Some properties of NTU sequences

Gangsan Kim and Hong-Yeop Song

Yonsei University, Seoul, Korea

2018 International Symposium on Information Theory and Its Applications

Notation

- q is an odd prime power.
- $\mathbb{F}_q$ is the finite field with q elements.
- $\mathbb{F}_{q^n}$ is the finite field with q^n elements.
- α is a primitive element of $\mathbb{F}_{q^n}$.
- $\mathrm{Tr}_1^n(x) \in \mathbb{F}_q$ is the trace function of $x \in \mathbb{F}_{q^n}$ defined by

$$\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{q^i}$$

- The periodic autocorrelation function of a binary sequence $\boldsymbol{s} = \{s_t \,|t = 0,1,2,\dots\}$ of period L is defined as $C_{\boldsymbol{s}}(\tau) = \sum_{t=0}^{L-1}(-1)^{s_t + s_{t+\tau}}$
- A binary sequence $\boldsymbol{s} = \{s_t \,|t = 0,1,2,\dots\}$ of period 2L, is a anti periodic if $s_t + s_{t+\tau} = 1$ for all t
- $\chi(x)$ is a quadratic character of $x \in \mathbb{F}_q$ defined as

$$\chi(x) = \begin{cases} 0, & x = 0 \\ 1, & x \text{ is a quadratic element of } \mathbb{F}_q \\ -1, & x \text{ is not a quadratic element of } \mathbb{F}_q \end{cases}$$

Proposed Sequence

A sequence $\mathbf{s} = \{s_t | t = 0,1,2,\dots\}$ of period $2\frac{q^n-1}{q-1}$ is defined as

$$s_t = \begin{cases} 1 & \text{if } \chi\left(\mathrm{Tr}_1^n(\alpha^t)\right) = +1 \\ 0 & \text{otherwise} \end{cases}$$

for $t = 0, 1, 2, \dots, \frac{q^n-1}{q-1} - 1$, and

$$s_t = \begin{cases} 0 & \text{if } \chi\left(\mathrm{Tr}_1^n(\alpha^t)\right) = -1 \\ 1 & \text{otherwise} \end{cases}$$

for $t = \frac{q^n-1}{q-1}, \frac{q^n-1}{q-1} + 1, \frac{q^n-1}{q-1} + 2, \dots, 2\frac{q^n-1}{q-1} - 1.$

Properties of proposed sequences

- The proposed sequence is modified at some positions of $\mathrm{Tr}_1^n(\alpha^t) = 0$ in the NTU sequences.
- It has balance property, and it is anti-periodic
- It has following 5-level autocorrelation profile

- **NTU sequences[3]**
  - The NTU sequences $\boldsymbol{s} = \{s_t \,|t = 0,1,2,\dots\}$ are defined by

$$s_t = \begin{cases} 1, & \chi(\mathrm{Tr}_1^n(\alpha^t)) = 1 \\ 0, & \text{otherwise} \end{cases}$$

  - Period: $2\frac{q^n-1}{q-1}$, 3-level autocorrelation

- **Relative difference sets[1]**
  - $D = \{d_1, d_2, \dots, d_k\} \subset \mathbb{Z}_{uw}$ is a $(u, w, k, \lambda) - RDS$ if it satisfies following two conditions

$$\text{I}.\ \{d_i - d_j \mid d_i \neq d_j, for\ d_i, d_j \in D\} = \mathbb{Z}_{uw} \backslash u\mathbb{Z}_{uw}$$

$$\text{II}.\ \text{For any } d \text{ in } \mathbb{Z}_{uw} \backslash u\mathbb{Z}_{uw}, \text{ the congruence } d_i - d_j \equiv d \text{ in } \mathbb{Z}_{uw} \text{ has exactly } \lambda \text{ Solution pairs}(d_i, d_j) \text{ with } d_i, d_j \in D$$

- **Theorem1[1].**
  The set $\mathrm{U} = \{t \mid \chi(Tr_1^n(\alpha^t)) = 1, 0 \leq t < 2\frac{q^n-1}{q-1}\}$ is a $(\frac{q^n-1}{q-1}, 2, q^{n-1}, q^{n-2}(\frac{q-1}{2}))$-RDS

- **Relation between NTU sequences and RDS**
  - NTU sequences are the characteristic sequences of RDS in Theorem 1.
  - Their 3-level autocorrelation property comes from the property of RDS

- **Theorem 2(Autocorrelation profile).**
  Consider the case where $n = 2$ of the proposed anti-periodic sequence $\boldsymbol{s}$. Then $\boldsymbol{s}$ have period $2(q+1)$, and $C_{\boldsymbol{s}}(\tau)$=

$$\begin{cases} 2(q+1), & \tau = 0 \\ -2(q+1), & \tau = q+1 \\ 0, & \text{all odd } \tau(\text{case a}) \text{ or all the remaining even } \tau(\text{case b}) \\ 4, & \text{some even } \tau, \frac{q-1}{2} \text{times(case a) or some odd } \tau, \frac{(q+1)}{2} \text{times(case b)} \\ -4, & \text{all the remaining even } \tau(\text{case a}) \text{ or all the remaining odd } \tau(\text{case b}) \end{cases}$$

  * case a: $\frac{(q+1)}{2}$ is odd, case b: : $\frac{(q+1)}{2}$ is even.

  - For the case n = 2,It would be considered to be good since their minor peak is only 4 regardless of q.

- **Reference**

[1]J. Elliott and A. Butson, “Relative difference sets,” *Illinois J. Math.*, 10, pp. 517–531, 1966.
[2] H. D. Luke, H. F. Shotten, “Odd-perfect, almost binary correlation sequences,” *IEEE reans. Aerosp, Electron. Systems,* 31(1), pp. 495–498, 1995.
[3] Y. Nogami, K. Tada, S. Uehara, “A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties,” *IEICE Trans. Fundamentals*, E.97-A(12), pp. 2336–2342, 2014.
[4] A. Pott, “Finite geometry and character theory,” *Springer*, 1995.on , pp. 755-760.