On Lengthening the Period of Known Binary Sequences Preserving the Ideal Autocorrelation*

Jong-Seon No[1], Kyeongcheol Yang[2],
Habong Chung[3], and Hong-Yeop Song[4]

December 1, 1997

ABSTRACT

Recently, No *et al.* presented a new construction of binary sequences with ideal autocorrelation property. In this paper, we applied this method into some of the well-known binary sequences with ideal autocorrelation, and the results are described in detail. First, the GMW sequences are shown to be a *natural extension* of m-sequences with respect to this method. Second, new binary sequences with ideal autocorrelation property are explicitly constructed from Legendre sequences, Hall's sextic residue sequences, and other known sequences of miscellaneous type.

Keywords : GMW sequences, m-sequences, Legendre sequences, ideal autocorrelation property

---

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

Balanced binary sequences with ideal autocorrelation have many applications in spread spectrum communication systems[6], [7], [14], [20], [18], [21], [23]. The ideal autocorrelation function of these sequences is the best level of imitation that one can achieve so that they look like ''true random sequences with statistical randomness,'' in addition to their balanced property of having as many 1's as in one period as 0's, but still these sequences can be deterministically produced[7].

Some of the well-known examples with period 2^n-1 can be classified as: (i) m-sequences for all $n=1,2,\cdots$; (ii) GMW sequences for composite values of n; (iii) ''Legendre'' sequences whenever 2^n-1 is a prime (so called, Mersenne prime); (iv) ''Hall's sextic residue'' sequences for $2^n-1=31,127,\text{ and }131071$; and (v) sequences of miscellaneous type of length 127, 255, 511, found by computer. The m-sequences and the GMW sequences are best described in terms of the trace function over a finite field [20]. It was recently shown that the Legendre sequences of period $p=2^n-1$ can be explicitly described using the trace function from the finite field with 2^n elements to the finite field with two elements[15].

Recently, No *et al.* presented a new construction of binary sequences with ideal autocorrelation property[16]. In this paper, we applied this method into some of the well-known binary sequences with ideal autocorrelation, and the results are described in detail. First, the GMW sequences are shown to be a *natural extension* of m-sequences with respect to this method. Second, new binary sequences with ideal autocorrelation property are explicitly constructed from Legendre sequences, Hall's sextic residue sequences, and other known sequences of miscellaneous type.

This paper is organized as follows. In Section II, we describe some of the necessary terminology and background materials for pesudorandom binary sequences and their trace representation. We will quote the main result of [16] of constructing new binary sequences with ideal autocorrelation for the sake of completeness. In Section III, the GMW sequences can be reinterpreted as the natural extensions of the m-sequences. As a first nontrivial example, the Legendere sequences of Mersenne prime period are extended to longer binary sequences with ideal autocorrelation property in Section IV.

Hall's sextic residue sequences and known sequences of miscellaneous type are also considered in Section IV.

II. Preliminary Background

A binary sequence $\{b(t)\}$ of period $N = 2^n - 1$ is said to be *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 $R(\tau)$ has only two values, that is, $R(\tau) = N$ for $\tau = 0 \pmod N$, and $R(\tau) = -1$ for $\tau \neq 0 \pmod N$. Here, $R(\tau)$ is defined as

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

where $t+\tau$ is computed mod N.

Let $\{b(t)\}$ and $\{c(t)\}$ be two binary sequences of period N. Two sequences $\{b(t)\}$ and $\{c(t)\}$ are said to be *cyclically equivalent* if there exists an integer τ such that $c(t) = b(t+\tau)$ for all t. Otherwise, they are said to be *cyclically distinct*. The sequence $\{c(t)\}$ is called the *decimation* by r, for some integer r, of a sequence $\{b(t)\}$ if $c(t) = b(rt)$ for all t. It is easy to check that the period of $\{c(t)\}$ is given by N divided by $\gcd(r, N)$. Any two sequences $\{b(t)\}$ and $\{c(t)\}$ of period N are said to be *equivalent* if there are some integers r and τ such that $c(t) = b(r[t+\tau])$ for all t. Otherwise, they are said to be *inequivalent*.

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

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{2^{mi}}.$$

It is easy to check that the trace function satisfies the following: (i) $tr_m^n(ax+by) = a\,tr_m^n(x) + b\,tr_m^n(y)$, for all $a, b \in F_{2^m}$, $x, y \in F_{2^n}$; (ii) $tr_m^n(x^{2^m}) = tr_m^n(x)$, for all $x \in F_{2^n}$; and (iii) $tr_1^n(x) = tr_1^m(tr_m^n(x))$, for all $x \in F_{2^n}$. See [10], [11] for the detailed properties of the trace function.

For the remaining, we are interested in the case where $n = em$ for integers

$m > 1$ and $e > 1$. We use the following notation:

- $N = 2^n - 1$, $M = 2^m - 1$, and $T = \frac{N}{M} = \frac{2^n - 1}{2^m - 1}$.
- α and β are primitive elements of F_{2^m} and F_{2^n}, respectively.
- $\{b(t_1),\ t_1 = 0,1,\cdots,M-1\}$

  = a binary sequence of period M with ideal autocorrelation property.
- $\{c(t),\ t = 0,1,\cdots,N-1\}$

  = a binary sequence of period N as an extension of $\{b(t_1)\}$.

Using these notations, we quote the construction of binary sequences with ideal autocorrelation property[16] by No. *et al.* as follows:

Theorem 1 [16] Let m and n be positive integers such that $m \mid n$. Let β 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 $\{b(t_1),\ t_1 = 0, 1,\cdots,M-1\}$ of period $M = 2^m - 1$ given by

$$b(t_1) = \sum_{a \in I} tr_1^m(\alpha^{at_1})$$

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

$$c(t) = \sum_{a \in I} tr_1^m\{[tr_m^n(\beta^t)]^{ar}\}$$

also has the ideal autocorrelation property.

III. GMW Sequences as the Extension of *m*-Sequences

The m-sequences and the GMW sequences are best described in terms of the trace function over a finite field [20]. In this section we show that GMW sequences are the natural extensions of m-sequences in the sense of Theorem 1.

Let m and n be positive integers such that $m \mid n$. Let α and β be primitive elements of F_{2^m} and F_{2^n}, respectively. Let $\{b(t_1),\ t_1 = 0,1,\cdots,M-1\}$ be a binary m-sequence of period $M = 2^m - 1$, given by

$$b(t_1) = tr_1^m(\alpha^{t_1}).$$

Note that the m-sequence $\{b(t_1)\}$ is a binary sequence with ideal autocorrelation

property. Let r be an integer relatively prime to M. Applying Theorem 1, the sequence $\{c(t),\ \ t=0,1,\cdots,N-1\}$ of period N defined by

$$c(t)=tr_1^m\{[tr_m^n(\beta^t)]^r\}$$

has the ideal autocorrelation property. Note that it is exactly the GMW sequence defined in [19]. In particular, the sequence $\{c(t)\}$ is an m-sequence of period N, when $r=1$.

Consider the number N_{seq} of cyclically distinct GMW sequences $\{c(t), t=0,1,\cdots,N-1\}$ of period $N=2^n-1$ with ideal autocorrelation property. Since $I=\{1\}$, it is easy to check that $N_I=\phi(M)/m$. Hence we have

$$N_{seq}=\frac{\phi(M)}{m}\cdot\frac{\phi(N)}{n},$$

which is a well-known result [19].

Example 2 Let $\{b(t_1),\ \ t_1=0,1,\cdots,6\}$ be a binary m-sequence of period 7, given by

$$b(t_1)=tr_1^3(\alpha^{t_1})$$

for a primitive element α of F_8. Let r be an integer relatively prime to 7. Since the m-sequence $\{b(t_1)\}$ is a binary sequence with ideal autocorrelation property, it can be extended to the GMW sequence $\{c(t),\ \ t=0,1,\cdots,62\}$ of period 63 defined by

$$c(t)=tr_1^3\{[tr_3^6(\beta^t)]^r\}$$

for a primitive element β in F_{64}, and hence $\{c(t)\}$ has the ideal autocorrelation property by Theorem 1.

IV. New Binary Sequences with Ideal Autocorrelation Property

A. Binary Sequences from Legendre Sequences

Let p be an odd prime. The Legendre sequence $\{b(t),\ \ t=0,1,\cdots p-1\}$ of period p is defined as

$$b(t)=\begin{cases}1 & \text{if } t=0 \mod p,\\ 0 & \text{if } t \text{ is a quadratic residue } \mod p,\\ 1 & \text{if } t \text{ is a quadratic non-residue } \mod p.\end{cases}$$

(1)

It is not difficult to show that $\{b(t)\}$ has the ideal autocorrelation property if and

only if $p = 3 \pmod 4$ [3], [7].

It seems to be quite difficult to find any simple and explicit representation of the Legendre sequence $\{b(t)\}$ for all primes $p = 3 \pmod 4$ using the trace function over a finite field. However, it is recently shown that the Legendre sequences of period $p = 2^m - 1$ can be explicitly described using the trace function from F_{2^m} to F_2 [15].

Proposition 3 Let $M = 2^m - 1$ be a prime for some integer $m \geq 3$ and let u be a primitive element of Z_M, the set of intgers mod M. Then there exists a primitive element α of F_{2^m} such that

$$\sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m(\alpha^{u^{2i}}) = 0,$$

and the sequence $\{s(t), \quad t = 0, 1, 2, \cdots, M-1\}$ of period M given by

$$s(t) = \sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^n(\alpha^{u^{2i}t}) \qquad (2)$$

is exactly the Legendre sequence given in Eq.(1).

Consider a decimation $\{s(u^j t)\}$ by u^j of the sequence $\{s(t)\}$ given in Eq. (2). Clearly, if j is an even integer, then $\{s(u^j t)\}$ is the Legendre sequence given in Eq. (1).

It is also easy to show that if j is an odd integer, then $\{s(u^j t)\}$ is the sequence given by

$$s(u^j t) = \begin{cases} 1 & \text{if } t = 0 \mod M, \\ 1 & \text{if } t \text{ is a quadratic residue } \mod M, \\ 0 & \text{if } t \text{ is a quadratic non-residue } \mod M. \end{cases}$$

Since $\{s(u^j t)\}$ has the ideal autocorrelation property regardless of j, we will also refer to it as a Legendre sequence hereafter. The following theorem is the consequence of Theorem 1 and Proposition 3.

Theorem 4 Let m be an integer such that $M = 2^m - 1$ is prime and let n be a multiple of m. Let u be a primitive element of Z_M, the set of intgers mod M, and let β be a primitive element of F_{2^n}. For an integer r, $1 \leq r \leq M-1$, relatively prime to

M, the sequence $\{c(t), \quad t = 0,1,\cdots,N-1\}$ of period $N = 2^n - 1$ given by

$$c(t) = \sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m\{[tr_m^n(\beta^t)]^{ru^{2i}}\}$$

has the ideal autocorrelation property.

Consider the number N_{seq} of cyclically distinct extensions $\{c(t)\}$ of period $N = 2^n - 1$ with ideal autocorrelation property, constructed from the Legendre sequences of period $2^m - 1$. Since we have

$$I = \{u^{2i} \mid i = 0,1,\cdots,(M-1)/2m-1\}$$

for a primitive element u in Z_M, it is easy to check that $N_I = 2$. Hence we get

$$N_{seq} = 2\frac{\phi(N)}{n}.$$

Example 5 Let $m = 7$ and thus $M = 127(=2^7-1)$. It is easy to check that the element $u = 3$ is primitive in Z_{127}. Let α be the primitive element of F_{2^7} satisfying $\alpha^7 + \alpha^4 + 1 = 0$. Then we have

$$\sum_{i=0}^{\frac{M-1}{2m}-1} tr_1^m(\alpha^{u^{2i}}) = \sum_{i=0}^{8} tr_1^7(\alpha^{3^{2i}}) = 0.$$

The sequence $\{b(t_1), \quad t_1 = 0,1,\cdots,126\}$ given by

$$b(t_1) = \sum_{i=0}^{8} tr_1^7(\alpha^{3^{2i}t_1}) = \sum_{i=0}^{8} tr_1^7(\alpha^{9^i t_1})$$

is the Legendre sequence of period 127.

Let n be a multiple of m=7. Let β be a primitive element of F_{2^n}. Then the sequence $\{b(t_1)\}$ can be extended to a binary sequence of period $2^n - 1$ with ideal autocorrelation property. That is, for an integer r, $1 \le r \le 6$, the sequence $\{c(t), \quad t = 0,1,\cdots,N-1\}$ of period $N = 2^n - 1$ given by

$$c(t) = \sum_{i=0}^{8} tr_1^7\{[tr_7^n(\beta^t)]^{r9^i}\}$$

has the ideal autocorrelation property by Theorem 4. Note that there are $2\phi(N)/n$ cyclically distinct extensions of period N with ideal autocorrelation property, constructed from the Legendre sequences of period 127.

B. Binary Sequences from Hall's Sextic Residue Sequences

Another construction for binary sequences of period $M = 2^m - 1$ with ideal autocorrelation is associated with Hall's difference set only when m is 5, 7, and 17 [1], [18]. In the case that $m = 5$, the Hall's sextic residue sequences are exactly the m-sequences.

Consider the case that $m = 7$ and $M = 127$. The element $u = 3$ is primitive in Z_{127}.

Let α be a primitive element of the finite field F_{2^7}. Using a computer search for a trace representation of the Hall's sextic residue sequence $\{b(t_1), \ t_1 = 0,1,\cdots, 126\}$ of period 127, it is found that it can be expressed as

$$b(t_1) = \sum_{i=0}^{2} tr_1^7(\alpha^{3^{6i}t_1}).$$

Note that its decimation by any integer r also has the ideal autocorrelation property. Hence, $\{b(t_1)\}$ and all of its decimations are called the Hall's sextic residue sequences.

Applying Theorem 1 to $\{b(t_1)\}$, we have extensions of Hall's sextic residue sequences of period 127.

Theorem 6 Let n be a multiple of 7 and let β be a primitive element of F_{2^n}. Then for any integer r, $1 \le r \le 126$, the sequence $\{c(t), \ t = 0,1,\cdots,N-1\}$ of period $N = 2^n - 1$ defined by

$$c(t) = \sum_{i=0}^{2} tr_1^7([tr_7^n(\beta^t)]^{r3^{6i}})$$

has the ideal autocorrelation property.

Consider the number N_{seq} of cyclically distinct extensions $\{c(t)\}$ of period $N = 2^n - 1$ with ideal autocorrelation property, constructed from the Hall's sextic residue sequences of period 127. Since $I = \{3^{6i} \mid i = 0,1,2\} \in Z_{127}$, it is easy to check that $N_I = 6$. Hence we have

$$N_{seq} = 6 \ \frac{\phi(N)}{n}.$$

C. Binary Sequences from Known Sequences of Miscellaneous Type

To classify and construct balanced binary sequences of period 2^n-1 is a very interesting problem in both theory and practice [6], [7]. Especially, the balanced binary sequences of period 2^n-1 with ideal autocorrelation property find many applications in spread spectrum communication systems. A complete search for those sequences was conducted for period 127 by Baumert and Fredrickson [2], 255 by Cheng [4], 511 by Drier [5].

It is well-known that there are 6 *inequivalent* binary sequences of period 127 with ideal autocorrelation property: an m-sequence, a Legendre sequence, a Hall's sextic residue sequence, and three others called the miscellaneous type I, II, and III. Let α be a primitive element of the finite field F_{2^7}. Then the sequences of miscellaneous type have the following trace representation by a computer search:

(i) Miscellaneous Type I

$$b_I(t_1) = tr_1^7(\alpha^{t_1}) + tr_1^7(\alpha^{5t_1}) + tr_1^7(\alpha^{7t_1}) + tr_1^7(\alpha^{11t_1}) + tr_1^7(\alpha^{31t_1}),$$

(ii) Miscellaneous Type II

$$b_{II}(t_1) = tr_1^7(\alpha^{t_1}) + tr_1^7(\alpha^{3t_1}) + tr_1^7(\alpha^{7t_1}) + tr_1^7(\alpha^{19t_1}) + tr_1^7(\alpha^{29t_1}),$$

(iii) Miscellaneous Type III

$$b_{III}(t_1) = tr_1^7(\alpha^{t_1}) + tr_1^7(\alpha^{9t_1}) + tr_1^7(\alpha^{13t_1})$$

where t_1 runs from 0 to 126. Hence, we have the extensions of these sequences in the following.

Theorem 7 Let n be a multiple of 7 and let β be a primitive element of F_{2^n}. Then there are the following inequivalent binary sequences of period $N = 2^n-1$ with ideal autocorrelation property:

$$\begin{aligned} c_I(t) &= tr_1^7([tr_7^n(\beta^t)]^r) + tr_1^7([tr_7^n(\beta^t)]^{5r}) + tr_1^7([tr_7^n(\beta^t)]^{7r}) \\ &\quad + tr_1^7([tr_7^n(\beta^t)]^{11r}) + tr_1^7([tr_7^n(\beta^t)]^{31r}), \end{aligned}$$

$$\begin{aligned} c_{II}(t) &= tr_1^7([tr_7^n(\beta^t)]^r) + tr_1^7([tr_7^n(\beta^t)]^{3r}) + tr_1^7([tr_7^n(\beta^t)]^{7r}) \\ &\quad + tr_1^7([tr_7^n(\beta^t)]^{19r}) + tr_1^7([tr_7^n(\beta^t)]^{29r}), \end{aligned}$$

and

$$c_{III}(t) = tr_1^7([tr_7^n(\beta^t)]^r) + tr_1^7([tr_7^n(\beta^t)]^{9r}) + tr_1^7([tr_7^n(\beta^t)]^{13r})$$

where t runs from 0 to $N-1$ and r, $1 \le r \le 126$, is an integer.

For a multiple n of 7, consider the number N_{seq} of cyclically distinct extensions $\{c(t)\}$ of period $N=2^n-1$ with ideal autocorrelation property, constructed from a miscellaneous type sequence of period 127. It is easily checked that $N_I=\phi(127)/7=18$. Hence we have $N_{seq}=18\ \phi(N)/n$ for a binary sequence of each miscellaneous type.

At period 255, it is found that there are 4 *inequivalent* binary sequences with ideal autocorrelation property: an m-sequence, a GMW sequence, and two others called the miscellaneous type I and II. Let α be a primitive element of the finite field F_{2^8}. The sequences of miscellaneous type have the following trace representation by a computer search:

(i) Miscellaneous Type I

$$b_I(t_1)=tr_1^8(\alpha^{t_1})+tr_1^8(\alpha^{3t_1})+tr_1^8(\alpha^{11t_1})+tr_1^8(\alpha^{43t_1})+tr_1^8(\alpha^{111t_1}),$$

(ii) Miscellaneous Type II

$$b_{II}(t_1)=tr_1^8(\alpha^{t_1})+tr_1^8(\alpha^{7t_1})+tr_1^8(\alpha^{9t_1})+tr_1^8(\alpha^{47t_1})+tr_1^8(\beta^{63t_1}).$$

where t_1 runs from 0 to 254. Hence, we have the following extensions of these sequences.

Theorem 8 Let n be a multiple of 8 and let β be a primitive element of F_{2^n}. Then there are the following inequivalent binary sequences of period $N=2^n-1$ with ideal autocorrelation property:

$$\begin{aligned}c_I(t) &= tr_1^8([tr_8^n(\beta^t)]^r)+tr_1^8([tr_8^n(\beta^t)]^{3r})+tr_1^8([tr_8^n(\beta^t)]^{11r})\\ &\quad+tr_1^8([tr_8^n(\beta^t)]^{43r})+tr_1^8([tr_8^n(\beta^t)]^{111r}),\end{aligned}$$

and

$$\begin{aligned}c_{II}(t) &= tr_1^8([tr_8^n(\beta^t)]^r)+tr_1^8([tr_8^n(\beta^t)]^{7r})+tr_1^8([tr_8^n(\beta^t)]^{9r})\\ &\quad+tr_1^8([tr_8^n(\beta^t)]^{47r})+tr_1^8([tr_8^n(\beta^t)]^{63r})\end{aligned}$$

where t runs from 0 to $N-1$ and r, $1\le r\le 254$, is an integer relatively prime to 255.

As in the case of period 127, it is easily checked that $N_I=\phi(255)/8=16$. Hence, for a multiple n of 8, the number N_{seq} of cyclically distinct extensions $\{c(t)\}$ of period $N=2^n-1$ with ideal autocorrelation property, constructed from a miscellaneous type sequence of period 255, is given by

$$N_{seq} = 16 \quad \phi(N)/n.$$

At period 511, there are 4 *inequivalent* examples: an *m*-sequence, a GMW sequence, and two others called the miscellaneous type I and II. Let α be a primitive element of the finite field F_{2^9}. The sequences of miscellaneous type have the following trace representation by a computer search:

(i) Miscellaneous Type I

$$b_I(t_1) = tr_1^9(\alpha^{t_1}) + tr_1^9(\alpha^{11t_1}) + tr_1^9(\alpha^{43t_1}),$$

(ii) Miscellaneous Type II

$$b_{II}(t_1) = tr_1^9(\alpha^{t_1}) + tr_1^9(\alpha^{17t_1}) + tr_1^9(\alpha^{25t_1})$$

where t_1 runs from 0 to 510. Hence, we have the extensions of these sequences in the following.

Theorem 9 Let n be a multiple of 9 and let β be a primitive element of F_{2^n}. Then there are the following inequivalent binary sequences of period $N = 2^n - 1$ with ideal autocorrelation property:

$$c_I(t) = tr_1^9([tr_9^n(\beta^t)]^r) + tr_1^9([tr_9^n(\beta^t)]^{11r}) + tr_1^9([tr_9^n(\beta^t)]^{43r})$$

and

$$c_{II}(t) = tr_1^9([tr_9^n(\beta^t)]^r) + tr_1^9([tr_9^n(\beta^t)]^{17r}) + tr_1^9([tr_9^n(\beta^t)]^{25r})$$

where t runs from 0 to $N-1$ and r, $1 \le r \le 510$, is an integer relatively prime to 511.

It is easily checked that $N_I = \phi(511)/9 = 48$. Thus for a multiple n of 9, there are $N_{seq} = 48 \quad \phi(N)/n$ cyclically distinct extensions $\{c(t)\}$ of period $N = 2^n - 1$ with ideal autocorrelation property, which are constructed from a miscellaneous type sequence of period 511.

In the case of period 1023, a computer search found that there is at least one binary sequence $\{b(t_1), \; t_1 = 0,1,\cdots,1022\}$ with ideal autocorrelation property, which is *inequivalent* to any of known sequences such as the *m*-sequences, the GMW sequences, and the extensions of the Legendre sequences. It is given by

$$b(t_1) = tr_1^{10}(\alpha^{t_1}) + tr_1^{10}(\alpha^{9t_1}) + tr_1^{10}(\alpha^{57t_1}) + tr_1^{10}(\alpha^{73t_1}) + tr_1^{10}(\alpha^{121t_1})$$

where α is a primitive element of the finite field $F_{2^{10}}$. Hence, we have its extension in the following.

Theorem 10 Let n be a multiple of 10 and let β be a primitive element of F_{2^n}. Then there is a binary sequences of period $N = 2^n - 1$ with ideal autocorrelation property, given by

$$\begin{aligned} c(t) &= tr_1^{10}([tr_{10}^n(\beta^t)]^r) + tr_1^{10}([tr_{10}^n(\beta^t)]^{9r}) + tr_1^{10}([tr_{10}^n(\beta^t)]^{57r}) \\ &\quad + tr_1^{10}([tr_{10}^n(\beta^t)]^{73r}) + tr_1^{10}([tr_{10}^n(\beta^t)]^{121r}) \end{aligned}$$

where t runs from 0 to $N-1$ and r, $1 \le r \le 1022$, is an integer relatively prime to 1023.

It is easily checked that $N_I = \phi(1023)/10 = 60$. Note that a multiple n of 10, there are $N_{seq} = 60\ \phi(N)/n$ cyclically distinct extensions $\{c(t)\}$ of period $N = 2^n - 1$ with ideal autocorrelation property, which are constructed from the above miscellaneous type sequence $\{b(t_1)\}$ of period 1023.

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer-Verlag, 1971.

[2] L. D. Baumert and Fredrickson, ''The cyclotomic numbers of order 18 with applications to difference sets,'' *Math. Comp.*, vol. 21, pp. 204-219, 1967.

[3] D. M. Burton, *Elementary Number Theory*, Allyn and Bacon, Inc., 1980.

[4] U. Cheng, ''Exhaustive construction of (255, 127, 63) cyclic difference sets,'' *J. Combinatorial Theory*, vol. A-35, pp. 115-125, 1983.

[5] R. Drier, ''(511, 255, 127) cyclic difference sets,'' IDA talk, July 1992.

[6] S. W. Golomb, ''On the classification of balanced binary sequences of period 2^n-1,'' *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730-732, Nov. 1980.

[7] S. W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA 1982.

[8] D. Jungnickel, ''Difference sets,'' in *Contemporary Design Theory*, J. H. Dinitz and D. R. Stinson, Eds., John Wiley and Sons, Inc., pp. 241-324, 1992.

[9] A. Klapper, A. H. Chan, and M. Goresky, ''Cascaded GMW sequences,'' *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 177-183, Jan. 1989.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*, Addison-Wesley, Reading, MA, 1983.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[12] J. -S. No, ''A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span,'' Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, May 1988.

[13] J. -S. No, ''Generalization of GMW sequences and No sequences,'' *IEEE Trans. Inform. Theory*. vol. 42, no. 1, pp. 260-262, Jan. 1996.

[14] 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. Inform. Theory*, vol. IT-35, pp. 371-379, Mar. 1989.

[15] 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. Inform. Theory*, vol. 42, No. 6, Nov., 1996.

[17] J. -S. No, K. Yang, H. Chung, and H. -Y. Song, ''Theory on the construction of binary sequences with ideal autocorrelation,'' preprint, 1997.

[18] H.-S. Oh, C.-M. Park, S.-H. Hwang, C.-E. Kang, and J.-Y. Son, ''Coherent demodulation performance of pilot aided QPSK modulation in wideband CDMA reverse channel,'' *J. of Elec. Engin. and Inform. Sci.*, A joint publication of KIEE, KITE, KISS, KICS, KEES, KIISC, and IEEE Korea, vol. 2, no. 1, pp. 28-33, Feb. 1997.

[19] D. V. Sarwate and M. B. Pursley, ''Crosscorrelation Properties of Pseudorandom and Related Sequences,'' *Proc. IEEE*, vol. IT-68, pp. 593-619, May 1980.

[20] R. A. Scholtz and L. R. Welch, ''GMW sequences,'' *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548-553, May 1984.

[21] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. 1, Computer Science Press, Rockville, MD, 1985.

[22] H. Y. Song and S. W. Golomb, ''On the existence of cyclic Hadamard difference sets,'' *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 1266-1268, July 1994.

[23] W. S. Yoon, '' Concatenated orthogonal/PN spreading scheme for a multitone CDMA system,'' *J. of Elec. Engin. and Inform. Sci.*, A joint publication of KIEE, KITE, KISS, KICS, KEES, KIISC, and IEEE Korea, vol. 2, no. 4, pp. 19-22, August 1997.

[24] TIA/EIA/IS-95, *Mobile Station -- Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, published by Telecommunications Industry Association as a North American 1.5 MHz Cellular CDMA Air-Interface Standard, July 1993.