Cyclotomic Numbers of Order 5 Over F_{p^n}

Jung-Soo Chung, Young-Sik Kim, Tae-Hyung Lim, and Jong-Seon No
School of EECS, Seoul National University,
Seoul 151-744, Korea
Email: {integer, kingsi, jayel}@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 derive the cyclotomic numbers of order 5 over an extension field F_{p^n} using the well-known results of quintic Jacobi sums over F_p [1]. For $p \not\equiv 1 \bmod 5$, we have obtained the simple closed-form expression of the cyclotomic numbers of order 5 over F_{p^n}. For $p \equiv 1 \bmod 5$, we express the cyclotomic number of order 5 over F_{p^n} in terms of the solution of the diophantine system which is required to evaluate the cyclotomic number of order 5 over F_p. Using the cyclotomic numbers of order 5 over F_{p^n}, autocorrelation distributions of 5-ary Sidel'nikov sequences of period $p^n - 1$ are also derived.**

I. Introduction

Recently, Kim, Chung, No, and Chung [5] have shown the relation between the autocorrelation distributions of M-ary Sidel'nikov sequences of period $p^n - 1$ [7] and the cyclotomic numbers of order M over the finite field F_{p^n} with p^n elements. Thus it is interesting to find the cyclotomic numbers of order 5 over F_{p^n} for the derivation of autocorrelation distributions of 5-ary Sidel'nikov sequences.

For a prime $p = Md + 1$, numerous studies have discussed the cyclotomic numbers of order M [1]–[3], [8]. In 1935, the cyclotomic numbers of order 5 over F_p are derived by Dickson [3]. He evaluated 25 cyclotomic numbers of order 5 over F_p for a prime $p \equiv 1 \bmod 5$, in terms of the solution of the diophantine system: $16p = x_0^2 + 50u_0^2 + 50v_0^2 + 126w_0^2$, $x_0 w_0 = v_0^2 - 4u_0 v_0 - u_0^2$, and $x_0 \equiv 1 \bmod 5$.

Noting that the above diophantine system has exactly four solutions and Dickson did not specify which of these four solutions was used, Karte and Rajwade [4] in 1985, supplemented two more conditions to the diophantine system for the unique determination of the cyclotomic numbers of order 5 not only over F_p but F_{p^n}. But their derivation is limited only to the case of $p \equiv 1 \bmod 5$ and still requires the solution of the diophantine system associated with the extension field F_{p^n}.

In this paper, we derive the cyclotomic numbers of order 5 over an extension field F_{p^n} using the well-known results of quintic Jacobi sums over F_p [1]. For $p \not\equiv 1 \bmod 5$, we have obtained the simple closed-form expression of the cyclotomic numbers of order 5 over F_{p^n}. For $p \equiv 1 \bmod 5$, our derivation becomes similar to Karte and Rajwade's, but only requires the solution of the diophantine system associated with the prime field F_p not F_{p^n}. Using the cyclotomic numbers of order 5 over F_{p^n}, autocorrelation distributions of 5-ary Sidel'nikov sequences of period $p^n - 1$ are also derived.

II. Preliminaries

Let $5|(p^n - 1)$ and α be a primitive element of F_{p^n}. Then the cyclotomic numbers of order 5 are defined as follows.

Definition 1: The cyclotomic class C_i of order 5, $0 \le i \le 4$, in F_{p^n} is defined as

$$C_i = \{\alpha^{5l+i} \mid 0 \le l < \frac{p^n - 1}{5}\}.$$

For fixed positive integers i and j, $0 \le i, j \le 4$, not necessarily distinct, the cyclotomic number $(i, j)_5$ is defined as the number of elements $z \in C_i$ such that $1 + z \in C_j$. □

The following lemma [8] shows the elementary relationships among the cyclotomic numbers of order 5.

Lemma 2: [8]

1) For any integers l_1 and l_2, $(i + 5l_1, j + 5l_2)_5 = (i, j)_5$
2) $(i, j)_5 = (5 - i, j - i)_5$
3) $(i, j)_5 = (j, i)_5$
4) $\sum_{j=0}^{4}(i, j)_5 = \frac{p^n-1}{5} - \theta_i$, for $\theta_i = \begin{cases} 1, & \text{if } i = 0 \\ 0, & \text{otherwise} \end{cases}$
5) $\sum_{i=0}^{4}(i, j)_5 = \frac{p^n-1}{5} - \eta_j$, for $\eta_j = \begin{cases} 1, & \text{if } j = 0 \\ 0, & \text{otherwise.} \end{cases}$

□

Let G be a finite abelian group of order $|G|$. A character χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. Then we can define the characters, Gauss sum, and Jacobi sum as in the following definitions.

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

$$\psi_M(\alpha^t) = e^{j\frac{2\pi t}{M}}, \quad \text{if } \alpha^t \in F_{p^n}^*, \quad \text{and } \psi_M(0) = 0$$

where $j = \sqrt{-1}$, α is a primitive element of F_{p^n}, $M|(p^n - 1)$, and $0 \le t \le p^n - 2$. □

Let $\mathrm{tr} : F_{p^n} \to F_p$ be the trace function from F_{p^n} to F_p. Then the function $\chi(c) = e^{\frac{j2\pi \mathrm{tr}(c)}{p}}$ is the canonical additive character of F_{p^n}. Let ψ be a multiplicative character and χ an additive character of F_{p^n}. Then the Gauss sum $G(\psi, \chi)$ is defined by

$$G(\psi, \chi) = \sum_{c \in F_{p^n}^*} \psi(c)\chi(c).$$

Definition 4: [6] Let $\lambda_1, \cdots, \lambda_k$ be k multiplicative characters of F_{p^n}. Then the sum

$$J(\lambda_1, \cdots, \lambda_k) = \sum_{c_1 + \cdots + c_k = 1} \lambda_1(c_1) \cdots \lambda_k(c_k)$$

0-7803-9151-9/05/$20.00 © 2005 IEEE

with the summation extended over all k-tuples $(c_1, \cdots, c_k)$ of elements of F_{p^n} satisfying $c_1 + \cdots + c_k = 1$, is called a Jacobi sum in F_{p^n}. □

For the nontrivial multiplicative character ψ of F_{p^n}, we have $|J(\psi, \psi)|^2 = p^n$.

Throughout the paper, we will denote the multiplicative character of order 5 by ψ and the Jacobi sum $J(\psi^i, \psi^j)$ by $J(i, j)$.

III. The Cyclotomic Numbers of Order 5 over F_{p^n}

From 2) and 3) of Lemma 2, we can name the following 7 cyclotomic numbers of order 5 over F_{p^n} from A to G.

$$A = (0,0)_5$$
$$B = (1,1)_5 = (4,0)_5 = (0,4)_5$$
$$C = (2,2)_5 = (3,0)_5 = (0,3)_5$$
$$D = (3,3)_5 = (2,0)_5 = (0,2)_5$$
$$E = (4,4)_5 = (1,0)_5 = (0,1)_5$$
$$F = (2,1)_5 = (3,4)_5 = (1,4)_5 = (4,1)_5 = (4,3)_5 = (1,2)_5$$
$$G = (3,2)_5 = (2,4)_5 = (1,3)_5 = (3,1)_5 = (2,3)_5 = (4,2)_5.$$

Then, from 4) of Lemma 2, we have

$$A + B + C + D + E = \frac{p^n - 1}{5} - 1$$
$$B + E + 2F + G = \frac{p^n - 1}{5}, \quad C + D + F + 2G = \frac{p^n - 1}{5}.$$

There are 7 unknowns, but we have only 3 equations. What we are going to do is reducing the number of unknowns to 3 by directly evaluating A, B, C, and F using quintic Jacobi sums.

Since $-1 \in C_0$, the cyclotomic number, $(i,j)_5$, $0 \le i, j \le 4$, corresponds to the number of the ordered pair (l_1, l_2) satisfying $\alpha^{5l_1+i} + \alpha^{5l_2+j} = 1$ for integers $0 \le l_1, l_2 < (p^n - 1)/5$. The next theorem tells us that the number of solutions (x, z) of $\alpha^i x^5 + \alpha^j z^5 = 1$, $x, z \in F_{p^n}$ can be expressed in terms of the Jacobi sums [6].

Theorem 5: [Lidl and Niederreiter [6]] The number $N_{i,j}$ of solutions (x, z) of a diagonal equation $\alpha^i x^5 + \alpha^j z^5 = 1$ in $F_{p^n}^2$ is given by

$$N_{i,j} = p^n + \sum_{k_1=1}^{4} \sum_{k_2=1}^{4} \psi^{k_1}(\alpha^{-i}) \psi^{k_2}(\alpha^{-j}) J(k_1, k_2).$$

□

Using the well-known properties of Jacobi sums, we can obtain the following relationships among the quintic Jacobi sums.

Lemma 6: The quintic Jacobi sums have the following equalities:

$$J(1,1) = J(1,3) = J(3,1), \quad J(2,2) = J(1,2) = J(2,1)$$
$$J(3,3) = J(3,4) = J(4,3), \quad J(4,4) = J(4,2) = J(2,4)$$
$$J(1,4) = J(2,3) = J(3,2) = J(4,1) = -1.$$

□

Using Theorem 5 and Lemma 6, we will evaluate A, B, C, and F in terms of Jacobi sums $J(1,1)$ and $J(2,2)$ in the following series of four lemmas. Let $J(1,1) = a + jb$, $J(2,2) = c + jd$, $j = \sqrt{-1}$, and a, b, c, and d be in the real number field $\mathbb{R}$. And let ω be a complex 5-th root of unity.

Lemma 7: The cyclotomic number $A = (0,0)_5$ over F_{p^n} is given as

$$25A = p^n + 6(a + c) - 14.$$

Proof: $A = (0,0)_5$ is the number of solutions $x^5 (\neq 0, 1)$ of $x^5 + z^5 = 1$, for a given $z^5 \in F_{p^n} \backslash \{0, 1\}$. It is clear that a single solution x^5 $(\neq 0, 1)$ in the computation of $(0,0)_5$ corresponds to 25 solutions $(x\beta^i, z\beta^j)$, $0 \le i, j \le 4$, in $N_{0,0}$, where $\beta = \alpha^{\frac{p^n - 1}{5}}$. Also in the computation of $(0,0)_5$, we have to exclude the ten solutions (x, z) in $N_{0,0}$, namely, $(0,1)$, $(0,\beta)$, $(0,\beta^2)$, $(0,\beta^3)$, $(0,\beta^4)$, $(1,0)$, $(\beta,0)$, $(\beta^2,0)$, $(\beta^3,0)$, $(\beta^4,0)$, since they correspond to either $x^5 = 0$ or $x^5 = 1$.

Thus we have

$$(0,0)_5 = \frac{N_{0,0} - 10}{25}.$$

From Lemma 6, we have

$$N_{0,0} = p^n + 3[J(1,1) + J(2,2) + J(3,3) + J(4,4)] - 4.$$

Let $\overline{J}(\cdot,\cdot)$ denote the complex conjugate of $J(\cdot,\cdot)$. Since $\overline{J}(1,1) = J(4,4)$ and $\overline{J}(2,2) = J(3,3)$, we have done. □

Lemma 8: The cyclotomic number $B = (4,0)_5$ over F_{p^n} is given as

$$50B = 2p^n - 3(a + c) + \sqrt{5}(a - c) - \sqrt{5 + 2\sqrt{5}}(b + 3d)$$
$$- \sqrt{5 - 2\sqrt{5}}(3b - d) - 4.$$

Proof: $B = (4,0)_5$ is the number of solutions x^5 of $\alpha^{-1} x^5 + z^5 = 1$, for a given $z^5 \in F_{p^n} \backslash \{0, 1\}$. If $x = 0$, we have $z^5 = 1$. Similarly to the previous case, we remove 5 solutions for $N_{4,0}$ and thus we have

$$(4,0)_5 = \frac{N_{4,0} - 5}{25}.$$

From Lemma 6, we have

$$N_{4,0} = p^n + (2\omega + \omega^3) J(1,1) + (\omega + 2\omega^2) J(2,2)$$
$$+ (2\omega^3 + \omega^4) J(3,3) + (\omega^2 + 2\omega^4) J(4,4) + 1.$$

Since $\overline{2\omega + \omega^3} = 2\omega^4 + \omega^2$ and $\overline{\omega + 2\omega^2} = \omega^4 + 2\omega^3$, we have done. □

Lemma 9: The cyclotomic number $C = (3,0)_5$ over F_{p^n} is given as

$$50C = 2p^n - 3(a + c) - \sqrt{5}(a - c) - \sqrt{5 + 2\sqrt{5}}(3b - d)$$
$$+ \sqrt{5 - 2\sqrt{5}}(b + 3d) - 4.$$

Proof: $C = (3,0)_5$ is the number of solutions x^5 of $\alpha^{-2} x^5 + z^5 = 1$, for a given $z^5 \in F_{p^n} \backslash \{0, 1\}$. If $x = 0$, we have

$z^5=1$. Similarly to the previous case, we remove 5 solutions for $N_{3,0}$ and thus we have

$$(3,0)_5 = \frac{N_{3,0}-5}{25}.$$

From Lemma 6, we have

$$N_{3,0} = p^n + (2\omega^2+\omega)J(1,1) + (\omega^2+2\omega^4)J(2,2) + (2\omega+\omega^3)J(3,3) + (\omega^4+2\omega^3)J(4,4)+1.$$

Since $\overline{2\omega^2+\omega} = 2\omega^3+\omega^4$ and $\overline{\omega^2+2\omega^4} = \omega^3+2\omega$, we have done. □

Lemma 10: The cyclotomic number $F=(3,4)_5$ over F_{p^n} is given as

$$25F = p^n + (a+c) - \sqrt{5}(a-c) + 1.$$

Proof: $F=(3,4)_5$ is the number of solutions x^5 of $\alpha^{-2}x^5 + \alpha^{-1}z^5 = 1$, for a given $z^5 \in F^*_{p^n}$. Since α is a primitive element of F_{p^n}, $x=0$ cannot be a solution of the above equation. Thus we have

$$(3,4)_5 = \frac{N_{3,4}}{25}.$$

From Lemma 6, we have

$$\begin{aligned} N_{3,4} &= p^n + (\omega^3+\omega^2+1)(J(1,1)+J(4,4)) \\ &\quad +(\omega^4+\omega+1)(J(2,2)+J(3,3)) - (\omega^4+\omega^3+\omega^2+\omega) \\ &= p^n - 4Re[\omega]Re[J(1,1)] - 4Re[\omega^2]Re[J(2,2)]+1. \end{aligned}$$

Since $Re[\omega] = \cos(\frac{2\pi}{5}) = (-1+\sqrt{5})/4$ and $Re[\omega^2] = \cos(\frac{4\pi}{5}) = (-1-\sqrt{5})/4$, we have done. □

Using the previous lemmas, we can calculate the 7 parameters $A, B, \cdots, G$ as follows.

Theorem 11: Let $x = 2(a+c)$, $25w = 2\sqrt{5}(a-c)$, $50v = -2\sqrt{5+2\sqrt{5}}(b+3d) - 2\sqrt{5-2\sqrt{5}}(3b-d)$, and $50u = -2\sqrt{5+2\sqrt{5}}(3b-d) + 2\sqrt{5-2\sqrt{5}}(b+3d)$. Then the cyclotomic numbers of order 5 over F_{p^n} are given as

$$25A = p^n + 3x - 14 \quad (1)$$
$$100B = 4p^n - 3x + 25w + 50v - 16 \quad (2)$$
$$100C = 4p^n - 3x - 25w + 50u - 16 \quad (3)$$
$$100D = 4p^n - 3x - 25w - 50u - 16 \quad (4)$$
$$100E = 4p^n - 3x + 25w - 50v - 16 \quad (5)$$
$$50F = 2p^n + x - 25w + 2 \quad (6)$$
$$50G = 2p^n + x + 25w + 2 \quad (7)$$

where the integers x, u, v, and w satisfy that $x^2+125w^2+50u^2+50v^2 = 16p^n$, $v^2-4uv-u^2 = xw$, and $x \equiv 1 \bmod 5$.

Proof: From Lemmas 7–10, it is not difficult to derive D, E, and G. By substituting $x=2(a+c)$, $25w = 2\sqrt{5}(a-c)$, $50v = -2\sqrt{5+2\sqrt{5}}(b+3d) - 2\sqrt{5-2\sqrt{5}}(3b-d)$, and $50u = -2\sqrt{5+2\sqrt{5}}(3b-d) + 2\sqrt{5-2\sqrt{5}}(b+3d)$, we can derive (1)–(7).

From (1), it is clear that x is an integer. And from (6) and (7), we have $G-F=w$. Thus w is an integer. From (3) and (4), we have $C-D=u$. Thus u is an integer. Finally from (2) and (5), we have $B-E=v$. Thus v is an integer.

Next, we will show that $x^2+125w^2+50u^2+50v^2 = 16p^n$ and $v^2-4uv-u^2 = xw$. Using

$$x^2 = 4(a+c)^2, \quad 125w^2 = 4(a-c)^2$$
$$50v^2 = \frac{4}{50}\Big[(5+2\sqrt{5})(b+3d)^2 + (5-2\sqrt{5})(3b-d)^2 + 2\sqrt{5}(b+3d)(3b-d)\Big] \quad (8)$$
$$50u^2 = \frac{4}{50}\Big[(5+2\sqrt{5})(3b-d)^2 + (5-2\sqrt{5})(b+3d)^2 - 2\sqrt{5}(b+3d)(3b-d)\Big], \quad (9)$$

we have $x^2+125w^2 = 8(a^2+c^2)$ and $50u^2+50v^2 = 8(b^2+d^2)$. Since $a^2+b^2=p^n$ and $c^2+d^2=p^n$, we have $x^2+125w^2+50u^2+50v^2 = 16p^n$.

From (8) and (9), we have

$$v^2-u^2 = \frac{4\sqrt{5}}{125}(-b^2+4bd+d^2) \quad (10)$$
$$4uv = \frac{4\sqrt{5}}{125}(4b^2+4bd-4d^2). \quad (11)$$

From (10) and (11), we have

$$v^2-4uv-u^2 = \frac{4\sqrt{5}}{25}(d^2-b^2) = \frac{4\sqrt{5}}{25}(a^2-c^2) = xw.$$

From (1), $p^n+3x-4 \equiv 0 \bmod 5$. Since $p^n \equiv 1 \bmod 5$, we have $x \equiv 1 \bmod 5$.

□

Now, we have to find the Jacobi sums $J(1,1)$ and $J(2,2)$.

A. The Case for $p \not\equiv 1 \bmod 5$

For $p \not\equiv 1 \bmod 5$, we can obtain the Jacobi sums over F_{p^n} using Stickelberger's Theorem.

Theorem 12: (Stickelberger's Theorem) [6] Let q be a prime power, ψ a nontrivial multiplicative character on F_{q^2} of order M dividing $q+1$, and χ the canonical additive character of F_{q^2}. Then,

$$G(\psi,\chi) = \begin{cases} q, & \text{if } M \text{ odd or } \frac{q+1}{M} \text{ even} \\ -q, & \text{if } M \text{ even and } \frac{q+1}{M} \text{ odd.} \end{cases}$$

□

For evaluating Jacobi sum $J(1,1)$ on F_{p^n}, we will use the lifting idea given in the following theorem.

Theorem 13: [6] Let $\lambda'_1, \cdots, \lambda'_k$ be multiplicative characters of F_q, not all of which are trivial. Suppose that $\lambda'_1, \cdots, \lambda'_k$ are lifted to characters $\lambda_1, \cdots, \lambda_k$, respectively, of the finite extension field E of F_q with $[E:F_q]=m$. Then

$$J(\lambda_1, \cdots, \lambda_k) = (-1)^{(m-1)(k-1)} J(\lambda'_1, \cdots, \lambda'_k)^m.$$

□

Lemma 14: For $p \not\equiv 1 \bmod 5$, the quintic Jacobi sums over F_{p^n} are given as

$$J(1,1) = J(2,2) = (-1)^{m-1}p^{n/2}$$

where

$$m = \begin{cases} \frac{n}{4}, & \text{if } p \equiv 2 \text{ or } 3 \bmod 5 \\ \frac{n}{2}, & \text{if } p \equiv 4 \bmod 5. \end{cases}$$

Proof: For $p \equiv 2 \bmod 5$ and $p^n \equiv 1 \bmod 5$, n must be a multiple of 4. Let $n = 4m$ and $q = p^2$. Let ψ' be a multiplicative character on F_q. By Stickelberger's Theorem, $G(\psi', \chi) = G(\psi'^2, \chi) = p^2$. Thus the Jacobi sum $J(\psi', \psi')$ on F_q is evaluated as

$$J(\psi', \psi') = \frac{(G(\psi', \chi))^2}{G(\psi'^2, \chi)} = \frac{p^4}{p^2} = p^2.$$

By lifting, we have $J(1,1) = (-1)^{m-1}p^{2m} = (-1)^{m-1}p^{n/2}$. The case for $p \equiv 3 \bmod 5$ is similar to the case for $p \equiv 2 \bmod 5$.

For the case when $p \equiv 4 \bmod 5$, n must have the divisor 2. Let $n = 2m$ and $q = p$. By Stickelberger's Theorem, $G(\psi', \chi) = G(\psi'^2, \chi) = p$. By lifting, we also have $J(1,1) = (-1)^{m-1}p^m = (-1)^{m-1}p^{n/2}$.

Since ψ^2 is also a multiplicative character of order 5, we can obtain the same result for $J(2,2)$.

□

Using Theorem 11 and Lemma 14, the cyclotomic numbers of order 5 over F_{p^n} for $p \not\equiv 1 \bmod 5$ can be computed as follows:

Theorem 15: For $p \not\equiv 1 \bmod 5$, we have

$$\begin{aligned} 25A &= p^n - 12(-1)^m p^{n/2} - 14 \\ 25B &= 25C = 25D = 25E = p^n + 3(-1)^m p^{n/2} - 4 \\ 25F &= 25G = p^n - 2(-1)^m p^{n/2} + 1 \end{aligned}$$

where

$$m = \begin{cases} \frac{n}{4}, & \text{if } p \equiv 2 \text{ or } 3 \bmod 5 \\ \frac{n}{2}, & \text{if } p \equiv 4 \bmod 5. \end{cases}$$

Proof: From Lemma 14, we have $x = 4(-1)^{m-1}p^{n/2}$ and $w = v = u = 0$. From Theorem 11, we can obtain the above relations. □

B. The Case for $p \equiv 1 \bmod 5$

Using the well known result of Jacobi sums over F_p [1], we will evaluate $J(1,1)$ and $J(2,2)$ over F_{p^n}.

Theorem 16: [1] For $p \equiv 1 \bmod 5$, the quintic Jacobi sums over F_p are given as

$$\begin{aligned} 4J(1,1) &= x_0 + 5w_0\sqrt{5} + ju_0\sqrt{50 + 10\sqrt{5}} \\ &\quad + jv_0\sqrt{50 - 10\sqrt{5}} \\ 4J(2,2) &= x_0 - 5w_0\sqrt{5} + jv_0\sqrt{50 + 10\sqrt{5}} \\ &\quad - ju_0\sqrt{50 - 10\sqrt{5}} \end{aligned}$$

where $j = \sqrt{-1}$ and the integers x_0, w_0, v_0, and u_0 are the solutions of

$$\begin{aligned} 16p &= x_0^2 + 125w_0^2 + 50v_0^2 + 50u_0^2 \\ x_0w_0 &= v_0^2 - u_0^2 - 4u_0v_0, \text{ and } x_0 \equiv 1 \pmod 5). \end{aligned} \quad (12)$$

□

Note that if (x_0, w_0, v_0, u_0) is a solution of (12), then $(x_0, w_0, -v_0, -u_0)$, $(x_0, -w_0, -u_0, v_0)$, and $(x_0, -w_0, u_0, v_0)$ are also solutions of (12). The integers, x_0, w_0, v_0, and u_0 satisfying (12) are listed in Table I for $p < 100$ and $p \equiv 1 \bmod 5$.

TABLE I
THE INTEGERS x_0, w_0, v_0, AND u_0 SATISFYING THE CONDITIONS (12) FOR $p < 100$ AND $p \equiv 1 \bmod 5$ [1].

p	x_0	w_0	v_0	u_0
11	1	1	1	0
31	11	−1	1	2
41	−9	−1	3	0
61	1	1	−1	4
71	−19	1	−3	−2

Using the lifting idea in Theorem 13, we can obtain the Jacobi sums over the extension field F_{p^n}. Let

$$\begin{aligned} D_1(k,r,s) &= \binom{n}{2k}\binom{k}{s}\binom{n-2k}{r} \\ D_2(k,r,s) &= \binom{n}{2k+1}\binom{k}{s}\binom{n-2k}{r} \\ B(k,r,s) &= x_0^{n-2k-r+s}w_0^{r+s}(u_0^2+v_0^2)^{k-s}(-10)^k 5^{k-s+r}. \end{aligned}$$

Lemma 17: Let

$$H_1 = \frac{(u_0\sqrt{50+10\sqrt{5}} + v_0\sqrt{50-10\sqrt{5}})}{x_0 + 5w_0\sqrt{5}}.$$

Then we have

$$\begin{aligned} a &= \frac{(-1)^{n-1}}{4^n} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_1(k,r,s)B(k,r,s)\sqrt{5}^{s+r}(-1)^s \\ b &= \frac{(-1)^{n-1}}{4^n} H_1 \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_2(k,r,s)B(k,r,s) \\ &\quad \times \sqrt{5}^{s+r}(-1)^s \end{aligned}$$

where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. □

Lemma 18: Let

$$H_2 = \frac{(v_0\sqrt{50+10\sqrt{5}} - u_0\sqrt{50-10\sqrt{5}})}{x_0 - 5w_0\sqrt{5}}.$$

Then we have

$$\begin{aligned} c &= \frac{(-1)^{n-1}}{4^n} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_1(k,r,s)B(k,r,s)\sqrt{5}^{s+r}(-1)^r \\ d &= \frac{(-1)^{n-1}}{4^n} H_2 \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_2(k,r,s)B(k,r,s) \\ &\quad \times \sqrt{5}^{s+r}(-1)^r. \end{aligned}$$

□

IV. AUTOCORRELATION DISTRIBUTIONS OF 5-ARY SIDEL'NIKOV SEQUENCES

The M-ary Sidel'nikov sequence $s(t)$ of period $N = p^n - 1$ [7] is defined as

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

where k_0 is some integer modulo M. The autocorrelation function of Sidel'nikov sequences is defined as

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

and in [5], it is shown that $R(\tau)$ is written as the following form

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

where ω_M is a complex M-th root of unity.

Also in [5], the autocorrelation distributions of M-ary Sidel'nikov sequences are expressed in terms of the cyclotomic numbers over F_{p^n} of order M. Using the cyclotomic numbers of order 5 in Section III, we can obtain the autocorrelation distribution of 5-ary Sidel'nikov sequences as in the following theorem.

Theorem 19: Let $N(R_{u,v})$ be the number of $R_{u,v}$ in $R(\tau)$ for $0 \le \tau \le N-1$. Then the out-of-phase autocorrelation distribution of a 5-ary Sidel'nikov sequence of period $p^n - 1$ is given as:

$$\begin{aligned}
N(0) &= A + 2B + 2C + 2D + 2E = (9p^n - 3x - 46)/25 \\
N(R_{1,1}) &= N(R_{4,4}) = F,\ N(R_{3,3}) = N(R_{2,2}) = G \\
N(R_{1,3}) &= N(R_{2,4}) = 2F = (2p^n + x - 25w + 2)/25 \\
N(R_{3,4}) &= N(R_{1,2}) = 2G = (2p^n + x + 25w + 2)/25 \\
N(R_{1,4}) &= B + E = (4p^n - 3x + 25w - 16)/50 \\
N(R_{2,3}) &= C + D = (4p^n - 3x - 25w - 16)/50.
\end{aligned}$$

□

Note that if $w = 0$, we have $B + E = C + D$ and $F = G$. Although the partition itself of $F_{p^n}^*$ into cyclotomic classes is invariant if we use the primitive element $\beta(= \alpha^s)$ instead of α, the name of each class, and accordingly the cyclotomic numbers can be switched. Let $(i,j)_{M,\alpha}$ denote the cyclotomic number $(i,j)_M$ obtained by using α as the primitive element. Then, for another primitive element $\beta(= \alpha^s)$, we have

$$(i,j)_{M,\alpha} = (is, js)_{M,\beta}.$$

Since the autocorrelation distribution of a 5-ary Sidelnikov sequence is expressed in terms of the cyclotomic number of order 5, the distribution can be altered if we change the primitive element.

Theorem 20: For $w \neq 0$, there are two different types of the autocorrelation distributions for the given period of 5-ary Sidel'nikov sequences.

Proof: Let $\beta = \alpha^{-s}$. If $s \equiv 4 \bmod 5$, then we have

$$\begin{aligned}
&A_\alpha = A_\beta,\ F_\alpha = F_\beta,\ G_\alpha = G_\beta \\
&B_\alpha = (1,1)_{5,\alpha} = (4,4)_{5,\beta} = E_\beta, \text{vice versa} \\
&C_\alpha = (2,2)_{5,\alpha} = (3,3)_{5,\beta} = D_\beta, \text{vice versa}
\end{aligned}$$

where the subscripts α and β denote the primitive elements of F_{p^n} used for the construction of the cyclotomic classes of order 5. Then the autocorrelation distribution of the Sidel'nikov sequence remains the same when we change the primitive element α with β. Similarly, if $s \equiv 2 \bmod 5$, we have

$$\begin{aligned}
&A_\alpha = A_\beta \\
&B_\alpha = (1,1)_{5,\alpha} = (2,2)_{5,\beta} = C_\beta \\
&C_\alpha = (2,2)_{5,\alpha} = (4,4)_{5,\beta} = E_\beta \\
&E_\alpha = (4,4)_{5,\alpha} = (3,3)_{5,\beta} = D_\beta \\
&D_\alpha = (3,3)_{5,\alpha} = (1,1)_{5,\beta} = B_\beta \\
&F_\alpha = (2,1)_{5,\alpha} = (4,2)_{5,\beta} = G_\beta, \text{vice versa}
\end{aligned}$$

and then the autocorrelation distribution of the 5-ary Sidel'nikov sequence is altered when we change the primitive element α with β. The autocorrelation distribution for $s \equiv 3 \bmod 5$ is the same as that for $s \equiv 2 \bmod 5$. If $w = 0$, we have $B + E = C + D$ and $F = G$, which means that there exists only a single autocorrelation distribution for the given period of 5-ary Sidel'nikov sequences. □

ACKNOWLEDGMENT

This work was supported by KT TETRA project.

REFERENCES

[1] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, *Canadian Mathematical Society Series of Monographs and Advanced Text.* vol. 21, New York: Wiley-Interscience, 1998.

[2] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. NY: Elsevier, 2004.

[3] L. E. Dickson, "Cyclotomy, higher congruences, and Waring's problem," *Amer. J. Math.*, vol. 57, pp. 391–424, and 463–474, 1935.

[4] S. A. Katre and A. R. Rajwade, "Unique determination of cyclotomic numbers of order five," *Manuscripta Math.*, vol. 53 no. 1–2, pp. 65–75, 1985.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," submmited for publication, 2004.

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

[7] 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.

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