International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

On the Number of Distinct Autocorrelation Distributions of M-ary Sidel'nikov Sequences

Jung-Soo Chung[†], Young-Sik Kim[‡], Jong-Seon No[†], and Habong Chung[††]

[†] Department of EECS and INMC
Seoul National University
Seoul, Korea
E-mail: integer@ccl.snu.ac.kr, jsno@snu.ac.kr

[‡] Samsung Electronics, Co., Ltd.
Yongin, Gyeonggi-do, Korea
E-mail: mypurist@gmail.com

[††] School of EEE,
Hongik University, Seoul, Korea
E-mail: habchung@hongik.ac.kr

Abstract

In this paper, we enumerate the number of distinct autocorrelation distributions of M-ary Sidel'nikov sequences of given length, while we change the primitive element for generating the sequence.

1. Introduction

For a prime p, positive integers M and 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.

Recently, Kim, Chung, No, and Chung [4] derived the autocorrelation distribution of M-ary Sidel'nikov sequences using cyclotomic numbers of order M. It was also pointed out that the total number of distinct autocorrelation values depends not only on M but also on the period of the sequence, but is always less than or equal to $\binom{M}{2}+1$.

In general, each M-ary Sidel'nikov sequence of period p^n-1 is distinct when we change the primitive element of the corresponding field used for generating the sequence. In this paper, by showing the relation between two M-ary Sidel'nikov sequences, each from different primitive elements, we enumerate the number of distinct autocorrelation distributions of M-ary Sidel'nikov sequences.

2. Preliminaries

For an M-ary sequence $s(t)$ of period N, the autocorrelation function $R(\tau)$ is defined as

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

where $\omega_M=e^{j2\pi/M}$ and $j=\sqrt{-1}$.

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 be a positive integer such that $M\ge 2$ and $M|p^n-1$. Let S_k, $k=0,1,\cdots,M-1$, be the disjoint subsets of F_{p^n} defined by

$$S_k=\left\{\alpha^{Mi+k}-1 \mid 0\le i<\frac{p^n-1}{M}\right\}. \tag{1}$$

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

$$s(t)=\begin{cases}k, & \text{if } \alpha^t\in S_k,\ 0\le k\le M-1\\ k_0, & \text{if } \alpha^t=-1\end{cases} \tag{2}$$

where k_0 is some integer modulo M. □

It is known that the M-ary Sidel'nikov sequence $s(t)$ in (2) can be represented in terms of the multiplicative character $\psi_M(\cdot)$ of order M in F_{p^n} and the indicator function $I(\cdot)$ as

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

Note that the indicator function is defined as

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

and the multiplicative character ψ_M is defined as $\psi_M(\alpha^t)=e^{j2\pi t/M}$ and $\psi_M(0)=0$.

It is shown in [4] that the autocorrelation distribution of a M-ary Sidel'nikov sequence can be represented by the cyclotomic numbers of order M defined below.

This work was supported by the IT R&D program of MKE/IITA [2008-F-007-01, Intelligent Wireless Communication Systems in 3 Dimensional Environment] and the MEST, the MKE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

Definition 2 [6] Let α be a primitive element of F_{p^n} and M a positive integer such that $M \geq 2$ and $M|p^n - 1$. 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 nonnegative 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 $1 + z_u \in C_v$. □

The following lemma lists some useful properties of cyclotomic numbers.

Lemma 3 (Storer [6])

1) $(i,j)_M = (M-i, j-i)_M$
2) $(i,j)_M = (pi, pj)_M$
3) $(i,j)_M = \begin{cases} (j,i)_M, & \text{if } p = 2 \\ (j,i)_M, & \text{if } \frac{p^n-1}{M} \text{is even} \\ (j+\frac{M}{2}, i+\frac{M}{2})_M, & \text{if } \frac{p^n-1}{M} \text{ is odd} \end{cases}$
4) $(i,j)_{M'} = \sum_{t=0}^{m-1} \sum_{s=0}^{m-1} (i+tM', j+sM')_M$, for $M = mM'$. □

Baumert, Mills, and Ward showed that the cyclotomic numbers of a certain order M over F_{p^n} are uniform as follows.

Theorem 4 [7] Let p be a prime, $q = p^{2ms}$, and M a divisor of p^s+1, such that $M \geq 3$. Then the cyclotomic numbers of order M over F_q are uniform as follows

$$(0,0)_M = \eta^2 - (M-3)\eta - 1$$
$$(0,i)_M = (i,0)_M = (i,i)_M = \eta^2 + \eta, \quad \text{for } i \neq 0$$
$$(i,j)_M = \eta^2, \quad \text{otherwise}$$

where $\eta = \begin{cases} (\sqrt{q}-1)/M, & \text{if } m \text{ is even} \\ (-\sqrt{q}-1)/M, & \text{if } m \text{ is odd.} \end{cases}$

3. Counting the Distinct Autocorrelation Distributions of Sidel'nikov Sequences

In this section, the number of distinct autocorrelation distributions of M-ary Sidel'nikov sequences $s^{(c)}(t)$, $\gcd(c, p^n - 1) = 1$, will be derived. Clearly from Definition 1, two M-ary Sidel'nikov sequences based on different primitive elements can be distinct. Let $S_k^{(c)}$ and $s^{(c)}(t)$ denote the disjoint subsets in (1) and the sequence in (2), respectively, when the primitive element α is replaced by another primitive element $\beta = \alpha^c$. Clearly, $S_k^{(c)} = S_{ck}$. The relation between $s(t)$ and $s^{(c)}(t)$ is derived in the following lemma.

Lemma 5

$$s^{(c)}(t) \equiv \begin{cases} s(ct) = k_0, & \text{if } \alpha^{ct} = -1 \\ c^{-1}s(ct), & \text{otherwise} \end{cases}$$

where $\gcd(c, p^n - 1) = 1$ and c^{-1} is computed modulo M.

Proof: Since $S_k^{(c)} = S_{ck}$, $s^{(c)}(t) = k$ implies that $\alpha^{ct} \in S_{ck}$, which further implies that $s(ct) \equiv ck \mod M$, i.e., $c^{-1}s(ct) \equiv k \mod M$. The proof for the opposite direction can be done in the exact same way. □

Using the previous lemma, we can derive the number of cyclically inequivalent Sidel'nikov sequences as in the following theorem.

Theorem 6 The nontrivial (that is, $\tau \not\equiv 0 \bmod p^n - 1$) autocorrelation function $R_c(\tau)$ of $s^{(c)}(t)$ is given as

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

where $\overline{\psi}_M$ denotes the complex conjugate of ψ_M. □

Using the result in [4], it can be shown that $R_c(\tau)$ also takes the values

$$R_{i,j} = -(\omega_M^i - 1)(\omega_M^j - 1)$$

when $\psi_M(-1) = 1$ or equivalently $(p^n - 1)/M$ is even, and

$$Q_{i,j} = (\omega_M^i + 1)(\omega_M^j + 1) - 2$$

when $\psi_M(-1) = -1$ or equivalently $(p^n - 1)/M$ is odd.

The autocorrelation distributions of $s^{(c)}(t)$ can be derived as in the following theorem, which can be viewed as the generalization of the autocorrelation distributions of $s(t)$ derived in [4].

Theorem 7 Let $N_c(a)$ be the number of $\tau (\neq 0)$ such that $R_c(\tau) = a$. Then the out-of-phase autocorrelation distributions of M-ary Sidel'nikov sequences $s^{(c)}(t)$ of period $p^n - 1$ are given as:

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

1) $N_c(0) = \sum_{i=1}^{M-1} \{(ci, ci + ck_0)_M + (ci, ck_0)_M\} + (0, ck_0)_M$
2) $N_c(R_{i,i}) = (2ci, ci + ck_0)_M,\ 1 \leq i \leq M-1$
3) $N_c(R_{i,j}) = (ci + cj, ci + ck_0)_M + (ci + cj, cj + ck_0)_M, 1 \leq i < j \leq M-1.$

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

1) $N_c(-2) = \sum_{i=0, i\neq\frac{M}{2}}^{M-1} \{(\frac{Mc}{2}+ci, ci+ck_0)_M$
$+(\frac{Mc}{2}+ci, \frac{Mc}{2}+ck_0)_M\} + (0, \frac{Mc}{2}+ck_0)_M$
2) $N_c(Q_{i,i}) = (2ci, ci+ck_0)_M$,
$0 \le i \le M-1$ and $i \neq M/2$
3) $N_c(Q_{i,j}) = (ci+cj, ci+ck_0)_M$
$+ (ci+cj, cj+ck_0)_M$,
$0 \le i < j \le M-1, i \neq M/2$, and $j \neq M/2$. □

Using the previous theorem, we can derive the number of distinct autocorrelation distributions of Sidel'nikov sequences as in the following theorem.

Theorem 8 Let p be a prime and $M|p^n-1$. Let ψ_M be nontrivial multiplicative characters of F_{p^n}. The number of the distinct autocorrelation distributions of M-ary Sidel'nikov sequences $s^{(c)}(t)$ with $\gcd(c, p^n-1) = 1$ is given as:

Case 1) For $M = 2$, there is a unique autocorrelation distribution.

Case 2) If $M > 2$ and $M|(p^k+1)$ for some k, $1 \le k < n$, then the autocorrelation distribution of M-ary Sidel'nikov sequences is unique.

Case 3) If $M > 2$ and $M \nmid (p^k+1)$ for any $k, 1 \le k < n$, then the number of their distinct autocorrelation distributions is less than or equal to $\phi(M)/k'$ for $k_0 \neq 0, M/2$ and is less than or equal to $\phi(M)/2k'$ for $k_0 = 0$ or $M/2$, where k' is the smallest integer satisfying $M|(p^{k'}-1)$.

Proof:

Case 1) Since $M = 2$, any c relatively prime to p^n-1 is odd. Thus, $s^{(c)}(t)$ is just the c-decimation of $s(t)$. Since the sequences decimated by any constant relatively prime to the period share the same autocorrelation distribution, there is a unique autocorrelation distribution.

Case 2) In this case, n must be even and k divides $n/2$. Thus $\psi_M(-1) = 1$ since $(p^n-1)/M$ is even. Using Theorems 4 and 7, we can conclude that the autocorrelation distribution is independent of the value c, and thus it is unique.

Case 3) For counting the number of distinct autocorrelation distributions, it is enough to count the number of distinct values that $N_c(R_{i,j})$ can take for a given $R_{i,j}$ as c varies under the condition of $\gcd(c, p^n-1) = 1$. Note from Theorem 7, that each $N_c(R_{i,j})$ is represented in terms of cyclotomic numbers of order M. Since $\gcd(c, p^n-1) = 1$ implies $\gcd(c, M) = 1$, it is clear that the number of distinct autocorrelation distributions is upper bounded by $\phi(M)$.

By the Euler's theorem, we have

$$p^{\phi(M)} \equiv 1 \bmod M.$$

If k' is the smallest integer satisfying $M|(p^{k'}-1)$, then $k'|\phi(M)$ and $c, cp, cp^2, cp^3, \cdots, cp^{k'-1}$ are all distinct mod M. From Lemma 3, we have

$$(cs, ct)_M = (cps, cpt)_M = \cdots = (cp^{k'-1}s, cp^{k'-1}t)_M.$$

Thus, the number of distinct autocorrelation distributions is less than or equal to $\phi(M)/k'$.

From 1) of Lemma 3, for any c and c' such that $c+c' = M$, we have $(2ci, ci+ck_0)_M = (2c'i, c'i-c'k_0)_M$ and $(c(i+j), ci+ck_0)_M + (c(i+j), cj+ck_0)_M = (c'(i+j), c'i-c'k_0)_M + (c'(i+j), c'j-c'k_0)_M$. Thus, when $k_0 = 0$ or $M/2$, we have $N_c(R_{i,j}) = N_{c'}(R_{i,j})$ from Theorem 7. From the fact that $c' \notin \{c, cp, cp^2, \cdots, cp^{k'-1}\}$, we can say that the number of distinct autocorrelation distributions is upper bounded by $\phi(M)/2k'$. □

Remark 1 From the numerical analysis for various values of M's, p's, and n's, it seems that the upper bound of Case 3) is achieved except for the case of $M = 8$, $p \equiv 1 (\bmod\ 8)$, and $k_0 = 0, 4$, the number of autocorrelation distributions of which is equal to 1. □

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. 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] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303–3307, Sep. 2005.

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

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

[7] L.D. Baumert, W.H. Mills, and R.L. Ward, "Uniform cyclotomy," *J. Number Theory*, vol. 14, pp. 67–82, 1982.

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

[9] R. J. McEliece and H. C. Rumsey, "Euler products, cyclotomy, and coding," *J. Number Theory*, vol. 4, pp. 302–311, 1972.