New M-Ary Sequence Families With Low Correlation From the Array Structure of Sidelnikov Sequences

Young-Tae Kim, Dae San Kim, *Member, IEEE*, and Hong-Yeop Song, *Senior Member, IEEE*

***Abstract*— In this paper, we extend the construction by Yu and Gong for families of M-ary sequences of period $q-1$ from the array structure of an M-ary Sidelnikov sequence of period q^2-1, where q is a prime power and $M|q-1$. The construction now applies to the cases of using any period q^d-1 for $3 \le d < (1/2)(\sqrt{q}-(2/\sqrt{q})+1)$ and $q > 27$. The proposed construction results in a family of M-ary seqeunces of period $q-1$ with: 1) the correlation magnitudes, which are upper bounded by $(2d-1)\sqrt{q}+1$ and 2) the asymptotic size of $(M-1)q^{d-1}/d$ as q increases. We also characterize some subsets of the above of size $\sim(r-1)q^{d-1}/d$ but with a tighter upper bound $(2d-2)\sqrt{q}+2$ on its correlation magnitude. We discuss reducing both time and memory complexities for the practical implementation of such constructions in some special cases. We further give some approximate size of the newly constructed families in general and an exact count when d is a prime power or a product of two distinct primes. The main results of this paper now give more freedom of tradeoff in the design of M-ary sequence family between the family size and the correlation magnitude of the family.**

***Index Terms*— Sidelnikov sequences, polyphase sequences, non-binary sequences, sequences for GNSS, family of sequences with good crosscorrelation, cyclotomic cosets.**

I. Introduction

PSEUDO-RANDOM sequences with good correlation property play some key roles in most of the communications engineering and cryptography [1], [7], [10], [16], [33], [36]. For example, sequences with good autocorrelation property have been used in various synchronization subsystems and RADAR systems [27], [29], [38]. Binary and/or non-binary sequence families with good auto and cross correlation properties have been used in various wireless multiuser multi-access communications including CDMA cellular systems [17], frequency hopping spread spectrum communication systems [3], [5], and Global Navigation Satellite Systems (GNSS) such as GPS [32] from U.S. Department of Defense and Galileo [6] from European Union and European Space Agency.

These sequences or sequence families are called pseudorandom because they look very much random for the third party observers but they are generated completely by some deterministic algorithms [37]. Required randomness of these sequences are determined by the application, but they usually include uniform distribution of each alphabet, run-length distribution, good correlation property, large family size, and sometimes, higher non-linearities for cryptographic applications [9], [37]. Non-binary sequence families with large size and good randomness properties have been studied for long time, and we now have various known families constructed by, for example, Trachtenberg [39], Helleseth [15], Kumar and Moreno [25], Kumar et al [24], Chu [2], [18], Gong [12], Anand and Kumar [1], Kim et al [20] and its generalization by Kim, Chae and Song [19]. These all achieve some of various upper bounds on the correlation magnitude and have been improved to fit the alphabet size for various applications and to the direction of maximizing the family size.

For a prime power $q = p^m$ and a positive integer M such that $M|q-1$, Sidelnikov in 1969 [35] introduced M-ary sequences (called the Sidelnikov sequences) of period $q-1$, and showed that the non-trivial autocorrelation magnitudes are upper bounded by 4 regardless of M and q. It is interesting to note that *binary* Sidelnikov sequences was re-discovered later in [26] and had been refered to as 'Sidelnikov-Lempel-Cohn-Eastman sequences' for a while [31]. Sidelnikov [35] also introduced so called M-ary power residue sequences of period p, for a prime p and $M|p-1$ with good autocorrelation property.

In 2006 [22] and subsequently in 2007 [21], for the first time, some results of designing sequence families with low crosscorrelation have been presented using power residue sequences and/or Sidelnikov sequences. The key idea was to consider the sequences using all distinct primitive elements of the field. It turned out that one can equivalently obtain all these sequences by multiplying a constant to each and every term of a given sequence. A weak point of this design is that the set size is not large enough (only $M-1$) even though the bound on their correlation magnitudes is optimal in the sense of Welch [42].

The improvement of enlarging the set size came from the idea of binary Gold sequence construction [8]. This result is first appeared in [14] and [23]. Not only considering all

Manuscript received July 13, 2013; revised July 24, 2014 and September 26, 2014; accepted November 4, 2014. Date of publication November 20, 2014; date of current version December 22, 2014. This work was supported in part by the National GNSS Research Center Program through the Defense Acquisition Program Administration and in part by the Agency for Defense Development. Part of this paper was presented at the 2013 IWSDA. Y.-T. Kim contributed to this work while he was with Yonsei University.

Y.-T. Kim was with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea. He is now with the Mobile Communications Research and Development Laboratory, LG Electronics, Inc., Seoul 153-802, Korea (e-mail: youngtae88.kim@lge.com).

D. S. Kim is with the Department of Mathematics, Sogang University, Seoul 121-742, Korea (e-mail: dskim@sogang.ac.kr).

H.-Y. Song is with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: hysong@yonsei.ac.kr).

Communicated by T. Helleseth, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2014.2371461

the constant-multiples of a Sidelnikov sequence, but also they added term-by-term additions of a (constant-multiple of) Sidelnikov sequence and its some cyclic shifts. Unlike the methods in [21], in order to prove the low correlation property of the proposed family of sequences, they both used Weil bound [41] on exponential sums, which was used in [34] to prove the conjecture appeared in [13]. This idea of using shift-and-add construction was fully generalized in [43] not only for Sidelnikov sequences but also for power residue sequences.

New horizon in this line of research has appeared by Yu and Gong [44] in 2010 by observing the $(q-1) \times (q+1)$ array structure of a (longer period) Sidelnikov sequence of period q^2-1. Note here that the number of columns in the array is $q+1 = (q^2-1)/(q-1)$. They identified cyclically inequivalent column sequences (of length $q-1$) of the array, and constructed a family of non-binary sequences with good correlation property. The family size in [44] is almost comparable to (in fact, slightly bigger than) those in [14] and [23], but this is truly a new construction.

This paper is a result of an attempt to extend the construction in [44]. We study the array structure of (much longer period) Sidelnikov sequences of period q^d-1 for $d \geq 3$ and $q > 27$, where the array now has size $(q-1) \times (\frac{q^d-1}{q-1})$, and investigate the cyclic equivalence as well as sub-period structure of column sequences in order to construct a series of some good families of M-ary sequences. As a result, we propose two constructions WITH and WITHOUT the condition $\gcd(d, M) = 1$. We furthermore characterize a subset of one of the construction with slightly tighter bound on the correlation magnitudes. These would enable one to apply the constructions to much more cases of the period q^d-1.

The resulting families have various sizes according to d, M, q, and the number of representatives of q-cyclotomic cosets mod $\frac{q^d-1}{q-1}$. We note that the families here have sizes approximately given by $(M-1)q^{d-1}/d$ (or $(r-1)q^{d-1}/d$ for some subsets, where $r \geq 2$ is a divisor of $\gcd(d, M)$) for given M and d as q increases, and has upper bound given by $(2d-1)\sqrt{q}+1$ (or $(2d-2)\sqrt{q}+2$ for the subsets) on their correlation magnitudes. Note that both the size and the bound increase as d increases. Therefore, it gives much more freedom of trade-off in the design of sequence family between the size and the maximum correlation magnitude.

This paper is organized as follows. Section II introduces some preliminaries including Sidelnikov sequences, q-cyclotomic cosets mod $\frac{q^d-1}{q-1}$, crosscorrelation, and Weil bound. Section III presents main results of this paper. Section III-A investigates the properties of column sequences and Sections III-B and III-C describe two main constructions. We count the proposed family size exactly for some special cases of d in Section III-D with one detailed example in Table II. We give some analysis on asymptotic values of this in Appendix. Section III-E discusses some practical issues on memory and time complexities for the constructions in some very special cases. Section IV gives brief concluding remarks as well as a table of comparison with previously constructed M-ary sequence families.

II. Preliminaries

A. Notation and Convention

We will fix the following notation throughout the paper:

- p: a prime number
- q: a prime power p^m with a positive integer m
- $\Delta = 1$ when q is odd and $\Delta = 2$ when q is even.
- $GF(q)$: the finite field with q elements
- $GF(q^d)$: the finite field with q^d elements with $d \geq 2$
- $GF(q)^* = GF(q)\backslash\{0\}$: the multiplicative group of $GF(q)$
- M: a divisor of $q-1$ with $M \geq 2$
- $\omega_M = \exp(j\frac{2\pi}{M})$ where $j = \sqrt{-1}$
- α: a fixed primitive element of $GF(q^d)$
- $\beta = \alpha^{(q^d-1)/(q-1)}$: the primitive element of $GF(q)$ obtained from α in $GF(q^d)$
- N: the norm function from $GF(q^d)$ to $GF(q)$ given by
$$N(x) = \prod_{i=0}^{d-1} x^{q^i} = x^{\frac{q^d-1}{q-1}}$$
- ψ: the multiplicative character of $GF(q)$ of order M defined by
$$\psi(x) = \exp\left(j\frac{2\pi}{M}\log_\beta x\right) = \omega_M^{\log_\beta x}$$
- We keep $\log_\beta(0) = 0$ and $\psi(0) = 1$ in this paper for convenience.

B. Sidelnikov Sequences

Definition 1 [35]: For any fixed primitive element β of $GF(q)$, let $D_k = \{\beta^{Mi+k} - 1 \mid 0 \leq i < \frac{q-1}{M}\}$. Then an M-ary Sidelnikov sequence $\{s(t)\}$ of period $q-1$ is defined as

$$s(t) = \begin{cases} 0, & \text{if } \beta^t = -1 \\ k, & \text{if } \beta^t \in D_k. \end{cases}$$

Equivalently,

$$s(t) \equiv \log_\beta(\beta^t + 1) \mod M, \quad 0 \leq t \leq q-2,$$

with the new convention that $\log_\beta 0 = 0$. □

In this paper, for an integer $M | q-1$, we will consider two different M-ary Sidelnikov sequences; one of shorter period $q-1$ and the other of longer period q^d-1. To distinguish one from the other, we will sometimes use $\{s_1(t)\}$ for those of period $q-1$ and $\{s_d(t)\}$ for those of period q^d-1. Then, by the above definition, an M-ary Sidelnikov sequence $\{s_d(t)\}$ of longer period can be represented as

$$s_d(t) \equiv \log_\alpha(\alpha^t + 1) \mod M, \quad 0 \leq t \leq q^d-2.$$

Note that any divisor M of $q-1$ is also a divisor of q^d-1. Sometimes, we use simply $\{s(t)\}$, but the distinction must be clear from the context.

C. Correlation

A correlation is a measure of distance between a sequence and its cyclic shifts or two sequences in a sequence family. We use the periodic correlation of two (not necessarily distinct) sequences. Following definition has been well-known [10].

Definition 2: Let $\{a(t)\}$ and $\{b(t)\}$ be M-ary sequences of period L, where $0 \le t \le L-1$. A periodic correlation between these two sequences is defined by, for $0 \le \tau \le L-1$,

$$C_{a,b}(\tau) = \sum_{t=0}^{L-1} \omega_M^{a(t)-b(t+\tau)},$$

where $\omega_M = \exp(j\frac{2\pi}{M})$ and $t+\tau$ is computed modulo L. For a sequence family $\mathcal{S}$, $C_{max}(\mathcal{S})$ is defined to be the maximum magnitude of all the nontrivial correlations of the pairs of sequences in $\mathcal{S}$. □

Note that when $\{a(t)\} = \{b(t+\delta)\}$ for some fixed δ, the correlation $C_{a,a}(\tau)$ is called the autocorrelation. It is called the crosscorrelation when they are cyclically distinct.

D. Weil Bound

Weil bound (see [28, Th. 5.41]) gives an upper bound on the magnitutde of the multiplicative character sums, and has been used to calculate some upper bounds on the crosscorrelation of various sequences [10]. Yu and Gong [43], [44] introduced some refined versions of the one by Wan [40] with an additional assumption that $\psi(0) = 1$. Here we state the version essentially the same as those in [44].

Theorem 1 [44]: Let $f_1(x), \ldots, f_m(x)$ be distinct monic irreducible polynomials over $GF(q)$ with degrees $d_1, \ldots, d_m$, with e_j the number of distinct roots in $GF(q)$ of $f_j(x)$ $(j = 1, \ldots, m)$. Let $\psi_1, \ldots, \psi_m$ be nontrivial multiplicative characters of $GF(q)$, with $\psi_j(0) = 1$ $(j = 1, \ldots, m)$. Then, for $a_1, \ldots, a_m \in GF(q)^*$, we have the estimate

$$\left|\sum_{x\in GF(q)} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x))\right| \le \left(\sum_{j=1}^{m} d_j - 1\right)\sqrt{q} + \sum_{j=1}^{m} e_j. \quad (1)$$

Furthermore, if $\prod_{i=1}^{m} \psi_i^{d_i}(x) = 1$ for all $x \in GF(q)^*$ in addition, then

$$\left|\sum_{x\in GF(q)} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x))\right| \le \left(\sum_{j=1}^{m} d_j - 2\right)\sqrt{q} + 1 + \sum_{j=1}^{m} e_j. \quad (2)$$

E. Cyclotomic Cosets Mod $q^d - 1$ and Mod $(q^d - 1)/(q - 1)$

In order to designate column sequences in the $(q-1) \times (\frac{q^d-1}{q-1})$ array of a Sidelnikov sequence $\{s_d(t)\}$ of period $q^d - 1$, we will use column indices from 0 to $(q^d-1)/(q-1) - 1$. These numbers have close relation with the integers mod $(q^d-1)/(q-1)$. Furthermore, we will prove in Section III that l-th column sequence is cyclically equivalent to lq-th column sequence where lq is computed mod $(q^d-1)/(q-1)$. This implies that we have to classify the column indices from 0 to $(q^d-1)/(q-1)-1$ into q-cyclotomic cosets mod $(q^d-1)/(q-1)$.

We observe that $\gcd(q, q^d-1) = 1 = \gcd(q, (q^d-1)/(q-1))$ for the following definition:

Definition 3:
1) *A q-cyclotomic coset C_l containing l mod q^d-1 is the set of all the integers $l, lq, lq^2, \ldots$, mod q^d-1. If we denote by d_l the size of C_l, then*

$$C_l = \{l, lq, \ldots, lq^{d_l-1}\}.$$

2) *A q-cyclotomic coset $\hat{C}_l$ containing l mod $\frac{q^d-1}{q-1}$ is the set of all the integers $l, lq, lq^2, \ldots$, mod $\frac{q^d-1}{q-1}$. If we denote by m_l the size of $\hat{C}_l$, then*

$$\hat{C}_l = \{l, lq, \ldots, lq^{m_l-1}\}. \quad (3)$$

3) *We denote by Λ the set of the smallest representatives of all the q-cyclotomic cosets $\hat{C}_l$'s mod $(q^d-1)/(q-1)$ except for $l = 0$. We denote by Λ_S the subset of Λ such that $l \in \Lambda_S$ if and only if $m_l = d_l$. We denote by Λ' the subset of Λ such that $l \in \Lambda'$ if and only if $m_l = d$.* □

For any $1 \le l < q^d - 1$, since d_l is the smallest positive integer such that $l \equiv lq^{d_l} \bmod q^d - 1$, we have that $d_l | d$. [28], [30]. For any $1 \le l < (q^d-1)/(q-1)$ similarly, since m_l is the smallest positive integer such that $l \equiv lq^{m_l} \bmod (q^d-1)/(q-1)$, we have that $m_l | d$. Furthermore, since $l \equiv lq^{d_l} \pmod{q^d-1}$ implies $l \equiv lq^{d_l} \bmod (q^d-1)/(q-1)$, from the definition of m_l, we see that $m_l | d_l$. Therefore, we must have $m_l | d_l | d$ for any $1 \le l < (q^d-1)/(q-1)$. This proves the following:

Lemma 1: With the definition above, for any prime power q and a positive integer d, we have

$$\Lambda' \subseteq \Lambda_S \subseteq \Lambda, \quad (4)$$

where we note that

(a) *$\Lambda' = \Lambda_S$ if and only if $m_l = d$ is true for $1 \le l < (q^d-1)/(q-1)$ with $m_l = d_l$,*

(b) *$\Lambda_S = \Lambda$ if and only if $m_l = d_l$ for all $1 \le l < (q^d-1)/(q-1)$ and*

(c) *$\Lambda' = \Lambda$ if and only if $\Lambda' = \Lambda_S = \Lambda$ if and only if $m_l = d$ for all $1 \le l < (q^d-1)/(q-1)$.*

When γ is a primitive element of $GF(q^d)$, the coset C_1 mod $q^d - 1$ contains j if and only if γ^j is a q-conjugate element of γ in $GF(q^d)$, and hence, the monic polynomial $\prod_{j\in C_1}(x - \gamma^j)$ is the minimal polynomial over $GF(q)$ of γ. It is well-known [28], [30] that $d_1 = m_1 = d$.

Example 1: Following four difference cases are worked out for examples.

Case-1 $\Lambda' = \Lambda_S = \Lambda$: Let $q = 5$ and $d = 3$. The integers mod $124/4 = 31$ is partitioned into only 1 coset $\{0\}$ of size 1 and 10 cosets of size 3. The result is shown in CASE 1 of Table I. Note that $d = 3$ is a prime and that $\gcd(q-1, d) = 1$ in this case. Except for $l = 0$, we have $m_l = d_l = d$ for all l in this case.

Case-2 $\Lambda' = \Lambda_S \neq \Lambda$: Let $q = 7$ and $d = 2$. The integers mod $48/6 = 8$ is partitioned into 5 cosets of size 2 and 1 as shown in CASE 2 of Table I. Therefore, $\Lambda' = \Lambda_S = \{1, 2, 3\} \subsetneq \Lambda = \{1, 2, 3, 4\}$. Except for $l = 0$ and those l with $m_l = d$, we have

TABLE I

FOUR CASES OF EXAMPLE 1

	m_l	d_l	d	l	comments
CASE 1	1	1	3	0	always, but excluded from Λ
	3	3	3	$1, 2, 3, 4, 6, 8, 11, 12, 16, 17$	$\in \Lambda' = \Lambda_S = \Lambda$
CASE 2	1	1	2	0	
	1	2	2	4	$\notin \Lambda_S$ and hence $\notin \Lambda'$
	2	2	2	$1, 2, 3$	$\in \Lambda' = \Lambda_S$
CASE 3	1	1	4	0	
	2	2	4	$65, 130, 195, 260$	$\notin \Lambda'$ but $\in \Lambda_S$
	4	4	4	144 values of l including 1	$\in \Lambda' \cap \Lambda_S$
CASE 4	1	1	4	0	
	1	2	4	78	
	1	4	4	$39, 117$	
	2	2	4	$26, 52, 91$	$\in \Lambda_S$ but $\notin \Lambda'$
	2	4	4	13	$\notin \Lambda_S$ and hence $\notin \Lambda'$
	4	4	4	36 values of l including 1	$\in \Lambda_S \cap \Lambda'$

$m_l < d_l$ for all other l in this case. Note also that $d = 2$ is a prime but $\gcd(q-1, d) \neq 1$.

Case-3 $\Lambda' \neq \Lambda_S = \Lambda$*: Let $q = 8$ and $d = 4$ so that $q^d - 1 = 4095$ and $(q^d - 1)/(q - 1) = 585$. The integers mod 585 is partitioned into 149 cosets of size 4, 2 and 1 as shown in CASE 3 of Table I. Therefore, we have $|\Lambda'| = 144$, and $|\Lambda_S| = |\Lambda| = 148$. Note that* $\gcd(q-1, d) = 1$ *in this case. Except for $l = 0$ and those l with $m_l = d$, we have $m_l = d_l < d$ for all other l in this case. Note also that $d = 4$ is not a prime but* $\gcd(q-1, d) = 1$.

Case-4 $\Lambda' \neq \Lambda_S \neq \Lambda$*: Let $q = 5$ and $d = 4$ so that $q^d - 1 = 624$ and $(q^d - 1)/(q - 1) = 156$. The integers mod 156 is partitioned into 44 cosets of size 4, 2, and 1 as shown in CASE 4 of Table I. Therefore, we have $|\Lambda'| = 36$, $|\Lambda_S| = 36 + 3 = 39$, and $|\Lambda| = 43$. In this case, neither d is prime nor* $\gcd(q-1, d) = 1$ *is true.* □

We now prove that the comment at the end of each case of the above example describes a sufficient condition.

Lemma 2: Assume all the same notations so far.

1) $\Lambda' = \Lambda_S$ *if d is a prime.*
2) $\Lambda_S = \Lambda$ *if* $\gcd(q-1, d) = 1$.

Proof:

1) Note that $\Lambda' = \Lambda_S$ if and only if $m_l = d$ is true for $1 \le l < (q^d - 1)/(q - 1)$ with $m_l = d_l$ if and only if $m_l = d$ is true for $1 \le l < (q^d - 1)/(q - 1)$ with $lq^{m_l} \equiv l \bmod q^d - 1$. Assume $lq^{m_l} \equiv l \bmod q^d - 1$ for some $1 \le l < (q^d - 1)/(q - 1)$. Then, $(q^d - 1) | l(q^{m_l} - 1)$, or $(q^d - 1)/(q^{m_l} - 1) | l$ since $m_l | d$. Note here that $m_l = 1$ implies $(q^d - 1)/(q - 1) | l$ which is impossible. Thus $m_l > 1$. Now, if d is prime, $m_l > 1$ and $m_l | d$, then $m_l = d$.
2) See Remark 3. ■

III. MAIN RESULT

We will first give a representation of a Sidelnikov sequence of period $q^d - 1$ in terms of log to the base $\beta \in GF(q)$. We will then discuss some properties of the column sequences in the $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$ array of these sequences in the subsection A. Main constructions of the sequence family will follow in the subsections B and C. We count the family size asymptotically in general (Appendix) and exactly for some simple cases in the subsection D.

A. Properties of Column Sequences of the Array of Sidelnikov Sequences of Period $q^d - 1$

Theorem 2: Let $\{s(t)\}$ be an M-ary Sidenikov sequence of period $q^d - 1$, with $M | q - 1$. Then, for $0 \le t \le q^d - 2$,

$$s(t) \equiv \log_\beta(N(\alpha^t + 1)) \mod M. \tag{5}$$

Proof: By definition, $s(t) \equiv y(t) \mod M$ for all t, where

$$y(t) = \log_\alpha(\alpha^t + 1).$$

When $\alpha^t + 1 = 0$, we have $\log_\beta(N(0)) = \log_\beta 0 = 0$ and this agrees with the definition of $s(t)$. Now, we may assume that $\alpha^t + 1 \neq 0$ and hence $N(\alpha^t + 1) \neq 0$. Then, with $N(\alpha^t + 1) = \beta^{x(t)}$,

$$\begin{aligned} \frac{q^d - 1}{q - 1} y(t) &\equiv \log_\alpha (\alpha^t + 1)^{\frac{q^d-1}{q-1}} \\ &\equiv \log_\alpha N(\alpha^t + 1) \\ &\equiv \log_\alpha \alpha^{\frac{q^d-1}{q-1} x(t)} \\ &\equiv \frac{q^d - 1}{q - 1} x(t) \mod q^d - 1. \end{aligned}$$

This implies that

$$x(t) \equiv y(t) \mod q - 1,$$

and hence that, as $M|q-1$,

$$x(t) \equiv y(t) \mod M.$$

Therefore,

$$s(t) \equiv y(t) \equiv x(t) \equiv \log_\beta N(\alpha^t + 1) \mod M.$$

■

We write a Sidelnikov sequence $\{s(t)\}$ of period $q^d - 1$ as an array of size $(q-1) \times \frac{q^d-1}{q-1}$ and denote by $\{v_l(t)\}$ its l-th column sequence for each $0 \le l < (q^d-1)/(q-1)$. Then, the l-th column sequence $\{v_l(t)\}$ is given by, for $0 \le t < q-1$,

$$v_l(t) = s\left(\frac{q^d-1}{q-1}t + l\right) \equiv \log_\beta N(\alpha^l \beta^t + 1) \mod M. \quad (6)$$

We now summarize some properties of the column sequences $\{v_l(t)\}$ of length $q-1$ for $0 \le l < (q^d-1)/(q-1)$ as follows:

Theorem 3: Let $\{s(t)\}$ *be a Sidelnikov sequence of period* $q^d - 1$ *given by* (5) *and its column sequences* $\{v_l(t)\}$ *for* $0 \le l < (q^d-1)/(q-1)$ *are given by* (6).

1) *The very first column sequence* $\{v_0(t)\}$ *is a* d*-multiple of the Sidelnikov sequence* $\{s_1(t)\}$ *of period* $q-1$ *defined by the primitive element* $\beta = \alpha^{(q^d-1)/(q-1)}$ *of* $GF(q)$*. That is, for all* t,

$$v_0(t) \equiv d \log_\beta(\beta^t + 1) \mod M. \quad (7)$$

2) *For any* $1 \le l < (q^d-1)/(q-1)$, $\{v_{lq}(t)\}$ *is a cyclic shift of* $\{v_l(t)\}$*, where the subscript* lq *is computed mod* $(q^d-1)/(q-1)$*. In particular,* $v_l(t) = v_{lq}(t+\tau)$ *for all* t*, where* τ *is the quotient when* lq *is divided by* $(q^d-1)/(q-1)$.

3) *Denote by* δ *the quotient when* lq^{m_l} *is divided by* $(q^d-1)/(q-1)$*. For any* $1 \le l < (q^d-1)/(q-1)$*, the column sequence* $\{v_l(t)\}$ *has a subperiod less than* $q-1$ *if and only if* $q-1$ *does not divide* δ *if and only if* $m_l < d_l$*. Write* $\delta = (q-1)a + r$ *where* $0 \le r < q-1$*. If* $r \ne 0$ *then the subperiod of* $\{v_l(t)\}$ *is given by* $\gcd(r, q-1) = \gcd(\delta, q-1)$.

Proof:

1) Observe that

$$\begin{aligned} v_0(t) &= s\left(\frac{q^d-1}{q-1}t\right) \\ &\equiv \log_\beta N(\beta^t + 1) \\ &\equiv \log_\beta(\beta^t+1)^{\frac{q^d-1}{q-1}} \\ &\equiv \frac{q^d-1}{q-1}\log_\beta(\beta^t+1) \\ &\equiv d\log_\beta(\beta^t+1) \mod M, \end{aligned}$$

where the last congruence holds since $(q^d-1)/(q-1) \equiv d \mod M$.

2) Since lq in $v_{lq}(t)$ is computed mod $\frac{q^d-1}{q-1}$ but the exponent l of α in the RHS of (6) is computed mod q^d-1, the term lq here should be carefully treated. For this, we divide lq by $\frac{q^d-1}{q-1}$ and put

$$lq = \frac{q^d-1}{q-1}\tau + \mu,$$

where $0 \le \mu < \frac{q^d-1}{q-1}$. Then $lq \equiv \mu \pmod{\frac{q^d-1}{q-1}}$ and $\tau = \frac{lq-\mu}{(q^d-1)/(q-1)}$, and the following comes easily:

$$\begin{aligned} v_{lq}(t) \equiv v_\mu(t) &\equiv \log_\beta N(\alpha^\mu \beta^t + 1) \\ &\equiv \log_\beta N(\alpha^{lq-(\frac{q^d-1}{q-1})\tau}\beta^t + 1) \\ &\equiv \log_\beta N(\alpha^{lq}\beta^{t-\tau} + 1) \\ &\equiv \log_\beta N((\alpha^{lq}\beta^{t-\tau} + 1)^{q^{d-1}}) \\ &\equiv \log_\beta N(\alpha^{l}\beta^{t-\tau} + 1) \\ &\equiv v_l(t-\tau) \mod M. \end{aligned}$$

In other words, we have $v_l(t) = v_{lq}(t+\tau)$ for all t.

3) Since $lq^{m_l} \equiv l \mod \frac{q^d-1}{q-1}$ we write

$$lq^{m_l} = \frac{q^d-1}{q-1}\delta + l, \quad (8)$$

where $1 \le l < \frac{q^d-1}{q-1}$. Then

$$\begin{aligned} \delta &= l\frac{q^{m_l}-1}{(q^d-1)/(q-1)} \\ &= l\frac{(q-1)(q^{m_l-1} + q^{m_l-2} + \cdots + 1)}{(q^d-1)/(q-1)}. \end{aligned} \quad (9)$$

Using the same argument as in the proof of the previous item, we see that $v_l(t) = v_{lq^{m_l}}(t+\delta)$ for all t. However, it is also true that $v_{lq^{m_l}}(t) = v_l(t)$ and hence that

$$v_l(t) = v_l(t+\delta) \quad \text{for all } t. \quad (10)$$

Write $\delta = (q-1)a + r$ for some $0 \le r < q-1$. If $r \ne 0$, then $\{v_l(t)\}$ must have a subperiod $\gcd(r, q-1)$ which is strictly less than $q-1$. If $r = 0$, then from (8) we have

$$lq^{m_l} \equiv l \mod (q^d-1),$$

which implies $d_l | m_l$, and hence $m_l = d_l$. It is easy to see that we must have $r = 0$ if $m_l = d_l$. Therefore, $r \ne 0$ if and only if $m_l < d_l$.

Finally, assume that $\{v_l(t)\}$ has a subperiod k where $1 \le k < q-1$ and $k|q-1$. Since $\{v_l(t)\}$ satisfies (10) where δ is given by (8) or (9), it has the subperiod $\gcd(\delta, q-1) = k$. We write again $\delta = (q-1)a + r$ for some $0 \le r < q-1$. Now, if $r = 0$ then $k = \gcd(\delta, q-1) = q-1$ is a desired contradiction. Therefore, we have proved that $\{v_l(t)\}$ has a subperiod less than $q-1$ if and only if $q-1$ does not divide δ given in (9). ■

Two important corollaries of the third item of the above theorem are the following:

Corollary 1: Assume all the same notations as in Theorem 3.

1) *If* $\gcd(d, q-1) = 1$*, then, for all* $1 \le l < (q^d-1)/(q-1)$*, the* l*-th column sequence* $\{v_l(t)\}$ *has no subperiod less than* $q-1$*. Note that this is true regardless of whether* $m_l = d_l = d$ *or* $m_l = d_l < d$.

2) *If* $m_l = d$ *for* $1 \le l < (q^d-1)/(q-1)$*, then the* l*-th column sequence* $\{v_l(t)\}$ *has no subperiod less than* $q-1$*. Note that this is true regardless of whether* $\gcd(d, q-1) = 1$ *or not.*

$$\begin{aligned} s(t) &= [v_0(t), v_1(t), v_2(t), ..., v_{30}(t)] \\ &= \left[\begin{array}{ccccccccccccccccccccccccccccccc} 1&3&1&0&2&3&1&1&1&0&1&3&3&2&2&0&0&1&3&3&2&0&0&3&2&3&1&3&0&0&1 \\ 2&2&3&1&1&2&1&0&0&1&3&2&2&0&0&1&1&1&1&1&1&3&1&0&3&2&1&2&1&3&1 \\ 0&0&3&2&0&0&2&0&2&0&3&2&3&0&1&2&3&3&0&3&0&2&1&1&2&0&2&2&3&2&2 \\ 3&3&3&0&0&3&2&2&0&2&3&2&0&1&0&0&1&0&1&3&0&3&3&1&2&3&2&2&1&3&2 \end{array}\right] \end{aligned}$$

Fig. 1. Array structure of the sidelnikov sequence in Example 2.

Proof:

1) Assume that $\gcd(d, q-1) = 1$. From the second item of Lemma 2 we have $m_l = d_l$ for all $1 \le l < (q^d - 1)/(q-1)$. Therefore, $\{v_l(t)\}$ has no subperiod less than $q-1$ by the third item of Theorem 3.
2) We observe that $m_l = d$ implies $m_l = d_l = d$ and we are done by the third item of Theorem 3. ■

Example 2: Let $q = 5$ and $d = 3$. Consider $GF(5^3)$ constructed by the primitive element α defined by $\alpha^3 = 2\alpha + 3$ over $GF(5)$. Then, $\beta = \alpha^{31} = 3$ is a primitive element of $GF(5)$. A 4-ary Sidelnikov sequence of period $5^3 - 1 = 124$ can be put into an array of size 4×31 as given in Fig. 1. *Here, $\Lambda' = \Lambda_S = \Lambda = \{1, 2, 3, 4, 6, 8, 11, 12, 16, 17\}$, and the 5-cyclotomic cosets mod $\frac{q^d-1}{q-1} = 31$ are $\{0\}$ and 10 cosets of size all 3.*

If we let $\{s_1(t)\}$ be the 4-ary Sidelnikov sequence of period 4 using $\beta = 3$, then $\{s_1(t)\}$ has the value $3, 2, 0, 1$ for $t = 0, 1, 2, 3$, and observe that $v_0(t) \equiv 3s_1(t)$ mod 4 for all t.

Since $\hat{C_1} = \{1, 5, 25\}$, we have $v_1(t) = v_5(t) = v_{25}(t)$. Similarly, we have $v_2(t) = v_{10}(t) = v_{19}(t+1)$, etc. Observe that $\gcd(d, q-1) = \gcd(3, 4) = 1$ *as well as $m_l = d = 3$ for all $l \neq 0$, and hence every $\{v_l(t)\}$, for $l = 1, 2, \ldots, 30$, does not have subperiod less than $q - 1 = 4$.* □

Example 3: Assume that $q = 7$ and $d = 4$ so that $\gcd(d, q-1) = (4, 6) = 2$. *We consider two types of q-cyclotomic cosets mod $(q^d - 1)/(q-1) = 400$ of size $2 < d$. When $l = 25$, we have $\hat{C_{25}} = \{25, 175\}$ and $C_{25} = \{25, 175, 1225, 1375\}$, and hence $m_l = 2 < d_l = 4$. Therefore, $\{v_{25}(t)\}$ has a subperiod 3. When $l = 50$, we have $\hat{C_{50}} = \{50, 350\} = C_{50}$, and hence $m_l = d_l = 2$. Therefore, $\{v_{50}(t)\}$ has no subperiod. Note that for any l with $m_l = 4$ (and hence $m_l = d_l$), the column sequence $\{v_l(t)\}$ has no subperiod. We further verify the following: $25 \cdot 7^2 = 1225 = 400 \cdot 3 + 25$ and $\delta = 3$ which is not a multiple of 6. On the other hand, $50 \cdot 7^2 = 2450 = 400 \cdot 6 + 50$ and $\delta = 6$ which is a multiple of 6.* □

The l-th column sequence $v_l(t)$ given in (6) can be written as follows:

$$v_l(t) \equiv \log_\beta f_l(\beta^t) \mod M,$$

where, for each l,

$$\begin{aligned} f_l(x) &\overset{\triangle}{=} N(\alpha^l x + 1) \\ &= \beta^l N(x + \alpha^{-l}) \\ &= \beta^l (x + \alpha^{-l})(x + \alpha^{-lq}) \cdots (x + \alpha^{-lq^{d-1}}) \\ &= \beta^l p_l(x)^{d/d_l}, \qquad (11) \end{aligned}$$

where $p_l(x)$ is the minimal polynomial over $GF(q)$ of $-\alpha^{-l}$ of degree d_l. Note here that $d_l | d$ and d_l is the smallest positive integer such that $q^{d_l} l \equiv l \mod q^d - 1$. From (6) and (11), we have

$$\begin{aligned} v_l(t) &\equiv \log_\beta f_l(\beta^t) \\ &\equiv \log_\beta \beta^l p_l(\beta^t)^{d/d_l} \mod M \qquad (12) \\ &\equiv \log_\beta (\beta^{\hat{l}} p_l(\beta^t))^{d/d_l} \mod M, \quad \text{for some } \hat{l}, \\ &\equiv \frac{d}{d_l} \log_\beta (\beta^{\hat{l}} p_l(\beta^t)) \mod M, \qquad (13) \end{aligned}$$

which is possible because of the following:

Lemma 3: Let β, d, d_l and l be as given in (12). *Then, there exists an integer $\hat{l}$ such that $\beta^l = \beta^{\hat{l} d/d_l}$.*

Proof: The statement is equivalent to the following: there exists an $\hat{l}$ such that $l \equiv \hat{l} d/d_l \mod q-1$, or the linear congruence equation $\frac{d}{d_l} x \equiv l \mod q-1$ has a solution x, or $\gcd(\frac{d}{d_l}, q-1)$ divides l. For this, observe first that $lq^{d_l} \equiv l \mod q^d - 1$ implies $q^d - 1$ divides $l(q^{d_l} - 1)$ and hence

$$\frac{q^d - 1}{q^{d_l} - 1} | l, \qquad (14)$$

since $d_l | d$.

We note that, since $(q^d - 1)/(q-1) \equiv d \mod q-1$,

$$\gcd(q-1, \frac{q^d-1}{q-1}) = \gcd(q-1, d). \qquad (15)$$

Next, use q^{d_l} for q and $\frac{d}{d_l}$ for d in (15) to obtain the following:

$$\begin{aligned} &\gcd(q^{d_l} - 1, (q^d - 1)/(q^{d_l} - 1)) \\ &\quad = \gcd(q^{d_l} - 1, ((q^{d_l})^{\frac{d}{d_l}} - 1)/(q^{d_l} - 1)) \\ &\quad = \gcd(q^{d_l} - 1, \frac{d}{d_l}). \qquad (16) \end{aligned}$$

Therefore, we are done by the following: $\gcd(q-1, \frac{d}{d_l})$ divides $\gcd(q^{d_l}-1, \frac{d}{d_l})$, which divides $\gcd(q^{d_l}-1, (q^d-1)/(q^{d_l}-1))$ by (16), which divides $\gcd(q^{d_l}-1, l)$ by (14), which obviously divides l. ■

Note that the above lemma is true regardless of whether $\gcd(d, q-1) = 1$ or not, and also regardless of whether $m_l = d$ or not. In particular, if $m_l = d$, then $m_l = d_l = d$ and $\hat{l} = l$ works. One final preparation for the main construction is to observe the following:

Lemma 4: Let l, k be elements in Λ and τ ($0 \le \tau < q-1$) be an integer. Let $p_l(x)$ be the minimal polynomials over

$GF(q)$ of $-\alpha^{-l}$ of degree d_l in (11)*, and similarly for $p_k(x)$. We consider the following monic polynomial:*

$$\beta^{-\tau d_k} p_k(\beta^\tau x) \\ = (x+\alpha^{-k}\beta^{-\tau})(x+\alpha^{-kq}\beta^{-\tau})\cdots(x+\alpha^{-kq^{d_k-1}}\beta^{-\tau}).$$

If l and k satisfy $m_l = d_l$ and $m_k = d_k$ (i.e., $l, k \in \Lambda_S$), then $p_l(x)$ and $\beta^{-\tau d_k}p_k(\beta^\tau x)$ are distinct monic irreducible polynomials over $GF(q)$, unless $l = k$ and $\tau = 0$.

Proof: Assume that they are the same. Then, we have $\alpha^{-l} = \alpha^{-kq^s}\beta^{-\tau}$ for some $s < d_k = m_k$. This implies

$$l \equiv kq^s + \tau\frac{q^d-1}{q-1} \mod q^d - 1. \tag{17}$$

Therefore, we have $l \equiv kq^s \mod \frac{q^d-1}{q-1}$, and this implies that l and k belong to the same q-coset mod $\frac{q^d-1}{q-1}$. Therefore, $l = k$, and we have

$$l \equiv lq^s \mod \frac{q^d-1}{q-1}.$$

By the definition of m_l, the above implies $m_l|s$, which in turn implies that $s = 0$ since $s < d_k = m_k = m_l$. Then, (17) becomes $\tau\frac{q^d-1}{q-1} \equiv 0 \mod q^d - 1$ which gives $q-1|\tau$ and thus $\tau = 0$ since we have assumed that $0 \le \tau < q-1$. ■

We note that the same conclusion of the above lemma is true when $l, k \in \Lambda'$ since in this case $m_l = d = m_k$ implies $m_l = d_l = d = d_k = m_k$.

B. Main Construction: Column Sequences and Their Constant Multiples

We will clearly distinguish two M-ary Sidelnikov sequences from now on: $\{s(t)\}$ of period $q-1$ and $\{s_d(t)\}$ of period q^d-1. For some reason to be explained later, we have to put some upper limit on d from now on, which is given by the following:

$$3 \le d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1) \tag{18}$$

We would like to emphasis again the contrapositive as well as the inversion of the third item of Theorem 3: for $1 \le l < (q^d-1)/(q-1)$, the l-th column sequence $\{v_l(t)\}$ has a full period $q-1$ if and only if $m_l = d_l$ if and only if $q-1$ divides δ in (9). This will play a key role in our main construction of the family. Recall also that Λ_S is a subset of Λ containing those l with $m_l = d_l$.

Definition 4: Assume that d is in the range given by (18) *and $q > 27$. We write an M-ary Sidelnikov sequence $\{s_d(t)\}$ of period q^d-1 as a $(q-1)\times\frac{q^d-1}{q-1}$ array, where $s_d(t)$ is given in* (5) *with α and $\beta = \alpha^{\frac{q^d-1}{q-1}}$, and denote by $\{v_l(t)\}$ its l-th column sequence for each $l = 1, 2, \ldots, (q^d-1)/(q-1)-1$. We denote by $\{s(t)\}$ the M-ary Sidelnikov sequence of period $q-1$ given by $s(t) \equiv \log_\beta(\beta^t+1)$ mod M for $0 \le t < q-1$.*

1) *We now construct a family Σ' of M-ary sequences of period $q-1$ using Λ' as follows:*

$$\Sigma' = \{cv_l(t) |\ 1 \le c < M,\ l \in \Lambda'\}. \tag{19}$$

2) *In paricular, for an integer $r \ge 2$ dividing* $\gcd(d, M)$*, we consider the following subset $\Sigma'_{r,c}$ of Σ':*

$$\Sigma'_{r,c} = \bigcup_{i=0}^{r-1}\left\{\left(c+\frac{iM}{r}\right)v_l(t)\ \middle|\ l \in \Lambda'\right\}, \tag{20}$$

where c is a fixed integer with $1 \le c \le \frac{M}{r}-1$. Using $c = \frac{M}{r}$ in this case, we also construct

$$\Sigma'_{M/r} = \bigcup_{i=1}^{r-1}\left\{\frac{iM}{r}v_l(t)\ \middle|\ l \in \Lambda'\right\}. \tag{21}$$

3) *When* $\gcd(d, M) = 1$*, using Λ_S (instead of Λ') we construct a family Σ_S as follows:*

$$\Sigma_S = \{cv_l(t) |\ 1 \le c < M,\ l \in \Lambda_S\}. \tag{22}$$

Theorem 4 (Properties of Families in Definition 4):

1) *The sequences in the family Σ' are cyclically inequivalent, and*

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

2) *All the members of $\Sigma'_{r,c}$ for $1 \le c \le \frac{M}{r}-1$ are cyclically distinct and*

$$C_{max}(\Sigma'_{r,c}) \le (2d-2)\sqrt{q}+2.$$

The same is true for the family $\Sigma'_{r,M/r}$ using $c = M/r$.

3) *All the members of Σ_S are cyclically distinct, and*

$$C_{max}(\Sigma_S) \le (2d-1)\sqrt{q}+1.$$

Proof:

1) Assume that $l \ne k$ and τ is in the range $0 \le \tau < q-1$. We recall that hence $m_l = d_l = d = m_k = d_k$. Let $1 \le c_1, c_2 < M$ be any two arbitrary constants. The crosscorrelation function between the sequences $\{c_1v_l(t)\}$ and $\{c_2v_k(t)\}$ in Σ' is given by

$$C_{c_1v_l,c_2v_k}(\tau) = \sum_{t=0}^{q-2}\omega_M^{c_1v_l(t)-c_2v_k(t+\tau)}. \tag{23}$$

Here, from (12),

$$\omega_M^{c_1v_l(t)} = \omega_M^{c_1\log_\beta\beta^l p_l(\beta^t)} = \psi^{c_1}(\beta^l p_l(\beta^t))$$

and similarly,

$$\omega_M^{-c_2v_k(t+\tau)} = \psi^{M-c_2}(\beta^k p_k(\beta^{t+\tau})).$$

Therefore, (23) becomes

$$C_{c_1v_l,c_2v_k}(\tau) \\ = \sum_{t=0}^{q-2}\psi^{c_1}(\beta^l p_l(\beta^t))\psi^{M-c_2}(\beta^{k+\tau d}\beta^{-\tau d}p_k(\beta^\tau\beta^t)) \\ = \sum_{x\in GF(q)^*}\psi_1(\beta^l p_l(x))\psi_2(\beta^{k+\tau d}\beta^{-\tau d}p_k(\beta^\tau x)), \tag{24}$$

where $\psi_1 = \psi^{c_1}$ and $\psi_2 = \psi^{M-c_2}$ are both non-trivial since both exponents c_1 and $M-c_2$ belong to the range from 1 to $M-1$. Furthermore, Lemma 4 proves that

$p_l(x)$ and $\beta^{-\tau d} p_k(\beta^\tau x)$ are distinct monic irreducible polynomials over $GF(q)$ unless $l = k$ and $\tau = 0$.

Now, assume that $l \neq k$ or $1 \le \tau < q-2$ and apply the Weil bound (1) in Theorem 1 with $e_1 = e_2 = 0$:

$$\begin{aligned}
&|C_{c_1 v_l, c_2 v_k}(\tau)| \\
&\quad = \left| \sum_{x \in GF(q)^*} \psi_1(\beta^l p_l(x)) \psi_2(\beta^{k+\tau d - \tau d} p_k(\beta^\tau x)) \right| \\
&\quad \le \left| \sum_{x \in GF(q)} \psi_1(\beta^l p_l(x)) \psi_2(\beta^{k+\tau d - \tau d} p_k(\beta^\tau x)) \right| + 1 \qquad (25) \\
&\quad \le (2d-1)\sqrt{q} + 1. \qquad (26)
\end{aligned}$$

Consider now the case that $c_1 \neq c_2$, but $l = k$ and $\tau = 0$. Then

$$C_{c_1 v_l, c_2 v_l}(\tau = 0) = \sum_{x \in GF(q)^*} \psi_3(\beta^l p_l(x)),$$

where $\psi_3 = \psi^{c_1 - c_2}$ is nontrivial, since $1 \le |c_1 - c_2| \le M - 1$. So, by the Weil bound (1) again,

$$|C_{c_1 v_l, c_2 v_l}(\tau = 0)| \le (d-1)\sqrt{q} + 1.$$

This completes the proof of the correlation upper bound on the family Σ'.

To show that the members in Σ' are all cyclically distinct, we proceed as follows. If $c_1 v_l(t)$ and $c_2 v_k(t)$ for $(c_1, l) \neq (c_2, k)$ are cyclically equivalent, then, for some τ $(0 \le \tau \le q-2)$, $c_1 v_l(t) = c_2 v_k(t+\tau)$ for all t. Then we have

$$\begin{aligned}
q - 1 &= \sum_{t=0}^{q-2} \omega_M^{c_1 v_l(t) - c_2 v_k(t+\tau)} \\
&= \left| C_{c_1 v_1, c_2 v_2}(\tau) \right| \le (2d-1)\sqrt{q} + 1, \qquad (27)
\end{aligned}$$

which is impossible because of the assumption $d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$.

2) Since $\Sigma'_{r,c}$ is a subset of Σ', it is obvious that its members are cyclically distinct by the above proof. For the correlation bound, we use the same process as in the above until the expression for $|C_{c_1 v_l, c_2 v_k}(\tau)|$ in (25), where $c_1 = c + iM/r$ and $c_2 = c + jM/r$ for some $0 \le i, j \le r-1$ and $1 \le c \le M/r - 1$.
Now, since $c_1 \equiv c_2 \bmod M/r$ and $r \,|\, \gcd(d, M)$, we have $M | d(c_1 - c_2)$. Therefore, since $m_l = d_l = d = d_1$ and $m_k = d_k = d = d_2$, we have

$$\prod_{i=1}^{2} \psi_i^{d_i}(x) = \psi^{d(c_1 - c_2)}(x) = 1$$

for all $x \in GF(q)^*$. Therefore, we apply the Weil Bound in (2), and obtain the improved upper bound as

$$\begin{aligned}
&|C_{c_1 v_l, c_2 v_k}(\tau)| \\
&\quad \le \left| \sum_{x \in GF(q)} \psi_1(\beta^l p_l(x)) \psi_2(\beta^{k+\tau d} \beta^{-\tau d} p_k(\beta^\tau x)) \right| + 1 \\
&\quad \le (2d-2)\sqrt{q} + 2.
\end{aligned}$$

Note that for $\Sigma'_{M/r}$, we have $c_1 = iM/r$ and $c_2 = jM/r$ for some $0 \le i, j \le r-1$. Therefore, the improved upper bound also applies.

3) Basically, the proof is almost the same as the above item 1), except for the steps from (23) to (24). New expression for (24) here would be

$$\begin{aligned}
C_{c_1 v_l, c_2 v_k}(\tau) = \sum_{x \in GF(q)^*} \Big[&\psi^{cd/d_l}(\beta^{\hat{l}} p_l(x)) \\
&\cdot \psi^{(M-c_2)d/d_k}(\beta^{\hat{k} + \tau d_k} \beta^{-\tau d_k} p_k(\beta^\tau x)) \Big],
\end{aligned}$$

for some $\hat{l}$ and $\hat{k}$ by Lemma 3. In this case, since $1 \le c_1, c_2 < M$, ψ^{cd/d_l} and $\psi^{(M-c_2)d/d_k}$ are non-trivial because of the condition $\gcd(d, M) = 1$, the remaining steps in the proof of 1) work. ■

Remark 1: When d is prime, Lemma 2 *implies $\Lambda' = \Lambda_S$. Therefore, we have $\Sigma' = \Sigma_S$ regardless of* $\gcd(d, M) = 1$ *or not. When d is not prime, Σ_S will possibly be slightly larger in size than Σ', and the difference is almost trivial. See* Example 6 *at the end of* Subsection III-D. $\Sigma'_{r,c}$ *or* $\Sigma'_{M/r}$ *can be constructed when* $\gcd(d, M) > 1$ *and it must be definitely smaller in size than Σ' but it has tighter bound on its maximum correlation magnitudes. Analysis on the sizes of various families will be given in* Subsection III-D. □

C. Main Construction: Combining With Previously Constructed Families

We follow [44] and now construct various families by combining those in Definition 4 and the families $\mathcal{I}_S$ in [21] and $\mathcal{A}_S$ in [23] and [14], where

$$\mathcal{I}_S = \{cs(t) |\ 1 \le c < M\} \qquad (28)$$

$$\mathcal{A}_S = \{c_0 s(t) + c_1 s(t+\delta) |\ 1 \le \delta \le \lfloor (q-1)/2 \rfloor\}, \qquad (29)$$

where $1 \le c_0, c_1 < M$ for $1 \le \delta \le \lfloor (q-1)/2 \rfloor$, and $c_0 < c_1$ if $\delta = \frac{q-1}{2}$ for odd prime power q. It has already been proved that the members of $\mathcal{I}_S \cup \mathcal{A}_S$ are cyclically distinct and

$$C_{max}(\mathcal{I}_S \cup \mathcal{A}_S) \le 3\sqrt{q} + 5 \qquad (30)$$

as [23, Th. 4] (which is mentioned in [44, Proof of Th. 9]). We will also use the following subset $\mathcal{A}_{S0}$ of $\mathcal{A}_S$:

$$\mathcal{A}_{S0} = \{c_0 s(t) + c_1 s(t+\delta) |\ 1 \le \delta \le \lfloor (q-1)/2 \rfloor\}, \qquad (31)$$

where $c_0 + c_1 \equiv 0 \bmod M$. It has also been proved that the members of $\mathcal{I}_S \cup \mathcal{A}_{S0}$ are cyclically distinct and

$$C_{max}(\mathcal{I}_S \cup \mathcal{A}_{S0}) \le 2\sqrt{q} + 6 \qquad (32)$$

as [14, Th. 18] (which is also mentioned in [44, Proof of Th. 9]).

In the following, we note that the definition of the family $\mathcal{I}_S$, $\mathcal{A}_S$ or $\mathcal{A}_{S0}$ has nothing to do with the value of d.

Definition 5: Assume all the same notation as in Definition 4, *and $\mathcal{I}_S$ and $\mathcal{A}_S$ in* (28) *and* (29), *respectively.*

1) *Using Σ', we construct a family Σ'^{ext} of M-ary sequences of period $q-1$ as*

$$\Sigma'^{ext} = \Sigma' \cup \mathcal{I}_S \cup \mathcal{A}_S. \qquad (33)$$

2) *Using* $\Sigma'_{M/r}$ *for* $r \geq 2$ *when* $r \mid \gcd(d, M)$, *we construct a family* $\Sigma'^{ext}_{M/r}$ *of* M*-ary sequences of period* $q-1$ *as*

$$\Sigma'^{ext}_{M/r} = \Sigma'_{M/r} \cup \mathcal{I}_S \cup \mathcal{A}_{S0}. \tag{34}$$

3) *Using* Σ_S *when* $\gcd(d, M) = 1$, *we construct a family* Σ_S^{ext} *of* M*-ary sequences of period* $q-1$ *as*

$$\Sigma_S^{ext} = \Sigma_S \cup \mathcal{I}_S \cup \mathcal{A}_S. \tag{35}$$

Theorem 5 (Properties of Extended Families in Definition 5): Assume all the notation and assumptions in Definition 5.

1) *The sequences in the family* Σ'^{ext} *are cyclically distinct, and*

$$C_{max}(\Sigma'^{ext}) \leq (2d-1)\sqrt{q} + 1.$$

2) *The sequences in the family* $\Sigma'^{ext}_{M/r}$ *are cyclically distinct, and*

$$C_{max}(\Sigma'^{ext}_{M/r}) \leq (2d-2)\sqrt{q} + 2.$$

3) *The sequences in the family* Σ_S^{ext} *are cyclically distinct, and*

$$C_{max}(\Sigma_S^{ext}) \leq (2d-1)\sqrt{q} + 1.$$

Proof:

1) We have already proved that

$$C_{max}(\Sigma') \leq (2d-1)\sqrt{q} + 1$$

in Theorem 4 above. Recall (30) for $C_{max}(\mathcal{I}_S \cup \mathcal{A}_S)$. Therefore, we only have to prove the correlation bound of $\{a(t)\}$ and $\{b(t)\}$ where $\{a(t)\} \in \mathcal{I}_S, \{b(t)\} \in \Sigma'$ and $\{a(t)\} \in \mathcal{A}_S, \{b(t)\} \in \Sigma'$ for the upper bound on $C_{max}(\Sigma'^{ext})$.

Case 1 $\{a(t)\} \in \mathcal{I}_S$, $\{b(t)\} \in \Sigma'$: Let $a(t) = c_1 s(t)$, $b(t) = c_2 \upsilon_l(t)$. Then the correlation between $\{a(t)\}$ and $\{b(t)\}$ is

$$\begin{aligned} C_{a,b}(\tau) &= \sum_{t=0}^{q-2} \omega_M^{c_1 s(t+\tau) - c_2 \upsilon_l(t)} \\ &= \sum_{t=0}^{q-2} \omega_M^{c_1 \log_\beta(\beta^{t+\tau}+1) - c_2 \log_\beta f_l(\beta^t)} \\ &= \sum_{x \in GF(q)^*} \omega_M^{c_1 \log_\beta(\beta^\tau x+1) - c_2 \log_\beta \beta^l p_l(x)}, \end{aligned}$$

where $f_l(x) = \beta^l p_l(x)$ for the irreducible polynomial $p_l(x)$ since $m_l = d_l = d$. Then, we can express the above correlation as a character sum and apply the Weil bound (1). Therefore,

$$\begin{aligned} &|C_{a,b}(\tau)| \\ &\quad = \left| \sum_{x \in GF(q)} \psi^{c_1}(\beta^\tau x + 1)\psi^{M-c_2}(\beta^l p_l(x)) - 1 \right| \\ &\quad \leq (d_l + 1 - 1)\sqrt{q} + 2 \\ &\quad \leq d\sqrt{q} + 2. \end{aligned}$$

Case 2 $\{a(t)\} \in \mathcal{A}_S$, $\{b(t)\} \in \Sigma'$: Let $a(t) = c_0 s(t) + c_1 s(t+\delta)$, $b(t) = c_2 \upsilon_l(t)$. Then the correlation between $\{a(t)\}$ and $\{b(t)\}$ is

$$\begin{aligned} &C_{a,b}(\tau) \\ &\quad = \sum_{t=0}^{q-2} \omega_M^{c_0 s(t+\tau) + c_1 s(t+\delta+\tau) - c_2 \upsilon_l(t)} \\ &\quad = \sum_{x \in GF(q)^*} \omega_M^{c_0 \log_\beta(\beta^\tau x+1) + c_1 \log_\beta(\beta^{\tau+\delta} x+1) - c_2 \log_\beta \beta^l p_l(x)}, \end{aligned}$$

and we can also apply the same method as **Case 1**. Hence,

$$C_{a,b}(\tau) \leq (d+1)\sqrt{q} + 3.$$

Cyclic inequivalence of members of Σ' has been proved in Theorem 4. Those for $\mathcal{I}_S$ or $\mathcal{A}_S$ have been done earlier by others. We only have to check the cyclic inequivalence between members of $\mathcal{I}_S$ and Σ', and also those in $\mathcal{A}_S$ and Σ'. These can be done easily by some similar methods used in the proof of Theorem 4.

2) We have already proved that

$$C_{max}(\Sigma'_{M/r}) \leq (2d-2)\sqrt{q} + 2$$

in Theorem 4 above. Recall (32) for $C_{max}(\mathcal{I}_S \cup \mathcal{A}_{S0})$. Therefore, we only have to prove the correlation bound of $\{a(t)\}$ and $\{b(t)\}$ where $\{a(t)\} \in \mathcal{I}_S, \{b(t)\} \in \Sigma'_{M/r}$ and $\{a(t)\} \in \mathcal{A}_{S0}, \{b(t)\} \in \Sigma'_{M/r}$ for the upper bound on $C_{max}(\Sigma'^{ext}_{M/r})$. Since $\Sigma'_{M/r}$ is a subset of Σ' and $\mathcal{A}_{S0}$ is a subset of $\mathcal{A}_S$, the same steps as in the proof of 1) apply and we have

$$|C_{a,b}(\tau)| \leq d\sqrt{q} + 2$$

for Case 1 and

$$|C_{a,b}(\tau)| \leq d\sqrt{q} + 4$$

for Case 2. Cyclic inequivalence of members of $\Sigma'^{ext}_{M/r}$ can be proved similarly.

3) This can be done similarly. ■

D. Counting the Size of the Proposed Families

We recall that we consider the value of d in the range given by (18) and hence $q > 27$. Also, Λ' is the set of representatives of the q-cyclotomic cosets mod $(q^d-1)/(q-1)$ of l with $m_l = d$, and Λ_S is the set of representatives of the q-cyclotomic cosets mod $(q^d-1)/(q-1)$ of l with $m_l = d_l$. From Definition 4, we see that

$$\begin{aligned} |\Sigma'| &= (M-1)|\Lambda'| \\ |\Sigma'_{r,c}| &= r|\Lambda'| \\ |\Sigma'_{M/r}| &= (r-1)|\Lambda'| \\ |\Sigma_S| &= (M-1)|\Lambda_S|, \end{aligned}$$

where $r \mid \gcd(d, M)$ and $r \geq 2$.

Recall that $\Delta = 1$ when q is odd and $\Delta = 2$ when q is even. For the families $\mathcal{I}_S$, $\mathcal{A}_S$ and $\mathcal{A}_{S0}$, it is easy to see that

$$\begin{aligned} |\mathcal{I}_S| &= M-1, \\ |\mathcal{A}_S| &= (M-1)\left(\frac{(M-1)(q-2)+\Delta-2}{2}\right), \end{aligned}$$

and

$$|\mathcal{A}_{S0}| = \begin{cases} \frac{1}{2}((M-1)(q-2)-1), & q \text{ odd and } M \text{ even} \\ \frac{1}{2}(M-1)(q-2), & \text{otherwise.} \end{cases}$$

Therefore, we have the following:

$$|\Sigma'^{ext}| = (M-1)|\Lambda'| + \frac{1}{2}((M-1)^2(q-2)+\Delta)$$
$$|\Sigma^{ext}_{S}| = (M-1)|\Lambda_S| + \frac{1}{2}((M-1)^2(q-2)+\Delta)$$
$$|\Sigma'^{ext}_{M/r}| = (M-1)+(r-1)|\Lambda'| + |\mathcal{A}_{S0}|$$

Asymptotic counting in the appendix gives $|\Lambda| \sim |\Lambda_S| \sim |\Lambda'| \sim q^{d-1}/d$ as q increases for $d > 3$. (Cor. 2 in Appendix) This proves the following:

Theorem 6: For $d > 3$ and as $q \to \infty$, we have

$$|\Sigma'^{ext}| \sim |\Sigma^{ext}_{S}| \sim (M-1)q^{d-1}/d,$$

and

$$|\Sigma'^{ext}_{M/r}| \sim (r-1)q^{d-1}/d.$$

We do not have explicit expressions for $|\Lambda|$ or $|\Lambda'|$ or $|\Lambda_S|$ in general, except for some special values of d. In this subsection, we give an exact counting of $|\Lambda|$ and $|\Lambda'|$ (and hence the size of the family Σ'^{ext}) when d is a prime power or d is a product of two distinct primes. These will cover, in particular, the values of d from 2 to 11 and we believe this would be practically enough for selecting the right value of d for any given q and M, We will use the same notation as all the previous subsections. We would like to recall that, from Lemmas 1 and 2, $|\Lambda'| = |\Lambda_S|$ if d is prime and $|\Lambda_S| = |\Lambda|$ if $\gcd(q-1, d) = 1$.

Theorem 7: When d is a prime, we have

$$|\Lambda| = |\Lambda'| + k - 1 = \frac{1}{d}\left(\frac{q^d-1}{q-1} - k\right) + k - 1,$$

where $k = \gcd(q-1, d)$ is either 1 or d. Therefore, with $\Delta = 1$ when q is odd and $\Delta = 2$ when q is even, we have

$$|\Sigma'^{ext}| = (M-1)\left(\frac{1}{d}\left(\frac{q^d-1}{q-1} - k\right) + \frac{(M-1)(L-1)+\Delta}{2}\right).$$

Proof: Note that every coset $\hat{C}_s$ in this case has size either 1 or d. Observe that s in the integers mod $\frac{q^d-1}{q-1}$ belongs to a singleton coset $\hat{C}_s = \{s\}$ if and only if $sq \equiv s \bmod \frac{q^d-1}{q-1}$. Now,

$$sq \equiv s \mod \frac{q^d-1}{q-1} \iff s(q-1) \equiv 0 \mod \frac{q^d-1}{q-1}$$
$$\iff s \equiv 0 \mod \frac{q^d-1}{q-1}/k,$$

where $k = \gcd(q-1, d)$.

Therefore, s belongs to a singleton coset if and only if it is of the form $i\ \frac{q^d-1}{q-1}/k$ for $0 \le i < k$. Hence, the number of singleton cosets is k including the coset $\{0\}$. All the other cosets have size d, and the number of such cosets is $\frac{1}{d}(\frac{q^d-1}{q-1} - k)$. Since $0 \notin \Lambda$, we have the desired result. ■

Example 4: When $d = 3$, we have $|\Lambda| = |\Lambda'| + k - 1 = \frac{q^2+q+1-k}{3} + k - 1$, where $k = \gcd(q-1, 3)$ is either 1 or 3. □

Theorem 8: Let $d = r^a$ for a prime r and a positive integer a. Then,

$$|\Lambda| = \sum_{i=1}^{a-1} \frac{\gcd(q^{r^i}-1, \frac{q^d-1}{q-1}) - \gcd(q^{r^{i-1}}-1, \frac{q^d-1}{q-1})}{r^i}$$
$$+ \gcd(d, q-1) - 1 + |\Lambda'|,$$

and

$$|\Lambda'| = \frac{1}{d}\left(\frac{q^d-1}{q-1} - \gcd\left(q^{d/r}-1, \frac{q^d-1}{q-1}\right)\right).$$

Therefore, with $\Delta = 1$ when q is odd and $\Delta = 2$ when q is even, we have

$$|\Sigma'^{ext}| = (M-1)\left(\frac{1}{d}\left(\frac{q^d-1}{q-1} - \gcd\left(q^{d/r}-1, \frac{q^d-1}{q-1}\right)\right)\right.$$
$$\left. + \frac{(M-1)(L-1)+\Delta}{2}\right).$$

Proof: Note that in this case the coset size is r^i for some $0 \le i \le k$. We may similarly count the number of singleton cosets, which is given by $\gcd(d, q-1)$. Now, we count the number of cosets of size r^i for each $1 \le i \le k$ as follows.

For any s in the integers mod $\frac{q^d-1}{q-1}$, we have $sq^d \equiv s \bmod \frac{q^d-1}{q-1}$. Observe that s belongs to a coset of size r^i if and only if $sq^{r^i} \equiv s$ but $sq^{r^{i-1}} \not\equiv s \bmod \frac{q^d-1}{q-1}$.

The number of elements s such that $sq^{r^i} \equiv s \bmod \frac{q^d-1}{q-1}$ is easily counted to be $\gcd(q^{r^i}-1, \frac{q^d-1}{q-1})$. Of these, the number of those with $sq^{r^{i-1}} \equiv s \bmod \frac{q^d-1}{q-1}$ is given by $\gcd(q^{r^{i-1}}-1, \frac{q^d-1}{q-1})$. ■

Example 5: When $d = 4$, we have

$$|\Lambda'| = \frac{q^3+q^2+q+1-j}{4},$$

where $j = \gcd(q^2-1, q^3+q^2+q+1)$, and

$$|\Lambda| = |\Lambda'| + \frac{j-k}{2} + k - 1,$$

where $k = \gcd(q-1, 4)$. □

Theorem 9: Let $d = uv$ be a product of two distinct primes u and v. Then we have

$$|\Lambda| = \left|\Lambda'\right| + \gcd(q-1, d) - 1$$
$$+ \frac{1}{u}\left(\frac{q^u-1}{q-1}\gcd(q-1, v) - \gcd(q-1, d)\right)$$
$$+ \frac{1}{v}\left(\frac{q^v-1}{q-1}\gcd(q-1, u) - \gcd(q-1, d)\right),$$

and

$$d\left|\Lambda'\right| = \frac{q^d-1}{q-1} + \gcd(q-1, d)$$
$$- \frac{q^u-1}{q-1}\gcd(q-1, v) - \frac{q^v-1}{q-1}\gcd(q-1, u).$$

Therefore, with $\Delta = 1$ *when* q *is odd and* $\Delta = 2$ *when* q *is even, we have*

$$\begin{aligned}|\Sigma'^{ext}| = \frac{M-1}{d}\Bigg(&\frac{q^d-1}{q-1} + \gcd(q-1,d)\\ &- \frac{q^u-1}{q-1}\gcd(q-1,v)\\ &- \frac{q^v-1}{q-1}\gcd(q-1,u)\Bigg)\\ &+ (M-1)\frac{(M-1)(L-1)+\Delta}{2}.\end{aligned}$$

Proof: Note in this case that the size of a coset must be either 1, u, v, or $uv = d$. Let $T = \frac{q^d-1}{q-1}$. We first observe that, for any s in the integers mod T, s belongs to a coset of size 1 if and only if $sq \equiv s \mod T$. Therefore, we have $s(q-1) \equiv 0 \mod T$, or $s \equiv 0 \mod \frac{T}{\gcd(q-1,T)}$. The integer s which satisfies $sq \equiv s \mod T$ has the following form:

$$s = \frac{T}{\gcd(q-1,T)}\, i, \quad 1 \le i < \gcd(q-1,T).$$

Therefore, the number of cosets of size 1 is given by $\gcd(q-1,T) - 1 = \gcd(q-1,d) - 1$. [see (15)].

Similarly, note that s belongs to a coset of size u if and only if $sq^u \equiv s \mod T$ and $sq \not\equiv s \mod T$. Since $sq^u \equiv s \mod T$ if and only if $s \equiv 0 \mod \frac{T}{\gcd(q^u-1,T)}$, the integer s which satisfies $sq^u \equiv s \mod T$ has the following form:

$$s = \frac{T}{\gcd(q^u-1,T)}\, i \quad 1 \le i < \gcd(q^u-1,T).$$

Therefore, the number of cosets of size u is given by the following:

$$\frac{1}{u}\Bigg(\gcd(q^u-1,T) - \gcd(q-1,d)\Bigg).$$

Observe that

$$\begin{aligned}T &= \frac{q^{uv}-1}{q-1}\\ &= \frac{((q^u-1+1)^v-1)}{q^u-1}\frac{q^u-1}{q-1}\\ &= \left(\sum_{i=1}^{v}\binom{v}{i}(q^u-1)^{i-1}\right)\frac{q^u-1}{q-1}\\ &= \left(v + \sum_{i=2}^{v}\binom{v}{i}(q^u-1)^{i-1}\right)\frac{q^u-1}{q-1}\\ &\equiv v\frac{q^u-1}{q-1} \mod q^u-1.\end{aligned}$$

Thus,

$$\begin{aligned}\gcd(T,q^u-1) &= \gcd\left(v\frac{q^u-1}{q-1}, q^u-1\right)\\ &= \gcd\left(v\frac{q^u-1}{q-1}, (q-1)\frac{q^u-1}{q-1}\right)\\ &= \frac{q^u-1}{q-1}\gcd(v,q-1).\end{aligned}$$

Similarly, we have

$$\gcd(T,q^v-1) = \frac{q^v-1}{q-1}\gcd(u,q-1).$$

Therefore, the number of cosets of size u becomes

$$\frac{1}{u}\left(\frac{q^u-1}{q-1}\gcd(q-1,v) - \gcd(q-1,d)\right),$$

and that of size v is given by

$$\frac{1}{v}\left(\frac{q^v-1}{q-1}\gcd(q-1,u) - \gcd(q-1,d)\right).$$

Therefore, the number $|\Lambda'|$ of cosets in Λ of size uv is given by the following:

$$\begin{aligned}|\Lambda'| = \frac{1}{uv}\Bigg(&T + \gcd(q-1,d) - \frac{q^u-1}{q-1}\gcd(q-1,v)\\ &- \frac{q^v-1}{q-1}\gcd(q-1,u)\Bigg),\end{aligned}$$

and $|\Lambda|$ is given as desired. ■

Remark 2: The size of Λ *in* Theorems 8 *and* 9 *becomes the same as that of* Λ_S *when* $\gcd(q-1,d) = 1$. *We further note that* $\gcd(d,M) = 1$ *if* $\gcd(q-1,d) = 1$. □

Example 6: Table II shows the sizes of various families for $q = 64$ ($M = 7$ *or* 63), $q = 97$ ($M = 2$ *or* 96), *and* $d = 3$ *or* $d = 4$, *and the correlation bounds given in Theorem 5. Followings are to be noted from this table:*

1) *Correlation magnitude of the families are from* Theorem 5.
2) *The construction for* Σ' *(and hence* Σ'^{ext}*) is applicable for any* $q > 27$, $M|(q-1)$ *and* d *satisfying* (18).
3) *The construction for* Σ_S *(and hence* Σ_S^{ext}*) will only be applicable whenever* $\gcd(d,M) = 1$. *There are four such cases in this table. The size of* Σ_S *is the same as that of* Σ' *if d is a prime* ($d = 3$ *in this table), and it is negligibly a bit larger otherwise.*
4) *The construction for* $\Sigma'_{M/r}$ *(and hence* $\Sigma'^{ext}_{M/r}$ *also) will be applicable for any* $r|\gcd(d,M)$ *and* $r \ge 2$. *If* $\gcd(d,M) = 1$ *then it will not be applicable. The size of* $\Sigma'^{ext}_{M/r}$ *is much smaller than that of* Σ'^{ext}, *but it has much tighter bound on the correlation magnitude.*
5) *This table clearly shows that one can have a trade-off between the size and the maximum correlation magnitude for given* q *and* M *by carefully selecting the value of* d. □

E. Practical Issues of Constructing Λ' *or* Λ_S

For the constructions of Σ'^{ext}, or its subset $\Sigma'^{ext}_{M/r}$, or Σ_S^{ext}, one has to first construct Λ_S or its subset Λ', both of which are subsets of Λ. This could be challenging since basically one has to take the following steps:

1) Determine Λ by finding all the q-cyclotomic cosets $\hat{C}_l$ containing l mod $(q^d-1)/(q-1)$ for $1 \le l \le (q^d-1)/(q-1)-1$.
2) Determine Λ_S and Λ' by finding the values d_l and m_l for all $l \in \Lambda$.

It is to be noted that only the first step above will require memory of size approximately $\frac{q^{d-1}}{d} \times \left\lceil \log_2 \frac{q^d-1}{q-1}\right\rceil$ bits (Cor. 2),

TABLE II
THE SIZES AND CORRELATION BOUNDS OF THE PROPOSED FAMILIES FOR $q = 64$ AND $q = 97$ WITH $d = 3$ AND 4 (EXAMPLE 6)

q	64				97			
M	7		63		2		96	
d	3	4	3	4	3	4	3	4
$\gcd(d, q-1)$	3	1	3	1	3	4	3	4
$\gcd(d, M)$	1	1	3	1	1	2	3	4
$\|\Lambda\|$	1388	66592	1388	66592	3170	230595	3170	230595
$\|\Lambda_S\|$	1386	66592	1386	66592	3168	230544	3168	230544
$\|\Lambda'\|$	1386	66560	1386	66560	3168	230496	3168	230496
q^{d-1}/d	1365	65536	1365	65536	3136	228168	3136	228168
$\|\Sigma_S\|$	8316	399552	-	4128704	3168	-	-	-
$\|\Sigma'\|$	8316	399360	85932	4126720	3168	230496	300960	21897120
$\|\Sigma'_{r,c}\|$	-	-	4158 ($r = 3$)	-	-	460992 ($r = 2$)	9504 ($r = 3$)	921984 ($r = 4$)
$\|\Sigma'_{M/r}\|$	-	-	2772 ($r = 3$)	-	-	230496 ($r = 2$)	6336 ($r = 3$)	691488 ($r = 4$)
$\|\mathcal{I}_S\|$	6	6	62	62	1	1	95	95
$\|\mathcal{A}_S\|$	1116	1116	119164	119164	47	47	428640	428640
$\|\mathcal{A}_{S0}\|$	-	-	1922 ($r = 3$)	-	-	47 ($r = 2$)	4512 ($r = 3$)	4512 ($r = 4$)
$\|\Sigma'^{ext}\|$	9438	400482	205158	4245946	3216	230544	729695	22325855
$\|\Sigma'_{M/r}\|$	-	-	4756 ($r = 3$)	-	-	230544 ($r = 2$)	10943 ($r = 3$)	696095 ($r = 4$)
$\|\Sigma_S^{ext}\|$	9438	400482	-	4245946	3216	-	-	-
$C_{max}(\Sigma'^{ext})$ $= C_{max}(\Sigma_S^{ext})$	41.00	57.00	41.00	57.00	50.24	69.94	50.24	69.94
$C_{max}(\Sigma'^{ext}_{M/r})$	34.00	50.00	34.00	50.00	41.40	61.09	41.40	61.09

which may be a big issue in engineering sense for large $q = L + 1$ and $d \geq 3$. Computational time-complexity may also be a bigger issue. For the first step of the above, one has to go through all the q-cyclotomic cosets of l mod $(q^d - 1)/(q - 1)$ from $l = 1$ to $l = (q^d - 1)/(q - 1) - 1$ checking whether it is new or not in order to determine Λ. Basically, this brute force algorithm may require approximate time-complexity which is at least linear in $((q^d - 1)/(q - 1))^2$.

However, one can do much better when d is prime and $\gcd(q - 1, d) = 1$, and furthermore, when $(q^d - 1)/(q - 1)$ is also prime. For $d = 3$, such cases occur when $q = 41$, 59, 71, or 89, etc. Note that, for each of these four values of q and $d = 3$, the value $(q^d - 1)/(q - 1)$ becomes 1723, 3541, 5113, or 8011, respectively, all of which are prime. It would be an interesting problem if one could determine whether there are infinitely many such cases for each prime d.

Let d be prime and $\gcd(q - 1, d) = 1$. Then $\Lambda' = \Lambda_S = \Lambda$ (Lemma 2), or $m_l = d_l = d$ for any $l \in \Lambda$. If $Q \triangleq (q^d - 1)/(q - 1)$ is prime in addition, then $|\Lambda| = (Q - 1)/d$, which we prove in the following by construction:

Theorem 10: Let d and $Q = (q^d - 1)/(q - 1)$ both be prime and $\gcd(q - 1, d) = 1$. *Then*

$$\Lambda' = \Lambda_S = \Lambda = \{s^i \mod Q \mid 0 \leq i \leq (Q - 1)/d - 1\},$$

where s is a primitive root mod Q.

Proof: It is enough to show that

$$\hat{C}_1 = \{q^i | 0 \leq i \leq d - 1\} = \{s^{i\frac{Q-1}{d}} | 0 \leq i \leq d - 1\} \triangleq T_1.$$

As Q is prime, the multiplicative group of integers mod Q is a cyclic group of order $Q - 1$. So, for each positive divisor e of $Q - 1$, it has one and only one subgroup of order e. As both $\hat{C}_1$ and T_1 are subgroups of order d, they must be the same. ■

Note that, in the cases of the above theorem, the require memory size would be approximately $\lceil \log_2 \frac{q^d-1}{q-1} \rceil$ bits since there is no need to save all distinct cosets, and the time-complexity reduces to approximately linear in $\frac{q^{d-1}}{d}$ plus some extra time for finding a primitive root s mod Q. There are some "good" algorithms [4] for finding a primitive root modulo a prime.

In all other cases in general, what we could do is to give some test of determining the values of m_l and d_l for $1 \leq l < (q^d - 1)/(q - 1)$ without going through checking the cosets mod $q^d - 1$.

Theorem 11: Let l be any integer with $1 \leq l < (q^d - 1)/(q - 1)$. Then

1) *d_l is the least positive integer such that $d_l | d$ and*

$$\left. \frac{q^d - 1}{q^{d_l} - 1} \right| l.$$

2) *m_l is the least positive integer such that $m_l | d$ and*

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

Proof: From the definitions of d_l and m_l, it is enough to observe that

$$\begin{aligned} lq^{d_l} \equiv l \mod q^d-1 \;&\Leftrightarrow\; (q^d-1)|l(q^{d_l}-1) \\ &\Leftrightarrow\; \frac{q^d-1}{q^{d_l}-1}\Bigg| l, \end{aligned}$$

and

$$\begin{aligned} &lq^{m_l} \equiv l \mod (q^d-1)/(q-1) \\ &\quad\Leftrightarrow\; (q^d-1)/(q-1)|l(q^{m_l}-1) \\ &\quad\Leftrightarrow\; \frac{(q^d-1)/(q-1)}{\gcd((q^d-1)/(q-1), q^{m_l}-1)}\Bigg| l. \end{aligned}$$

Observe that

$$\begin{aligned} &\frac{(q^d-1)/(q-1)}{\gcd((q^d-1)/(q-1), q^{m_l}-1)} \\ &\quad= \frac{q^d-1}{\gcd((q^d-1), (q^{m_l}-1)(q-1))} \\ &\quad= \frac{q^d-1}{(q^{m_l}-1)\gcd(\frac{q^d-1}{q^{m_l}-1}, q-1)} \\ &\quad= \frac{q^d-1}{(q^{m_l}-1)\gcd(\frac{d}{m_l}, q-1)}, \end{aligned}$$

where we use the fact that the remainder when $\frac{q^d-1}{q^{m_l}-1}$ is divided by $q-1$ is $\frac{d}{m_l}$. ■

Example 7: Let $q = 53$ and $d = 4$. Then, $(q^4-1)/(q-1) = 151740$ and for $1 \le l \le 151739$, we have

$$d_l = \begin{cases} 2 & \text{if} \quad 2810 \mid l \\ 4 & \text{otherwise,} \end{cases}$$

and

$$m_l = \begin{cases} 1 & \text{if} \quad 37935 \mid l \\ 2 & \text{if} \quad 1405 \mid l \text{ and } 37935 \nmid l \\ 4 & \text{otherwise.} \end{cases}$$

Remark 3: If $\gcd(d, q-1) = 1$ then we have $\gcd(\frac{d}{m_l}, q-1) = 1$ for any divisor m_l of d. Therefore, two sufficient conditions coincide, and $m_l = d_l$ for any such l, and hence, $\Lambda_S = \Lambda$, which is the second item of Lemma 2. □

IV. Conclusion

In this paper, we investigate the $(q-1) \times \frac{q^d-1}{q-1}$ array structure of M-ary Sidelnikov sequences of period q^d-1, and propose two constructions Σ'^{ext} and Σ_S^{ext} for families of M-ary sequences of period $q-1$ with: (1) the correlation magnitudes which are upper bounded by $(2d-1)\sqrt{q}+1$ for $d \ge 3$ and (2) the sizes are given approximately by $(M-1)q^{d-1}/d$. Two constructions of this paper depend on whether $\gcd(d, M) = 1$ or not. We furthermore give the exact count of them when d is a prime power or a product of two distinct primes.

We note that Σ'^{ext} is applicable for all prime powers $q > 27$ and $3 \le d < \frac{1}{2}(\sqrt{q}-2/\sqrt{q}+1)$, and so is Σ_S^{ext} with an extra condition that $\gcd(d, M) = 1$ with a minor increase in the family size compared with Σ'^{ext}.

We are able to find some subset $\Sigma'^{ext}_{M/r}$ of Σ'^{ext} for $r \ge 2$ and $r | \gcd(d, M)$, which has a tighter upper bound on its correlation magnitude: $(2d-2)\sqrt{q}+2$. However its size is much smaller than that of Σ'^{ext}.

It is shown by construction that Λ' can be constructed with reasonable size of memory and time for practical applications when both d and $(q^d-1)/(q-1)$ are prime and $\gcd(q-1, d) = 1$.

Table III shows some of the well-known non-binary sequence families, and their period L, alphabet size M, the upper bound on their correlation magnitude, and the family size.

Appendix
Asymptotic Counting That $|\Lambda| \sim |\Lambda_S| \sim |\Lambda'| \sim \frac{q^{d-1}}{d}$

We will use the same notation as before in this appendix.

Proposition 1: The number of monic irreducible factors of $x^{\frac{q^d-1}{q-1}}-1$ over $GF(q)$ is equal to $|\Lambda|+1$.

Proof: Let $\gamma = \alpha^{q-1}$ be a primitive $\frac{q^d-1}{q-1}$-th root of unity in $GF(q^d)$. Then, with

$$M^{(l)}(x) = \prod_{j \in \hat{C}_l} (x-\gamma^j)$$

denoting the minimal polynomial of γ^l over $GF(q)$ where $\hat{C}_l$ is the q-cyclotomic coset mod $\frac{q^d-1}{q-1}$ containing l described in (3), we have

$$x^{\frac{q^d-1}{q-1}}-1 = \prod_{l \in \Lambda \cup \{0\}} M^{(l)}(x).$$

This proves the proposition. ■

Theorem 12 [45]: For each positive integer f, let

$$A_f = \{r \;:\; r | q^f-1 \text{ but } r \nmid q^i-1 \text{ for } 1 \le i < f\}.$$

For $r \in A_f$, write $r = d_{rf} m_{rf}$, with $d_{rf} = \gcd(r, \frac{q^f-1}{q-1})$. Assume $b \in GF(q)^*$ has order m, and let $\mathcal{N}(f, b, q)$ denote the number of monic irreducible polynomials over $GF(q)$ of degree f with constant term $(-1)^f b$. Then

$$\mathcal{N}(f, b, q) = \frac{1}{f\phi(m)} \sum_{\substack{r \in A_f \\ m_{rf}=m}} \phi(r),$$

where $\phi(m)$ is the Euler totient function and counts the number of integers from 1 to m which are relatively prime to m.

Lemma 5: Let $p(x) = x^e + \cdots + (-1)^e b$ be a monic irreducible factor over $GF(q)$ of $x^{\frac{q^d-1}{q-1}}-1$. Then $e|d$, and $b^{d/e} = 1$.

Proof: Clearly, $e|d$. For a root γ of $p(x)$ in $GF(q^d)$, $N(\gamma) = 1$, and $((-1)^e b)^{d/e} = (-1)^d b^{d/e}$ is the constant term of $p(x)^{d/e} = x^d + \cdots + (-1)^d N(\gamma)$. ■

TABLE III

COMPARISON OF WELL KNOWN POLYPHASE SEQUENCE FAMILIES (p IS AN ODD PRIME)

		Period L	Alphabet size	$C_{\max}$	Family size
Chu	[2]	any odd integer L	L	$\sqrt{L}$	$\geq$ (smallest prime factor of L) -1
Trachtenberg	[39]	$p^m - 1$, m odd	p	$\sqrt{p(L+1)} + 1$	$L + 2$
Helleseth	[15]	$p^m - 1$, m even	p	$2\sqrt{L+1} + 1$	$L + 2$
			extra condition: $p^{m/2} \not\equiv 2 \mod 3$		
Kumar, Moreno	[25]	$p^m - 1$	p	$\sqrt{L+1} + 1$	$L + 1$
Gong	[12]	$(p^m - 1)^2$	p	$2\sqrt{L} + 3$	$\sqrt{L}$
Kumar, Helleseth	$S(2)$ [24]	$2^m - 1$	4	$4\sqrt{L+1} + 1$	$\geq L^3 + 4L^2 + 5L + 2$
Kim, No, Chung	S [20]	$\frac{p^m-1}{2}$	$p \equiv 3 \mod 4$	$2\sqrt{L + \frac{1}{2}}$	$4L$
Kim, Chae, Song	$\widetilde{S}$ [19]	$\frac{p^m-1}{e}$	p	$2\sqrt{eL+1}$	$e^2 L$
Kim, Song	[21]	$p^m - 1$	$M \mid p^m - 1$	$\sqrt{L+1} + 3$	$M - 1$
Han, Yang	$\widetilde{\mathcal{F}}_s$ [14]	$p^m - 1$	$M \mid p^m - 1$	$2\sqrt{L+1} + 6$	$(M-1)\frac{L}{2} + \lfloor \frac{M-1}{2} \rfloor$
Kim, No, Chung	$\mathcal{L}$ [23]	$p^m - 1$	$M \mid p^m - 1$	$3\sqrt{L+1} + 5$	$(M-1)^2 \lfloor \frac{L-2}{2} \rfloor + \frac{(M-1)(M-2)}{2}$
Yu, Gong	$\mathcal{H}_s^{(2)}$ [43]	$p^m - 1$	$M \mid p^m - 1$	$5\sqrt{L+1} + 7$	$\approx \frac{(L-2)(L-4)}{8}(M-1)^3$
Yu, Gong	$\mathcal{U}$ [44]	$p^m - 1$	$M \mid p^m - 1$	$3\sqrt{L+1} + 5$	$\frac{M(M-1)}{2}(L-1) + (M-1)$
Yu, Gong	$\tilde{\mathcal{U}}$ (a subset of $\mathcal{U}$) [44]	$p^m - 1$	$M \mid p^m - 1$	$2\sqrt{L+1} + 6$	$\frac{M}{2}(L+1) - 1$
In this paper	Σ'^{ext} and Σ_S^{ext}	$p^m - 1$	$M \mid p^m - 1$	$(2d-1)\sqrt{L+1} + 1$	$\approx (M-1)\frac{(L+1)^{d-1}}{d}$
			extra condition: $p^m > 27$ and $3 \leq d < (\sqrt{p^m} - 2/\sqrt{p^m} + 1)/2$ for both, $\gcd(d, M) = 1$ for Σ_S^{ext} in addition to the above		
In this paper	$\Sigma'^{ext}_{M/r}$ (a subset of Σ'^{ext})	$p^m - 1$	$M \mid p^m - 1$	$(2d-2)\sqrt{L+1} + 2$	$\approx (r-1)\frac{(L+1)^{d-1}}{d}$
			extra condition: $p^m > 27$ and $3 \leq d < (\sqrt{p^m} - 2/\sqrt{p^m} + 1)/2$ and $r \mid \gcd(d, M)$ and $r \geq 2$		

Theorem 13: The number $|\Lambda| + 1$ of monic irreducible factors of $x^{\frac{q^d-1}{q-1}} - 1$ is given by

$$\sum_{e|d} \frac{1}{e} \sum_{m \mid \gcd(\frac{d}{e}, q-1)} \sum_{\substack{r \in A_e \\ m_{re} = m}} \phi(r).$$

Proof: In view of Lemma 5, that number is equal to $\sum_{e|d} \sum_{b^{d/e}=1} \lambda(b, e)$ where $\lambda(b, e)$ is the number of monic irreducible factors over $GF(q)$ of $x^{\frac{q^d-1}{q-1}} - 1$, with degree e and the constant term equal to $(-1)^e b$. This is equal to

$$\sum_{e|d} \sum_{m \mid \gcd(\frac{d}{e}, q-1)} \sum_{\substack{b \\ o(b)=m}} \lambda'(b, e)$$

where $\lambda'(b, e)$ is the number of monic irreducible polynomials over $GF(q)$ with degree e and the constant term equal to $(-1)^e b$, and $o(b)$ denotes the order of b. Hence,

$$|\Lambda| + 1 = \sum_{e|d} \sum_{m \mid \gcd(\frac{d}{e}, q-1)} \sum_{\substack{b \\ o(b)=m}} \mathcal{N}(e, b, q).$$

The desired result now follows from Theorem 12. ■

The next theorem follows from [40] by taking $f(T) = T$. It gives an estimate for $\mathcal{N}(f, b, q)$.

Theorem 14 [40]: Let $\mathcal{N}(f, b, q)$ denote the number of monic irreducible polynomials over $GF(q)$ of degree f with constant term $(-1)^f b$, for some element $b \in GF(q)^*$. Then

$$\left|\mathcal{N}(f, b, q) - \frac{q^f}{f(q-1)}\right| \le \frac{2}{f}\sqrt{q^f}.$$

Corollary 2: Let $d > 3$. The asymptotic sizes of Λ, Λ_S, and Λ', as $q \to \infty$, are given by:

$$|\Lambda| \sim |\Lambda_S| \sim |\Lambda'| \sim \frac{q^{d-1}}{d}.$$

Proof: Assume that $d > 3$. From Theorem 14,

$$\left| |\Lambda| + 1 - \sum_{e|d} \frac{\gcd(\frac{d}{e}, q-1)q^e}{e(q-1)} \right| \le 2 \sum_{e|d} \frac{\gcd(\frac{d}{e}, q-1)q^{e/2}}{e}.$$

This implies that

$$|\Lambda| \sim \frac{q^{d-1}}{d} \quad \text{as} \quad q \to \infty.$$

Observe that $|\Lambda'| = \mathcal{N}(d, 1, q)$, and hence that

$$\left| |\Lambda'| - \frac{q^d}{d(q-1)} \right| \le \frac{2}{d} q^{d/2},$$

again from Theorem 14. This yields that

$$|\Lambda'| \sim \frac{q^{d-1}}{d} \quad \text{as} \quad q \to \infty.$$

Finally, as $|\Lambda'| \le |\Lambda_S| \le |\Lambda|$, we also have

$$|\Lambda_S| \sim \frac{q^{d-1}}{d} \quad \text{as} \quad q \to \infty.$$

ACKNOWLEDGEMENT

The authors wish to thank both the anonymous referees and the associate editor for the careful reviewing of the initially submitted version of this paper and for various suggestions and comments in order to improve the quality of this paper.

REFERENCES

[1] M. Anand and P. V. Kumar, "Low-correlation sequences over the QAM constellation," *IEEE Trans. Inf. Theory*, vol. 54, no. 2, pp. 791–810, Feb. 2008.

[2] D. Chu, "Polyphase codes with good periodic correlation properties (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 18, no. 4, pp. 531–532, Jul. 1972.

[3] W. Chu, S. W. Golomb, and H.-Y. Song, "Tuscan squares," in *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., 2nd ed. Boca Raton, FL, USA: Taylor & Francis, 2007.

[4] J. Dubrois and J. G. Dumas, "Efficient polynomial time algorithms computing industrial-strength primitive roots," *Inf. Process. Lett.*, vol. 97, no. 2, pp. 41–45, 2006.

[5] Y.-C. Eun, S.-Y. Jin, Y.-P. Hong, and H.-Y. Song, "Frequency hopping sequences with optimal partial autocorrelation properties," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2438–2442, Oct. 2004.

[6] *European GNSS (Galileo) Open Service Signal in Space Interface Control Document*, European Union and European Space Agency, Paris, France, Sep. 2010.

[7] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. Baldock, U.K.: Research Studies Press, 1996.

[8] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 14, no. 1, pp. 154–156, Jan. 1968.

[9] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA, USA: Holden-Day, 1967.

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

[11] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 400–411, Mar. 1995.

[12] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847–2867, Nov. 2002.

[13] Z. Guohua and Z. Quan, "Pseudonoise codes constructed by Legendre sequence," *Electron. Lett.*, vol. 38, no. 8, pp. 376–377, Apr. 2002.

[14] 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, Apr. 2009.

[15] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, no. 3, pp. 209–232, 1976.

[16] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. Pless and C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998.

[17] T. Helleseth and P. V. Kumar, "Pseudonoise sequences," in *Mobile Communications Handbook*, J. D. Gibson, Ed., 3rd ed. Boca Raton, FL, USA: Taylor & Francis, 2013.

[18] J. W. Kang, Y. Whang, B. H. Ko, and K. S. Kim, "Generalized cross-correlation properties of Chu sequences," *IEEE Trans. Inf. Theory*, vol. 58, no. 1, pp. 438–444, Jan. 2012.

[19] D. S. Kim, H.-J. Chae, and H. -Y. Song, "A generalization of the family of p-ary decimated sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7614–7617, Nov. 2011.

[20] J.-Y. Kim, S.-T. Choi, J.-S. No, and H. Chung, "A new family of p-ary sequences of period $(p^n - 1)/2$ with low correlation," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3825–3830, Jun. 2011.

[21] 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, Mar. 2007.

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

[23] 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.

[24] 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, Mar. 1996.

[25] 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.

[26] A. Lempel, M. Cohn, and W. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 38–42, Jan. 1977.

[27] N. Levanon and E. Mozeson, *Radar Signals*. New York, NY, USA: Wiley, 2004.

[28] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[29] W. C. Lindsey and M. K. Simon, *Telecommunication Systems Engineering*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1973.

[30] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Norwell, MA, USA: Kluwer, 1987.

[31] W. Meidle and A. Winterhof, "Some notes on the linear complexity of Sidelnikov–Lempel–Cohn–Eastman sequences," *Designs, Codes Cryptogr.*, vol. 38, no. 2, pp. 159–178, 2006.

[32] *IS-GPS-200 Revision D Navstar Global Positioning System Interface Specification: Navstar GPS Space Segment/Navigation User Interface*, Navstar GPS Joint Program Office, El Segundo, CA, USA, Jul. 2004.

[33] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology, the Science of Information Integrity*, G. J. Simmons, Ed. New York, NY, USA: IEEE Press, 1992, ch. 2.

[34] J. J. Rushanan, "Weil sequences: A family of binary sequences with good correlation properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 1648–1652.

[35] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Problems Inf. Transmiss.*, vol. 5, no. 1, pp. 12–16, 1969.

[36] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. Rockville, MD, USA: Computer Science Press, 1985.

[37] H.-Y. Song, "Feedback shift register sequences," in *Encyclopedia of Telecommunications*, vol. 2, J. G. Proakis, Ed. Hoboken, NJ, USA: Wiley, 2003, pp. 789–802.

[38] H. Taylor and Z. Dinitz, "Costas arrays," in *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., 2nd ed. Boca Raton, FL, USA: Taylor & Francis, 2007.

[39] 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.

[40] D. Wan, "Generators and irreducible polynomials over finite fields," *Math. Comput.*, vol. 66, no. 219, pp. 1195–1212, Jul. 1997.

[41] A. Weil, *Basic Number Theory*, 3rd ed. New York, NY, USA: Springer-Verlag, 1974.

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

[43] 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.

[44] 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.

[45] J. L. Yucas, "Irreducible polynomials over finite fields with prescribed trace/prescribed constant term," *Finite Fields Appl.*, vol. 12, no. 2, pp. 211–221, Apr. 2006.

Young-Tae Kim received his BS degree in Mathematics and MS degree in Electronics and Electrical engineering both from Yonsei University, Seoul, Korea, in 2011 and 2013, respectively. He is currently working as a communication engineer in LG Electronics. His area of research interest includes design and analysis of PN sequences and various implementation of mobile application services on mobile handsets.

Dae San Kim (M'05) received his BS and MS degrees in mathematics from Seoul National University, Seoul, Korea, in 1978 and 1980, respectively, and the Ph.D. degree in mathematics from University of Minnesota, Minneapolis, MN, in 1989. He is a professor in the Department of Mathematics at Sogang University, Seoul, Korea. He has been there since 1997, following a position at Seoul Women's University. His research interests include number theory (exponential sums, modular forms, zeta functions, p-adic analysis, umbral calculus) and coding theory. He is a member of AMS (American Mathematical Society) and IEEE.

Hong-Yeop Song (S'85–M'92–SM'07) 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. 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), KICS, KIISC and KMS.