invoked with EXPAND $(\emptyset, 0)$ and M is a global variable whose initial value is

$$\left\lfloor \frac{2^{nR}}{\prod_{i=1}^{T-1} S_i} \right\rfloor$$

where R is the largest previously known sum rate.

In prescribing the sizes of the constituent codes, we let

$$S_1 \leq S_2 \leq \cdots \leq S_{T-1} \leq M + 1.$$

Algorithm 1 should be invoked for all (minimal) combinations of sizes that could improve on the best known bound.

The software packages Cliquer [9] and *nauty* [8] were used for finding independent sets and detecting equivalent solutions, respectively. Using Algorithm 1 the following record-breaking codes were found for T-user binary adder channels with $3 \leq T \leq 5$. For the 3-user channel, the code (with the binary codewords in decimal format)

$$C_1 = \{3, 4, 59, 60\}$$
$$C_2 = \{22, 23, 24, 25, 30, 33, 38, 39, 40, 41\}$$
$$C_3 = \{8, 10, 13, 15, 18, 21, 23, 32, 42, 45, 46, 48, 50, 53, 55\}$$

of length $n = 6$ has sum rate

$$\frac{\log_2 600}{6} \approx 1.5381.$$

For the 4-user channel, the code

$$C_1 = \{0, 15\}$$
$$C_2 = \{6, 7, 8, 9\}$$
$$C_3 = \{3, 4, 11, 12\}$$
$$C_4 = \{1, 5, 10, 14\}$$

of length $n = 4$ has sum rate

$$\frac{\log_2 128}{4} = 1.75.$$

There are exactly two inequivalent codes with these parameters and values of S_i. Finally, for the 5-user channel, the code

$$C_1 = \{6, 9\}$$
$$C_2 = \{5, 10\}$$
$$C_3 = \{3, 12\}$$
$$C_4 = \{0, 15\}$$
$$C_5 = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 11, 13, 14\}$$

of length $n = 4$ has sum rate

$$\frac{\log_2 192}{4} \approx 1.8962.$$

There are exactly two inequivalent codes also in this case.

As in the case of good 2-user codes, many of the constituent codes are self-complementary, that is, if $c \in C_i$, then $\bar{c} \in C_i$; cf. [7]. In fact, to speed up the search that led to the record-breaking 3-user code, we required that the first two constituent codes be self-complementary.

The current approach is obviously computationally feasible only for small lengths and small numbers of users, the bottleneck being the number of partial solutions (and thereby the number of times a clique search has to be carried out). One could, however, impose further structure on the codes to be able to consider larger values of n.

REFERENCES

[1] R. Ahlswede and V. B. Balakirsky, "Construction of uniquely decodable codes for the two-user binary adder channel," *IEEE Trans. Inf. Theory*, vol. 45, pp. 326–330, Jan. 1999.

[2] S.-C. Chang and E. J. Weldon, Jr, "Coding for T-user multiple access channels," *IEEE Trans. Inf. Theory*, vol. IT-25, pp. 684–691, Nov. 1979.

[3] P. A. B. M. Coebergh van den Braak and H. C. A. van Tilborg, "A family of good uniquely decodable code pairs for the two-access binary adder channel," *IEEE Trans. Inf. Theory*, vol. IT-31, pp. 3–9, Jan. 1985.

[4] T. Kasami, S. Lin, V. K. Wei, and S. Yamamura, "Graph theoretic approaches to the code construction for the two-user multiple access binary adder channel," *IEEE Trans. Inf. Theory*, vol. IT-29, pp. 114–130, Jan. 1983.

[5] G. H. Khachatrian and S. S. Martirossian, "Code construction for the T-user noiseless adder channel," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1953–1957, Sep. 1998.

[6] H. J. Liao, "Multiple Access Channels," Ph.D. dissertation, Dep. Elect. Eng., Univ. Hawaii, Honolulu, HI, 1972.

[7] M. Mattas and P. R. J.Östergård, "A new bound for the zero-error capacity region of the two-user binary adder channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 3289–3291, Sep. 2005.

[8] B. D. McKay, *nauty* User's Guide (Version 1.5), Comput. Sci. Dep., Australian Nat. Univ., Canberra, Tech. Rep. TR-CS-90-02, 1990.

[9] S. Niskanen and P. R. J Östergård, Cliquer User's Guide, Version 1.0, Commun. Lab., Helsinki Univ. Technol., Tech. Rep. T48, 2003.

[10] R. Urbanke and Q. Li, "The zero-error capacity region of the 2-user synchronous BAC is strictly smaller than its Shannon capacity region," in *Proc. IEEE Inf. Theory Workshop*, Killarney, Ireland, 1998.

Cross Correlation of Sidel'nikov Sequences and Their Constant Multiples

Young-Joon Kim, *Student Member, IEEE*, and Hong-Yeop Song, *Member, IEEE*

***Abstract*—In this correspondence, we prove that the complex crosscorrelation of a k-ary Sidel'nikov sequence of period $q-1$ and its constant multiple sequence is upper bounded by $\sqrt{q}+3$, where $q = p^m$ and here p is an odd prime and m is a positive integer.**

***Index Terms*—Autocorrelation, cross correlation, Sidel'nikov sequences.**

I. INTRODUCTION

In code-division multiple-access (CDMA) communication systems, the sequences used as signature codes are required to have a good correlation property. The correlations are classified into two categories.

Manuscript received June 8, 2006; revised November 28, 2006. This work was supported by the Basic Research Program of the Korea Science and Engineering Foundation under Grant (R01-2003-000-10330-0).

The authors are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 121-749, Korea (e-mail: yj.kim@yonsei.ac.kr; hysong@yonsei.ac.kr).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2006.890723

One is the autocorrelation property and an impulse like autocorrelation is essential for synchronization. Many researchers have studied the sequences with a low autocorrelation [1]–[3]. The other category is a crosscorrelation of a pair of or a number of sequences. For the purpose of using sequences as signature codes in the multiple access system, we need a set of sequences with a low crosscorrelation. In an environment in which multiple users share the resources (e.g., time and frequency), it is more desirable to use the set of sequences having as low crosscorrelation values as possible with each other [4].

In 1969, Sidelnikov showed that two kinds of character sequences have a good autocorrelation. These sequences are defined as follows.

Definition 1 (Type-1 [5]): Let p be an odd prime, k a divisor of $p-1$ and μ a primitive root $\bmod p$. The nonzero integers $\bmod p$ can be partitioned into k cosets C_i, $0 \le i \le k-1$, where C_0 is the set of the kth power residues $\bmod p$, and $C_i = \mu^i C_0$ for $i > 0$. Define a k-ary sequence $\{s(n) | 0 \le n < p\}$ of length p as follows:

$$s(n) = \begin{cases} 0, & \text{if } n = 0 \\ i, & \text{if } n \in C_i = \mu^i\, C_0 \end{cases}$$

For convenience, we will call this Type-1 sequence. Note that the index n of $\{s(n)\}$ can be regarded as an integer $\bmod p$, while the value $s(n)$ can be regarded as an integer $\bmod k$. □

Definition 2 (Type-2 [5]): Let $\mathbf{F}_q$ be a finite field with $q = p^m$ elements, k a divisor of $q-1$, and μ a primitive element in $\mathbf{F}_q$, where p is an odd prime and m is a positive integer. Define a k-ary sequence $\{t(n) | 0 \le n < q-1\}$ of length $q-1$ as follows:

$$t(n) = \begin{cases} 0, & \text{if } \mu^n + 1 = 0 \left(\Longleftrightarrow n = \frac{q-1}{2}\right) \\ i, & \text{if } \mu^n + 1 \in \mu^i C_0 \end{cases}$$

where C_0 is the set of kth power residues in $\mathbf{F}_q$. For convenience, we will call this Type-2 sequence. Note that the index n of $\{t(n)\}$ can be regarded as an integer $\bmod\ q-1$, while the value $t(n)$ can be regarded as an integer $\bmod k$. □

Definition 3: Let $\{s(n)\}$ be a k-ary sequence of length N. Then a constant c multiple sequence $\{cs(n)\}$ of $\{s(n)\}$ is defined as the sequence whose ith term is given as $cs(i) \bmod k$, where c is an integer such that $1 \le c < k$ and $s(i)$ is the ith term of $\{s(n)\}$. □

Recently, in [6], they have applied the constant multiplication and decimation to Type-1 sequences and calculated the crosscorrelation, which will be recalled briefly in Section III. In this correspondence, we consider the constant multiple of a k-ary Type-2 sequence and calculate the crosscorrelation of a k-ary Type-2 sequence and its constant multiple sequences.

II. Properties of k-ary Type-1/Type-2 Sequences

The properties of k-ary Type-1 sequences are summarized as follows.

Lemma 1 (Properties of Type-1 Sequences [5]): Let $\{s(n)\}$ be a k-ary Type-1 sequence of period p and w a complex primitive kth root of unity. Then,

i) $s(1) = 0$.

ii) For $u \ne 0,\ v \ne 0$, we have

$$s(u) + s(v) \equiv s(uv) \bmod k$$

and

$$s(u) - s(v) \equiv s(u/v) \bmod k$$

where uv and u/v are computed modulo p.

iii) For any $u \in Z_p^*$, we have

$$w^{s(-u)} = \begin{cases} -w^{s(u)}, & \text{if } p \equiv k+1 \bmod 2k \\ w^{s(u)}, & \text{if } p \equiv 1 \bmod 2k. \end{cases}$$

iv) $\sum_{n=0}^{p-1} w^{s(n)} = 0$.

v) For any $\tau \ne 0$, the autocorrelation is given as follows:

$$R_s(\tau) \triangleq \sum_{x=0}^{p-1} w^{s(x+\tau)-s(x)} = \begin{cases} -1 - j2\beta(\tau), & \text{if } p \equiv k+1 \bmod 2k \\ -1 + 2\alpha(\tau), & \text{if } p \equiv 1 \bmod 2k \end{cases}$$

where $\alpha(u)$ and $\beta(u)$ are the real and imaginary part of $w^{s(u)}$, respectively.

Remark 1: Type-1 sequence of period p can easily generalized so that it can be defined over some prime power field $\mathbf{F}_q$ as follows. Let μ be a primitive element of $\mathbf{F}_q$ where $q = p^m$ is a power of a prime p, and k be a divisor of $q-1$. Let C_0 be the set of kth powers in $\mathbf{F}_q^* = \mathbf{F}_q \backslash \{0\}$, and $C_i = \mu^i C_0$ for $1 \le i < k$. Then, for any $x \in \mathbf{F}_q^*$ we define $s(x) = i$ if $x \in C_i$ and $s(0) = 0$. Note that $s(x)$ for each $x \in \mathbf{F}_q$ is well defined, but it can no longer be viewed a "sequence" of period q unless some reference order of elements of $\mathbf{F}_q$ is chosen. However, we call it a **generalized Type-1** sequence (over $\mathbf{F}_q$) of period q (defined by μ) if the order does not matter (which is mostly the case in the following). Note that the property (ii) in Lemma 1 still holds, in other words, $s(u) - s(v) \equiv s(uv) (\bmod k)$ and $s(u) - s(v) \equiv s(u/v) (\bmod k)$ for $u, v \in \mathbf{F}_q^*$. □

Theorem 1 ([5]): Let $\{t(n)\}$ be a k-ary Type-2 sequence of period $q-1$ defined by a primitive element μ. Then, for any $\tau \ne 0$, the autocorrelation is given as follows:

$$R_t(\tau) = \sum_{x=0}^{q-2} w^{t(x+\tau)-t(x)} = -w^{s(\mu^\tau)} - 1 + w^{s(-\mu^\tau+1)} + w^{-s(-\mu^{-\tau}+1)}$$

where $\{s(x) | x \in \mathbf{F}_q\}$ is the generalized Type-1 sequence of period q defined by μ as in Remark 1.

Corollary 1: Let $\{t(n)\}$ be a k-ary Type-2 sequence of period $q-1$ defined by a primitive element μ. Then, for any $\tau \ne 0$, the autocorrelation of the sequence which is obtained by multiplying a nonzero constant c to $\{t(n)\}$ is given as follows:

$$R_{c\cdot t}(\tau) = \sum_{x=0}^{q-2} w^{c\cdot t(x+\tau)-c\cdot t(x)} = -w^{c\cdot s(\mu^\tau)} - 1 + w^{c\cdot s(-\mu^\tau+1)} + w^{-c\cdot s(-\mu^{-\tau}+1)}$$

where $\{s(x) | x \in \mathbf{F}_q\}$ is the generalized Type-1 sequence of period q defined by μ as in Remark 1.

Note that the magnitude of out-of-phase autocorrelation of Type-2 sequence is not greater than 4. Furthermore, the magnitude of the out-of-phase autocorrelation of the sequence which is obtained by multiplying a nonzero constant $\bmod k$ is also not greater than 4.

As is stated above, the magnitude of autocorrelation of Type-1/2 sequences does not increase as the period of sequences increases. Therefore, it is interesting to extend the number of sequences by applying some simple transformations (e.g., constant multiplication, affine shift and/or decimation) and to compute their crosscorrelation. We found some interesting crosscorrelations when we multiplied a constant to a k-ary Type-1/Type-2 sequence. In Section III, these results will be presented.

III. Crosscorrelation of k-ary Sequence and Their Constant Multiples

The periodic crosscorrelation between two k-ary sequences $\{u_1(n)\}$ and $\{u_2(n)\}$ of period N is defined by

$$C_{u_1,u_2}(\tau) = \sum_{n=0}^{N-1} w^{u_1(n+\tau)-u_2(n)}$$

where w is a complex primitive kth root of unity.

Theorem 2 ([6]): The crosscorrelation of k-ary Type-1 sequence $\{s_1(n)\}$ and its constant multiple sequence $\{s_2(n)\}$ both of length p is upper bounded by $\sqrt{p}+2$, i.e.

$$|C_{s_1,s_2}(\tau)| \le \sqrt{p}+2.$$

Theorem 3 (Main Result): Let $\{t(n)|0 \le n < q-1\}$ be a k-ary Type-2 sequence of length $q-1$ and $t_1(n) = c_1 t(n), t_2(n) = c_2 t(n)$ for all n, where c_1, c_2 are integers with $1 \le c_1 \ne c_2 \le k-1$. Then the crosscorrelation of $\{t_1(n)\}$ and $\{t_2(n)\}$ is upper bounded by $\sqrt{q}+3$, i.e.

$$|C_{t_1,t_2}(\tau)| \le \sqrt{q}+3.$$

For the proof of Theorem 3, we need the properties of the generalized Type-1 sequences defined over the prime power field $\mathbf{F}_q$ as in Remark 1. We also need the following lemma.

Lemma 2: Let q be a power of a prime and $\{s(x)|x \in \mathbf{F}_q\}$ be a k-ary generalized Type-1 sequence of period q defined by μ as discussed in Remark 1. Let w be a complex primitive kth root of unity, and e be any integer from 1 to $k-1$. Then we have the following identity:

$$\sum_{x \in \mathbf{F}_q^*} w^{s(yx^e)} = 0, \quad \forall\, y \in \mathbf{F}_q^*. \tag{1}$$

Proof: The generalized Type-1 sequence $\{s(x)|x \in \mathbf{F}_q\}$ satisfies $s(u)+s(v) = s(uv) \bmod k$ for all $u, v \in \mathbf{F}_q^*$. Letting $d \triangleq (e,k)$ be the gcd of e and k, and $k_1 = k/d$, we have

$$\begin{aligned}\sum_{x \in \mathbf{F}_q^*} w^{s(yx^e)} &= \sum_{x \in \mathbf{F}_q^*} w^{s(y)} w^{s(x^e)} \\ &= w^{s(y)} \sum_{0 \le i < q-1} w^{s(\mu^{ei})} \\ &= w^{s(y)} \frac{q-1}{k_1} \sum_{0 \le i < k_1} w^{id} = 0\end{aligned}$$

where we note that $s(\mu^{ei})$ takes all the values $0, d, 2d, \ldots, (k_1-1)d$ exactly $\frac{q-1}{k_1}$ times as i takes values from 0 to $q-2$ □

Proof of Theorem 3: We now calculate the crosscorrelation of $\{t_1(n) = c_1 t(n)\}$ and $\{t_2(n) = c_2 t(n)\}$ where c_1, c_2 are any given integers from 1 to $k-1$. Without loss of generality, assume that $0 < c_2 < c_1 < k$.

Note that since $t(n) = i$ when $\mu^n + 1 \in C_i = \mu^i C_0$, we have $t(n) = s(\mu^n+1)$, where $s(x)$ is the generalized Type-1 sequence defined by the primitive element μ. For simplicity, denote $a(x) = w^{s(x)}$. Therefore, when $\mu^n + 1 \ne 0$, $w^{t(n)} = w^{s(\mu^n+1)} = a(\mu^n+1)$.

We will first take care of the case where $\tau = 0$ as follows:

$$\begin{aligned}C_{t_1,t_2}(\tau=0) &= \sum_{n=0}^{q-2} w^{c_1 t(n) - c_2 t(n)} \\ &= a(0)^{c_1} a(0)^{-c_2} \\ &\quad + \sum_{\substack{0 \le n < q-1 \\ n \ne \frac{q-1}{2}}} a(\mu^n+1)^{c_1} a(\mu^n+1)^{-c_2} \\ &= 1 + \sum_{x \in \mathbf{F}_q^* \setminus \{1\}} a(x^{c_1-c_2}) = 0\end{aligned}$$

from Lemma 2, since $1 < c_1 - c_2 < k$.

We now assume that $\tau \ne 0$. Then

$$\begin{aligned}C_{t_1,t_2}(\tau) &= \sum_{0 \le n < q-1} w^{c_1 t(n+\tau) - c_2 t(n)} \\ &= a(0)^{c_1} a(-\mu^{-\tau}+1)^{-c_2} + a(-\mu^{\tau}+1)^{c_1} a(0)^{-c_2} \\ &\quad + \sum_{\substack{0 \le n < q-1 \\ n \ne \frac{q-1}{2}, \frac{q-1}{2}-\tau}} a(\mu^{n+\tau}+1)^{c_1} a(\mu^n+1)^{-c_2} \\ &= a(-\mu^{-\tau}+1)^{-c_2} + a(-\mu^{\tau}+1)^{c_1} \\ &\quad + \sum_{x \in \mathbf{F}_q^* \setminus \{-1, -\mu^{-\tau}\}} a\left(\frac{(\mu^{\tau}x+1)^{c_1}}{(x+1)^{c_2}}\right). \end{aligned} \tag{2}$$

Denote the third term of (2) by $\theta(\tau)$. Since magnitude of the sum of the first two terms cannot exceed 2, it is now sufficient to show that, for any $\tau \ne 0$

$$|\theta(\tau)| \le \sqrt{q}+1.$$

Observe the equation shown at the bottom of the page, where $*$ is a complex conjugate. Denote $-1+\mu^{-\tau}$ by v. Note that since $\tau \ne 0$, $v \notin \{0, -1\}$.

$$|\theta(\tau)|^2 = \sum_{\substack{x \in \mathbf{F}_q^* \\ x \ne 1, -v}} \sum_{\substack{y \in \mathbf{F}_q^* \\ y \ne 1, -v}} a\left(\left(\frac{x+v}{y+v}\right)^{c_1} \left(\frac{y}{x}\right)^{c_2}\right).$$

Substitute $1/x$ instead of x. Then

$$|\theta(\tau)|^2 = \sum_{\substack{x \in \mathbf{F}_q^* \\ x \ne 1, -1/v}} \sum_{\substack{y \in \mathbf{F}_q^* \\ y \ne 1, -v}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1} (yx)^{c_2}\right).$$

$$\begin{aligned}|\theta(\tau)|^2 &= \sum_{x \in \mathbf{F}_q^* \setminus \{-1, -\mu^{-\tau}\}} a\left(\frac{(\mu^{\tau}x+1)^{c_1}}{(x+1)^{c_2}}\right) \left(\sum_{y \in \mathbf{F}_q^* \setminus \{-1, -\mu^{-\tau}\}} a\left(\frac{(\mu^{\tau}y+1)^{c_1}}{(y+1)^{c_2}}\right)\right)^* \\ &= \sum_{x \in \mathbf{F}_q^* \setminus \{-1, -\mu^{-\tau}\}} \sum_{y \in \mathbf{F}_q^* \setminus \{-1, -\mu^{-\tau}\}} a\left(\left(\frac{\mu^{\tau}x+1}{\mu^{\tau}y+1}\right)^{c_1} \left(\frac{y+1}{x+1}\right)^{c_2}\right) \\ &= \sum_{x \in \mathbf{F}_q^* \setminus \{1, 1-\mu^{-\tau}\}} \sum_{y \in \mathbf{F}_q^* \setminus \{1, 1-\mu^{-\tau}\}} a\left(\left(\frac{x-1+\mu^{-\tau}}{y-1+\mu^{-\tau}}\right)^{c_1} \left(\frac{y}{x}\right)^{c_2}\right)\end{aligned}$$

Let us consider the number of terms in the above double summation. There are $(q-3)^2$ terms. These can be re-ordered according to whether $yx=1$ or $yx\neq 1$. See (3) shown at the bottom of the page. Now, all we have to show is that the last term of (3) is less than or equal to $2\sqrt{q}+4$. We will denote the term by $\Theta(\tau)$. We now change the variables from x and y to x and $yx=z$ so that

$$\begin{aligned}\Theta(\tau)&=\sum_{\substack{yx\neq 1\\ x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{1,-v\}}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1}(yx)^{c_2}\right)\\ &=\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ z\in\mathbf{F}_q^*\setminus\{1,x,-vx\}}} a\left(\left(\frac{1+vx}{z+vx}\right)^{c_1}z^{c_2}\right)\\ &=\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{-1/v\}\\ z\in\mathbf{F}_q^*\setminus\{1,-vx\}}} a\left(\left(\frac{1+vx}{z+vx}\right)^{c_1}z^{c_2}\right)\\ &\quad-\sum_{\substack{x=1\\ z\in\mathbf{F}_q^*\setminus\{1,-v\}}} a\left(\left(\frac{1+v}{z+v}\right)^{c_1}z^{c_2}\right)\\ &\quad-\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ z=x}} a\left(\left(\frac{1+vx}{x+vx}\right)^{c_1}x^{c_2}\right).\end{aligned}\tag{4}$$

Denote the first, the second and the third term in (4) as $\Delta(v)$, $A(v)$ and $B(v)$, respectively. Therefore

$$\Theta(\tau)=\Delta(v)-A(v)-B(v)\tag{5}$$

where $v=-1+\mu^{-\tau}$. Observe that

$$\begin{aligned}A(v)&=\sum_{\substack{x=1\\ z\in\mathbf{F}_q^*\setminus\{1,-v\}}} a\left(\left(\frac{1+v}{z+v}\right)^{c_1}z^{c_2}\right)\\ &=a(1+v)^{c_1}\sum_{z\in\mathbf{F}_q^*\setminus\{-v\}} a\left(\frac{z^{c_2}}{(z+v)^{c_1}}\right)-a(1),\\ B(v)&=\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ z=x}} a\left(\left(\frac{1+vx}{x+vx}\right)^{c_1}x^{c_2}\right)\\ &=\sum_{x\in\mathbf{F}_q^*\setminus\{-v\}} a\left(\left(\frac{1+v/x}{1/x+v/x}\right)^{c_1}\left(\frac{1}{x}\right)^{c_2}\right)-a(1)\\ &=a(1+v)^{-c_1}\sum_{x\in\mathbf{F}_q^*\setminus\{-v\}} a\left(\frac{(x+v)^{c_1}}{x^{c_2}}\right)-1.\end{aligned}\tag{6}$$

By denoting the summation term in (6) as $\delta(v)$, we obtain $A(v)=a(1+v)^{c_1}\delta(v)^*-1$ and $B(v)=a(1+v)^{-c_1}\delta(v)-1$.

Observe the following:

$$\begin{aligned}|\delta(v)|^2&=\sum_{x\in\mathbf{F}_q^*\setminus\{-v\}} a\left(\frac{(x+v)^{c_1}}{x^{c_2}}\right)\\ &\quad\times\left(\sum_{y\in\mathbf{F}_q^*\setminus\{-v\}} a\left(\frac{(y+v)^{c_1}}{y^{c_2}}\right)\right)^*\\ &=\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{-v\}\\ y\in\mathbf{F}_q^*\setminus\{-v\}}} a\left(\left(\frac{x+v}{y+v}\right)^{c_1}\left(\frac{y}{x}\right)^{c_2}\right).\end{aligned}$$

Substitute $1/x$ instead of x. Then

$$|\delta(v)|^2=\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{-v\}}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1}(yx)^{c_2}\right).$$

Let us think about how many terms are in the above double summation. There are $(q-2)^2$ terms. These can be re-ordered according to whether $yx=1$ or $yx\neq 1$

$$\begin{aligned}|\delta(v)|^2&=\sum_{\substack{yx=1\\ x\in\mathbf{F}_q^*\setminus\{-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{-v\}}} a(1)\\ &\quad+\sum_{\substack{yx\neq 1\\ x\in\mathbf{F}_q^*\setminus\{-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{-v\}}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1}(yx)^{c_2}\right)\\ &=q-2+\sum_{\substack{x\in\mathbf{F}_q^*\setminus\{-1/v\}\\ z\in\mathbf{F}_q^*\setminus\{1,-vx\}}} a\left(\left(\frac{1+vx}{z+vx}\right)^{c_1}z^{c_2}\right).\end{aligned}\tag{7}$$

Note that the last term of (7) is exactly the same with $\Delta(v)$ in (4). We put further $vx=u$. Then, we have

$$\begin{aligned}\Delta(v)&=\sum_{\substack{u\in\mathbf{F}_q^*\setminus\{-1\}\\ z\in\mathbf{F}_q^*\setminus\{1,-u\}}} a\left(\left(\frac{1+u}{z+u}\right)^{c_1}z^{c_2}\right)\\ &=\sum_{\substack{z\in\mathbf{F}_q^*\setminus\{1\}\\ u\in\mathbf{F}_q^*\setminus\{-1,-z\}}} a(z^{c_2})a\left(\frac{1+u}{z+u}\right)^{c_1}\\ &=\sum_{z\in\mathbf{F}_q^*\setminus\{1\}} a(z^{c_2})\sum_{u\in\mathbf{F}_q^*\setminus\{-1,-z\}} a\left(\frac{1+u}{z+u}\right)^{c_1}.\end{aligned}$$

The inner sum of the above can be computed to be the sum of $a(x)^{c_1}$ for all $x\in\mathbf{F}_q^*$ except for two terms which are $a(1)^{c_1}$ and $a(z^{-1})^{c_1}$

$$\begin{aligned}|\theta(\tau)|^2&=\sum_{\substack{yx=1\\ x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{1,-v\}}} a(1)+\sum_{\substack{yx\neq 1\\ x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{1,-v\}}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1}(yx)^{c_2}\right)\\ &=q-3+\sum_{\substack{yx\neq 1\\ x\in\mathbf{F}_q^*\setminus\{1,-1/v\}\\ y\in\mathbf{F}_q^*\setminus\{1,-v\}}} a\left(\left(\frac{1+vx}{yx+vx}\right)^{c_1}(yx)^{c_2}\right).\end{aligned}\tag{3}$$

since the map $u \to \frac{1+u}{z+u}$ is one-to-one for $u \in \mathbf{F}_q^* \setminus \{-1, -z\}$. Therefore

$$\begin{aligned}\Delta(v) &= \sum_{z \in \mathbf{F}_q^* \setminus \{1\}} a(z^{c_2})(-a(1)^{c_1} - a(z^{-1})^{c_1}) \\ &= -\sum_{z \in \mathbf{F}_q^* \setminus \{1\}} a(z^{c_2}) - \sum_{z \in \mathbf{F}_q^* \setminus \{1\}} a(z^{c_2 - c_1}) \\ &= a(1) + a(1) = 2.\end{aligned}$$

Hence, we have $|\delta(v)|^2 = q$. It gives us

$$\begin{aligned}\Theta(\tau) &= \Delta(v) - A(v) - B(v) \\ &= 4 - a(1+v)^{c_1}\delta(v)^* - a(1+v)^{-c_1}\delta(v).\end{aligned}$$

Therefore, $4 - 2\sqrt{q} \le \Theta(\tau) \le 4 + 2\sqrt{q}$.

By revisiting the (2), we obtain

$$C_{t_1,t_2}(\tau) = a(-\mu^{-\tau} + 1)^{-c_2} + a(-\mu^{\tau} + 1)^{c_1} + \theta(\tau)$$

where $\sqrt{q} - 1 \le |\theta(\tau)| \le \sqrt{q} + 1$. It completes the proof of Theorem 3. □

In the proof of Theorem 3, we see that the crosscorrelation at $\tau = 0$ is 0 for any $c_1 \neq c_2$, which we emphasize here in the following corollary.

Corollary 2: Keep the notations in Theorem 3. Then $C_{t_1,t_2}(\tau = 0) = 0$.

IV. Comparison With Welch Bound

Let $R_{max}^{\mathbf{a}}$ denote the maximum out-of-phase autocorrelation of a given sequence $\mathbf{a} = \{a(n)\}$. Let $C_{max}^{\mathbf{a},\mathbf{b}}$ denote the maximum cross correlation of two sequences $\mathbf{a} = \{a(n)\}$ and $\mathbf{b} = \{b(n)\}$. In 1974, Welch derived a periodic correlation bound of a signal set $\mathbf{S}$ with M signals of length L[7] as

$$C_{\max}^2 \ge \frac{L^2(M-1)}{(ML-1)} \tag{8}$$

where $C_{\max} = \max\{R_{\max}^{\mathbf{a}}, C_{\max}^{\mathbf{a},\mathbf{b}} | \mathbf{a}, \mathbf{b}(\neq \mathbf{a}) \in \mathbf{S}\}$.

Consider a sequence set $\mathbf{S}$ which consists of a k-ary Type-2 sequence $\{t(n)\}$ of length $q-1$ and its all the constant multiple sequences. Since $k-1$ distinct ways are possible to multiply a constant c to $\{t(n)\}$ and $c = 1$ gives us the same sequence as $\{t(n)\}$, the cardinality of $\mathbf{S}$ is $k-1$, i.e., $M = |\mathbf{S}| = k-1$. From Theorem 1 and Corollary 1, we know that $R_{max}^{\mathbf{a}} \le 4$ for any $a \in \mathbf{S}$. Furthermore, from Theorem 3, $C_{max}^{\mathbf{a},\mathbf{b}} \le \sqrt{q}+3$ for any distinct $\mathbf{a}, b \in S$. Therefore, $C_{max} \le \sqrt{q}+3$.

Now apply the Welch bound (8) to this sequence set $\mathbf{S}$. Since $L = q-1$ and $M = k-1$, (8) becomes as follows:

$$C_{\max} \ge \sqrt{\frac{(q-1)^2(k-2)}{(q-1)(k-1)-1}}. \tag{9}$$

Denote the right hand side of (9) as L_B. Note that this bound depends on the value of k, a divisor of $q-1$. For two divisors k_1 and k_2 of $q-1$, if $k_1 < k_2$, then $L_B^{(k_1)} < L_B^{(k_2)}$ where $L_B^{(k_1)}$ and $L_B^{(k_2)}$ are L_B values corresponding to k_1 and k_2, respectively. Therefore, the larger k is, the larger L_B is. It can be understood intuitively because a larger k means that more sequences exist in the set and cross correlation of the set increases accordingly. If $q - 1 = k \cdot t$ for some integer t, L_B converges to $\sqrt{q-1-t}$ as q increases. Note that for a sufficiently large q and k such that $\frac{q-1}{k} = t \ll q$, $\sqrt{q-1-t} \approx \sqrt{q}$. On the other hand, the actual $C_{\max}$ of $\mathbf{S}$ is less than or equal to $\sqrt{q}+3$, which does not depend on the value of k. Therefore, in these cases, the L_B and the actual $C_{\max}$ of the set $\mathbf{S}$ are approximately same.

TABLE I
Comparison of Cross Correlation and its Bound of Type-2 Sequences

q	k	max	Bound (=$\sqrt{q}$+3)	L_B
7	3	3.000	5.646	1.809
11	5	5.584	6.317	2.774
13	6	6.245	6.606	3.125
17	8	6.878	7.123	3.720
19	9	7.231	7.359	3.982
23	11	7.762	7.796	4.460
29	14	8.318	8.385	5.091
31	10	8.467	8.568	5.174
31	15	8.362	8.568	5.284
37	18	9.077	9.083	5.826
41	20	9.394	9.403	6.160
43	21	9.530	9.557	6.320
47	23	9.812	9.856	6.630
59	29	10.644	10.681	7.481
61	30	10.796	10.810	7.613
67	33	11.158	11.185	7.998
71	35	11.395	11.426	8.244
73	36	11.533	11.544	8.365
79	39	11.875	11.888	8.716
83	41	12.103	12.110	8.943
89	44	12.427	12.434	9.272
97	48	12.840	12.849	9.694
101	50	13.043	13.050	9.898
103	51	13.137	13.149	9.999

To compare the actual cross correlation and the upper bound given in the previous section and the Welch bound L_B, we present Table I for all the primes $q \le 103$ and the maximum divisor $k < q-1$ of $q-1$.

V. Conclusion

In this correspondence, we have proved that the cross correlation between k-ary Type-2 sequences of period $q-1$ which was originally suggested by Sidel'nikov and its constant multiple sequences is upper bounded $\sqrt{q}+3$. Since there are $k-1$ distinct ways to multiply a constant to the given k-ary Type-2 sequence, it gives us a sequence family where there are $k-1$ sequences whose maximum out-of-phase autocorrelation are less than 4 and the maximum cross correlation between any distinct sequences in the family is not greater than $\sqrt{q}+3$. For a sufficiently large q and k, the maximum cross correlation of the family is approximately the same as the Welch's bound.

References

[1] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. New York: Wiley, 1996.

[2] V. S. Pless and W. C. Huffman, Eds., *Handbook of Coding Theory*. New York: Elsevier, 1998.

[3] S. W. Golomb and G. Gong, *Signal Design for Good Correlation—For Wireless Communication, Cryptography and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[4] J. S. Lee and L. E. Miller, *CDMA Systems Engineering Handbook*. Boston, MA: Artech House, 1998.

[5] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistance codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16–22, 1969.

[6] Y. -J. Kim, H. -Y. Song, G. Gong, and H. Chung, "Cross correlation of q-ary power residue sequences of period p," in *Proc. IEEE Int. Symp. Information Theory*, Seattle, WA, Jul. 2006, pp. 311–315.

[7] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 3, pp. 397–399, May 1974.