New Cyclic Relative Difference Sets Constructed from d-Homogeneous Functions with Difference-balanced Property

Sang-Hyo Kim^o and Jong-Seon No
School of EE and CS, Seoul National University
E-mail: kimsh@ccl.snu.ac.kr

Abstract

In this paper, for any prime power q, it is shown that new cyclic relative difference sets with parameters $(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2})$ can be constructed by using d-homogeneous functions on $F_{q^n}\backslash\{0\}$ over F_q with difference-balanced property, where F_{q^n} is a finite field with q^n elements. Several new cyclic relative difference sets with parameters $(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2})$ are constructed by using p-ary sequences of period q^n-1 with ideal autocorrelation property introduced by Helleseth and Gong and d-form sequences.

I. Introduction

It is well known that the cyclic difference set with Singer parameters $(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1})$ is equivalent to the pseudo-noise sequence of period q^n-1 with ideal autocorrelation property, where q is a prime power [1]. No introduced the construction method of a new cyclic difference set with Singer parameters from the d-homogeneous function with difference-balanced property [8]. A new cyclic difference set with Singer parameters was constructed using the Helleseth-Kumar-Martinsen (HKM) sequence for $p = 3$ [5][8]. Recently, Chandler and Xiang [2] constructed a new cyclic relative difference set with parameters $(\frac{q^{3n}-1}{q-1}, q-1, q^{3n-1}, q^{3n-2})$ for $q = 3^e$ using HKM sequences.

Let G be a multiplicative group of order $u \cdot v$ and let N be a normal subgroup of order u. A subset D of k-elements of the group G is called an (v, u, k, λ) *relative difference set* in G relative to N if the set of $k(k-1)$ elements given by

$$\{d_1 d_2^{-1} \mid d_1, d_2 \in D \text{ with } d_1 \neq d_2\}$$

contains every non-identity element of $G\backslash N$ exactly λ times and no element in N [2]. Thus, the parameters of relative difference sets satisfy the following equation

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

If G is a cyclic group, D is called a cyclic relative difference set. If $u = 1$, D becomes a (v, k, λ) difference set. Two cyclic difference sets D_1, D_2 are equivalent if there exists an integer h, $gcd(h, uv) = 1$, such that $D_1^h = D_2 g$ for some $g \in G$, where $D_1^h = \{d^h \mid d \in D_1\}$ and $D_2 g = \{dg \mid d \in D_2\}$.

In this paper, for any prime power q, it is shown that new cyclic relative difference sets with parameters $(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2})$ can be constructed by using d-homogeneous functions on $F_{q^n}\backslash\{0\}$ over F_q with difference-balanced property, where F_{q^n} is a finite field with q^n elements. Several new cyclic relative difference sets with parameters $(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2})$ are constructed by using p-ary sequences of period q^n-1 with ideal autocorrelation property introduced by Helleseth and Gong and d-form sequences.

II. Main Theorem

Let q be a prime power and $n = e \cdot m > 1$ for some positive integers e and m. Then the trace function $tr_{q^m}^{q^n}(\cdot)$ is a mapping from finite field F_{q^n} to its subfield F_{q^m} defined by $tr_{q^m}^{q^n}(x) = \sum_{i=0}^{e-1} x^{q^{m \cdot i}}$, where x is an element in F_{q^n}.

Let q be a prime power. Let $f(\alpha^t)$ be a function from $F_{q^n}^*$ onto F_q, where $F_{q^n}^* = F_{q^n}\backslash\{0\}$ and F_{q^n} and F_q are finite fields with q^n elements and q elements, respectively and α is a primitive element of F_{q^n}. A function $f(\alpha^t)$ is said to be *balanced* if the element '0' appears one less time than each nonzero element in F_q in the list $f(\alpha^0)$, $f(\alpha^1)$, $f(\alpha^2)$, $f(\alpha^3)$, $\cdots$, $f(\alpha^{q^n-2})$. A function $f(\alpha^t)$ is said to be *difference-balanced* if a difference of sequence $f(\alpha^{t+\tau}) - f(\alpha^t)$ is balanced for any nonzero shift τ, $1 \leq \tau \leq q^n-2$, where indices are computed modulo q^n-1.

Klapper constructed d-form sequences [6] by using the d-homogeneous function on F_{q^n} over F_q, which is defined as

$$H(xy) = y^d H(x)$$

for any $x \in F_{q^n}$ and $y \in F_q$.

It was shown in [8] that the d-homogeneous function with difference-balanced property is balanced as follows:

Lemma 1 [No [8]]: Let q be a prime power and n be a positive integer. Let α be a primitive element of a finite field F_{q^n} and $f(\alpha^t)$ be a function from $F_{q^n}^*$ onto F_q. If $f(\alpha^t)$ is a d-homogeneous function with difference-balanced property, then $f(\alpha^t)$ is balanced.

□

New cyclic relative difference sets were introduced by Chandler and Xiang [2], from HKM sequences. It can be generalized that for any prime power q, cyclic relative difference sets are constructed using d-homogeneous functions with difference-balanced property as in the following theorem.

Theorem 2 (Main): Let q be a prime power and n be a positive integer. Let α be a primitive element of F_{q^n}. If $f(\alpha^t)$ is a d-homogeneous function on $F_{q^n}^*$ over F_q with difference-balanced property, where d is relatively prime to $q-1$, then a set

$$D = \{\ \alpha^t \mid f(\alpha^t) = 1, \alpha^t \in F_{q^n}^*\} \tag{1}$$

is a cyclic relative difference set with parameters

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

in a multiplicative group $F_{q^n}^*$ relative to its normal subgroup F_q^*.

Proof: From Lemma 1, $f(\alpha^t)$ is balanced and thus as t varies from 0 to q^n-2, $f(\alpha^t)$=1 appears q^{n-1} times, which proves that the cardinality of the set D is $k = q^{n-1}$.

Let $T = \frac{q^n-1}{q-1}$. Then, $\beta = \alpha^T$ is a primitive element of F_q. Using the d-homogeneous property, we have the relation

$$f(\alpha^{t+iT}) = \alpha^{di\cdot T} \cdot f(\alpha^t) = \beta^{di} \cdot f(\alpha^t).$$

Because $\beta^{di} \neq 0$, $f(\alpha^{t+iT})$ is equal to zero if and only if $f(\alpha^t) = 0$. Therefore, for $0 \le t \le T-1$, $f(\alpha^t) = 0$ occurs $\frac{q^{n-1}-1}{q-1}$ times.

Since d is relatively prime to $q-1$, there exist d^{-1} such that $d \cdot d^{-1} \equiv 1 \mod q-1$. Instead of $f(\alpha^t)$, it is possible to consider the function $f(\alpha^{d^{-1}t})$, which is an 1-homogeneous function. Therefore, without loss of generality, we assume that $f(\alpha^t)$ is an 1-homogeneous function.

Now, we have to prove that for $1 \le \tau \le q^n-2$, the pairs of elements $\alpha^{t+\tau}$ and α^t, $(i.e., d_1 \cdot d_2^{-1} = \alpha^{t+\tau} \cdot \alpha^{-t} = \alpha^\tau)$ in D occur $\lambda = q^{n-2}$ times for any $\tau \neq 0 \mod T$ and don't occur for $\tau = 0 \mod T$ as t varies $0 \le t \le q^n-2$ because the multiplicative normal subgroup F_q^* of $F_{q^n}^*$ can be expressed as $\{\alpha^{iT} \mid 0 \le i \le q-2\}$. It is equivalent to show that for $1 \le \tau \le q^n-2$, $(f(\alpha^{t+\tau}), f(\alpha^t)) = (1,1)$ occurs $\lambda = q^{n-2}$ times for any $\tau \neq 0 \mod T$ and doesn't occur for $\tau = 0 \mod T$ as t varies $0 \le t \le q^n-2$.

Case 1) $\tau = 0 \mod T$ and $\tau \neq 0 \mod q^n-1$;

Let $\tau = i \cdot T$ for an integer i, $1 \le i \le q-2$. Then, $f(\alpha^{t+iT}) = \beta^i \cdot f(\alpha^t)$ because $f(\alpha^t)$ is an 1-homogeneous function. It is obvious that $(f(\alpha^{t+iT}), f(\alpha^t)) = (1,1)$ can't occur as t varies over $0 \le t \le q^n-2$. Thus, for any $d_1, d_2 \in D$, $d_1 d_2^{-1} \neq \alpha^{iT}$ for some integer i, which means that $d_1 d_2^{-1} \notin F_q^*$.

Case 2) $\tau \neq 0 \mod T$;

Let $x_i = \beta^i$ and $x_j = \beta^j$ for $0 \le i,j \le q-2$ and $x_\infty = 0$. Let $a_{i,j}$ be a number of occurrence $(f(\alpha^{t+\tau}), f(\alpha^t)) = (x_i, x_j)$ for a fixed $x_i, x_j \in F_q$ when t varies over $0 \le t \le q^n-2$. From the difference-balanced property of the function $f(\alpha^t)$, $f(\alpha^{t+\tau}) - f(\alpha^t) = x_i - x_j = 0$ occurs $q^{n-1}-1$ times for any $\tau \neq 0 \mod T$ as t varies over $0 \le t \le q^n-2$, which leads to the relation as

$$\sum_{i=0}^{q-2} a_{i,i} + a_{\infty,\infty} = q^{n-1} - 1. \tag{2}$$

For any integer k, we have the pair

$$\begin{aligned} (f(\alpha^{t+\tau}), f(\alpha^{t+kT})) &= (f(\alpha^{t+\tau}), \beta^k \cdot f(\alpha^t)) \\ &= (x_i, \beta^k \cdot x_j). \end{aligned}$$

As t varies over $0 \le t \le q^n-2$, the pair $(x_i, \beta^k \cdot x_j)$ occurs $a_{i,j}$ times and the difference of $f(\alpha^{t+\tau})$ and $f(\alpha^{t+kT})$ given by

$$f(\alpha^{t+\tau}) - f(\alpha^{t+kT}) = x_i - \beta^k \cdot x_j$$

must be balanced. Using the notation of x_i and x_j, we can rewrite the difference as

$$x_i - \beta^k \cdot x_j = \begin{cases} x_i - x_{j+k}, & \text{for } x_j \neq 0 \\ x_i, & \text{for } x_j = 0, \end{cases}$$

where the subscript of x_{j+k} is computed modulo $q-1$. As t varies over $0 \le t \le q^n-2$, the occurrence of the pairs is given as:

For $x_j \neq 0$, (x_i, x_{j+k}) occurs $a_{i,j}$ times.

For $x_j = 0$, (x_i, x_∞) occurs $a_{i,\infty}$ times.

For $x_j \neq 0$, $x_i - x_{j+k} = \beta^i - \beta^{j+k} = 0$ means $j + k \equiv i \mod q-1$ and it occurs $a_{i,j} = a_{i,i-k}$ times, where indices are computed modulo $q-1$. For $x_j = 0$, $x_i - x_j = 0$ occurs $a_{\infty,\infty}$ times. From the difference-balanced property, as t varies over $0 \le t \le q^n-2$, the number of occurrences $f(\alpha^{t+\tau}) - f(\alpha^{t+kT}) = 0$ is equal to $q^{n-1}-1$. Thus, for k, $0 \le k \le q-2$, we have

$$\sum_{i=0}^{q-2} a_{i,i-k} + a_{\infty,\infty} = q^{n-1} - 1 \tag{3}$$

where indices are computed modulo $q-1$. Therefore, we can rewrite the equation (3) as follows:

$$\begin{aligned}
k=0: &\quad a_{0,0}+a_{1,1}+\cdots+a_{q-2,q-2}+a_{\infty,\infty} &= q^{n-1}-1\\
k=1: &\quad a_{0,q-2}+a_{1,0}+\cdots+a_{q-2,q-3}+a_{\infty,\infty} &= q^{n-1}-1\\
k=2: &\quad a_{0,q-3}+a_{1,q-2}+\cdots+a_{q-2,q-4}+a_{\infty,\infty} &= q^{n-1}-1\\
&\quad\cdots & (4)\\
k=q-2: &\quad a_{0,1}+a_{1,2}+\cdots+a_{q-2,0}+a_{\infty,\infty} &= q^{n-1}-1\\
k=\infty: &\quad a_{0,\infty}+a_{1,\infty}+\cdots+a_{q-2,\infty}+a_{\infty,\infty} &= q^{n-1}-1.
\end{aligned}$$

The last equation comes from the fact that the function $f(\alpha^t)$ is balanced and $f(\alpha^t)$ takes on the value of zero $q^{n-1}-1$ times for $0 \le t \le q^n-2$. If we add all terms in left hand side of (4), we have

$$LHS = \sum_{i=0}^{q-2}\left\{\sum_{j=0}^{q-2} a_{i,j} + a_{i,\infty}\right\} + q\cdot a_{\infty,\infty}, \quad (5)$$

where the inner summation corresponds to the column-wise summation of the set of equations of (4). We also have the summation of right hand side of (4) as

$$RHS = q\cdot(q^{n-1}-1). \quad (6)$$

It can be easily shown that the inner summation in (5) is the number of occurrences $f(\alpha^{t+\tau}) = \beta^i (\neq 0)$ for a fixed i as t varies over $0 \le t \le q^n-2$, which is clearly q^{n-1}. From (5) and (6), we have the relation as follows:

$$(q-1)\cdot q^{n-1} + q\cdot a_{\infty,\infty} = q\cdot(q^{n-1}-1).$$

Then the value of $a_{\infty,\infty}$ is equal to $q^{n-2}-1$.

Now, we have to determine $a_{0,0}$, which is the number of occurrence $(f(\alpha^{t+\tau}), f(\alpha^t)) = (1,1)$ as t varies over $0 \le t \le q^n-2$. If $(f(\alpha^{t_1+\tau}), f(\alpha^{t_1})) = (1,1)$ for some $t = t_1$, then we have

$$\begin{aligned}
\left(f(\alpha^{t_1+\tau+T}), f(\alpha^{t_1+T})\right) &= (\beta\cdot f(\alpha^{t_1+\tau}), \beta\cdot f(\alpha^{t_1})) = (\beta,\beta)\\
\left(f(\alpha^{t_1+\tau+2T}), f(\alpha^{t_1+2T})\right) &= (\beta^2\cdot f(\alpha^{t_1+\tau}), \beta^2\cdot f(\alpha^{t_1})) = (\beta^2,\beta^2)\\
\left(f(\alpha^{t_1+\tau+3T}), f(\alpha^{t_1+3T})\right) &= (\beta^3\cdot f(\alpha^{t_1+\tau}), \beta^3\cdot f(\alpha^{t_1})) = (\beta^3,\beta^3)\\
&\cdots\\
\left(f(\alpha^{t_1+\tau+(q-3)T}), f(\alpha^{t_1+(q-3)T})\right)&\\
= (\beta^{q-3}\cdot f(\alpha^{t_1+\tau}), \beta^{q-3}\cdot f(\alpha^{t_1})) &= (\beta^{q-3},\beta^{q-3})\\
\left(f(\alpha^{t_1+\tau+(q-2)T}), f(\alpha^{t_1+(q-2)T})\right)&\\
= (\beta^{q-2}\cdot f(\alpha^{t_1+\tau}), \beta^{q-2}\cdot f(\alpha^{t_1})) &= (\beta^{q-2},\beta^{q-2}),
\end{aligned}$$

which means that all $a_{i,i}$'s takes the same value for $i = 0,1,2,\cdots,q-2$. From (2) and $a_{\infty,\infty}$, $a_{i,i}$ is equal to q^{n-2} for $i, 0 \le i \le q-2$, which proves the theorem.

□

If we can find a d-homogeneous function with difference-balanced property, then the cyclic relative difference sets can be constructed using the above theorem, which is described in the following section.

III. Relative Difference Sets from q-ary sequences

If $f(\alpha^t)$ is a function from $F_{p^n}^*$ to F_p, it can be considered as a p-ary sequence of period p^n-1, where p be a prime. The periodic autocorrelation function of a p-ary sequence is defined as

$$R(\tau) = \sum_{t=0}^{p^n-2} \omega^{f(\alpha^{t+\tau})-f(\alpha)},$$

where ω is a p-th root of unity. A sequence $f(\alpha^t)$ is said to have an *ideal autocorrelation property* if the distribution of the autocorrelation function takes the values given by

$$R(\tau) = \begin{cases} p^n-1, & \text{for } \tau \equiv 0 \mod p^n-1\\ -1, & \text{for } \tau \neq 0 \mod p^n-1.\end{cases}$$

Recently, Helleseth and Gong introduced new p-ary sequences of period p^n-1 with ideal autocorrelation property [4], which include ternary Helleseth-Kumar-Martinsen sequences [5] as a special case in the following theorem.

Theorem 3 [Helleseth and Gong[4]]: Let p be a prime and α be a primitive element of F_{p^n}. Let $n = (2m+1)\cdot k$ and let s, $1 \le s \le 2m$ be an integer such that $gcd(s, 2m+1) = 1$. Let $q = p^k$. Define

$$g(x) = \sum_{i=0}^{m} u_i \cdot x^{\frac{q^{2i}+1}{2}} \quad (7)$$

and let $b_0 = 2u_0, u_i = b_{2i} = b_{2m+1-2i}$ for $i = 1,2,3,\cdots,m$. Suppose $b_0 = \pm 1$ and $b_{is} = (-1)^i$ for $i = 1,2,\cdots,m$, then the sequence over F_p defined by

$$f(\alpha^t) = tr_p^{p^n}(g(\alpha^t)) \quad (8)$$

has an ideal autocorrelation property, where indices of b_{is} are taken modulo $2m+1$.

□

The above sequence can be rewritten as

$$f(\alpha^t) = \sum_{i=0}^{m} u_i \cdot tr_p^{p^n}(\alpha^{\frac{q^{2i}+1}{2}t}), \quad (9)$$

where $u_i \in F_p$. It is shown that the above sequences has an 1-homogeneous function with difference-balanced property as follows. we omit the proof here.

Lemma 4 : Let $f(\alpha^t)$ be a function defined in (9). Then $f(\alpha^t)$ is an 1-homogeneous function on $F_{p^n}^*$ over F_p with difference-balanced property. □

Let l be a positive integer such that $l|k$. Then the sequence (9) can be rewritten as

$$f(\alpha^t) = tr_p^{p^l}\{\sum_{i=0}^{m} u_i \cdot tr_{p^l}^{p^n}(\alpha^{\frac{q^{2i}+1}{2}t})\}, \quad (10)$$

where $u_i \in F_p$. Let $h(\alpha^t)$ is a function from $F_{p^n}^*$ to F_{p^l} given by

$$h(\alpha^t) = \sum_{i=0}^{m} u_i \cdot tr_{p^l}^{p^n}(\alpha^{\frac{q^{2i}+1}{2}} t). \quad (11)$$

Then the function $h(\alpha^t)$ has the following property.

Theorem 5 : Let $h(\alpha^t)$ be a function defined in (11). Then $h(\alpha^t)$ is an 1-homogeneous function on $F_{p^n}^*$ over F_{p^l} with difference-balanced property. □

Using the 1-homogeneous function $h(\alpha^t)$ with difference-balanced property and main theorem, the cyclic relative difference set is constructed as in the following theorem.

Theorem 6 Let $n = (2m+1)k$ and l be a positive integer such that $l|k$. Let $h(\alpha^t)$ be a function defined in (11). Then, a set of elements

$$D = \{\alpha^t \mid h(\alpha^t) = 1, \alpha^t \in F_{p^n}^*\}$$

is a cyclic relative difference set in $F_{p^n}^*$ relative to $F_{p^l}^*$ with parameters $(\frac{p^n-1}{p^l-1}, p^l-1, p^{n-l}, p^{n-2l})$.

□

It is clear that the cyclic relative difference set in Theorem 6 contains the cyclic relative difference set by Chandler and Xiang [2] as a special case of $p = 3$ and $m = 1$.

Using the above theorem we can construct a cyclic relative difference set with parameters $(\frac{5^6-1}{5^2-1}, 5^2 - 1, 5^4, 5^2)$. From the computer simulation, it turns out that this cyclic relative difference sets given are inequivalent to the classical relative difference sets which means that this cyclic relative difference set is new.

From the construction method of the cyclic difference sets in [8], it is easy to show that a set of elements

$$D = \{\alpha^t \mid h(\alpha^t) = 0, \alpha^t \in F_{p^n}^*\}$$

becomes a cyclic difference set with Singer parameters $(\frac{p^n-1}{p^l-1}, \frac{p^{n-l}-1}{p^l-1}, \frac{p^{n-2l}-1}{p^l-1})$ because $h(\alpha^t)$ is an 1-homogeneous function with difference-balanced property.

From the construction method of p-ary d-form sequences [7], we can construct the p-ary d-form sequences with ideal autocorrelation property by using new sequences by Helleseth and Gong [4]. Let l_1 and l_2 be positive integers such that $l_1|l_2|k$. Then the sequence (11) can be rewritten as

$$f(\alpha^t) = tr_p^{p^{l_2}}\{\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}(\alpha^t)\}.$$

Let r be an integer relatively prime to $p^{l_2} - 1$, $1 \le r \le p^{l_2} - 2$. Then the p-ary d-from sequence with ideal autocorrelation property is constructed as follows;

$$f_d(\alpha^t) = tr_p^{p^{l_2}}\{[\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}(\alpha^{\frac{q^{2i}+1}{2}} t)]^r\},$$

which can be rewritten as

$$f_d(\alpha^t) = tr_p^{p^{l_1}}\{tr_{p^{l_1}}^{p^{l_2}}\{[\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}(\alpha^{\frac{q^{2i}+1}{2}} t)]^r\}\}.$$

Let $h_d(\alpha^t)$ be a function given by

$$h_d(\alpha^t) = tr_{p^{l_1}}^{p^{l_2}}\{[\sum_{i=0}^{m} u_i \cdot tr_{p^{l_2}}^{p^n}(\alpha^{\frac{q^{2i}+1}{2}} t)]^r\}. \quad (12)$$

Using the ideal autocorrelation property of $f_d(\alpha^t)$ and the proof of Theorem 5, it is easy to show that $h_d(\alpha^t)$ is a r'-homogeneous function on $F_{p^n}^*$ over $F_{p^{l_1}}$ with difference-balanced property, where $r = r' \mod p^{l_1} - 1$. Since $gcd(r, p^{l_2} - 1) = 1$, it is easy to show that $gcd(r', p^{l_1} - 1) = 1$.

Thus, new cyclic relative difference sets can be constructed as follows:

Theorem 7 Let $n = (2m+1)k$ and l_1 and l_2 be positive integers such that $l_1|l_2|k$. Let $h_d(\alpha^t)$ be a function defined in (12). A set of elements

$$D = \{\alpha^t \mid h_d(\alpha^t) = 1, \alpha^t \in F_{p^n}^*\}$$

is a cyclic relative difference set in $F_{p^n}^*$ relative to $F_{p^{l_1}}^*$ with parameters $(\frac{p^n-1}{p^{l_1}-1}, p^{l_1}-1, p^{n-l_1}, p^{n-2l_1})$.

□

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, 2001.

[3] B. Gordon, W.H. Mills and L.R. Welch, "Some new difference sets," *Canad. J. Math.*, vol. 14, pp. 614-625, 1962.

[4] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," preprint, 2001.

[5] T. Helleseth, P.V. Kumar and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation," preprint, 1999.

[6] A. Klapper, "d-form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423-431, Mar. 1995.

[7] J.S. No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property," preprint, 2001.

[8] J.S. No, "New cyclic difference sets with Singer parameters constructed from d-homogeneous function," preprint, 2001.