Extended Binary d-form Sequences with the Good Correlation Properties*

Chusheng Fu¹,², Hong Wen¹,²

1. National Key Lab of Communication of University of Electronic Science Technology of China
   Chengdu 610054, China
2. State Key Lab of Mobile Communication of Southeast University, Nanjing 210096, China
E-mail: fuchush@uestc.edu.cn

Abstract—In this paper, a construction method to generate binary extended d-form sequences with the same correlation properties as d-form sequences is proposed and using the TN sequences (a special case of d-form sequences), the extended TN sequences with the optimal correlation are constructed. Finally, we give an example of the families of the extended TN sequences, which are constructed from Legendre sequences.

Key words: Correlation, d-form sequences, binary sequences, spread-spectrum, families of sequences, No sequences, extended sequences

I. INTRODUCTION AND PRELIMINARIES

Binary sequences have many applications in Code Division Multiple Access (CDMA) system, which has been adopted as a standard for multiple-access methods in mobile radio communication systems. Signal designing for CDMA systems has become an interesting research topic in application areas. One of the most important research areas for signal design for CDMA system is the design of binary sequences with good correlation properties.


In this paper, we use the method [4] introduced by No to construct the new families, called extended d-form sequences, with the same crosscorrelation as the d-form sequences families [1]. Using TN sequences found by Klapper, extended TN sequences with optimal correlation property are constructed. Finally, an example of optimal families of binary extended TN sequences constructed from the Legendre sequences of Mersenne prime period is given. The new families with k = 1 include the families No introduced [4] as a special case.

In what follows, let e and m be positive integers, let n = em , and let \( T_{m}^{n} \) be the trace function from GF \((2^{e})\) to GF \((2^{m})\)

\[ \text{Tr}_{m}^{n}(x) = \sum_{i=0}^{m-1} x^{2^{i}} \]  \hspace{1cm} (1)

Also, let \( N_{m}^{n} \) be the norm function from GF \((2^{e})\) to GF \((2^{m})\)

\[ N_{m}^{n} = \prod_{i=0}^{m-1} x^{2^{2^{i}}} = x^{(2^{e}-1)(2^{m}-1)} \]  \hspace{1cm} (2)

For simplicity we write \( q = 2^{m} \).

If \( q \) is a prime congruent to \( 3 \) modulo \( 4 \), then \( \alpha = \sqrt{-1} \) is a primitive element of \( \mathbb{F}_{q} \) and \( y \in \mathbb{F}_{q} \), a function that satisfies

\[ H(y\alpha) = y^{q}H(x) \]  \hspace{1cm} (3)

Using the d-form function \( H(x) \), he introduces the d-form sequences as follows.

Definition [6]: For an integer \( r \), \( 1 \leq r < M \), relatively prime to \( M = q - 1 \), a d-form sequence of period \( N = q^{r} - 1 \) is defined as

\[ c_{r}(t) = \text{Tr}_{m}^{n}(H(\alpha^{t})) \]  \hspace{1cm} (4)

where \( \alpha \) is a primitive element in \( \mathbb{F}_{q^{r}} \) and \( H(\alpha^{t}) \) is a d-form function, as defined in (3).

Recall that the cross-correlation \( R_{n}(\tau) \) with shift \( \tau \), of two sequences \( \{c^{i}(t)\} \) and \( \{c^{j}(t)\} \) of period \( N = q^{r} - 1 \) is defined by

\[ R_{n}(\tau) = \sum_{t=0}^{N-1} (-1)^{c^{i}(t)\oplus c^{j}(t\oplus \tau)} \]  \hspace{1cm} (5)

II. CONSTRUCTION OF EXTENDED D-FORM SEQUENCES

In this section, we will present the method to construct extended d-form sequences \( s \).

Theorem 1: Let \( e \) and \( m \) be positive integers, let \( n = em \) , and let \( q = 2^{m} \). Let \( \alpha, \beta \) be primitive elements of \( \mathbb{F}_{q^{r}} \), \( \mathbb{F}_{q} \), respectively, and set \( \alpha^{T} = \beta \) where \( T = (q^{r} - 1)/(q - 1) \). Assume that for an index set \( I \), the sequence \( \{b(t), t_{1}, 0, 1, \ldots, M - 1\} \) of period \( M = q - 1 \) given by

\[ b(t) = \sum_{x=1}^{q} \text{Tr}_{m}^{n}(\beta x^{t}) \]  \hspace{1cm} (6)
has the ideal autocorrelation property. Let $r$ and $d$ be positive integers such that $gcd(r, M) = gcd(d, M) = 1$, $1 \leq r < M$. Let the index set $I$ be in (6), and let $H_1(\alpha^I r)$ be a $d$-form function in (1). Define the extended $d$-form sequence $\{c_1(t)\}$ as

$$c_1(t) = \sum_{m=t}^\infty \text{Tr}^m_1[H(\alpha^I r)]^r$$

(7)

Let the integers $m$, $e$, and $r$, and primitive elements $\alpha$ be fixed. Let $R_0(t)$ be the crosscorrelation of sequence $\{c_1^{(j)}(t)\}$, which are defined in (6) according to $d$-form functions $H_1(\alpha^I r)$ and $H_1(\alpha^I r)$, respectively, at shift $\tau$. Let

$$z_{1} = \|0 \leq t < q^e - 1 H_1(\alpha^t) + H_1(\alpha^{t+e}) = 0\|$$

(8)

Then

$$R_0(t) = \frac{z_{1}(\alpha^e - 1)}{q - 1}$$

(9)

**Proof:** Let $T = (q^e - 1)/(q - 1) N = q^e - 1$. For any $t$, $0 \leq t < N$, we can write

$$t = T_{1}t_1 + t_2 \quad 0 \leq t_2 < M_2 \leq T$$

(10)

Since for any $\alpha \in GF(q)$, we have $\alpha^{-1} = \beta \in GF(q)$, it follows that $H_1(\alpha^e) = H_1(\alpha^{t+e})$

Thus the terms of the sequence $\{c_1(t)\}$ can be written

$$c_1(t) = \sum_{m=t}^\infty \text{Tr}^m_1[H(\alpha^t)]^r$$

(11)

Letting

$$f(t) = [H_1(\alpha^t)]^r + [H_1(\alpha^{t+e})]$$

(12)

we have

$$c_1^{(j)}(t) + c_1^{(j)}(t + \tau) = \sum_{m=t}^\infty \text{Tr}^m_1[H(\alpha^t)]^r$$

(13)

$$R_0(t) = \sum_{j=0}^{N-1} \sum_{t_2=0}^{M-1} \left( -1 \right) c_1^{(j)}(t + \tau)$$

(14)

We note that the inner sum $\sum_{m=t}^\infty \text{Tr}^m_1[H(\alpha^m)]^r$ yields $M$ when $f(t_2) = 0$. When $f(t_2) \neq 0$ we claim that the inner sum is $-1$. If $f(t_2) \neq 0$, the exponent to $(-1)$ in the inner sum is essentially a shift of the sequence $\{b(t_2)\}$.

Since $gcd(r, M) = 1$, it is obvious that the sequence $\{b(t_2)\}$ is balanced and has the ideal autocorrelation property. This implies that the inner sum gives $-1$. If we let $z$ be the number of values of $t_2$, $0 \leq t_2 < T$, for which $f(t_2) = 0$, then

$$R_0(t) = [T - z] + [q - 3] = \frac{q - 1}{q - 1}$$

(15)

To complete the proof, we observe that $f(t + \tau) = \alpha^{r+\tau} f(t)$, so that

$$z = \|0 \leq t < N \|$$

(16)

This is precisely $z_1/q - 1$, and the result follows immediately.

### III. Extended TN Sequences

Klapper [1] introduces TN sequences as a special case of the $d$-form sequences. As an example, extended TN sequences can be constructed as follows.

Theorem 2: Let $m$ and $k$ be positive integers, let $n = 2mk$, and let $q = 2^n$. Let $r$ be a positive integer such that $gcd(r, M) = 1$, $1 \leq r < M = q - 1$. Let $\alpha$ be a primitive element in $GF(q^k)$ and let $\gamma$ be an element of $GF(q^k)$. Let the index set $I$ be in (5). Then the sequence $\{c_{1}^{(j)}(t)\}$ given by

$$c_{1}^{(j)}(t) = \sum_{m=t}^\infty \text{Tr}^m_1[H_1(\alpha^T)]^r$$

(17)

is a extended TN sequence.

Let $\{c_{1}^{(j)}(t)\}$ and $\{c_{2}^{(j)}(t)\}$ be two extended TN sequences defined in (6), based on the same integers $m$, $k$, and $r$. Then the crosscorrelations $R_0(t)$ of $\{c_{1}^{(j)}(t)\}$ and $\{c_{2}^{(j)}(t)\}$ are three-valued with values in $\{-q^e - 1, -q^e, 1\}$ unless $i = j$ and $\tau = 0$.

**Proof:** Note that the $d$-form function is:

$$H_1(\alpha^t) = \text{Tr}^{mk}[H_1(\alpha^t) + \gamma N_{mk}^r(\alpha^t)]$$

(18)

if we let

$$T = (q^e - 1)/(q - 1) = q^e + 1$$

then $N_{mk}^r(\alpha^t) = \alpha^{t+e}$.

By Theorem 1, we have to determine the number of zeroes $z_1$ (defined as in (4)) of the quadratic form:

$$H_1(\alpha^t) + H_1(\alpha^{t+e}) = \text{Tr}^{mk}[H_1(\alpha^t) + \gamma N_{mk}^r(\alpha^t)]$$

(19)

Let $T = q^e + 1$, $N = q^e - 1$. For any $t$, $0 \leq t < N$, we can write

$$t = T_{1}t_1 + t_2 \quad 0 \leq t_2 < T$$

(20)

It follows that:

$$H_1(\alpha^t) + H_1(\alpha^{t+e}) = \text{Tr}^{mk}[H_1(\alpha^t) + \gamma N_{mk}^r(\alpha^t)]$$

(21)

Then $f(t) = \text{Tr}^{mk}[1 + \alpha^{t+e}]$.

**Proof:** Let $T = T_{1}t_1 + t_2 \quad 0 \leq t_2 < T$.

If $\omega_1$ denotes the number of values of $t_2$ for which $f(t_2) = 0$, i.e.

$$\omega_1 = \{|t_2| 0 \leq t_2 < T | f(t_2) = 0\|$$

(25)

then $f(t_2)$ takes any nonzero value precisely $(q^e - 1 - \omega_1)$ times. Moreover, $\text{Tr}^{mk}[\cdot]$ is a balanced function. It follows that

$$z_1 = (q^e + 1 - \omega_1)(q^e - 1) + \omega_1(q^e - 1)$$

(26)
We note that \( f(t + T) = \alpha^{q} f(t) \), \( 0 \leq t < N \).

Consequently, if \( \omega_{2} \) denotes the number of zeroes of the function \( f(t) \) as \( t \) varies over the range \( 0 \) to \( N - 1 \), then it must be that:

\[
\omega_{i} = \frac{\omega_{2}}{q^{i} - 1} \tag{27}
\]

Let \( \alpha = \omega_{2} \cdot 0 \leq t < N \), we write

\[
f(x) = \sum_{i=0}^{\frac{N}{2}} \chi^i(x^2 + \alpha^{2i}) = \chi^y(x^2 + \alpha^{2i}) \tag{28}
\]

where \( y = x^{q^{i} - 1} \). Here we must distinguish between two cases:

**Case 1:** \( \tau = 0 \), \( \gamma_{j} \neq \gamma_{i} \)

Here \( f(x) = \chi^y(\gamma_{j} + \gamma_{i}) \) and thus \( f(x) \) does not vanish for any nonzero value of \( x \), i.e., \( \omega_{i} = \omega_{2} = 0 \).

**Case 2:** \( \tau \neq 0 \)

In this case, \( f(x) \) vanishes if and only if the quadratic in \( y \) (28) vanishes. Since the coefficients of the quadratic in \( GF(q^{k}) \), the quadratic has 0,1, or 2 roots over \( GF(q^{k}) \). So \( \omega_{2} \in \{0,q^{k} - 1,2(q^{k} - 1)\} \), depending upon whether the roots of the quadratic in \( y \) can be expressed as \( (q^{k} - 1) \)th powers in the field.

Thus, in either case, \( \omega_{2} = 0,1, \) or \( 2 \). Note that by (8) this implies that \( \omega_{i} \) takes three-valued, with values in \( \{q^{k-1} - q + 1, q^{2k-1} - q^{k-1} - 1, q^{k-1} - 1\} \). From Theorem 1, the result follows immediately.

**Remark 1:** The families that No [4] introduced in 1997 can be obtained from Theorem 2 by letting \( k = 1 \).

Let \( p \) be an odd prime. The Legendre sequence \( \{b(t)\} \) of period \( p \) is defined as:

\[
b(t) = \begin{cases} 
1, & \text{if } t = 0 \text{ mod } p \\
0, & \text{if } t \text{ is a quadratic residue } \text{ mod } p \\
1, & \text{if } t \text{ is a quadratic nonresidue } \text{ mod } p
\end{cases} \tag{29}
\]

It is not difficult to show that \( \{b(t)\} \) has the ideal autocorrelation property if and only if \( p = 3 \text{(mod 4)} \). A trace represent of the Legendre sequence of period \( p = 2^n - 1 \) (called Mersenne prime) was derived as follows:

**Lemma 5:** Let \( M = 2^n - 1 \) be a prime for some integer \( m \geq 3 \) and let \( u \) be a primitive element of \( Z_{M} \), the set of integers mod \( M \). Then there exists a primitive element \( \alpha \) of \( GF(2^{n}) \) such that

\[
\sum_{i=0}^{(M-1)/2m} Tr_{m}^{i}(\alpha^{2j}) = 0 \tag{30}
\]

and the sequence \( \{c(t)\} \) of period \( M \) given by

\[
c(t) = \sum_{i=0}^{(M-1)/2m} Tr_{m}(\alpha^{2i}) \tag{31}
\]

is exactly the Legendre sequence in (29).

The following theorem is the consequence of Theorem 2.

**Theorem 3:** Let \( m \) be an integer such that \( M = 2^{n} - 1 \) is a prime. Let \( k \) be an integer, let \( n = 2m\cdot k \), let \( q = 2^{n} \). Let \( u \) be a primitive element of \( Z_{M} \), the set of integers mod \( M \). Let \( \alpha \) be a primitive element in \( GF(q^{k}) \) and let \( \gamma \) be an element of \( GF(q^{k}) \). For an integer \( r \), \( 1 \leq r < M \), let \( \{c(j)(t)\} \) be the sequence of period \( N = q^{2k} - 1 \) given by

\[
c(j)(t) = \sum_{i=0}^{(M-1)/2m} Tr_{m}(\alpha^{3i}) \tag{32}
\]

Then the family \( \Gamma \) defined by

\[
\Gamma = \{\{c(j)(t)\} \mid j = 1,2,...,M\} \tag{33}
\]

The crosscorrelation function \( R_{0}(\tau) \) associated with the \( i \)th and \( j \)th sequences in the family \( \Gamma \) takes only three values \(-q^{k} - 1, 1, \) or \( q^{k} - 1 \) for any \( i, j \), and \( \tau \) except for the case where \( i = j \) and \( \tau = 0 \text{(mod N)} \).

Example: Let \( m = 7 \) be an integer such that \( M = 2^{7} - 1 = 127 \) is a prime. It is easy to check that \( u = 3 \) is a primitive element of \( Z_{127} \). Let \( \beta \) be a primitive element of \( GF(2^{7}) \). The sequence \( \{b(t)\} \) given by

\[
b(t) = \sum_{k=0}^{9} Tr_{7}(\beta^{3k}) \tag{34}
\]

is the Legendre sequence of period 127.

Let \( k = 2 \) and \( n = 2m\cdot k = 28 \). Let \( \alpha \) be a primitive element in \( GF(2^{n}) \). For \( \gamma \in GF(2^{n}) \), we define:

\[
c(j)(t) = \sum_{i=0}^{8} Tr_{7}(\alpha^{2i}) \tag{35}
\]

Where \( r, 1 \leq r < 127, \) is an integer, Then the family \( \Gamma \) defined by:

\[
\Gamma = \{\{c(j)(t)\} \mid j = 1,2,...,16384\} \tag{36}
\]

The crosscorrelation function \( R_{0}(\tau) \) associated with the \( i \)th and \( j \)th sequences in the family \( \Gamma \) takes only three values \(-16387, 1, \) or \( 16385 \) for any \( i, j \), and \( \tau \) except for the case where \( i = j \) and \( \tau = 0 \text{(mod N)} \).

**Remark 2:** As in the case of legrende sequences, other binary sequences with ideal autocorrelation property such as Hall’s sextic residue sequences and three miscellaneous sequences can be used to construction extended TN sequences.

QF sequences are another special case of the d-form sequences. By this method presented in this paper, we can construct extended QF sequences that have the same crosscorrelation as the QF sequences.

**IV. CONCLUSION**

In this paper, using the method introduced by No the new families with the optimal crosscorrelation are constructed. Using TN sequences found by krapper, extended TN sequences with optimal crosscorrelation property are obtained. Finally, an example of optimal...
families of binary extended TN sequences constructed from the Legendre sequences of Mersenne prime period is given.

As in the case of Legendre sequences, other binary sequences with ideal autocorrelation property such as Hall’s sextic residue sequences and three miscellaneous sequences can be used to construct extended TN sequences. QF sequences [7] are another special case of the d-form sequences. By this method presented in this paper, we can construct extended QF sequences that have the same crosscorrelation as the QF sequences.

REFERENCE