PAPER

Correlation of Column Sequences from the Arrays of Sidelnikov Sequences of Different Periods*

Min Kyu SONG[†a)], ***Nonmember and*** **Hong-Yeop SONG**[†b)], ***Member***

SUMMARY We show that the non-trivial correlation of two properly chosen column sequences of length $q-1$ from the array structure of two Sidelnikov sequences of periods q^e-1 and q^d-1, respectively, is upper-bounded by $(2d-1)\sqrt{q}+1$, if $2 \le e < d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$. Based on this, we propose a construction by combining properly chosen columns from arrays of size $(q-1) \times \frac{q^e-1}{q-1}$ with $e = 2, 3, \ldots, d$. The combining process enlarge the family size while maintaining the upper-bound of maximum non-trivial correlation. We also propose an algorithm for generating the sequence family based on Chinese remainder theorem. The proposed algorithm is more efficient than brute force approach.

key words: *Sidelnikov sequences, array structure, correlation*

1. Introduction

Sequences with good correlation properties have been used for various applications such as serving multiple users over the same channel, estimating the channel state in digital communications [3], and ranging the distance in GPS/GNSS systems [1]. For communication systems employing code division multiple access using direct-sequence spread spectrum (DS-CDMA), it is important to serve a given number of multiple users with as low interference as possible, since such systems are known to be interference-limited [5], [13]. Therefore, sequences have been designed so that their correlation properties satisfy some optimality condition maintaining certain reasonable size restriction.

Recent success in commercial mobile communications through various generations up to 5G has reached a position where "massive connectivity" and "grant-free access" are getting more and more attentions and non-orthogonal multiple access schemes need to be studied [11]. Dai et al. [11, page.74] mentioned that "*...due to the rapid development of the Internet of Things (IoT), 5G needs to support massive connectivity of users and/or devices to meet the demand for low latency, low-cost devices, and diverse service types.*" Lots of multiple access (MA) schemes have recently been proposed for massive connectivity and/or grant-free access. Among these, the code-based MA schemes, for example, MUSA (Multi-User Shared Access), are getting an attention for supporting massive connectivity and grant-free access [19]. Therefore, now, we have to pay a lot more attention on increasing the family size as much as possible in the designing sequences for MA with correlation properties somewhat compromised. This gives a motivation of studying and developing sequence families of size as big as possible with reasonable condition on correlation magnitude.

For the DS-CDMA, one has to find sequence families with as low complex correlation as possible, with reasonable number in size. Gold sequence family [2], constructed using an m-sequence and its decimations, is a famous example of optimal binary sequences family in correlation magnitude with fairly large size. From then on, so many examples of both binary and non-binary families with optimal correlation properties have been studied with limited number in sizes [4], [6]–[10], [17]. Sidelnikov sequences [12], which have been initially presented as having good auto-correlation property, have also been considered for the multiple acess for the first time in [6] and this family has been considerably improved in size by many others [4], [7], [8], [17]. The approach in this line was to employ 'multiplying constants' or 'shift-and-add' to increase the family size [4], [6], [7]. In 2010, Yu and Gong proposed a sequence family construction from the $(q-1) \times \frac{q^2-1}{q-1}$ array structure of Sidelnikov sequences of period q^2-1 [17]. Later, this idea is generalized to use Sidelnikov sequences of period q^d-1 and its array structures of size $(q-1)\times\frac{q^d-1}{q-1}$ [8]. Their main contribution is to study the various properties of the column sequences of such array structures [8]. Here, we would like to note that [17] and [8] are considered correlation properties of column sequences from the array structure of the same Sidelnikov sequence.

The main theme of this paper is investigation of correlation properties of some column sequences of length $q-1$ from the array structure of Sidelnikov sequences of possibly different periods q^e-1 and q^d-1, respectively, where $2 \le e < d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$. For this, we first present a brief review of previous results in Sect. 2. After then, Sect. 3 is devoted to discuss correlation of some column sequences from the array structure of Sidelnikov sequences of different lengths. This allows us to combine columns sequences from Sidelnikov-sequence-arrays of different lengths while remaining the same upper-bound on the maximum non-trivial correlation. By this process, the combined sequence family is of size slightly larger than that of sequence families given by [8]. For some efficient implementation of the proposed family, we give a construction in Sect. 4, which is

Manuscript received August 13, 2018.
Manuscript revised February 28, 2019.

[†] The authors are with Yonsei University, Seoul, Korea.

[*] This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2017R1A2B4011191). This paper was presented in part at 2016 International Symposium on Information Theory.

a) E-mail: mk.song@yonsei.ac.kr
b) E-mail: hysong@yonsei.ac.kr (Corresponding author)

DOI: 10.1587/transfun.E102.A.1333

much better than brute force approach discussed in [8]. In Sect. 5, we finish this paper with some concluding remarks.

Throughout this paper, we will use the following notation:

- p is a prime number.
- q is a prime power $q = p^r$ with a positive integer r.
- $GF(q)$ is the finite field with q elements.
- $\mathbb{Z}_n$ is the integers modulo n.
- M is a divisor of $q-1$ with $M \geq 2$.
- α is a primitive element of $GF(q^d)$.
- $\beta = \alpha^{\frac{q^d-1}{q-1}}$ is a primitive element of $GF(q)$.
- $\log_\beta(\cdot)$ is a discrete log over $GF(q)$ such that $\log_\beta(x) = k$ if and only if non-zero $x = \beta^k$ in $GF(q)$. We use $\log_\beta(0) = 0$ for convenience.
- $p_l(x)$ is the minimal polynomial of $-\alpha^{-l}$ over $GF(q)$.
- $\omega_M = \exp\left(\frac{2\pi\sqrt{-1}}{M}\right)$ is a primitive M-th root of unity.
- ψ is a multiplicative character of $GF(q)$ of order M defined by $\psi(x) = \omega_M^{\log_\beta(x)}$. Note that $\psi(0) = 1$.

2. Preliminaries

2.1 Correlation of Sequences

Let $x = \{x(n)\}_{n=0}^{L-1}$ and $y = \{y(n)\}_{n=0}^{L-1}$ be two M-ary sequences of period L. When we regard them as the phase sequences of certain polyphase sequences, then the (periodic) complex correlation between x and y at time shift τ is given by

$$C_{x,y}(\tau) = \sum_{n=0}^{L-1} \omega_M^{x(n)-y(n+\tau)}.$$

If y is cyclically equivalent to x, i.e., y is a cyclic shifted version of x, then it is called autocorrelation and denoted by $C_x(\tau)$, simply. Otherwise, $C_{x,y}(\tau)$ is correlation of two cyclically inequivalent sequences x, y. In this case, it is called crosscorrelation.

For a given set $\mathcal{K}$ of M-ary sequences of period L, the maximum non-trivial complex correlation among sequences in $\mathcal{K}$, denoted by $C_{\max}(\mathcal{K})$, is

$$C_{\max}(\mathcal{K}) = \max\left\{ \max_{\substack{x\in\mathcal{K}\\ \tau\neq 0}} |C_x(\tau)|, \max_{\substack{x,y\in\mathcal{K}\\ x\neq y}} \left|C_{x,y}(\tau)\right| \right\}.$$

2.2 Sidelnikov Sequences and Their Array Structure

Let α be a primitive element of $GF(q^d)$, and β be the primitive element of $GF(q)$ given by the relation

$$\beta = \alpha^{\frac{q^d-1}{q-1}}.$$

$$\begin{pmatrix} s_d(0) & s_d(1) & \cdots & s_d(\frac{q^d-1}{q-1}-1) \\ s_d(\frac{q^d-1}{q-1}) & s_d(\frac{q^d-1}{q-1}+1) & \cdots & s_d(2\times\frac{q^d-1}{q-1}-1) \\ \vdots & \vdots & \ddots & \vdots \\ s_d((q-2)\times\frac{q^d-1}{q-1}) & s_d((q-2)\times\frac{q^d-1}{q-1}+1) & \cdots & s_d(q^d-2) \end{pmatrix}$$

Fig. 1 The 2-D array structure of a Sidelnikov sequence $s_d(t)$ of period q^d-1.

Then, for a divisor M of $q-1$ with $M \geq 2$, the t-th term of an M-ary Sidelnikov sequence $\{s_d(t)\}_{t=0}^{q^d-1}$ of period q^d-1 can be written by [8]

$$s_d(t) \equiv \log_\beta\left(N_1^d(\alpha^t+1)\right) \pmod{M}, \tag{1}$$

where $N_1^d(x)$ is the norm function from $GF(q^d)$ to $GF(q)$, defined by

$$N_1^d(x) = \prod_{i=0}^{d-1} x^{q^d} = x^{(q^d-1)/(q-1)}.$$

Consider the array of a Sidelnikov sequence by writing the M-ary Sidelnikov sequence of period q^d-1 as a $(q-1)\times\frac{q^d-1}{q-1}$ array shown in Fig. 1. Then, the t-th term of the l-th column $\{v_l(t)\}_{t=0}^{q-1}$ of the array can be written as

$$v_l(t) = s_d\left(\frac{q^d-1}{q-1}t + l\right). \tag{2}$$

According to [8], these can be classified cyclically inequivalent columns by using a q-cyclotomic coset mod $\frac{q^d-1}{q-1}$. For a given integer l, denote by $\hat{C}_l(d)$ the q-cyclotomic coset mod $\frac{q^d-1}{q-1}$ defined by

$$\hat{C}_l(d) = \left\{l, lq, lq^2, \ldots\right\},$$

and let m_l be the cardinality of $\hat{C}_l(d)$. Then, m_l is the least positive integer such that [8]

$$\frac{q^d-1}{(q^{m_l}-1)\gcd(\frac{d}{m_l}, q-1)} \Big| l. \tag{3}$$

Then, the l-th column sequence given by (2) has the following properties:

Fact 1 (Theorem 3 and Corollary 1 in [8]) *Let $\{s_d(t)\}$ be an M-ary Sidelnikov sequence of period q^d-1 given by* (1) *and consider its $(q-1)\times\frac{q^d-1}{q-1}$ array structure.*

1. *The first column $\{v_0(t)\}$ can be written as*
$$v_0(t) \equiv d\log_\beta(\beta^t+1) \pmod{M}.$$
2. *Two column sequences $\{v_{l_1}(t)\}$ and $\{v_{l_2}(t)\}$ are cyclically equivalent if l_1, l_2 are in the same q-cyclotomic coset mod $\frac{q^d-1}{q-1}$.*
3. *If $m_l = d$, then $\{v_l(t)\}$ is of period $q-1$ for any M.*

To consider cyclically inequivalent columns of period $q-1$ regardless of M, we will consider the set $\Lambda'(d)$ defined as the following: $\Lambda(d)$ is the set of smallest representatives of all the q-cyclotomic cosets $\hat{C}_l(d)$ mod $\frac{q^d-1}{q-1}$ except for $l = 0$, and

$$\Lambda'(d) = \{l \in \Lambda(d) | m_l = d\}. \tag{4}$$

The exact size of $\Lambda'(d)$ was known by [17] for $d = 2$ as $\lfloor q/2 \rfloor$ and was known by [8] for some cases of d. It is also known by [8] that, for $d \geq 3$, as $q \to \infty$,

$$|\Lambda'(d)| \sim \frac{q^{d-1}}{d}. \tag{5}$$

If $l \in \Lambda'(d)$, a column sequence $\{v_l(t)\}$ defined by (2) can be alternatively written as [8]

$$v_l(t) = \log_\beta \left(\beta^l p_l\left(\beta^t\right)\right), \tag{6}$$

where $p_l(x)$ is a minimal polynomial over $GF(q)$ which has $-\alpha^{-l}$ as a root. In [8], there were some constructions for sequence families having good correlation properties by using different subsets of $\Lambda(d)$. Here, we review only the case with $\Lambda'(d)$, which will be considered in this paper:

Fact 2 (Theorems 4, 6 in [8]) *For an integer d in the range* $2 \leq d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$, *define a set of column sequences* $\Sigma'(d)$ *by*

$$\Sigma'(d) = \{cv_l(t) | l \in \Lambda'(d), 1 \leq c < M\},$$

where $v_l(t)$ *is given by* (2).

1. $C_{\max}(\Sigma'(d)) \leq (2d-1)\sqrt{q} + 1$. *As a result, all the sequences in* $\Sigma'(d)$ *are cyclically inequivalent to each other.*
2. $|\Sigma'(d)| \sim \frac{(M-1)q^{d-1}}{d}$.

In [8], they combined $\Sigma'(d)$ with two previous known sequence families $\mathcal{I}_S$ of [6] and $\mathcal{A}_S$ of [7] and [4] which are sequence sets of period $q-1$ and defined by

$$\mathcal{I}_S = \{cs_1(t) | 1 \leq c < M\}, \tag{7}$$

$$\mathcal{A}_S = \left\{c_0 s_1(t) + c_1 s_1(t+\delta) | 1 \leq \delta \leq \left\lfloor \frac{q-1}{2} \right\rfloor\right\}, \tag{8}$$

respectively, where $s_1(t)$ is the Sidelnikov sequence of period $q-1$ generated by $\beta = \alpha^{\frac{q^d-1}{q-1}}$ and $1 \leq c_0, c_1 < M$ if $1 \leq \delta \leq \lfloor \frac{q-1}{2} \rfloor$ and $1 \leq c_0 < c_1$ if $\delta = \frac{q-1}{2}$. One interesting point is that, even those are combined, the maximum non-trivial complex correlation is still upper-bounded by $(2d-1)\sqrt{q}+1$. The folowing have been used to obtain upper-bound on the maximum non-trivial complex correlation:

Fact 3 (Weil bound [16]) *Let* $f_1(x), \ldots, f_l(x)$ *be* l *distinct monic irreducible polynomials over* $GF(q)$ *which are of positive degree* $d_1, \ldots, d_l$, *respectively. Let* e_i *be the number of distinct roots of* $f_i(x)$ *in* $GF(q)$ *for* $1 \leq i \leq l$ *and* k *be the number of distinct roots of* $\prod_{i=1}^{l} f_i(x)$ *in its splitting field over* $GF(q)$. *Let* $\psi_1, \ldots, \psi_l$ *be multiplicative characters of* $GF(q)$, *with* $\psi_i(0) = 1$ *for* $1 \leq i \leq l$. *If the product character* $\prod_{i=1}^{l} \psi_i(f_i(x))$ *is non-trivial for some* x, *then*

$$\left| \sum_{x \in GF(q)} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq (\sum_{i=1}^{l} d_i - 1)\sqrt{q},$$

for any $a_i \in GF(q) \setminus \{0\}$, $1 \leq i \leq l$.

3. Column Sequences from Sidelnikov Sequences of Different Lengths

Our first goal is analyzing the cross-correlation of two column sequences of period $q-1$ from arrays of two M-ary Sidelnikov sequences of periods $q^e - 1$ and $q^d - 1$, respectively, where $2 \leq e \leq d < \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right)$.

Lemma 1 *Let* e, d *be two positive integers with* $2 \leq e \leq d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$ *and consider* $GF(q^e)$ *and* $GF(q^d)$. *There exist primitive elements of these fields, say,* α_e *and* α_d, *respectively, such that* $\alpha_e^{\frac{q^e-1}{q-1}} = \alpha_d^{\frac{q^d-1}{q-1}} \in GF(q)$.

Proof *Let* $h = \operatorname{lcm}(e, d)$, *and* α_h *be a primitive element of* $GF(q^h)$. *Choose* $\alpha_e = \alpha_h^{\frac{q^h-1}{q^e-1}}$ *and* $\alpha_d = \alpha_h^{\frac{q^h-1}{q^d-1}}$. *Then, it is obvious that*

$$\alpha_e^{\frac{q^e-1}{q-1}} = \alpha_d^{\frac{q^d-1}{q-1}} \in GF(q),$$

which is desired. ■

Here after, we will use the notation that

$$\alpha_e^{\frac{q^e-1}{q-1}} = \alpha_d^{\frac{q^d-1}{q-1}} = \beta$$

is the primitive element of $GF(q)$ in the representation (1).

Theorem 1 *Let* e *and* d *be some integers with* $2 \leq e < d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$. *If we construct* $\Sigma'(e)$ *and* $\Sigma'(d)$ *by choosing primitive elements* α_e *and* α_d *as in Lemma 1, then any two sequences* $a(t) \in \Sigma'(e)$ *and* $b(t) \in \Sigma'(d)$ *have*

$$|C_{a,b}(\tau)| \leq (e + d - 1)\sqrt{q} + 1$$

as their maximum correlation magnitude. Hence, they are cyclically inequivalent.

Proof *From Lemma 1, make* $N_1^e(\alpha_e^t + 1)$ *and* $N_1^d(\alpha_d^t + 1)$ *be functions of a primitive element* β *of* $GF(q)$. *Then,* $a(t) \in \Sigma'(e)$ *with constant* $1 \leq c_1 < M$ *and column index* l_1 *is*

$$a(t) = c_1 \log_\beta \beta^{l_1} p_{l_1}(\beta^t),$$

and $b(t) \in \Sigma'(d)$ *with constant* $1 \leq c_2 < M$ *and column index* l_2 *is*

$$b(t+\tau) = c_2 \log_\beta \beta^{l_2} p_{l_2}(\beta^{t+\tau}),$$

Table 1 Comparison of $\Sigma'(d)$ in [8] and $\Sigma'^{U}(d)$ in Def. 1 when $q = 101$, $M = 100$, and $d = 3, 4$.

	Set size	Asymptotic size (10)	Maximum correlation	Bound (9)
$\Sigma'(3)$ in [8]	339,966	336,633	39.849	50.249
$\Sigma'^{U}(3)$	344,916	336,633	39.849	50.249
$\Sigma'(4)$ in [8]	25,749,900	25,499,950	43.475	70.349
$\Sigma'^{U}(4)$	26,094,816	25,499,950	44.147	70.349

where $\beta^{l_1}p_{l_1}(x)$ and $\beta^{l_2}p_{l_2}(\beta^{\tau}x)$ are two distinct monic irreducible polynomials of degree e and d, respectively. Then, their complex cross-correlation function becomes

$$\begin{aligned}C_{a,b}(\tau) &= \sum_{t=0}^{q-2} \omega_M^{a(t)-b(t+\tau)} \\ &= \sum_{t=0}^{q-2} \psi_1(\beta^{l_1}p_{l_1}(\beta^t))\psi_2(\beta^{l_2+\tau d}\beta^{-\tau d}p_{l_2}(\beta^{t+\tau})),\end{aligned}$$

where $\psi_1 = \psi^{c_1}$ and $\psi_2 = \psi^{M-c_2}$ are both non-trivial multiplicative characters. Here, note that $\beta^{-\tau d}p_{l_2}(\beta^{t+\tau}) = p_{l_2}(\beta^t)$. So, by applying the Weil bound in Fact 3, we have

$$\begin{aligned}&|C_{a,b}(\tau)| \\ &= \left| \sum_{x\in GF(q)^*} \psi_1\left(\beta^{l_1}p_{l_1}(x)\right)\psi_2\left(\beta^{l_2}p_{l_2}(\beta^{\tau}x)\right)\right| \\ &\le \left| \sum_{x\in GF(q)} \psi_1\left(\beta^{l_1}p_{l_1}(x)\right)\psi_2\left(\beta^{l_2}p_{l_2}(\beta^{\tau}x)\right)\right| + 1 \\ &\le (e+d-1)\sqrt{q}+1.\end{aligned}$$

Note that, since $(e+d-1)\sqrt{q}+1 < q-1$ under the assumption, $a(t)$ and $b(t)$ are cyclically inequivalent. ■

From Theorem 1, we can construct a set of sequences by taking a union of all the sequence families from the array structures of Sidelnikov sequences of periods q^2-1, q^3-1, ..., q^d-1 without increasing the upper-bound on the maximum non-trivial complex correlation. Here, we have to use some appropriate primitive elements of $GF(q^2), GF(q^3), ..., GF(q^d)$, respectively, all obtained from a primitive element of $GF(q^h)$ where $h = \mathrm{lcm}(2, ..., d)$.

Definition 1 (Unified sequence family) *Assume that all the primitive elements are chosen properly and let $\Sigma'^{U}(d)$ be the set of M-ary sequences of period $q-1$, given by*

$$\Sigma'^{U}(d) = \bigcup_{e=2}^{d} \Sigma'(e).$$

Corollary 1 *If $2 \le d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$, then*

$$C_{\max}(\Sigma'^{U}(d)) \le (2d-1)\sqrt{q}+1. \qquad (9)$$

Since the sequence family in **Definition 1** is the union of $\Sigma'(d)$ in [8], we can directly combine it with $\mathcal{I}_S$ and $\mathcal{A}_S$ to construct new sequence families.

Corollary 2 *With all the previous assumptions and notations, construct a new set of sequences by combining $\Sigma'^{U}(d)$, $\mathcal{I}_S$, and $\mathcal{A}_S$. Then, any pair of sequences in the set are cyclically inequivalent and*

$$C_{\max}(\Sigma'^{U}(d) \cup \mathcal{I}_S \cup \mathcal{A}_S) \le (2d-1)\sqrt{q}+1.$$

Note that, even though $\Sigma'^{U}(d)$ is union of properly chosen columns from arrays of size $(q-1)\times\frac{q^e-1}{q-1}$ with $e = 2, 3, ..., d$, from the asymptotic size of $\Sigma'(d)$ in (5), we have

$$\left|\Sigma'^{U}(d)\right| \sim (M-1)q^{d-1}/d. \qquad (10)$$

Table 1 shows the comparison of $\Sigma'(d)$ of [8] and $\Sigma'^{U}(d)$ of this paper for $q = 101$, $M = 100$, and $d = 3, 4$. Here, all the appeared maximum correlation magnitudes are calculated by using up to one million pairs of sequences. In this table, $\Sigma'^{U}(d)$ is of size slightly larger than that of $\Sigma'(d)$. This is because $\Sigma'^{U}(d)$ additionally contains $\Sigma'(2)$, ... $\Sigma'(d-1)$, all of which are only of marginal size compared with that of $\Sigma'(d)$. We finish this section with Table 2 which gives a comparison of the proposed family $\Sigma'^{U}(d)$ with some well-known polyphase sequence families.

4. Problem of Constructing for $\Lambda'(d)$

So far, we have just defined the set $\Lambda'(d)$ mathematically over the integers mod $(q^d-1)/(q-1)$. As mentioned in [8], a brute force approach for obtaining $\Lambda'(d)$ may take time-complexity on the order of $\left(\frac{q^d-1}{q-1}\right)^2$ and the required memory size is approximately $\frac{q^{d-1}}{d} \times \lceil \log_2 \frac{q^d-1}{q-1} \rceil$. This may be huge for large q and d. To overcome this, we need more efficient construction for $\Lambda'(d)$.

Let $\frac{q^d-1}{q-1} = \prod_{i=1}^{k} p_k^{e_k}$ be the prime factorization of $\frac{q^d-1}{q-1}$ and consider a map from $\mathbb{Z}_{\frac{q^d-1}{q-1}}$ to $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$ given by

$$\begin{aligned}f : x \longmapsto &\left(x \mod p_1^{e_1},\ x \mod p_2^{e_2}, ...,\ x \mod p_k^{e_k}\right) \\ &\triangleq (x_1, x_2, ..., x_k). \qquad (11)\end{aligned}$$

By the Chinese remainder theorem, it is known that the map in (11) defines a ring isomorphism

Table 2 Comparison with some known polyphase sequence families.

	Length L	Alphabet Size M	$C_{\max}$	Family Size
Trachtenberg [15]	$p^m - 1$	L	$= \sqrt{p(L+1)} + 1$	$= L + 2$
Kumar, Moreno [10]	$p^m - 1$	p	$\le \sqrt{L+1} + 1$	$= L + 1$
Kumar, Helleseth [9]	$2^m - 1$	4	$\le 4\sqrt{L+1} + 1$	$\ge L^3 + 4L^2 + 5^L + 2$
Kim, Song [6]	$q - 1$	$M \mid q$	$\le \sqrt{q} + 3$	$= M - 1$
Kim et al. [7]	$q - 1$	$M \mid q$	$\le 3\sqrt{q} + 5$	$= (M-1)\left(\frac{(M-1)(q-1)+\delta-2}{2}\right)$
Yu, Gong [17]	$q - 1$	$M \mid q$	$\le 3\sqrt{q} + 5$	$= \frac{M(M-1)}{2}(q-2) + (M-1)$
Kim, Kim, Song [8]	$q - 1$	$M \mid q$	$\le (2d-1)\sqrt{q} + 1$	$\sim (M-1)q^{d-1}/d$
$\Sigma'^{U}(d)$ in this paper	$q - 1$	$M \mid q$	$\le (2d-1)\sqrt{q} + 1$	$\sim (M-1)q^{d-1}/d$, slightly larger than the above; See Table 1.

$$\mathbb{Z}_{\frac{q^d-1}{q-1}} \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}} = \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

That is, the map preserves additions and multiplications of elements. (Here, additions and multiplications over $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$ are performed component-wise.) The inverse map of (11) is well-known by

$$g : (x_1, x_2, ..., x_k) \longmapsto \sum_{i=1}^{k} x_i y_i z_i = x, \qquad (12)$$

where $y_i = (q^d - 1)/(q-1)p_i^{e_i}$ and $z_i = y_i^{-1} \pmod{p_i^{e_i}}$. Here, $q \not\equiv 0 \pmod{p_i^{e_i}}$ for any i since $q^d \equiv 1 \pmod{\frac{q^d-1}{q-1}}$.

Lemma 2 *For a prime power q, let $\prod_{i=1}^{k} p_k^{e_k}$ be the prime factorization of $\frac{q^d-1}{q-1}$ and f be the function given by* (11).

1. *For an integer $a \in \mathbb{Z}_{\frac{q^d-1}{q-1}}$, the q-cyclotomic coset $\hat{C}_a(d)$ mod $\frac{q^d-1}{q-1}$ is of size d if and only if there exists some index i such that $q^j a_i \equiv a_i \pmod{p_i^{e_i}}$ only when j is a multiple of d.*
2. *Two integers $a, b \in \mathbb{Z}_{\frac{q^d-1}{q-1}}$ are not in the same q-cyclotomic coset mod $\frac{q^d-1}{q-1}$ if and only if there exists some j such that $a_j \neq q^u b_j$ for any $u = 0, 1, 2, ..., d-1$.*

Proof *We omit the proof since it is straightforward.* ■

Based on Lemma 2, $\Lambda'(d)$ can be obtained by picking up an element in $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$ according to the following rules and applying the map g given by (12):

FIRST RULE: For the condition $\left|\hat{C}_a(d)\right| = d$, from Lemma 2-1, pick up an element a from $\prod_{i=1}^{k} \mathbb{Z}_{p_i^{e_i}}$ in which $q^j a_i \equiv a_i \pmod{p_i^{e_i}}$ only when j is a multiple of d.

SECOND RULE: To pick up representatives of different q-cyclotomic cosets mod $\frac{q^d-1}{q-1}$, there should be at least one index i for which those elements have distinct representatives of q-cyclotomic cosets mod $p_i^{e_i}$.

Here, if $e_i = 1$, finding all the representatives of q-cyclotomic cosets mod p_i can be done in a straightforward manner as follow:

Lemma 3 *For a prime power q and an integer $d \ge 2$, let p_i be a prime factor of $\frac{q^d-1}{q-1}$, and δ be a primitive root of $\mathbb{Z}_{p_i}$. Then,*

$$\left\{\delta^x \mid 0 \le x \le \frac{p_i - 1}{v} - 1\right\}$$

is a set of all the representatives of q-cyclotomic cosets mod p_i, where v is the smallest positive integer such that $q^v \equiv 1 \pmod{p_i}$.

Proof *Note that $q \not\equiv 0 \pmod{p_i}$, since $q^d \equiv 1 \pmod{\frac{q^d-1}{q-1}}$. Therefore, q can be written as a power of δ, i.e.,*

$$q = \delta^{\frac{u(p-1)}{v}}$$

where v is the smallest positive integer such that $q^v \equiv 1 \pmod{p_i}$. Then, $\delta^x \not\equiv q^i \delta^y \pmod{p_i}$ for any i, if $0 \le x < y \le \frac{p_i-1}{v} - 1$. And, obviously, if $\frac{p_i-1}{v} \le y \le p_i - 1$, there exist some x with $0 \le x \le \frac{p_i-1}{v} - 1$ such that $\delta^x = q^i \delta^y$ for some i. ■

Example 1 *Let $q = 7$ and $d = 3$. Then, $(q^d - 1)/(q-1) = 57 = 3 \times 19$ is a multiple of two odd prime numbers. By Lemma 3, we can find representatives of all the q-cyclotomic cosets mod 3 and all the q-cyclotomic cosets mod 19, respectively. Here, since $q \equiv 1 \pmod 3$, any element of $\mathbb{Z}_3$ is a representative of a q-cyclotomic coset mod 3. Note that any elements of $\mathbb{Z}_3$ represents a q-cyclotomic coset mod 3 with cardinality 1. Therefore, according to* **FIRST RULE**, *it is enough to consider $\mathbb{Z}_{19}$. Choose 2 as a primitive root of $\mathbb{Z}_{19}$. Lemma 3 implies that*

Algorithm 1 An Algorithm for constructing $\Lambda'(d)$

```
Input: Two integers $q$ and $d$
Output: The set $\Lambda'(d)$
Determine prime factors: $\frac{q^d-1}{q-1} = \prod_{i=1}^{k} p_k^{e_k}$
Determine $(q_1, q_2, \ldots, q_k) = f(q)$ by (11)
Set $T = \left\{ i \mid q_i^x \not\equiv 1 \pmod{p_i^{e_i}} \text{ for any } x \text{ not a multiple of } d \right\}$
for $i = 1$ to $k$ do
    Set $A_i = \emptyset$
    if $i \in T$ then
        Find all the representatives of $q$-cyclotomic cosets mod $p_i^{e_i}$
        of size $d$, and put them into $A_i$
    end if
end for
Set $U = \{(u_1, u_2, \ldots, u_k) \mid u_i \in \mathbb{Z}_2$ for $i \in T$ and
        $u_i = 0$ for $i \notin T\} \setminus \{(0, 0, \ldots, 0)\}$
Set $B = \emptyset$
for each $u \in U$ do
    $B \leftarrow B \cup \{(x_1, x_2, \ldots, x_k) \mid x_i \in A_i$ for $u_i = 1$ and
        $x_i \in \mathbb{Z}_{p_i^{e_i}} \setminus A_i$ for $u_i = 0\}$
end for
return $\{g(b) \mid b \in B\}$ where $g$ is defined in (12)
```

$$\left\{ 2^x \mid 0 \le \frac{p_2 - 1}{3} - 1 = 5 \right\} = \{1, 2, 4, 8, 16, 13\} \qquad (13)$$

is the set of all the representatives 2^x *of* 7*-cyclotomic cosets mod* 19*. Note that the size of the coset represented by* 2^x *above can be either* 1 *or* 3*. Just check the size of each and obtain the set* A_2 *of representatives of* q*-cyclotomic cosets mod* 19 *of size* $d = 3$*, as*

$$A_2 = \{1, 2, 4, 8, 16, 13\}.$$

By using the function g *defined in* (12)*, we can construct* $\Lambda'(d)$ *as*

$$\Lambda'(d = 3) = \{g\,(b_1, b_2) \mid b_1 \in \mathbb{Z}_3, b_2 \in A_2\},$$

and hence,

$$|\Lambda'(3)| = |\mathbb{Z}_3| \times |A_2| = 18.$$

The process in Example 1 can be generalized as Algorithm 1. When we use Algorithm 1 without pre-computed information about A_i's, the time-complexity of constructing each A_i by checking 1 to $p_i^{e_i} - 1$ is order of $p_i^{2e_i}$. So, total time-complexity is at most order of $\sum_{i=1}^{k} p_i^{2e_i}$, which becomes much smaller than $\left(\frac{q^d-1}{q-1}\right)^2 = \prod_{i=1}^{k} p_i^{2e_i}$.

When we use Algorithm 1 with pre-computed information of A_i's, the required memory size is reduced to at most $\sum_{i=1}^{k} \frac{p_i^{e_i}}{d} \times \lceil \log_2 p_i^{e_i} \rceil$ bits, and hence, the required memory size also becomes smaller as the number of distinct prime factors of $\frac{q^d-1}{q-1}$ becomes larger.

5. Concluding Remarks

The main contribution of this paper is the analysis of cross-correlation of some column sequences from the array structure of Sidelnikov sequences of period $q^2-1, q^3-1, \ldots, q^d-1$, and enlarging size of the previous family by involving all of them while preserving upper-bound on the correlation. The proposed sequence family may be applicable to code-based non-orthogonal multiple access schemes for massive connectivity and/or grant-free access. We also gave an algorithm to generate the proposed family. The proposed algorithm is more efficient than brute force approach, but it might be not enough to use them in practice. Therefore, it would be important to find a more efficient manner for identifying the set $\Lambda'(d)$.

References

[1] Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification, document IS-GPS-200H, March 2014.

[2] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," IEEE Trans. Inf. Theory, vol.14, no.1, pp.154–156, Jan. 1968.

[3] S.W. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communications, Cryptography, and Radar, Cambridge University Press, 2005.

[4] Y.K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," IEEE Trans. Inf. Theory, vol.55, no.4, pp.1815–1823, April 2009.

[5] J.K. Holmes, Spread Spectrum Systems for GNSS and Wireless Communications, Artech House, 2007.

[6] Y.-J. Kim and H.-Y. Song, "Cross correlation of Sidelnikov sequences and their constant multiples," IEEE Trans. Inf. Theory, vol.53, no.3, pp.1220–1224, March 2007.

[7] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidelnikov sequences," IEEE Trans. Inf. Theory, vol.54, no.8, pp.3768–3774, Aug. 2008.

[8] Y.-T. Kim, D.S. Kim, and H.-Y. Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences," IEEE Tans. Inf. Theory, vol.61, no.1, pp.655–670, Jan. 2015.

[9] P.V. Kumar, T. Helleseth, A.R. Calderbank, and A.R. Hammons, Jr., "Large families of quaternary sequences with low correlation," IEEE Trans. Inf. Theory, vol.42, no.2, pp.579–592, March 1996.

[10] P.V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inf. Theory, vol.37, no.3, pp.603–616, May 1991.

[11] L. Dai, Y. Yuan, S. Han, I. Chih-Lin, and Z. Wang, "Non-orthogonal multiple access for 5G: Solutions, challenges, opportunities, and future research trends," IEEE Commun. Mag., vol.53, no.9, pp.74–81, Sept. 2015.

[12] V.M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," Problemy peredachi Information, vol.5, no.1, pp.16–22, 1969.

[13] M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill, New York, 1994.

[14] M.K. Song, H.-Y. Song, D.S. Kim, and J.Y. Lee, "Correlation properties of sequences from the 2-D array structure of Sidelnikov sequences of different lengths and their union," Proc. 2016 IEEE International Symposium on Information Theory (ISIT 2016), pp.105–109, Barcelona, Spain, July 2016.

[15] H.M. Trachtenberg, On the Crosscorrelation Functions of Maximal Linear Sequences, Ph.D. dissertation, Dept. EE-Syst., Univ. Southern California, Los Angeles, CA, USA, 1970.

[16] N.Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," IEEE Trans. Inf. Theory, vol.56, no.12, pp.6376–6387, Dec. 2010.

[17] N.Y. Yu and G. Gong, "New construction of M-ary sequence families

with low correlation from the structure of Sidelnikov sequences," IEEE Trans. Inf. Theory, vol.56, no.8, pp.4061–4070, Aug. 2010.

[18] Z. Yuan, G. Yu, W. Li, Y. Yuan, X. Wang, and J. Xu, "Multi-user shared access for Internet of Things," Proc. IEEE 83th Conf. Veh. Tech., pp.1–5, May 2016.

[19] T. Yunzheng, L. Long, L. Shang, and Z. Zhi, "A survey: Several technologies of non-orthogonal transmission for 5G," China commun., vol.12, no.10, pp.1–15, Oct. 2015.

Min Kyu Song received his B.S. degree in Electronic Engineering from Konkuk University, Seoul, Korea, and M.S. degree in Electrical and Electronic Engineering from Yonsei University, Seoul, Korea, in 2011 and 2013, respectively. He is currently a Ph.D. candidate working in Channel Coding and Crypto Lab. at Yonsei University. His area of research interest includes PN sequences, cryptography, and coding theory.

Hong-Yeop Song received his BS degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, California, in 1986 and 1991, respectively. He spent 2 years as a research associate at USC and then 2 years as a senior engineer at the standard team of Qualcomm Inc., San Diego, California. Since Sept. 1995, he has been with Dept. of electrical and electronic engineering, Yonsei University, Seoul, Korea. He had been serving IEEE IT society Seoul Chapter as a chair from 2009 to 2016, and served as a general co-chair of IEEE ITW 2015 in Jeju, Korea. He was awarded the 2017 Special Contribution Award from Korean Mathematical Society for his contribution to the global wide-spread of the fact that Choi (1646–1715) from Korea had discovered a pair of orthogonal Latin squares of order 9 much earlier than Euler. His area of research interest includes digital communications and channel coding, design and analysis of various pseudo-random sequences for communications and cryptography. He is a member of IEEE, MAA(Mathematical Association of America) and domestic societies KICS, IEIE, KIISC and KMS.