \alpha^{it} + \cdots + \sum_{\alpha^t \in S_{M-1}} (M-1)\alpha^{it} \\ &= k_0(-1)^i + \sum_{u=1}^{M-1} \sum_{l=0}^{L-1} u(\alpha^{Ml+u} - 1)^i \\ &= k_0(-1)^i + \sum_{u=1}^{M-1} u \sum_{l=0}^{L-1} \sum_{r=0}^{i} \binom{i}{r} (-1)^{i-r} \alpha^{(Ml+u)r} \\ &= k_0(-1)^i + \sum_{u=1}^{M-1} \sum_{r=0}^{i} u \binom{i}{r} (-1)^{i-r} \alpha^{ur} \sum_{l=0}^{L-1} \alpha^{Mlr}. \end{aligned}$$

The innermost sum is equal to L for $r = 0, L, \cdots, (M-1)L$, and is equal to zero, otherwise. Therefore, we have

$$\begin{aligned} nA_{-i} &= k_0(-1)^i + \sum_{v=0}^{M-1} \sum_{u=1}^{M-1} Lu \binom{i}{vL} (-1)^{i-vL} \alpha^{uvL} \\ &= k_0(-1)^i + \sum_{v=0}^{M-1} L \binom{i}{vL} (-1)^{i-vL} \sum_{u=1}^{M-1} u\alpha^{uvL}. \end{aligned}$$

For $v = 0$ in the above summation, we have

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

and thus

$$nA_{-i} = k_0(-1)^i + \frac{n(M-1)}{2}(-1)^i + \sum_{v=1}^{M-1} L \binom{i}{vL} (-1)^{i-vL} \sum_{u=1}^{M-1} u\alpha^{uvL}. \qquad (2)$$

We can modify the inner sum in the last term of (2) as

$$\sum_{u=1}^{M-1} u\alpha^{uvL} = \frac{1}{1-\alpha^{vL}}\left(\sum_{u=1}^{M-1}\alpha^{uvL} - (M-1)\alpha^{vLM}\right) = \frac{-M}{1-\alpha^{vL}}. \tag{3}$$

Applying (3) to (2) and $n \equiv -1 \bmod p$, we have

$$A_{-i} \equiv \left(\frac{(M-1)}{2} - k_0\right)(-1)^i - (-1)^i \sum_{v=1}^{M-1} \frac{B_v(i)(-1)^{-vL}}{1-\alpha^{vL}} \bmod p$$

where $B_v(i) = \binom{i}{vL}$. □

Let F be number of integers i, $0 \le i < n$, satisfying the relation

$$\frac{(M-1)}{2} - k_0 \equiv \sum_{v=1}^{M-1} \frac{B_v(i)(-1)^{-vL}}{1-\alpha^{vL}} \bmod p, \tag{4}$$

which corresponds to $A_{-i} = 0$ in (1). Then the linear complexity over F_p of the M-ary Sidel'nikov sequences of period n is given as

$$L_M(p) = n - F.$$

In order to compute the linear complexity of M-ary Sidel'nikov sequences, we have to find F in (4). $B_v(i)$ in (4) can be factored into Lucas factors using Lucas' theorem. Since the Lucas factors are integers, they can be represented by the primitive element β of the prime field F_p.

Note that for $0 \le i < vL$, we have $B_v(i) = B_{v+1}(i) = \cdots = B_{M-1}(i) = 0$. Let $b_v = (-1)^{-vL}/(1-\alpha^{vL})$. Note that for $p \equiv 1 \bmod M$, $\alpha^L \in F_p$ because $(\alpha^L)^{p-1} = (\alpha^{\frac{p-1}{M}})^{p^m-1} = 1$. Thus, we also have $b_v \in F_p$.

By dividing the range of i into M subranges, (4) can be separately rewritten as

$$\begin{array}{ll} 0 = \frac{M-1}{2} - k_0, & \text{for } 0 \le i < L \\ b_1 B_1(i) = \frac{M-1}{2} - k_0, & \text{for } L \le i < 2L \\ b_1 B_1(i) + b_2 B_2(i) = \frac{M-1}{2} - k_0, & \text{for } 2L \le i < 3L \\ \vdots & \vdots \\ \sum_{v=1}^{M-1} b_v B_v(i) = \frac{M-1}{2} - k_0, & \text{for } (M-1)L \le i < ML. \end{array} \tag{5}$$

For $1 \le l \le M-1$, let $F_l(c_1, c_2, \cdots, c_l)$ be the number of i, $lL \le i < (l+1)L$, such that $(B_1(i), B_2(i), \cdots, B_l(i)) = (c_1, c_2, \cdots, c_l)$. Then the total number of i satisfying the $(l+1)$-th equation is given as

$$\sum_{b_1c_1 + b_2c_2 + \cdots + b_lc_l = \frac{M-1}{2} - k_0} F_l(c_1, c_2, \cdots, c_l).$$

Let the number of i satisfying the first equation in (5) be denoted by F_0. If $k_0 \neq (M-1)/2$, the solutions for (4) do not exist in the subrange $0 \leq i < L$. And if $k_0 = (M-1)/2$, all i's, $0 \leq i < L$, satisfy (4). That is, we have

$$F_0 = \begin{cases} L, \text{ if } k_0 = \frac{M-1}{2} \\ 0, \text{ otherwise.} \end{cases}$$

Using the above procedure, we can obtain the number of i satisfying (4) as

$$F = F_0 + \sum_{l=1}^{M-1} \sum_{b_1c_1+b_2c_2+\cdots+b_lc_l=\frac{M-1}{2}-k_0} F_l(c_1, c_2, \cdots, c_l),$$

which corresponds to the number of i, $0 \leq i < n$, such that $A_{-i} = 0$. Thus, we have the following theorem.

Theorem 3. The linear complexity over F_p of the M-ary Sidel'nikov sequences of period $n = p^m - 1$ equals

$$L_M(p) = \begin{cases} n - L - \sum\limits_{l=1}^{M-1} \sum\limits_{b_1c_1+b_2c_2+\cdots+b_lc_l=\frac{M-1}{2}-k_0} F_l(c_1, c_2, \cdots, c_l), \text{ for } k_0 = \frac{M-1}{2} \\ n - \sum\limits_{l=1}^{M-1} \sum\limits_{b_1c_1+b_2c_2+\cdots+b_lc_l=\frac{M-1}{2}-k_0} F_l(c_1, c_2, \cdots, c_l), \qquad \text{otherwise.} \end{cases}$$

□

In general, it is not easy to find $F_l(c_1, c_2, \cdots, c_l)$ for M-ary Sidel'nikov sequences. In the next section, we will find the linear complexity for $M = 3$ as a special case.

4 Linear Complexity of Ternary Sidel'nikov Sequences

Let β be a primitive element of F_p. For $M = 3$, we have to count the number of nonzero A_{-i}'s, $0 \leq i < n$ in (4). Note that for $M = 3$, we have $(-1)^L = 1$ and $(\alpha^L)^3 = 1$. Thus, we have

$$(\alpha^L + 2)(1 - \alpha^L) = 3. \tag{6}$$

Lemma 1. For $M = 3$, (5) is written as

$$3(1 - k_0) = \big(B_1(i) - B_2(i)\big)\alpha^L + 2B_1(i) + B_2(i). \tag{7}$$

Proof. From Theorem 3, for $M = 3$, we have

$$1 - k_0 = \sum_{v=1}^{2} \frac{B_v(i)}{1 - \alpha^{vL}} = \frac{B_1(i)}{1 - \alpha^L} + \frac{B_2(i)}{1 - \alpha^{2L}} = \frac{(1 - \alpha^{2L})B_1(i) + (1 - \alpha^L)B_2(i)}{1 - \alpha^L - \alpha^{2L} + \alpha^{3L}}.$$

From $1 + \alpha^L + \alpha^{2L} = 0$, (7) is easily derived. □

Now, we are going to derive the linear complexities of the ternary Sidel'nikov sequences of period $n = p^m - 1$ for $p = 3d+1$ and $p = 3d+2$, as in the following two theorems.

Theorem 4. Let $n = p^m - 1$ and $p = 3d + 2$ be a prime, where d is a positive integer. Let $3|n$. Let $\beta^h = 1 - k_0$ for $k_0 \neq 1$. For $0 \leq k \leq p-1$, let $\beta^{f_k} \equiv \binom{k}{d} \bmod p$, $\beta^{g_k} \equiv \binom{k}{2d+1} \bmod p$, and v_k and u_k be the numbers of $\binom{k}{d}$ and $\binom{k}{2d+1}$ among the Lucas factors of $B_v(i)$, respectively. Let $V_1 = \sum_{k=2d+1}^{p-1}(v_k f_k + u_k g_k)$ and $V_2 = \sum_{k=2d+1}^{p-1}(v_k g_k + u_k f_k)$. Then the linear complexity $L_3(p)$ over F_p of ternary Sidel'nikov sequences of period n is given as

$$L_3(p) = \begin{cases} n - \sum\limits_{\substack{V_1 \equiv h \bmod (p-1) \\ V_2 \equiv h \bmod (p-1)}} \Big[(v_{2d+1}, \cdots, v_{p-1})!(u_{2d+1}, \cdots, u_{p-1})!\Big] + \frac{1}{2}(2 - k_0), & \\ & \text{for } k_0 \neq 1 \\ (d+1)^m\big(2^{\frac{m}{2}+1} - 1\big) - 1, & \text{for } k_0 = 1 \end{cases}$$

where $m = 2\sum_{k=2d+1}^{p-1} v_k$ and $(x_1, x_2, \cdots, x_l)!$ is a multinomial coefficient defined as

$$(x_1 x_2, \cdots, x_l)! = \frac{(x_1 + x_2 + \cdots + x_l)!}{x_1! x_2! \cdots x_l!}.$$

Proof. Since $3|n$, m should be even. From (5), (6), and Lemma 1, we have to consider the following three equations.

$$0 = 3(1 - k_0), \qquad \text{for } 0 \leq i < L \tag{8}$$

$$(\alpha^L + 2)B_1(i) = 3(1 - k_0), \qquad \text{for } L \leq i < 2L \tag{9}$$

$$\big(B_1(i) - B_2(i)\big)\alpha^L + 2B_1(i) + B_2(i) = 3(1 - k_0), \qquad \text{for } 2L \leq i < 3L. \tag{10}$$

We will derive the linear complexity for the following two cases.

Case 1) $k_0 \neq 1$;

In this case, we have to consider the following three subcases.

Case 1-a) For $0 \leq i < L$: Certainly, (8) cannot be satisfied. Thus $A_{-i} \neq 0$, for $0 \leq i < L$.

Case 1-b) For $L \leq i < 2L$: Since $p \equiv 2 \bmod 3$, we have $(\alpha^L)^{p-1} \neq 1$, i.e., $\alpha^L \notin F_p$. Then the right hand side of (9) is an element of F_p while its left hand side is not an element of F_p. It is a contradiction. Therefore, $A_{-i} \neq 0$ for $L \leq i < 2L$.

Case 1-c) $2L \leq i < 3L$: In (10), if $B_1(i) - B_2(i) \neq 0$, $A_{-i} \neq 0$ because $\alpha^L \notin F_p$ and $B_1(i)$ and $B_2(i)$ are elements of F_p. If $B_1(i) - B_2(i) = 0$, we have $B_1(i) = B_2(i) \equiv 1 - k_0 \bmod p$.

In order to apply Lucas' theorem, we need to expand L as

$$L = \frac{p^m - 1}{3} = \frac{p^2 - 1}{3} \sum_{j=0}^{(m-2)/2} p^{2j} = \Big[dp + (2d+1)\Big] \sum_{j=0}^{(m-2)/2} p^{2j}$$
$$= dp^{m-1} + (2d+1)p^{m-2} + dp^{m-3} + (2d+1)p^{m-4} + \cdots + dp + (2d+1).$$

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

$$B_1(i) = \binom{i}{L} \equiv \binom{i_{m-1}}{d}\binom{i_{m-2}}{2d+1}\cdots\binom{i_1}{d}\binom{i_0}{2d+1} \equiv 1 - k_0 \bmod p. \quad (11)$$

Similarly, we can expand $2L$ as

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

and we have

$$B_2(i) = \binom{i}{2L} \equiv \binom{i_{m-1}}{2d+1}\binom{i_{m-2}}{d}\cdots\binom{i_1}{2d+1}\binom{i_0}{d} \equiv 1 - k_0 \bmod p. \quad (12)$$

Since β is a primitive element of F_p, $\beta^h = 1 - k_0$, $\beta^{f_k} \equiv \binom{k}{d} \bmod p$, and $\beta^{g_k} \equiv \binom{k}{2d+1} \bmod p$, (11) and (12) can be rewritten as

$$B_1(i) = \beta^{f_{i_{m-1}} + g_{i_{m-2}} \cdots + f_{i_1} + g_{i_0}} \equiv \beta^h \bmod p \quad (13)$$

$$B_2(i) = \beta^{g_{i_{m-1}} + f_{i_{m-2}} + \cdots + g_{i_1} + f_{i_0}} \equiv \beta^h \bmod p. \quad (14)$$

Since all of the Lucas factors of $B_1(i)$ and $B_2(i)$ are not equal to zero, from (13) and (14), we have

$$V_1 = \sum_{i=2d+1}^{p-1} (v_i f_i + u_i g_i) \equiv h \bmod (p-1) \quad (15)$$

$$V_2 = \sum_{i=2d+1}^{p-1} (v_i g_i + u_i f_i) \equiv h \bmod (p-1). \quad (16)$$

In order to count the number of i satisfying $B_1(i) = B_2(i) \equiv 1 - k_0 \bmod p$, we have to count the number of solutions v_i and u_i, $2d+1 \le i \le p-1$, satisfying (15) and (16). For $k_0 = 0$, we must rule out the case, $i_0 = \cdots = i_{m-1} = p-1$, which corresponds to $i = p^m - 1$. Then we have

$$F_2(1-k_0, 1-k_0) = \sum_{\substack{V_1 \equiv h \bmod (p-1) \\ V_2 \equiv h \bmod (p-1)}} (v_{2d+1}, \cdots, v_{p-1})!(u_{2d+1}, \cdots, u_{p-1})! - \frac{1}{2}(2 - k_0).$$

Since the linear complexity $L_3(p)$ of ternary Sidel'nikov sequences is

$$L_3(p) = n - F_2(1-k_0, 1-k_0),$$

we proved this case.

Case 2) $k_0 = 1$;

From (8), we have $F_0 = L$. And for $L \le i < 2L$, from (9), we know that $A_{-i} = 0$ if and only if $B_1(i) = 0$. For $2L \le i < 3L$, (10) tells us that $A_{-i} = 0$

if and only if $B_1(i) = B_2(i) = 0$. Thus, the linear complexity is equal to the number of i satisfying the following three cases.

i) $B_1(i) \neq 0$ and $B_2(i) \neq 0$
ii) $B_1(i) = 0$ and $B_2(i) \neq 0$
iii) $B_1(i) \neq 0$ and $B_2(i) = 0$.

From (11) and (12), the number of i satisfying i) is the number of i such that all i_a's are greater than or equal to $2d+1$, which is given as $(d+1)^m - 1$. Now, let us count the number of i satisfying ii). From (11) and (12), we have $i_a \geq d$, $0 \leq a < m$, because $B_2(i) \neq 0$. Since $B_1(i) = 0$, at least one Lucas factor $\binom{i_a}{2d+1}$ in $B_1(i)$ is equal to 0, i.e., there is at least one Lucas factor satisfying $d \leq i_a < 2d+1$, which can be counted as

$$\sum_{j=1}^{m/2} \binom{\frac{m}{2}}{j} (d+1)^m = (d+1)^m (2^{\frac{m}{2}} - 1).$$

Clearly, ii) and iii) give us the same values. Thus, for $k_0 = 1$, the linear complexity of ternary Sidel'nikov sequences can be derived as in the theorem. □

Example 1. Let $M = 3$. Let $p = 3d + 2 = 5$ and $\beta = 3$, where m is even. For $k_0 = 0$, we have

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

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

$$V_1 = v_3 + 2v_4 + 2u_4 \equiv 0 \bmod 4$$
$$V_2 = 2v_4 + u_3 + 2u_4 \equiv 0 \bmod 4.$$

Therefore, v_3 and u_3 are multiples of 4 and $v_4 + u_4$ is a multiple of 2. And $v_3 + v_4 = m/2$ and $u_3 + u_4 = m/2$. Then the linear complexity $L_3(5)$ of ternary Sidel'nikov sequences is written as

$$L_3(5) = p^m - \sum_{\substack{V_1 \equiv 0 \bmod 4 \\ V_2 \equiv 0 \bmod 4}} (v_3, v_4)!(u_3, u_4)! = p^m - \left\{ \sum_{j=0}^{\lfloor \frac{m}{8} \rfloor} \binom{\frac{m}{2}}{4j} \right\}^2.$$

For $k_0 = 1$, from the above theorem, it can be easily derived as

$$L_3(5) = 2^{\frac{3m}{2}+1} - 2^m - 1. \qquad \square$$

Now, we will derive the linear complexity of ternary Sidel'nikov sequences for the case of $p \equiv 1 \bmod 3$. The following lemma can be used in the calculation of $B_v(i)$.

Lemma 2. Let M and d be positive integers. For $p = Md + 1$ and $1 \le j \le d$, we have

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

Proof. Since $Md \equiv -1 \bmod p$, we have

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

Then the proof is done by noting that

$$\binom{(M-1)d-j}{d-j} = \binom{(M-1)d}{d} \prod_{i=0}^{j-1} \frac{d-i}{(M-1)d-i}$$

and

$$\binom{(M-1)d+j}{d+j} = \binom{(M-1)d}{d} \prod_{i=0}^{j-1} \frac{(M-1)d+i+i}{d+i+1}.$$

□

For $M = 3$, it can be easily modified as

$$\binom{2d-j}{d} \equiv \binom{2d+j}{d} \bmod p. \tag{17}$$

The following lemmas are need to derive the linear complexity for $p = 3d+1$.

Lemma 3. Let $p = 3d + 1$ and $k_0 \neq 1$. Let $\beta^{f'} = (1-\alpha^L)(1-k_0)$. For $0 \le k \le p-1$, let $\beta^{f_k} = \binom{k}{d}$ and v_k be the number of $\binom{k}{d}$ among the Lucas factors of $B_1(i)$. Let $\sum_{j=k}^{p-1} v_j = m$ and $V(k) = \sum_{j=k}^{p-1} v_j f_j$. For $L \le i < 3L$, the number of i satisfying $B_1(i) \equiv (1-\alpha^L)(1-k_0) \bmod p$ and $B_2(i) = 0$ in (9) and (10) is given as

$$F_1((1-\alpha^L)(1-k_0)) + F_2((1-\alpha^L)(1-k_0), 0) = E(d) - E(2d)$$

where

$$E(k) = \sum_{V(k) \equiv f' \bmod p-1} (v_k, \cdots, v_{p-1})!.$$

Proof. Clearly, we have

$$L = \frac{p^m - 1}{3} = \Big(\frac{p-1}{3}\Big) \sum_{i=0}^{m-1} p^i = d \sum_{i-0}^{m-1} p^i. \tag{18}$$

By Lucas' theorem, it can be easily derived that

$$B_1(i) = \prod_{a=0}^{m-1} \binom{i_a}{d} = \beta^{f_{i_0}+f_{i_1}+\cdots+f_{i_{m-1}}} = (1-\alpha^L)(1-k_0) \equiv \beta^{f'} \bmod p.$$

Then we have

$$V(d) = \sum_{j=d}^{p-1} v_j f_j = f'$$

$$E(d) = \sum_{V(d)\equiv f' \bmod (p-1)} (v_d, \cdots, v_{p-1})!.$$

Since $B_2(i) = 0$, we have to rule out the case $B_2(i) \neq 0$ from $E(d)$. $E(2d)$ is the number of i such that all the coefficients i_a, $0 \leq a < m$, of its p-ary expansion are in the range $2d \leq i_a \leq p-1$, which corresponds to $B_2(i) \neq 0$ and $B_1(i) \equiv (1-\alpha^L)(1-k_0) \bmod p$. Thus, we prove it. □

Similarly, we can easily obtain the following lemma.

Lemma 4. Let $p = 3d+1$. Let $\beta^{f'} = B_1(i) \neq 0$ and $\beta^{g'} = B_2(i) \neq 0$. For $0 \leq k \leq p-1$, let $\beta^{f_k} = \binom{k}{d}$ and $\beta^{g_k} = \binom{k}{2d}$. Let $\sum_{j=2d}^{p-1} v_j = m$, $V_1 = \sum_{j=2d}^{p-1} v_j f_j$, and $V_2 = \sum_{j=2d}^{p-1} v_j g_j$. For $2L \leq i < 3L$, the number of i satisfying $(B_1(i), B_2(i)) = (c_1, c_2)$ is given as

$$F_2(c_1, c_2) = \sum_{\substack{V_1 \equiv f' \bmod (p-1) \\ V_2 \equiv g' \bmod (p-1)}} (v_{2d}, \cdots, v_{p-1})!. \tag{19}$$

□

Since $p = 3d+1$, we have $(\alpha^L)^{p-1} = (\alpha^L)^3 = 1$, $\alpha^L \in F_p$, and $\alpha^{2L} + \alpha^L + 1 = 0$. Let $\gamma = \alpha^L$. Note that $(1-\gamma)(\gamma+2) = 2 - \gamma - \gamma^2 = 3$. Then we can derive the linear complexity of ternary Sidel'nikov sequences for $p \equiv 1 \bmod 3$ as in the following theorem.

Theorem 5. Let $n = p^m - 1$ and $p = 3d+1$ be a prime, where d is a positive integer. Let $3|n$. Then the linear complexity $L_3(p)$ over F_p of ternary Sidel'nikov sequences of period n is given as

$$L_3(p) = \begin{cases} n - \sum\limits_{V(d)\equiv f' \bmod (p-1)} (v_d, \cdots, v_{p-1})! + \sum\limits_{V(2d)\equiv f' \bmod (p-1)} (v_{2d}, \cdots, v_{p-1})! \\ \quad - \sum\limits_{\substack{(\gamma+2)c_{21} - (\gamma-1)c_{22} = 3(1-k_0) \\ c_{22} \neq 0}} \sum\limits_{\substack{V_1 \equiv f' \bmod (p-1) \\ V_2 \equiv g' \bmod (p-1)}} (v_{2d}, \cdots, v_{p-1})! - \frac{1}{2}(2-k_0), \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k_0 \neq 1 \\ (2d+1)^m - 1 - \sum\limits_{\substack{(\gamma+2)c_{21} - (\gamma-1)c_{22} = 0 \\ c_{21} \neq 0,\ c_{22} \neq 0}} \sum\limits_{\substack{V_1 \equiv f' \bmod (p-1) \\ V_2 \equiv g' \bmod (p-1)}} (v_{2d}, \cdots, v_{p-1})!, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k_0 = 1. \end{cases}$$

Proof. Since γ is an element of F_p with order 3, (7) can be represented as

$$3(1-k_0) = (\gamma+2)B_1(i) - (\gamma-1)B_2(i). \tag{20}$$

Similarly to (8), (9), and (10), we have to consider the following three equations.

$$0 = 3(1-k_0), \qquad \text{for } 0 \le i < L \tag{21}$$
$$(\gamma+2)B_1(i) = 3(1-k_0), \qquad \text{for } L \le i < 2L$$
$$(\gamma+2)B_1(i) + (1-\gamma)B_2(i) = 3(1-k_0), \qquad \text{for } 2L \le i < 3L. \tag{22}$$

Case 1) $k_0 \neq 1$;
Case 1-a) $0 \le i < L$: Clearly, (21) cannot be satisfied. Thus $A_{-i} \neq 0$, for $0 \le i < L$.
Case 1-b) $L \le i < 2L$: We have to count the number of i satisfying $B_1(i) \equiv (1-\gamma)(1-k_0) \bmod p$ and $B_2(i) = 0$, i.e., $F_1((1-\gamma)(1-k_0))$.
Case 1-c) $2L \le i < 3L$: We have to count the number $F_2(c_1, c_2)$ of i satisfying (22) for $(B_1(i), B_2(i)) = (c_1, c_2)$. If $c_2 = 0$, we have $c_1 = (1-\gamma)(1-k_0)$, which corresponds to $F_2((1-\gamma)(1-k_0), 0)$. Lemma 3 gives us the value of $F_1((1-\gamma)(1-k_0)) + F_2((1-\gamma)(1-k_0), 0)$, which includes the cases of **Case 1-b)**. If $c_2 \neq 0$, we also have $c_1 \neq 0$ and Lemma 4 gives us the value of $F_2(c_1, c_2)$.

Here, we need to exclude the case that all i_a's are equal to $p-1$, $0 \le a < m$. When $i_a = p-1$, $0 \le a < m$, from (17), we have $f_{p-1} = 0$, $g_{p-1} = 0$, and $v_{p-1} = m$. Thus, counting of i for $(c_1, c_2) = (1, 1)$ contains the case that all i_a's are equal to $p-1$, $0 \le a < m$, which occurs only when $k_0 = 0$.

Therefore, the linear complexity $L_3(p)$ of ternary Sidel'nikov sequences for $p \equiv 1 \bmod 3$ is given as

$$L_3(p) = n - F_1((1-\gamma)(1-k_0)) - \sum_{(\gamma+2)c_1-(\gamma-1)c_2=3(1-k_0)} F_2(c_1, c_2) + \frac{1}{2}(2-k_0).$$

Using Lemmas 3 and 4, we prove this case.

Case 2) $k_0 = 1$;
Case 2-a) $0 \le i < L$: The number of i satisfying (20) is given as $F_0 = L$.
Case 2-b) $L \le i < 2L$: We need to count the number of i satisfying $B_1(i) = B_2(i) \equiv 0 \bmod p$.
Case 2-c) $2L \le i < 3L$: We need to count the number of i satisfying $(B_1(i), B_2(i)) = (c_1, c_2)$, where $(\gamma+2)c_1 - (\gamma-1)c_2 = 0$. Note that $c_1 = c_2 = 0$ is always a solution of it. From $B_1(i) = 0$ and $B_2(i) = 0$, there is at least one Lucas factor $\binom{i_a}{d}$ and $\binom{i_a}{2d}$ such that $0 \le i_a < d$. It is equivalent to subtract the number of i satisfying $B_1(i) \neq 0$ or $B_2(i) \neq 0$ from $2L$. Thus, we can easily find the value, $F_1(0) + F_2(0, 0) = 2L - (2d+1)^m + 1$, where all cases in **Case 2-b)** are included but the case of $i = p^m - 1$ is excluded.

Finally, we have to find $F_2(c_1, c_2)$ for nonzero c_1 and c_2, which is given by Lemma 4. Therefore, for $k_0 = 1$, the linear complexity $L_3(p)$ of ternary Sidel'nikov sequences for $p \equiv 1 \bmod 3$ is given as

$$L_3(p) = n - L - 2L + (2d+1)^m - 1 - \sum_{\substack{(\gamma+2)c_1-(\gamma-1)c_2=0 \\ c_1\neq 0,\ c_2\neq 0}} F_2(c_1, c_2).$$

Using Lemma 4, we prove the theorem. □

For $M = 3$ and $p = 7$, the linear complexity of ternary Sidel'nikov sequences is given in the following example.

Example 2. Let $p = 7$, $\beta = 3$, $\gamma = 2$, and $M = 3$. For $k_0 = 0$, 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 $v_2 + \cdots + v_6 = m$ and

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

Also we have $v_4 + v_5 + v_6 = m$ and

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

We can calculate the numbers c_1 and c_2 satisfying (20). Finally, we have

$$L_3(7) = p^m - \big(E(d) - E(2d)\big) - \sum_{4c_1-c_2=3} \sum_{\substack{3v_4+v_5\equiv f' \bmod 6 \\ 5v_5\equiv g' \bmod 6}} (v_4, v_5, v_6)!.$$

Table 1. Linear complexity of ternary Sidel'nikov sequences for $p = 7$

m	Period	$k_0 = 0$		$k_0 = 1$		$k_0 = 2$	
	$p^m - 1$	$\gamma = 2$	$\gamma = 4$	$\gamma = 2$	$\gamma = 4$	$\gamma = 2$	$\gamma = 4$
3	342	323	315	118	121	322	314
4	2,400	2,301	2,274	607	612	2,307	2,287
5	16,806	16,300	16,236	3,079	3,083	16,300	16,296
6	117,648	115,088	114,988	15,498	15,498	114,956	115,120
7	823,542	810,620	810,633	77,759	77,746	809,863	810,633
8	5,764,800	5,699,809	5,700,521	389,544	389,503	5,697,118	5,699,176
9	40,353,606	40,027,751	40,030,599	1,949,884	1,949,803	40,020,946	40,023,794

For $k_0 = 1$, from the above theorem, the linear complexity of ternary Sidel'nikov sequence is given as

$$L_3(7) = 5^m - \sum_{4c_1 - c_2 = 0} \sum_{\substack{3v_4 + v_5 \equiv f' \bmod 6 \\ 5v_5 \equiv g' \bmod 6}} (v_4, v_5, v_6)! - 1.$$

Table 1 lists the linear complexities $L_3(7)$ over F_7 of some ternary Sidel'nikov sequences. □

References

1. E. R. Berlekamp, *Algebraic Coding Theory*. 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. T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Inf. Theory*, vol. 49, no. 6, pp. 1548–1552, June 2003.
4. T. Helleseth, M. Maas, J. E. Mathiassen, and T. Segers, "Linear complexity over F_p of Sidel'nikov sequences," *IEEE Trans. Inf. 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. SETA 2001*, 2001, pp. 29–30.
6. Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the linear complexity over F_p of M-ary Sidel'nikov sequences," in *Proc. IEEE ISIT 2005*, Sept. 2005, pp. 2007–2011.
7. G. M. Kyureghyan and A. Pott, "On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Des., Codes and Cryptogr.*, vol. 29, pp. 149–164, 2003.
8. A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inf. Theory*, vol. IT-23, no. 1, pp. 38–42, Jan. 1977.
9. 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.