Designs, Codes and Cryptography, 33, 23–37, 2004

On the *p*-Ranks and Characteristic Polynomials of Cyclic Difference Sets

JONG-SEON NO
School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-742, Korea

DONG-JOON SHIN
Division of Electrical and Computer Engineering, Hanyang University, Seoul 133-791, Korea

TOR HELLESETH
Department of Informatics, University of Bergen, N-5020 Bergen, Norway

Communicated by: D. Jungnickel

Received February 15, 2001; Revised September 24, 2002; Accepted October 9, 2002

Abstract. In this paper, the *p*-ranks and characteristic polynomials of cyclic difference sets are derived by expanding the trace expressions of their characteristic sequences. Using this method, it is shown that the 3-ranks and characteristic polynomials of the Helleseth–Kumar–Martinsen (HKM) difference set and the Lin difference set can be easily obtained. Also, the *p*-rank of a Singer difference set is reviewed and the characteristic polynomial is calculated using our approach.

Keywords: cyclic difference set, characteristic polynomial, *p*-rank

AMS Classification: 05B10, 11B50

1. Introduction

It is well-known that a cyclic difference set with Singer parameters $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$ [7,17] is equivalent to a binary sequences of period 2^n-1 with ideal autocorrelation [4,5,14–16]. Recently, nonbinary sequences with ideal autocorrelation have been investigated. Helleseth et al. [8] found ternary sequences with ideal autocorrelation that turned out to be cyclic difference sets with Singer parameters $((3^{3k}-1)/(3-1), (3^{3k-1}-1)/(3-1), (3^{3k-2}-1)/(3-1))$ [9,13]. Lin [12] found a new family of ternary sequences of period 3^n-1 and conjectured that it has the ideal autocorrelation property, when $n=2m+1$. Under this assumption, a cyclic difference set (Lin difference set) with Singer parameters $((3^n-1)/(3-1), (3^{n-1}-1)/(3-1), (3^{n-2}-1)/(3-1))$ can be obtained [9,13].

In this paper, the *p*-ranks and characteristic polynomials of cyclic difference sets are derived by expanding the trace expressions of their characteristic sequences. Using this method, it is shown that the 3-ranks and characteristic polynomials of the Helleseth–Kumar–Martinsen (HKM) difference set and the Lin difference set can be

easily obtained. Also, the p-rank of a Singer difference set is reviewed and its characteristic polynomial is calculated using our approach.

2. Preliminaries

Let D be a (v, k, λ) difference set [3,10] defined as a set of k distinct residues modulo v expressed by

$$D = \{c_1, c_2, c_3, \ldots, c_k\}. \tag{1}$$

Then each non-zero residue occurs exactly λ times among the $k(k-1)$ differences $c_i - c_j, i \neq j$ and thus it satisfies

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

The complementary difference set of D is a $(v, v-k, v-2k+\lambda)$ difference set defined as

$$\overline{D} = Z_v \backslash D,$$

where Z_v is the ring of integers modulo v.

Then for integers a and b, a set $aD + b$ is defined as

$$aD + b = \{a \cdot c_1 + b, a \cdot c_2 + b, a \cdot c_3 + b, \ldots, a \cdot c_k + b\},$$

where $a \cdot c_i + b$ is taken modulo v. For integers a and b, two (v, k, λ) difference sets D_1 and D_2 are said to be inequivalent if D_1 is distinct from $aD_2 + b$ for any integer a and b, $1 \leq a \leq v-1$, $0 \leq b \leq v-1$, where a is relatively prime to v. The characteristic sequence of a cyclic difference set D in (1) is defined as the binary sequence

$$s(t) = \begin{cases} 1, & \text{if } t \in D, \\ 0, & \text{if } t \notin D, \end{cases}$$

and the characteristic sequence of its complementary difference set $\overline{D}$ is defined as

$$\begin{aligned} s_c(t) &= \begin{cases} 1, & \text{if } t \in \overline{D}, \\ 0, & \text{if } t \notin \overline{D}, \end{cases} \\ &= 1 - s(t). \end{aligned}$$

The characteristic polynomial of a cyclic difference set D is defined as a least-degree linear recursion equation over F_p of the characteristic sequence $s(t)$ of D. The p-rank [6] of a cyclic difference set D is defined as the degree of characteristic polynomial of the cyclic difference set D. In order to prove the inequivalence of two cyclic difference sets, the p-rank is often used. However, it is very difficult to find the p-ranks of cyclic difference sets.

Let $n = e \cdot m > 1$ for some positive integers e and m. Then the trace function $tr_m^n(\cdot)$ is the mapping from the finite field F_{p^n} to its subfield F_{p^m} defined by Lidl and Niederreiter [11]

$$tr_m^n(x) = \sum_{i=0}^{e-1} x^{p^{m \cdot i}},$$

where x is an element in F_{p^n}.

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

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

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

iii. $tr_1^n(x) = tr_1^m(tr_m^n(x))$, for all $x \in F_{p^n}$.

Using the trace function, a p-ary m-sequence $m(t)$ of period $p^n - 1$ can be expressed as

$$m(t) = tr_1^n(\alpha^t), \tag{2}$$

where p is a prime and α is a primitive element of F_{p^n}.

3. p-Ranks and Characteristic Polynomials of Cyclic Difference Sets

As will be given in the following theorem and lemma, the characteristic sequences of a cyclic difference set and its complementary difference set can be expressed by using the trace expressions and the p-rank can be calculated by counting the number of terms in the trace expression. Moreover, by finding the minimal polynomials corresponding to this trace expression, we can easily obtain the characteristic polynomial. This method will be used to find the 3-ranks and characteristic polynomials of the HKM and the Lin difference sets in the following sections.

Let $f(t)$ be a function from the finite field F_{p^n} to its subfield F_{p^m}. Then we have the following relation:

$$[f(t)]^{p^m - 1} = \begin{cases} 1, & \text{if } f(t) \neq 0; \\ 0, & \text{if } f(t) = 0. \end{cases}$$

Therefore, using this relation, the characteristic sequence of a cyclic difference set is given in the following theorem.

THEOREM 1. *Assume that a (v, k, λ) cyclic difference set D and its complementary difference set $\overline{D}$ are defined as*

$$D = \{t \mid f(t) = 0, 0 \leq t < v\}, \tag{3}$$

$$\overline{D} = \{t \mid f(t) \neq 0, 0 \leq t < v\}, \tag{4}$$

where $f(t)$ is given as a summation of the trace function from the finite field F_{p^n} to its subfield F_{p^m}, that is

$$f(t) = \sum_{a \in I} b_a \cdot tr_m^n(\alpha^{at}),$$

for some index set $I, b_a \in F_{p^m}^*$ and a primitive elements α in F_{p^n}.

Then the characteristic sequences of the cyclic difference set D and its complementary difference set $\overline{D}$ can be expressed as

$$s(t) = 1 - s_c(t), \quad 0 \le t < v,$$

and

$$s_c(t) = [f(t)]^{p^m - 1}, \quad 0 \le t < v. \tag{5}$$

In order to find the p-rank of the cyclic difference set $\overline{D}$, we have to expand the trace expression in (5) as given in the following lemma.

LEMMA 2. *Let D and $\overline{D}$ be a (v, k, λ) cyclic difference set and its complementary difference set defined by* (3) *and* (4)*, respectively. Suppose that the trace expression of the characteristic sequence $s_c(t)$ of $\overline{D}$ can be expanded as*

$$\begin{aligned} s_c(t) &= [f(t)]^{p^m - 1} \\ &= \left[\sum_{a \in I} b_a \cdot tr_m^n(\alpha^{at}) \right]^{p^m - 1} \\ &= \sum_{j \in J} c_j \alpha^{jt}, \end{aligned} \tag{6}$$

where J is an index set and $c_j \in F_p^*$. Then the p-rank of the complementary difference set $\overline{D}$ is given as $|J|$, which means that the degree of the characteristic polynomial of $\overline{D}$ is $|J|$. Further, the p-rank of the cyclic difference set D is given as $|J| + 1$, if $|\overline{D}| = v - k$ is divisible by p.

Proof. Let $g(x)$ and $g_c(x)$ be the characteristic polynomials over F_p of a cyclic difference set D and its complementary difference set $\overline{D}$, respectively. Since there is the relationship between $s_c(t)$ and $s(t)$ given as

$$s(t) = 1 - s_c(t),$$

their characteristic polynomials are related as

$$\begin{aligned} \frac{a(x)}{g(x)} &= \frac{1}{x-1} - \frac{b(x)}{g_c(x)} \\ &= \frac{g_c(x) - (x-1)b(x)}{(x-1) \cdot g_c(x)}, \end{aligned}$$

where the polynomials $a(x)$ and $b(x)$ are relatively prime to $g(x)$ and $g_c(x)$, respectively. If $|\overline{D}| = v - k$ is divisible by p, then the number of 1's in one period of the characteristic sequence of the cyclic difference set $\overline{D}$ is a multiple of p. Therefore, the polynomial expression of the characteristic sequence possesses the factor $x - 1$ and this cancels the factor $x - 1$ in the characteristic polynomial, which means that the characteristic polynomial $g_c(x)$ is not divisible by $x - 1$. Therefore, the polynomial $g_c(x) - (x - 1)b(x)$ is relatively prime to $(x - 1)g_c(x)$ and we obtain

$$g(x) = (x - 1)g_c(x), \tag{7}$$

if $|\overline{D}| = v - k$ is divisible by p. Therefore, the p-rank of the cyclic difference set D is $|J| + 1$, if $|\overline{D}| = v - k$ is divisible by p. ■

If (6) is expressed as a summation of trace functions as

$$[f(t)]^{p^m-1} = \sum_{k\,|\,n,k>1} \sum_{a_k \in J_k} c_{a_k} \cdot tr_1^k(\alpha_k^{a_k t}),$$

where $c_{a_k} \in F_p^*, J_k$'s are index sets and α_k is a primitive element of F_{p^k}, the characteristic polynomials of the cyclic difference set D and its complementary difference set $\overline{D}$ can be expressed as in the following theorem.

THEOREM 3. *If the characteristic sequence of a cyclic difference set $\overline{D}$ is expressed as*

$$s_c(t) = \sum_{k|n,k>1} \sum_{a_k \in J_k} c_{a_k} \cdot tr_1^k(\alpha_k^{a_k t}),$$

where $c_{a_k} \in F_p^*$ and if $|\overline{D}| = v - \lambda$ is divisible by p, then the characteristic polynomials $g(x)$ and $g_c(x)$ of the cyclic difference set D and its complementary difference set $\overline{D}$ are given as follows:

$$g(x) = (x - 1) \cdot g_c(x), \tag{8}$$

$$g_c(x) = \prod_{k|n,k>1} \prod_{a_k \in J_k} M_{a_k}(x), \tag{9}$$

where $M_{a_k}(x)$ is the minimal polynomial of the element $\alpha_k^{a_k} \in F_{p^k}$.

Note that the p-rank of D is one bigger than that of $\overline{D}$. For the cyclic difference set with Singer parameters $((q^n - 1)/(q - 1), (q^{n-1} - 1)/(q - 1), (q^{n-2} - 1)/(q - 1))$, where $q = p^m, v - k = q^{n-1} = p^{m(n-1)}$ is divisible by p. Therefore, the above theorem can be applied to find the p-ranks and characteristic polynomials of the cyclic difference set with Singer parameters and its complementary difference set.

4. 3-Ranks and Characteristic Polynomials of HKM Difference Sets

Recently, Helleseth et al. [8] introduced a new ternary sequence ($p = 3$) with ideal autocorrelation. It turned out to be a cyclic difference set (HKM difference set) with Singer parameters [9,13] and the p-ranks of the HKM difference set and its complementary difference set are derived in the following theorem.

THEOREM 4. *The HKM difference set with parameters* $((3^n - 1)/(3 - 1), (3^{n-1} - 1)/(3 - 1), (3^{n-2} - 1)/(3 - 1))$ *is defined as*

$$D = \left\{ t | tr_1^n(\alpha^t) + tr_1^n(\alpha^{dt}) = 0, 0 \le t < \frac{3^n - 1}{3 - 1} \right\}, \tag{10}$$

where $n = 3k > 3$, $d = 3^{2k} - 3^k + 1$, *and* α *is a primitive element of* F_{3^n}. *Then the 3-ranks of the HKM difference set D and its complementary difference set* $\overline{D}$ *are given as* $2n^2 - 2n + 1$ *and* $2n^2 - 2n$, *respectively*.

Proof. Let $x = \alpha^t$. Then we can expand the square of the trace function as

$$\begin{aligned}
\left[tr_1^n(\alpha^t)\right]^2 &= \left[tr_1^n(x)\right]^2 \\
&= tr_1^n(x) \cdot tr_1^n(x) \\
&= tr_1^n(x \cdot tr_1^n(x)) \\
&= tr_1^n(x \cdot (x + x^3 + x^{3^2} + \cdots + x^{3^{n-1}})) \\
&= \sum_{i=0}^{n-1} tr_1^n(x^{1+3^i}) \\
&= tr_1^n(x^{1+1}) + \sum_{i=1}^{n-1} tr_1^n(x^{1+3^i}) \\
&= \begin{cases} tr_1^n(x^{1+1}) + 2 \cdot \sum_{i=1}^{(n-1)/2} tr_1^n(x^{1+3^i}), & \text{for } n = \text{odd}; \\ tr_1^n(x^{1+1}) + 2 \cdot tr_1^{n/2}(x^{1+3^{(n/2)}}) + 2 \cdot \sum_{i=1}^{(n/2)-1} tr_1^n(x^{1+3^i}), & \text{for } n = \text{even}. \end{cases}
\end{aligned}$$

The characteristic sequence of the cyclic difference set $\overline{D}$ is given as

$$\left[tr_1^n(x) + tr_1^n(x^d)\right]^2. \tag{11}$$

Using the expansion of the square of trace function, we can also expand (11) as follows.

(i) $n = 2m + 1$ (odd case)

$$\begin{aligned}\left[tr_1^n(x) + tr_1^n(x^d)\right]^2 &= \left[tr_1^n(x)\right]^2 + \left[tr_1^n(x^d)\right]^2 + 2 \cdot tr_1^n(x) \cdot tr_1^n(x^d) \\ &= tr_1^n(x^{1+1}) + 2 \cdot \sum_{i=1}^{(n-1)/2} tr_1^n(x^{1+3^i}) + tr_1^n(x^{(1+1)d}) \\ &\quad + 2 \cdot \sum_{i=1}^{(n-1)/2} tr_1^n(x^{(1+3^i)d}) + 2 \cdot tr_1^n(x^d \cdot tr_1^n(x)) \\ &= tr_1^n(x^{1+1}) + 2 \cdot \sum_{i=1}^{(n-1)/2} tr_1^n(x^{1+3^i}) + tr_1^n(x^{(1+1)d}) \\ &\quad + 2 \cdot \sum_{i=1}^{(n-1)/2} tr_1^n(x^{(1+3^i)d}) + 2 \cdot \sum_{i=0}^{n-1} tr_1^n(x^{d+3^i}).\end{aligned}$$

Since

$$d \cdot (3^k + 1) = 3^{3k} + 1 = 3^{3k} - 1 + 2 \equiv 2 \bmod (3^{3k} - 1),$$

we have

$$tr_1^n(x^{(1+3^k)d}) = tr_1^n(x^{1+1}).$$

Using

$$d + 3^k = 3^{2k} + 1,$$

we obtain

$$tr_1^n(x^{d+3^k}) = tr_1^n(x^{3^{2k}+1}) = tr_1^n(x^{3^k+1}).$$

Therefore,

$$\begin{aligned}\left[tr_1^n(x) + tr_1^n(x^d)\right]^2 &= 2 \cdot \sum_{i=1, i\neq k}^{m} tr_1^n(x^{1+3^i}) + tr_1^n(x^{(1+1)d}) + 2 \cdot \sum_{i=1, i\neq k}^{m} tr_1^n(x^{(1+3^i)d}) \\ &\quad + 2 \cdot \sum_{i=0, i\neq k}^{n-1} tr_1^n(x^{d+3^i}) + tr_1^n(x^{1+3^k}). \qquad (12)\end{aligned}$$

It is easy to prove that for $n > 3$, all exponents belong to different cyclotomic coset of size n. Therefore, the 3-rank of $\overline{D}$ is

$$(m-1)n + n + (m-1)n + (n-1)n + n = 2 \cdot n(n-1),$$

and the 3-rank of the HKM difference set D is therefore $2n^2 - 2n + 1$.

(ii) $n = 2m$ (even case): Similar to the odd case, we expand

$$\begin{aligned}\left[tr_1^n(x) + tr_1^n(x^d)\right]^2 &= \left[tr_1^n(x)\right]^2 + \left[tr_1^n(x^d)\right]^2 + 2 \cdot tr_1^n(x) \cdot tr_1^n(x^d) \\ &= tr_1^n(x^{1+1}) + 2 \cdot tr_1^m(x^{1+3^m}) + 2 \cdot \sum_{i=1}^{m-1} tr_1^n(x^{1+3^i}) \\ &\quad + tr_1^n(x^{(1+1)d}) + 2 \cdot tr_1^m(x^{(1+3^m)d}) + 2 \cdot \sum_{i=1}^{m-1} tr_1^n(x^{(1+3^i)d}) \\ &\quad + 2 \cdot \sum_{i=0}^{n-1} tr_1^n(x^{d+3^i}).\end{aligned}$$

Using

$$(1 + 3^k) \cdot d = 2 \bmod (3^{3k} - 1),$$

we have

$$tr_1^n(x^{(1+3^k)d}) = tr_1^n(x^2),$$

and since

$$d + 3^k = 3^{2k} + 1,$$

we get

$$tr_1^n(x^{d+3^k}) = tr_1^n(x^{1+3^{2k}}) = tr_1^n(x^{1+3^k}).$$

Adding up the same trace terms, we have

$$\begin{aligned}\left[tr_1^n(x) + tr_1^n(x^d)\right]^2 &= 2 \cdot tr_1^m(x^{(1+3^m)}) + 2 \cdot \sum_{i=1, i\neq k}^{m-1} tr_1^n(x^{1+3^i}) \\ &\quad + tr_1^n(x^{(1+1)d}) + 2 \cdot tr_1^m(x^{(1+3^m)d}) + 2 \cdot \sum_{i=1, i\neq k}^{m-1} tr_1^n(x^{d(1+3^i)}) \\ &\quad + 2 \cdot \sum_{i=0, i\neq k}^{n-1} tr_1^n(x^{d+3^i}) + tr_1^n(x^{1+3^k}). \qquad (13)\end{aligned}$$

It can be shown that all exponents belong to different cosets of size n or m. Therefore the 3-rank of the difference set $\overline{D}$ is

$$m + (m-2)n + n + m + (m-2)n + (n-1)n + n = 2 \cdot n(n-1),$$

and from (8), the 3-rank of the HKM difference set D is therefore $2n^2 - 2n + 1$. ■

Note: Using (12), for $n = 3$, it can be easily derived that the 3-ranks of the HKM difference set D and its complementary difference set $\overline{D}$ are 7 and 6, respectively.

From (12) and (13), we can derive the characteristic polynomials of the HKM difference set and its complementary difference set as in the following theorem.

THEOREM 5. *Let D be the HKM difference set with parameters $((3^n-1)/(3-1), (3^{n-1}-1)/(3-1), (3^{n-2}-1)/(3-1))$ defined in (10). Then the characteristic polynomials of the HKM difference set D and its complementary difference set $\overline{D}$ are*:

For $n = 2m+1$:

$$g(x) = (x-1)g_c(x),$$
$$g_c(x) = M_{2d}(x)M_{1+3^k}(x)\prod_{i=1,i\neq k}^{m} M_{1+3^i}(x) \times \prod_{i=1,i\neq k}^{m} M_{(1+3^i)d}(x)\prod_{i=0,i\neq k}^{n-1} M_{d+3^i}(x).$$

For $n = 2m$:

$$g(x) = (x-1)g_c(x),$$
$$g_c(x) = M_{2d}(x)M_{1+3^m}(x)M_{(1+3^m)d}(x)M_{1+3^k}(x)\prod_{i=1,i\neq k}^{m-1} M_{1+3^i}(x) \times \prod_{i=1,i\neq k}^{m-1} M_{(1+3^i)d}(x)\prod_{i=0,i\neq k}^{n-1} M_{d+3^i}(x).$$

Note: For $n = 3$, the characteristic polynomials of the HKM difference set D and its complementary difference set $\overline{D}$ are derived as $(x-1)M_4(x)M_8(x)$ and $M_4(x)M_8(x)$, respectively.

5. 3-Ranks and Characteristic Polynomials of Lin Difference Sets

Lin [12] has conjectured that the family of ternary sequences $c(t) = tr_1^n(\alpha^t) + tr_1^n(\alpha^{dt})$ has the ideal autocorrelation property, where $n = 2m+1$ and $d = 2\cdot 3^m + 1$. If this is true, then it gives a cyclic difference set (Lin difference set) with Singer parameters [9,13]. Under this assumption, we can derive the 3-ranks and characteristic polynomials of the Lin difference set and its complementary difference set as in the following theorems.

THEOREM 6. *The Lin difference set with parameters* $((3^n-1)/(3-1),(3^{n-1}-1)/(3-1),(3^{n-2}-1)/(3-1))$ *is defined as*

$$D=\left\{t|tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})=0,0\le t<\frac{3^n-1}{3-1}\right\}, \tag{14}$$

where $n=2m+1>3$, $d=2\cdot 3^m+1$ *and* α *is a primitive element of* F_{3^n}. *Then the 3-ranks of the Lin difference set D and its complementary difference set* $\overline{D}$ *are given as* $2n^2-2n+1$ *and* $2n^2-2n$, *respectively*.

Proof. Let $x=\alpha^t$. Then the characteristic sequence of the difference set $\overline{D}$ is

$$\left[tr_1^n(x)+tr_1^n(x^d)\right]^2. \tag{15}$$

Using the expansion of the square of the trace function in the proof of the previous theorem, we can expand (15) as follows.

$$\begin{aligned}\left[tr_1^n(\alpha^t)+tr_1^n(\alpha^{dt})\right]^2&=\left[tr_1^n(x)\right]^2+\left[tr_1^n(x^d)\right]^2+2\cdot tr_1^n(x)\cdot tr_1^n(x^d)\\&=tr_1^n(x^{1+1})+2\cdot\sum_{i=1}^{m}tr_1^n(x^{1+3^i})+tr_1^n(x^{(1+1)d})\\&\quad+2\cdot\sum_{i=1}^{m}tr_1^n(x^{(1+3^i)d})+2\cdot\sum_{i=0}^{n-1}tr_1^n(x^{d+3^i}).\end{aligned}$$

Since

$$d+3^m=2\cdot 3^m+1+3^m=3^{m+1}+1,$$

we have

$$tr_1^n(x^{d+3^m})=tr_1^n(x^{1+3^m}),$$

and using

$$d+3^{n-1}=3^{n-1}+2\cdot 3^m+1,$$

we obtain

$$\begin{aligned}tr_1^n(x^{d+3^{n-1}})&=tr_1^n(x^{2\cdot 3^{m+1}+3+1})\\&=tr_1^n(x^{2\cdot(3^{m+1}+2)})\\&=tr_1^n(x^{2\cdot(1+2\cdot 3^m)})\\&=tr_1^n(x^{(1+1)d}).\end{aligned}$$

Adding up the same trace terms, we have

$$\left[tr_1^n(x) + tr_1^n(x^d)\right]^2 = tr_1^n(x^{1+1}) + 2 \cdot \sum_{i=1}^{m-1} tr_1^n(x^{1+3^i}) + tr_1^n(x^{1+3^m}) + 2 \cdot \sum_{i=1}^{m} tr_1^n(x^{(1+3^i)d}) + 2 \cdot \sum_{i=0, i\neq m}^{n-2} tr_1^n(x^{3^i+d}). \quad (16)$$

It can be shown that for $n > 3$, all exponents belong to different cosets of size n. Therefore, the 3-rank of the difference set $\overline{D}$ is

$$n + (m-1)n + n + m \cdot n + n(n-2) = 2n(n-1),$$

and from (8), the 3-rank of the Lin difference set D is $2n^2 - 2n + 1$. ■

Note: For $n = 3$, the Lin difference set is identical to the HKM difference set. Therefore, the 3-ranks and characteristic polynomials of the Lin difference set D and its complementary difference set $\overline{D}$ are the same as those of the HKM difference set and its complementary difference set.

From (16), we can derive the characteristic polynomials of the Lin difference set and its complementary difference set as in the following theorem.

THEOREM 7. *Let D be the Lin difference set with parameters $((3^n-1)/(3-1), (3^{n-1}-1)/(3-1), (3^{n-2}-1)/(3-1))$ defined in (14). Then the characteristic polynomials of the Lin difference set D and its complementary difference set $\overline{D}$ are given as*:

$$g(x) = (x-1)g_c(x),$$

$$g_c(x) = M_2(x)M_{1+3^m}(x) \prod_{i=1}^{m-1} M_{1+3^i}(x) \times \prod_{i=1}^{m} M_{(1+3^i)d}(x) \prod_{i=0, i\neq m}^{n-2} M_{d+3^i}(x).$$

6. Characteristic Polynomials of Singer Difference Sets

The p-rank of a Singer difference set is well-known [1,2,6,18]. In this section, the p-ranks of a Singer difference set and its complementary difference set are reviewed as given in the following theorem. Also the characteristic polynomials are obtained by using our approach.

THEOREM 8 [1,2,6,18]. *The Singer difference set with parameters* $((q^n-1)/(q-1), (q^{n-1}-1)/(q-1), (q^{n-2}-1)/(q-1))$ *is defined as*

$$D = \left\{ t | tr_s^{ns}(\alpha^t) = 0, 0 \le t < \frac{q^n-1}{q-1} \right\},$$

where $q = p^s$ *and* α *is a primitive element of* F_{q^n}. *Then the p-ranks of the Singer difference set D and its complementary difference set* $\overline{D}$ *are given as*

$$\binom{p+n-2}{n-1}^s + 1 \quad \textit{and} \quad \binom{p+n-2}{n-1}^s,$$

respectively.

The sketchy proof of Theorem 8 is given here and it will be used to derive the characteristic polynomials in the following theorem. Let $x = \alpha^t$. Then the characteristic sequence of the difference set $\overline{D}$ is given as $\left[tr_s^{ns}(x)\right]^{p^s-1}$.

By using $p^s - 1 = (p-1)p^{s-1} + (p-1)p^{s-2} + \cdots + (p-1)p + (p-1)$, we get

$$\begin{aligned}\left[tr_s^{ns}(x)\right]^{p^s-1} &= \left[[tr_s^{ns}(x)]^{p-1}\right]^{p^{s-1}+p^{s-2}+\cdots+p+1} \\ &= \sum_{(l_{i,0},l_{i,1},\ldots,l_{i,n-1})\in I_0} \cdots \sum_{(l_{i,0},l_{i,1},\ldots,l_{i,n-1})\in I_{s-1}} \prod_{i=0}^{s-1} \binom{p-1}{l_{i,0}, l_{i,1}, \ldots, l_{i,n-1}} x^{c(l)},\end{aligned}$$

where

$$c(l) = \sum_{j=0}^{n-1} p^{js} \sum_{i=0}^{s-1} l_{i,j} p^i, \tag{17}$$

$$I_i = \left\{ (l_{i,0}, l_{i,1}, \ldots, l_{i,n-1}) | \sum_{j=0}^{n-1} l_{i,j} = p-1, l_{i,j} \ge 0 \right\}, \quad 0 \le i \le s-1.$$

First, it will be shown that all $c(l)$'s are distinct mod $q^n - 1$. Suppose $c(l) = c(l')$ mod $q^n - 1$. The value of $c(l)$ is upper-bounded by $q^n - 1$, where the equality holds if and only if $l_{i,j} = p - 1$ for all i, j. Since this equality cannot happen, $c(l) < q^n - 1$ and the mod $q^n - 1$ can be ignored. By comparing the coefficients $l_{i,j}$ and $l'_{i,j}$ of p^{i+js} in the expansion of $c(l)$ and $c(l')$, it is easy to show that $l_{i,j} = l'_{i,j}$ and therefore, all $c(l)$'s are distinct for different l.

There are

$$\binom{p+n-2}{n-1}$$

cases satisfying $\sum_{i=0}^{n-1} l_{j,i} = p - 1$ and the corresponding coefficient values are in the form

$$\prod_{i=0}^{s-1} \binom{p-1}{l_{i,0}, l_{i,1}, \ldots, l_{i,n-1}} \neq 0 \bmod p.$$

Therefore, the p-ranks of Singer difference set and its complementary difference set are given as

$$\binom{p+n-2}{n-1}^s + 1 \quad \text{and} \quad \binom{p+n-2}{n-1}^s,$$

respectively.

From (17), we can derive the characteristic polynomials of a Singer difference set and its complementary difference set as in the following theorem.

THEOREM 9. *The Singer difference set with parameters* $((q^n-1)/(q-1), (q^{n-1}-1)/(q-1), (q^{n-2}-1)/(q-1))$ *is defined as*

$$D = \left\{ t | tr_s^{ns}(\alpha^t) = 0, 0 \leq t < \frac{q^n-1}{q-1} \right\},$$

where $q = p^s$ *and* α *is a primitive element of* F_{q^n}. *Then the characteristic polynomials of Singer difference set* D *and its complementary difference set* $\overline{D}$ *are given as*:

$$g(x) = (x-1)g_c(x),$$
$$g_c(x) = \prod_{c(l) \in I} M_{c(l)}(x),$$

where I *is a set of all coset leaders of the cosets including the elements* $\sum_{i=0}^{s-1} \sum_{j=0}^{n-1} l_{i,j} p^{i+js}$ *satisfying* $\sum_{j=0}^{n-1} l_{i,j} = p-1, 0 \leq i < s$.

Proof. From the proof of the previous theorem, we get

$$\begin{aligned} c(l) = & p^0(l_{0,0} + l_{1,0}p^1 + \cdots + l_{s-1,0}p^{s-1}) \\ & + p^s(l_{0,1} + l_{1,1}p^1 + \cdots + l_{s-1,1}p^{s-1}) \\ & \vdots \\ & + p^{(n-1)s}(l_{0,n-1} + l_{1,n-1}p^1 + \cdots + l_{s-1,n-1}p^{s-1}), \end{aligned}$$

where $\sum_{i=0}^{n-1} l_{j,i} = p-1$ for all j. It is easy to show that $c(l) \cdot p$ also appears as one of the valid $c(l)$'s and has the same coefficient value as that of $c(l)$ case. Hence, the theorem follows. ■

EXAMPLE 10. *Consider a Singer difference set with parameters* $((3^6-1)/(3^2-1), (3^4-1)/(3^2-1), (3^2-1)/(3^2-1)) = (91, 10, 1)$ *which is defined by*

$$D = \left\{ t | tr_2^6(\alpha^t) = 0, 0 \leq t < \frac{3^6-1}{3^2-1} = 91 \right\},$$

where $p = 3$ *and* α *is a primitive element of* F_{3^6}. *Using the primitive polynomial* $x^6 + 2x + 2 = 0$, *it can be shown that* $\{0, 7, 19, 21, 57, 58, 63, 67, 80, 83\}$ *forms this Singer difference set.*

We can obtain seven cosets from $c(l) = l_{0,0} + l_{1,0}3 + l_{0,1}3^2 + l_{1,1}3^3 + l_{0,2}3^4 + l_{1,2}3^5$ *where* $\sum_{j=0}^{2} l_{i,j} = 2, 0 \le i < 2$. *The valid values for* $(l_{i,0}, l_{i,1}, l_{i,2}), 0 \le i < 2$, *are among* $\{(2,0,0), (0,2,0), (0,0,2), (1,1,0), (1,0,1), (0,1,1)\}$. *Therefore, the number of possible nonzero exponents* $c(l)$ *for* $i = 0, 1$ *is* $6 \times 6 = 36$ *and it is the same value as*

$$\begin{pmatrix} 3+3-2 \\ 3-1 \end{pmatrix}^2.$$

We can select one value (*coset leader*) *from each coset and the following values*

$$\begin{pmatrix} l_{0,0} & l_{1,0} \\ l_{0,1} & l_{1,1} \\ l_{0,2} & l_{1,2} \end{pmatrix},$$

form seven such coset leaders.

$$\left\{ \begin{pmatrix} 2 & 2 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

and the corresponding $c(l)$ *values are* (8, 16, 32, 40, 56, 64, 112). *Therefore, the characteristic polynomials of a Singer difference set with parameters* (91, 10, 1) *and its complementary difference set are given as:*

$$\begin{aligned} g(x) &= (x-1)g_c(x), \\ g_c(x) &= M_8(x)M_{16}(x)M_{32}(x)M_{40}(x)M_{56}(x)M_{64}(x)M_{112}(x), \end{aligned}$$

where

$$\begin{aligned} M_8(x) &= x^6 + x^4 + x^3 + 1, \\ M_{16}(x) &= x^6 + 2x^5 + x^4 + x^3 + 2x^2 + 1, \\ M_{32}(x) &= x^6 + x^5 + x^4 + 2x^3 + x + 1, \\ M_{40}(x) &= x^6 + x^5 + 2x^4 + 2x^3 + 1, \\ M_{56}(x) &= x^3 + 2x^2 + 2x + 2, \\ M_{64}(x) &= x^6 + x^5 + 2x^3 + x^2 + 2x + 1, \\ M_{112}(x) &= x^3 + 2x + 2. \end{aligned}$$

Acknowledgments

This work was supported in part by the Korean Ministry of Information and Communications and the Norwegian Research Council.

References

1. M. Antweiler and L. Bömer, Complex sequences over $GF(p^M)$ with a two-level autocorrelation function and a large linear span, *IEEE Trans. Inform. Theory*, Vol. 38 (1992) pp. 120–130.
2. E. F. Assmus, Jr. and J. D. Key, *Designs and their codes*, Cambridge University Press, Cambridge (1992).
3. L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer Verlag (1971).
4. J. F. Dillon, Multiplicative difference sets via additive characters, *Designs, Codes and Cryptography*, Vol. 17 (1999) pp. 225–235.
5. J. F. Dillon and H. Dobbertin, Cyclic difference sets with Singer parameters, Preprint (1999).
6. R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets, *Journals of Combin. Theory*, Ser. A, Vol. 87 (1999) pp. 74–119.
7. B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, *Canad. J. Math.*, Vol. 14 (1962) pp. 614–625.
8. T. Helleseth, P. V. Kumar and H. M. Martinsen, A new family of ternary sequences with ideal two-level autcorrelation, *Design, Codes and Cryptography*, Vol. 23 (2001) pp. 157–166.
9. T. Helleseth and M. Martinsen, Open problems in sequence design and correlation, Preprint (2000).
10. D. Jungnickel, Difference sets, In (J. Dinitz and D. R. Stinson eds.) *Contemporary Design Theory: A Collection of Surveys*, John Wiley and Sons (1992).
11. R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20 of Encyclopedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA (1983).
12. H. A. Lin, From cyclic Hadamard difference sets to perfectly balanced sequences, Ph.D. Dissertation, University of Southern California, May (1998).
13. J. S. No, New cyclic difference sets with Singer parameters constructed from d-homogeneous functions, Preprint (2000).
14. J. S. No, H. Chung and M. S. Yun, Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$, *IEEE Trans. Inform. Theory*, Vol. 44 (1998) pp. 1278–1282.
15. J. S. No, S. W. Golomb, G. Gong, H. K. Lee and P. Gaal, Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation, *IEEE Trans. Inform. Theory*, Vol. 44 (1998) pp. 814–817.
16. J. S. No, K. Yang, H. Chung and H. Y. Song, On the construction of binary sequences with ideal autocorrelation property, *Proceedings of 1996 IEEE International Symposium on Information Theory and Its Applications* (ISITA '96), Victoria, B.C., Canada, Sept. 17–20 (1996) pp. 837–840.
17. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc*, Vol. 43 (1938) pp. 377–385.
18. K. J. C. Smith, On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry, *J. Comb. Theory*, Vol. 7 (1969) pp. 122–129.