Derivation of Cyclotomic Numbers of Order 5 over F_{p^n} [1]

*Jung-Soo Chung^{O}, *Young-Sik Kim, *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 derive the cycltomic numbers of order 5 over the extension field F_{p^n} using well-known results of quintic Jacobi sums over F_p [5]. For $p \not\equiv 1 \bmod 5$, we have obtained the simple closed-form expression of the cyclotomic numbers of order 5. For $p \equiv 1 \bmod 5$, the expression involves rather complicated summations.

1. Introduction

Recently, Kim, Chung, No, and Chung [6] have shown the relation between the autocorrelation distribution of M-ary Sidel'nikov sequences and the cyclotomic numbers over F_{p^n} of order M.

For prime $p = Md+1$, various studies have discussed the cyclotomic numbers of order M [1],[2],[3],[5]. But most of these studies have focussed on the cyclotomic numbers over a prime field F_p. The cyclotomic numbers of order 3,4,6, and 8 over an extension field F_{p^n} are given by Store [3]. But to our knowledge, the closed-form expression for the cyclotomic numbers of order 5 over F_{p^n} is not known yet.

In this paper, we derive the cycltomic numbers of order 5 over the extension field F_{p^n} using well-known results of quintic Jacobi sums over F_p [5]. For $p \not\equiv 1 \bmod 5$, we have obtained the simple closed-form expression of the cyclotomic numbers of order 5. For $p \equiv 1 \bmod 5$, the expression involves rather complicated summations. Our method of using Jacobi sums can also be applicable to derive the cyclotomic numbers having other orders over the extension fields.

2. Preliminaries

Let $N = p^n - 1$, $5|N$, and α be a primitive element of F_{p^n}. And let ψ be a multiplicative character on F_{p^n} of order 5. Then the cyclotomic number of order 5 is defined as follows.

Definition 1 The cyclotomic class C_u, $0 \le u \le 4$, in F_{p^n} is defined as

$$C_u = \left\{\alpha^{5l+u} \mid 0 \le l < \frac{p^n-1}{5}\right\}.$$

For fixed positive integers u and v, not necessarily distinct, the cyclotomic number $(u,v)_5$ is defined as the number of elements $z \in C_u$ such that $1+z \in C_v$. □

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

The following lemma [3] shows the elementary relationships among the cyclotomic numbers of order 5.

Lemma 2 [3]

1) For any integers l_1, 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) $\sum_{j=0}^{4}(i,j)_5 = \frac{p^n-1}{5} - \theta_i$
where $\theta_i = \begin{cases} 1, & \text{if } i=0 \\ 0, & \text{otherwise} \end{cases}$

5) $\sum_{i=0}^{4}(i,j)_5 = \frac{p^n-1}{5} - \eta_j$
where $\eta_j = \begin{cases} 1, & \text{if } j=0 \\ 0, & \text{otherwise.} \end{cases}$

□

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

From 2) and 3) of Lemma 2, we can classify the following 7 parameters from A to G.

$$\begin{aligned}
A &= (0,0)_5\\
B &= (1,1)_5 = (4,0)_5 = (0,4)_5\\
C &= (2,2)_5 = (3,0)_5 = (0,3)_5\\
D &= (3,3)_5 = (2,0)_5 = (0,2)_5\\
E &= (4,4)_5 = (1,0)_5 = (0,1)_5\\
F &= (2,1)_5 = (3,4)_5 = (1,4)_5 = (4,1)_5\\
&= (4,3)_5 = (1,2)_5\\
G &= (3,2)_5 = (2,4)_5 = (1,3)_5 = (3,1)_5\\
&= (2,3)_5 = (4,2)_5.
\end{aligned}$$

Then, from 4) of Lemma 2, we have

$$A+B+C+D+E=\frac{N}{5}-1 \quad (1)$$

$$B+E+2F+G=\frac{N}{5} \quad (2)$$

$$C+D+F+2G=\frac{N}{5}. \quad (3)$$

There are 7 unknown parameters, but we have only 3 equations. Here, we are going to evaluate A, B, C, and F using Jacobi sums of order 5.

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

Theorem 3 [Lidl and Niederreiter [4]] The number $N_{u,v}$ of solutions of a diagonal equation $\alpha^u x^5+\alpha^v z^5=1$ in $F_{p^n}^2$ is given by

$$N_{u,v}=p^n+\sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\psi^{j_1}(\alpha^{-u})\psi^{j_2}(\alpha^{-v})J(\psi^{j_1},\psi^{j_2}).$$

□

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

Lemma 4 The quintic Jacobi sums have the following equalities:

$$\begin{aligned}
J(\psi,\psi)&=J(\psi,\psi^3)=J(\psi^3,\psi)\\
J(\psi^2,\psi^2)&=J(\psi,\psi^2)=J(\psi^2,\psi)\\
J(\psi^3,\psi^3)&=J(\psi^3,\psi^4)=J(\psi^4,\psi^3)\\
J(\psi^4,\psi^4)&=J(\psi^4,\psi^2)=J(\psi^2,\psi^4)\\
J(\psi,\psi^4)&=J(\psi^2,\psi^3)=J(\psi^3,\psi^2)=J(\psi^4,\psi)=-1.
\end{aligned}$$

□

Using Theorem 3 and Lemma 4, we will evaluate A, B, C, and F in the following lemmas.

Lemma 5 The cyclotomic number $A=(0,0)_5$ is given as

$$25A=p^n+6Re[J(\psi,\psi)]+6Re[J(\psi^2,\psi^2)]-14$$

where $Re(\cdot)$ denotes real part.

Proof: $A=(0,0)_5$ is the number of solutions of $x^5+z^5=1$, $x,z \in F_{p^m}\backslash\{0,1\}$, $0 \le x, z < \frac{N}{5}$. 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 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

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

From Lemma 4, we have

$$\begin{aligned}
N_{0,0}&=p^n+\sum_{j_1=1}^{4}\sum_{j_2=1}^{4}J(\psi^{j_1},\psi^{j_2})\\
&=p^n+3[J(\psi,\psi)+J(\psi^2,\psi^2)+J(\psi^3,\psi^3)\\
&\quad+J(\psi^4,\psi^4)]-4.
\end{aligned}$$

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

$$N_{0,0}=p^n+6Re[J(\psi,\psi)]+6Re[J(\psi^2,\psi^2)]-4.$$

□

Lemma 6 The cyclotomic number $B=(4,0)_5$ is given as

$$\begin{aligned}
25B&=p^n+2Re[(2\omega+\omega^3)J(\psi,\psi)]\\
&\quad+2Re[(\omega+2\omega^2)J(\psi^2,\psi^2)]-4.
\end{aligned}$$

Proof: $B=(4,0)_5$ is the number of solutions of $\alpha^{-1}x^5+z^5=1$, $x \in F_{p^m}^*$, $z \in F_{p^m}\backslash\{0,1\}$, $0 \le x, z < \frac{N}{5}$. 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 4, we have

$$\begin{aligned}
N_{4,0}&=p^n+\sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\psi^{j_1}(\alpha)J(\psi^{j_1},\psi^{j_2})\\
&=p^n+\sum_{j_1=1}^{4}\sum_{j_2=1}^{4}\omega^{j_1}J(\psi^{j_1},\psi^{j_2})\\
&=p^n+(2\omega+\omega^3)J(\psi,\psi)+(\omega+2\omega^2)J(\psi^2,\psi^2)\\
&+(2\omega^3+\omega^4)J(\psi^3,\psi^3)+(\omega^2+2\omega^4)J(\psi^4,\psi^4)+1.
\end{aligned}$$

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

$$\begin{aligned}
N_{4,0}&=p^n+2Re[(2\omega+\omega^3)J(\psi,\psi)]\\
&\quad+2Re[(\omega+2\omega^2)J(\psi^2,\psi^2)]+1.
\end{aligned}$$

□

Lemma 7 The cyclotomic number $C = (3,0)_5$ is given as

$$\begin{aligned}25C &= p^n + 2Re[(2\omega^2+\omega)J(\psi,\psi)] \\ &\quad + 2Re[(\omega^2+2\omega^4)J(\psi^2,\psi^2)] - 4.\end{aligned}$$

Proof: $C = (3,0)_5$ is the number of solutions of $\alpha^{-2}x^5 + z^5 = 1$, $x \in F^*_{p^m}$, $z \in F_{p^m}\backslash\{0,1\}$, $0 \le x, z < \frac{N}{5}$. 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 4, we have

$$\begin{aligned}N_{3,0} &= p^n + \sum_{j_1=1}^{4}\sum_{j_2=1}^{4} \psi^{j_1}(\alpha^2)J(\psi^{j_1},\psi^{j_2}) \\ &= p^n + \sum_{j_1=1}^{4}\sum_{j_2=1}^{4} \omega^{2j_1}J(\psi^{j_1},\psi^{j_2}) \\ &= p^n + (2\omega^2+\omega)J(\psi,\psi) + (\omega^2+2\omega^4)J(\psi^2,\psi^2) \\ &\quad + (2\omega+\omega^3)J(\psi^3,\psi^3) + (\omega^4+2\omega^3)J(\psi^4,\psi^4) + 1.\end{aligned}$$

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

$$\begin{aligned}N_{3,0} &= p^n + 2Re[(2\omega^2+\omega)J(\psi,\psi)] \\ &\quad + 2Re[(\omega^2+2\omega^4)J(\psi^2,\psi^2)] + 1.\end{aligned}$$

□

Lemma 8 The cyclotomic number $F = (3,4)_5$ is given as

$$\begin{aligned}25F &= p^n + (Re[J(\psi,\psi)] + Re[J(\psi^2,\psi^2)]) \\ &\quad - \sqrt{5}(Re[J(\psi,\psi)] - Re[J(\psi^2,\psi^2)]) + 1.\end{aligned}$$

Proof: $F = (3,4)_5$ is the number of solutions of $\alpha^{-2}x^5 + \alpha^{-1}z^5 = 1$, $x \in F^*_{p^m}$, $z \in F_{p^m}\backslash\{0,1\}$, $0 \le x, z < \frac{N}{5}$. In this case, $z^5 = \alpha$ when $x = 0$. Since α is a primitive element of F_{p^n}, we have $1 = (z^5)^{\frac{p^n-1}{5}} = \alpha^{\frac{p^n-1}{5}} \ne 1$. Thus we have

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

From Lemma 4, we have

$$\begin{aligned}N_{3,4} &= p^n + \sum_{j_1=1}^{4}\sum_{j_2=1}^{4} \omega^{2j_1+j_2}J(\psi^{j_1},\psi^{j_2}) \\ &= p^n + (\omega^3+\omega^2+1)(J(\psi,\psi)+J(\psi^4,\psi^4)) \\ &\quad + (\omega^4+\omega+1)(J(\psi^2,\psi^2)+J(\psi^3,\psi^3)) \\ &\quad - (\omega^4+\omega^3+\omega^2+\omega) \\ &= p^n - (\omega^4+\omega)2Re[J(\psi,\psi)] \\ &\quad - (\omega^3+\omega^2)2Re[J(\psi^2,\psi^2)] + 1 \\ &= p^n - 4Re[\omega]Re[J(\psi,\psi)] - 4Re[\omega^2]Re[J(\psi^2,\psi^2)] \\ &\quad + 1.\end{aligned}$$

Since $\omega = \cos(\frac{2\pi}{5}) + j\sin(\frac{2\pi}{5})$ and $\omega^2 = \cos(\frac{4\pi}{5}) + j\sin(\frac{2\pi}{5})$, we have

$$\begin{aligned}N_{3,4} &= p^n - 4\cos(\frac{2\pi}{5})Re[J(\psi,\psi)] \\ &\quad - 4\cos(\frac{4\pi}{5})Re[J(\psi^2,\psi^2)] + 1.\end{aligned}$$

Since $\cos(\frac{2\pi}{5}) = \frac{-1+\sqrt{5}}{4}$ and $\cos(\frac{4\pi}{5}) = \frac{-1-\sqrt{5}}{4}$, we have

$$\begin{aligned}N_{3,4} &= p^n + (Re[J(\psi,\psi)] + Re[J(\psi^2,\psi^2)]) \\ &\quad - \sqrt{5}(Re[J(\psi,\psi)] - Re[J(\psi^2,\psi^2)]) + 1.\end{aligned}$$

□

The next part is about the evaluations of the Jacobi sums $J(\psi,\psi)$ and $J(\psi^2,\psi^2)$.

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 9 (Stickelberger's Theorem) [4] 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,

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

□

Now we have to evaluate Jacobi sum $J(\psi,\psi)$ on F_{p^n}. We will use the lifting idea given in the following theorem.

Theorem 10 [4] Let $\lambda'_1, \cdots, \lambda'_k$ be multiplicative characters of F_q, not all of which are trivial. Suppose $\lambda'_1, \cdots, \lambda'_k$ 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 11 For $p \not\equiv 1 \bmod 5$, the quintic Jacobi sums over F_{p^n} are given as

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

If $p \equiv 2 \bmod 5$ or $p \equiv 3 \bmod 5$, $n = 4m$ and if $p \equiv 4 \bmod 5$, $n = 2m$.

Proof: Since $p \equiv 2 \bmod 5$ and $5|p^n - 1$, $4|n$. Let $n = 4m$ and $q = p^2$. By Stickelberger's Theorem, $G(\psi,\chi) = G(\psi^2,\chi) = p^2$. Thus we have

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

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

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

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

□

Now, we can determine 7 cyclotomic numbers over F_{p^n} using Lemmas 5–8. For $p \not\equiv 1 \bmod 5$, from (1), (2), and (3), we can obtain:

Theorem 12 For $p \not\equiv 1 \bmod 5$, we have

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

If $p \equiv 2 \bmod 5$ or $p \equiv 3 \bmod 5$, $n = 4m$ and if $p \equiv 4 \bmod 5$, $n = 2m$. □

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

For $p \equiv 1 \bmod M$, it is well-known the Jacobi sum over F_p for orders $M = 3, 4, 5, 6, 7, 8, 10, 12, 16, 20$, and 24 [5]. Using these results, we will evaluate $J(\psi, \psi)$ and $J(\psi^2, \psi^2)$ over F_{p^n}.

Theorem 13 [5] For $p \equiv 1 \bmod 5$, the quintic Jacobi sums over F_p are given as

$$4J(\psi, \psi) = x + 5w\sqrt{5} + ju\sqrt{50 + 10\sqrt{5}} + jv\sqrt{50 - 10\sqrt{5}} \tag{4}$$

$$4J(\psi^2, \psi^2) = x - 5w\sqrt{5} + jv\sqrt{50 + 10\sqrt{5}} - ju\sqrt{50 - 10\sqrt{5}} \tag{5}$$

where the integers x, w, v, and u have the following relations

$$\begin{aligned} 16p &= x^2 + 125w^2 + 50v^2 + 50u^2, \\ xw &= v^2 - u^2 - 4uv, \text{ and } x \equiv 1 \pmod 5. \end{aligned} \tag{6}$$

□

The integers, x, w, v, and u satisfying (6) is listed in Table 1.

Using the lifting idea in Theorem 10, we can obtain the Jacobi sums over the extension field F_{p^n}.

Lemma 14 Let $D_1(k, r, s) = \binom{n}{2k}\binom{k}{s}\binom{n-2k}{r}$, $D_2(k, r, s) = \binom{n}{2k+1}\binom{k}{s}\binom{n-2k}{r}$, $B(k, r, s) = x^{n-2k-r+s}w^{r+s}(u^2 + v^2)^{k-s}(-10)^k 5^{k-s+r}$, and $H_1 = \frac{(u\sqrt{50+10\sqrt{5}}+v\sqrt{50-10\sqrt{5}})}{x+5w\sqrt{5}}$. Then we have

$$Re[J(\psi, \psi)] = \frac{(-1)^{n-1}}{4^n} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_1(k, r, s) B(k, r, s) \times \sqrt{5}^{s+r}(-1)^s \tag{7}$$

Table 1: The integers x, w, v, and u satisfying the conditions (6) for $p < 100$ [5].

p	x	w	v	u
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

and

$$Im[J(\psi, \psi)] = \frac{(-1)^{n-1}}{4^n} H_1 \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_2(k, r, s) \times B(k, r, s)\sqrt{5}^{s+r}(-1)^s \tag{8}$$

where $Im(\cdot)$ denotes imaginary part and $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.

Proof: We can lift the Jacobi sums over F_p in (4) and (5) to the extension field F_{p^n}. From Theorem 10, we have

$$J(\psi, \psi) = \frac{(-1)^{n-1}}{4^n}\Big(x + 5w\sqrt{5} + ju\sqrt{50 + 10\sqrt{5}} + jv\sqrt{50 - 10\sqrt{5}}\Big)^n.$$

Using binomial expansion, we have (7) and (8).

□

Lemma 15 Let $D_1(k, r, s) = \binom{n}{2k}\binom{k}{s}\binom{n-2k}{r}$, $D_2(k, r, s) = \binom{n}{2k+1}\binom{k}{s}\binom{n-2k}{r}$, $B(k, r, s) = x^{n-2k-r+s}w^{r+s}(u^2 + v^2)^{k-s}(-10)^k 5^{k-s+r}$, and $H_2 = \frac{(v\sqrt{50+10\sqrt{5}}-u\sqrt{50-10\sqrt{5}})}{x-5w\sqrt{5}}$. Then we have

$$Re[J(\psi^2, \psi^2)] = \frac{(-1)^{n-1}}{4^n} \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_1(k, r, s) \times B(k, r, s)\sqrt{5}^{s+r}(-1)^r \tag{9}$$

and

$$Im[J(\psi^2, \psi^2)] = \frac{(-1)^{n-1}}{4^n} H_2 \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \sum_{s=0}^{k} \sum_{r=0}^{n-2k} D_2(k, r, s) \times B(k, r, s)\sqrt{5}^{s+r}(-1)^r. \tag{10}$$

Proof: From (5), we have

$$J(\psi^2, \psi^2) = \frac{(-1)^{n-1}}{4^n}\Big(x - 5w\sqrt{5} + jv\sqrt{50 + 10\sqrt{5}} \times -ju\sqrt{50 - 10\sqrt{5}}\Big)^n.$$

Using binomial expansion, we can also obtain (9) and (10).

□

Now, we can evaluate the A, B, C, D, E, F, and G using Lemmas 5–8 as follows:

Theorem 16 Let $J(\psi, \psi) = a+jb$, $J(\psi^2, \psi^2) = c+jd$, $j = \sqrt{-1}$, $a, b, c, d \in \mathbb{R}$. Then the cyclotomic numbers of order 5 over F_{p^m} are given as

$$
\begin{aligned}
25A =& p^n + 6(a+c) - 14 \\
25B =& p^n - \frac{3}{2}(a+c) + \frac{1}{2}\sqrt{5}(a-c) - \frac{1}{2}\sqrt{5+2\sqrt{5}} \\
& \times (b+3d) - \frac{1}{2}\sqrt{5-2\sqrt{5}}(3b-d) - 4 \\
25C =& p^n - \frac{3}{2}(a+c) - \frac{1}{2}\sqrt{5}(a-c) - \frac{1}{2}\sqrt{5+2\sqrt{5}} \\
& \times (3b-d) + \frac{1}{2}\sqrt{5-2\sqrt{5}}(b+3d) - 4 \\
25D =& p^n - \frac{3}{2}(a+c) - \frac{1}{2}\sqrt{5}(a-c) + \frac{1}{2}\sqrt{5+2\sqrt{5}} \\
& \times (3b-d) - \frac{1}{2}\sqrt{5-2\sqrt{5}}(b+3d) - 4 \\
25E =& p^n - \frac{3}{2}(a+c) + \frac{1}{2}\sqrt{5}(a-c) + \frac{1}{2}\sqrt{5+2\sqrt{5}} \\
& \times (b+3d) + \frac{1}{2}\sqrt{5-2\sqrt{5}}(3b-d) - 4 \\
25F =& p^n + (a+c) - \sqrt{5}(a-c) + 1 \\
25G =& p^n + (a+c) + \sqrt{5}(a-c) + 1.
\end{aligned}
$$

Proof: Let $r_1 = \frac{-3+\sqrt{5}}{4}$, $r_2 = \frac{-3-\sqrt{5}}{4}$, $s_1 = \frac{\sqrt{5+2\sqrt{5}}+3\sqrt{5-2\sqrt{5}}}{4}$, and $s_2 = \frac{3\sqrt{5+2\sqrt{5}}-\sqrt{5-2\sqrt{5}}}{4}$. From Lemmas 5–8, we have

$$
\begin{aligned}
25A &= p^n + 6(a+c) - 14 \\
25B &= p^n + 2(r_1 a - s_1 b) + 2(r_2 c - s_2 d) - 4 \\
25C &= p^n + 2(r_2 a - s_2 b) + 2(r_1 c + s_1 d) - 4 \\
25D &= p^n + 2(r_2 a + s_2 b) + 2(r_1 c - s_1 d) - 4 \\
25E &= p^n + 2(r_1 a + s_1 b) + 2(r_2 c + s_2 d) - 4 \\
25F &= p^n + (a+c) - \sqrt{5}(a-c) + 1 \\
25G &= p^n + (a+c) + \sqrt{5}(a-c) + 1.
\end{aligned}
$$

It is easy to evaluate the above equations using r_1, r_2, s_1, and s_2. □

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. The autocorrelation of Sidel'nikov sequences is given as [6]

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

which can be expressed as

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

where ω_M is an M-th root of unity.

In [6], the autocorrelation distribution of M-ary Sidel'nikov sequences is expressed in terms of the cyclotomic numbers over F_{p^n} of order M.

Using the cyclotomic numbers of order 5 in Theorems 12 and 16, we can obtain the correlation distributions of 5-ary Sidel'nikov sequences as the following example.

Example 17 Let $N(R_{u,v})$ be the number of $R_{u,v}$ for $0 \le \tau \le N-1$. Then the out-of-phase autocorrelation distributions of a 5-ary Sidel'nikov sequences of period $p^n - 1$ are given as:

$$
\begin{aligned}
N(0) =& (1,1)_5 + (2,2)_5 + (3,3)_5 + (4,4)_5 + (1,0)_5 \\
& + (2,0)_5 + (3,0)_5 + (4,0)_5 + (0,0)_5 \\
=& A + 2B + 2C + 2D + 2E \\
=& (9p^n - 6(a+c) - 46)/25 \\
N(R_{1,1}) =& (2,1)_5 = F, \; N(R_{4,4}) = (3,4)_5 = F \\
N(R_{3,3}) =& (1,3)_5 = G, \; N(R_{2,2}) = (4,2)_5 = G \\
N(R_{1,2}) =& (3,2)_5 + (3,1)_5 = 2G \\
N(R_{3,4}) =& (2,4)_5 + (2,3)_5 = 2G \\
N(R_{1,3}) =& (4,3)_5 + (4,1)_5 = 2F \\
N(R_{2,4}) =& (1,4)_5 + (1,2)_5 = 2F \\
N(R_{1,4}) =& (0,4)_5 + (0,1)_5 = B + E \\
=& (2p^n - 3(a+c) + \sqrt{5}(a-c) - 8)/25 \\
N(R_{2,3}) =& (0,3)_5 + (0,2)_5 = C + D \\
=& (2p^n - 3(a+c) - \sqrt{5}(a-c) - 8)/25.
\end{aligned}
$$

□

References

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

[2] Thomas W. Cusick, Cunsheng Ding, and Ari Renvall, *Stream Ciphers and Number Theory.* NY: Elsevier, 2004.

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

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

[5] 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.

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