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

ITA 2013 @ UCSD, San Diego
Feb 10-15, 2013

Hong-Yeop Song
School of EEE
Yonsei University

and

Dae San Kim
Dept. Math
Sogang 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 $q - 1$


(Lempel-Cohn-Eastman-77)
Re-discovered binary “Sidelnikov sequences”

  - Sarwate, Comments on… 1978.
Power Residue Sequences of period $p$

- $p$ = an odd prime
- $\beta$ = 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 $0 \leq k \leq M - 1$

- An $M$-ary PRS of period $p$ is defined as, for $t = 0, 1, ..., p-1$,

  $$s(t) = \begin{cases} 
  0, & \text{if } t = 0 \\
  k, & \text{if } t \in C_k 
  \end{cases}$$
Sidelnikov Sequences of period \( q-1 \)

- \( GF(q) = \) finite field of size \( q \) where \( q = p^n \)
- \( \beta = \) 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 \( 0 \leq k \leq M-1 \)

An \( M \)-ary Sidelnikov sequence of period \( q - 1 \) is defined as, for \( t = 0, 1, 2, \ldots, q-2, \)

\[
s(t) = \begin{cases} 
0, & \text{if } \beta^t + 1 = 0 \\
k, & \text{if } \beta^t + 1 \in C_k 
\end{cases}
\]
Comparison

- An $M$-ary Power Residue Sequence of period $p$:

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

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

$$s(t) = \begin{cases} 0, & \text{if } \beta^t + 1 = 0 \\ k, & \text{if } \beta^t + 1 \in C_k \end{cases}$$
(Examples) \( p = q = 13, \; M = 3, \; \beta = 2 \)

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

<table>
<thead>
<tr>
<th>( t )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>SS</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( t )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \beta^t )</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>3</td>
<td>6</td>
<td>12</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>10</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>( \beta^t + 1 )</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>4</td>
<td>7</td>
<td>0</td>
<td>12</td>
<td>10</td>
<td>6</td>
<td>11</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
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.
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 \( \sqrt{q} + 3 \)
  - \( \rightarrow \) 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


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 $4\left\lfloor 2\sqrt{p/4} \right\rfloor + 1$
It is proved by Rushanan at ISIT-06


- **Main Result:**

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

- **Major Technique:**

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

  product of 4 linear polynomials

  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

- $\psi = \text{multiplicative character of } GF(q)^* \text{ of order } M$, where $M | q - 1$:
  
  $$\psi(x) = \exp\left(\frac{j2\pi}{M} \log_\alpha x\right) \text{ with } \psi(0) = 0$$

(Weil-48) Let $\psi$ 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 $M$th 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

$$\left| \sum_{x \in GF(q)} \psi(cf(x)) \right| \leq (d - 1)\sqrt{q}$$
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 $T = \lceil (q - 1)/2 \rceil$.

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

$$\mathcal{L} = \{ c_1 s(t) \mid 1 \leq c_1 \leq M - 1 \}$$

$$\cup \{ c_1 s(t) + c_2 s(t + l) \mid 1 \leq c_1, c_2 \leq M - 1, \ 1 \leq l \leq T - 1 \}$$

$$\cup \{ c_1 s(t) + c_2 s(t + T) \mid 1 \leq c_1 < c_2 \leq M - 1 \}$$

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

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

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**

<table>
<thead>
<tr>
<th>Family</th>
<th>Period $L$</th>
<th>Alphabet</th>
<th>$C_{max}$</th>
<th>Family size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_r^{0}$ (or $\tilde{F}_r$ [24])</td>
<td>$p$</td>
<td>$M$</td>
<td>$2\sqrt{L} + 5$</td>
<td>$(L+1) \cdot (M-1)$</td>
</tr>
<tr>
<td>$L_r$ (or $F_r$ [24])</td>
<td>$p$</td>
<td>$M$</td>
<td>$3\sqrt{L} + 4$</td>
<td>$M - 1 + \frac{(M-1)^2(L-1)}{2}$</td>
</tr>
<tr>
<td>$G_r^{(s,2)}$, $\delta \neq 0$ (in this paper)</td>
<td>$p$</td>
<td>$M$</td>
<td>$4\sqrt{L} + 7$</td>
<td>$(M - 1) + \frac{(L-1)}{2} \cdot (M - 1)^2 + \frac{(L-1)(L-3)}{8} \cdot (M^2 - 3M + 3)$</td>
</tr>
<tr>
<td>$H_r^{(2)}$ (in this paper)</td>
<td>$p$</td>
<td>$M$</td>
<td>$5\sqrt{L} + 6$</td>
<td>$(M - 1) + \frac{(L-1)}{2} \cdot (M - 1)^2 + \frac{(L-1)(L-3)}{8} \cdot (M - 1)^3$</td>
</tr>
<tr>
<td>$S_s^{0}$ (or $\tilde{F}_s$ [24])</td>
<td>$p^m - 1$</td>
<td>$M$</td>
<td>$2\sqrt{L + 1} + 6$</td>
<td>$(M - 1) \cdot \left(\frac{L}{2}\right) + \left[\frac{M-1}{2}\right] + \frac{M(M-1)}{2}$</td>
</tr>
<tr>
<td>$L_s$ (or $L$ [23])</td>
<td>$p^m - 1$</td>
<td>$M$</td>
<td>$3\sqrt{L + 1} + 5$</td>
<td>$(M - 1)^2(L-2) + M(M-1)^2$</td>
</tr>
<tr>
<td>$G_s^{(s,2)}$, $\delta \neq 0$ (in this paper)</td>
<td>$p^m - 1$</td>
<td>$M$</td>
<td>$4\sqrt{L + 1} + 8$</td>
<td>$(M - 1) + \frac{(L-2)}{2} \cdot (M - 1)^2 + \frac{(L-2)(L-4)}{8} \cdot (M^2 - 3M + 3)$</td>
</tr>
<tr>
<td>$H_s^{(2)}$ (in this paper)</td>
<td>$p^m - 1$</td>
<td>$M$</td>
<td>$5\sqrt{L + 1} + 7$</td>
<td>$(M - 1) + \frac{(L-2)}{2} \cdot (M - 1)^2 + \frac{(L-2)(L-4)}{8} \cdot (M - 1)^3$</td>
</tr>
</tbody>
</table>
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 $(q-1) \times (q+1)$
- 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 $f_1(x), \ldots, f_l(x)$ be $l$ monic and irreducible polynomial over $GF(q)$ which have positive degrees $d_1, \ldots, d_l$, 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 $\psi_1, \ldots, \psi_l$ 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 $a_i \in \mathbb{F}_q \setminus \{0\}$,

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq (d - 1) \sqrt{q} + \sum_{i=1}^{l} e_i.$$
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 \( q \)
- \( \beta \) = primitive element of \( GF(q) \)
- \( D_k = \{ \beta^{Mi+k} - 1 | 0 \leq i < \frac{q-1}{M} \} \) for \( 0 \leq k \leq M - 1 \).

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

\[
s(t) \equiv \log_\beta (\beta^t + 1) \pmod{M}, \quad 0 \leq t \leq q - 2
\]
\[ s(t) \equiv \log_\beta (\beta^t + 1) \pmod{M} \]

Is this the **ADDONE table (Zech Log)** of finite field?

- Consider the case \( q = 13 \) with a primitive element \( \beta = 2 \)

<table>
<thead>
<tr>
<th>( t )</th>
<th>( \beta^t )</th>
<th>( \beta^t + 1 )</th>
<th>( log_\beta (\beta^t + 1) \pmod{12} )</th>
<th>( \pmod{3} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>( \beta = 2 )</td>
<td>3</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>( \beta^2 = 4 )</td>
<td>5</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>( \beta^3 = 8 )</td>
<td>9</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>( \beta^4 = 16 = 3 )</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>( \beta^5 = 6 )</td>
<td>7</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>( \beta^6 = 12 )</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>11</td>
<td>12</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>6</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>7</td>
<td>8</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
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 $6 \times 8$ array as follows:

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

\[
\begin{bmatrix}
4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\
2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\
2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\
0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\
4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\
0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \\
\end{bmatrix}.
\]

- $v_l(t) = s((q + 1) t + l)$ for $0 \leq t \leq q - 2$ 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 $0 \leq t \leq q - 2$ and each $l = 1, 2, \ldots, q$. 

Example (Yu-Gong-10)
Theorem (Yu-Gong-10)

Column sequences \( \nu_l(t) \) of the array can be represented as

\[
\nu_l(t) = \log_\beta V_l(\beta^t)
\]

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:

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

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 $(q - 1) \times \left(\frac{q^k - 1}{q-1}\right)$?
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 $(q - 1) \times \left(\frac{q^k - 1}{q - 1}\right)$.

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

$$\nu_l(t) = \log_\beta f_l(\beta^t) \pmod{M}$$

where

$$f_l(x) = N(\alpha^lx + 1).$$
Main result

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

Construct a family

$$\Sigma = \{ cv_l(t) \mid 1 \leq c < M \text{ and } l \in \Lambda \setminus \{0\} \}$$

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

Then

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

2. The 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 $\mathbb{GF}(343)$.
Then 6-ary Sidelnikov sequence $s(t)$ of period 342 is represented by the $6 \times 57$ array as follows:

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

- $v_l(t) = v_{lq}(t)$.
- If $l_1 \equiv l_2 \mod \frac{q^k-1}{q-1}$, then $v_{l_1}(t)$ and $v_{l_2}(t)$ are cyclically equivalent.
Roughly, $k < \frac{\sqrt{q}}{2}$.

Size of some column sequence families

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

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

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 $q - 1$:

<table>
<thead>
<tr>
<th>Family</th>
<th>Size</th>
<th>$c_{max}$</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Song-07</td>
<td>$M - 1$</td>
<td>$\sqrt{q} + 3$</td>
<td>Constant multiples</td>
</tr>
<tr>
<td>Yang-09, No-08</td>
<td>$\frac{(q - 3)}{2}(M - 1)^2 + \frac{M(M - 1)}{2}$</td>
<td>$3\sqrt{q} + 5$</td>
<td>+ Shift-and-add</td>
</tr>
<tr>
<td>Yu-Gong-10 (1)</td>
<td>$\frac{(q - 3)(q - 5)}{8}(M - 1)^3 + \ldots$</td>
<td>$5\sqrt{q} + 7$</td>
<td>+ more Shift-and-add</td>
</tr>
<tr>
<td>Yu-Gong-10 (2)</td>
<td>$\frac{(q - 2)}{2}M(M - 1) + M - 1$</td>
<td>$3\sqrt{q} + 5$</td>
<td>+ array structure</td>
</tr>
<tr>
<td>Kim-10</td>
<td>$\frac{q^{k-1}}{k}(M - 1)$ as $q$ approached $\infty$</td>
<td>$(2k - 1)\sqrt{q} + 1$</td>
<td>Generalization of array</td>
</tr>
</tbody>
</table>
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 sidelinkov sequence or column sequences of the array structure) **without increasing the max correlation** (around $3\sqrt{q} + 5$)?

- Yes, we may....
- will be coming soon ^_^