Derivation of Autocorrelation Distributions of Sidel'nikov Sequences Using Cyclotomic Numbers

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

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

***Abstract*— In this paper, we 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 $\binom{M}{2}+1$.**

I. Introduction

For a prime p and a positive integer M such that $M|p-1$, Sidel'nikov [8] 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 [8].

Later, Lempel, Cohn, and Eastman [4] independently introduced the binary Sidel'nikov sequences of period p^n-1. 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]. D. H. Green and P. R. Green [1], [2] introduced the polyphase Legendre sequences of prime period p, which later turned out to be the power residue sequences constructed by Sidel'nikov [8].

Lüke, Schotten, and Hadinejad-Mahram [6], [7] 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 paper, 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 $\binom{M}{2}+1$.

II. Preliminaries

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

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

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

Sidel'nikov [8] introduced M-ary sequences as follows.

Definition 1: [8] Let p be a prime and α a primitive element in the finite field F_{p^n} with p^n elements. Let $M|p^n-1$. Let $\mathcal{S}_k$, $k = 0, 1, \cdots, M-1$, be the disjoint subsets of F_{p^n} defined as

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

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

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

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 $0 \in \mathcal{S}_0$.

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

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

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

$$C_u = \{\alpha^{Ml+u} \mid 0 \le l < \frac{p^n-1}{M}\}.$$

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

Following lemma [9, p. 25] shows the elementary relationship between two cyclotomic numbers.

Lemma 5: [9] $(i,j)_M = (M-i, j-i)_M$. □

III. Autocorrelation of the Sidel'nikov Sequences

From [5], we can get some useful properties of the multiplicative character.

Property 6: [5] 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) $\overline{\psi}_M(a) = \psi_M^{-1}(a) = \psi_M(a^{-1})$ for $a \in F_{p^n}^*$
3) $\psi_M(a)\psi_M(b) = \psi_M(ab)$ for $a, b \in F_{p^n}$
4) $\psi_M(a)\overline{\psi}_M(b) = \psi_M(\frac{a}{b})$ for $a \in F_{p^n}$ and $b \in F_{p^n}^*$

where $\overline{\psi}$ 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: [8] Let $s(t)$ be an M-ary Sidel'nikov sequence of period $N = p^n - 1$. Then the nontrivial (i.e., $\tau \not\equiv 0 \bmod p^n-1$) autocorrelation function of $s(t)$ is given as

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

Proof: Although the similar proof has been done by Sidel'nikov [8], here we will restate it in detail for the subsequent corollaries.

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

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

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

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

Using Property 6, we have

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

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

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

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

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

□

Let $y = \alpha^\tau$ in $F_{p^n}\backslash\{0,1\}$. Using the fact that $\psi_M(-1)\,\psi_M\left(\frac{1}{y}\right) = \psi_M\left(\frac{1}{1-y}\right)\psi_M(\frac{y-1}{y})$, 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 modified as follows: When $\psi_M(-1) = 1$,

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

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

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

□

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

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

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

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,

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

□

IV. Autocorrelation Distributions of Sidel'nikov Sequences

In this section, we derive the values of the autocorrelation function of an M-ary Sidel'nikov sequences and express the frequency of each value in terms of the cyclotomic numbers of order M. 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 with $k_0 \neq 0$ is the same as that for $R_{u,v}$ with $k_0 = 0$. 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 $R_{u,v} = R_{v,u}$, it is not difficult to find the number of distinct out-of-phase autocorrelation values in the above. □

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

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

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

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 $\psi_M(\frac{1}{1-y})\psi_M(\frac{y-1}{y}) = \psi_M(\frac{1}{y}) = \omega_M^{u+v}$. 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 Lemma 5, we have

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

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

Similarly, we have $\psi_M(\frac{1}{1-y})\psi_M(\frac{y-1}{y}) = \psi_M(-\frac{1}{y}) = \omega_M^{u+v}$. 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:

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

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

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

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

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

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

Thus, we have

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

Similarly, we have

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

and

$$\begin{aligned} N(R_{u,v}) &= A_{u-k_0,v+k_0} + A_{v-k_0,u+k_0} \\ &= (u+v, v+k_0)_M + (u+v, u+k_0)_M. \end{aligned}$$

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

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

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

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

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

Case 1. If $\psi_M(-1) = 1$, from (3), we have

$$R_{u,v} = -4\sin(\frac{\pi u}{M})\sin(\frac{\pi v}{M})\exp\Big[j(\pi + \frac{\pi}{M}(u+v))\Big].$$

Then, the magnitude of autocorrelation values is maximum 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. Since $\sin^2(\frac{\pi}{2}\frac{M\pm1}{M}) = \cos^2(\frac{\pi}{2M})$, the maximum magnitude of autocorrelation values of M-ary Sidel'nikov sequences is

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

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

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

Then after some trigonometric manipulation, we can obtain that

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

Then, the magnitude of autocorrelation values is maximum when $(u,v) = (\frac{M}{4}, \frac{M}{4})$ or $(\frac{3M}{4}, \frac{3M}{4})$ if $M \equiv 0 \bmod 4$ or $(u,v) = (\frac{M\pm2}{4}, \frac{M\pm2}{4})$ or $(\frac{3M\pm2}{4}, \frac{3M\pm2}{4})$ if $M \equiv 2 \bmod 4$. Since $\sqrt{\sin^2(\frac{\pi}{2}\frac{M\pm2}{M})+1} = \sqrt{\sin^2(\frac{\pi}{2}\frac{3M\pm2}{M})+1} = \sqrt{\cos^2(\frac{\pi}{M})+1}$, the maximum magnitude of autocorrelation values of M-ary Sidel'nikov sequences is

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

□

V. Examples

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

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

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

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

And finally, the cyclotomic numbers of order 3 can be obtained from [9] and they are

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

□

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

Corollary 15: The autocorrelation distributions of the quaternary ($M = 4$) Sidel'nikov sequences of period $p^n - 1$ with $k_0 = 0$ are given by:

If $\psi_4(-1) = 1$,

$$R_{u,v} = \begin{cases} p^n - 1, & \text{once} \\ 0, & \frac{7p^n-29+6s}{16} \text{ times} \\ \pm j2, & \frac{p^n+1-2s}{16} \text{ times, respectively} \\ -4, & \frac{p^n-3+2s}{16} \text{ times} \\ -2 \pm j2, & \frac{p^n+1-2s}{8} \text{ times, respectively} \\ -2, & \frac{p^n-3+2s}{8} \text{ times} \end{cases}$$

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

$$R_{u,v} = \begin{cases} p^n - 1, & \text{once} \\ -2, & \frac{7p^n-9+6s}{16} \text{ times} \\ 2, & \frac{p^n-7+2s}{16} \text{ times} \\ -2 \pm j2, & \frac{p^n-3-2s}{16} \text{ times, respectively} \\ \pm j2, & \frac{p^n-3-2s}{8} \text{ times, respectively} \\ 0, & \frac{p^n+1+2s}{8} \text{ times} \end{cases}$$

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 [9], and they are

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

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

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

And finally, the cyclotomic numbers of order 4 can be obtained from [9], and they are

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

□

ACKNOWLEDGMENT

This work was supported by University IT Research Center Project.

REFERENCES

[1] D. H. Green and P. R. Green, "Polyphase related-prime sequences," *IEE Proc. Comput. Digit. Tech.*, vol. 148, no. 2, pp. 53–62, Mar. 2001.
[2] D. H. Green and P. R. Green, "Polyphase power-residue sequences," *Proc. R. Soc. Lond.*, Series A, vol 459, pp. 817-827, 2003.
[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. Inform. Theory*, vol. 49, no. 6, pp. 1548–1552, June 2003.
[4] A. Lempel, M. Cohn, and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 38–42, Jan. 1977.
[5] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Reading, MA: Addison-Wesley, 1983.
[6] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A survey," *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3271–3282, Dec. 2003.
[7] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Generalised Sidel'nikov sequences with optimal autocorrelation properties," *Electron. Lett.*, vol. 36, no. 6, pp. 525–528, Mar. 2000.
[8] V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12–16, 1969.
[9] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham Publishing Company, 1967.