

Binary Sequences of Even Period with 5-Level Autocorrelation and Their Variations for Optimum Odd Autocorrelation

Gangsan Kim*, Hong-Yeop Song^o

ABSTRACT

In this paper, we propose a balanced binary sequence of period $2u$ for some even values of u with 5-level autocorrelation from a cyclic relative difference set with parameters $(u, 2, u-1, \frac{u}{2}-1)$. Furthermore, we identify its half-period as those having an optimum odd autocorrelation, and we found that changing one specific bit of this binary sequence results in an almost perfect sequence. Various relations of these with some previous constructions by others are discussed.

Key Words : Binary sequences, Cyclic relative difference sets, Favourable autocorrelation

I. Introduction

Binary sequences with good autocorrelation properties are advantageous for synchronization in various communication systems^[1-4]. There have been a lot of results on the constructions of sequences (binary, almost binary, ternary, non-binary, polyphase, almost polyphase, etc) for the last half century or more for improved performance of various communications systems. Most of the sequences in this paper are over the binary alphabet $\mathbb{F}_2 = \{0, 1\}$ but the correlation is computed over \mathbb{C} with the correspondence

$$x \in \mathbb{F}_2 = \{0, 1\} \leftrightarrow (-1)^x \in \mathbb{C}. \quad (1)$$

When we are given a binary sequence $\mathbf{s} = s(i) \in \mathbb{F}_2 \mid i = \{0, 1, \dots, L-1\}$ of length L , we may consider its (usual) periodic expansion for computing its periodic autocorrelation. In that sense, we will use the term ‘length’ and ‘period’ of a binary sequence interchangeably. Then, the periodic autocorrelation of \mathbf{s} at shift τ , denoted by $C_{\mathbf{s}}(\tau)$, is given by

$$C_{\mathbf{s}}(\tau) = \sum_{i=0}^{L-1} (-1)^{s(i)+s(i+\tau)}, \quad (2)$$

where $i+\tau$ is computed mod L . There is an alternative way of expanding the sequence \mathbf{s} of length L periodically. Let \mathbf{s}' be a complement of \mathbf{s} defined by

$$s'(i) = s(i) + 1, \quad i = 0, 1, \dots, L-1.$$

Then, the alternative periodic expansion, called odd-periodic expansion, is to repeat \mathbf{s} in concatenation with \mathbf{s}' of total length $2L$. The autocorrelation of \mathbf{s} with this type of expansion is called the odd autocorrelation of \mathbf{s} . The odd autocorrelation at shift τ with $0 \leq \tau < L$, denoted by $C_{\mathbf{s}}^{odd}(\tau)$, is given by

$$C_{\mathbf{s}}^{odd}(\tau) = \sum_{i=0}^{L-\tau-1} (-1)^{s(i)+s(i+\tau)} + \sum_{i=L-\tau}^{L-1} (-1)^{s(i)+s(i+\tau)+1}, \quad (3)$$

where $i+\tau$ is computed mod L . In fact, $C_{\mathbf{s}}(\tau)$ can be said to be an even autocorrelation.

※ This work was supported by the National Research Foundation of Korea (NRF) Grant by the Korea Government through Ministry of Sciences and ICT (MSIT) under Grant RS-2023-002090000.

• First Author : Department of Electrical and Electronic Engineering, Yonsei University, gs.kim@yonsei.ac.kr, 정회원

◦ Corresponding Author : Department of Electrical and Electronic Engineering, Yonsei University, hysong@yonsei.ac.kr, 종신회원
논문번호 : 202502-024-B-RE, Received February 3, 2025; Revised March 10, 2025; Accepted March 14, 2025

The binary sequence \mathbf{s} of even period L is said to have optimal autocorrelation^[3,5] if

$$C_s(\tau) = \begin{cases} 0 \text{ or } -4 & \text{if } L \equiv 0 \pmod{4} \\ 2 \text{ or } -2 & \text{if } L \equiv 2 \pmod{4}. \end{cases}$$

for any $\tau \neq 0$. A lot of binary sequences of even period L above with (non-perfect) optimal autocorrelation have been constructed^[6-11], which would be best possible in terms of its periodic autocorrelation, since the perfect binary sequence is known only for $L = 4$ ^[3].

Instead of suppressing all the out-of-phase autocorrelation magnitudes, one started to consider having all-zero out-of-phase autocorrelations except for one non-zero value at some $\tau \neq 0$. It is called almost perfect sequences^[12] and investigated immediately by many others^[13-16] and further generalized into some non-binary zero-correlation zone sequences^[17-22]. We would like to mention that Pott and Bradley^[13,14] established some fundamental relation between cyclic relative difference sets and almost perfect binary sequences, which is very much similar to the relation between cyclic difference sets and binary sequences with two-level autocorrelation. For example, binary NTU sequences^[15] are closely related with binary sequences from a cyclic relative difference set^[16,23-25].

In search of sequences with better autocorrelation property, on the other hand, almost binary sequences or ternary sequences have been studied a lot^[13,26,27]. Here, an almost binary sequence is a ternary sequence over $\{0, +1, -1\}$ but the term 0 occurs only once or a few times. Such sequences with 'perfect' autocorrelation have been found, for example, in [27].

Some reviews on the binary and almost binary sequences with good odd autocorrelation follows now. In [28], especially in Section IV. A. 4 there, a binary sequence of even period is said to have an odd optimal autocorrelation if the magnitude of out of phase odd autocorrelation is no larger than 2. The binary sequences with low or optimal odd periodic autocorrelation have also been proposed a lot^[15,26-29].

In this paper, we propose (Theorem 1) a balanced binary sequence of length $2u$ for some integer u with 5-level autocorrelation from a cyclic relative

difference set. The out-of-phase autocorrelation magnitudes are all zero except for three indices at which the value is either $2u$ ($\tau = u$, once) or 4 (at some $\tau \neq 0$, u twice). We observe the half period of this sequence and found that it has optimal odd autocorrelation (Corollary 1). We also observe that changing one specific bit of this balanced binary sequence results in an almost perfect sequence (Corollary 2). Furthermore, we explain some of previously known constructions for sequences with good (even or odd) autocorrelation are closely related with the two variations of the main result in this paper.

This paper is organized as follows. Section 2 introduces some preliminaries. Section 3 discusses main results of this paper. We propose a construction for a binary 5-level autocorrelation sequence and its two variations. Section 4 explains as concluding remarks the relation between our constructions and other known constructions, especially in [15],[26].

II. Preliminaries

2.1 Notation

We will fix the following notation throughout the paper.

- \mathbb{Z} is the set of integers and \mathbb{Z}_L is the integers mod L .
- \mathbb{C} is the set of complex numbers and \mathbb{F}_q is the finite field of size q .
- Given a binary sequence $\mathbf{s} = \{s(i) \in \mathbb{F}_2 \mid i = 0, 1, \dots, L-1\}$ of length L , the periodic autocorrelation of \mathbf{s} at shift τ , denoted by $C_s(\tau)$, is given by (2) and the odd autocorrelation $C_s^{odd}(\tau)$ is given by (3), both in the beginning of Introduction.
- For a subset X of \mathbb{Z}_L and an element $\tau \in \mathbb{Z}_L$, we define

$$\Delta_X(\tau) \triangleq |(\tau + X) \cap X|,$$

where $\tau + X = \{\tau + x \mid x \in X\}$. Note that

$$\Delta_X(\tau) = \Delta_X(-\tau)$$

for any subset X and any τ .

2.2 Relative Difference Sets

Definition 1 (Relative Difference Sets^[13,30,31]). Let u, v, k, λ be positive integers. A (u, v, k, λ) relative difference set (RDS) D in the (additive) cyclic group \mathbb{Z}_{uv} relative to its subgroup $(u) = u\mathbb{Z}_{uv}$ is a k -subset $\{d_1, d_2, \dots, d_k\} \subset \mathbb{Z}_{uv}$, satisfying the following condition:

$$\Delta_D(d) = \begin{cases} \lambda, & d \in \mathbb{Z}_{uv} \setminus u\mathbb{Z}_{uv} \\ k, & d = 0 \\ 0, & \text{otherwise,} \end{cases} \quad (4)$$

for any $d \in \mathbb{Z}_{uv}$.

It is well-known that a (u, k, λ) -cyclic difference set (CDS) in \mathbb{Z}_u is a $(u, v=1, k, \lambda)$ -RDS in \mathbb{Z}_u (relative to its trivial subgroup $\{0\}$). We are mostly interested in the case where $v=2^{[31]}$ and $k=u-1$ so that the parameters become $(u, v=2, k=u-1, \lambda=\frac{u}{2}-1)$, since the existence of a cyclic (u, v, k, λ) -RDS implies the relation

$$k(k-1) = \lambda v(u-1).$$

This set of parameters further implies that u itself must be even. The following provides an equal-size partition of \mathbb{Z}_{2u} so that a binary sequence can be constructed from such RDS D .

Proposition 1. Let D be a $(u, 2, u-1, \frac{u}{2}-1)$ -RDS in \mathbb{Z}_{2u} relative to its subgroup $u\mathbb{Z}_{2u}$. Then, \mathbb{Z}_{2u} can be decomposed into the following disjoint union:

$$\mathbb{Z}_{2u} = D \cup (u+D) \cup \{z\} \cup \{u+z\},$$

for some z .

Proof. By (4), $\Delta_D(u) = 0$. Therefore,

$$D \cap (u+D) = \emptyset.$$

Therefore,

$$|\mathbb{Z}_{2u} \setminus (D \cup (u+D))| = 2u - 2k = 2.$$

Let $z \in \mathbb{Z}_{2u} \setminus (D \cup (u+D))$. Claim that $u+z$ can be in neither D nor $u+D$. If $u+z \in D$, then $z = u + v + z \in u+D$. If $u+z \in u+D$, then $z \in D$. Therefore, two elements in $\mathbb{Z}_{2u} \setminus (D \cup (u+D))$ are z and $u+z$ for some z . \square

III. Binary Sequences with Favourable Autocorrelation from RDS

In this section, we propose a balanced binary sequence $\mathbf{s} = \{s(i) \mid i \in \mathbb{Z}_{2u}\}$ of length $2u$ with 5-level autocorrelation from a $(u, 2, u-1, \frac{u}{2}-1)$ -RDS and discuss its two variations with (somewhat) better correlation property: the first is its half period portion of length u which has 4-level optimal odd autocorrelation; the second is its one-bit-changed version so that the result is almost balanced but with 3-level autocorrelation so that it is almost perfect.

Theorem 1 (Main Construction). Let D be a $(u, v=2, k=u-1, \lambda=\frac{u}{2}-1)$ -RDS. Let $z \in \mathbb{Z}_{2u}$ so that \mathbb{Z}_{2u} is partitioned as in Proposition 1:

$$\mathbb{Z}_{2u} = D \cup (u+D) \cup \{z\} \cup \{u+z\}. \quad (5)$$

Define a binary sequence $\mathbf{s} = \{s(i) \mid i = 0, 1, \dots, 2u-1\}$ as follows:

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\}. \end{cases} \quad (6)$$

Then, the periodic (even) autocorrelation of \mathbf{s} becomes:

$$C_s(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau, -\tau \in -z + u + D \\ -4, & \tau, -\tau \in -z + D \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

Proof. The binary sequence $\mathbf{s} = \{s(i) \mid i = 0, 1, \dots, 2u-1\}$

is balanced since

$$|D \cup \{z\}| = |(u+D) \cup \{u+z\}|.$$

Note also that

$$(u+D) \cup \{u+z\} = u + (D \cup \{z\}). \quad (8)$$

This explains its special periodic property. When it is (cyclically) shifted by half the period, then the result is a complement of the original sequence. Therefore, its half period portion of length u is expanded odd-periodically, the result is the same as the (even) periodic expansion of the original sequence \mathbf{s} of length $2u$. This gives the value

$$C_s(\tau = u) = -2u.$$

For the other cases, we calculate the autocorrelation as follows.

$$\begin{aligned} C_s(\tau) &= \sum_{i \in \mathbb{Z}_{2u}} (-1)^{s(i)+s(i+\tau)} \\ &= \sum_{i \in D} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in u+D} (-1)^{s(i)+s(i+\tau)} \quad (9) \\ &\quad + (-1)^{s(z)+s(z+\tau)} + (-1)^{s(u+z)+s(u+z+\tau)}. \end{aligned}$$

The first sum in (9) can be split into the following three cases: (a) $i \in D$ and $i+\tau \in D$ so that $s(i) + s(i+\tau) = 0$, (b) $i \in D$ and $i+\tau \in u+D$ so that $s(i) + s(i+\tau) = 1$ and (c) $i \in D$ and $i+\tau \in \{z, u+z\}$ so that $s(i) + s(i+\tau) = s(i+\tau)$ which is 1 if $i+\tau = z$ and 0 if $i+\tau = u+z$.

Then the case (a) becomes

$$\sum_{\substack{i \in D \\ i+\tau \in D}} (+1) = |D \cap (-\tau+D)| = |\tau+D \cap D| = \Delta_D(\tau).$$

Similarly, the case (b) becomes

$$\sum_{\substack{i \in D \\ i+\tau \in u+D}} (-1) = -|D \cap (-\tau+u+D)| = -\Delta_D(u-\tau).$$

Similarly, the second sum can be split into the following three cases: (a) $i \in u+D$ and $i+\tau \in D$ so

that $s(i) + s(i+\tau) = 1$, (b) $i \in u+D$ and $i+\tau \in u+D$ so that $s(i) + s(i+\tau) = 0$, and (c) $i \in u+D$ and $i+\tau \in \{z, u+z\}$. Then, similar to the first two cases of the first sum, the cases (a) and (b) become:

$$\sum_{\substack{i \in u+D \\ i+\tau \in D}} (-1) = -|(u+D) \cap (-\tau+D)| = -\Delta_D(u+\tau)$$

and

$$\sum_{\substack{i \in u+D \\ i+\tau \in u+D}} (+1) = |(u+D) \cap (u-\tau+D)| = \Delta_{u+D}(\tau) = \Delta_D(\tau).$$

Therefore, the autocorrelation of \mathbf{s} at shift τ becomes:

$$\begin{aligned} C_s(\tau) &= 2\Delta_D(\tau) - \Delta_D(u+\tau) - \Delta_D(u-\tau) \\ &\quad + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau = z, u+z}} (-1)^{s(i)+s(i+\tau)} \quad (10) \\ &\quad + (-1)^{s(z+\tau)} + (-1)^{s(u+z+\tau)+1} \end{aligned}$$

Assume that $\tau \neq 0$ and $\tau \neq u$. Then, the first line of $C_s(u)$ in (10) becomes

$$2\Delta_D(\tau) - \Delta_D(u+\tau) - \Delta_D(u-\tau) = 0,$$

since $\Delta_D(\tau) = \Delta_D(u \pm \tau) = \lambda = \frac{u}{2} - 1$. Now, the middle sum in (10) becomes the sum of only two terms corresponding to $i = z - \tau$ and $i = u + z - \tau$:

$$\begin{aligned} &\sum_{\substack{i \in D \cup (u+D) \\ i+\tau = z, u+z}} (-1)^{s(i)+s(i+\tau)} \\ &= (-1)^{s(z-\tau)+s(z)} + (-1)^{s(u+z-\tau)+s(u+z)} \\ &= (-1)^{s(z-\tau)} + (-1)^{s(u+z-\tau)+1}. \end{aligned}$$

Therefore, (10) finally becomes

$$\begin{aligned} C_s(\tau) &= (-1)^{s(z-\tau)} + (-1)^{s(u+z-\tau)+1} \\ &\quad + (-1)^{s(z+\tau)} + (-1)^{s(u+z+\tau)+1}. \end{aligned}$$

Therefore,

$$C_s(\tau) = \begin{cases} -4, & z - \tau, z + \tau \in D \\ 4, & z - \tau, z + \tau \in u + D \\ 0, & \text{otherwise.} \end{cases}$$

This proves the theorem. \square

From the half-odd-periodic property of \mathbf{s} in the proof of Theorem 1, we may identify its half period as a binary sequence having an optimal odd autocorrelation:

Corollary 1. *Let \mathbf{s} be the binary sequence of period $2u$ constructed from Theorem 1 with some $(u, 2, u - 1, u - 1)$ -RDS and an integer z satisfying the relation (5). Let the binary sequence \mathbf{t} of length u be any half period of \mathbf{s} . Then,*

$$C_t^{odd}(\tau) = \begin{cases} u, & \tau = 0 \\ 2, & \tau, -\tau \in -z + u + D \\ -2, & \tau, -\tau \in -z + D \\ 0, & \text{otherwise.} \end{cases}$$

Remark 1. *The binary sequence \mathbf{t} constructed from Corollary 1 is optimal in the sense of minimizing the maximum magnitude of out of phase odd autocorrelation described in Section IV. A. 4 of [28], as mentioned in Introduction.*

Remark 2. *In Corollary 1, since \mathbf{s} is balanced and u is even, a suitably chosen half period always allows \mathbf{t} to be balanced.*

Remark 3. *All the known parameters of a $(u, v = 2, k = u - 1, \lambda)$ -RDS are $(u = q + 1, v = 2, k = q, \lambda = \frac{q-1}{2})$ for some odd prime power q [13, 32-34]. Indeed, our construction in Corollary 1 gives some binary sequences of period $q + 1$ with optimal odd autocorrelation. We may conjecture that it is the only way of getting a binary sequence of period $q + 1$ with optimal odd autocorrelation for some odd prime power q .*

Now, we construct a sequence by changing the only one term of \mathbf{s} from the construction in Theorem 1

at index z . The resulting sequence is no longer balanced (we may call this almost balanced) but with better autocorrelation property which is only 3-level as in the following.

Corollary 2. *Let \mathbf{s} be the binary sequence of period $2u$ constructed from Theorem 1 with some $(u, 2, u - 1, u - 1)$ -RDS and an integer z satisfying the relation (5). Let the binary sequence \mathbf{r} be exactly the same as \mathbf{s} except that it is complemented only at the index z . That is, $r(z) = s(z) + 1$. Then,*

$$C_r(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u + 4, & \tau = u \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We assume $\tau \neq 0$. Then, since $r(i)$ and $s(i)$ differ only at $i = z$, we have

$$\begin{aligned} C_r(\tau) &= \sum_{i \in \mathbb{Z}_{2u}} (-1)^{r(i) + r(i+\tau)} \\ &= \sum_{i \in \mathbb{Z}_{2u}} (-1)^{s(i) + s(i+\tau)} \\ &\quad - ((-1)^{s(z) + s(z+\tau)} + (-1)^{s(z-\tau) + s(z)}) \\ &\quad + ((-1)^{r(z) + r(z+\tau)} + (-1)^{r(z-\tau) + r(z)}) \quad (11) \\ &= \sum_{i \in \mathbb{Z}_{2u}} (-1)^{s(i) + s(i+\tau)} \\ &\quad - 2((-1)^{s(z) + s(z+\tau)} + (-1)^{s(z-\tau) + s(z)}) \\ &= C_s(\tau) - 2((-1)^{s(z+\tau)} + (-1)^{s(z-\tau)}) \end{aligned}$$

When $\tau = u$, then

$$(-1)^{s(z+\tau)} + (-1)^{s(z-\tau)} = -2.$$

When $\tau \neq u$, both $z + \tau$ and $z - \tau$ are in $D \cup (u + D)$. If both $z + \tau$ and $z - \tau$ are in D , then

$$(-1)^{s(z+\tau)} + (-1)^{s(z-\tau)} = +2.$$

If both $z + \tau$ and $z - \tau$ are in $u + D$, then

$$(-1)^{s(z+\tau)} + (-1)^{s(z-\tau)} = -2.$$

If $z + \tau$ and $z - \tau$ are such that one is in D and

the other is in $u + D$, then

$$(-1)^{s(z+\tau)} + (-1)^{s(z-\tau)} = 0.$$

Therefore, we complete the proof from (7) and (11). \square

Remark 4. The binary sequence $\mathbf{r} = \{r(i) \mid i = 0, 1, \dots, 2(q+1)-1\}$ in Cor. 2 is given in fact as

$$r(i) = \begin{cases} 0, & i \in D \\ 1, & i \notin D. \end{cases}$$

Compare this with the definition of \mathbf{s} in (6).

Remark 5. The value z (for one-bit change) in Cor. 2 can be in the range $0 \leq z < u$ (first half) or in the range $u \leq z < 2u$ (second half). When we choose it to be the second half, we may identify the first half of \mathbf{r} (which is exactly the same as the first half of \mathbf{s}) to be the binary sequence \mathbf{t} in Cor. 1.

Remark 6. The binary sequence \mathbf{r} in Cor. 2 has the property that its autocorrelation value is zero except for the only two time shifts. This type of binary sequences has been defined to be the almost perfect sequence^[12,14]. Pott and Bradley proved^[14] that they are equivalent to some $(u, 2, u-1, \lambda)$ -RDS in \mathbb{Z}_{2u} relative to its subgroup $u\mathbb{Z}_{2u}$.

IV. Some Interesting Relations and Concluding Remarks

We now conclude this paper by discussing the relation between our construction in Corollaries 1 and 2 from an RDS of parameters $(u, 2, u-1, \frac{u}{2}-1)$ and other previous constructions, for example, those in [15], [26], [28] which were given without mentioning any RDS structure.

Nogami, Tada and Uehara^[15] in 2014 proposed some binary sequences as in the following. Let q be an odd prime power and $\alpha \in \mathbb{F}_{q^2}$ be a primitive element. Let $\text{Tr}(a) = a + a^q$ be the trace of $a \in \mathbb{F}_{q^2}$ to \mathbb{F}_q , and $\beta \triangleq \alpha^{q+1}$ be primitive in \mathbb{F}_q . The binary NTU

sequence $\mathbf{x} = \{x(i) \mid i = 0, 1, \dots, 2(q+1)-1\}$ of length $2(q+1)$ is defined as [15]

$$x(i) = \begin{cases} 1, & \text{Tr}(\alpha^i) \text{ is an odd power of } \beta \\ 0, & \text{Tr}(\alpha^i) = 0 \text{ or else it is an even power of } \beta. \end{cases} \quad (12)$$

We just note the values of i above so that $x(i) = 1$. It is not difficult to observe that the set of these values of i forms an RDS of parameters $(q+1, 2, q, \frac{q-1}{2})$ ^[30]. That is, claim that

$$D \triangleq \{i \in \mathbb{Z}_{2(q+1)} \mid \text{Tr}(\alpha^i) \text{ is an odd power of } \beta\}. \quad (13)$$

is a $(q+1, 2, q, \frac{q-1}{2})$ -RDS in $\mathbb{Z}_{2(q+1)}$ relative to its sub-group $(q+1)\mathbb{Z}_{2(q+1)}$. For the proof, see Cor. 5.1.1 in [30] or Sec. 2.2 in [13].

From Remark 4 and (13), we have the following conclusion:

Remark 7. The binary NTU sequence \mathbf{x} of length $2(q+1)$ in (12) is equivalent to the binary sequence constructed from Cor. 2 with the RDS D in (13).

A construction of some binary sequences with optimal odd autocorrelation is given in 2003 by Luke et.al.[28], where the binary odd optimal sequence is obtained from a ternary odd perfect sequence. To explain this technique, we must be careful of representing the sequence whether it is over the complex or its phases. A binary sequence uses the complex values $+1$ or -1 and its phase notation would be 0 or 1, corresponding to the relation in (1). Similar situation happens for ternary sequences. However, there are many different ways to consider the ternary alphabet. One choice is the complex values $\{0, +1, -1\}$ and its phase notation would be $\{*, 0, 1\}$. Using this phase notation for ternary sequences, Krengel defined in 2004 the odd perfect ternary sequence $\mathbf{y} = \{y(i) \mid i = 0, 1, \dots, q\}$ of length $q+1$ as follows^[26]:

$$y(i) = \begin{cases} 1, & \text{Tr}(\alpha^i) \text{ is an odd power of } \beta \\ *, & \text{Tr}(\alpha^i) = 0 \\ 0, & \text{Tr}(\alpha^i) \text{ is an even power of } \beta. \end{cases} \quad (14)$$

When we apply the technique by Luke et.al. to the ternary Kregel sequence above, we found that we obtain a binary sequence with odd optimal autocorrelation property. The resulting binary Kregel sequence $\mathbf{y}' = \{y'(i) \mid i = 0, 1, \dots, q\}$ of length $q + 1$ is given as follows:

$$y'(i) = \begin{cases} 1, & \text{Tr}(\alpha^i) \text{ is an odd power of } \beta \\ 0, & \text{Tr}(\alpha^i) = 0 \text{ or else it is an even power of } \beta. \end{cases} \quad (15)$$

It is interesting that the only difference between the binary Kregel sequence in (15) and the binary NTU sequence is the range of i at which the sequence is defined. The range of i for the binary Kregel sequence is half of those for the binary NTU sequence. From Remark 5, we see that the half period of the binary NTU sequence (which is called the modified Kregel sequence) is equivalent to the binary sequence in Cor. 1:

Remark 8. *The modified Kregel sequence \mathbf{y}' of length $q + 1$ in (15) is equivalent to those constructed from Cor. 1 with the RDS D in (13).*

Example 1. *Let $q = 3^2$, α be a primitive element of \mathbb{F}_{3^4} and $\beta \triangleq \alpha^{10}$ be primitive in \mathbb{F}_{3^2} . Then, the (10, 2, 9, 4)-RDS D in (13) becomes:*

$$D = \{4, 8, 10, 11, 12, 13, 16, 17, 19\}.$$

Then, \mathbb{Z}_{20} is partitioned as follows:

$$\mathbb{Z}_{20} = \{5\} \cup \{15\} \cup D \cup (10 + D).$$

Using the above RDS D and an integer $z \triangleq 5$, the sequence \mathbf{s} of period 20 constructed from Theorem 1 becomes:

$$\mathbf{s} = (1, 1, \underline{1, 1, 0, 0}, \underline{1, 1, 0, 1}, \underline{0, 0, 0, 0}, 1, 1, 0, 0, 1, 0).$$

The above sequence \mathbf{s} is actually the same as the binary NTU sequence \mathbf{x} of period 20 in (12). The first half period of \mathbf{s} is the same as the binary Kregel sequence \mathbf{y}' of period 10 in (15). In this case, the binary Kregel sequence \mathbf{y}' is not balanced. By choosing the half period of \mathbf{s} as specified in the underlined part, we obtain the following balanced binary sequence \mathbf{t} of period 10 constructed from Corollary 1, as Remark 2 states that a half period of \mathbf{s} can always be chosen for \mathbf{t} to be balanced.

$$\mathbf{t} = (1, 1, 0, 0, 1, 1, 0, 1, 0, 0).$$

Table 1 summarizes well-known constructions and the proposed construction of even-length balanced or almost balanced binary sequences. Here, an almost balanced binary sequence is defined as a binary sequence in which the number of 0s and 1s differs by 2. The proposed sequence has a period that conventional balanced or almost balanced binary sequences with ideal autocorrelation in [6], [9], [35],

Table 1. Well-known and proposed even-length balanced or almost balanced binary sequences

Type	Construction	Period	Correlation Property
Balanced	Sidelnikov [9] and Lempel-Cohn-Eastman [35]	$q - 1$	Ideal autocorrelation
	Ding-Helleseth-Martinsen [6]	$2p_1$	Ideal autocorrelation
	Theorem 1 and Nogami-Uehara-Tada [15]	$2(q + 1)$	5-level autocorrelation
	Corollary 1	$q + 1$	Ideal odd autocorrelation
Almost balanced	Arasu-Ding-Helleseth-Kumar-Martinsen [36]	$4p, 4p(p_1 + 2), 4(2^n - 1)$	Ideal autocorrelation
	Corollary 2 and Pott-Bradley [14]	$2(q + 1)$	Almost perfect

- q is an odd prime power
- p_1 and p_2 are odd primes with $p_1 \equiv 5 \pmod{8}$ and $p_2 \equiv 3 \pmod{4}$
- p_1 is an odd prime such that $(p_1, p_1 + 2)$ is a twin prime pair

[36] do not typically possess. Instead, it exhibits alternative correlation properties such as 5-level autocorrelation, almost perfect autocorrelation, or ideal odd autocorrelation.

References

- [1] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Wiley, 1996.
- [2] S. W. Golomb, *Shift register sequences: Secure and limited-access code generators, efficiency code generators, prescribed property generators, mathematical models, (3rd Revised)*, World Scientific, 2017.
(<https://doi.org/10.1142/9361>)
- [3] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, 2005.
(<https://doi.org/10.1017/CBO9780511546907>)
- [4] G. Kim and H.-Y. Song, "Statistical span property of binary run sequences," *IEEE Trans. Inf. Theory*, vol. 69, no. 4, pp. 2713-2721, 2023.
(<https://doi.org/10.1109/TIT.2022.3222527>)
- [5] T. Helleseht and K. Yang, "On binary sequences of period $n = pm - 1$ with optimal autocorrelation," in *Proc. 2001 Sequences and Their Appl. (SETA)*, pp. 209-217, 2002.
(https://doi.org/10.1007/978-1-4471-0673-9_15)
- [6] C. Ding, T. Helleseht, and H. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 428-433, 2001.
(<https://doi.org/10.1109/18.904555>)
- [7] C. Ding, T. Helleseht, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2606-2612, 1999.
(<https://doi.org/10.1109/18.796414>)
- [8] H. D. Luke, H. D. Schotten, and H. Hadinejad-Mahram, "New construction for binary sequences of period $pm - 1$ with optimal autocorrelation using $(z + 1)d + azd + b_z$," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271-3282, 2003.
(<https://doi.org/10.1109/18.923752>)
- [9] V. M. Sidel'nikov, "Some k -valued pseudo-random sequences and nearly equidistant codes," *Problems Inf. Transmission*, vol. 5, no. 1, pp. 16-22, 1969.
(<https://www.mathnet.ru/eng/ppi1781>)
- [10] N. Y. Yu and G. Gong, "New binary sequences with optimal autocorrelation magnitude," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4771-4779, 2008.
(<https://doi.org/10.1109/TIT.2008.928999>)
- [11] X. H. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1278-1286, 2010.
(<https://doi.org/10.1109/TIT.2009.2039159>)
- [12] J. Wolfmann, "Almost perfect autocorrelation sequences," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1412-1418, 1992.
(<https://doi.org/10.1109/18.144729>)
- [13] A. Pott, *Finite Geometry and Character Theory*, Springer, 2006.
(<https://doi.org/10.1007/BFb0094449>)
- [14] A. Pott and S. P. Bradley, "Existence and nonexistence of almost-perfect autocorrelation sequences," *IEEE Trans. Inf. Theory*, vol. 41, no. 1, pp. 301-304, 1995.
(<https://doi.org/10.1109/18.370094>)
- [15] Y. Nogami, K. Tada, and S. Uehara, "A geometric sequence binarized with legendre symbol over odd characteristic field and its properties," *IEICE Trans. Fundamentals of Electr., Commun. and Computer Sci.*, vol. 97, no. 12, pp. 2336-2342, 2014.
(<https://doi.org/10.1587/transfun.E97.A.2336>)
- [16] G. Kim and H.-Y. Song, "Some properties of NTU sequences," in *Proc. ISITA 2018*, 2018.
(<https://doi.org/10.34385/proc.55.We-AM-Poster.7>)
- [17] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlation zone," *Electr. Lett.*, vol. 36, no. 6, p. 1, 2000.

- (<https://doi.org/10.1049/el:20000462>)
- [18] A. Z. Tirkel, E. Krengel, and T. Hall, "Sequences with large ZCZ," in *Proc. 8th IEEE Int. Symp. Spread Spectrum Techniques and Applications-Programme and Book of Abstracts (IEEE Cat. No. 04TH8738)*, pp. 270-274, 2004.
(<https://doi.org/10.1109/ISSSTA.2004.1371704>)
- [19] H. Torii, M. Nakamura, and N. Suehiro, "A new class of zero-correlation zone sequences," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 559-565, 2004.
(<https://doi.org/10.1109/TIT.2004.825399>)
- [20] G. Kim and H.-Y. Song, "Almost perfect sequence family with perfect cross correlation," in *Proc. ISITA 2020*, pp. 456-459, 2020.
(<https://doi.org/10.34385/proc.65.C04-3>)
- [21] G. Kim, H. Choi, D.-K. Kim, W. Kim, X. Jin, and H.-Y. Song, "Optimal uncorrelated polyphase ZCZ sequences over an alphabet of minimum size," in *Proc. 2023 IEEE ISIT*, pp. 897-902, 2023.
(<https://doi.org/10.1109/ISIT54713.2023>)
- [22] G. Kim and H.-Y. Song, "The unique form of the uncorrelated optimal ZCZ sequence families," in *Proc. 2024 IEEE ISIT*, pp. 1338-1342, 2024.
(<https://doi.org/10.1109/ISIT57864.2024>)
- [23] M. H. Lee, G. Kim, M. K. Song, and H.-Y. Song, "3-level autocorrelation properties of binary sequences using legendre symbol and trace function," in *Proc. KICS Winter Conf.*, pp. 860-861, 2018.
- [24] M. H. Lee, G. Kim, M. K. Song, and H.-Y. Song, "5-level autocorrelation properties of binary sequences using legendre symbol and trace function," in *Proc. KICS Winter Conf.*, pp. 875-876, 2018.
- [25] G. Kim, H.-Y. Song, and M. K. Song, "Relative difference set design for binary three-level autocorrelation sequence using legendre symbol and trace function," in *Proc. 28th JCCI 2018*, pp. 278-279, 2018.
- [26] E. I. Krengel, "Almost-perfect and odd-perfect ternary sequences," in *Proc. 2004 Sequences and Their Appl. (SETA)*, pp. 197-207, 2004.
(<https://doi.org/10.1007/b136167>)
- [27] H. D. Luke and H. D. Schotten, "Odd-perfect, almost binary correlation sequences," *IEEE Trans. Aerospace and Electr. Syst.*, vol. 31, no. 1, pp. 495-498, 1995.
(<https://doi.org/10.1109/7.366335>)
- [28] H. D. Luke, H. D. Schotten, and H. Hadinejad-Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271-3282, 2003.
(<https://doi.org/10.1109/TIT.2003.820035>)
- [29] Y. Yang and X. H. Tang, "Generic construction of binary sequences of period $2N$ with optimal odd correlation Magnitude based on quaternary sequences of odd period N ," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 384-392, 2017.
(<https://doi.org/10.1109/TIT.2017.2767076>)
- [30] J. Elliott and A. Butson, "Relative difference sets," *Illinois J. Mathematics*, vol. 10, no. 4, pp. 517-531, 1966.
(<https://doi.org/10.1215/IJM/1256055004>)
- [31] K. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, "Relative difference sets with $n = 2$," *Discrete Mathematics*, vol. 147, no. 1-3, pp. 1-17, 1995.
([https://doi.org/10.1016/0012-365X\(94\)00226-9](https://doi.org/10.1016/0012-365X(94)00226-9))
- [32] K. Arasu, J. F. Dillon, K. H. Leung, and S. L. Ma, "Cyclic relative difference sets with classical parameters," *J. Combinatorial Theory, Series A*, vol. 94, no. 1, pp. 118-126, 2001.
(<https://doi.org/10.1006/jcta.2000.3137>)
- [33] D. B. Chandler and Q. Xiang, "Cyclic relative difference sets and their p -ranks," *Designs, Codes and Cryptography*, vol. 30, pp. 325-343, 2003.
(<https://doi.org/10.1023/A:1025750228679>)
- [34] S.-H. Kim, J.-S. No, H. Chung, and T. Hellesest, "New cyclic relative difference sets constructed from d-homogeneous functions

with difference-balanced property,” *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1155-1163, 2005.

(<https://doi.org/10.1109/TIT.2004.842712>)

- [35] A. Lempel, M. Cohn, and W. Eastman, “A class of balanced binary sequences with optimal autocorrelation properties,” *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 38-42, 1977.

(<https://doi.org/10.1109/TIT.1977.1055672>)

- [36] K. Arasu, C. Ding, T. Hellesteth, P. V. Kumar, and H. M. Martinsen, “Almost difference sets and their sequences with optimal autocorrelation,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2934-2943, 2001.

(<https://doi.org/10.1109/18.959271>)

Gangsan Kim



Feb. 2016 : B.S., Dept. of Electrical and Electronic Engineering, Yonsei University

Feb. 2025 : Ph.D., Dept. of Electrical and Electronic Engineering, Yonsei University

May 2022~Oct. 2023 : AI

Science and Technology Soldier, Republic of Korea Army Training and Doctrine Command
Mar. 2025~Current : Postdoctoral Fellow, Yonsei University

<Research Interests> Digital Communication, Information Theory, Coding Theory, Sequence Design.

[ORCID:0000-0002-3864-5379]

Hong-Yeop Song



Feb. 1984 : B.S., Dept. of Electronic Engineering, Yonsei University

May 1986 : M.S., Dept. of EE. Systems, University of Southern California

Dec. 1991 : Ph.D., Dept. of EE.

Systems, University of Southern California

Jan. 1992~Dec. 1993 : Postdoctoral Fellow, University of Southern California

Jan. 1994~Aug. 1995 : Senior Engineer, Qualcomm, San Diego

Sep. 1995~Current : Professor, Dept. of Electrical and Electronic Engineering, Yonsei University

<Research Interests> Digital Communication, Information Theory, Coding Theory, Sequence Design

[ORCID:0000-0001-8764-9424]