Theory on the construction of Binary Sequences
with Ideal Autocorrelation*

Jong-Seon No1\textsuperscript{1}, Kyeongcheol Yang2\textsuperscript{1},
Habong Chung3\textsuperscript{1}, and Hong-Yeop Song4\textsuperscript{1}

December 1, 1997

ABSTRACT

In this paper, we present a closed-form expression of binary sequences of longer
period with ideal autocorrelation property in a trace representation, if a given binary
sequence with ideal autocorrelation property is described using the trace function.
We also enumerate the number of cyclically distinct binary sequences of a longer
period with ideal autocorrelation property, which are extended from a given binary
sequence with ideal autocorrelation property.

Keywords: ideal autocorrelation property, m-sequences

1) J.-S. No is with Dept. of Electronic Engineering, Konkuk University, Seoul 143-701,
Korea.
2) K. Yang is with Dept. of Electronic Communication Engineering, Hanyang University,
Seoul 133-791, Korea.
3) H. Chung is with Dept. of Electronic Engineering, Hong-Ik University, Seoul 121-791,
Korea.
4) H.-Y Song is with Dept. of Electronic Engineering, Yonsei University, Seoul 120-749,
Korea.

*This work was supported in part by the Korea Ministry of Information and
Communications.
I. Introduction

A binary (0 or 1) sequence \( \{ b(t), t = 0,1,\ldots,N-1 \} \) of period \( N = 2^n - 1 \) is called balanced if the number of 1's is one more than the number of 0's. It is said to have the ideal autocorrelation property if its periodic autocorrelation function \( R(\tau) \) is given by

\[
R(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \mod N, \\ -1, & \text{for } \tau \not\equiv 0 \mod N, \end{cases}
\]

where \( R(\tau) \) is defined as

\[
R(\tau) = \sum_{t=0}^{N-1} (-1)^{b(t+\tau) + b(t)}
\]

and \( t + \tau \) is computed mod \( N \). Note that \( R(\tau) \) is the number of agreements between \( \{ b(t) \} \) and \( \{ b(t+\tau) \} \) minus the number of disagreements for any \( \tau \not\equiv 0 \mod N \) as \( t \) runs from 0 to \( N-1 \) [2], [3], [16].

Balanced binary sequences of period \( 2^n - 1 \) having the ideal autocorrelation function find many applications in spread spectrum communication systems [2], [3], [10], [12], [13], [15], [16], [17]. Some of the well-known binary sequences of period include \( m \)-sequences, GMW sequences, Legendre sequences, etc.

Let \( \{ b(t) \} \) and \( \{ c(t) \} \) be two binary sequences of period \( N \). Two sequences \( \{ b(t) \} \) and \( \{ c(t) \} \) are defined to be cyclically equivalent if there exists an integer \( \tau \) such that \( c(t) = b(t+\tau) \) for all \( t \). Otherwise, they are said to be cyclically distinct. For an integer \( r \), the sequence \( \{ c(t) \} \) is called the decimation by \( r \) of the sequence \( \{ b(t) \} \) if \( c(t) = b(rt) \) for any integer \( t \). It is easily checked that the period of \( \{ c(t) = b(rt) \} \) is given by \( N \) divided by \( \gcd(r,N) \). Two sequences \( \{ b(t) \} \) and \( \{ c(t) \} \) are said to be inequivalent if there are no integers \( r \) and \( \tau \) such that \( c(t) = b(r[t+\tau]) \) for all \( t \).

In this paper, we present a generalization method of extending binary sequences with ideal autocorrelation property as a closed-form expression. We also enumerate the number of cyclically distinct binary sequences of a longer period with ideal
autocorrelation property, which are extended from a given binary sequence with ideal autocorrelation property.

This paper is organized as follows. In Section II, we present the main theorems to extend binary sequences with ideal autocorrelation property. We also enumerate the number of cyclically distinct extensions of a given binary sequence with ideal autocorrelation property. We mention an important question on linear span of the extended sequences in Concluding Remarks.

II. Extension of Binary Sequences with Ideal Autocorrelation

It has been known that binary sequences of longer period with ideal autocorrelation property can be constructed from a binary sequence of shorter period with ideal autocorrelation property, but an explicit construction method has not been well described except for the GMW sequences. Our main result is to give a closed-form expression of binary sequences of longer period with ideal autocorrelation property in their trace representation.

The new binary sequences of longer period constructed in this method will be referred to as extensions of a given sequence.

Let \( q \) be a prime power and let \( F_q \) be the finite field with \( q \) elements. Let \( n = e m > 1 \) for some positive integers \( e \) and \( m \). Then the trace function \( tr_m^a(\cdot) \) is a mapping from \( F_{2^n} \) to its subfield \( F_{2^m} \), given by

\[
tr_m^a(x) = \sum_{i=0}^{2^m-1} x^{2^i a}.
\]

It is easy to check that the trace function satisfies the following:

(i) \( tr_m^a(ax+by) = a tr_m^a(x) + b tr_m^a(y) \), for all \( a,b \in F_{2^m}, x,y \in F_{2^n} \).

(ii) \( tr_m^a(x^{2^m}) = tr_m^a(x) \), for all \( x \in F_{2^n} \).

(iii) \( tr_m^1(x) = tr_1^m(tr_m^a(x)) \), for all \( x \in F_{2^n} \).

See [6], [7] for the detailed properties of the trace function.

For the remaining, we are interested in the case where \( n = e m \) for integers \( m > 1 \) and \( e > 1 \). We use the following notation:

- \( N = 2^n - 1, M = 2^m - 1 \), and \( T = \frac{N}{M} = \frac{2^n - 1}{2^m - 1} \).
\begin{itemize}
  \item $\alpha, \beta$ : primitive elements of $F_{2^m}, F_{2^n}$ respectively.
  \item $\{b(t_1), \ t_1 = 0, 1, \ldots, M-1\}$
    \hspace{1cm} = a binary sequence of period $M$ with ideal autocorrelation property.
  \item $\{c(t), \ t = 0, 1, \ldots, N-1\}$
    \hspace{1cm} = binary sequence of period $N$ as an extension of $\{b(t_1)\}$.
\end{itemize}

It is well-known that the ideal autocorrelation property of a sequence of period $N$ is invariant under the decimation by $r$, if $r$ is an integer relatively prime to $N$. The statement is restated in the following proposition.

**Proposition 1** Let $r, \ 1 \leq r \leq N-1$, be an integer relatively prime to $N$. If a sequence $\{c(t), \ t = 0, 1, \ldots, N-1\}$ of period $N-1$ has the ideal autocorrelation property, so does its decimation $\{c(rt), \ t = 0, 1, \ldots, N-1\}$ by $r$.

**Theorem 2** Let $m$ and $n$ be positive integers such that $m | n$. Let $\beta$ be a primitive element of $F_{2^n}$ and set $\alpha = \beta^T$ where $T = (2^n - 1)/(2^m - 1)$. Assume that for an index set $I$, the sequence $\{b(t_1), \ t_1 = 0, 1, \ldots, M-1\}$ of period $M = 2^m - 1$ given by

$$b(t_1) = \sum_{a \in I} tr_{m}^a(\alpha^{at_1})$$

has the ideal autocorrelation property. For an integer $r, \ 1 \leq r \leq M-1$, relatively prime to $M$, the sequence $\{c(t), \ t = 0, 1, \ldots, N-1\}$ of period $N = 2^n - 1$ defined by

$$c(t) = \sum_{a \in I} tr_{m}^a(\{tr_{m}^a(\beta^t)\}^r)$$

also has the ideal autocorrelation property.

**Proof:** Consider an $m$-sequence $\{v(t) = tr_{m}^a(\beta^t), \ t = 0, 1, \ldots, N-1\}$ of period $N = 2^n - 1$. Arrange it in the $M \times T$ rectangular array $X_0 = [x(t_1,t_2)]$ such that $x(t_1,t_2) = v(t_1T + t_2)$, where $t_1 = 0, 1, \ldots, 2^m - 2$, and $t_2 = 0, 1, \ldots, T-1$. Since

$$v(t) = v(t_1T + t_2) = tr_{m}^a(tr_{m}^a(\beta^{t_1T + t_2})) = tr_{m}^a(a^{t_1} \cdot tr_{m}^a(\beta^{t_2})),$$

the $t_2$-th column $\{x(t_1,t_2), \ t_1 = 0, 1, \ldots, M-1\}$ of $X_0$ is either a cyclic shift of an $m$-sequence $\{tr_{m}^a(\alpha^t), \ t = 0, 1, \ldots, M-1\}$ of period $M = 2^m - 1$ or the all-zero
sequence. That is,

\[ x^{(0)}_{t_1 t_2} = \begin{cases} 
tr_1^m(\alpha^{t_1 + \tau}) & \text{if } \tr_2^m(\beta^{t_2}) = \alpha^l, \\
0 & \text{if } \tr_2^m(\beta^{t_2}) = 0,
\end{cases} \]

(1)

where \( l, 0 \leq l \leq M - 1 \), is an integer. Similarly, if we arrange \( \{ v(t + \tau), t = 0, 1, \ldots, N - 1 \} \) for \( \tau \equiv 0 \pmod{N} \) in the \( M \times T \) rectangular array \( X_{\tau} = [x^{(\tau)}_{t_1 t_2}] \) such that \( x^{(\tau)}_{t_1 t_2} = v(t_1 T + t_2 + \tau) \), where \( t_1 = 0, 1, \ldots, M - 1 \), and \( t_2 = 0, 1, \ldots, T - 1 \), then the \( t_2 \)-th column \( \{x^{(\tau)}_{t_1 t_2}, t_1 = 0, 1, \ldots, M - 1 \} \) of \( X_{\tau} \) is also either a cyclic shift of an \( m \)-sequence \( \{tr_1^m(\alpha^{t_1}), t_1 = 0, 1, \ldots, M - 1 \} \) of period \( M \) or the all-zero sequence. That is,

\[ x^{(\tau)}_{t_1 t_2} = \begin{cases} 
tr_1^m(\alpha^{t_1 + \tau}) & \text{if } \tr_2^m(\beta^{t_2}) = \alpha^l, \\
0 & \text{if } \tr_2^m(\beta^{t_2}) = 0,
\end{cases} \]

(2)

where \( t + \tau = t_1 T + t_2 \), \( 0 \leq t_1 \leq M - 1 \), \( 0 \leq t_2 \leq T - 1 \). Expressing \( \tau \) into

\( \tau = \tau_1 T + \tau_2, 0 \leq \tau_1 \leq M - 1, 0 \leq \tau_2 \leq T - 1, \)

it is easy to check that

\[
\begin{align*}
t_2' &= t_2 + \tau_2 \mod T, \\
t_1' &= t_1 + \tau_1 + (t_2 + \tau_2 - t_2')/T.
\end{align*}
\]

Since \( \{v(t)\} \) has the ideal autocorrelation property, we have

\[
-1 = \sum_{t=0}^{N-1} \sum_{t=0}^{T-1} (-1)^{v(t) + v(t + \tau)} = \sum_{t_1=0}^{M-1} \sum_{t_2=0}^{T-1} (-1)^{x^{(0)}_{t_1 t_2} + x^{(\tau)}_{t_1 t_2}}
\]

for any integer \( \tau \not\equiv 0 \pmod{N} \). Note that the inner sum can yield the value \( 2^m - 1 \) when both \( \{x^{(0)}_{t_1 t_2}, 0 \leq t_1 \leq M - 1 \} \) and \( \{x^{(\tau)}_{t_1 t_2}, 0 \leq t_1 \leq M - 1 \} \) are identical as an \( m \)-sequence of the same phase or as the all-zero sequence, and the value \( -1 \) when either of them is the all-zero sequence or both are the distinct cyclic shifts of an \( m \)-sequence. In order to satisfy Equation (5), the inner sum gives the value \( 2^m - 1 \) with \( (T - 1)/2^m \) times, and the value \(-1\) with \( T - (T - 1)/2^m \) times.
times as \( t_2 \) runs from 0 to \( T - 1 \).

Now consider the sequence \( \{ c( t ), \ t = 0,1,\ldots,N - 1 \} \) and arrange it in the \( M \times T \) rectangular array \( Y_0 = [ y^{(0)}_{t_1,t_2} ] \) in the same manner as the previous case. Since
\[
c( t ) = c( t_1 T + t_2 ) = \sum_{a \in I} \text{tr}_m \{ \text{tr}_m ( \beta^{t_1 T + t_2} ) \} a \text{tr}_1 \}
\]
we know that the \( t_2 \)-th column \( \{ y^{(0)}_{t_1,t_2}, \ t_1 = 0,1,\ldots,M - 1 \} \) of \( Y_0 \) is either a decimation
\[
( b( r[t_1 + l]), \ t_1 = 0,1,\ldots,M - 1 ) \quad \text{by} \quad r \quad \text{of} \quad \{ b( t_1 ) \} \quad \text{when} \quad tr_m( \beta^{t_2} ) = a', \quad \text{or}
\]
the all-zero sequence when \( tr_m( \beta^{t_2} ) = 0 \). That is,
\[
y^{(0)}_{t_1,t_2} = \left\{ \begin{array}{ll}
b( r[t_1 + l]) & \text{if} \ tr_m( \beta^{t_2} ) = a', \\
0 & \text{if} \ tr_m( \beta^{t_2} ) = 0,
\end{array} \right.
\]
(6)
where \( l, \ 0 \leq l \leq M - 1, \) is an integer. Similarly, if we arrange \( \{ c( t + \tau ), \ t = 0,1,\ldots,N - 1 \} \) for \( \tau \neq 0 \ ( \text{mod} \ N ) \) in the \( M \times T \) rectangular array
\[
Y_\tau = [ y^{(\tau)}_{t_1,t_2} ] \quad \text{such that} \quad y^{(\tau)}_{t_1,t_2} = c( t_1 T + t_2 + \tau ), \quad \text{where}
\]
\( t_1 = 0,1,\ldots,M - 1 \) and \( t_2 = 0,1,\ldots,T - 1, \) then the \( t_2 \)-th column
\[
\{ y^{(\tau)}_{t_1,t_2}, \ t_1 = 0,1,\ldots,M - 1 \} \quad \text{of} \quad Y_0 \quad \text{is also either a cyclic shift of the decimation}
\]
\( ( b( r[t_1]), \ t_1 = 0,1,\ldots,M - 1 ) \quad \text{by} \quad r \quad \text{of} \quad \{ b( t_1 ), \ t_1 = 0,1,\ldots,M - 1 \} \quad \text{of period} \ M \quad \text{or}
\]
the all-zero sequence. That is,
\[
y^{(\tau)}_{t_1,t_2} = \left\{ \begin{array}{ll}
b( r[t_1' + l]) & \text{if} \ tr_m( \beta^{t_2'} ) = a', \\
0 & \text{if} \ tr_m( \beta^{t_2'} ) = 0,
\end{array} \right.
\]
(7) where \( t_1' \) and \( t_2' \) are defined in Eq. (3) and (4), respectively. Since \( \{ b( t_1 ), \ t_1 = 0,1,\ldots,M - 1 \} \) has the ideal autocorrelation property, so does \( \{ b( r[t_1]) \} \) by Proposition I. Comparing Eq. (1) and (2) with Eq. (6) and (7), we observe that the