Recent development on M-ary sequence family construction using Sidelnikov sequences

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

ITA 2013 @ UCSD, San Diego

Feb 10-15, 2013

Hong-Yeop Song and **Dae San Kim**

School of EEE
Yonsei Universtiy

Dept. Math
Sogang University

YONSEI UNIVERSITY

In The Beginning

(Sidelnikov-69)

Sidelnikov introduced two different types of non-binary (*M*-ary) sequences with **low** non-trivial **autocorrelation**.

- **Power Residue Sequences (PRS in short) of period p**
- **Sidelnikov Sequences of period $q-1$**

✓ V. M. Sidelnikov, “Some k-valued pseudo-random sequences and nearly equidistant codes,” *Probl. Inf. Transm.*, vol. 5, pp. 12-16, 1969.

(Lempel-Cohn-Eastman-77)

Re-discovered binary “Sidelnikov sequences”

✓ Lempel-Cohn-Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE* Trans. *Inform. Theory,* vol. *23,* No. 1, pp. 38-42, Jan. 1977.

✓ Sarwate, Comments on… 1978.

Power Residue Sequences of period p

- p = an odd prime
- β = a primitive root mod p
- M = a divisor of $p - 1$
- Coset Partition
  - ✓ C_0 : a set of M-th powers in the integers mod p
  - ✓ $C_k = \beta^k \cdot C_0$ for $0 \le k \le M-1$

◆ **An M-ary PRS of period p is defined as, for $t = 0, 1, \ldots, p-1$,**

$$s(t) = \begin{cases} 0, & \text{if } t = 0 \\ k, & \text{if } t \in C_k \end{cases}$$

Sidelnikov Sequences of period q-1

- $GF(q)$ = finite field of size q where $q = p^n$
- β = primitive element of $GF(q)$
- M = a divisor of $q - 1$
- **Coset Partition**
  - ✓ C_0 : a set of M-th powers in $GF(q)$
  - ✓ $C_k = \beta^k \cdot C_0$ for $0 \le k \le M$-1

■ **An M-ary Sidelnikov sequence of period $q - 1$** is defined as, **for t = 0, 1, 2,…, q-2,**

$$s(t) = \begin{cases} \mathbf{0}, & \textbf{if } \boldsymbol{\beta^t + 1 = 0} \\ k, & \textbf{if } \beta^t + 1 \in C_k \end{cases}$$

Comparison

- An M-ary **P**ower **R**esidue **S**equence of period p:

$$s(t) = \begin{cases} 0, & \textbf{if} \quad t = 0 \\ k, & \textbf{if} \quad t \in C_k \end{cases}$$

- An M-ary **Sidelnikov sequence** of period $q - 1$:

$$s(t) = \begin{cases} 0, & \textbf{if} \quad \beta^t + 1 = 0 \\ k, & \textbf{if} \quad \beta^t + 1 \in C_k \end{cases}$$

CCL

YONSEI UNIVERSITY

(Examples) $p = q = 13, \;\; M = 3, \; \beta = 2$

- $C_0 = 2^0 \cdot C_0 = \{1,5,8,12\}$ = cubic residues mod 13
- $C_1 = 2^1 \cdot C_0 = \{2,10,3,11\}$
- $C_2 = 2^2 \cdot C_0 = \{4,7,6,9\}$

t	0	1	2	3	4	5	6	7	8	9	10	11	12
PRS	**0**	**0**	**1**	**1**	**2**	**0**	**2**	**2**	**0**	**2**	**1**	**1**	**0**
SS	**1**	**1**	**0**	**2**	**2**	**2**	**0**	**0**	**1**	**2**	**1**	**0**	

t	0	1	2	3	4	5	**6**	7	8	9	10	11
β^t	1	2	4	8	3	6	**12**	11	9	5	10	7
$\beta^t + 1$	2	3	5	9	4	7	**0**	12	10	6	11	8

Summary of this talk

- **QUESTION:** Can we construct a family of sequences with **GOOD auto- & cross-correlation** from these sequences?

- **Yes**, we may...

- **We have an interesting development here... for both Power Residue sequences and Sidelnikov sequences... including some new results.**

CCL

YONSEI UNIVERSITY

First Family

- (Kim-Song-Gong-Chung - ISIT 06) **For PRS sequences, changing the primitive element yields another PRS sequence which are cyclically distinct, and having a GOOD crosscorrelation**
  - The number of distinct PRS of period p *obtainable by changing the primitive root* is given as $\phi(M)$

    $\rightarrow$ a family!

    $\rightarrow$ **all obtainable by multiplying some constants term-by-term**
  - **Crosscorrelation is upper bounded by $\sqrt{p}+2$**

- (Kim-Song - IT Trans 07) **Crosscorrelation of a set which consists of an M-ary Sidel'nikov sequence $s(t)$ of length $q-1$ and its constant multiple sequence is upper bounded by $\sqrt{q}+3$**
  - When $c \neq 1$, the resulting sequence is NOT a sidelnikov sequence in general.

Comparison and Main Problem

- **For PRS sequences of period p**
  - Generating a family by using all different primitive elements
    = taking all the distinct constant multiples of a sequence
  - Forms a family with GOOD cross correlation property

- **For Sidelnikov sequences of period q-1**
  - Taking a constant multiple does NOT result in a Sidelnikov sequence
  - But still, forms a family with GOOD cross correlation property

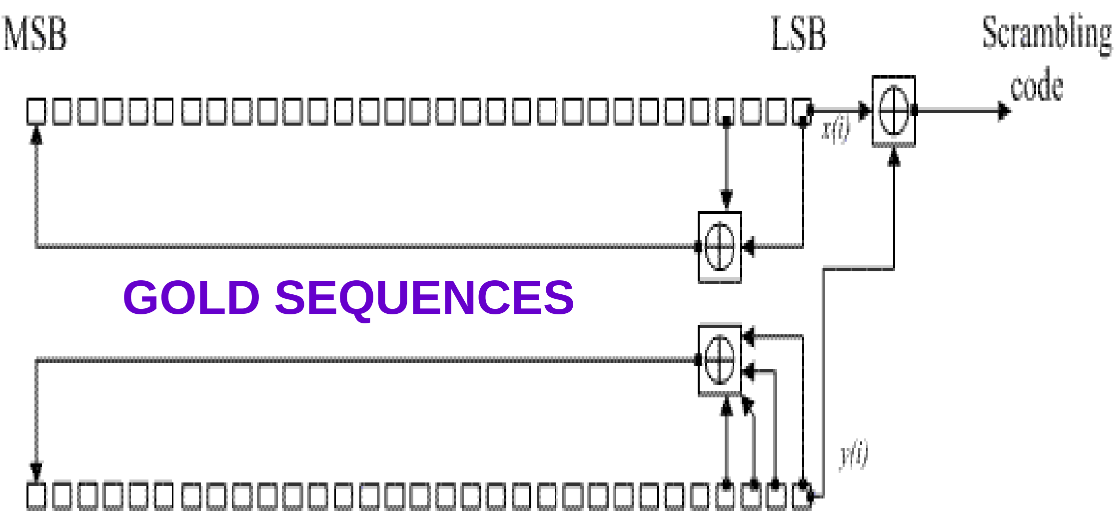
- **PROBLEM: The size is only $\phi(M)$ or M,** which is **sooo SMALL**…

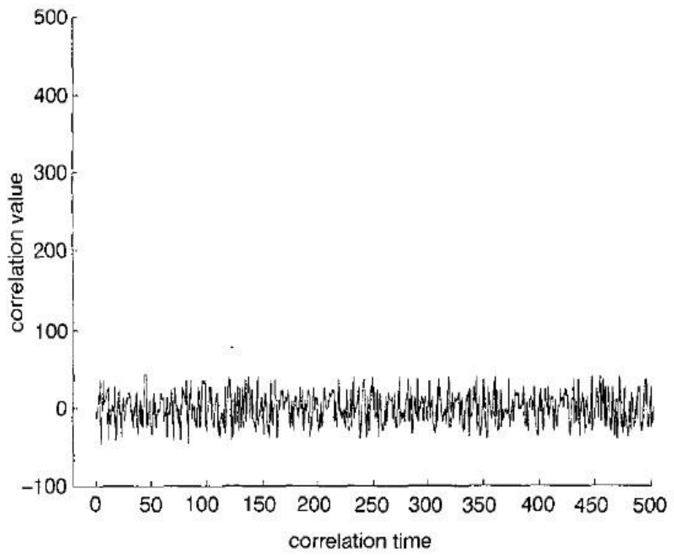
An improvement has started from somewhere else

- **Z. Guohua and Z. Quan**, "Pseudonoise codes constructed by Legendre sequence," IEE Electronic Letters, vol. 38, no. 8, pp. 376-377, **2002**.
- **Main Result + Conjecture:**

  The technique of **shift-and-add** **(as in the construction of GOLD sequences)** using a given **Legendre sequence** **(so called, quadratic residue sequence)** can construct a sequence **family with good crosscorrelation**.

  Crosscorrelation is **(conjectured to be)** upper bounded by $4\lfloor 2\sqrt{p/4}\rfloor + 1$





It is proved by Rushanan at ISIT-06

- **J. Rushanan**, "Weil Sequences: A Family of Binary Sequences with Good correlation Properties," *Proc. of IEEE Int. Symp. Information Theory(ISIT2006)*, Seattle, WA, USA, July **2006**.

- **Main Result:**

Crosscorrelation of the sequence family containing a Legendre sequence and its some shift-and-add sequences is upper bounded by $\mathbf{2\sqrt{p}+5}$.

- **Major Technique:**

product of 4 linear polynomials

$$\left|\sum_{x=0}^{p-1}\left(\frac{(x+a_1)\cdots(x+a_4)}{p}\right)\right| \leq 2\sqrt{p}+1$$

quadratic character

What Yang and No have noticed: (1) Weil Bound on Character Sum

- Kim-Chung-No-Chung, *IT Trans.* 2008
- Han-Yang, *IT Trans.* 2009
  - Rushanan's major tool is a famous and well-known technique for the proof of crosscorrelation of some sequences
  - ψ = **multiplicative character** of $GF(q)^*$ of order M, where $M|q-1$:

$$\psi(x) = \exp\left(\frac{j2\pi}{M}\log_\alpha x\right) \text{ with } \psi(0) = 0$$

(Weil-48) Let ψ be a multiplicative character of $GF(q)$ of order M and $f(x)$ a monic polynomial of positive degree over $GF(q)$ that is not an Mth power of a polynomial. Let d be the number of distinct roots of $f(x)$ in its splitting field $GF(q)$.Then for every $c \in GF(q)^*$, we have

$$\left|\sum_{x\in GF(q)} \psi(cf(x))\right| \le (d-1)\sqrt{q}$$

What Yang and No have noticed: (2) Shift-and-add sequences

- **Main Theorem (No-08,Yang-09)**

Let $s(t)$ be an M-ary Sidelnikov sequence of period $q-1$, with p odd.

Let $T = \lfloor (q-1)/2 \rfloor$.

Let $\mathcal{L}$ be the set of M-ary sequences of period $q-1$ given as follows.

$$\begin{aligned}\mathcal{L} = \{ \quad & c_1 s(t) \quad && \mid 1 \le c_1 \le M-1 \} \\ \cup \{ \; & c_1 s(t) + c_2 s(t+l) && \mid 1 \le c_1, c_2 \le M-1, \quad 1 \le l \le T-1 \} \\ \cup \{ \; & c_1 s(t) + c_2 s(t+T) && \mid 1 \le c_1 < c_2 \le M-1 \}\end{aligned}$$

$\Longrightarrow$ ① Correlations of the family $\mathcal{L}$ is upper bounded by

$$|C(\tau)| \le 3\sqrt{q} + 5$$

② Family size is $\frac{(M-1)^2(q-3)}{2} + \frac{M(M-1)}{2}$

Second Improvement by Yu-Gong

- **Yu-Gong – IT Trans 2010:** Multiplicative Characters, the Weil Bound, and Polyphase Sequence Families With Low Correlation
- **Fully generalize the family from both Power Residue Sequences of period p and Sidelnikov Sequences of period q-1**

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

	Period L	Alphabet	$C_{\max}$	Family size
$\mathcal{S}_{\mathbf{r}}^{(0)}$ (or $\tilde{\mathcal{F}}_{\mathbf{r}}$ [24])	p	M	$2\sqrt{L}+5$	$\left(\frac{L+1}{2}\right)\cdot(M-1)$
$\mathcal{L}_{\mathbf{r}}$ (or $\mathcal{F}_{\mathbf{r}}$ [24])	p	M	$3\sqrt{L}+4$	$M-1+\frac{(M-1)^2(L-1)}{2}$
$\mathcal{G}_{\mathbf{r}}^{(\delta,2)}, \delta\neq 0$ (in this paper)	p	M	$4\sqrt{L}+7$	$(M-1)+\left(\frac{L-1}{2}\right)(M-1)^2 + \frac{(L-1)(L-3)}{8}\cdot(M^2-3M+3)$
$\mathcal{H}_{\mathbf{r}}^{(2)}$ (in this paper)	p	M	$5\sqrt{L}+6$	$(M-1)+\left(\frac{L-1}{2}\right)(M-1)^2 + \frac{(L-1)(L-3)}{8}\cdot(M-1)^3$
$\mathcal{S}_{\mathbf{s}}^{(0)}$ (or $\tilde{\mathcal{F}}_{\mathbf{s}}$ [24])	p^m-1	M	$2\sqrt{L+1}+6$	$(M-1)\cdot\left(\frac{L}{2}\right)+\left\lfloor\frac{M-1}{2}\right\rfloor$
$\mathcal{L}_{\mathbf{s}}$ (or $\mathcal{L}$ [23])	p^m-1	M	$3\sqrt{L+1}+5$	$\frac{(M-1)^2(L-2)}{2}+\frac{M(M-1)}{2}$
$\mathcal{G}_{\mathbf{s}}^{(\delta,2)}, \delta\neq 0$ (in this paper)	p^m-1	M	$4\sqrt{L+1}+8$	$(M-1)+\left(\frac{L-2}{2}\right)(M-1)^2 + \frac{(L-2)(L-4)}{8}\cdot(M^2-3M+3)$
$\mathcal{H}_{\mathbf{s}}^{(2)}$ (in this paper)	p^m-1	M	$5\sqrt{L+1}+7$	$(M-1)+\left(\frac{L-2}{2}\right)(M-1)^2 + \frac{(L-2)(L-4)}{8}\cdot(M-1)^3$

YONSEI UNIVERSITY

New Direction by Yu-Gong

- Yu-Gong – IT Trans 2010: New Construction of M-ary Sequence Families With Low Correlation From the Structure of Sidelnikov Sequences

  - Only for family from Sidelnikove sequences of period q-1
  - Introduced ARRAY STRUCTURES of a longer Sidelnikov sequence of period q^2 -1 by listing it as an array of size (q-1) x (q+1)
  - Now, the family consists of some of its column sequences, their constant multiples, and their shift-and-add sequences.
  - They generalize the Weil Bound for the computation of the crosscorrelation.

- Use $\psi(0) = 1$ from now on.
- **(Refined Weil bound by Yu-Gong-10)**
  - Let $f_1(x), \dots, f_l(x)$ be l monic and irreducible polynomial over $GF(q)$ which have positive degrees $d_1, \dots, d_l$, respectively. Let d be the number of distinct roots of $f(x) = \prod_{i=1}^{l} f_i(x)$ in its splitting field over $\mathbb{F}_q$. Let e_i be the number of distinct roots in $\mathbb{F}_q$ of $f_i(x)$.
  - Let $\psi_1, \dots, \psi_l$ be multiplicative characters of $\mathbb{F}_q$. Assume that the product character $\prod_{i=1}^{l} \psi_i(f_i(x))$ is nontrivial.
  - If $\psi_i(0) = 1$, then, for every $a_i \in \mathbb{F}_q \backslash \{0\}$,

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq (d-1)\sqrt{q} + \sum_{i=1}^{l} e_i \,.$$

Sidelnikov Sequences (again)

- p = prime, and $q = p^n$ = prime power with a positive integer n
- M is a divisor of $q-1$
- $GF(q)$ = finite field of order q
- β = primitive element of $GF(q)$
- $D_k = \{\beta^{Mi+k} - 1 | 0 \le i < \frac{q-1}{M}\}$ for $0 \le k \le M-1$.

- **The M-ary Sidelnikov sequence of period $q-1$ is defined by**

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

- (Yu-Gong-10) **Equivalently, $s(t)$ is defined by**

$$\boldsymbol{s(t) \equiv \log_\beta(\beta^t + 1) \pmod{M},\ 0 \le t \le q-2}$$

$$s(t) \equiv \log_\beta(\beta^t + 1) \pmod{M}$$

- **Is this the ADDONE table (Zech Log) of finite field?**
  - Consider the case $q = 13$ with a primitive element $\beta = 2$

t	β^t	$\beta^t + 1$	$log_\beta\ (\beta^t + 1\ )$ **(mod 12)**	**(mod 3)**
*	0	1	0	0
0	1	2	1	1
1	$\beta = 2$	3	4	1
2	$\beta^2 = 4$	5	9	0
3	$\beta^3 = 8$	9	8	2
4	$\beta^4 = 16 = 3$	4	2	2
5	$\beta^5 = 6$	7	11	2
6	$\beta^6 = 12$	0	**0**	**0**
7	11	12	6	0
8	9	10	10	1
9	5	6	5	2
10	10	11	7	0
11	7	8	3	0

Array structure of Sidelnikov sequences

- **(Yu-Gong-10)**

  Write a sidelnikov sequence of period $q^2 - 1$ as an array of size $(q-1) \times (q+1)$.

  1) the first column sequence is always a multiple of a Sidelnikov sequence of period $q - 1$.
  2) other column sequences (not necessarily a sidelnikov sequence) have GOOD correlations.

- They used cyclically distinct column sequences in the array to construct a new family, with the set size comparable to those in (No-08, Yang-09).
- The construction is still a combination of adopting **constant multiples** and **shift-and-add sequences of a sidelnikov sequence of period $q-1$** in addition to **column sequences and their constant multiples from the array structure of a sidelnikov sequence of period q^2-1**.

Example (Yu-Gong-10)

- Let $q = 7,\ M = 6.$ A 6-ary Sidelnikov sequence $s(t)$ of period $q^2 - 1 = 48$ is represented by 6×8 array as follows:

$$s(t) = [v_0(t), v_1(t), v_2(t), v_3(t), v_4(t), v_5(t), v_6(t), v_7(t)]$$

$$= \begin{bmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{bmatrix}.$$

- $v_l(t) = s\big((q+1)t + l\big)$ for $0 \le t \le q-2$ and each $l = 0,1,2,\ldots,q$.
  - $v_0(t) = 2s'(t)$, where $s'(t) = (2,4,1,0,5,3)$ is a 6-ary Sidelnikov sequence of period 6.
  - $v_l(t) = v_{q+1-l}(t+1-l)$ for $0 \le t \le q-2$ and each $l = 1,2,\ldots,q$.

◆ Theorem (Yu-Gong-10)

Column sequences $v_l(t)$ of the array can be represented as

$$\boldsymbol{v_l(t) = \log_\beta V_l(\beta^t)}$$

where $V_l(x) = \beta^l x^2 + Tr_q^{q^2}(\alpha^l)x + 1$.

◆ Theorem (Yu-Gong-10)

Let $\mathcal{U}$ be the set of sequences of period $q-1$ given as follows:

$$\mathcal{U} = \{cs(t) | 1 \le c \le M-1\}$$
$$\cup \left\{ c_0 s(t) + c_1 s(t+l_1) \middle| 1 \le l_1 \le \left\lfloor \frac{q-1}{2} \right\rfloor \right\}$$
$$\cup \left\{ c_2 v_{l_2}(t) \middle| 1 \le l_2 \le \lfloor q/2 \rfloor \right\}$$

① The maximum correlation of $\mathcal{U}$ is upper bounded by $3\sqrt{q}+5$.

② This family have size $\frac{M(M-1)(q-2)}{2} + M - 1$.

Recently (2010-current) by Kim-Song

- **D.S. Kim, 2010**: A family of sequences with large size and good correlation property arising from *M*-ary Sidelnikov sequences of period q^d -1, arXiv:1009.1225v1 [cs.IT]

  - Why not considering a sidelnikov sequence of period $q^3 - 1,\ q^4 - 1$ or $q^k - 1$ in general in the first place and then using an array of size $(q-1) \times (\frac{q^k - 1}{q-1})$?

YONSEI UNIVERSITY

Generalization of the Array Structure

- **Theorem**

  Let $k \geq 2$, and write a Sidelnikove sequence of length $q^k - 1$ as an array of size $(q-1) \times (\frac{q^k-1}{q-1})$.

  Then, the column sequences $v_l(t)$ of the array can be represented as

$$\boldsymbol{v_l(t) = \log_\beta f_l(\beta^t)} \quad \textbf{(mod M)}$$

  where

$$f_l(x) = N(\alpha^l x + 1).$$

Main result

Assume that $(k, q-1) = 1,\ k < \frac{\sqrt{q}-\frac{2}{\sqrt{q}}+1}{2}$.

Construct a family

$$\boldsymbol{\Sigma} = \{\, \boldsymbol{c v_l(t)} \mid\ \mathbf{1} \le \boldsymbol{c} < \boldsymbol{M} \text{ and } \boldsymbol{l} \in \boldsymbol{\Lambda} \backslash \{\mathbf{0}\} \,\}$$

where Λ is the set of all the representatives from each q-cyclotomic coset mod $\frac{q^k-1}{q-1}$.

Then

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

②The asymptotic size of the family is $\frac{(M-1)q^{k-1}}{k}$ as $q \to \infty$.

Example

Let $q = 7, M = 6, k = 3$. Consider finite field $GF(343)$.

Then 6-ary Sidelnikov sequence $s(t)$ of period 342 is

represented by the 6×57 array as follows:

$$s(t) = [v_0(t), v_1(t), \cdots, v_{55}(t), v_{56}(t)]$$

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6
0	4	0	1	5	4	3	4	0	4	1	5	5	0	0	3	4	2	4	3	2	1	3	0	1	1	4	0	5	4	0	3	4	2	0	4	3	2	1	2	1	2	3	3	2	3	0	5	3	4	0	3	3	4	3	3	0
3	0	5	4	5	3	4	0	1	5	1	4	5	1	5	2	2	3	5	5	5	4	4	1	4	4	1	5	5	0	2	2	4	3	0	3	5	2	2	5	5	0	4	4	0	0	2	2	3	0	1	2	4	0	5	4	1
3	1	3	1	2	2	5	1	5	2	5	2	4	1	3	5	1	3	0	3	4	1	1	0	4	5	2	5	2	0	4	0	1	1	1	2	1	3	1	3	3	5	5	2	1	2	2	0	2	1	5	5	1	0	1	2	5
0	3	1	1	1	3	2	3	0	2	1	4	5	5	1	5	0	5	0	5	2	1	3	3	4	5	5	4	1	4	2	0	4	4	1	3	4	2	2	0	4	3	2	1	0	4	3	1	5	3	0	5	3	4	4	1	0
3	2	0	2	4	3	2	2	2	0	0	1	0	1	0	1	4	4	5	3	4	2	1	5	3	5	4	5	4	4	5	2	0	1	5	3	4	0	1	2	1	1	2	0	3	2	2	0	5	2	2	1	1	4	4	0	2
0	4	2	3	5	5	0	4	3	3	0	2	0	0	2	3	3	3	5	5	1	3	5	2	5	2	2	0	5	1	3	2	0	1	1	5	4	0	2	4	3	0	0	4	5	5	0	3	1	4	3	3	5	1	4	4	3

- $v_l(t) = v_{lq}(t)$.
- If $l_1 \equiv l_2 \bmod \frac{q^k - 1}{q - 1}$, then $v_{l_1}(t)$ and $v_{l_2}(t)$ are cyclically equivalent.

- Roughly, $k < \frac{\sqrt{q}}{2}$.

Asymptotic size is $\frac{q^{k-1}}{k}(M-1)$.

- Size of some column sequence families

q	$7^2 = 49$	$11^2 = 121$	$13^2 = 169$	$3^5 = 243$	$2^8 = 256$	$17^2 = 289$	$7^3 = 343$
$k = 2$	24	60	84	121	128	144	171
Asymp.	24	60	84	121	128	144	171
$k = 3$	816	4921	9577	19764	21931	27937	39331
Asymp.	800	4880	9520	19683	21845	27840	39216
$k = 4$	X	446581	1213885	3602050	4210752	6055345	10117900
Asymp.	X	442890	1206702	3587226	4194304	6034392	10088401

In all the values of the table, the constant factor $M - 1 = 5$ is omitted.

Comparison of the Families so far

- The following M–ary sequence families have period $q-1$:

Family	Size	C_{max}	Remark
Song-07	$M-1$	$\sqrt{q}+3$	**Constant multiples**
Yang-09, No-08	$\frac{(q-3)}{2}(M-1)^2+\frac{M(M-1)}{2}$	$3\sqrt{q}+5$	**+ Shift-and-add**
Yu-Gong-10 (1)	$\frac{(q-3)(q-5)}{8}(M-1)^3+\cdots$	$5\sqrt{q}+7$	+ more Shift-and-add
Yu-Gong-10 (2)	$\frac{(q-2)}{2}M(M-1)+M-1$	$3\sqrt{q}+5$	**+ array structure**
Kim-10	$\frac{q^{k-1}}{k}(M-1)$ as q approached ∞	$(2k-1)\sqrt{q}+1$	Generalization of array

Still More to Come: Decimation Sequences

- **Definition:** Let $a(t)$ be a sequence of period L. Then d-decimation sequence $b(t)$ of $a(t)$ is

$$b(t) = a(dt), \text{ for } t = 0,1,....$$

- **Can we add some decimations of the members** (either sidelnikov sequence or column sequences of the array sturcture) **without increasing the max correlation (around** $3\sqrt{q}+5$**) ?**
  - Yes, we may….
  - will be coming soon **^.^**

CCL

YONSEI UNIVERSITY