Some Upper Bounds and Exact Values on Linear Complexities Over $\mathbb{F}_M$ of Sidelnikov Sequences for $M = 2$ and 3

Min Zeng, Yuan Luo, *Member, IEEE*, Guo-Sheng Hu, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*— Sidelnikov sequences, a kind of cyclotomic sequences with many desired properties such as low correlation and variable alphabet sizes, can be employed to construct a polyphase sequence family that has many applications in high-speed data communications. Recently, cyclotomic numbers have been used to investigate the linear complexity of Sidelnikov sequences, mainly about binary ones, although the limitation on the orders of the available cyclotomic numbers makes it difficult. This paper continues to study the linear complexity over $\mathbb{F}_M$ of M-ary Sidelnikov sequence of period $q-1$ using Hasse derivative, which implies $q = p^m$, $m \geq 1$ and $M|(q-1)$. The tth Hasse derivative formulas are presented in terms of cyclotomic numbers, and some upper bounds on the linear complexity for $M = 2$ and 3 are obtained only with some additional restrictions on q. Furthermore, concrete illustrations for several families of these sequences, such as $q \equiv 1 \pmod 2$ and $q \equiv 1 \pmod 3$, show these upper bounds are tight and reachable; especially for $q = 2\times 3^{\lambda}+1 (1 \leq \lambda \leq 20)$, the exact linear complexities over $\mathbb{F}_3$ of the ternary Sidelnikov sequences are determined; and it turns out that all the linear complexities of the sequences considered are very close to their periods.**

***Index Terms*— Array structure, cyclotomic numbers, Hasse derivative, linear complexity, Sidelnikov sequences.**

I. Introduction

PSEUDO random sequences with certain properties are widely used in the communication engineering and cryptography [1]. The cyclotomic sequences have a number of attractive randomness properties [2]–[4]. Ding [5] studied their linear complexity, minimal polynomial, and autocorrelation function.

For $q = p^m$ where p is an odd prime and m is a positive integer, Sidelnikov [6] introduced a kind of cyclotomic sequence called the M-ary Sidelnikov sequence of period $q-1$ where $M|(q-1)$. Soon afterwards, Lempel, Cohn and Eastman [7] re-introduced its binary form called Sidelnikov-Lempel-Cohn-Eastman sequence. In the last two decades, a lot of attention has been devoted to this binary sequence. For example, using the cyclotomic numbers, Helleseth and Yang [8] originally investigated the autocorrelation function and linear complexity over $\mathbb{F}_2$ of the binary Sidelnikov sequences. Later on, Kyureghan and Pott [9], and Meidl and Winterhof [10] determined the exact linear complexity over $\mathbb{F}_2$ of some of these sequences with well-known results on cyclotomic numbers; a lower bound on the linear complexity profile of these sequences was also introduced in [10], which is the desirable important property of applications. Then, Wang [11] and Su [12] studied the linear complexity of binary cyclotomic sequences of order 6 and Legendre-Sidelnikov sequences of period $p(q-1)$, respectively. Ye *et al.* [13] further studied the linear complexity of a new kind of binary cyclotomic sequence, with length p^r, and Liang *et al.* [14] computed the linear complexity of Ding-Helleseth generalized cyclotomic sequences by using cyclotomic numbers of order 8. Following the footsteps of these pioneers, Zeng *et al.* [15] discussed the $\mathbb{F}_M$-linear complexity of M-ary Sidelnikov sequences of period $p-1 = f\times M^{\lambda}$ where M is not just equal to 2. On the other hand, using the discrete Fourier transform (i.e., DFT), Helleseth *et al.* [16], [17] also determined the linear complexity over $\mathbb{F}_p$ of binary Sidelnikov sequences, and Garaev *et al.* [18] derived the lower bound of the linear complexity over $\mathbb{F}_p$. For the k-error linear complexity over $\mathbb{F}_p$ of the d-ary Sidelnikov sequence, Chung and Yang [19] presented many results of interest, then Aly and Meidl [20] further complemented these results.

In this paper, we continue to study the linear complexity over $\mathbb{F}_M$ of M-ary Sidelnikov sequence of period $q-1$ using Hasse derivative, where $q = p^m$, $m \geq 1$ and $M|(q-1)$. Some upper bounds on the linear complexity for $M = 2$ and 3 are obtained, and some exact values of the linear complexity for several families of these sequences, such as $q \equiv 1 \pmod 2$ and $q \equiv 1 \pmod 3$, illustrate these upper bounds are tight and reachable. In particular, the exact linear complexities over

Manuscript received 7 September 2021; revised 13 February 2022; accepted 4 April 2022. Date of publication 13 April 2022; date of current version 13 July 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 62171279 and in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean Government through the Ministry of Sciences and Information Technology (MSIT) under Grant 2020R1A2C2011969. An earlier version of this paper was presented in part at the 2019 IEEE International Symposium on Information Theory (2019ISIT) [DOI: 10.1109/ISIT.2019.8849276]. *(Corresponding author: Yuan Luo.)*

Min Zeng is with the Shanghai Technical Institute of Electronics & Information, Shanghai 201411, China, and also with the Information and Coding Theory Laboratory, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: inform_code@sjtu.edu.cn).

Yuan Luo is with the Department of Computer Science and Engineering and the MoE Key Laboratory of Artificial Intelligence, AI Institute, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: yuanluo@sjtu.edu.cn).

Guo-Sheng Hu is with the Shanghai Technical Institute of Electronics & Information, Shanghai 201411, China (e-mail: huguosheng@stiei.edu.cn).

Hong-Yeop Song is with the School of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by K.-U. Schmidt, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2022.3167097

$\mathbb{F}_3$ of the ternary Sidelnikov sequences are determined for $q = 2 \times 3^\lambda + 1 (1 \leq \lambda \leq 20)$, and it turns out that all the linear complexities of the sequences considered are very close to their periods. Some examples over $\mathbb{F}_2$ have been confirmed for binary Sidelnikov sequences by Helleseth and Yang.

The rest of this paper is organized as follows. In Section II, after reviewing some notations and definitions, we present formulas for the tth Hasse derivative of the generating function $S(x)$ of the M-ary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ in terms of the cyclotomic numbers. In Section III, the multiplicities of some rth primitive roots of unity over $\mathbb{F}_M$ as roots of $S(x)$ are determined using the Hasse derivative to estimate the $\mathbb{F}_M$-linear complexity of M-ary Sidelnikov sequences for the two cases of $q \equiv 1 \pmod 2$ and $q \equiv 1 \pmod 3$. Some special examples are listed in Table I for $q = 2 \times 3^\lambda + 1 (1 \leq \lambda \leq 20)$. Note that this section extends our conference version [15] by adding Subsection III-A on the case $q \equiv 1 \pmod 2$ which includes Theorem 1 and Examples 4 and 5, by supplementing a main result on the case $q \equiv 1 \pmod 3$ in Theorem 2 of Subsection III-B, and by giving all proofs of the relevant results here. In Section IV, there are some concluding remarks. In addition, some known cyclotomic numbers of orders $2, 2r, 3, 6$ and 9 are displayed in Chapter IV due to the need to prove the results of this paper.

II. Preliminaries

In this section, after some notations are listed, the M-ary Sidelnikov sequence, the $\mathbb{F}_M$-linear complexity and the cyclotomic number are defined in Definitions 1, 3 and 4, respectively. Lemma 3 presents Hasse derivates in terms of cyclotomic numbers, and will be used to determine the $\mathbb{F}_M$-linear complexity of the M-ary Sidelnikov sequence.

- p: an odd prime.
- q: an odd prime power p^m with $m \geq 1$.
- $\mathbb{F}_p$ and $\mathbb{F}_q$: the finite fields with p and q elements, respectively.
- M: M is a prime with $M|(q-1)$.
- α: a fixed primitive element of $\mathbb{F}_q$.
- $\{s_n\}_{n\geq 0}$: the M-ary Sidelnikov sequence of period $q-1$.
- $S(x)$: the generating function of $\{s_n\}_{0\leq n\leq q-2}$.
- $\mathbb{F}_M[x]$: the polynomial ring over finite field $\mathbb{F}_M$.
- $R(\gamma)$: the multiplicity of a primitive rth root γ of unity over $\mathbb{F}_M$ as a root of $S(x)$, where $\gamma = e^{j\frac{2\pi}{r}}$ and $j = \sqrt{-1}$.
- $LC(\cdot)$: the $\mathbb{F}_M$-linear complexity of a sequence. It is written as LC for short if the context is clear.
- Ind x: the index of $x \in \mathbb{F}_q$ to the base g modulo q [21].

The M-ary Sidelnikov sequence is defined as follows.

Definition 1 ([22]): For a fixed primitive element α of $\mathbb{F}_q$ and $M|(q-1)$, let $D_k^{(\alpha)}$, $k = 0, 1, \ldots, M-1$, be the disjoint subsets of $\mathbb{F}_q$ defined as

$$D_k^{(\alpha)} = \{\alpha^{Mi+k} - 1 \mid 0 \leq i \leq \frac{q-1}{M} - 1\}.$$

The M-ary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ of period $q-1$ is defined as

$$s_n = \begin{cases} k & \text{if } \alpha^n \in D_k^{(\alpha)}, \\ 0 & \text{if } \alpha^n = -1. \end{cases} \quad (1)$$

Equivalently,

$$s_n \equiv \log_\alpha(\alpha^n + 1) \pmod M. \quad (2)$$

Note that $\bigcup_{k=0}^{M-1} D_k^{(\alpha)} = \mathbb{F}_q \backslash \{-1\}$, $0 \in D_0^{(\alpha)}$, and let $\log_\alpha(0) = 0$.

Example 1: Let $q = 7$ and $M = 3$. For $\alpha = 3$, we have a ternary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ of period 6, that is, $\{s_n\}_{0\leq n\leq 5} = \{2, 1, 1, 0, 2, 0\}$.

Definition 2: A polynomial $C(x) = x^L + c_1 x^{L-1} + \cdots + c_{L-1}x + 1 \in \mathbb{F}_M[x]$ is the connection polynomial of the M-ary sequence $\{s_n\}_{n\geq 0}$ of period $T = q-1$ if there exist constants $c_0 = 1, c_1, \ldots, c_{L-1}, c_L = 1 \in \mathbb{F}_M$, such that

$$s_j \equiv -\sum_{i=0}^{L-1} c_i s_{j-L+i} \pmod M, \text{ for all } j \geq L. \quad (3)$$

Definition 3: The linear complexity over $\mathbb{F}_M$ of $\{s_n\}_{n\geq 0}$ is defined as

$$LC(\{s_n\}_{n\geq 0}) = \min\{\deg(C(x)) : C(x) \text{ is the connection polynomial of } \{s_n\}_{n\geq 0}\}.$$

Lemma 1 ([23]): Let $S(x) = s_0 + s_1 x + \cdots + s_{q-2}x^{q-2}$. Then $C(x)$ is the connection polynomial of $\{s_n\}_{n\geq 0}$ if and only if $S(x)C(x) \equiv 0 \mod (x^{q-1} - 1)$.

Therefore, the $\mathbb{F}_M$-linear complexity of the M-ary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ can be determined by

$$LC(\{s_n\}_{n\geq 0}) = q - 1 - \deg[\gcd(x^{q-1} - 1, S(x))], \quad (4)$$

where $S(x)$ is by (1)

$$S(x) = \sum_{k=1}^{M-1} k \sum_{\substack{\alpha^n \in D_k^{(\alpha)} \\ 0\leq n\leq q-2}} x^n \in \mathbb{F}_M[x]. \quad (5)$$

Example 2: The $\mathbb{F}_3$-linear complexity of the ternary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ of period 6 in Example 1 is 5 since $\gcd(x^6 - 1, 2x^4 + x^2 + x + 2) = x - 1$.

Similar to Example 2, in order to evaluate $LC(\{s_n\}_{n\geq 0})$ from (4), we will determine the multiplicity of γ as a root of $S(x)$, where γ is also a $(q-1)$-th root of unity over $\mathbb{F}_M$ or in an extension field of $\mathbb{F}_M$, by using the cyclotomic numbers defined as follows.

Definition 4: Let α be a primitive element in the finite field $\mathbb{F}_q$, and $e|(q-1)$. Then the cyclotomic classes $C_u^{(\alpha)}$, $0 \leq u \leq e-1$, are defined in $\mathbb{F}_q$ as

$$C_u^{(\alpha)} = \{\alpha^{ed+u} \mid 0 \leq d \leq \frac{q-1}{e} - 1\}.$$

For fixed positive integers u and v, not necessarily distinct, the cyclotomic number $(u, v)_e$ is defined as the number of elements $z_u \in C_u^{(\alpha)}$ such that $z_u + 1 \in C_v^{(\alpha)}$, where e is called the order of the cyclotomic number.

Example 3: Let $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\} = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ where $\alpha = 3$ is a primitive element in $\mathbb{F}_7$. Let $e = 3$. Then $C_0^{(\alpha)} = \{1, \alpha^3\}$, $C_1^{(\alpha)} = \{\alpha, \alpha^4\}$, and $C_2^{(\alpha)} = \{\alpha^2, \alpha^5\}$. It is easy to see that $1+1 = 2 = \alpha^2$ and $\alpha^3+1 = 0$, thus $(0,0)_3 = 0$, $(0,1)_3 = 0$, and $(0,2)_3 = 1$. Similarly, $(1,0)_3 = 0$, $(1,1)_3 = 1$, $(1,2)_3 = 1$, $(2,0)_3 = 1$, $(2,1)_3 = 1$, and $(2,2)_3 = 0$.

Let $q = f \times M^{\lambda}+1$ where f and λ are two positive integers. Then $x^{q-1}-1 = (x^f-1)^{M^\lambda} \in \mathbb{F}_M[x]$. Let γ be a primitive rth root of unity over $\mathbb{F}_M$ or in an extension field of $\mathbb{F}_M$ where $r|f$. Then the multiplicity of γ as a root of $S(x)$ is i, i.e.,

$$R(\gamma) = i,$$

if $S(\gamma) = S(\gamma)^{(1)} = \cdots = S(\gamma)^{(i-1)} = 0$ and $S(\gamma)^{(i)} \neq 0$, where $S(x)^{(t)}$ $(t = 0, 1, \ldots, i)$ is the tth Hasse derivative of $S(x)$ [24], and defined as

$$S(x)^{(t)} = \sum_{k=1}^{M-1} k \sum_{\substack{\alpha^n \in D_k^{(\alpha)} \\ t \le n \le q-2}} \binom{n}{t} x^{n-t} \in \mathbb{F}_M[x], \tag{6}$$

where the binomial coefficients $\binom{n}{t}$ modulo M can be evaluated with the following Corollary 1.

Lemma 2 (Lucas' Theorem [25]): Let $0 \le b_j \le a_j \le M-1$ for $j = 0, 1, \ldots, l-1$, where M is a prime. Then

$$\begin{pmatrix} a_0 + a_1 M + \cdots + a_{l-1} M^{l-1} \\ b_0 + b_1 M + \cdots + b_{l-1} M^{l-1} \end{pmatrix} \equiv \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} \\ b_{l-1} \end{pmatrix} \pmod M.$$

It is clear from Lemma 2 that $b_j \le a_j$ for $j = 0, 1, \ldots, l-1$. However, since there exists a convention that if $x < y$ then $\binom{x}{y} = 0$, the Lucas' theorem can be extended to the following corollary.

Corollary 1 (Extension of Lucas' Theorem): Let M be a prime.

1) Let $0 \le b_j, a_j \le M-1$ for $j = 0, 1, \ldots, l-1$. Then

$$\begin{pmatrix} a_0 + a_1 M + \cdots + a_{l-1} M^{l-1} \\ b_0 + b_1 M + \cdots + b_{l-1} M^{l-1} \end{pmatrix} \equiv \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \cdots \begin{pmatrix} a_{l-1} \\ b_{l-1} \end{pmatrix} \pmod M. \tag{7}$$

2) Let $n \equiv i \pmod{M^l}$ where $l = \lfloor \log_M(t) \rfloor + 1$ if $t \ge 1$, and $l = 1$ if $t = 0$. Then

$$\binom{n}{t} \equiv \binom{i}{t} \pmod M, \tag{8}$$

where $\binom{i}{t} = 0$ if $i < t$.

Proof: First, we prove Lucas' theorem is still true if there exists j such that $b_j > a_j$. To the end, we need to compare the coefficients of binomial expansion of $(1+x)^a$, where $a = \sum_{j=0}^{l-1} a_j M^j$ and $a_0, \ldots, a_{l-1}$ are the digits in the M-ary representation of a.

Since M is a prime, it follows that

$$(1+x)^{M^j} \equiv 1 + x^{M^j} \pmod M \text{ for } j \ge 1. \tag{9}$$

Then we have

$$\begin{aligned} &(1+x)^a \\ =&(1+x)^{a_0}((1+x)^M)^{a_1} \cdots ((1+x)^{M^{l-1}})^{a_{l-1}} \\ \equiv&(1+x)^{a_0}(1+x^M)^{a_1} \cdots (1+x^{M^{l-1}})^{a_{l-1}} \pmod M. \end{aligned} \tag{10}$$

Let $b = \sum_{j=0}^{l-1} b_j M^j$ where $b_0, \ldots, b_{l-1}$ are the digits in the M-ary representation of b. It is clear that the items of x^b on the left and right sides of (10) should be equal by using the unique M-ary representation property,

$$\begin{aligned} \binom{a}{b} x^b &= \binom{a_0}{b_0} x^{b_0} \binom{a_1}{b_1} x^{b_1 M} \cdots \binom{a_{l-1}}{b_{l-1}} x^{b_{l-1} M^{l-1}} \\ &= \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \binom{a_{l-1}}{b_{l-1}} x^b. \end{aligned} \tag{11}$$

Thus, if $b_j \le a_j$ for all $0 \le j \le l-1$, the coefficient on the left of (11) must be congruent modulo M to the coefficient on the right, which is exactly the result of Lucas' theorem. Otherwise, if there exists $0 \le j \le l-1$ such that $b_j > a_j$, then $\binom{a_j}{b_j} = 0$, which means there is no item of $x^{b_j M^j}$ on the right of (11), leading to there is no item of x^b. Then, the coefficients on both sides of (11) are equal to 0, that is to say, the Lucas' theorem is also true for $b_j > a_j$ $(0 \le j \le l-1)$. So, (7) is true.

Secondly, we prove (8) is also true.

(i) If $t = 0$, the result is obvious.

(ii) If $t \ge 1$, let $l = \lfloor \log_M(t) \rfloor + 1$. Then $t < M^l$. Let $n_0, n_1, \ldots, n_{l-1}, n_l, \ldots, n_{l'}$ and $t_0, \ldots, t_{l-1}$ be the digits in the M-ary representations of n and t, respectively. Then $n = \sum_{j=0}^{l'} n_j M^j$ and $t = \sum_{j=0}^{l-1} t_j M^j$. Since $n \equiv i \pmod{M^l}$, it follows that $i = \sum_{j=0}^{l-1} n_j M^j$. From (7), it is easy to see that

$$\begin{aligned} \binom{n}{t} &= \binom{n_0 + \cdots + n_{l-1} M^{l-1} + n_l M^l + \cdots + n_{l'} M^{l'}}{t_0 + \cdots + t_{l-1} M^{l-1} + 0 \times M^l + \cdots + 0 \times M^{l'}} \\ &\equiv \binom{n_0}{t_0} \cdots \binom{n_{l-1}}{t_{l-1}} \binom{n_l}{0} \cdots \binom{n_{l'}}{0} \pmod M \\ &\equiv \binom{i}{t} \pmod M. \end{aligned}$$

Thus, the proof completes. □

Next, the tth Hasse derivatives $(t = 0, 1, \ldots)$ in terms of cyclotomic numbers are listed in the following lemma that will be used to determine the multiplicities of all the fth roots of unity, as the roots of $S(x)$.

Lemma 3: [15] Let $q = p^m \equiv 1 \pmod M$ where p is an odd prime and M is prime. Let γ be a primitive rth root of unity over $\mathbb{F}_M$ or in an extension field of $\mathbb{F}_M$. $S(x)$ is the generating function of an M-ary Sidelnikov sequence $\{s_n\}_{0 \le n \le q-2}$. Then the tth Hasse derivatives $S(x)^{(t)} \in \mathbb{F}_M[x]$ $(t = 0, 1, \ldots)$ satisfy the following identities.

1)

$$S(1) = \sum_{k=1}^{M-1} k \sum_{u=0}^{M-1} (u, k)_M, \tag{12}$$

where $n \equiv u \pmod M$;

2)

$$S(1)^{(t)} = \sum_{k=1}^{M-1} k \sum_{i=t}^{M^l-1} \binom{i}{t} \sum_{j=0}^{M^{l-1}-1} (i, Mj+k)_{M^l}, \tag{13}$$

where $n \equiv i \pmod{M^l}$, and $l = \lfloor \log_M(t) \rfloor + 1$ if $t \ge 1$;

3) (see (14a) and (14b), as shown at the bottom of the next page;)

4) (see (15a) and (15b), as shown at the bottom of the next page.)

Remark 1: 1) The Hasse derivative in Lemma 3 is a bridge across the cyclotomic number and the linear complexity. Using this technique, one can determine the exact $\mathbb{F}_M$-linear complexity of an M-ary Sidelnikov sequence according to certain cyclotomic numbers. However, the well-known results on cyclotomic numbers are now just limited to the orders $e \le 24$. This limitation hinders our ability to calculate the multiplicity of γ if r is large. So, it seems difficult to determine the exact $\mathbb{F}_M$-linear complexity. 2) For the proof details of Lemma 3, please refer to [10], [15].

III. Upper Bounds and Some Exact Values

This section investigates the $\mathbb{F}_M$-linear complexities of the M-ary Sidelnikov sequences. In the case of $q \equiv 1 \pmod 2$, Theorem 1 shows that the $\mathbb{F}_2$-linear complexities of binary Sidelnikov sequences of period $q-1$ are upper bounded by $q-2r$ if r satisfies certain conditions. In the case of $q \equiv 1 \pmod 3$, for the trivial root 1, the primitive 2nd root and the primitive 3rd root of unity over $\mathbb{F}_3$ or in an extension field of $\mathbb{F}_3$, the multiplicities of them as the roots of $S(x)$ are determined in Propositions 1, 2 and 3, respectively. Furthermore, the $\mathbb{F}_3$-linear complexities of the ternary Sidelnikov sequences are presented in Theorem 2 and Corollary 2.

Note that, for the detailed meanings of the capital letters such as "A", "B", "C", etc. in this section, please refer to Appendices IV.

A. Binary Case

The linear complexity of binary Sidelnikov sequence was originally investigated by Helleseth and Yang, and later extended by Kyureghyan and Pott, and Meidl and Winterhof. In the following theorem, we continue to estimate the linear complexity of the Sidelnikov sequence for $q \equiv 1 \pmod 2$ using the technique introduced by Meidl and Winterhof, and the result is an extension of that in [10].

Theorem 1: Let $q = p^m \equiv 1 \pmod{2r}$ for $m = uv$, where p and r are both odd primes, $u \ge 1$, v is the order of p modulo r, and v is even. Let 2 be a primitive root modulo r and $\{s_n\}_{n\ge0}$ be a binary Sidelnikov sequence of period $q-1$. Then the linear complexity of $\{s_n\}_{n\ge0}$ over $\mathbb{F}_2$ is less than or equal to $q-2r$ if

1) u is even; or
2) u is odd, and $4 \nmid v$ with $p \equiv 3 \pmod 4$.

Proof: Let $S(x)$ be the generating function of $\{s_n\}_{0\le n\le q-2}$. The multiplicities of 1 as a root of $S(x)$ have been intensively discussed in [9] and [10]. Here we consider the multiplicity of γ as a root of $S(x)$ where $\gamma(\ne 1)$ is a primitive rth root of unity in an extension field of $\mathbb{F}_2$. Note that $(x^{2r}-1)|(x^{q-1}-1)$ since $2r|(q-1)$. Let $x^r - 1 = (x-1)(x^{r-1}+x^{r-2}+\cdots+1) = (x-1)\Phi_r(x)$ where $\Phi_r(x) = \prod_{\substack{1\le k\le r\\ \gcd(k,r)=1}}(x - e^{2\pi ik/r})$ is a cyclotomic polynomial. Then $\Phi_r(x)$ is irreducible over $\mathbb{F}_2$ since 2 is a primitive root modulo r [26], and $\Phi_r(\gamma)=0$. Let $M=2$.

First, consider γ is a single root of $S(x)$. Let $n \equiv h \pmod r$. Then $1 \le M - \lceil \frac{h+1}{r} \rceil < M$. Thus, we get from (14a) that

$$
\begin{aligned}
S(\gamma) &= \sum_{k=1}^{2-1} k \sum_{h=0}^{r-1}\sum_{j=0}^{r-1}\sum_{i=0}^{1}(ir+h, 2j+k)_{2r}\gamma^h\\
&= \sum_{h=0}^{r-1}\Big(\sum_{j=0}^{r-1}((h,2j+1)_{2r} + (r+h,2j+1)_{2r})\Big)\gamma^h = \sum_{h=1}^{r-1} T_{(0,h)}\gamma^h,
\end{aligned}
$$

where $T_{(0,h)} = \sum_{j=0}^{r-1}((h,2j+1)_{2r} + (r+h,2j+1)_{2r} - (0,2j+1)_{2r} - (r,2j+1)_{2r})$ since $\Phi_r(\gamma)=0$. From Appendix B, it follows that

$$
\begin{aligned}
T_{(0,h)} &= \sum_{j=0}^{r-1}((h,2j+1)_{2r} + (r+h,2j+1)_{2r} - (0,2j+1)_{2r}\\
&\quad -(r,2j+1)_{2r})\\
&\overset{*}{=} B + (2r-1)C - rB - B - (r-1)C \equiv C - B \pmod 2\\
&= \frac{1-(-1)^u p^{(uv)/2}}{2r},
\end{aligned}
$$

where * means that for a fixed h, one and only one of h and $h+r$ is odd, and is taken once by $2j+1$ when j runs from 0 to $r-1$.

$$
S(\gamma) = \begin{cases}
\displaystyle\sum_{k=1}^{M-1} k \sum_{h=0}^{r-1}\sum_{j=0}^{r-1}\sum_{i=0}^{M-1}(ir+h, Mj+k)_{rM}\cdot\gamma^h & \text{if } M \ne r, \quad (14a)\\
\displaystyle\sum_{k=1}^{M-1} k \sum_{h=0}^{M-1}(h,k)_M\cdot\gamma^h & \text{if } M = r, \quad (14b)
\end{cases}
$$

where $n = h \pmod r$;

$$
S(\gamma)^{(t)} = \begin{cases}
\displaystyle\sum_{k=1}^{M-1} k \sum_{i=t}^{M^l-1}\binom{i}{t}\sum_{h=0}^{r-1}\sum_{j=0}^{M^{l-1}r-1}(u(i,h), Mj+k)_{rM^l}\cdot\gamma^h & \text{if } M \ne r, \quad (15a)\\
\displaystyle\sum_{k=1}^{M-1} k \sum_{i=t}^{M^l-1}\binom{i}{t}\sum_{h=0}^{M-1}\sum_{j=0}^{M^{l-1}-1}(u(i,h), Mj+k)_{M^l}\cdot\gamma^h & \text{if } M = r, \quad (15b)
\end{cases}
$$

where $l = \lfloor \log_M(t) \rfloor + 1$ if $t \ge 1$, and $u(i,h)$ is (by the Chinese-Remainder-Theorem) the unique integer u satisfying $u - t \equiv h \pmod r$ and $u \equiv i \pmod{M^l}$, with $0 \le u \le rM^l - 1$ or $0 \le u \le M^l - 1$.

Since $\gamma, \ldots, \gamma^{r-1}$ are linear independent over $\mathbb{F}_2$, it follows that $S(\gamma) = 0$ if and only if

$$T_{(0,h)} \equiv 0 \pmod 2 \text{ for } h = 1, 2, \ldots, r-1,$$

which means that

$$\begin{aligned} p^{(uv)/2} &\equiv (-1)^u \pmod 4 & (16)\\ &\equiv \begin{cases} 1 \pmod 4 & \text{if } u \text{ is even,}\\ 3 \pmod 4 & \text{if } u \text{ is odd.}\end{cases} & (17)\end{aligned}$$

Then, we can get that

1) if u is even and v is even, then $p^{(uv)/2} \equiv 1 \pmod 4$,

2) if u is odd, and v is even and $4 \nmid v$, then $p^{(uv)/2} \equiv 3 \pmod 4$ if $p \equiv 3 \pmod 4$.

So, in these two cases, γ is a root of $S(x)$, and $\Phi_r(x) | \gcd(x^{q-1} - 1, S(x))$.

Second, we consider whether γ is a double root of $S(x)$ in the above cases. According to Lemma 3, let $l = 1$ since $t = 1 < M = 2$. From (15a),

$$\begin{aligned} S(\gamma)^{(1)} &= \sum_{k=1}^{M-1} k \sum_{i=1}^{M-1} \binom{i}{1} \sum_{h=0}^{r-1}\sum_{j=0}^{r-1} (u(i,h), Mj+k)_{Mr}\gamma^h\\ &= \sum_{h=0}^{r-1}\sum_{j=0}^{r-1} (u(1,h), 2j+1)_{2r}\gamma^h,\end{aligned}$$

where $u(1,h)$ is the unique integer u with $0 \le u \le 2r-1$, $u - 1 \equiv h \pmod r$, and $u \equiv 1 \pmod 2$. Then we have $u(1,h) = h+1$ if h is even, and $u(1,h) = r+h+1$ if h is odd. So,

$$S(\gamma)^{(1)} = \sum_{h=1}^{r-1} T_{(1,h)}\gamma^h,$$

where

$$\begin{aligned} &T_{(1,h)}\\ &= \sum_{j=0}^{r-1} ((u(1,h), 2j+1)_{2r} - (1, 2j+1)_{2r})\\ &= \begin{cases} \sum_{j=0}^{r-1} ((h+1, 2j+1)_{2r} - (1, 2j+1)_{2r}) & \text{if } h \text{ is even,}\\ \sum_{j=0}^{r-1} ((r+h+1, 2j+1)_{2r} - (1, 2j+1)_{2r}) & \text{if } h \text{ is odd.}\end{cases}\end{aligned}$$

For any fixed h, $u(1,h)$ is always odd, and can be equal to $2j+1$ once with j running from 0 through $r-1$. This means that $T_{(1,h)} = B + (r-1)C - (B + (r-1)C) = 0$ for $h = 1, 2, \ldots, r-1$ according to Appendix B. Thus, γ is a double root of $S(x)$ in the above cases. In addition, since $q = (p^{(uv)/2})^2 \equiv 1 \pmod 4$ from (17), we have $S(1) = (0,1)_2 + (1,1)_2 = \frac{q-1}{2} \equiv 0 \pmod 2$ according to Appendix A, that is to say, 1 is a root of $S(x)$. Thus, the upper bound immediately follows. □

Next, there are two examples to illustrate Theorem 1.

Example 4: Let $p = 5$, $u = 2$, $v = 2$, and $r = 3$. Then we have a binary Sidelnikov sequence $\{s_n\}_{n\ge0}$ of period 624. From the proof of Theorem 1, it is clear that 1 is a root of $S(x)$, and for any $\gamma(\neq 1)$ being a primitive 3rd root of unity, γ is a double root of $S(x)$, which means $(x^2+x+1)^2 | S(x)$. Thus, the linear complexity of $\{s_n\}_{n\ge0}$ over $\mathbb{F}_2$ is $LC(\{s_n\}_{n\ge0}) \le 619$ from Theorem 1 1). In addition, from Proposition 2 in [10], it is easy to see that the multiplicity of 1 as a root of $S(x)$ is 9, so, $LC(\{s_n\}_{n\ge0}) \le 611$. Indeed, we can get $\gcd(x^{624} - 1, S(x)) = (x-1)^{12}(x^2+x+1)^{10}$, that is, $LC(\{s_n\}_{n\ge0}) = 592$.

Example 5: Let $p = 19$, $u = 1$, $v = 2$, and $r = 5$. Then we have a binary Sidelnikov sequence $\{s_n\}_{n\ge0}$ of period 360. Similar to example 4, it is clear that 1 is a root of $S(x)$, and for any $\gamma(\neq 1)$ being a primitive 5th root of unity, γ is a double root of $S(x)$, which means $(x^4+x^3+x^2+x+1)^2 | S(x)$. Thus, the linear complexity of $\{s_n\}_{n\ge0}$ over $\mathbb{F}_2$ is $LC(\{s_n\}_{n\ge0}) \le 351$ from Theorem 1 2). In addition, from Proposition 1 in [10], it is clear that the multiplicity of 1 as a root of $S(x)$ is 2, so, $LC(\{s_n\}_{n\ge0}) \le 350$. In fact, it follows that $\gcd(x^{360} - 1, S(x)) = (x-1)^2(x^2+x+1)^6(x^4+x^3+x^2+x+1)^4(x^6+x^3+1)^2$, that is, $LC(\{s_n\}_{n\ge0}) = 318$.

Remark 2: 1) In the proof of Theorem 1, we make full use of the formulas in Appendix B for the cyclotomic numbers of order $2r$ over $\mathbb{F}_q$ with $q = p^{uv} \equiv 1 \pmod{2r}$, where the order v of p modulo r is only even. Unfortunately, when v is odd, the cyclotomic problem is more intricate [27]. 2) In general, the determination of cyclotomic numbers of order e is difficult if e is not small [10], meaning that we can only utilize these formulas for small r. Here we consider the cases $r = 3$ and 5 as examples.

B. Ternary Case

In this subsection, let $q \equiv 1 \pmod 3$ where q is a prime. For the trivial root 1, the primitive 2nd and 3rd roots of unity, the multiplicities of them as the roots of $S(x)$ are determined in Propositions 1, 2 and 3, respectively, by using the cyclotomic numbers of orders e's (e.g, 3, 6 and 9). However, if e is not small, it is very difficult to calculate the cyclotomic numbers, so the determined values of the multiplicity R are not very large in these propositions. For all that, Theorem 2 and Corollary 2 present the $\mathbb{F}_3$-linear complexities of the ternary Sidelnikov sequences, especially in the case of $q = 2 \times 3^\lambda + 1$ where λ is a positive integer.

Firstly, we determine the multiplicities of the trivial root 1 of unity, as a root of $S(x)$, in the case of Ind $3 \equiv 0 \pmod 3$.

Proposition 1: Let $q \equiv 1 \pmod 3$ be a prime where $4q = c^2 + 27d^2$ and $c \equiv 1 \pmod 3$. Let $q = (\sum_{i=0}^{5} c_i\xi^i)(\sum_{i=0}^{5} c_i\xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$ and $c_i (i = 1, 2, \ldots, 5)$ are integers. $S(x)$ is the generating function of a ternary Sidelnikov sequence $\{s_n\}_{0\le n\le q-2}$. Then in the case of Ind $3 \equiv 0 \pmod 3$, the multiplicity (R) of 1 as a root of $S(x)$ can be determined by

1) $R(1) = 1$ is trivial;

2) $R(1) = 2$ if and only if $q \equiv 1 \pmod 9$;

3) $R(1) = 3$ if and only if $q \equiv 1 \pmod 9$ and $d \equiv 0 \pmod 3$;

4) $R(1) = 4$ if and only if $q \equiv 1 \pmod 9$, $d \equiv 0 \pmod 3$, and $c_1 + c_5 \equiv 2(c_2 + c_4) \pmod 9$;

5) $R(1) = 5$ *or* 6 if and only if $q \equiv 1 \pmod 9$, $d \equiv 0 \pmod 3$, $c_1 + c_5 \equiv 2(c_2 + c_4) \pmod 9$, and $c_4 \equiv 2c_1 \pmod 9$;

6) $R(1) = 7$ if and only if $q \equiv 1 \pmod 9$, $d \equiv 0 \pmod 3$, $c_1 + c_5 \equiv 2(c_2 + c_4) \pmod 9$, $c_4 = 2c_1 \pmod 9$, and $c_3 + c_4 + c_5 \equiv 0 \pmod 9$;

7) $R(1) = 8$ if and only if $q \equiv 1 \pmod 9$, $d \equiv 0 \pmod 3$, $c_1 + c_5 \equiv 2(c_2 + c_4) \pmod 9$, $c_4 \equiv 2c_1 \pmod 9$, $c_3 + c_4 + c_5 \equiv 0 \pmod 9$, and $1 + c_0 + c_2 + 2c_4 \equiv 0 \pmod 9$;

8) $R(1) = 9$ if and only if $q \equiv 1 \pmod 9$, $d \equiv 0 \pmod 3$, and $c_0 \equiv -1 + 2c_5, c_1 \equiv -c_5, c_2 \equiv 2c_5, c_3 \equiv c_5, c_4 \equiv -2c_5 \pmod 9$.

Proof: Let $M = 3$. According to Appendix C, we have from (12) in Lemma 3 that $S(1) = (0,1)_3 + (1,1)_3 + (2,1)_3 + 2((0,2)_3 + (1,2)_3 + (2,2)_3) = 3(B + C + D) \equiv 0 \pmod 3$, that is to say, 1 is always a root of $S(x)$.

According to Lemma 3, let $l = 1$ if $t = 1$ or 2. From (13), $S(1)^{(1)} = (1,1)_3 + 2(2,1)_3 + 2(1,2)_3 + 4(2,2)_3 = B + C + D = \frac{q-1}{3}$ and $S(1)^{(2)} = (2,1)_3 + 2(2,2)_3 = 2B + D = \frac{q-1}{3} - d$. Thus, $S(1)^{(1)} = 0$ if and only if $q \equiv 1 \pmod 9$, and $S(1)^{(2)} = 0$ if and only if $q \equiv 1 \pmod 9$ and $d \equiv 0 \pmod 3$.

Similarly, let $l = 2$ if $t = 3, 4, 5, 6, 7, 8$. From (13),

$$S(1)^{(t)} = \sum_{k=1}^{2} k \sum_{i=t}^{9-1} \binom{i}{t} \sum_{j=0}^{3-1} (i, 3j + k)_9. \tag{18}$$

Let $q = (\sum_{i=0}^{5} c_i \xi^i)(\sum_{i=0}^{5} c_i \xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$ and $c_i (i = 1, 2, \dots, 5)$ are integers. In the case Ind $3 \equiv 0 \pmod 3$, according to Appendix E, it follows that

$$\begin{aligned}
&S(1)^{(3)} \\
\equiv&(3,1)_9 + (3,4)_9 + (3,7)_9 + (4,1)_9 + (4,4)_9 + (4,7)_9 + (5,1)_9 \\
&+(5,4)_9 + (5,7)_9 + 2(6,1)_9 + 2(6,4)_9 + 2(6,7)_9 + 2(7,1)_9 \\
&+2(7,4)_9 + 2(7,7)_9 + 2(8,1)_9 + 2(8,4)_9 + 2(8,7)_9 + 2(3,2)_9 \\
&+2(3,5)_9 + 2(3,8)_9 + 2(4,2)_9 + 2(4,5)_9 + 2(4,8)_9 + 2(5,2)_9 \\
&+2(5,5)_9 + 2(5,8)_9 + (6,2)_9 + (6,5)_9 + (6,8)_9 + (7,2)_9 \\
&+(7,5)_9 + (7,8)_9 + (8,2)_9 + (8,5)_9 + (8,8)_9 \pmod 3 \\
\equiv&B + 2C + 2E + F + 2J + K + M + 2N + 2P + 2Q + 2R \\
&\pmod 3 \\
\equiv&\frac{c_1 - 2c_2 - 2c_4 + c_5}{3} \pmod 3, \qquad (19) \\
&S(1)^{(4)} \\
\equiv&(4,1)_9 + (4,4)_9 + (4,7)_9 + 2(5,1)_9 + 2(5,4)_9 + 2(5,7)_9 \\
&+2(7,1)_9 + 2(7,4)_9 + 2(7,7)_9 + (8,1)_9 + (8,4)_9 + (8,8)_9 \\
&+2(4,2)_9 + 2(4,5)_9 + 2(4,8)_9 + (5,2)_9 + (5,5)_9 + (5,8)_9 \\
&+(7,2)_9 + (7,5)_9 + (7,8)_9 + 2(8,2)_9 + 2(8,5)_9 + 2(8,8)_9 \\
&\pmod 3 \\
\equiv&2B + 2C + E + F + 2K + M + 2P + R \pmod 3 \\
\equiv&\frac{-2c_1 + c_4}{3} \pmod 3, \qquad (20) \\
&S(1)^{(5)} \\
\equiv&(5,1)_9 + (5,4)_9 + (5,7)_9 + 2(8,1)_9 + 2(8,4)_9 + 2(8,7)_9 \\
&+2(5,2)_9 + 2(5,5)_9 + 2(5,8)_9 + (8,2)_9 + (8,5)_9 + (8,8)_9 \\
&\pmod 3 \\
\equiv&B + 2E + J + K + N + Q + 2R \pmod 3 \\
\equiv&\frac{3c_1 - 2c_2 - 3c_4 + c_5}{6} \pmod 3, \qquad (21) \\
&S(1)^{(6)} \\
\equiv&(6,1)_9 + (6,4)_9 + (6,7)_9 + (7,1)_9 + (7,4)_9 + (7,7)_9 + (8,1)_9 \\
&+(8,4)_9 + (8,7)_9 + 2(6,2)_9 + 2(6,5)_9 + 2(6,8)_9 + 2(7,2)_9 \\
&+2(7,5)_9 + 2(7,8)_9 + 2(8,2)_9 + 2(8,5)_9 + 2(8,8)_9 \pmod 3 \\
\equiv&2B + C + J + 2M + N + Q + R \pmod 3 \\
\equiv&\frac{c_1 + 2c_2 - 2c_3 - c_4 - 3c_5}{6} \pmod 3, \qquad (22) \\
&S(1)^{(7)} \\
\equiv&(7,1)_9 + (7,4)_9 + (7,7)_9 + 2(8,1)_9 + 2(8,4)_9 + 2(8,7)_9 \\
&+2(7,2)_9 + 2(7,5)_9 + 2(7,8)_9 + (8,2)_9 + (8,5)_9 + (8,8)_9 \\
&\pmod 3 \\
\equiv&B + C + K + 2N + O + P + Q + S \pmod 3 \\
\equiv&\frac{2 + 2c_0 - 4c_1 - 4c_2 - c_3 + 5c_4 + 2c_5}{18} \pmod 3, \qquad (23) \\
&S(1)^{(8)} \\
\equiv&(8,1)_9 + (8,4)_9 + (8,7)_9 + 2(8,2)_9 + 2(8,5)_9 + 2(8,8)_9 \\
\equiv&2B + 2J + 2K + N + 2O \pmod 3 \\
\equiv&\frac{-2 - 2c_0 + 7c_1 - 2c_2 + 4c_3 - 5c_4 + c_5}{9} \pmod 3. \qquad (24)
\end{aligned}$$

So, $S(1)^{(3)} = 0$ if and only if $c_1 + c_5 \equiv 2(c_2 + c_4) \pmod 9$. $S(1)^{(4)} = 0$ if and only if $2c_1 \equiv c_4 \pmod 9$. $S(1)^{(5)} = 0$ if and only if $c_2 + c_5 \equiv 3(c_2 + c_4 - c_1) \pmod{18}$. Fortunately, $S(1)^{(3)} = 0$ and $S(1)^{(4)} = 0$ imply that $S(1)^{(5)} = 0$. $S(1)^{(6)} = 0$ if and only if $c_4 + c_5 - c_1 \equiv 2(c_2 - c_3 - c_5) \pmod{18}$. However, it follows from (19), (20), and (22) that $c_3 + c_4 + c_5 \equiv 0 \pmod 9$. $S(1)^{(7)} = 0$ if and only if $2(1+c_0+c_5)+c_4 \equiv 4(c_1+c_2-c_4)+c_3 \pmod{54}$. From (19), (20), (22), and (23), it can be reduced to $1+c_0+c_2+2c_4 \equiv 0 \pmod 9$. $S(1)^{(8)} = 0$ if and only if $2(1 + c_0 + c_2) + 5c_4 \equiv 7c_1+4c_3+c_5 \pmod{27}$. Similarly, from (19), (20), (22), (23), and (24), we have $c_0 \equiv -1 + 2c_5, c_1 \equiv -c_5, c_2 \equiv 2c_5, c_3 \equiv c_5, c_4 \equiv -2c_5 \pmod 9$. □

Secondly, note that if $q \equiv 1 \pmod 2$, then $2^{q-1} - 1 \equiv 0 \pmod 3$, which implies that 2 is a root of $x^{q-1} - 1$ over $\mathbb{F}_3 = \{0, 1, 2\}$. In the following proposition, the multiplicity of 2 as a root of $S(x)$ is presented for the case that $q \equiv 1 \pmod 6$ where $q = a^2 + 3b^2$ and $a \equiv 1 \pmod 3$.

Proposition 2: Let $q = 6f + 1$ be a prime where $q = a^2 + 3b^2$ and $a \equiv 1 \pmod 3$. Let $\gamma\ (\neq 1)$ be a primitive 2nd root of unity over $\mathbb{F}_3$. $S(x)$ is the generating function of a ternary Sidelnikov sequence $\{s_n\}_{0 \le n \le q-2}$. Then in the case of f being even, the multiplicity (R) of γ as a root of $S(x)$ can be determined by

1) $R(\gamma) = 1$ *or* 2 if and only if $b \equiv 0 \pmod 3$;
2) (see the bottom line of the next page.)

Proof: Let $q = 6f + 1$ where f is even. Since $\gamma \neq 1$ and $\gamma^2 = 1$, $1 + \gamma = 0$. The Appendix D lists the cyclotomic numbers of order 6, which distinguish among the following three cases: Ind $2 \equiv 0 \pmod 6$, Ind $2 \equiv 2$ or $5 \pmod 6$, and Ind $2 \equiv 1$ or $4 \pmod 6$. Let $M = 3$ and $r = 2$.

We will determine the multiplicities of γ as a root of $S(x)$ using Appendix D.

1) First, consider the case $R(\gamma)=1$. From (14a), it follows that

$$\begin{aligned} S(\gamma) &= \sum_{k=1}^{3-1} k \sum_{h=0}^{2-1}\sum_{j=0}^{2-1}\sum_{i=0}^{3-1}(2i+h,3j+k)_6\gamma^h \\ &= \sum_{h=0}^{1}\sum_{j=0}^{1}\sum_{i=0}^{2}((2i+h,3j+1)_6+2(2i+h,3j+2)_6)\gamma^h \\ &= \sum_{h=1}^{1} T_{(0,h)}\gamma^h, \end{aligned}$$

where $T_{(0,h)}=\sum_{j=0}^{1}\sum_{i=0}^{2}((2i+h,3j+1)_6+2(2i+h,3j+2)_6-(2i,3j+1)_6-2(2i,3j+2)_6)$. According to Appendix D,

$$\begin{aligned} T_{(0,1)} &\equiv (1,1)_6+2(1,2)_6-(0,1)_6-2(0,2)_6+(3,1)_6 \\ &\quad +2(3,2)_6-(2,1)_6-2(2,2)_6+(5,1)_6+2(5,2)_6 \\ &\quad -(4,1)_6-2(4,2)_6+(1,4)_6+2(1,5)_6-(0,4)_6 \\ &\quad -2(0,5)_6+(3,4)_6+2(3,5)_6-(2,4)_6-2(2,5)_6 \\ &\quad +(5,4)_6+2(5,5)_6-(4,4)_6-2(4,5)_6 \\ &\equiv B-F-H+I \pmod 3 \\ &= \begin{cases} b & \text{if Ind } 2\equiv 0 \pmod 6 \\ b & \text{if Ind } 2\equiv 2 \text{ or } 5 \pmod 6 \\ b & \text{if Ind } 2\equiv 1 \text{ or } 4 \pmod 6 \end{cases} \\ &\equiv 0 \pmod 3 \text{ for all cases if } b\equiv 0 \pmod 3, \end{aligned}$$

which implies that γ is a single root of $S(x)$ if and only if $b\equiv 0 \pmod 3$.

Second, consider the case $R(\gamma)=2$. From (15a), it follows that

$$\begin{aligned} &S(\gamma)^{(1)} \\ &=\sum_{k=1}^{3-1} k\sum_{i=1}^{3-1}\binom{i}{1}\sum_{h=0}^{2-1}\sum_{j=0}^{2-1}(u(i,h),3j+k)_6\gamma^h \\ &=\sum_{h=0}^{1}\sum_{i=1}^{2}\binom{i}{1}\sum_{j=0}^{1}((u(i,h),3j+1)_6+2(u(i,h),3j+2)_6)\gamma^h \\ &=\sum_{h=1}^{1}T_{(1,h)}\gamma^h, \end{aligned}$$

where $u(i,h)$ is the unique integer u with $0\le u\le 5$, $u-1\equiv h \pmod 2$, and $u\equiv i \pmod 3$; $T_{(1,h)}=\sum_{j=0}^{1}((u(1,h),3j+1)_6+2(u(1,h),3j+2)_6+2(u(2,h),3j+1)_6+4(u(2,h),3j+2)_6-(1,3j+1)_6-2(1,3j+2)_6-2(5,3j+1)_6-4(5,3j+2)_6)$. According to Appendix D, it follows that

$$\begin{aligned} T_{(1,1)} &\equiv \sum_{j=0}^{1}((4,3j+1)_6+2(4,3j+2)_6+2(2,3j+1)_6 \\ &\quad +4(2,3j+2)_6-(1,3j+1)_6-2(1,3j+2)_6 \\ &\quad -2(5,3j+1)_6-4(5,3j+2)_6) \\ &\equiv J-G+E-F+C-B \pmod 3 \\ &= \begin{cases} 0 & \text{if Ind } 2\equiv 0 \pmod 6 \\ 0 & \text{if Ind } 2\equiv 2 \text{ or } 5 \pmod 6 \\ 0 & \text{if Ind } 2\equiv 1 \text{ or } 4 \pmod 6 \end{cases} \\ &\equiv 0 \pmod 3, \end{aligned}$$

which implies that if γ is a root of $S(x)$, it must be a double root of $S(x)$.

2) Consider the case $R(\gamma)=3$. Similar to above,

$$\begin{aligned} &S(\gamma)^{(2)} \\ &=\sum_{k=1}^{3-1} k\sum_{i=2}^{3-1}\binom{i}{2}\sum_{h=0}^{2-1}\sum_{j=0}^{2-1}(u(i,h),3j+k)_6\gamma^h \\ &=\sum_{h=0}^{1}\sum_{i=2}^{2}\binom{i}{2}\sum_{j=0}^{1}((u(i,h),3j+1)_6+2(u(i,h),3j+2)_6)\gamma^h \\ &=\sum_{h=0}^{1}\sum_{j=0}^{1}((u(2,h),3j+1)_6+2(u(2,h),3j+2)_6)\gamma^h \\ &=\sum_{h=1}^{1}T_{(2,h)}\gamma^h, \end{aligned}$$

where $T_{(2,h)}=\sum_{j=0}^{1}((u(2,h),3j+1)_6+2(u(2,h),3j+2)_6-(u(2,0),3j+1)_6-2(u(2,0),3j+2)_6)$. According to Appendix D, it follows that

$$\begin{aligned} &T_{(2,1)} \\ &=\sum_{j=0}^{1}((5,3j+1)_6+2(5,3j+2)_6-(2,3j+1)_6-2(2,3j+2)_6) \\ &\equiv E-B+G-J \pmod 3 \\ &=\begin{cases} \frac{-2b}{3} & \text{if Ind } 2\equiv 0 \pmod 6 \\ \frac{-a+b}{3} & \text{if Ind } 2\equiv 2 \text{ or } 5 \pmod 6 \\ \frac{-2a-2b}{3} & \text{if Ind } 2\equiv 1 \text{ or } 4 \pmod 6 \end{cases} \\ &\equiv\begin{cases} 0 \pmod 3 & \text{if Ind } 2\equiv 0 \pmod 6 \text{ and } b\equiv 0 \pmod 9 \\ 0 \pmod 3 & \text{if Ind } 2\equiv 2 \text{ or } 5 \pmod 6 \\ & \quad \text{and } a\equiv b \pmod 9 \\ 0 \pmod 3 & \text{if Ind } 2\equiv 1 \text{ or } 4 \pmod 6 \\ & \quad \text{and } a\equiv -b \pmod 9), \end{cases} \end{aligned}$$

which completes the proof. □

Thirdly, it is worth noting from Proposition 1 that $q\equiv 1 \pmod 9$ is one of necessary and sufficient conditions of 1 as a multiple root of $S(x)$. Then, we are interested in the multiplicity of γ (a primitive 3rd root of unity in an extension field of $\mathbb{F}_3$) as a root of $S(x)$.

Proposition 3: Let $q\equiv 1 \pmod 9$ be a prime where $4q=c^2+27d^2$ and $c\equiv 7 \pmod 9$.

$$R(\gamma)=3 \text{ if and only if } \begin{cases} b\equiv 0 \pmod 9 & \text{if Ind } 2\equiv 0 \pmod 6, \\ a\equiv b \pmod 9 \text{ and } b\equiv 0 \pmod 3 & \text{if Ind } 2\equiv 2 \text{ or } 5 \pmod 6, \\ a\equiv -b \pmod 9 \text{ and } b\equiv 0 \pmod 3 & \text{if Ind } 2\equiv 1 \text{ or } 4 \pmod 6, \end{cases}$$

where Ind 2 means the index of 2 to a base g modulo q.

Let $q=(\sum_{i=0}^{5}c_i\xi^i)(\sum_{i=0}^{5}c_i\xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$ and $c_i (i=1,2,\ldots,5)$ are integers. Let $\gamma\ (\neq 1)$ be a primitive 3rd root of unity in an extension field of $\mathbb{F}_3$. $S(x)$ is the generating function of a ternary Sidelnikov sequence $\{s_n\}_{0\leq n\leq q-2}$. Then, the multiplicity (R) of γ as a root of $S(x)$ can be determined by

1) $R(\gamma)=1$ if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 1 \pmod 2$, or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 2$;

2) $R(\gamma)=2$ or 3 if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$, or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$;

3) $R(\gamma)=4$ if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$(or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$), and $c_4\equiv 2c_1 \pmod 9$ and $c_5\equiv 3c_1+2c_2 \pmod{18}$;

4) $R(\gamma)=5$ if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$(or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$), and $c_1\equiv c_2\equiv c_4\equiv c_5\equiv 0 \pmod 9$.

Proof: Since $\gamma\ (\neq 1)$ is a primitive 3rd root of unity, $1+\gamma+\gamma^2=0$.

1) From (14b), we get

$$\begin{aligned}S(\gamma) &= \sum_{k=1}^{3-1}k\sum_{h=0}^{3-1}(h,k)_3\gamma^h=\sum_{h=0}^{2}((h,1)_3+2(h,2)_3)\gamma^h\\ &= \sum_{h=1}^{2}T_{(0,h)}\gamma^h,\end{aligned}$$

where $T_{(0,h)}=(h,1)_3+2(h,2)_3-(0,1)_3-2(0,2)_3$. Let $T_{(0,1)},T_{(0,2)}\equiv 0 \pmod 3$, and then according to Appendix C,

$$\begin{cases} T_{(0,1)}=\frac{2+c}{3}\equiv 0 \pmod 3\\ T_{(0,2)}=\frac{2+c-9d}{6}\equiv 0 \pmod 3.\end{cases}$$

Then, $S(\gamma)=0$ if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 1 \pmod 2$, or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 2$.

2) According to Lemma 3, let $l=1$ since $t=1$. Then $M^{l-1}-\lceil\frac{k+1}{M}\rceil=0$. From (15b),

$$\begin{aligned}S(\gamma)^{(1)} &=\sum_{k=1}^{3-1}k\sum_{i=1}^{3-1}\binom{i}{1}\sum_{h=0}^{3-1}(u(i,h),k)_3\gamma^h\\ &=\sum_{h=0}^{2}\sum_{i=1}^{2}\binom{i}{1}((u(i,h),1)_3+2(u(i,h),2)_3)\gamma^h\\ &=\sum_{h=1}^{2}\sum_{i=1}^{2}\binom{i}{1}((u(i,h),1)_3+2(u(i,h),2)_3\\ &\quad-(u(i,0),1)_3-2(u(i,0),2)_3)\gamma^h\\ &=\sum_{h=1}^{2}T_{(1,h)}\gamma^h,\end{aligned}$$

where $u(i,h)$ is the unique integer u with $0\leq u\leq 2$, $u-1\equiv h \pmod 3$, and $u\equiv i \pmod 3$. Let $T_{(1,1)}=0$ and $T_{(1,2)}=0$. It follows from Appendix C that

$$\begin{aligned}T_{(1,1)} &= -(1,1)_3-2(1,2)_3+2(2,1)_3+4(2,2)_3\\ &\equiv B-C \pmod 3\\ &\equiv -d \pmod 3),\\ T_{(1,2)}&=-(1,1)_3-2(1,2)_3\\ &\equiv -C-2D \pmod 3\\ &\equiv \frac{-2q-c-3d}{6} \pmod 3).\end{aligned}$$

Thus, $S(\gamma)^{(1)}=0$ if and only if $d\equiv 0 \pmod 3$ and $-2q-c-3d\equiv 0 \pmod{18}$. From $S(\gamma)=0$ and $S(\gamma)^{(1)}=0$, it follows that $R(\gamma)=2$ if and only if $c\equiv 7 \pmod{18}$ and $d\equiv 1 \pmod 2$, or $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 2$.

Similarly, let $l=1$ since $t=2$. It follows from (15b) that

$$\begin{aligned}S(\gamma)^{(2)} &= \sum_{k=1}^{2}k\sum_{i=2}^{2}\binom{i}{2}\sum_{h=0}^{2}(u(i,h),k)_3\gamma^h\\ &= \sum_{h=0}^{2}((u(2,h),1)_3+2(u(2,h),2)_3)\gamma^h\\ &= \sum_{h=1}^{2}T_{(2,h)}\gamma^h,\end{aligned}$$

where $T_{(2,h)}=(u(2,h),1)_3+2(u(2,h),2)_3-(u(2,0),1)_3-2(u(2,0),2)_3$. Let $T_{(2,h)}=0$ $(h=1,2)$. Then

$$\begin{aligned}T_{(2,1)}=T_{(2,2)} &= -(2,1)_3-2(2,2)_3\\ &\equiv -D-2B \pmod 3\\ &\equiv -\frac{q-1-3d}{3} \pmod 3).\end{aligned}$$

Thus, $S(\gamma)^{(2)}=0$ if and only if $q-1-3d\equiv 0 \pmod 9$, that is, $S(\gamma)^{(2)}=0$ if and only if $d\equiv 0 \pmod 3$. It is clear that $S(\gamma)^{(1)}=0$ implies $S(\gamma)^{(2)}=0$.

3) According to Lemma 3, let $l=2$ since $t=3$. From (15b),

$$\begin{aligned}&S(\gamma)^{(3)}\\ &=\sum_{k=1}^{2}k\sum_{i=3}^{8}\binom{i}{3}\sum_{h=0}^{2}\sum_{j=0}^{3-1}(u(i,h),3j+k)_9\gamma^h\\ &=\sum_{h=0}^{2}\sum_{j=0}^{2}\sum_{i=3}^{8}\binom{i}{3}((u(i,h),3j+1)_9+2(u(i,h),3j+2)_9)\gamma^h\\ &=\sum_{h=1}^{2}T_{(3,h)}\gamma^h,\end{aligned}$$

where

$$\begin{aligned}&T_{(3,h)}\\ &=\sum_{j=0}^{2}\sum_{i=3}^{8}\binom{i}{3}((u(i,h),3j+1)_9+2(u(i,h),3j+2)_9\\ &\quad-(u(i,0),3j+1)_9-2(u(i,0),3j+2)_9),\end{aligned}$$

where $u(i,h)$ is the unique integer u with $0\leq u\leq 8$, $u-1\equiv h \pmod 3$, and $u\equiv i \pmod 9$. Let $T_{(3,h)}=0$ for $h=1,2$. According to Appendix E,

$$\begin{aligned}&T_{(3,1)}\\ &=\sum_{j=0}^{2}(\binom{4}{3}(4,3j+1)_9+\binom{7}{3}(7,3j+1)_9+2\binom{4}{3}(4,3j+2)_9\\ &\quad+2\binom{7}{3}(7,3j+2)_9-\binom{3}{3}(3,3j+1)_9-\binom{6}{3}(6,3j+1)_9\end{aligned}$$

$$
\begin{aligned}
&-2\binom{3}{3}(3,3j+2)_9-2\binom{6}{3}(6,3j+2)_9)\\
\equiv&2C+F+J-2M+N-P+Q \pmod 3\\
=&\frac{-c_1-2c_2-c_4+c_5}{6}\\
\equiv&0 \pmod 3,
\end{aligned}
$$

$$
\begin{aligned}
&T_{(3,2)}\\
=&\sum_{j=0}^{2}(\binom{5}{3}(5,3j+1)_9+\binom{8}{3}(8,3j+1)_9+2\binom{5}{3}(5,3j+2)_9\\
&+2\binom{8}{3}(8,3j+2)_9-\binom{3}{3}(3,3j+1)_9-\binom{6}{3}(6,3j+1)_9\\
&-2\binom{3}{3}(3,3j+2)_9-2\binom{6}{3}(6,3j+2)_9)\\
\equiv&B+2E+J+K+N+Q-R \pmod 3\\
=&\frac{3c_1-2c_2-3c_4+c_5}{6}\\
\equiv&0 \pmod 3.
\end{aligned}
$$

Thus, $S(\gamma)^{(3)}=0$ if and only if $c_4\equiv 2c_1 \pmod 9$ and $c_5\equiv 3c_1+2c_2 \pmod{18}$.

4) Similar to 3), let $l=2$ since $t=4$. From (15b),

$$
\begin{aligned}
&S(\gamma)^{(4)}\\
=&\sum_{k=1}^{2}k\sum_{i=4}^{8}\binom{i}{4}\sum_{h=0}^{2}\sum_{j=0}^{3-1}(u(i,h),3j+k)_9\gamma^h\\
=&\sum_{h=0}^{2}\sum_{j=0}^{2}\sum_{i=4}^{8}\binom{i}{4}((u(i,h),3j+1)_9+2(u(i,h),3j+2)_9)\gamma^h\\
=&\sum_{h=1}^{2}T_{(4,h)}\gamma^h.
\end{aligned}
$$

Let $T_{(4,h)}=0$ for $h=1,2$.

$$
\begin{aligned}
&T_{(4,1)}\\
=&\sum_{j=0}^{2}(\binom{5}{4}(5,3j+1)_9+\binom{8}{4}(8,3j+1)_9+2\binom{5}{4}(5,3j+2)_9\\
&+2\binom{8}{4}(8,3j+2)_9-\binom{4}{4}(4,3j+1)_9-\binom{7}{4}(7,3j+1)_9\\
&-2\binom{4}{4}(4,3j+2)_9-2\binom{7}{4}(7,3j+2)_9)\\
\equiv&2B-2C+E-F+J+2K-M+N-2P-2Q+R \pmod 3\\
=&\frac{c_1+4c_2+c_4-5c_5}{6}\\
\equiv&0 \pmod 3,
\end{aligned}
$$

$$
\begin{aligned}
&T_{(4,2)}\\
=&\sum_{j=0}^{2}(\binom{6}{4}(6,3j+1)_9+2\binom{6}{4}(6,3j+2)_9-\binom{4}{4}(4,3j+1)_9\\
&-\binom{7}{4}(7,3j+1)_9-2\binom{4}{4}(4,3j+2)_9-2\binom{7}{4}(7,3j+2)_9)\\
\equiv&-2C-F-J+2M-N-2P-Q \pmod 3\\
=&\frac{2c_1+c_2-c_4-2c_5}{3}\\
\equiv&0 \pmod 3.
\end{aligned}
$$

Thus, $S(\gamma)^{(4)}=0$ if and only if $c_1+c_4-c_5\equiv 4(c_5-c_2) \pmod{18}$ and $2(c_1-c_5)\equiv c_4-c_2 \pmod 9$. Solving the simultaneous equations $c_4\equiv 2c_1 \pmod 9$, $c_5\equiv 3c_1+2c_2 \pmod{18}$, $c_1+c_4-c_5\equiv 4(c_5-c_2) \pmod{18}$ and $2(c_1-c_5)\equiv c_4-c_2 \pmod 9$, we get $c_1\equiv c_2\equiv c_4\equiv c_5\equiv 0 \pmod 9$, which completes the proof. □

Combining Propositions 1 and 3 yields the following theorem.

Theorem 2: Let $q\equiv 1 \pmod 9$ be a prime where $4q=c^2+27d^2$ and $c\equiv 7 \pmod 9$. Let $q=(\sum_{i=0}^{5}c_i\xi^i)(\sum_{i=0}^{5}c_i\xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$. Then, in the case of Ind $3\equiv 0 \pmod 3$, the $\mathbb{F}_3$-linear complexity of the ternary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ of period $q-1$ is

1) $LC\leq q-4$ if $d\equiv 0 \pmod 3$;
2) $LC\leq q-10$ if $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$, or $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$;
3) $LC\leq q-15$ if $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$, or $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$; and $c_4\equiv 2c_1 \pmod 9$ and $c_5\equiv 3c_1+2c_2 \pmod{18}$;
4) $LC\leq q-17$ if $c\equiv 16 \pmod{18}$ and $d\equiv 0 \pmod 6$, or $c\equiv 7 \pmod{18}$ and $d\equiv 3 \pmod 6$; and $c_1\equiv c_2\equiv c_4\equiv c_5\equiv 0 \pmod 9$.

Proof: Let $q=9f+1$. Then $x^{q-1}-1\equiv(x^3-1)^{3f} \pmod 3$. It is clear that $f\geq 2$. Thus, the multiplicities of the 3rd roots γ ($\gamma^3=1$) as roots of $x^{q-1}-1$ are at least 6. Let $q=(\sum_{i=0}^{5}c_i\xi^i)(\sum_{i=0}^{5}c_i\xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$.

1) It is clear from Proposition 1 3).

2) From Proposition 3 2), it follows by solving the simultaneous equations $c+2\equiv 0 \pmod 9$, $d\equiv 0 \pmod 3$, and $2+c-9d\equiv 0 \pmod{18}$.

3) From Proposition 1 5) and Proposition 3 3), we have $c_4\equiv 2c_1 \pmod 9$ and $c_5\equiv 3c_1+2c_2 \pmod{18}$, which imply that $c_1+c_5\equiv 2(c_2+c_4)$. Thus, the result is true.

4) It is clear from Proposition 1 5) and Proposition 3 4). □

Example 6: Let $q=73$ and $M=3$. Then a ternary Sidelnikov sequence $\{s_n\}_{n\geq 0}$ of period 72 defined by $\alpha=5$ of $\mathbb{F}_{73}$ is represented as {2, 2, 1, 2, 2, 2, 1, 2, 0, 1, 0, 1, 0, 0, 0, 2, 1, 0, 1, 0, 2, 2, 2, 1, 2, 1, 2, 0, 1, 1, 2, 2, 0, 2, 1, 0, 0, 1, 0, 0, 1, 1, 2, 2, 0, 0, 0, 0, 0, 2, 1, 2, 0, 2, 1, 1, 0, 2, 1, 2, 0, 2, 2, 1, 1, 1, 1, 0, 1, 2, 2, 1}, and $2=\alpha^8$ and $3=\alpha^6$ over $\mathbb{F}_{73}=\{0,1,2,3,\ldots,72\}$, i.e., Ind $2\equiv 2 \pmod 6$ and Ind $3\equiv 0 \pmod 3$. From $4q=c^2+27d^2$ and $c\equiv 1 \pmod 3$, we have $c=7$ and $d=-3$. Then, according to Proposition 1 3) and Theorem 2 1), 1 is a triple root of $S(x)$. In addition, although 2 is a root of $x^{72}-1$, it is clear that 2 is not a root of $S(x)$ because $S(2)\equiv 2 \pmod 3$, which can also be further confirmed from Proposition 2 since $73=(-5)^2+3\times 4^2$ and $4\equiv 1 \pmod 3$. Thus, the linear complexity of this sequence

TABLE I

THE $\mathbb{F}_3$-LINEAR COMPLEXITIES OF TERNARY SIDELNIKOV SEQUENCES OF PERIOD $q-1=2\times 3^{\lambda}$ FOR $1\le\lambda\le 20$

λ	$q=2\times 3^{\lambda}+1$	LC	from Corollary 2	comments
1	7	5	1)	$b=d=1$
2	19	16	2)	$b=d=1$
3	55	-		no prime
4	163	160	2)	$b=7, d=1$
5	487	484	2)	$b=1, d=7$
6	1459	1454	3)	$b=15, d=10$ $\alpha=3$, and $\mathrm{Ind}_{\alpha}2\equiv 723$
7	4375	-	-	no prime
8	13123	-	-	no prime
9	39367	39362	3)	$b=33, d=22$ $\alpha=3$, and $\mathrm{Ind}_{\alpha}2\equiv 19674$
10	118099	-	-	no prime
11	354295	-	-	no prime
12	1062883	-	-	no prime
13	3188647	-	-	no prime
14	9565939	-	-	no prime
15	28697815	-	-	no prime
16	86093443	86093440	2)	$b=1591, d=2423$
17	258280327	$q^{1/2}-1\le LC\le q-7$	5)	$b=7281, d=4854, \alpha=5$ $\mathrm{Ind}_{\alpha}2\equiv 159499944$, and $\mathrm{Ind}_{\alpha}3\equiv 104564853$
18	774840979	-		no prime
19	2324522935	-		no prime
20	6973568803	-		no prime

Note: $\mathrm{Ind}_{\alpha}x$ is the index of $x\in\mathbb{F}_q$ to the base α modulo q.

is $LC\le 69$. In fact, we know that its linear complexity is exactly 69 since $\gcd(x^{72}-1,S(x))=(x-1)^3$, which means this upper bound is reachable.

Finally, for the special case of $q=2\times 3^{\lambda}+1$ where λ is an integer, the following corollary can be obtained, and Table I lists all examples for $1\le\lambda\le 20$. From this table, it is easy to see that the linear complexities of all sequences considered are extremely close to their periods.

Corollary 2: Let a prime $q=2\times 3^{\lambda}+1$ $(\lambda\ge 1)$. Let q have the decompositions $q=a^2+3b^2$ and $4q=c^2+27d^2$ where $a\equiv 1 \pmod 3$ and $c\equiv 1$ or $7 \pmod 9$. Let $q=(\sum_{i=0}^{5}c_i\xi^i)(\sum_{i=0}^{5}c_i\xi^{-i})$ where ξ is a primitive 9th root of unity of $\mathbb{F}_q$. Then, the $\mathbb{F}_3$-linear complexity of ternary Sidelnikov sequence $\{s_n\}_{n\ge 0}$ of period $q-1$ satisfies

1) $LC=q-2$ if $q=7$;

2) $LC=q-3$ if $q\equiv 1 \pmod 9$ and $b,d\not\equiv 0 \pmod 3$;

3) $LC=q-5$ if $q\equiv 1 \pmod 9$, $b\equiv 0, d\not\equiv 0 \pmod 3$, and Ind $2\equiv 0 \pmod 3$;

4) $LC\le q-6$ if $q\equiv 1 \pmod 9$, $b\equiv d\equiv 0 \pmod 3$, and Ind $2\equiv$ Ind $3\equiv 0 \pmod 3$. More precisely, it follows that

4-1) $LC=q-7$ if $c_1+c_5\equiv 2(c_2+c_4) \pmod 9$,

4-2) $LC=q-9$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1 \pmod 9$,

4-3) $LC=q-10$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1$, $c_3+c_4+c_5\equiv 0 \pmod 9$,

4-4) $LC=q-11$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1$, $c_3+c_4+c_5\equiv 0$, $1+c_0+c_2+2c_4\equiv 0 \pmod 9$,

4-5) $LC\le q-12$ if $c_0\equiv -1+2c_5, c_1\equiv -c_5, c_2\equiv 2c_5, c_3\equiv c_5, c_4\equiv -2c_5 \pmod 9$;

5) $LC\le q-7$ if $q\equiv 1 \pmod 9$, $b\equiv 0 \pmod 9$ and $d\equiv 0 \pmod 3$, and Ind $2\equiv$ Ind $3\equiv 0 \pmod 3$. More precisely, it follows that

5-1) $LC=q-8$ if $c_1+c_5\equiv 2(c_2+c_4) \pmod 9$,

5-2) $LC=q-10$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1 \pmod 9$,

5-3) $LC=q-11$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1$, $c_3+c_4+c_5\equiv 0 \pmod 9$,

5-4) $LC=q-12$ if $c_1+c_5\equiv 2(c_2+c_4)$, $c_4\equiv 2c_1$, $c_3+c_4+c_5\equiv 0$, $1+c_0+c_2+2c_4\equiv 0 \pmod 9$,

5-5) $LC\le q-13$ if $c_0\equiv -1+2c_5, c_1\equiv -c_5, c_2\equiv 2c_5, c_3\equiv c_5, c_4\equiv -2c_5 \pmod 9$.

IV. CONCLUSION

The main purpose of this paper is to give the Hasse derivative formulas to determine the multiplicity of γ, the primitive rth root of unity over $\mathbb{F}_M$ or in an extension field of $\mathbb{F}_M$, as a root of $S(x)$ which is the generating function of an M-ary Sidelnikov sequence $\{s_n\}_{0\le n\le q-2}$. In general, this proposed method can be used to determine the exact $\mathbb{F}_M$-linear complexity of the M-ary Sidelnikov sequence whenever the value of certain cyclotomic numbers and the factorization of $x^{q-1}-1$ over $\mathbb{F}_M$ are known. However, the well-known results on cyclotomic numbers are currently limited to the orders

$e \leq 24$. This limitation hinders our ability to calculate the multiplicity of γ if r is large. On the other hand, it is not easy to factorize the polynomial $x^{q-1}-1$ over $\mathbb{F}_M$. Based on the above, it seems that the determination of the exact $\mathbb{F}_M$-linear complexity of the M-ary Sidelnikov sequence is a difficult problem, especially when the characteristic of the field is a factor of the period of Sidelnikov sequence [9]. Nevertheless, one may determine the $\mathbb{Z}_4$-linear complexity of 4-ary Sidelnikov sequences when $q = 3 \cdot 4^{\lambda} + 1$ [28].

Appendices

Appendix A
The Cyclotomic Numbers of Order 2

Let $q = ef + 1$ be a prime power. When $e = 2$, the cyclotomic numbers are given in [25] by

(1) f even: $(0,0)_2 = (f-2)/2$; $(0,1)_2 = (1,0)_2 = (1,1)_2 = f/2$;

(2) f odd: $(0,0)_2 = (1,0)_2 = (1,1)_2 = (f-1)/2$; $(0,1)_2 = (f+1)/2$.

Appendix B
The Cyclotomic Numbers of Order $2r$

Let $q = p^m \equiv 1 \pmod{2r}$ for any prime p such that $m = uv$, $u \geq 1$, v is the order of p modulo r and v is even. Then, the cyclotomic numbers of order $2r$ over $\mathbb{F}_q$ are given in [27] by:

(1) $(0,j)_{2r} = (j,0)_{2r} = (j,j)_{2r}$;

(2) $4r^2A := 4r^2(0,0)_{2r} = q - 6r + 1 - (4r^2 - 6r + 2)(-1)^u q^{1/2}$;

(3) $4r^2B := 4r^2(0,j)_{2r} = q - 2r + 1 + 2(r-1)(-1)^u q^{1/2}$ for $j \not\equiv 0 \pmod{2r}$;

(4) $4r^2C := 4r^2(i,j)_{2r} = q + 1 - 2(-1)^u q^{1/2}$ for $i, j, i-j \not\equiv 0 \pmod{2r}$.

Appendix C
The Cyclotomic Numbers of Order 3

Let $q = ef + 1$ be a prime. When $e = 3$ and $4q = c^2 + 27d^2$ with $c \equiv 1 \pmod 3$, the cyclotomic numbers are given in [25] by

(1) $A := (0,0)_3 = (q - 8 + c)/9$;

(2) $B := (0,1)_3 = (1,0)_3 = (2,2)_3 = (2q - 4 - c - 9d)/18$;

(3) $C := (0,2)_3 = (1,1)_3 = (2,0)_3 = (2q - 4 - c + 9d)/18$;

(4) $D := (1,2)_3 = (2,1)_3 = (q + 1 + c)/9$.

Appendix D
The Cyclotomic Numbers of Order 6

Let $q = ef + 1$ be a prime. When $e = 6$ and $q = a^2 + 3b^2$ with $a \equiv 1 \pmod 3$, the cyclotomic numbers $(u,v)_6$ when f is even are given in Table II [29] by

I. Case Ind $2 \equiv 0 \pmod 6$
(1) $36A := (0,0)_6 = q - 17 - 20a$,
(2) $36B := (0,1)_6 = q - 5 + 4a + 18b$,
(3) $36C := (0,2)_6 = q - 5 + 4a + 6b$,
(4) $36D := (0,3)_6 = q - 5 + 4a$,
(5) $36E := (0,4)_6 = q - 5 + 4a - 6b$,
(6) $36F := (0,5)_6 = q - 5 + 4a - 18b$,
(7) $36G := (1,2)_6 = q + 1 - 2a$,
(8) $36H := (1,3)_6 = q + 1 - 2a$,
(9) $36I := (1,4)_6 = q + 1 - 2a$,
(10) $36J := (2,4)_6 = q + 1 - 2a$;
II. Case Ind $2 \equiv 2 (or\ 5) \pmod 6$
(1) $36A := (0,0)_6 = q - 17 - 8a - 6b$,
(2) $36B := (0,1)_6 = q - 5 + 4a + 6b$,
(3) $36C := (0,2)_6 = q - 5 - 8a$,
(4) $36D := (0,3)_6 = q - 5 + 4a + 6b$,
(5) $36E := (0,4)_6 = q - 5 + 4a + 6b$,
(6) $36F := (0,5)_6 = q - 5 + 4a - 12b$,
(7) $36G := (1,2)_6 = q + 1 - 2a + 6b$,
(8) $36H := (1,3)_6 = q + 1 - 2a - 12b$,
(9) $36I := (1,4)_6 = q + 1 - 2a + 6b$,
(10) $36J := (2,4)_6 = q + 1 + 10a - 6b$;
III. Case Ind $2 \equiv 1 (or\ 4) \pmod 6$
(1) $36A := (0,0)_6 = q - 17 - 8a + 6b$,
(2) $36B := (0,1)_6 = q - 5 + 4a + 12b$,
(3) $36C := (0,2)_6 = q - 5 + 4a - 6b$,
(4) $36D := (0,3)_6 = q - 5 + 4a - 6b$,
(5) $36E := (0,4)_6 = q - 5 - 8a$,
(6) $36F := (0,5)_6 = q - 5 + 4a - 6b$,
(7) $36G := (1,2)_6 = q + 1 - 2a - 6b$,
(8) $36H := (1,3)_6 = q + 1 - 2a - 6b$,
(9) $36I := (1,4)_6 = q + 1 - 2a + 12b$,
(10) $36J := (2,4)_6 = q + 1 + 10a + 6b$.

TABLE II
Cyclotomic Numbers of Order 6 and f Even

u	v					
	0	1	2	3	4	5
0	A	B	C	D	E	F
1	B	F	G	H	I	G
2	C	G	E	I	J	H
3	D	H	I	D	H	I
4	E	I	J	H	C	G
5	F	G	H	I	G	B

Appendix E
The Cyclotomic Numbers of Order 9

Let $q = ef + 1$ be a prime. When $e = 9$ and $4q = c^2 + 27d^2$ with $c \equiv 7 \pmod 9$, the cyclotomic numbers $(u,v)_9$ are given in Table III [21]. Each cyclotomic number is expressed as a constant plus a linear combination of $q, c, d, c_0, c_1, c_2, c_3, c_4,$ and c_5 where

$$q = (\sum_{i=0}^{5} c_i \xi^i)(\sum_{i=0}^{5} c_i \xi^{-i})$$

is a factorization of q in the field of 9th roots of unity, and ξ is a primitive 9th root of unity. The following cyclotomic numbers are only for Ind $3 \equiv 0 \pmod 3$.

TABLE III
CYCLOTOMIC NUMBERS OF ORDER 9

u	*v* 0	1	2	3	4	5	6	7	8
0	A	B	C	D	E	F	G	H	I
1	B	I	J	K	M	N	O	P	J
2	C	J	H	P	Q	R	S	Q	K
3	D	K	P	G	O	S	T	R	M
4	E	M	Q	O	F	N	R	S	N
5	F	N	R	S	N	E	M	Q	O
6	G	O	S	T	R	M	D	K	P
7	H	P	Q	R	S	Q	K	C	J
8	I	J	K	M	N	O	P	J	B

(1) $162A := 2q - 52 + 2c + 108c_0 - 54c_3$.

(2) $162B := 2q - 16 - c + 9d - 12c_0 + 42c_1 - 12c_2 + 24c_3 - 30c_4 + 24c_5$.

(3) $162C := 2q - 16 - c - 9d - 12c_0 + 24c_1 + 42c_2 - 12c_3 - 12c_4 - 12c_5$.

(4) $162D := 2q - 16 + 2c - 18c_0 + 36c_3$.

(5) $162E := 2q - 16 - c + 9d - 12c_0 - 12c_1 + 24c_2 + 24c_3 + 42c_4 - 12c_5$.

(6) $162F := 2q - 16 - c - 9d - 12c_0 - 12c_1 - 30c_2 - 12c_3 - 12c_4 + 42c_5$.

(7) $162G := 2q - 16 + 2c - 18c_0 - 18c_3$.

(8) $162H := 2q - 16 - c + 9d - 12c_0 - 30c_1 - 12c_2 + 24c_3 - 12c_4 - 12c_5$.

(9) $162I := 2q - 16 - c - 9d - 12c_0 - 12c_1 - 12c_2 - 12c_3 + 24c_4 - 30c_5$.

(10) $162J := 2q + 2 + 2c - 18c_1 + 18c_2$.

(11) $162K := 2q + 2 - c + 9d + 6c_0 + 6c_1 - 12c_2 - 12c_3 + 6c_4 + 6c_5$.

(12) $162M := 2q + 2 - c - 9d + 6c_0 - 12c_1 + 6c_2 + 6c_3 + 6c_4 + 6c_5$.

(13) $162N := 2q + 2 + 2c + 18c_1 - 18c_4 - 18c_5$.

(14) $162O := 2q + 2 - c + 9d + 6c_0 - 12c_1 + 6c_2 - 12c_3 + 6c_4 + 6c_5$.

(15) $162P := 2q + 2 - c - 9d + 6c_0 + 6c_1 - 12c_2 + 6c_3 + 6c_4 + 6c_5$.

(16) $162Q := 2q + 2 + 2c - 18c_2 + 18c_4 + 18c_5$.

(17) $162R := 2q + 2 - c + 9d + 6c_0 + 6c_1 + 6c_2 - 12c_3 - 12c_4 - 12c_5$.

(18) $162S := 2q + 2 - c - 9d + 6c_0 + 6c_1 + 6c_2 + 6c_3 - 12c_4 - 12c_5$.

(19) $162T := 2q + 2 + 2c$.

REFERENCES

[1] Y. Luo, C. Xing, and L. You, "Construction of sequences with high nonlinear complexity from function fields," *IEEE Trans. Inf. Theory*, vol. 63, no. 12, pp. 7646–7650, Dec. 2017.

[2] C. Ding, "Binary cyclotomic generators," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 1008, B. Preneel, Ed. Berlin, Germany: Springer, 1995, pp. 29–60.

[3] C. Ding and T. Helleseth, "On cyclotomic generator of order r," *Inf. Process. Lett.*, vol. 66, no. 1, pp. 21–25, Apr. 1998.

[4] Ş. Alaca and G. Millar, "Character values of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Cryptogr. Commun.*, vol. 9, no. 6, pp. 665–682, 2017.

[5] C. Ding, "Linear complexity of generalized cyclotomic binary sequences of order 2," *Finite Fields Appl.*, vol. 3, pp. 159–174, Apr. 1997.

[6] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Problemy Peredachi Informatsii*, vol. 5, no. 1, pp. 12–16, 1969.

[7] A. Lempel, M. Cohn, and W. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 38–42, Jan. 1997.

[8] T. Helleseth and K. Yang, "On binary sequences of period $n = p^m - 1$ with optimal autocorrelation," in *Sequences and Their Application*, T. Helleseth, P. Kummar, and E. K. Yang, Eds. London, U.K.: Springer, 2002, pp. 209–217.

[9] G. M. Kyureghyan and A. Pott, "On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences," *Des., Codes, Cryptogr.*, vol. 29, pp. 149–164, May 2003.

[10] W. Meldl and A. Winterhof, "Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences," *Des., Codes, Cryptogr.*, vol. 38, pp. 159–178, Feb. 2006.

[11] Q. Wang, "Linear complexity of binary cyclotomic sequences of order 6," *J. Appl. Math. Comput.*, vol. 49, nos. 1–2, pp. 119–125, Oct. 2015.

[12] M. Su, "On the linear complexity of Legendre–Sidelnikov sequences," *Des., Codes Cryptogr.*, vol. 74, no. 3, pp. 703–717, Mar. 2015.

[13] Z. Ye, P. Ke, and C. Wu, "A further study of the linear complexity of new binary cyclotomic sequence of length p^r," *Applicable Algebra Eng., Commun. Comput.*, vol. 30, pp. 217–231, Jun. 2019.

[14] Y. Liang, J. Cao, X. Chen, S. Cai, and X. Fan, "Linear complexity of Ding-Helleseth generalized cyclotomic sequences of order eight," *Cryptogr. Commun.*, vol. 11, pp. 1037–1056, Jan. 2019.

[15] M. Zeng, Y. Luo, M. K. Song, and H.-Y. Song, "The F_M-linear complexity of M-ary Sidel'nikov sequences of period $p-1 = f \cdot M^{\lambda}$," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 2274–2278.

[16] 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, Jun. 2003.

[17] 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, Jun./Jul. 2004.

[18] M. Z. Garaev, F. Luca, I. E. Shparlinski, and A. Winterhof, "On the lower bound of the linear complexity over $\mathbb{F}_p$ of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3299–3304, Jul. 2006.

[19] J. H. Chung and K. Yang, "Bounds on the linear complexity and the 1-error linear complexity over $\mathbb{F}_p$ of M-ary Sidel'nikov sequences," in *Proc. Int. Conf. Sequences Their Appl.*, Berlin, Germany, G. Gong, T. Helleseth, H. Song, and K. Yang, Eds., 2006, pp. 74–87.

[20] H. Aly and W. Meidl, "On the linear complexity and k-error linear complexity over $\mathbb{F}_p$ of the d-ary Sidel'nikov sequence," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4755–4761, Dec. 2007.

[21] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," *Math. Comput.*, vol. 21, no. 98, pp. 204–219, 1967.

[22] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303–3307, Sep. 2005.

[23] Z. X. Wan, *Algebra and Coding Theory*. Beijing, China: Science Press, 1979.

[24] H. Hasse, "Theorie der höheren differentiale in einem algebraischen funktionenkörper mit vollkommenem konstantenkörper bei beliebiger charakteristik," *J. Reine Angew. Math.*, vol. 175, pp. 50–54, Dec. 1936.

[25] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL, USA: Markham, 1967.

[26] P. Diaconis, J. He, and I. M. Isaacs, "The-square-and-add Markov chain," *Math. Intelligencer*, vol. 43, no. 2, pp. 27–36, Jun. 2021.

[27] N. Anuradha and S. A. Katre, "Number of points on the projective curves $aY^l = bX^l + cZ^l$ and $aY^{2l} = bX^{2l} + cZ^{2l}$ defined over finite fields, l an odd prime," *J. Number Theory*, vol. 77, no. 2, pp. 288–313, Aug. 1999.

[28] C. Fan and G. Ge, "A unified approach to Whiteman's and Ding-Helleseth's generalized cyclotomy over residue class rings," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1326–1336, Feb. 2014.

[29] L. E. Dickson, "Cyclotomy, higher congruences, and warning's problems," *Amer. J. Math.*, vol. 57, no. 2, pp. 391–424, Apr. 1935.

Min Zeng received the B.S. degree in mathematics from Central China Normal University, Wuhan, China, in 1988, and the M.S. and Ph.D. degrees in computer science and technology from Shanghai Jiao Tong University, Shanghai, China, in 2007 and 2015, respectively. He was a Post-Doctoral Researcher at the School of Electrical and Electronic Engineering, Yonsei University, from 2015 to 2017. He is currently with the School of Communication and Information Engineering, Shanghai Technical Institute of Electronics and Information. His research interests include sequences, coding theory, and artificial intelligence.

Yuan Luo (Member, IEEE) received the B.S. degree in applied mathematics and the M.S. and Ph.D. degrees in probability statistics from Nankai University, Tianjin, China, in 1993, 1996, and 1999, respectively. From July 1999 to April 2001, he held a post-doctoral position with the Institute of Systems Science, Chinese Academy of Sciences, Beijing, China. From May 2001 to April 2003, he held another post-doctoral position with the Institute for Experimental Mathematics, University of Duisburg-Essen, Essen, Germany. Since June 2003, he has been with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. Since 2006, he has been a Full Professor and the Vice Dean of the department from 2016 to 2018 and since 2021, respectively. His current research interests include coding theory, information theory, and big data analysis.

Guo-Sheng Hu received the M.S. degree in computer science from Sun Yat-sen University, Guangzhou, China, in 1995, and the Ph.D. degree in control theory and control engineering from the South China University of Technology, Guangzhou, in 2002. He is currently a Professor at the Department of Communication and Information Engineering, STIEI. His research focuses on signal processing and machine learning.

Hong-Yeop Song (Senior Member, IEEE) received the B.S. degree in electronic engineering from Yonsei University, Seoul, South Korea, in 1984, and the M.S.E.E. and Ph.D. degrees from the University of Southern California, Los Angeles, CA, USA, in 1986 and 1991, respectively. He spent two years as a Research Associate at USC and then two years as a Senior Engineer in standard team of Qualcomm Inc., San Diego, CA, USA. Since September 1995, he has been with the Department of Electrical and Electronic Engineering, Yonsei University. His research interests include digital communications and channel coding, design and analysis of various pseudo-random sequences for communications, and cryptography. He is a member of the National Academy of Engineering of Korea (NAEK), the Mathematical Association of America (MAA), the Korean Mathematical Society (KMS), KICS, IEIE, and KIISC. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society and the 2021 S. J. Choi Award from the Korean Government, both for his contribution to the global wide-spread of the fact that S. J. Choi (1646–1715) from South Korea had discovered a pair of orthogonal Latin squares of order nine much earlier than Euler. He has been serving for IEEE IT Society Seoul Chapter as the Chair from 2009 to 2016. He served as the General Co-Chair for IEEE ITW 2015, Jeju, South Korea.