Designs, Codes and Cryptography, 33, 199–213, 2004

New Cyclic Difference Sets with Singer Parameters Constructed from *d*-Homogeneous Functions

JONG-SEON NO
School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea

Communicated by: K. T. Arasu

Received December 27, 2000; Revised August 29, 2002; Accepted January 17, 2003

Abstract. In this paper, for a prime power q, new cyclic difference sets with Singer parameters $((q^n-1/q-1),(q^{n-1}-1/q-1),(q^{n-2}-1/q-1))$ are constructed by using q-ary sequences (d-homogeneous functions) of period q^n-1 and the generalization of GMW difference sets is proposed by combining the generation methods of d-form sequences and extended sequences. When q is a power of 3, new cyclic difference sets with Singer parameters $((q^n-1/q-1),(q^{n-1}-1/q-1),(q^{n-2}-1/q-1))$ are constructed from the ternary sequences of period q^n-1 with ideal autocorrelation introduced by Helleseth, Kumar, and Martinsen.

Keywords: cyclic difference sets, d-homogeneous functions, generalized GMW difference sets, GMW difference sets, sequences

AMS Classification: 05B10, 11B50

1. Introduction

It is well-known that cyclic difference sets can be constructed from pseudonoise (PN) sequences with ideal autocorrelation [1,11,12]. Specially, a cyclic difference set with Singer parameters $(2^n-1,2^{n-1}-1,2^{n-2}-1)$ [7,24] is equivalent to a binary sequence $s(\alpha^t)$ of period 2^n-1 with ideal autocorrelation, where a $(2^n-1,2^{n-1}-1,2^{n-2}-1)$ difference set is defined as

$$D=\{t\,|\,s(\alpha^t)=0,0\le t<2^n-1\},$$

where α is a primitive element of the finite field F_{2^n}. Recently, new binary sequences of period 2^n-1 with ideal autocorrelation are introduced by No et al. [19,20], Dillon and Dobbertin [5], and Xiang [25]. Dillon proved the conjectures of No et al. [19,20] using Fourier analysis on the additive group [4]. Dillon and Dobbertin [5] introduced new cyclic difference sets with Singer parameters $(2^n-1,2^{n-1}-1,2^{n-2}-1)$ constructed from binary sequences of period 2^n-1 with ideal autocorrelation.

Up to now, most of work for cyclic difference sets with Singer parameters $((q^n-1/q-1),(q^{n-1}-1/q-1),(q^{n-2}-1/q-1))$ has been done on binary sequences, q-ary m-sequences (Singer difference sets) [24], q-ary GMW sequences [6], and q-ary cascaded GMW sequences [14] (GMW difference sets) [7], where q is a

prime power. Klapper introduced the d-form sequences constructed by using d-homogeneous functions [13]. Recently, p-ary sequences with ideal autocorrelation have been investigated and some research results have been introduced. Helleseth et al. [9] found ternary sequences with ideal autocorrelation, which are the first nonbinary sequences with ideal autocorrelation, except for the p-ary m-sequences, the p-ary GMW sequences, and the p-ary cascaded GMW sequences.

In this paper, for a prime power q, new cyclic difference sets with Singer parameters $((q^n-1/q-1),(q^{n-1}-1/q-1),(q^{n-2}-1/q-1))$ are constructed by using d-homogeneous functions with difference-balance property. Generalization of the GMW difference sets with Singer parameter is also proposed by using d-homogeneous functions with difference-balance property. When q is a power of 3, new cyclic difference sets with Singer parameter are constructed from the ternary sequences of period q^n-1 with ideal autocorrelation introduced by Helleseth et al. [9].

In this paper, we use the following notation:

q: power of prime p; m, n: positive integers such that $n>2, m \mid n$; d: positive integer relatively prime to $q-1$; F_q, F_{q^m}, F_{q^n}: finite fields with q, q^m, and q^n elements, respectively; α: primitive element of F_{q^n}; $\beta=\alpha^T$: primitive element of F_{q^m}, where $T=(q^n-1/q^m-1)$; $F_{q^n}^*=F_{q^n}\backslash\{0\}$.

A function $f(x)$ is said to be balanced if the element "0" appears one less time than each nonzero element in F_q in the list $f(\alpha^0)$, $f(\alpha^1)$, $f(\alpha^2)$, $f(\alpha^3),\ldots,f(\alpha^{q^n-2})$. A function $f(x)$ is said to be difference-balanced if $f(xz)-f(x)$ is balanced for any $z\in F_{q^n}\backslash\{0,1\}$. By replacing x by α^t, a function $f(x)$ can be considered as a q-ary sequence $f(\alpha^t)$ of period q^n-1. Hence, for convenience, we will use the expression "a sequence $f(\alpha^t)$ of period q^n-1" interchangeably with "a function $f(\alpha^t)$ (or $f(x)$) from $F_{q^n}^*$ to F_q".

Let D be the (v,k,λ) difference set defined as the set of k distinct residues modulo v expressed by

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

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

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

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

$$aD+b=\{ac_1+b,ac_2+b,ac_3+b,\ldots,ac_k+b\},$$

where ac_i+b is computed 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. A characteristic sequence of cyclic difference set D is defined as the binary sequence given by

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

The definition of p-rank of a cyclic difference set D is given as a degree of the linear recursion equation over F_p of its characteristic sequence $c(t)$. In order to prove inequivalence of two difference sets, p-rank of cyclic difference sets is often used. But it is very difficult to find p-rank of cyclic difference sets.

Let $n = em > 1$ for some positive integers e and m. Then the trace function $\mathrm{tr}_{q^m}^{q^n}(\cdot)$ is the mapping from F_{q^n} to its subfield F_{q^m} defined by Lidl and Niederreiter [15]

$$\mathrm{tr}_{q^m}^{q^n}(x) = \sum_{i=0}^{e-1} x^{q^{mi}},$$

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

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

$$m(\alpha^t) = \mathrm{tr}_q^{q^n}(\alpha^t). \tag{1}$$

It is known that the q-ary m-sequence defined in (1) has the balance and difference-balance properties.

2. Main Theorem

Klapper introduced d-homogeneous functions, which can be used to construct the d-form sequences [13]. A function $f(x)$ is said to be d-homogeneous on F_{q^n} over F_q if for any $x \in F_{q^n}$ and $y \in F_q$, it satisfies

$$f(yx) = y^d f(x).$$

Using d-homogeneous property, it can be easily derived that a d-homogeneous function with difference-balance property is balanced as follows:

LEMMA 1. *If $f(x)$ is a d-homogeneous function on $F_{q^n}^*$ over F_q with difference-balance property, then $f(x)$ is balanced.*

Proof. For $q = 2$, it is easy to prove it. For $q > 2$, let $y \in F_q \backslash \{0, 1\}$. From the homogeneous property of $f(x)$, we have

$$\begin{aligned} f(yx) - f(x) &= y^d f(x) - f(x) \\ &= (y^d - 1) f(x). \end{aligned}$$

From $y^d - 1 \neq 0$ and the difference-balance property of $f(x)$, $f(x)$ is balanced. ■

Up to now, most of cyclic difference sets with Singer parameter were constructed from binary sequences, q-ary m-sequences, q-ary GMW sequences, and q-ary

cascaded GMW sequences. In this section, it is shown for a prime power q that cyclic difference sets with Singer parameter can be constructed from the d-homogeneous functions with difference-balance property.

THEOREM 2 (Main). *If $f(x)$ is a d-homogeneous function on $F_{q^n}^*$ over F_q with difference-balance property, then the set of integers defined by*

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

forms a cyclic difference set with Singer parameters

$$\left(\frac{q^n - 1}{q - 1}, \frac{q^{n-1} - 1}{q - 1}, \frac{q^{n-2} - 1}{q - 1} \right). \tag{2}$$

Proof. From Lemma 1, it is clear that $f(x)$ is balanced. As x varies over $F_{q^n}^*$, $f(x) = 0$ appears $q^{n-1} - 1$ times. Let $h = \alpha^{i(q^n-1/q-1)}, 1 \le i \le q - 2$, that is, $h \in F_q^*$. Then $f(hx) = 0$ iff $f(x) = 0$ and thus we proved the cardinality of D.

Since d is relatively prime to $q - 1$, without loss of generality, we assume that $f(x)$ is 1-homogeneous. For $z \in F_{p^n} \backslash F_q$ and $a, b, g \in F_q, g \neq 0$, let $x_g(a, b)$ be the number of solutions of $(f(xz), f(xg)) = (a, b), x \in F_{q^n}^*$. Since $f(x)$ is 1-homogeneous, we have

$$x_g(a, b) = x_1(a, g^{-1}b).$$

We will show that $x_1(0, 0) = q^{n-2} - 1$. Since $f(xz) - f(xg)$ is balanced, 0 occurs $q^{n-1} - 1$ as a difference. Thus we have

$$q^{n-1} - 1 = \sum_{y \in F_q} x_g(y, y) = \sum_{y \in F_q} x_1(y, g^{-1}y), \quad \text{for all } g \in F_q^*.$$

Note that

$$\sum_{a,b \in F_q} x_1(a, b) = q^n - 1$$

and

$$\sum_{a \in F_q} x_1(a, 0) = \sum_{b \in F_q} x_1(0, b) = q^{n-1} - 1.$$

Putting all together, we get

$$\begin{aligned}(q-1)(q^{n-1}-1) &= \sum_{g\in F_q^*}\sum_{y\in F_q} x_1(y, g^{-1}y)\\ &= (q-1)x_1(0,0) + \sum_{g\in F_q^*}\sum_{y\in F_q^*} x_1(y, g^{-1}y)\\ &= (q-1)x_1(0,0) + \sum_{a,b\in F_q^*} x_1(a,b)\\ &= (q-1)x_1(0,0) + q^n - 1 - \left(\sum_{a\in F_q} x_1(a,0) + \sum_{b\in F_q} x_1(0,b) - x_1(0,0)\right)\\ &= (q-1)x_1(0,0) + q^n - 1 - 2(q^{n-1}-1) + x_1(0,0).\end{aligned}$$

This implies $x_1(0,0) = q^{n-2} - 1$. Clearly, $(f(hxz), f(hxg)) = (0,0)$ iff $(f(xz), f(xg)) = (0,0)$ and thus we proved the theorem. ■

It is already known that we can construct the cyclic difference sets with Singer parameter defined in (2) by using q-ary m-sequences, q-ary GMW sequences, and q-ary cascaded GMW sequences. Those sequences of period $q^n - 1$ are defined as

$$\begin{aligned}c_m(\alpha^t) &= \mathrm{tr}_q^{q^n}(\alpha^t),\\ c_g(\alpha^t) &= \mathrm{tr}_q^{q^m}\left\{\left[\mathrm{tr}_{q^m}^{q^n}(\alpha^t)\right]^r\right\},\\ c_{cg}(\alpha^t) &= \mathrm{tr}_q^{q^k}\left\{\left[\mathrm{tr}_{q^k}^{q^m}\left\{\left[\mathrm{tr}_{q^m}^{q^n}(\alpha^t)\right]^r\right\}\right]^u\right\},\end{aligned}$$

where k, m, and n are integers such that $k \mid m$, $m \mid n$, and $\gcd(q^k - 1, u) = 1, 1 \le u < q^k - 1$ and $\gcd(q^m - 1, r) = 1, 1 \le r < q^m - 1$, respectively. It is easy to prove that those sequences are the d-homogeneous functions with difference-balance property. Therefore, Theorem 2 includes the cyclic difference sets with Singer parameter constructed from the q-ary m-sequences, the q-ary GMW sequences, and the q-ary cascaded GMW sequences.

Gordon et al. [7] constructed a cyclic difference set with Singer parameter by using lifting idea, called GMW difference set. Generalization of the GMW difference sets with Singer parameter is proposed by constructing the general class of d-homogeneous functions with difference-balance property as in the following theorem.

THEOREM 3 (Generalized GMW difference sets). *Let I be an index set. Assume that the function given by*

$$b(y) = \sum_{a\in I} b_i \mathrm{tr}_q^{q^m}(y^a), \tag{3}$$

is d_1-homogeneous on F_{q^m} over F_q with difference-balance property. Let $m \mid n$. Let $H(x)$

be a d_2-homogeneous function on $F_{q^n}^*$ over F_{q^m} with difference-balance property, where $b_i \in F_q^*$, $\gcd(q-1, d_1) = 1$, and $\gcd(q^m - 1, d_2) = 1$. Let $\gcd(q^m - 1, r) = 1$, $1 \le r < q^m - 1$. Then the function

$$f(x) = \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{[H(x)]^{ar}\},$$

is also d-homogeneous on $F_{q^n}^*$ over F_q with difference-balance property, where $d_1 d_2 r \equiv d \bmod q - 1$. And the set of integers defined by

$$D = \left\{ t \,|\, f(\alpha^t) = 0, 0 \le t < \frac{q^n - 1}{q - 1} \right\}, \tag{4}$$

forms a cyclic difference set with Singer parameter in (2), called generalized GMW difference set.

Proof. Let $y = \beta^{t_1}$ and $x = \alpha^t$, where $\beta = \alpha^T$. Then $b(\beta^{t_1})$ and $f(\alpha^t)$ can be considered as q-ary sequences of period $q^m - 1$ and $q^n - 1$, respectively. Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 T + t_2$, $0 \le t_1 \le q^m - 2$, $0 \le t_2 \le T - 1$. Then the sequence $f(\alpha^t)$ can be expressed in the two-dimensional representation as

$$\begin{aligned} f(\alpha^t) &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{[H(\alpha^t)]^{ar}\} \\ &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{\alpha^{ad_2 r T t_1}[H(\alpha^{t_2})]^{ar}\} \\ &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{\beta^{ad_2 r t_1}[H(\alpha^{t_2})]^{ar}\}, \end{aligned}$$

where the subsequence of $f(\alpha^t)$ for a fixed value of t_2, $0 \le t_2 \le T - 1$, is either all-zero sequence of period $q^m - 1$ if $H(\alpha^{t_2}) = 0$ or a cyclic shift of the decimated (by $d_2 r$) sequences of the q-ary sequence in (3), i.e.,

$$b(\beta^{d_2 r t_1}) = \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}(\beta^{ad_2 r t_1}),$$

which has period $q^m - 1$, because it is a d_2-homogeneous function with difference-balance property and $\gcd(q^m - 1, d_2 r) = 1$. From the assumption of the d-homogeneous and difference-balance property of $b(\beta^{t_1})$, it is balanced and so does $b(\beta^{dr t_1})$. That is, the element "0" appears $q^{m-1} - 1$ times and each nonzero element in F_q appears q^{m-1} times in one period of $b(\beta^{d_2 r t_1})$.

Then the difference of $f(\alpha^t)$ can be expressed as

$$\begin{aligned} f(\alpha^{t+\tau}) - f(\alpha^t) &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{\beta^{ad_2rt_1}[H(\alpha^{t_2+\tau})]^{ar}\} - \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}\{\beta^{ad_2rt_1}[H(\alpha^{t_2})]^{ar}\} \\ &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}(\beta^{ad_2rt_1}[\beta^{g(t_2+\tau)}]^{ad_2r} - \beta^{ad_2rt_1}[\beta^{g(t_2)}]^{ad_2r}) \\ &= \sum_{a \in I} b_i \mathrm{tr}_q^{q^m}(\beta^{ad_2rt_1}(\beta^{ad_2rg(t_2+\tau)} - \beta^{ad_2rg(t_2)})), \end{aligned}$$

where the function $g(t_2)$ is defined as

$$\beta^{d_2 g(t_2)} = H(\alpha^{t_2}),$$

for $H(\alpha^{t_2}) \neq 0$ and $g(t_2) = -\infty$ if $H(\alpha^{t_2}) = 0$.

It is clear that $g(t_2 + \tau) = g(t_2)$ iff $g(t_2 + \tau + iT) = g(t_2 + iT)$. From the d_2-homogeneous and difference-balance property of $H(\alpha^t), g(t_2 + \tau) = g(t_2)$ occurs $(q^{n-m} - 1/q^m - 1)$ times and $g(t_2 + \tau) \neq g(t_2)$ occurs $(q^n - 1/q^m - 1) - (q^{n-m} - 1/q^m - 1)$ times as t_2 varies over $0 \leq t_2 \leq T - 1$. From the balance property of $b(\beta^{t_1})$, it can be obtained that as t varies over $0 \leq t \leq q^n - 2, f(\alpha^{t+\tau}) - f(\alpha^t) = 0$ occurs

$$(q^m - 1) \times \frac{q^{n-m} - 1}{q^m - 1} + (q^{m-1} - 1)\left(\frac{q^n - 1}{q^m - 1} - \frac{q^{n-m} - 1}{q^m - 1}\right) = q^{n-1} - 1,$$

times and each nonzero element in F_q appears

$$q^{m-1} \times \left(\frac{q^n - 1}{q^m - 1} - \frac{q^{n-m} - 1}{q^m - 1}\right) = q^{n-1},$$

times. Therefore, $f(\alpha^t)$ is difference-balanced. Since $b(y)$ is d_1-homogeneous on F_{q^m} over F_q and $H(x)$ is d_2-homogeneous on $F_{q^n}^*$ over $F_{q^m}, f(x)$ is also d-homogeneous on $F_{q^n}^*$ over F_q, where $d_1 d_2 r \equiv d \bmod q - 1$. From the main theorem, the set D in (4) becomes a cyclic difference set. ■

Using the q-ary sequence $f(\alpha^t)$ of period $q^n - 1$, we can construct a cyclic difference set in the following section.

3. Construction of Difference Sets from q-ary Sequences

A function $s(\alpha^t)$ from $F_{p^n}^*$ to F_p can be considered as a p-ary sequence of period $N = p^n - 1$, where p be a prime. Let ω be a primitive p-th root of unity. Then the periodic autocorrelation $R(\tau)$ of the sequence $s(\alpha^t)$ is defined as

$$R(\tau) = \sum_{t=0}^{N-1} \omega^{s(\alpha^{t+\tau}) - s(\alpha^t)}.$$

A sequence is said to have the ideal autocorrelation property if its periodic

autocorrelation function $R(\tau)$ is given as

$$R(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \bmod N; \\ -1, & \text{for } \tau \not\equiv 0 \bmod N. \end{cases}$$

LEMMA 4. *Let p be a prime. A p-ary sequence of period $p^n - 1$ has the ideal autocorrelation property if and only if it has the difference-balance property.*

Proof. It is clear that from the definition of autocorrelation, $s(\alpha^t)$ has the ideal autocorrelation property if it has the difference-balance property.

Let a_i be the number of occurrences of $s(\alpha^{t+\tau}) - s(\alpha^t) = i, 0 \le i \le p-1$ as t varies over $0 \le t \le p^n - 2$. If $s(\alpha^t)$ has the ideal autocorrelation property, then for all nonzero shift τ and some integers a_i', we have

$$R(\tau) = \sum_{i=0}^{p-1} a_i' \omega^i = -1.$$

Let $a_i = a_i'$ for all nonzero i and $a_0 = a_0' + 1$. Then we have

$$\sum_{i=0}^{p-1} a_i \omega^i = 0,$$

which is satisfied only if $a_i = a$ for all i. Thus we proved the balance property. ■

Using the trace function, a d-homogeneous function can be constructed as in the following theorem.

LEMMA 5. *Let $s \equiv d \bmod (q^m - 1)$ for all s in an index set I and $b_i \in F_{q^m}^*$. Then the function given by*

$$H(x) = \sum_{s \in I} b_i \mathrm{tr}_{q^m}^{q^n}(x^s)$$

is d-homogeneous on $F_{q^n}^*$ over F_{q^m}.

Proof. For $\gamma \in F_{q^m}$, we have

$$\begin{aligned} H(\gamma x) &= \sum_{s \in I} b_i \mathrm{tr}_{q^m}^{q^n}((\gamma x)^s) \\ &= \sum_{s \in I} \gamma^d b_i \mathrm{tr}_{q^m}^{q^n}(x^s) \\ &= \gamma^d H(x), \end{aligned}$$

where $\gamma^s = \gamma^d$ because $s \equiv d \bmod (q^m - 1)$ for all s in the index set I. ■

For a composite integer n, it is possible to construct d-homogeneous functions on $F_{q^n}^*$ over its subfield F_{q^m} with difference-balance property by using the d-homogeneous function on $F_{q^n}^*$ over F_q with difference-balance property as follows:

THEOREM 6. *Assume that for an index set I and $b_i \in F_q^*$, the function from $F_{q^n}^*$ to F_q given by*

$$c(x) = \sum_{s \in I} b_i \mathrm{tr}_q^{q^n}(x^s), \tag{5}$$

has the difference-balance property and for all $s \in I, s \equiv d \bmod q^m - 1$. Then the function given by

$$f(x) = \sum_{s \in I} b_i \mathrm{tr}_{q^m}^{q^n}(x^s),$$

is d-homogeneous on $F_{q^n}^*$ over F_{q^m} with difference-balance property.

Proof. From Lemma 5 and $s \equiv d \bmod q^m - 1$ for all $s \in I$, it is clear that $f(x)$ is a d-homogeneous function on $F_{q^n}^*$ over F_{q^m}. Let $x = \alpha^t$. Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 T + t_2$, $0 \le t_1 \le q^m - 2, 0 \le t_2 \le T - 1$. The two-dimensional representation of the function $c(\alpha^t)$ in (5) can be expressed as

$$\begin{aligned} c(\alpha^t) &= \sum_{s \in I} b_i \mathrm{tr}_q^{q^n}(\alpha^{s(t_1 T + t_2)}) \\ &= \sum_{s \in I} b_i \mathrm{tr}_q^{q^m}\{\alpha^{dt_1 T} \mathrm{tr}_{q^m}^{q^n}(\alpha^{st_2})\} \\ &= \mathrm{tr}_q^{q^m}\{\beta^{dt_1} \sum_{s \in I} b_i \mathrm{tr}_{q^m}^{q^n}(\alpha^{st_2})\} \\ &= \mathrm{tr}_q^{q^m}\{\beta^{dt_1} f(\alpha^{t_2})\}, \end{aligned}$$

where the subsequence of $c(\alpha^t)$ for a fixed value of $t_2, 0 \le t_2 \le T - 1$, is either all-zero sequence of period $q^m - 1$ if $f(\alpha^{t_2}) = 0$ or a cyclic shift of the decimated m-sequence of period $q^m - 1$, $\mathrm{tr}_q^{q^m}(\beta^{dt_1})$, otherwise. From the balance property of m-sequences, the element "0" appears $q^{m-1} - 1$ times and each nonzero element in F_q appears q^{m-1} times in one period of the subsequence $\mathrm{tr}_q^{q^m}(\beta^{dt_1})$. Assume that as t_2 varies over $0 \le t_2 \le T - 1, f(\alpha^{t_2+\tau}) = f(\alpha^{t_2})$ occurs B times and $f(\alpha^{t_2+\tau}) \ne f(\alpha^{t_2})$ occurs $T - B$ times. Then the element "0" appears $(q^m - 1)B + (q^{m-1} - 1)(T - B)$ times and each nonzero element in F_q appears $q^{m-1}(T - B)$ times in one period of the difference of $c(\alpha^t), \mathrm{tr}_q^{q^m}(\beta^{dt_1} f(\alpha^{t_2+\tau})) - \mathrm{tr}_q^{q^m}(\beta^{dt_1} f(\alpha^{t_2}))$. From the assumption that the

function $c(\alpha^t)$ is difference-balanced, we have

$$(q^m-1)B+(q^{m-1}-1)(T-B)=q^{n-1}-1$$
$$q^{m-1}(T-B)=q^{n-1},$$

and thus B is computed as $(q^{n-m}-1)/(q^m-1)$ and $T-B=q^{n-m}$. And we have the relation as

$$f(\alpha^{t_1T+t_2+\tau})-f(\alpha^{t_1T+t_2})=\beta^{dt_1}\{f(\alpha^{t_2+\tau})-f(\alpha^{t_2})\}.$$

For a fixed t_2 such that $f(\alpha^{t_2+\tau})-f(\alpha^{t_2})\neq 0, f(\alpha^{t_1T+t_2+\tau})-f(\alpha^{t_1T+t_2})$ takes all nonzero elements in F_{q^m} exactly once as t_1 varies over $0\le t_1\le q^m-2$. Therefore, as t varies over $0\le t\le q^n-2$, the element "0" appears

$$(q^m-1)B=q^{n-m}-1,$$

times and each nonzero element in F_{q^m} appears

$$T-B=q^{n-m},$$

times in the difference $f(\alpha^{t+\tau})-f(\alpha^t)$, which proves the difference-balance property of $f(\alpha^t)$. ■

Recently, Helleseth et al. [9] introduced a new ternary sequence ($p=3$) with ideal autocorrelation, which is the first nonbinary sequence with ideal autocorrelation except for the p-ary m-sequences, the p-ary GMW sequences, and the p-ary cascaded GMW sequences. It is restated in the following theorem.

THEOREM 7 (Helleseth et al. [9]). *Let $s=3^{2k}-3^k+1$ and k be a positive integer. Let α be a primitive element of $F_{3^{3k}}$. Then the ternary sequence of period $3^{3k}-1$ given by*

$$f(\alpha^t)=\mathrm{tr}_3^{3^{3k}}(\alpha^t)+\mathrm{tr}_3^{3^{3k}}(\alpha^{st}),$$

has the ideal autocorrelation property.

Let $n=3ek$ in Theorem 7, where e and k are positive integers. From Lemmas 4, 5 and Theorem 6, we can easily derive that the function given by

$$\mathrm{tr}_{3^k}^{3^{3ek}}(x)+\mathrm{tr}_{3^k}^{3^{3ek}}(x^s),$$

is d-homogeneous on $F_{q^{3ek}}^*$ over F_{q^k} with difference-balance property. From Theorem 2, we can construct a cyclic difference set as follows:

COROLLARY 8. *Let $n = 3ek$ and e and k be positive integers and $s = 3^{2ek} - 3^{ek} + 1$. Let α be a primitive element of $F_{3^{3ek}}$. Then the set of integers defined by*

$$D = \left\{ t \,|\, \mathrm{tr}_{3^k}^{3^{3ek}}(\alpha^t) + \mathrm{tr}_{3^k}^{3^{3ek}}(\alpha^{st}) = 0, 0 \le t < \frac{3^{3ek}-1}{3^k-1} \right\},$$

forms a cyclic difference set with Singer parameters

$$\left(\frac{3^{3ek}-1}{3^k-1}, \frac{3^{(3e-1)k}-1}{3^k-1}, \frac{3^{(3e-2)k}-1}{3^k-1} \right).$$

For $k = 1$ and $e = 1$, Corollary 8 has been obtained in Helleseth and Martinsen [10]. The 3-rank of cyclic difference set in Corollary 8 for $k = 1$ and $e = 1$ has been derived as $18k^2 - 6k + 1$ [21], which proved that the cyclic difference set in Corollary 8 for $k = 1$ and $e = 1$ is inequivalent to the known cyclic difference sets with the same parameter.

From the numerical analysis, it is also shown that the (364, 121, 40) cyclic difference set defined in Corollary 8 for $k = 2$ is inequivalent to the (364, 121, 40) Singer difference set given by

$$\{ t \,|\, \mathrm{tr}_3^{3^6}(\alpha^t) = 0, 0 \le t < 364 \},$$

and the (364, 121, 40) GMW difference sets constructed from the ternary GMW sequences as in

$$\{ t \,|\, \mathrm{tr}_3^{3^2}([\mathrm{tr}_{3^2}^{3^6}(\alpha^t)]^5) = 0, 0 \le t < 364 \},$$
$$\{ t \,|\, \mathrm{tr}_3^{3^3}([\mathrm{tr}_{3^3}^{3^6}(\alpha^t)]^5) = 0, 0 \le t < 364 \},$$
$$\{ t \,|\, \mathrm{tr}_3^{3^3}([\mathrm{tr}_{3^3}^{3^6}(\alpha^t)]^7) = 0, 0 \le t < 364 \},$$
$$\{ t \,|\, \mathrm{tr}_3^{3^3}([\mathrm{tr}_{3^3}^{3^6}(\alpha^t)]^{17}) = 0, 0 \le t < 364 \}.$$

Let $e = 1$ and $q = 3^k$. Then the difference set in Corollary 8 becomes a cyclic planar difference set and we have a conjecture as follows:

Conjecture 9. Let $q = 3^k$. Let k be a positive integer and $s = q^2 - q + 1$. Let α be a primitive element of F_{q^3}. Then the $(q^2 + q + 1, q + 1, 1)$ cyclic planar difference set defined by

$$\left\{ t \,|\, \mathrm{tr}_q^{q^3}(\alpha^t) + \mathrm{tr}_q^{q^3}(\alpha^{st}) = 0, 0 \le t < \frac{q^3-1}{q-1} \right\},$$

is the same as the $(q^2 + q + 1, q + 1, 1)$ Singer difference set given by

$$\left\{ t \,|\, \mathrm{tr}_q^{q^3}\alpha^{((q+1)/2)t} = 0, 0 \le t < \frac{q^3-1}{q-1} \right\}.$$

Recently, it has been proved by Chandler and Xiang [2].

Let e and k be positive integers and q be a power of 3. Clearly, the function given by

$$b(y) = \mathrm{tr}_q^{q^k}(y),$$

is d_1-homogeneous on F_{q^k} over F_q with difference-balance property. Let $J = \{1, q^{2ek} - q^{ek} + 1\}$ be an index set, where clearly $s \equiv 1 \bmod (q^k - 1)$ for all s in the index set J and $d = 1$ is relatively prime to $q^k - 1$. From Lemma 4, Theorems 6 and 7, the function given by

$$H(x) = \sum_{s \in J} \mathrm{tr}_{q^k}^{q^{3ek}}(x^s),$$

is d-homogeneous on $F^*_{q^{3ek}}$ over F_{q^k} with difference-balance property. From Theorem 3, we can construct a difference set with Singer parameter as follows.

COROLLARY 10. *Let q be a power of 3 and α be a primitive element of $F_{q^{3ek}}$. Let* $\gcd(q^k - 1, r) = 1, 1 \le r < q^k - 1$. *Then the set of integers defined by*

$$D = \left\{ t \,|\, \mathrm{tr}_q^{q^k}\left\{ \left[\mathrm{tr}_{q^k}^{q^{3ek}}(\alpha^t) + \mathrm{tr}_{q^k}^{q^{3ek}}(\alpha^{st}) \right]^r \right\} = 0, 0 \le t < \frac{q^{3ek} - 1}{q - 1} \right\},$$

forms a cyclic difference set with Singer parameters

$$\left(\frac{q^{3ek} - 1}{q - 1}, \frac{q^{3ek-1} - 1}{q - 1}, \frac{q^{3ek-2} - 1}{q - 1} \right).$$

Let e and k be positive integers and q be a power of 3. From Lemma 4 and Theorems 6 and 7, it can be easily proved that the function $b(y)$ given by

$$b(y) = \sum_{a \in I} \mathrm{tr}_q^{q^{3k}}(y^a),$$

is 1-homogeneous on $F_{q^{3k}}$ over F_q with difference-balance property and the function given by

$$H(x) = \sum_{s \in J} \mathrm{tr}_{q^{3k}}^{q^{9ek}}(x^s),$$

is also 1-homogeneous on $F^*_{q^{9ek}}$ over $F_{q^{3k}}$ with difference-balance property, where $I = \{1, q^{2k} - q^k + 1\}$ and $J = \{1, q^{6ek} - 3^{3ek} + 1\}$. From Theorem 3, we can construct the difference set with Singer parameter in the following theorem without proof.

COROLLARY 11. *Let q be a power of 3 and α be a primitive element of $F_{q^{9ek}}$. Let $\gcd(q^{3k}-1, r) = 1, 1 \le r < q^{3k}-1$. Then the set of integers defined by*

$$D = \left\{ t \,|\, \mathrm{tr}_q^{q^{3k}} \left\{ \left[\mathrm{tr}_{q^{3k}}^{q^{9ek}}(\alpha^t) + \mathrm{tr}_{q^{3k}}^{q^{9ek}}(\alpha^{st}) \right]^r \right\} + \mathrm{tr}_q^{q^{3k}} \left\{ \left[\mathrm{tr}_{q^{3k}}^{q^{9ek}}(\alpha^t) + \mathrm{tr}_{q^{3k}}^{q^{9ek}}(\alpha^{st}) \right]^{ar} \right\} = 0, . \right.$$
$$\left. 0 \le t < \frac{q^{9ek}-1}{q-1} \right\}$$

forms a cyclic difference set with Singer parameters

$$\left(\frac{q^{9ek}-1}{q-1}, \frac{q^{9ek-1}-1}{q-1}, \frac{q^{9ek-2}-1}{q-1} \right).$$

As an example, a new cyclic difference set with Singer parameter is constructed using the ternary sequence of period $3^{27}-1$ with ideal autocorrelation as follows. Let $k = 3$, $q = 3$, and $e = 1$. Then $a = 3^6 - 3^3 + 1$ and $s = 3^{18} - 3^9 + 1$. Let α be a primitive element of $F_{3^{27}}$. Let $\gcd(3^9 - 1, r) = 1, 1 \le r < 3^9 - 1$. Then the function given by

$$f(x) = \mathrm{tr}_3^{3^9} \left\{ \left[\mathrm{tr}_{3^9}^{3^{27}}(x) + \mathrm{tr}_{3^9}^{3^{27}}(x^s) \right]^r \right\} + \mathrm{tr}_3^{3^9} \left\{ \left[\mathrm{tr}_{3^9}^{3^{27}}(x) + \mathrm{tr}_{3^9}^{3^{27}}(x^s) \right]^{ar} \right\},$$

is 1-homogeneous on $F_{3^{27}}^*$ over F_3 with difference-balance property. Then the set of integers defined by

$$D = \left\{ t \,|\, f(\alpha^t) = 0, 0 \le t < \frac{3^{27}-1}{3-1} \right\},$$

forms a cyclic difference set with Singer parameters

$$\left(\frac{3^{27}-1}{3-1}, \frac{3^{26}-1}{3-1}, \frac{3^{25}-1}{3-1} \right).$$

Recently, Lin conjectured a ternary sequence with ideal autocorrelation, which is given as:

Conjecture 12 (Lin [16]). Let $m = 2k+1$ and $s = 2 \times 3^k + 1$. Let α be a primitive element of F_{3^m}. Then the ternary sequence of period $3^m - 1$ given by

$$f(\alpha^t) = \mathrm{tr}_3^{3^m}(\alpha^t) + \mathrm{tr}_3^{3^m}(\alpha^{st}), \tag{6}$$

has the ideal autocorrelation property.

It is clear that Lin sequence in (6) is 1-homogeneous on $F_{3^m}^*$ over F_3 with difference-balance property. Therefore, if the Lin conjecture is proved, then it can also be used to construct a cyclic difference set with Singer parameter. Recently, for any odd prime p, Helleseth and Gong [8] introduced a large class of p-ary sequences

with ideal autocorrelation. They can also be used to construct the cyclic difference sets with Singer parameter for any odd prime p using the construction methods in Corollaries 8, 10, and 11.

In order to prove the inequivalence of new cyclic difference sets, we have to find their p-ranks, but it is difficult to do it in these cases. In this paper, using the 3-rank of new difference sets with parameter $((3^{3k}-1/2),(3^{3k-1}-1/2),(3^{3k-2}-1/2))$ in No et al. [21], their inequivalence was mentioned and we gave an example of new cyclic difference set, which is inequivalent to the known cyclic difference sets with the same parameter.

Acknowledgments

The author would like to thank referees and J. F. Dillon for their valuable comments and suggestions. This work was supported in part by ITRC program of the Korean Ministry of Information and Communications.

References

1. L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Mathematics, Springer Verlag (1971).
2. D. Chandler and Q. Xiang, Cyclic relative difference sets and their p-ranks, preprint.
3. A. Chang, S. W. Golomb, G. Gong and P. V. Kumar, Trace expansion and linear span of ideal autocorrelation sequences associated to the Segre hyperoval, preprint.
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.
6. G. Gong, Q-ary cascaded GMW sequences, *IEEE Trans. Inform. Theory*, Vol. 42 (1966) pp. 263–267.
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 and G. Gong, New nonbinary sequences with ideal two-level autcorrelation function, *IEEE Trans. Inform. Theory*, Vol. 48 (2002) pp. 2868–2872.
9. T. Helleseth, P. V. Kumar and H. M. Martinsen, A new family of ternary sequences with ideal two-level autcorrelation, *Proc. of International Symposium on Information Theory*, Sorrento, Italy (2000) p. 3289.
10. T. Helleseth and H. M. Martinsen, Sequences with ideal autocorrelation and difference sets, preprint.
11. D. Jungnickel, Difference sets, *Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. R. Stinson (eds), John Wiley and Sons (1992).
12. D. Jungnickel and A. Pott, Difference sets: An introduction, *Proc. of Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth and D. Jungnickel (eds), Kulwer, Amsterdam (1999) pp. 259–295.
13. A. Klapper, d-form sequences: Families of sequences with low correlation values and large linear spans, *IEEE Trans. Inform. Theory*, Vol. 41 (1995) pp. 423–431.
14. A. Klapper, A. H. Chan and M. Goresky, Cascaded GMW sequences, *IEEE Trans. Inform. Theory*, Vol. 39 (1993) pp. 177–183.
15. R. Lidl and H. Niederreiter, *Finite Fields*, Vol. 20 of Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, MA (1983).
16. H. A. Lin, From cyclic Hadamard difference sets to perfectly balanced sequences, Ph.D. Dissertation, University of Southern California (1998).

17. J.-S. No, Generalization of GMW sequences and No sequences, *IEEE Trans. Inform. Theory*, Vol. IT-42 (1996) pp. 260–262.
18. J.-S. No, p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property, *IEEE Trans. Inform. Theory*, Vol. 48 (2002) pp. 2540–2546.
19. 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.
20. 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.
21. J.-S. No, D. J. Shin and T. Helleseth, On the P-ranks and characteristic polynomials of cyclic difference sets, accepted for publication in *Designs, Codes and Cryptography*, (2002).
22. J.-S. No, K. Yang, H. Chung and H. Y. Song, On the construction of binary sequences with ideal autocorrelation property, *Proc. of 1996 IEEE International Symposium on Information Theory and Its Applications (ISITA '96)*, Victoria, B.C., Canada (1996) pp. 837–840.
23. R. A. Scholtz and L. R. Welch, GMW sequences, *IEEE Trans. Inform. Theory*, Vol. IT-30 (1984) pp. 548–553.
24. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc*, Vol. 43 (1938) pp. 377–385.
25. Q. Xiang, Recent results on difference sets with classical parameters, *Proc. Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. V. Kumar, T. Helleseth and D. Jungnickel (eds), Kluwer, Amsterdam (1999) pp. 419–434.