On the Autocorrelation Distributions of Sidel'nikov Sequences

Young-Sik Kim, Jung-Soo Chung, Jong-Seon No, *Member, IEEE*, and Habong Chung, *Member, IEEE*

***Abstract*—For a prime p and positive integers M and n such that $M|p^n - 1$, Sidel'nikov introduced M-ary sequences (called *Sidel'nikov sequences*) of period $p^n - 1$, the out-of-phase autocorrelation magnitude of which is upper bounded by 4. In this correspondence, we derived the autocorrelation distributions, i.e., the values and the number of occurrences of each value of the autocorrelation function of Sidel'nikov sequences. The frequency of each autocorrelation value of an M-ary Sidel'nikov sequence is expressed in terms of the cyclotomic numbers of order M. It is also pointed out that the total number of distinct autocorrelation values is dependent not only on M but also on the period of the sequence, but always less than or equal to $\binom{M}{2} + 1$.**

***Index Terms*—Autocorrelation, autocorrelation distribution, cyclotomic numbers, M-ary sequences, Sidel'nikov sequences.**

I. Introduction

With the growing need of high-speed data communications, which usually adopt M-ary modulation schemes as a transmission standard, it becomes more important to find M-ary codes with good error correctability and M-ary sequences with good correlation property.

For a prime p and a positive integer M such that $M|p - 1$, Sidel'nikov [1] introduced the M-ary power residue sequences of period p with the magnitude of out-of-phase autocorrelation values upper-bounded by $\sqrt{5}$ or 3. For a positive integer n such that $M|p^n - 1$, he also constructed M-ary sequences (called *Sidel'nikov sequences*) of period $p^n - 1$, the out-of-phase autocorrelation magnitude of which is upper-bounded by 4 [1].

Later, Lempel, Cohn, and Eastman [2] introduced the binary Sidel'nikov sequences of period $p^n - 1$ without knowledge of the earlier work of Sidel'nikov. These binary sequences have near-ideal autocorrelation property which, under the condition of balancedness, is optimal. Recently, Helleseth, Kim, and No derived the linear complexity over F_p of binary Sidel'nikov sequences and their trace representation [3]. Green and Green [4], [5] introduced the polyphase Legendre sequences of prime period p, which later turned out to be the power residue sequences constructed by Sidel'nikov [1].

Boztas, Hammons, and Kumar [6] proposed quaternary sequences with near-optimum cross-correlation properties. And Kumar, Helleseth, Calderbank, and Hammons [7] constructed large families of quaternary sequences with low cross correlation. These sequences have relatively large magnitude of out-of-phase autocorrelation values, but low cross-correlation values.

Lee [8] devised a coding rule based on multiplicative characters of F_p for constructing the almost M-ary sequences with perfect periodic autocorrelation property. The term "almost M-ary" means that in a period of the sequence, the symbol "zero" occurs exactly once and all the other symbols are taken from the set of complex Mth roots of unity. Through the replacement of the symbol "zero" by any M-ary symbol, the almost M-ary Lee sequence can be easily transformed into an M-ary sequence, the magnitude of out-of-phase autocorrelation values of which is upper-bounded by 2 [9]. However, this sequence does not have the balance property.

Lüke, Schotten, and Hadinejad-Mahram [9], [10] introduced the generalized Sidel'nikov sequences, which are almost quaternary. These sequences have better autocorrelation properties than Sidel'nikov sequences at the cost of alphabet size.

In this correspondence, we derived the autocorrelation distributions, i.e., the values and the number of occurrences of each value of the autocorrelation function of Sidel'nikov sequences. The frequency of each correlation value of an M-ary Sidel'nikov sequence is expressed in terms of the cyclotomic numbers of order M. It is also pointed out that the total number of distinct autocorrelation values is dependent not only on M but also on the period of the sequence, but always less than or equal to $\binom{M}{2} + 1$.

Manuscript received April 3, 2004; revised April 30, 2005. This work was supported by University IT Research Center Project.

Y.-S. Kim, J.-S. Chung, and J.-S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: kingsi@ccl.snu.ac.kr; integer@ccl.snu.ac.kr; jsno@snu.ac.kr).

H. Chung is with School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2005.853310

II. Preliminaries

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

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

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

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

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

$$\mathcal{S}_k = \left\{ \alpha^{Mi+k} - 1 \,|\, 0 \le i < \frac{p^n - 1}{M} \right\}.$$

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

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

where k_0 is some integer modulo M. □

Note that $\alpha^{\frac{p^n-1}{2}} = -1$, $\bigcup_{k=0}^{M-1} \mathcal{S}_k = F_{p^n} \backslash \{-1\}$, and $0 \in \mathcal{S}_0$. Let N_k be the number of occurrences of symbol k in one period of Sidel'nikov sequence, i.e.,

$$N_k = |\{t \,|\, s(t) = k, 0 \le t \le p^n - 2\}|.$$

If $k_0 \ne 0$, then we have

$$N_k = \begin{cases} \frac{p^n-1}{M}, & \text{if } k \ne 0, k_0 \\ \frac{p^n-1}{M} + 1, & \text{if } k = k_0 \\ \frac{p^n-1}{M} - 1, & \text{if } k = 0. \end{cases}$$

It is clear that the M-ary Sidel'nikov sequences with $k_0 = 0$ are balanced.

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

Definition 2: The indicator function is defined as

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

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

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

and

$$\psi_M(0) = 0$$

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

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

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

Later, we will see the close relation between autocorrelation distributions of Sidel'nikov sequences and cyclotomic numbers.

Definition 4: Let α be a primitive element in F_{p^n}. The cyclotomic classes C_u, $0 \le u \le M-1$, in F_{p^n} are defined as

$$C_u = \left\{ \alpha^{Ml+u} \,\middle|\, 0 \le l < \frac{p^n - 1}{M} \right\}.$$

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

Following lemma [11, p. 25] shows the elementary relationships between the cyclotomic numbers.

Lemma 5 : [11]

1) For any integers l_1, l_2, $(i + Ml_1, j + Ml_2)_M = (i,j)_M$;
2) $(i,j)_M = (M - i, j - i)_M$;
3)
$$(i,j)_M = \begin{cases} (j,i)_M, & \text{if } \frac{p^n-1}{M} \text{ is even} \\ (j + M/2, i + M/2)_M, & \text{if } \frac{p^n-1}{M} \text{ is odd;} \end{cases}$$
4) $\sum_{j=0}^{M-1} (i,j)_M = (p^n - 1)/(M) - \theta_i$, where
$$\theta_i = \begin{cases} 1, & \text{if } \frac{p^n-1}{M} \text{ is even and } i = 0 \\ 1, & \text{if } \frac{p^n-1}{M} \text{ is odd and } i = M/2 \\ 0, & \text{otherwise;} \end{cases}$$
5) $\sum_{i=0}^{M-1} (i,j)_M = (p^n - 1)/(M) - \eta_j$, where
$$\eta_j = \begin{cases} 1, & \text{if } j = 0 \\ 0, & \text{otherwise.} \end{cases}$$

III. Autocorrelation of the Sidel'nikov Sequences

From [12], we can get some useful properties of the multiplicative character.

Property 6 : [12] Let $M \,|\, p^n - 1$. The multiplicative character $\psi_M(x)$ of F_{p^n} has the following properties:

1) $\sum_{x \in F_{p^n}} \psi_M(x) = 0$,
2) $\bar{\psi}_M(a) = \psi_M^{-1}(a) = \psi_M(a^{-1})$ for $a \in F_{p^n}^*$,
3) $\psi_M(a)\psi_M(b) = \psi_M(ab)$ for $a, b \in F_{p^n}$,
4) $\psi_M(a)\bar{\psi}_M(b) = \psi_M(a/b)$ for $a \in F_{p^n}$ and $b \in F_{p^n}^*$,

where $\bar{\psi}$ denotes complex conjugate of ψ. □

Using Property 6, the autocorrelation function of the M-ary Sidel'nikov sequences can be derived as follows.

Theorem 7 : [1] Let $s(t)$ be the M-ary Sidel'nikov sequence of period $N = p^n - 1$ given by

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

Then the nontrivial (i.e., $\tau \not\equiv 0 \bmod p^n - 1$) autocorrelation function of $s(t)$ is given as

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

Proof: Although a similar proof has been done by Sidel'nikov [1], here we will restate it in detail for the subsequent corollary.

Using (1), the autocorrelation $R(\tau)$ of $s(t)$ can be written as

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} \Big[\Big(\omega_M^{k_0} I(\alpha^t + 1) + \psi_M(\alpha^t + 1) \Big) \\ &\qquad \times \Big(\omega_M^{-k_0} I(\alpha^{t+\tau} + 1) \bar{\psi}_M(\alpha^{t+\tau} + 1) \Big) \Big] \\ &= \sum_{t=0}^{N-1} \Big[I(\alpha^t + 1) I(\alpha^{t+\tau} + 1) + \omega_M^{k_0} I(\alpha^t + 1) \\ &\qquad \times \bar{\psi}_M(\alpha^{t+\tau} + 1) + \psi_M(\alpha^t + 1)\omega_M^{-k_0} I(\alpha^{t+\tau} + 1) \\ &\qquad + \psi_M(\alpha^t + 1)\bar{\psi}_M(\alpha^{t+\tau} + 1) \Big]. \end{aligned}$$

Clearly, $I(\alpha^t + 1)I(\alpha^{t+\tau} + 1) = 0$ for $\tau \not\equiv 0 \bmod N$ and we have

$$\sum_{t=0}^{N-1} I(\alpha^t + 1)\bar{\psi}_M(\alpha^{t+\tau} + 1) = \bar{\psi}_M(-\alpha^\tau + 1)$$
$$\sum_{t=0}^{N-1} I(\alpha^{t+\tau} + 1)\psi_M(\alpha^t + 1) = \psi_M(-\alpha^{-\tau} + 1).$$

Thus, we have

$$R(\tau) = \omega_M^{k_0} \bar{\psi}_M(-\alpha^\tau + 1) + \omega_M^{-k_0} \psi_M(-\alpha^{-\tau} + 1) + \sum_{t=0}^{N-1} \psi_M(\alpha^t + 1)\bar{\psi}_M(\alpha^{t+\tau} + 1).$$

Using Property 6, we have

$$\sum_{t=0}^{N-1} \psi_M(\alpha^t + 1)\bar{\psi}_M(\alpha^{t+\tau} + 1) = \sum_{t=0, t \ne \frac{p^n-1}{2} - \tau}^{N-1} \psi_M\left(\frac{\alpha^t + 1}{\alpha^{t+\tau} + 1} \right). \tag{2}$$

Note that as t varies from 0 to $N - 1$ except $\frac{p^n-1}{2} - \tau$, $\frac{\alpha^t+1}{\alpha^{t+\tau}+1}$ covers all elements in $F_{p^n} \backslash \{1, \alpha^{-\tau}\}$. Then (2) can be rewritten as

$$\begin{aligned} \sum_{t=0, t \ne \frac{p^n-1}{2} - \tau}^{N-1} \psi_M\left(\frac{\alpha^t + 1}{\alpha^{t+\tau} + 1} \right) &= \sum_{x \in F_{p^n}} \psi_M(x) - \psi_M(1)\psi_M(\alpha^{-\tau}) \\ &= -\psi_M(\alpha^{-\tau}) - \psi_M(1). \end{aligned}$$

Thus, we have for $\tau \ne 0$

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

□

Let $y = \alpha^\tau$ in $F_{p^n} \backslash \{0, 1\}$. Using the fact that

$$\psi_M(-1)\psi_M\left(\frac{1}{y}\right) = \psi_M\left(\frac{1}{1-y}\right)\psi_M\left(\frac{y-1}{y}\right)$$

we can modify Theorem 7 into the more useful form as follows.

Corollary 8: The autocorrelation of the M-ary Sidel'nikov sequences can be written as follows: When $\psi_M(-1) = 1$

$$R(y) = -\left(\omega_M^{k_0} \psi_M\left(\frac{1}{1-y}\right) - 1 \right)\left(\omega_M^{-k_0} \psi_M\left(\frac{y-1}{y}\right) - 1 \right).$$

When $\psi_M(-1) = -1$

$$R(y) = \left(\omega_M^{k_0}\psi_M\left(\frac{1}{1-y}\right)+1\right)\left(\omega_M^{-k_0}\psi_M\left(\frac{y-1}{y}\right)+1\right)-2.$$

□

For $y \in F_{p^n}\backslash\{0,1\}$ such that $\psi_M(\frac{1}{1-y}) = \omega_M^u$ and $\psi_M(\frac{y-1}{y}) = \omega_M^v$, the autocorrelation $R(y)$ can be rewritten as

$$R_{u,v} = -\left(\omega_M^{u+k_0}-1\right)\left(\omega_M^{v-k_0}-1\right), \qquad \text{for } \psi_M(-1)=1 \quad (3)$$

$$R_{u,v} = \left(\omega_M^{u+k_0}+1\right)\left(\omega_M^{v-k_0}+1\right)-2, \qquad \text{for } \psi_M(-1)=-1. \quad (4)$$

The following lemma tells us about when $\psi_M(-1)$ takes the value of $+1$ or -1. We omit the proof.

Lemma 9: Let $M \,|\, p^n - 1$. For $p = 2$, $\psi_M(-1) = \psi_M(1) = 1$. For an odd prime p

$$\psi_M(-1) = \begin{cases} +1, & \text{if } \frac{p^n-1}{M} \text{ is even} \\ -1, & \text{if } \frac{p^n-1}{M} \text{ is odd.} \end{cases}$$

□

IV. Autocorrelation Distributions of Sidel'nikov Sequences

In this section, we derive the values of the autocorrelation function of an M-ary Sidel'nikov sequence given in Corollary 8 and express the frequency of each value in terms of the cyclotomic numbers of order M. The following lemma gives us the number of *possible* distinct out-of-phase autocorrelation values of M-ary Sidel'nikov sequences. Here, by the term *possible*, we imply that some of the autocorrelation values may have frequency zero depending on M and the period of the sequences.

Lemma 10: The number of distinct out-of-phase autocorrelation values of M-ary Sidel'nikov sequences is less than or equal to

$$\frac{M(M-1)}{2}+1.$$

Proof: It is clear that the number of distinct $R_{u,v}$'s does not depend on k_0. Thus, we will prove it for the case of $k_0 = 0$. It is obvious that $R_{u,v} = 0$ (or -2) if $u = 0$ or $v = 0$ (or $u = M/2$ or $v = M/2$). As $R_{u,v} = R_{v,u}$, the number of distinct out-of-phase autocorrelation values is $1 + (M-1) + \binom{M-1}{2}$. □

It is clear that some of the out-of-phase autocorrelation values might not occur, specially for the case of the large alphabet size M compared to the period of the sequences.

Corollary 8 tells us that the autocorrelation distribution is solely dependent on $A_{u,v}$, the cardinality of the sets $S_{u,v}$ defined as

$$S_{u,v} = \left\{y \in F_{p^n}\backslash\{0,1\} \,\middle|\, \psi_M\left(\frac{1}{1-y}\right) = \omega_M^u,\ \psi_M\left(\frac{y-1}{y}\right) = \omega_M^v\right\}$$

for $u, v \in \{0, 1, 2, \ldots, M-1\}$.

Then $A_{u,v}$ can be represented in terms of cyclotomic numbers of order M as in the following theorem.

Theorem 11: $A_{u,v}$ is represented as

$$A_{u,v} = (u+v, v)_M.$$

Proof:

Case 1: $\psi_M(-1) = 1$

From $\psi_M(\frac{1}{1-y}) = \omega_M^u$ and $\psi_M(\frac{y-1}{y}) = \omega_M^v$, we have

$$\psi_M\left(\frac{1}{1-y}\right)\psi_M\left(\frac{y-1}{y}\right) = \psi_M\left(\frac{1}{y}\right) = \omega_M^{u+v}.$$

In other words, $1 - y \in C_{-u}$ and $y \in C_{-u-v}$. Since $-y$ and y are in the same cyclotomic class, by applying part 2) of Lemma 5, we have

$$A_{u,v} = (-u-v, -u)_M = (u+v, v)_M.$$

Case 2: $\psi_M(-1) = -1$

Similarly, we have

$$\psi_M\left(\frac{1}{1-y}\right)\psi_M\left(\frac{y-1}{y}\right) = \psi_M\left(-\frac{1}{y}\right) = \omega_M^{u+v}.$$

Therefore, we have $1 - y \in C_{-u}$ and $-y \in C_{-u-v}$. Thus, again we have $A_{u,v} = (-u-v, -u)_M = (u+v, v)_M$. □

Theorem 12: Let $N(R_{u,v})$ be the number of $y \in F_{p^n}\backslash\{0,1\}$ such that $R(y) = R_{u,v}$. Then the out-of-phase autocorrelation distributions of an M-ary Sidel'nikov sequences of period $p^n - 1$ are given as follows.

If $\psi_M(-1) = 1$

1) $N(0) = \sum_{i=1}^{M-1}((i, i+k_0)_M + (i, k_0)_M) + (0, k_0)_M$;
2) $N(R_{k,k}) = (2k, k+k_0)_M$, for $1 \le k \le M-1$;
3) $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, for $1 \le u < v \le M-1$.

If $\psi_M(-1) = -1$

1) $N(-2) = \sum_{i=0, i\neq \frac{M}{2}}^{M-1}\left(\left(\frac{M}{2}+i, i+k_0\right)_M + \left(\frac{M}{2}+i, \frac{M}{2}+k_0\right)_M\right) + \left(0, \frac{M}{2}+k_0\right)_M$;
2) $N(R_{k,k}) = (2k, k+k_0)_M$, for $0 \le k \le M-1$ and $k \neq (M/2)$;
3) $N(R_{u,v}) = (u+v, v+k_0)_M + (u+v, u+k_0)_M$, for $0 \le u < v \le M-1$, $u \neq (M/2)$, and $v \neq (M/2)$.

Proof: If $\psi_M(-1) = 1$, we have

$$R_{u,v} = -(\omega^{u+k_0}-1)(\omega^{v-k_0}-1).$$

Thus, we have

$$N(0) = \sum_{u=0}^{M-1} A_{u,k_0} + \sum_{v=0}^{M-1} A_{-k_0,v} - A_{-k_0,k_0} = \sum_{i=1}^{M-1}((i, i+k_0)_M + (i, k_0)_M) + (0, k_0)_M.$$

Similarly, we have

$$N(R_{k,k}) = A_{k-k_0,k+k_0} = (2k, k+k_0)_M$$

and

$$N(R_{u,v}) = A_{u-k_0,v+k_0} + A_{v-k_0,u+k_0} = (u+v, v+k_0)_M + (u+v, u+k_0)_M.$$

The proof for the case of $\psi_M(-1) = -1$ can be done similarly. □

We can easily derive the upper bound of maximum magnitude of the autocorrelation values of M-ary Sidel'nikov sequences as follows.

Theorem 13: The upper bound of the maximum magnitude of out-of-phase autocorrelation values of M-ary Sidel'nikov sequences is given as follows.

If $\psi_M(-1) = 1$

$$\max_{0\le\tau\le p^n-2}|R(\tau)| \le \begin{cases} 4, & \text{if } M \text{ is even} \\ 4\cos^2\left(\frac{\pi}{2M}\right), & \text{if } M \text{ is odd} \end{cases} \quad (5)$$

and if $\psi_M(-1) = -1$

$$\max_{0\le\tau\le p^n-2} |R(\tau)| \le \begin{cases} 2\sqrt{2}, & \text{if } M \equiv 0 \bmod 4 \\ 2\sqrt{\cos^2\left(\frac{\pi}{M}\right)+1}, & \text{if } M \equiv 2 \bmod 4. \end{cases} \quad (6)$$

Proof: It is also clear that the upper bound of the maximum magnitude of $R_{u,v}$ does not depend on k_0. Thus, we will prove it for $k_0 = 0$.

Case 1. If $\psi_M(-1) = 1$, from (3), it is easy to see that the maximum magnitude of autocorrelation values is achieved when $(u, v) = (\frac{M}{2}, \frac{M}{2})$ if M is even or $(u, v) = (\frac{M\pm1}{2}, \frac{M\pm1}{2})$ if M is odd. Thus, (5) can be easily derived.

Case 2. If $\psi_M(-1) = -1$, from (4), we have

$$R_{u,v} = 4\cos\left(\frac{\pi u}{M}\right)\cos\left(\frac{\pi v}{M}\right)\exp\left[j\left(\frac{\pi}{M}(u+v)\right)\right] - 2.$$

Then after some trigonometric manipulation, we can obtain that

$$|R_{u,v}|^2 = 4\sin\left(\frac{2\pi u}{M}\right)\sin\left(\frac{2\pi v}{M}\right) + 4.$$

Then, the maximum magnitude of autocorrelation values is achieved when

$$(u,v) = \left(\frac{M}{4}, \frac{M}{4}\right) \text{ or } \left(\frac{3M}{4}, \frac{3M}{4}\right), \quad \text{if } M \equiv 0 \bmod 4$$

or

$$(u,v) = \left(\frac{M\pm2}{4}, \frac{M\pm2}{4}\right) \text{ or } \left(\frac{3M\pm2}{4}, \frac{3M\pm2}{4}\right), \quad \text{if } M \equiv 2 \bmod 4.$$

Thus, (6) is easily derived. □

V. Examples

The cyclotomic numbers of order $2, 3, 4, 6,$ and 8 in the field F_{p^n} have been known [11]. Using the result of the preceding section and the already known cyclotomic numbers $(u, v)_M$, we can derive the autocorrelation distributions of Sidel'nikov sequences for the cases of binary, ternary, quaternary, sextary, and octary sequences.

In this section, autocorrelation distributions of ternary and quaternary Sidel'nikov sequences are evaluated. Using Corollary 8, we can have the following corollary.

Corollary 14: The autocorrelation distribution of the ternary $(M = 3)$ Sidel'nikov sequences of period $p^n - 1$ with $k_0 = 0$ is given by

$$R(\tau) = \begin{cases} p^n-1, & \text{once} \\ 0, & \frac{5p^n-16-c}{9} \text{ times} \\ -3, & \frac{2p^n-4-c}{9} \text{ times} \\ 3\omega_3, & \frac{p^n+1+c}{9} \text{ times} \\ 3\omega_3^2, & \frac{p^n+1+c}{9} \text{ times} \end{cases}$$

where $4p^n = c^2 + 27d^2$, $c \equiv 1 \pmod 3$, and ω_3 is a complex third root of unity.

Proof: From Lemma 9, it is clear that $\psi_3(-1) = 1$. Since $R_{u,v} = -(\omega_3^u - 1)(\omega_3^v - 1)$, we have

$$R_{u,v} = \begin{cases} 0, & \text{if } u=0 \text{ or } v=0 \\ 3\omega_3, & \text{if } u=1 \text{ and } v=1 \\ 3\omega_3^2, & \text{if } u=2 \text{ and } v=2 \\ -3, & \text{if } u=1 \text{ and } v=2 \text{ or } vice\ versa. \end{cases}$$

From Theorem 12, we have

$$\begin{aligned} N(0) &= (0,0)_3 + (1,1)_3 + (2,2)_3 + (1,0)_3 + (2,0)_3 \\ N(R_{1,1}) &= (2,1)_3 \\ N(R_{2,2}) &= (1,2)_3 \\ N(R_{1,2}) &= (0,1)_3 + (0,2)_3. \end{aligned}$$

And finally, the cyclotomic numbers of order 3 can be obtained from [11] and they are

$$\begin{aligned} (0,0)_3 &= \frac{p^n-8+c}{9} \\ (0,1)_3 = (1,0)_3 = (2,2)_3 &= \frac{2p^n-4-c-9d}{18} \\ (0,2)_3 = (1,1)_3 = (2,0)_3 &= \frac{2p^n-4-c+9d}{18} \\ (1,2)_3 = (2,1)_3 &= \frac{p^n+1+c}{9}. \end{aligned}$$ □

The following example shows the autocorrelation distribution of the ternary Sidel'nikov sequences of period $7^3 - 1$ with $k_0 = 0$.

Example 15: For $p = 7$ and $n = 3$, from $4p^n = c^2 + 27d^2$ and $c \equiv 1 \pmod 3$, we have $c = -20$ and $d = \pm 6$. From Corollary 14, we have

$$R(\tau) = \begin{cases} 342, & \text{once} \\ 0, & 191 \text{ times} \\ -3, & 78 \text{ times} \\ 3\omega_3, & 36 \text{ times} \\ 3\omega_3^2, & 36 \text{ times.} \end{cases}$$ □

Similarly, for quaternary Sidel'nikov sequences, we have the following corollary.

Corollary 16: The autocorrelation distributions of the quaternary $(M = 4)$ Sidel'nikov sequences of period $p^n - 1$ with $k_0 = 0$ are given as follows.

If $\psi_4(-1) = 1$

$$R(\tau) = \begin{cases} p^n-1, & \text{once} \\ 0, & \frac{7p^n-29+6s}{16} \text{ times} \\ j2, & \frac{p^n+1-2s}{16} \text{ times} \\ -4, & \frac{p^n-3+2s}{16} \text{ times} \\ -j2, & \frac{p^n+1-2s}{16} \text{ times} \\ -2+j2, & \frac{p^n+1-2s}{8} \text{ times} \\ -2, & \frac{p^n-3+2s}{8} \text{ times} \\ -2-j2, & \frac{p^n+1-2s}{8} \text{ times} \end{cases}$$

and if $\psi_4(-1) = -1$

$$R(\tau) = \begin{cases} p^n-1, & \text{once} \\ -2, & \frac{7p^n-9+6s}{16} \text{ times} \\ 2, & \frac{p^n-7+2s}{16} \text{ times} \\ -2+j2, & \frac{p^n-3-2s}{16} \text{ times} \\ -2-j2, & \frac{p^n-3-2s}{16} \text{ times} \\ j2, & \frac{p^n-3-2s}{8} \text{ times} \\ -j2, & \frac{p^n-3-2s}{8} \text{ times} \\ 0, & \frac{p^n+1+2s}{8} \text{ times} \end{cases}$$

where $p^n = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$.

Proof: If $\psi_4(-1) = 1$

$$R_{u,v} = \begin{cases} 0, & \text{if } u = 0 \text{ or } v = 0 \\ j2, & \text{if } u = 1 \text{ and } v = 1 \\ -4, & \text{if } u = 2 \text{ and } v = 2 \\ -j2, & \text{if } u = 3 \text{ and } v = 3 \\ -2+j2, & \text{if } u = 1 \text{ and } v = 2 \text{ or } vice\ versa \\ -2, & \text{if } u = 1 \text{ and } v = 3 \text{ or } vice\ versa \\ -2-j2, & \text{if } u = 2 \text{ and } v = 3 \text{ or } vice\ versa. \end{cases}$$

From Theorem 12, we have

$$\begin{aligned} N(0) &= (0,0)_4 + (1,1)_4 + (2,2)_4 + (3,3)_4 + (1,0)_4 \\ &\quad + (2,0)_4 + (3,0)_4 \\ N(R_{1,1}) &= (2,1)_4, \quad N(R_{2,2}) = (0,2)_4, \quad N(R_{3,3}) = (2,3)_4 \\ N(R_{1,2}) &= (3,2)_4 + (3,1)_4, \quad N(R_{1,3}) = (0,3)_4 + (0,1)_4 \\ N(R_{2,3}) &= (1,3)_4 + (1,2)_4. \end{aligned}$$

And finally, the cyclotomic numbers of order 4 can be obtained from [11], and they are

$$\begin{aligned} (0,0)_4 &= \frac{p^n - 11 - 6s}{16} \\ (0,1)_4 &= (1,0)_4 = (3,3)_4 = \frac{p^n - 3 + 2s + 8t}{16} \\ (0,2)_4 &= (2,0)_4 = (2,2)_4 = \frac{p^n - 3 + 2s}{16} \\ (0,3)_4 &= (3,0)_4 = (1,1)_4 = \frac{p^n - 3 + 2s - 8t}{16} \\ (1,2)_4 &= (1,3)_4 = (2,1)_4 \\ &= (3,1)_4 = (2,3)_4 = (3,2)_4 = \frac{p^n + 1 - 2s}{16}. \end{aligned}$$

And if $\psi_4(-1) = -1$

$$R_{u,v} = \begin{cases} -2, & \text{if } u = 2 \text{ or } v = 2 \\ 2, & \text{if } u = 0 \text{ and } v = 0 \\ -2+2j, & \text{if } u = 1 \text{ and } v = 1 \\ -2-j2, & \text{if } u = 3 \text{ and } v = 3 \\ j2, & \text{if } u = 0 \text{ and } v = 1 \text{ or } vice\ versa \\ -2j, & \text{if } u = 0 \text{ and } v = 3 \text{ or } vice\ versa \\ 0, & \text{if } u = 1 \text{ and } v = 3 \text{ or } vice\ versa. \end{cases}$$

From Theorem 12, we have

$$\begin{aligned} N(-2) &= (0,2)_4 + (2,0)_4 + (3,1)_4 + (1,3)_4 \\ &\quad + (2,2)_4 + (3,2)_4 + (1,2)_4 \\ N(R_{0,0}) &= (0,0)_4, \quad N(R_{1,1}) = (2,1)_4, \quad N(R_{3,3}) = (2,3)_4 \\ N(R_{0,1}) &= (1,0)_4 + (1,1)_4, \quad N(R_{0,3}) = (3,0)_4 + (3,3)_4 \\ N(R_{1,3}) &= (0,3)_4 + (0,1)_4. \end{aligned}$$

And finally, the cyclotomic numbers of order 4 can be obtained from [11], and they are

$$\begin{aligned} (0,0)_4 &= (2,2)_4 = (2,0) = \frac{p^n - 7 + 2s}{16} \\ (0,1)_4 &= (1,3)_4 = (3,2)_4 = \frac{p^n + 1 + 2s - 8t}{16} \\ (0,2)_4 &= \frac{p^n + 1 - 6s}{16} \\ (0,3)_4 &= (1,2)_4 = (3,1)_4 = \frac{p^n + 1 + 2s + 8t}{16} \\ (1,0)_4 &= (1,1)_4 = (2,1)_4 \\ &= (2,3)_4 = (3,0)_4 = (3,3)_4 = \frac{p^n - 3 - 2s}{16}. \end{aligned}$$ □

The following example shows the autocorrelation distribution of the quaternary Sidel'nikov sequences of period $17^3 - 1$ with $k_0 = 0$.

Example 17: For $p = 17$ and $n = 3$, we have $\psi_4(-1) = 1$. From $p^n = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$, we have $s = -47$ and $t = \pm 26$. From Corollary 16, we have

$$R(\tau) = \begin{cases} 4912, & \text{once} \\ 0, & \text{2130 times} \\ -4, & \text{301 times} \\ -2, & \text{602 times} \\ -2+j2, & \text{626 times} \\ -2-j2, & \text{626 times} \\ j2, & \text{313 times} \\ -j2, & \text{313 times.} \end{cases}$$ □

And the following example shows the autocorrelation distribution of the quaternary Sidel'nikov sequences of period $13^3 - 1$ with $k_0 = 0$.

Example 18: For $p = 13$ and $n = 3$, we have $\psi_4(-1) = -1$. From $p^n = s^2 + 4t^2$ and $s \equiv 1 \pmod 4$, we have $s = 9$ and $t = \pm 23$. From Corollary 16, we have

$$R(\tau) = \begin{cases} 2196, & \text{once} \\ -2, & \text{964 times} \\ 2, & \text{138 times} \\ 0, & \text{277 times} \\ -2+j2, & \text{136 times} \\ -2-j2, & \text{136 times} \\ j2, & \text{272 times} \\ -j2, & \text{272 times.} \end{cases}$$ □

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their valuable comments and suggestions that much improved the presentation of this correspondence.

REFERENCES

[1] 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.

[2] 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.

[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] D. H. Green and P. R. Green, "Polyphase related-prime sequences," *Proc. Inst. Elec. Eng.-Comput. Digit. Technol.*, vol. 148, no. 2, pp. 53–62, Mar. 2001.

[5] D. H. Green and P. R. Green, "Polyphase power-residue sequences," *Proc. Roy. Soc. London*, ser. A, vol. 459, pp. 817–827, 2003.

[6] S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 1101–1113, May 1992.

[7] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons Jr., "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579–592, Mar. 1996.

[8] C. E. Lee, "Perfect q-ary sequences from multiplicative characters over $GF(p)$," *Electron. Lett.*, vol. 28, no. 9, pp. 833–835, Apr. 1992.

[9] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271–3282, Dec. 2003.

[10] ——, "Generalized Sidel'nikov sequences with optimal autocorrelation properties," *Electron. Lett.*, vol. 36, no. 6, pp. 525–528, Mar. 2000.

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

[12] R. Lidl and H. Niederreiter, *Finite Fields*. Reading, MA: Addison-Wesley, 1983, vol. 20. *Encyclopedia of Mathematics and Its Applications*.