

Analysis of Autocorrelation Distributions of M -ary Sidel'nikov Sequences ¹

*Young-Sik Kim, *Jung-Soo Chung^O, *Jong-Seon No, and **Habong Chung
 *School of Electrical Engineering and Computer Science, Seoul National University
 **School of Electronics and Electrical Engineering, Hong-Ik University
 Email: jsno@snu.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 using cyclotomic numbers. 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 $\binom{M}{2} + 1$.

1. Introduction

For positive integer n such that $M|p^n - 1$, Sidel'nikov [1] 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] 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.

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 using cyclotomic numbers. 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 $\binom{M}{2} + 1$.

2. 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 $0 \leq \tau \leq N - 1$.

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

¹This work was supported by University IT Research Center Project.

$M|p^n - 1$. Let \mathcal{S}_k , $k = 0, 1, \dots, M - 1$, be the disjoint subsets of F_{p^n} defined as

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

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

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

where k_0 is some integer modulo M . □

Note that $\alpha^{\frac{p^n - 1}{2}} = -1$, $\bigcup_{k=0}^{M-1} \mathcal{S}_k = F_{p^n} \setminus \{-1\}$, 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

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

□

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 $0 \leq t \leq p^n - 2$. □

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

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

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 , $0 \leq u \leq M - 1$, in F_{p^n} are defined as

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

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

Following Lemma [12, p. 25] shows the elementary relationship between the cyclotomic numbers.

Lemma 5 [4] $(i, j)_M = (M - i, j - i)_M$.

3. Autocorrelation of the Sidel'nikov Sequences

The autocorrelation function of the M -ary Sidel'nikov sequences can be derived as follows:

Theorem 6 [1] Let $s(t)$ be the M -ary Sidel'nikov sequence of period $N = p^n - 1$. Then the nontrivial (i.e., $\tau \not\equiv 0 \pmod{p^n - 1}$) autocorrelation function of $s(t)$ is given as

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

\square

Let $y = \alpha^\tau$ in $F_{p^n} \setminus \{0, 1\}$. Using the fact that $\psi_M(-1) \psi_M\left(\frac{1}{y}\right) = \psi_M\left(\frac{1}{1-y}\right) \psi_M\left(\frac{y-1}{y}\right)$, Kim, Chung, No, and Chung modify Theorem 6 into the more useful form as follows:

Corollary 7 [5] The autocorrelation of the M -ary Sidel'nikov sequences can be modified 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 $\psi_M(-1) = -1$,

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

\square

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

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

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

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

Lemma 8 Let $M \mid p^n - 1$. For $p = 2$, $\psi_M(-1) = \psi_M(1) = 1$. For an odd prime p ,

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

\square

4. 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 9 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 $k_0 = 0$.

Case 1: $R_{u,v} = -(\omega_M^u - 1)(\omega_M^v - 1)$

By applying simple equalities, $\cos 2\theta = 2 \cos^2 \theta - 1$ and $\sin 2\theta = 2 \sin \theta \cos \theta$, it is not difficult to see that

$$\omega_M^u - 1 = 2 \sin\left(\frac{\pi u}{M}\right) \exp\left[j\left(\frac{\pi}{2} + \frac{\pi u}{M}\right)\right]$$

for $0 \leq u \leq M - 1$.

Thus we have

$$R_{u,v} = -(\omega_M^u - 1)(\omega_M^v - 1)$$

$$= -4 \sin\left(\frac{\pi u}{M}\right) \sin\left(\frac{\pi v}{M}\right) \exp\left[j\pi\left(\frac{M+u+v}{M}\right)\right]$$

$$= 2 \left(\cos\left(\frac{\pi(u+v)}{M}\right) - \cos\left(\frac{\pi(u-v)}{M}\right) \right)$$

$$\times \exp\left[j\pi\left(\frac{M+u+v}{M}\right)\right]. \quad (2)$$

Now, suppose that $R_{u_1, v_1} = R_{u_2, v_2}$, i.e.,

$$(\omega_M^{u_1} - 1)(\omega_M^{v_1} - 1) = (\omega_M^{u_2} - 1)(\omega_M^{v_2} - 1). \quad (3)$$

From (2), (3) becomes

$$\begin{aligned} & \left(\cos\left(\frac{\pi(u_1 + v_1)}{M}\right) - \cos\left(\frac{\pi(u_1 - v_1)}{M}\right) \right) \\ & \quad \times \exp\left[j\pi\left(\frac{M + u_1 + v_1}{M}\right)\right] \\ = & \left(\cos\left(\frac{\pi(u_2 + v_2)}{M}\right) - \cos\left(\frac{\pi(u_2 - v_2)}{M}\right) \right) \\ & \quad \times \exp\left[j\pi\left(\frac{M + u_2 + v_2}{M}\right)\right]. \quad (4) \end{aligned}$$

Since $0 \leq u_i + v_i \leq 2(M-1)$ and $-(M-1) \leq u_i - v_i \leq M-1$, the conditions for (4) to be satisfied are

$$u_1 + v_1 = u_2 + v_2 \quad \text{and} \quad u_1 - v_1 = \pm(u_2 - v_2)$$

which further imply that either $u_1 = u_2$ and $v_1 = v_2$ or $u_1 = v_2$ and $v_1 = u_2$.

Case 2: $R_{u,v} = (\omega_M^u + 1)(\omega_M^v + 1) - 2$

Similarly, $\omega_M^u + 1$ can be written as

$$(\omega_M^u + 1) = 2 \cos\left(\frac{\pi u}{M}\right) \exp\left[j\left(\frac{\pi u}{M}\right)\right]$$

and thus we have

$$\begin{aligned} (\omega_M^{u_1} + 1)(\omega_M^{v_1} + 1) = & 2 \left[\cos\frac{\pi(u+v)}{M} + \cos\frac{\pi(u-v)}{M} \right] \\ & \times \exp\left[j\left(\frac{\pi(u+v)}{M}\right)\right]. \quad (5) \end{aligned}$$

Similarly to the previous case, we can derive that $R_{u_1, v_1} = R_{u_2, v_2}$ only if $u_1 = u_2$ and $v_1 = v_2$ or $u_1 = v_2$ and $v_1 = u_2$.

Now, remaining is the simple counting of the number of out-of-phase autocorrelation values of M -ary Sidel'nikov sequences. For the Case 1, the correlation value is equal to 0 if u or v is equal to 0. The number of cases $u = v \neq 0$ is equal to $M-1$. Finally, the number of cases for selecting two distinct elements u and v from the set $\{1, 2, \dots, M-1\}$ is equal to $\binom{M-1}{2} = \frac{(M-1)(M-2)}{2}$.

Again for the Case 2, the correlation value is equal to -2 if u or v is equal to $\frac{M}{2}$. The number of cases $u = v \neq \frac{M}{2}$ is equal to $M-1$. And the number of cases for selecting two distinct elements u and v from the set $\{0, 1, \dots, \frac{M}{2}-1, \frac{M}{2}+1, \dots, M-1\}$ is equal to $\binom{M-1}{2} = \frac{(M-1)(M-2)}{2}$.

Thus the number of possible distinct out-of-phase autocorrelation values of M -ary Sidel'nikov sequences is equal to

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

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

$$S_{u,v} = \left\{ y \in F_{p^n} \setminus \{0, 1\} \mid \begin{aligned} & \psi_M\left(\frac{1}{1-y}\right) = \omega_M^u, \\ & \psi_M\left(\frac{y-1}{y}\right) = \omega_M^v \end{aligned} \right\}$$

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

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

Theorem 10 $A_{u,v}$ is represented as

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

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

From $\psi_M\left(\frac{1}{1-y}\right) = \omega_M^u$ and $\psi_M\left(\frac{y-1}{y}\right) = \omega_M^v$, 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 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 $A_{u,v} = (-u - v, -u)_M = (u + v, v)_M. \quad \square$

Theorem 11 Let $N(R_{u,v})$ be the number of $y \in F_{p^n} \setminus \{0, 1\}$ 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) $N(0) = \sum_{i=1}^{M-1} \left((i, i+k_0)_M + (i, k_0)_M \right) + (0, k_0)_M$
- 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) $N(-2) = \sum_{i=0, i \neq \frac{M}{2}}^{M-1} \left(\left(\frac{M}{2} + i, i+k_0 \right)_M + \left(\frac{M}{2} + i, \frac{M}{2} + k_0 \right)_M \right) + (0, \frac{M}{2} + k_0)_M$
- 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

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

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. \square

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

Theorem 12 The upper bound of the maximum magnitude of out-of-phase autocorrelation values of M -ary Sidel'nikov sequences is given as: If $\psi_M(-1) = 1$,

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

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

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

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 (2), we have

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

Then, the magnitude of autocorrelation values is maximum when $(u, v) = \left(\frac{M}{2}, \frac{M}{2}\right)$ if M is even or $(u, v) = \left(\frac{M \pm 1}{2}, \frac{M \pm 1}{2}\right)$ if M is odd. Since $\sin^2\left(\frac{\pi}{2}\frac{M \pm 1}{M}\right) = \cos^2\left(\frac{\pi}{2M}\right)$, the maximum magnitude of autocorrelation values of M -ary Sidel'nikov sequences is

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

Case 2. If $\psi_M(-1) = -1$, from (5), 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

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

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

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

5. Examples

In this section, autocorrelation distributions of ternary and quaternary Sidel'nikov sequences are evaluated. Using Corollary 7, we can have the following corollary.

Corollary 13 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 8, 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 11, 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 [4] 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 14 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 11, we have

$$N(0) = (0, 0)_4 + (1, 1)_4 + (2, 2)_4 + (3, 3)_4 + (1, 0)_4 + (2, 0)_4 + (3, 0)_4$$

$$N(R_{1,1}) = (2, 1)_4, \quad N(R_{2,2}) = (0, 2)_4$$

$$N(R_{3,3}) = (2, 3)_4$$

$$N(R_{1,2}) = (3, 2)_4 + (3, 1)_4$$

$$N(R_{1,3}) = (0, 3)_4 + (0, 1)_4$$

$$N(R_{2,3}) = (1, 3)_4 + (1, 2)_4.$$

And finally the cyclotomic numbers of order 4 can be obtained from [4], 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 11, we have

$$N(-2) = (0, 2)_4 + (2, 0)_4 + (3, 1)_4 + (1, 3)_4 + (2, 2)_4 + (3, 2)_4 + (1, 2)_4$$

$$N(R_{0,0}) = (0, 0)_4, \quad N(R_{1,1}) = (2, 1)_4$$

$$N(R_{3,3}) = (2, 3)_4$$

$$N(R_{0,1}) = (1, 0)_4 + (1, 1)_4$$

$$N(R_{0,3}) = (3, 0)_4 + (3, 3)_4$$

$$N(R_{1,3}) = (0, 3)_4 + (0, 1)_4.$$

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

$$(0, 0)_4 = (2, 2)_4 = (2, 0) = \frac{p^n - 7 + 2s}{16}$$

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

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

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

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

□

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. Inform. Theory*, vol. IT-23, no. 1, pp. 38–42, Jan. 1977.
- [3] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Reading, MA: Addison-Wesley, 1983.
- [4] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics*. Chicago, IL: Markham Publishing Company, 1967.
- [5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, " q -ary Lempel-Cohn-Eastman sequences," *Proc. JCCI 2004*, vol. 14, Apr. 2004, I-B.1.1-4.