New Construction of Quaternary Sequences with Good Correlation Using Binary Sequences with Good Correlation

Tae-hyung Lim, Ji-Youp Kim, Jong-Seon No,
and Habong Chung

Seoul National University
Hongik University

May 28, 2010

Outline

Outline

Well-Known Binary Sequences and Families

- m-sequences
- GMW sequences
- Legendre sequences
- Gold sequence families
- Small set of Kasami sequences
- Set of No sequences

Quaternary Sequences with good autocorrelation

- Schotten's complementary-based sequences (2003)
  - Good autocorrelation for odd period
  - Almost binary
- Luke, Schotten, and Hadinejad-Mahram (2003)
  - Good autocorrelation for even period
  - Almost binary
- Jang, Kim, Kim and No (2009)
  - ideal autocorrelation, balanced
  - 0, 2 for even indices and 1, 3 for odd indices
- X.Tang, T.Helleseth, and P.Fan (2009)
  - Families with Good autocorrelation property
  - Constructed from Galois rings

In this presentation...

- Construction of quaternary sequences of even period with ideal autocorrelation and balance properties is presented.
- Uses the reverse Gray mapping and binary sequences of odd period with ideal autocorrelation.
- Autocorrelation distribution is derived.
- Construction of quaternary sequence families of even period is proposed.
- Family size and the maximum absolute value of correlation are derived.

Outline

Balancedness, Correlations

- $g(t)$: q-ary sequence of period N
- $g(t)$ is balanced if all the differences among numbers of occurrences of each element in a period are less than or equal to one.
- Autocorrelation function $R_g(\tau)$ of $g(t)$ is defined as

$$R_g(\tau) = \sum_{t=0}^{N-1} \omega_q^{g(t)-g(t+\tau)}$$

- Cross-correlation function $R_{g_1 g_2}(\tau)$ of $g_1(t)$, $g_2(t)$ is defined as

$$R_{g_1 g_2}(\tau) = \sum_{t=0}^{N-1} \omega_q^{g_1(t)-g_2(t+\tau)}$$

Ideal Autocorrelation

- A binary sequence $g(t)$ of odd period N has the ideal autocorrelation property if

$$R_g(\tau) = \begin{cases} N, & \text{onces} \\ -1, & N-1 \text{ times.} \end{cases}$$

- A quaternary sequence $g(t)$ of even period N has the ideal autocorrelation property if

$$R_g(\tau) = \begin{cases} N, & \text{onces} \\ 0, & N/2 \text{ times} \\ -2, & N/2-1 \text{ times} \end{cases}$$

or

$$R_g(\tau) = \begin{cases} N, & \text{onces} \\ 0, & N/2-1 \text{ times} \\ -2, & N/2 \text{ times.} \end{cases}$$

Welch Bound

- $\mathcal{F}$: family of sequence
- N : period of sequence
- M : size of family
- C_{max} : Maximum absolute value of all nontrivial autocorrelation and cross-correlation in the family.

$$(C_{max})^{2k} \geqslant \frac{1}{MN-1}\{\frac{MN^{2k+1}}{\binom{k+N-1}{N-1}} - N^{2k}\}$$

- can be approximated as $\sqrt{N}$.

Reverse Gray Mapping

$$\phi[s_0, s_1] = \begin{cases} 0, & \text{if } (s_0, s_1) = (0, 0) \\ 1, & \text{if } (s_0, s_1) = (0, 1) \\ 2, & \text{if } (s_0, s_1) = (1, 1) \\ 3, & \text{if } (s_0, s_1) = (1, 0). \end{cases}$$

- For two binary sequence $s_0(t)$, $s_1(t)$ of period N, $q(t) = \phi[s_0(t), s_1(t)]$ is a quaternary sequence of period N.

$$\omega_4^{q(t)} = \frac{1+\omega_4}{2}(-1)^{s_0(t)} + \frac{1-\omega_4}{2}(-1)^{s_1(t)}.$$

Cross-correlation of the quaternary sequences

Theorem 1 [6] Let $s_0(t)$, $s_1(t)$, $s_2(t)$, and $s_3(t)$ be binary sequences of the same period. Let $q_0(t)$ and $q_1(t)$ be quaternary sequences defined by $q_0(t) = \phi[s_0(t), s_1(t)]$ and $q_1(t) = \phi[s_2(t), s_3(t)]$, respectively. Then the cross-correlation function $R_{q_0q_1}(\tau)$ between $q_0(t)$ and $q_1(t)$ is given as

$$R_{q_0q_1}(\tau) = \frac{1}{2}\{R_{s_0s_2}(\tau) + R_{s_1s_3}(\tau) + \omega_4(R_{s_0s_3}(\tau) - R_{s_1s_2}(\tau))\}$$

where $R_{s_is_j}(\tau)$ is the cross-correlation function of $s_i(t)$ and $s_j(t)$.

Outline

Construction of Sequences

- $a(t)$, $b(t)$ be two binary sequences of odd period N with the ideal autocorrelation.
- Define binary sequences $s_0(t)$, $s_1(t)$ of $2N$ as

$$s_0(t) = \begin{cases} a(t), & \text{for } t = 0 \bmod 2 \\ a(t), & \text{for } t = 1 \bmod 2 \end{cases}$$

$$s_1(t) = \begin{cases} b(t), & \text{for } t = 0 \bmod 2 \\ b(t) \oplus 1, & \text{for } t = 1 \bmod 2 \end{cases}$$

- Define a quaternary sequence $q(t)$ as

$$q(t) = \phi[s_0(t), s_1(t)] \tag{1}$$

Balance Property

Lemma 2 Let $q(t)$ be the quaternary sequences defined as in (1). If $a(t)$ has the balance property, then $q(t)$ also has the balance property, i.e.,

$$q(t) = \begin{cases} 0, & \frac{N-1}{2} \text{ times} \\ 1, & \frac{N-1}{2} \text{ times} \\ 2, & \frac{N+1}{2} \text{ times} \\ 3, & \frac{N+1}{2} \text{ times.} \end{cases}$$

Balance Property

Proof Let B_i, $i = 0, 1, 2, 3$ be the numbers defined by

$$B_i = |\{t|q(t) = i, 0 \leqslant t < 2N\}|.$$

If we define N_0, N_1, N_2, and N_3 as

$$\begin{aligned}
N_0 &= |\{t|a(t) = 0 \text{ and } b(t) = 0, 0 \leqslant t < N\}| \\
N_1 &= |\{t|a(t) = 0 \text{ and } b(t) = 1, 0 \leqslant t < N\}| \\
N_2 &= |\{t|a(t) = 1 \text{ and } b(t) = 1, 0 \leqslant t < N\}| \\
N_3 &= |\{t|a(t) = 1 \text{ and } b(t) = 0, 0 \leqslant t < N\}|
\end{aligned}$$

then, by using the definition in (2), we have

$$\begin{aligned}
B_0 = B_1 = N_0 + N_1 &= |\{t|a(t) = 0, 0 \leqslant t < N\}| \\
B_2 = B_3 = N_2 + N_3 &= |\{t|a(t) = 1, 0 \leqslant t < N\}|.
\end{aligned}$$

Balance Property

Proof Since $a(t)$ has the balance property, it is clear that

$$N_0 + N_1 = \frac{N-1}{2}$$
$$N_2 + N_3 = \frac{N+1}{2}.$$

Autocorrelation

Lemma 3 Let $q(t)$ be the quaternary sequence defined in (1). Then autocorrelation distribution of $q(t)$ can be expressed as

$$R_q(\tau) = \begin{cases} R_a(\tau) + R_b(\tau), & \text{for } \tau = 0 \bmod 2 \\ R_a(\tau) - R_b(\tau), & \text{for } \tau = 1 \bmod 2 \end{cases}$$

Proof From Theorem 1, $R_q(\tau)$ can be rewritten as

$$R_q(\tau) = \frac{1}{2}\{R_{s_0}(\tau) + R_{s_1}(\tau) + \omega_4(R_{s_0 s_1}(\tau) - R_{s_1 s_0}(\tau))\}.$$

Autocorrelation

Proof From the definition of $s_0(t)$ and $s_1(t)$, the autocorrelation functions $R_{s_0}(\tau)$ and $R_{s_1}(\tau)$ and $s_0(t)$ and $s_1(t)$ are expressed as

$$R_{s_0}(\tau) = 2R_a(\tau)R_{s_1}(\tau) = \begin{cases} 2R_b(\tau), & \text{for } \tau = 0 \bmod 2 \\ -2R_b(\tau), & \text{for } \tau = 1 \bmod 2. \end{cases}$$

From the definition of $s_0(t)$ and $s_1(t)$, it is easy to check that

$$s_0(t) + s_1(t+\tau) = s_0(t+N) + s_1(t+N+\tau) \oplus 1, 0 \leqslant t < N,$$

and thus we have

$$R_{s_0 s_1}(\tau) = R_{s_1 s_0}(\tau) = 0.$$

Balancedness and Ideal Autocorrelation

Theorem 4 Let $a(t)$ and $b(t)$ be two binary sequences of odd period N with the ideal autocorrelation. Then, a quaternary sequence $q(t)$ in (1) of period $2N$ has the ideal autocorrelation and balance properties with the following distribution

$$R_q(\tau) = \begin{cases} 2N, & \text{for } \tau = 0 \\ 0, & \text{for } \tau = 1 \bmod 2 \\ -2, & \text{for } \tau = 0 \bmod 2 \text{ and } \tau \neq 0. \end{cases}$$

Proof It is balanced by Lemma 2. Since $a(t)$ and $b(t)$ have the ideal autocorrelation property, by Lemma 3, the theorem follows.

Example

- $a(t)$: binary m-sequence of period 63

$$a(t) = 000001000011000101001111010001110010010110111011001101010111111.$$

- $b(t)$: binary GMW sequence of period 63

$$b(t) = 011110111001111010010110111010001101011001101000111010001000000.$$

- $q(t)$: quaternary sequence of period 126

$$q(t) = 001012101133101212003322131112321030031230222132102212021232323110103010022010303112233020003230121120321333023013303130323232.$$

Example

- Autocorrelation of $q(t)$ is calculated as

$$R_q(\tau) = \begin{cases} 126, & \text{for } \tau = 0 \\ 0, & \text{for } \tau = 1 \bmod 2 \\ -2, & \text{for } \tau = 0 \bmod 2 \text{ and } \tau \neq 0. \end{cases}$$

Outline

Construction of Quaternary Sequence Families

- $\mathcal{F}_a = \{a_i(t) | 0 \leqslant t < N, 0 \leqslant i < M_a\}$
- $\mathcal{F}_b = \{b_i(t) | 0 \leqslant t < N, 0 \leqslant i < M_a\}$
  - binary sequence families of odd period N
- $s_{i0}(t)$, $s_{i1}(t)$: binary sequences of period $2N$ defined by

$$s_{i0}(t) = \begin{cases} a_i(t), & \text{for } t = 0 \bmod 2 \\ a_i(t), & \text{for } t = 1 \bmod 2 \end{cases}$$

$$s_{i1}(t) = \begin{cases} b_i(t), & \text{for } t = 0 \bmod 2 \\ b_i(t) \oplus 1, & \text{for } t = 1 \bmod 2 \end{cases}$$

Construction of Quaternary Sequence Families

- $M_q = \min(M_a, M_b)$
- Quaternary sequence family $\mathcal{F}_q$ is defined as

$$\mathcal{F}_q = \{q_i(t) | 0 \leqslant t < 2N, 0 \leqslant i < M_q\} \tag{2}$$

where

$$q_i(t) = \phi[s_{i0}(t), s_{i1}(t)] \tag{3}$$

Cross-correlation of Quaternary Sequences

Lemma 5 Let $q_i(t)$ and $q_j(t)$ be two quaternary sequences defined in (3). Then cross-correlation function between $q_i(t)$ and $q_j(t)$ can be expressed as

$$R_{q_iq_j}(\tau) = \begin{cases} R_{a_ia_j}(\tau) + R_{b_ib_j}(\tau), & \text{for } \tau = 0 \bmod 2 \\ R_{a_ia_j}(\tau) - R_{b_ib_j}(\tau), & \text{for } \tau = 1 \bmod 2. \end{cases}$$

Proof From Theorem 1, $R_{q_iq_j}(\tau)$ can be rewritten as

$$R_{q_iq_j}(\tau) = \frac{1}{2}\{R_{s_i0s_j0}(\tau) + R_{s_i1s_j1}(\tau) + \omega_4(R_{s_i0s_j1}(\tau) - R_{s_i1s_j0}(\tau))\}.$$

Cross-correlation of Quaternary Sequences

Proof From the definition of $s_i0(t)$, $s_i1(t)$, $s_j0(t)$, and $s_j1(t)$, the cross-correlation functions $R_{i0j0}(\tau)$ and $R_{i1j1}(\tau)$ are expressed as

$$R_{s_i0s_j0}(\tau) = 2R_{a_ia_j}(\tau)$$

$$R_{s_i1s_j1}(\tau) = \begin{cases} 2R_{b_ib_j}(\tau), & \text{for } \tau = 0 \bmod 2 \\ -2R_{b_ib_j}(\tau), & \text{for } \tau = 1 \bmod 2. \end{cases}$$

Also it is easy to check that

$$s_{i0}(t) + s_{j1}(t+\tau) = s_{i0}(t+N) + s_{j1}(t+N+\tau) \oplus 1, 0 \leqslant t < N$$
$$s_{i1}(t) + s_{j0}(t+\tau) = s_{i1}(t+N) + s_{j0}(t+N+\tau) \oplus 1, 0 \leqslant t < N$$

and thus we have

$$R_{s_{i0}s_{j1}}(\tau) = R_{s_{i1}s_{j0}}(\tau) = 0.$$

C_{max} of Quaternary Sequence Family

Theorem 6 Let $\mathcal{F}_a = \{a_i(t)|0 \leqslant t < N, 0 \leqslant i < M_a\}$ and $\mathcal{F}_b = \{b_i(t)|0 \leqslant t < N, 0 \leqslant i < M_b\}$ be two binary sequence families of odd period N. And assume that both $\mathcal{F}_a$ and $\mathcal{F}_b$ are optimal with respect to the Welch bound. Then C_{max} of the quaternary sequence family $\mathcal{F}_q = \{q_i(t)|0 \leqslant t < 2N, 0 \leqslant i < M_q, M_q = min(M_a, M_b)\}$ in (2) is less than or equal to the sum of C_{max} of $\mathcal{F}_a$ and C_{max} of $\mathcal{F}_b$, which is an about $\sqrt{2}$ times of the Welch bound for $\mathcal{F}_q$.

C_{max} of Quaternary Sequence Family

Proof Let C_{max} of $\mathcal{F}_q$, $\mathcal{F}_a$, and $\mathcal{F}_b$ be $C_{q,max}$, $C_{a,max}$, and $C_{b,max}$, respectively. From Lemma 5,

$$C_{q,max} \leqslant C_{a,max} + C_{b,max}.$$

Since $\mathcal{F}_a$ and $\mathcal{F}_b$ are optimal with respect to the Welch bound, $C_{a,max}$ and $C_{b,max}$ are about $\sqrt{N}$. Since the Welch bound of the $\mathcal{F}_q$ is $\sqrt{2N}$ and the upper bound of $C_{q,max}$ is about $2\sqrt{N}$, we prove the theorem.

Example

- $\mathcal{F}_a$: a small set of Kasami sequences of period N and family size $M = \sqrt{N+1}$
  - Spectrum of correlation values is given by

$$\{-1, -1-\sqrt{N+1}, -1+\sqrt{N+1}\}$$

- $\mathcal{F}_b$: a set of No sequences of period N and family size $M = \sqrt{N+1}$
  - Same spectrum of correlation values
- $\mathcal{F}_q$: quaternary sequence family defined in (2)
  - Period $2N$ and family size $M = \sqrt{N+1}$
  - Spectrum of correlation values is given by

$$\{-2-2\sqrt{N+1}-2\sqrt{N+1}, -2-\sqrt{N+1}, -\sqrt{N+1}, -2,$$
$$0, -2+\sqrt{N+1}, \sqrt{N+1}, -2+2\sqrt{N+1}, 2\sqrt{N+1}\}$$

  - $C_{q,max} = 2+2\sqrt{N+1} \quad 2\sqrt{N} = \sqrt{2}\sqrt{2N}$

Outline

References

1. B.Gordon, W.H.Mills, and L.R.Welch, "Some new difference sets," Candian J. Math., vol, 14, no. 4, pp. 614-625, 1962.
2. T.Hellseth and P.Vijay Kumar, "Sequences with low correlation," in Handbook of Coding Theory., Elsevier Science B.V, 1998, vol.2.
3. J.-W. Jang, Y.-S. Kim, S.-H. Kim, and J.-S. No, "New quaternary sequences with ideal autocorrelation constructed from binary sequences with ideal autocorrelation," in ISIT 2009, Seoul, Korea, 2009, pp. 278-281.
4. T.Kasami, "Weight distribution formula for some class of cyclic codes," Technical Report R-285 (AD 632574), Coordinated Science Laboratory, University of Illinois, Urbana (April 1966).

References

5. Y.-S. Kim, J.-W. Jang, S.-H. Kim, and J.-S. No, "New construction of quaternary sequences with ideal autocorrelation from Legendre sequences," in ISIT 2009, Seoul, Korea, 2009, pp.282-285.
6. S.M.Krone and D.V.Sarwate, "Quadriphase sequences for spread spectrum multiple-access communicatin," IEEE Trans. Inf. Theory, vol. IT-30, no.3, pp.520-529, May 1984.
7. R.Lidl and H.Niederreiter, "Finite fields," in Encyclopedia of Mathematics and Its applications., vol.20, Reading, MA: Addison-Wesley, 1983.
8. H.Dieter Luke, H.D.Schotten, and H.Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A Survey," IEEE Trans. Inf. Theroy, vol.49, no.12, pp.3271-3282, Dec.2003.

References

9. J.-S. No and P.V.Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," IEEE Trans. Inf. Theory, vol.35, no.2, pp.371-379, Mar. 1989.
10. J.-S.No, H.-K.Lee, H.Chung, H.-Y. Song, and K.Yang, "Trace representation of Legendre Sequences of Mersenne Prime Period," IEEE Trans. Inf. Theory, vol.42, No.6, pp.2254-2255, Nov.1996.
11. R.A.Scholtz, and L.R.Welch, "GMW sequences," IEEE Trans. Inf. Theory, vol. IT-30, pp.548-553, May 1984.
12. X.Tang, T.Helleseth, and P.Fan, "A new optimal quaternary sequence family of length $2(2^n - 1)$ obtained from the orthogonal transformation of Failies $\mathcal{B}$ and $\mathcal{C}$," Des. Codes Cryptogr., vol.53, pp.137-148, Dec. 2009.
13. L.R.Welch, "Lower bounds on the maximum cross correlation of signals," IEEE Trans. Inf. Theory, vol. IT-20, pp. 397-399, May 1974.