# A family of sequences with large size and good correlation property arising from $M$-ary Sidelnikov sequences of period $q^d - 1$

Dae San Kim, *Member, IEEE*



***Abstract*—Let $q$ be any prime power and let $d$ be a positive integer greater than 1. In this paper, we construct a family of $M$-ary sequences of period $q-1$ from a given $M$-ary, with $M|q-1$, Sidelikov sequence of period $q^d-1$. Under mild restrictions on $d$, we show that the maximum correlation magnitude of the family is upper bounded by $(2d-1)\sqrt{q}+1$ and the asymptotic size, as $q \to \infty$, of that is $\frac{(M-1)q^{d-1}}{d}$. This extends the pioneering work of Yu and Gong for $d = 2$ case.**

***Index Terms*—Correlation, Family size, Sidelnikov sequence, Array structure.**

## I. Introduction

IN a code-division multiple-access (CDMA) communication systems, sequences with low correlation are required for synchronization and minimization of multiple-access interference. For adaptive modulation schemes, sequences with variable lengths and alphabet sizes are desirable to maximize data rate according to channel characteristics. Moreover, a large number of distinct sequences are needed to support as many users as possible.

In [6], for any prime power $q$ and a positive integer $M$, with $M|q-1$, Sidelnikov introduced $M$-ary sequences(called Sidelnikov sequences) of period $q-1$, which have the maximum out-of-phase autocorrelation magnitude of 4. Kim and Song in [3] showed that the cross-correlation of an $M$-ary Sidelnikov sequence of period $q-1$ and its constant multiple has the maximum magnitude of $\sqrt{q}+3$.

Sidelnikov sequences can be used in constructing a large number of distinct sequences. In this direction of efforts, one refers to the papers [2], [4], and [8]- [11].

In this paper, we consider $M$-ary Sidelnikov sequences, with $M|q-1$, of period $q^d-1(q = p^n$ a prime power) and study the $(q-1) \times (\frac{q^d-1}{q-1})$ array structure of such sequences. Then we construct a family of $M$-ary sequences with period $q-1$, with large size and good correlation property. It is formed as the constant multiples of those column sequences corresponding to a set of $q$-cyclotomic coset representatives mod $(\frac{q^d-1}{q-1})$. Under the mild restrictions on $d$(cf. (9)), it is shown that the maximum correlation magnitude of the family is upper bounded by $(2d-1)\sqrt{q}+1$, and the asymptotic size, as $q \to \infty$, of that is $\frac{(M-1)q^{d-1}}{d}$. Also, we derive an exact but less explicit expression of the size of the family of sequences by using a result of Yucas [12]. One refers to the tables either in [2] or [9] to compare our result with the known ones. This generalizes the pioneering work of Yu and Gong for $d = 2$ case in [9] and [10].

## II. Preliminaries

We will use the following notations throughout this paper.

- $p$ a prime number,
- $n$ a positive integer,
- $q = p^n$,
- $\mathbb{F}_q$ the finite field with $q$ elements,
- $\mathbb{F}_{q^d}$ the finite field with $q^d$ elements, with $d \geq 2$,
- $M$ a positive divisor of $q-1$, with $M \geq 2$,
- $w_M = \exp(\frac{2\pi i}{M})$,
- $\alpha$ a fixed primitive element of $F_{q^d}$,
- $\beta = \alpha^{\frac{q^d-1}{q-1}} = N(\alpha)$ a primitive element of $\mathbb{F}_q$,
- $N$ the norm map from $\mathbb{F}_{q^d} \to \mathbb{F}_q$, given by $N(x) = x^{\frac{q^d-1}{q-1}}$,
- $Tr$ the trace map from $\mathbb{F}_{q^d} \to \mathbb{F}_q$, given by $Tr(x) = \sum_{j=0}^{d-1} x^{q^j}$,
- $\psi$ the multiplicative character of $\mathbb{F}_q$ of order $M$, defined by $\psi(x) = \exp(\frac{2\pi i \log_\beta x}{M}) = w_M^{\log_\beta x}$.

Here we recall that, for any fixed primitive element $\beta$ of $\mathbb{F}_q$, a logarithm over $\mathbb{F}_q$ is defined by

$$\log_\beta x = \begin{cases} t, & \text{if } x = \beta^t \ (0 \leq t \leq q-2), \\ 0, & \text{if } x = 0. \end{cases}$$

so that, in particular, $\psi(0) = 1$. This convention is not the usual one requiring $\psi(0) = 0$. However, this agreement turns out to be very convenient, as this has been fruitfully demonstrated in the papers [8]- [11].

Again, for any fixed primitive element $\beta$ of $\mathbb{F}_q$, the $M$-ary Sidelnikov sequence $s(t)$ of period $q-1$ is defined as

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

where $D_k = \{\beta^{Mj+k} - 1 | 0 \leq j < \frac{q-1}{M}\}$, for $0 \leq k \leq M-1$. It is clear that $s(t)$ can be defined equivalently as

$$s(t) \equiv \log_\beta(\beta^t + 1) \mod M, \tag{2}$$

or as

$$w_M^{s(t)} = \psi(\beta^t + 1).$$

The Weil's estimate for multiplicative character sums is well known(cf. [5], Theorem 5.41). In [7, Corollary 2.3], Wan generalized his estimate to the case of multiple multiplicative character sums. On the other hand, Yu and Gong(cf. [8]-[11])introduced a refined version of Wan's bound that works under the assumption that the value of the multiplicative characters at 0 are equal to 1 rather than the traditional 0. Here we state only a special case that is just suitable for our purpose.

*Theorem 1 ( [7], [9]):* Let $f_1(x), \ldots, f_m(x)$ be monic distinct irreducible polynomials over $\mathbb{F}_q$ with degrees $d_1, \ldots, d_m$, with $e_j$ the number of distinct roots in $\mathbb{F}_q$ of $f_j(x)(j = 1, \ldots, m)$. Let $\psi_1, \ldots, \psi_m$ be nontrivial multiplicative characters of $\mathbb{F}_q$, with $\psi_j(0) = 1$ $(j = 1, \ldots, m)$. Then, for $a_1, \ldots, a_m \in \mathbb{F}_q^\times$, we have the estimate

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x)) \right| \leq \left( \sum_{j=1}^m d_j - 1 \right) \sqrt{q} + \sum_{j=1}^m e_j. \tag{3}$$

## III. ARRAY STRUCTURE OF THE $M$-ARY SIDELNIKOV SEQUENCES OF PERIOD $q^d - 1$

Here we investigate the $(q-1) \times (\frac{q^d-1}{q-1})$ array structure of $M$-ary Sidelnikov sequences of period $q^d - 1$, with $M | q-1$. This is a generalization of the $d = 2$ case in [9] and [10] that has its origin in the paper [1].

*Theorem 2:* Let $\{s(t)\}$ be an $M$-ary Sidelnikov sequences of period $q^d - 1$, with $M | q - 1$. Then

$$s(t) \equiv \log_\beta(N(\alpha^t + 1)) \mod M, \tag{4}$$

where $0 \leq t \leq q^d - 2$.

In other words,

$$s(t) = \begin{cases} 0, & \text{if } N(\alpha^t + 1) = 0, \\ k, & \text{if } N(\alpha^t + 1) \in S_k, \end{cases}$$

where $S_k = \{\beta^{Mj+k} | 0 \leq j < \frac{q-1}{M}\}$, for $0 \leq k \leq M - 1$.

*Remark 1:* Note here that the sets $S_k$ are different from those $D_k$ in (1).

*Proof:* By definition of Sidelnikov sequence,

$$s(t) \equiv y(t) \mod M, \text{ with } y(t) = \log_\alpha(\alpha^t + 1).$$

To prove the statement, we may assume that $N(\alpha^t + 1) \neq 0$. 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 $M | q - 1$,

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

Thus

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

■

We list the sequence $\{s(t)\}(0 \leq t \leq q^d - 2)$ as an $(q - 1) \times (\frac{q^d-1}{q-1})$ array so that the $l$-th column $v_l(t)(0 \leq t \leq q - 2)$ of the array is given by:

$$v_l(t) = s\left(\left(\frac{q^d-1}{q-1}\right)t + l\right), \quad (0 \leq l \leq \frac{q^d-1}{q-1} - 1).$$

Then

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

Let $f_l(x)$ be the polynomial of degree $d$ over $\mathbb{F}_q$ given by: for any nonnegative integer $l$,

$$\begin{aligned} f_l(x) &= N(\alpha^l x + 1) \\ &= (\alpha^l x + 1)(\alpha^{lq} x + 1) \cdots (\alpha^{lq^{d-1}} x + 1) \\ &= \beta^l x^d + \cdots + Tr(\alpha^l) x + 1. \end{aligned}$$

Then

$$v_l(t) \equiv \log_\beta f_l(\beta^t) \mod M. \tag{6}$$

For each $l(0 \leq l \leq \frac{q^d-1}{q-1} - 1)$,

$$\begin{aligned} f_l(x) &= \beta^l N(x + \alpha^{-l}) \\ &= \beta^l (x + \alpha^{-l})(x + \alpha^{-lq}) \cdots (x + \alpha^{-lq^{d-1}}) \\ &= \beta^l p_l(x)^{\frac{d}{d_l}}, \end{aligned} \tag{7}$$

where $p_l(x)$ is the irreducible polynomial over $\mathbb{F}_q$ of $-\alpha^{-l}$ of degree $d_l$. Note here that $d_l | d$.

*Remark 2:* Note that the $q$-cyclotomic coset containing $l(0 \leq l \leq q^d - 2) \mod q^d - 1$ is

$$C_l = \{l, ql, \cdots, q^{d_l - 1} l\},$$

where each $q^j l$ is reduced modulo $q^d - 1$, $d_l$ is the smallest positive integer satisfying $q^{d_l} l \equiv l \mod q^d - 1$, and

$$p_l(x) = \prod_{j \in C_l} (x + \alpha^{-j}). \tag{8}$$

Here $l$ is taken as the smallest positive integer in $C_l$ modulo $q^d - 1$, as usual.

*Proposition 1:* 1) $v_l(t) = v_{lq}(t)$.

2) $p_l(x)$ has no roots in $\mathbb{F}_q$, for $l$, with $1 \leq l \leq \frac{q^d-1}{q-1} - 1$.
3) For nonnegative integers $l_1, l_2$, with $l_1 \equiv l_2 \mod \frac{q^d-1}{q-1}$, $v_{l_1}(t)$ and $v_{l_2}(t)$ are cyclically equivalent.
4) $v_{\frac{q^d-1}{q-1} - \frac{q^{d-1}-1}{q-1} l}(t) \equiv v_l(t - l + 1) \mod M$, so that $v_{\frac{q^d-1}{q-1} - \frac{q^{d-1}-1}{q-1} l}(t)$ and $v_l(t)$ are cyclically equivalent for each $l(1 \leq l \leq q)$.

*Proof:*

1) $f_l(x) = f_{lq}(x)$, so that $v_l(t) = v_{lq}(t)$, by (6).

2) This follows from the observation that $d_l = 1$ iff $\alpha^l \in \mathbb{F}_q$ iff $\frac{q^d-1}{q-1} | l$.
3) is easy to see.
4) This is a generalization of the result for $d = 2$ discovered by Yu and Gong in [9] and [10]: for each $l(1 \le l \le q)$,

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

Also, this follows from 1) and 3), since

$$q \left( \frac{q^d-1}{q-1} - \frac{q^{d-1}-1}{q-1} l \right) \equiv l \mod \frac{q^d-1}{q-1}.$$

∎

*Remark 3:* Because of 1) and 3) of Proposition 1, we are led to consider the $q$-cyclotomic cosets $\mod \frac{q^d-1}{q-1}$. Recall that the $q$-cyclotomic coset containing $l(0 \le l \le \frac{q^d-1}{q-1} - 1)$ $\mod \frac{q^d-1}{q-1}$ is

$$\hat{C}_l = \{l, ql, \ldots, q^{m_l - 1} l\},$$

where each $q^j l$ is reduced modulo $\frac{q^d-1}{q-1}$, $m_l$ is the smallest positive integer satisfying $q^{m_l} l \equiv l \mod \frac{q^d-1}{q-1}$. Again, here $l$ is taken as the smallest positive integer in $\hat{C}_l$ modulo $\frac{q^d-1}{q-1}$, as usual. Here $m_l | d_l$. So if $q_l(x) = \prod_{j \in \hat{C}_l} (x + \alpha^{-j})$, then

$$p_l(x) = q_l(x) q_l(x)^{\sigma^{m_l}} q_l(x)^{\sigma^{2m_l}} \cdots q_l(x)^{\sigma^{d_l - m_l}}.$$

Here $\sigma$ is the Frobenius automorphism of $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$, given by $\sigma(a) = a^q$, so that

$$q_l(x)^{\sigma^{i m_l}} = \prod_{j \in \hat{C}_l} (x + \alpha^{-j q^{i m_l}}) \quad (0 \le i \le \frac{d_l}{m_l} - 1).$$

## IV. Construction of a Family of Sequences

Here we construct a family $\Sigma$ of $M$-ary sequences with period $q-1$, consisting of the constant multiples of those column sequences $v_l(t)$ corresponding to a set of $q$-cyclotomic coset representatives $\mod \frac{q^d-1}{q-1}$, for the set consisting of $l(1 \le l \le \frac{q^d-1}{q-1})$. Then it is shown that, under mild restrictions on $d$ (cf. (9)), it has a large family size and good correlation property. Actually, we show that the maximum correlation magnitude of the family is upper bounded by $(2d-1)\sqrt{q} + 1$, and the asymptotic size, as $q \to \infty$, of that is $\frac{(M-1)q^{d-1}}{d}$. Also, we derive an exact but less explicit expression of the size of the family of sequences by using a result of Yucas(cf. Theorem 5). This generalizes the pioneering work of Yu and Gong for $d = 2$ case in [9] and [10].

*Definition 1:* Let $\Lambda$ be the set of all integers $l(0 \le l \le \frac{q^d-1}{q-1} - 1)$ consisting of the smallest $q$-cyclotomic coset representative from each $q$-cyclotomic coset $\mod \frac{q^d-1}{q-1}$.

*Proposition 2:* 1) $|\Lambda|$ = the number of $q$-cyclotomic cosets $\mod \frac{q^d-1}{q-1}$ = the number of monic irreducible factors of $x^{\frac{q^d-1}{q-1}} - 1$.

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

*Proof:* 1) The first equality is just Definition 1. Let $\gamma = \alpha^{q-1}$ be a primitive $(\frac{q^d-1}{q-1})$-th root of unity in $\mathbb{F}_{q^d}$. Then, with $M^{(l)}(x) = \prod_{j \in \hat{C}_l} (x - \gamma^j)$ denoting the irreducible polynomial of $\gamma^l$ over $\mathbb{F}_q$, we have

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

Thus we have the desired equality.

2) Clearly, $e|d$. For a root $\alpha$ of $p(x)$ in $\mathbb{F}_{q^d}$, $N(\alpha) = 1$, and $((-1)^e b)^{\frac{d}{e}} = (-1)^d b^{\frac{d}{e}}$ is the constant term of $p(x)^{\frac{d}{e}} = x^d + \cdots + (-1)^d N(\alpha)$. ∎

Assume from now on that

$$(d, q-1) = 1, \quad d < \frac{\sqrt{q} - \frac{2}{\sqrt{q}} + 1}{2}. \tag{9}$$

*Proposition 3:* Let $l_1, l_2$ be elements in $\Lambda \setminus \{0\}$, and let $\tau(0 \le \tau \le q-2)$ be an integer. Then $p_{l_1}(x)$ and $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ are distinct irreducible polynomials over $\mathbb{F}_q$, unless $l_1 = l_2$ and $\tau = 0$. Here

$$\begin{aligned} &\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x) \\ &= (x + \alpha^{-l_2} \beta^{-\tau})(x + \alpha^{-l_2 q} \beta^{-\tau}) \cdots (x + \alpha^{-l_2 q^{d_{l_2} - 1}} \beta^{-\tau}). \end{aligned} \tag{10}$$

*Proof:* We know that $p_{l_1}(x)$ and $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ are irreducible polynomials over $\mathbb{F}_q$. Assume that they are the same. Then $\alpha^{-l_1} = \alpha^{-l_2 q^s} \beta^{-\tau}$, for some nonnegative integer $s(0 \le s \le d_{l_2} - 1)$, and hence $l_1 \equiv l_2 q^s + \tau(\frac{q^d-1}{q-1})$ $\mod q^d - 1$. So $l_1 \equiv l_2 q^s \mod \frac{q^d-1}{q-1}$ and thus $l_1$ and $l_2$ are in the same $q$-cyclotomic coset $\mod \frac{q^d-1}{q-1}$. This implies $l_1 = l_2$. Now, $l_1 \equiv l_1 q^s \mod \frac{q^d-1}{q-1}$, and hence $l_1(q^s - 1) = \tau'(\frac{q^d-1}{q-1})$.

Observe that we have $\frac{q^d-1}{q-1} = f(q)(q-1) + d$, for $f(q) = \sum_{j=1}^{d-1} j q^{d-j-1}$, and hence that $(q-1, \frac{q^d-1}{q-1}) = (q-1, d) = 1$. Hence $l_1(q^s - 1) \equiv 0 \mod q^d - 1$, and so $d_{l_1} | s$. As $0 \le s \le d_{l_1} - 1 = d_{l_2} - 1$, we have $s = 0$. In all, $l_1 \equiv l_1 + \tau(\frac{q^d-1}{q-1})$ $\mod q^d - 1$ which implies $q - 1 | \tau$, and therefore $\tau = 0$. ∎

*Definition 2:* Let $\Sigma$ be the family consisting of $M$-ary sequences of period $q-1$, given by

$$\Sigma = \{c v_l(t) | 1 \le c \le M-1, l \in \Lambda \setminus \{0\}\}.$$

*Remark 4:* When $d = 2, \Lambda \setminus \{0\} = \{1, \ldots, [\frac{q+1}{2}]\}$. This follows from the simple observation that the $q$-cyclotomic coset containing $l \mod q+1$ is $\hat{C}_l = \{l, ql\}$, and $ql \equiv q - l + 1$ $\mod q + 1$. So the family $\mathbf{S}_v$ considered in [9] and [10] is identical to our $\Sigma$, for $q = p^n$ even and contains $M-1$ less sequences, namely $c v_{\frac{q+1}{2}}(t)(1 \le c \le M-1)$, for $q$ odd.

Recall that the maximum correlation of $\Sigma$, $\delta_{\max} = \delta_{\max}(\Sigma)$, is defined as the maximum absolute value of all nontrivial auto- and cross-correlations of the sequences in $\Sigma$.

*Theorem 3:* For the family $\Sigma = \{cv_l(t) | 1 \le c \le M-1, l \in \Lambda \setminus \{0\}\}$ of $M$-ary sequences of period $q-1$, we have

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

*Proof:* Assume that $l_1 \ne l_2 (l_1, l_2 \in \Lambda \setminus \{0\})$ or $\tau$ is in the range $1 \le \tau \le q-2$. Then $p_{l_1}(x)$ and $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ are distinct irreducible polynomials over $\mathbb{F}_q$, by Proposition 3. The cross-correlation function $R(\tau) = R_{c_1,l_1,c_2,l_2}(\tau)$ between the sequence $c_1 v_{l_1}(t)$ and $c_2 v_{l_2}(t)$ in $\Sigma$ is given by

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{q-2} {w_M}^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)} \\ &= \sum_{t=0}^{q-2} \psi^{c_1}(f_{l_1}(\beta^t)) \psi^{M-c_2}(f_{l_2}(\beta^{t+\tau})) \\ &= \sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^\tau x)) - 1, \end{aligned} \tag{11}$$

where $\psi_1 = \psi^{c_1 \frac{d}{d_{l_1}}}$ and $\psi_2 = \psi^{c_2 \frac{d}{d_{l_2}}}$. Observe that both $c_1 \frac{d}{d_{l_1}}$ and $c_2 \frac{d}{d_{l_2}}$ are not divisible by $M$ and hence $\psi_1$ and $\psi_2$ are both nontrivial, since $(d, q-1) = 1$. In view of (3), the sum in (11) in absolute value is

$$\begin{aligned} &|\sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^\tau x))| \\ &\qquad \le (d_{l_1} + d_{l_2} - 1)\sqrt{q} \\ &\qquad \le (2d-1)\sqrt{q}. \end{aligned}$$

So we get the desired result in this case. Note here that $p_{l_1}(x)$ and $\beta^{-\tau d_{l_2}} p_{l_2}(\beta^\tau x)$ have no roots in $\mathbb{F}_q$, by Proposition 1 2), and (10). Then we consider the case that $c_1 \ne c_2$, but $l_1 = l_2$ and $\tau = 0$. In this case,

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{q-2} w_M^{(c_1 - c_2) v_{l_1}(t)} \\ &= \sum_{x \in \mathbb{F}_q} \psi^*(p_{l_1}(x)) - 1, \end{aligned}$$

where $\psi^* = \psi^{(c_1 - c_2)\frac{d}{d_{l_1}}}$ is nontrivial, as $(c_1 - c_2)\frac{d}{d_{l_1}}$ is not divisible by $M$. So, by the classical Weil's theorem(the $m = 1$ case of Theorem 1),

$$\begin{aligned} |R(\tau)| &\le (d_{l_1} - 1)\sqrt{q} + 1 \\ &\le (d-1)\sqrt{q} + 1. \end{aligned}$$

Note that these take care of the cases that $(c_1, l_1) \ne (c_2, l_2)$ and $(c_1, l_1) = (c_2, l_2)$, but with $\tau \ne 0$. ∎

*Theorem 4:* The sequences in the family $\Sigma = \{cv_l(t) | 1 \le c \le M-1, l \in \Lambda \setminus \{0\}\}$ are cyclically inequivalent.

*Proof:* If $c_1 v_{l_1}(t)$ and $c_2 v_{l_2}(t)$ are cyclically equivalent, then, for some $\tau (0 \le \tau \le q-2)$, $c_1 v_{l_1}(t) = c_2 v_{l_2}(t+\tau)$ and hence

$$\begin{aligned} q - 1 &= \sum_{t=0}^{q-2} w_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)} \\ &= |\sum_{t=0}^{q-2} w_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)}| \\ &\le |\sum_{x \in \mathbb{F}_q} \psi_1(p_{l_1}(x)) \psi_2(\beta^{-\tau d_{l_2}} \times \beta^{\tau d_{l_2}} p_{l_2}(\beta^\tau x))| + 1 \\ &\le (2d-1)\sqrt{q} + 1, \end{aligned}$$

if $(c_1, l_1) \ne (c_2, l_2)$. Here $\psi_1 = \psi^{c_1 \frac{d}{d_{l_1}}}$ and $\psi_2 = \psi^{c_2 \frac{d}{d_{l_2}}}$. This is impossible in view of our assumption in (9). Thus $c_1 v_{l_1}(t)$ and $c_2 v_{l_2}(t)$ are the same. ∎

*Remark 5:* Under the mild restrictions in (9), we proved Proposition 3, and Theorems 3 and 4. Assume that $d = 2$. The second condition in (9) needed in proving Theorem 4 misses only a few values of $q$. Namely, $q = 2, 4, 8, 3, 9, 5, 7$, and 11. Note that $(2, q-1) = 1$ for $q$ even and $(2, q-1) = 2$ for $q$ odd. Suppose we are in the latter case. Then the first condition in (9) is not necessary in showing Theorems 3 and 4, since $\frac{d}{d_{l_1}} = \frac{d}{d_{l_2}} = 1$, and so the $\psi_1$ and $\psi_2$ are nontrivial. In addition, if we replace $\Lambda \setminus \{0\}$ by $\Lambda \setminus \{0, \frac{q+1}{2}\} = \{1, \ldots, \frac{q-1}{2}\}$, then one easily checks that the statement of Proposition 3 holds true.

*Theorem 5 (12, Theorem 3.5):* Let $A_f = \{r | \; r | q^f - 1$ but $r$ does not divide $q^g - 1$ for $1 \le g < f\}$, for each positive integer $f$, and, for $r \in A_f$, write $r = d_{rf} m_{rf}$, with $d_{rf} = (r, \frac{q^f - 1}{q-1})$.

Assume $b \in \mathbb{F}_q^\times$ has order $m$, and let $N(f, b, q)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree $f$ with constant term $(-1)^f b$. Then

$$N(f, b, q) = \frac{1}{f \phi(m)} \sum_{\substack{r \in A_f \\ m_{rf} = m}} \phi(r). \tag{12}$$

*Theorem 6:* The size of the family $\Sigma = \{cv_l(t) | 1 \le c \le M-1, l \in \Lambda \setminus \{0\}\}$, with the notations in the above, can be expressed as:

$$|\Sigma| = (M-1)(|\Lambda| - 1), \tag{13}$$

where the number of monic irreducible factors $|\Lambda|$ of $x^{\frac{q^d - 1}{q-1}} - 1$ is given by

$$\sum_{e | d} \frac{1}{e} \sum_{m | \frac{d}{e}} \sum_{\substack{r \in A_e \\ m_{re} = m}} \phi(r). \tag{14}$$

*Proof:* Clearly, we have (13). By Proposition 2 1), the size of $\Sigma$ is also given by

$$|\Sigma| = (M-1) \times ((\text{the number of monic irreducible factors of } x^{\frac{q^d - 1}{q-1}} - 1) - 1).$$

Thus we only need to verify that the number of irreducible factors $|\Lambda|$ of $x^{\frac{q^d - 1}{q-1}} - 1$ is given by the expression in (14). In view of Proposition 2 2), that number is equal to

$$\sum_{e|d}\sum_{b^{\frac{d}{e}}=1}(\text{\# of monic irreducible factors over } \mathbb{F}_q \text{ of } x^{\frac{q^d-1}{q-1}}-1, \text{ with degree } e \text{ and the constant term equal to } (-1)^e b)$$
$$=\sum_{e|d}\sum_{m|\frac{d}{e}}\sum_{\substack{b\\ o(b)=m}}(\text{\# of monic irreducible polynomials over } \mathbb{F}_q \text{ with degree } e \text{ and the constant term equal to } (-1)^e b)$$
$$=\sum_{e|d}\sum_{m|\frac{d}{e}}\sum_{\substack{b\\ o(b)=m}} N(e,b,q). \tag{15}$$

The desired result now follows from (12). ■

*Remark 6:* Let's consider the case of $d = 2$. In that case,

$$|\Lambda| = \sum_{\substack{r\in A_1\\ m_{r1}=1}}\phi(r) + \sum_{\substack{r\in A_1\\ m_{r1}=2}}\phi(r) + \frac{1}{2}\sum_{\substack{r\in A_2\\ m_{r2}=1}}\phi(r)$$
$$= 1 + \sum_{2|q-1} 1 + \frac{1}{2}\sum_{\substack{r|q+1\\ r\neq 1,2}}\phi(r)$$

and hence

$$|\Lambda| - 1 = \left[\frac{q+1}{2}\right] = \begin{cases} \frac{q+1}{2}, & \text{if } q \text{ odd},\\ \frac{q}{2}, & \text{if } q \text{ even}.\end{cases} \tag{16}$$

This is what is expected(cf. Remark 4).

The next theorem follows from [7, Theorem 5.1] by taking $f(T) = T$. It gives an estimate for $N(f, b, q)$ in (12).

*Theorem 7 ( [7]):* Let $N(f, b, q)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree $f$ with constant term $(-1)^f b$, for some element $b \in \mathbb{F}_q^\times$. Then

$$\left|N(f,b,q) - \frac{q^f}{f(q-1)}\right| \le \frac{2}{f}q^{\frac{f}{2}}. \tag{17}$$

*Theorem 8:* The asymptotic size of $\Sigma = \{cv_l(t)|1 \le c \le M-1, l \in \Lambda\setminus\{0\}\}$, as $q \to \infty$, is given by:

$$|\Sigma| \sim \frac{(M-1)q^{d-1}}{d}, \text{ as } q \to \infty.$$

*Proof:* Assume first that $d > 2$. From (15) and (17),

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

This implies that

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

and hence

$$|\Sigma| \sim \frac{(M-1)q^{d-1}}{d}, \text{ as } q \to \infty. \tag{18}$$

Even for $d = 2$, we get the same result as in (18). Indeed, from (16), we have

$$|\Sigma| = (M-1)[\frac{q+1}{2}] \sim \frac{(M-1)q}{2}, \text{ as } q \to \infty.$$

■

## V. Conclusion

In this paper, starting with $M$-ary Sidelnikov sequences, with $M|q-1$, of period $q^d - 1 (q = p^n$ a prime power) and considering the $(q-1)\times(\frac{q^d-1}{q-1})$ array structure of such sequences, we constructed a family of $M$-ary sequences with period $q-1$, with large size and good correlation property. It is formed as the constant multiples of those column sequences corresponding to a set of $q$-cyclotomic coset representatives $\bmod \frac{q^d-1}{q-1}$. Then, under the mild restrictions on $d$ (cf. (9)), it is shown that the maximum correlation magnitude of the family is upper bounded by $(2d-1)\sqrt{q}+1$, and the asymptotic size, as $q \to \infty$, of that is $\frac{(M-1)q^{d-1}}{d}$. Also, we derived an exact but less explicit expression of the size of the family of sequences by using a result of Yucas [12]. This generalizes the pioneering work of Yu and Gong for $d = 2$ case in [9] and [10].

## Acknowledgment

I would like to thank Prof. H.-Y. Song for drawing the paper [10] to my attention. [This work was supported by National Foundation of Korea Grant funded by the Korean Government(2009-0072514)].

## References

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

[2] 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.

[3] Y.-J. Kim and H.-Y. Song, *Cross correlation of Sidel'nikov sequences and their constant multiples*, IEEE Trans. Inf. Theory, vol. 53, no. 3, pp. 1220-1224, Mar. 2007.

[4] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, *New families of $M$-ary sequences with low correlation constructed from Sidel'nikov sequences*, IEEE Trans. Inf. Theory, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[5] R. Lidl and H. Niederreiter, *Finite Fields*, in Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1997.

[6] V. M. Sidelnikov, *Some $k$-valued pseudo-random sequences and nearly equidistant codes*, Probl. Inf. Transm., vol. 5, pp. 12-16, 1969.

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

[8] N. Y. Yu and G. Gong, *Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation*, IEEE Trans. Inf. Theory, submitted. Also available at CACR 2009-25, CACR Technical Report, University of Waterloo, 2009.

[9] 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, to appear. Also available at CACR 2010-01, CACR Technical Report, University of Waterloo, 2010.

[10] N. Y. Yu and G. Gong, *On the structure of $M$-ary Sidelnikov sequences of period $p^{2m}-1$*, in Proc. of IEEE Int. Symp. Information Theory(ISIT2010), pp. 1233-1237, Austin, TX, Jun. 2010.

[11] N. Y. Yu and G. Gong, *Generalized constructions of polyphase sequence families using shift and addition of multiplicative character sequences*, in Proc. of IEEE Int. Symp. Information Theory(ISIT2010), pp. 1258-1262, Austin, TX, Jun. 2010.

[12] 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.

**Dae San Kim(M'05)** received the B.S. and M. S. 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) and coding theory. He has been an editor of Journal of the Korean Mathematical Society since 2005.