where $\gamma = k/2^n$ is the proportion of k of the period length, and $H(x)$ is the binary entropy function (cf. [6, p. 55]).

The magnitude of the bounds (8) and (9) depends on the value of the sum

$$\begin{aligned}\Omega &= \sum_{t=2}^{n-1} 2^{-2^t+t} \sum_{j=0}^{k} \binom{2^t}{j} \\ &= 2^{\rho+1} - 4 + 2^{-2^{\rho+1}+\rho+1} \sum_{j=0}^{k} \binom{2^{\rho+1}}{j} \\ &\quad + 2^{-2^{\rho+2}+\rho+2} \sum_{j=0}^{k} \binom{2^{\rho+2}}{j} + \sum_{t=\rho+3}^{n-1} 2^{-2^t+t} \sum_{j=0}^{k} \binom{2^t}{j}\end{aligned}$$

where $\rho = \lfloor \log_2 k \rfloor$. Because we easily can evaluate $\sum_{j=0}^{k} \binom{2^{\rho+i}}{j}$, $i = 1, 2$, if $k = 2^{\rho+1} - 1$, we compare the lower bounds (8) and (10) at these values of k to indicate the improvement. Note that then $k \approx N/2^l$ for a certain $l \geq 1$, where $N = 2^n$ is the period length. In the considered case we get

$$\Omega = 3 \cdot 2^{\rho+1} - 4 - 2^{-2^{\rho+2}+\rho+1} \binom{2^{\rho+2}}{2^{\rho+1}} - 2^{-2^{\rho+1}+\rho+1} + \sum_{t=\rho+3}^{n-1} 2^{-2^t+t} \sum_{j=0}^{k} \binom{2^t}{j}.$$

The last sum is upper-bounded by

$$\sum_{i=3}^{\infty} 2^{\rho+1-2^{\rho+i}(1-H(2^{1-i}))}$$

and we can obtain the lower bound

$$E_k \geq 2^n - 1 - 3 \cdot 2^{\rho+1} - \frac{1}{2^{2^n}} \sum_{j=0}^{k} \binom{2^n}{j}. \tag{11}$$

In order to compare this bound with (10) we essentially have to compare the terms $3 \cdot 2^{\rho+1}$ and $2^n H((2^{\rho+1} - 1)/2^n)$ or, equivalently, the terms $3 \cdot 2^{\rho+1-n}$ and $H(2^{\rho+1-n} - 2^{-n})$. We may assume that the integer n is not very small. The first term is smaller as soon as $n \geq \rho + 3$ means that the bound (11) is greater than (10) for $k \approx N/2^l$, $l \geq 2$.

REFERENCES

[1] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 561.

[2] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 144–146, Jan. 1983.

[3] A. Klimov and A. Shamir, "Cryptographic applications of T-functions," in *Selected Areas in Cryptography—SAC 2003 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2004, vol. 3006, pp. 248–261.

[4] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "A relationship between linear complexity and k-error linear complexity," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 694–698, Mar. 2000.

[5] G. B. Lauder and K. G. Paterson, "Computing the linear complexity spectrum of a binary sequence of period 2^n," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 273–280, Jan. 2003.

[6] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.

[7] W. Meidl and H. Niederreiter, "Counting functions and expected values for the k-error linear complexity," *Finite Fields Appl.*, vol. 8, pp. 142–154, 2002.

[8] ——, "Linear complexity k-error linear complexity, and the discrete fourier transform," *J. Complexity*, vol. 18, pp. 87–103, 2002.

[9] ——, "On the expected value of the linear complexity and the k-error linear complexity of periodic sequences," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2817–2825, Nov. 2002.

[10] H. Niederreiter, "Some computable complexity measures for binary sequences," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London, U.K.: Springer-Verlag, 1999, pp. 67–78.

[11] H. Niederreiter and H. Paschinger, "Counting functions and expected values in the stability theory of stream ciphers," in *Sequences and Their Applications*, C. Ding, T. Helleseth, and H. Niederreiter, Eds. London: Springer-Verlag, 1999, pp. 318–329.

[12] R. A. Rueppel, *Analysis and Design of Stream Ciphers*. Berlin, Germany: Springer-Verlag, 1986.

[13] M. Stamp and C. F. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1398–1401, Jul. 1993.

New Cyclic Relative Difference Sets Constructed From d-Homogeneous Functions With Difference-Balanced Property

Sang-Hyo Kim, Jong-Seon No, *Member, IEEE*, Habong Chung, *Member, IEEE*, and Tor Helleseth, *Fellow, IEEE*

***Abstract*—For a prime power q, we show that a cyclic relative difference set with parameters $(\frac{q^n-1}{q-1}, q-1, q^{n-1}, q^{n-2})$ can be constructed from a d-homogeneous function from $F_{q^n} \setminus \{0\}$ onto F_q with difference-balanced property, where F_{q^n} is the finite field with q^n elements. This construction method enables us to construct several new cyclic relative difference sets with parameters $(\frac{p^n-1}{p^l-1}, p^l - 1, p^{n-l}, p^{n-2l})$ from p-ary sequences of period $p^n - 1$ with ideal autocorrelation property introduced by Helleseth and Gong. Using a lifting idea, other new cyclic relative difference sets can be constructed from the Helleseth–Gong (HG) sequences. Also, the 3-ranks and the trace representation of the characteristic sequences of cyclic relative difference sets from a specific class of ternary HG sequences and ternary Lin sequences are derived.**

***Index Terms*—Cyclic difference sets, cyclic relative difference sets, d-homogeneous functions, p-rank, sequences.**

I. INTRODUCTION

It is well known that some cyclic difference set with Singer parameters

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

can be constructed from the pseudonoise sequence of period $p^n - 1$ with ideal autocorrelation property, where p is a prime [1], [6], [13]. Recently, No [18] introduced a method of constructing cyclic difference sets with Singer parameters from a d-homogeneous function on $F_{q^n}^*$ with difference-balanced property. Using this method, a new cyclic difference set with Singer parameters was constructed from Helleseth–Kumar–Martinsen (HKM) sequence for $p = 3$ [11], [18].

Manuscript received August 5, 2003; revised September 21, 2004. This work was supported in part by BK21, ITRC program of the Korean Ministry of Information and Communications and the Norwegian Research Council.

S. H. Kim and J. S. No are with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: kimsh@ccl.snu.ac.kr, jsno@snu.ac.kr).

H. Chung is with the School of Electronic and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020, Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no).

Communicated by K. G. Paterson. Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2004.842712

Also this method was modified by Chandler and Xiang [4] to construct new cyclic relative difference sets with parameters

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

for $q = 3^e$ from HKM sequences. They also derived the 3-ranks of HKM relative difference sets.

The concept of relative difference set was introduced by Butson [3] and formally defined by Elliott and Butson [7]. Let G be a multiplicative group of order uv and let N be a normal subgroup of order u. A subset D of k elements of the group G is called a (v, u, k, λ) relative difference set in G relative to N if the set of $k(k-1)$ elements given by

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

contains every nonidentity element of $G\backslash N$ exactly λ times and no element in N [4]. 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 relative difference sets D_1 and D_2 are equivalent if there exists an integer e, $\gcd(e, uv) = 1$, such that $D_1^e = D_2 g$ for some $g \in G$, where $D_1^e = \{d^e \mid d \in D_1\}$ and $D_2 g = \{dg \mid d \in D_2\}$.

It is well known that projections of cyclic relative difference sets are cyclic difference sets with Singer parameters [4], which are equivalent to the sequences with two-level autocorrelation property [6], [13]. Some of cyclic relative difference sets with Singer parameters are also equivalent to the sequences with two-level autocorrelation property. Further, cyclic relative difference sets and cyclic differences sets with Singer parameters are useful for constructions of optical orthogonal codes [5], difference families, and Hadamard matrices [21], [22].

Helleseth and Gong introduced p-ary sequences, namely, Helleseth–Gong (HG) sequences, with ideal autocorrelation property [10]. They include HKM sequences as a special case. This finding of HG sequences motivates us to generalize Chandler and Xiang's construction of cyclic relative difference sets from HKM sequences.

In this correspondence, for a prime power q, we construct cyclic relative difference sets with parameters

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

by using d-homogeneous functions from $F_{q^n}^*$ onto F_q with difference-balanced property, where F_{q^n} is the finite field with q^n elements. Using the result, new cyclic relative difference sets with parameters

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

are constructed from p-ary HG sequences. Then, the constructions are extended by applying the lifting idea [17], [18]. Thus, we give the general class of new cyclic relative difference sets including the relative difference sets introduced by Chandler and Xiang.

This correspondence is organized as follows. The main theorem of constructing cyclic relative difference sets from d-homogeneous functions with difference-balanced property is in Section II. In Section III, we identify the d-homogeneous functions underlying HG sequences and their extensions obtained from a lifting idea, and construct the cyclic relative difference sets, many of which are new. Finally, Section IV contains the 3-rank derivation and the trace representation of the characteristic sequences of cyclic relative difference sets from a specific class of ternary HG sequences and ternary Lin sequences.

II. Main Theorem

Let q be a prime power and n, m be positive integers such that $m|n$. 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 [15]

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

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

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

i) $\mathrm{tr}_{q^m}^{q^n}(ax+by) = a\mathrm{tr}_{q^m}^{q^n}(x) + b\mathrm{tr}_{q^m}^{q^n}(y)$, for all $a, b \in F_{q^m}$, $x, y \in F_{q^n}$;

ii) $\mathrm{tr}_{q^m}^{q^n}(x^{q^m}) = \mathrm{tr}_{q^m}^{q^n}(x)$, for all $x \in F_{q^n}$;

iii) $\mathrm{tr}_q^{q^n}(x) = \mathrm{tr}_q^{q^m}\left(\mathrm{tr}_{q^m}^{q^n}(x)\right)$, for all $x \in F_{q^n}$.

Let q be a prime power and α a primitive element in F_{q^n}. Let $f(x)$ be a function from $F_{q^n}^*$ onto F_q. Such a function $f(x)$ is said to be *balanced* if the element "0" appears one less time than every nonzero element of 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 the difference function $f(xz) - f(x)$ is balanced for any $z \in F_{q^n}\backslash\{0,1\}$.

Klapper introduced the d-homogeneous function from F_{q^n} onto F_q [14] which is defined as

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

for any $x \in F_{q^n}$ and $y \in F_q$. The following lemma shows [18] that the d-homogeneous function with difference-balanced property is balanced.

Lemma 1: (No [18]): Let q be a prime power and n be a positive integer. Let $f(x)$ be a function from $F_{q^n}^*$ onto F_q. If $f(x)$ is a d-homogeneous function with difference-balanced property, then $f(x)$ is balanced. □

New cyclic relative difference sets with parameters

$$\left(\frac{q^{3n}-1}{q-1}, q-1, q^{3n-1}, q^{3n-2}\right), \qquad \text{for } q = 3^e$$

were introduced by Chandler and Xiang [4], which were constructed from ternary sequences with ideal autocorrelation property introduced by Helleseth, Kumar, and Martinsen. The construction by Chandler and Xiang can be generalized so 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 a positive integer. Let α be a primitive element in F_{q^n}. If $f(x)$ is a d-homogeneous function on $F_{q^n}^*$ over F_q with difference-balanced property, where d is relatively prime to $q^n - 1$, then the set

$$D_f = \left\{x \mid f(x) = 1, x \in F_{q^n}^*\right\} \tag{1}$$

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

Proof: From Lemma 1, $f(x)$ is balanced and as x varies over $F_{q^n}^*$, $f(x) = 1$ appears q^{n-1} times and, thus, we proved that the cardinality of the set D_f is $k = q^{n-1}$.

Let $g \in F_q^*$ and $x \in F_{q^n}^*$. Using the d-homogeneous property, we have the relation

$$f(gx) = g^d f(x).$$

The condition that d is relatively prime to $q^n - 1$ implies that d is also relatively prime to $q - 1$. Thus, there exists d^{-1} such that $dd^{-1} = 1 \bmod q - 1$. Now, we define a new function

$$h(x) = f(x^{d^{-1}}).$$

Then we have

$$h(gx) = f(g^{d^{-1}}x^{d^{-1}}) = g^{d^{-1}d}f(x^{d^{-1}}) = gh(x)$$

which means that $h(x)$ is 1-homogeneous. Also, we have the relation that

$$D_h = D_f^d \doteq \{x^d | x \in D_f\}$$

which implies that D_h is also a cyclic relative difference set if D_f is a cyclic relative difference set. Therefore, without loss of generality, we can assume that f is a 1-homogeneous function.

For $z \in F_{q^n}^*$, $a, b \in F_q$, let $n_z(a,b)$ be the number of solutions for $x \in F_{q^n}^*$ satisfying the two equations

$$f(xz) = a, \quad f(x) = b.$$

Then, in order to prove the theorem, we only have to show that

$$n_z(1,1) = q^{n-2} \text{ for } z \in F_{q^n} \backslash F_q$$
$$n_z(1,1) = 0 \text{ for } z \in F_q \backslash \{0,1\}.$$

Case 1) When $z \in F_q \backslash \{0,1\}$:

We have $f(zx) = zf(x)$. It is obvious that $n_z(1,1) = 0$. Thus, for any distinct pair $d_1, d_2 \in D_f$, $d_1 d_2^{-1} \notin F_q$.

Case 2) When $z \in F_{q^n} \backslash F_q$:

Since $f(zx) - f(g^{-1}x)$ is balanced for any $g \in F_q^*$, 0 occurs $q^{n-1} - 1$ times as x varies over $F_{q^n}^*$. Thus, we have

$$\sum_{a \in F_q} n_z(a, ga) = q^{n-1} - 1. \tag{2}$$

Since $f(x)$ is balanced, we have

$$\sum_{a \in F_q} n_z(a,0) = \sum_{b \in F_q} n_z(0,b) = q^{n-1} - 1. \tag{3}$$

Also, note that

$$\sum_{a \in F_q} \sum_{b \in F_q} n_z(a,b) = q^n - 1. \tag{4}$$

Now, we have

$$\begin{aligned} \sum_{a \in F_q} \sum_{b \in F_q} n_z(a,b) &= \sum_{a \in F_q} n_z(a,0) + \sum_{b \in F_q} n_z(0,b) \\ &\quad - n_z(0,0) + \sum_{g \in F_q^*} \sum_{a \in F_q^*} n_z(a, ga) \\ &= \sum_{a \in F_q} n_z(a,0) + \sum_{b \in F_q} n_z(0,b) - n_z(0,0) \\ &\quad + \sum_{g \in F_q^*} \left\{ \sum_{a \in F_q} n_z(a, ga) - n_z(0,0) \right\}. \end{aligned} \tag{5}$$

Plugging (2), (3), and (4) into (5), we have

$$q^n - 1 = 2(q^{n-1} - 1) + (q-1)(q^{n-1} - 1) - qn_z(0,0)$$

which gives

$$n_z(0,0) = q^{n-2} - 1.$$

Now, we have to compute $n_z(1,1)$. Since it is obvious that $n_z(b,b)$ has the same value for all $b \in F_q^*$, we have

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

Therefore, $n_z(1,1) = q^{n-2}$. □

III. Cyclic Relative Difference Sets From p-Ary Sequences

When $f(x)$ is a function from $F_{p^n}^*$ onto F_p, $f(\alpha^t)$ can be considered as a p-ary sequence of period $p^n - 1$, where p is a prime and α a primitive element in F_{p^n}. The periodic autocorrelation function of a p-ary sequence is defined as

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

where ω is a complex pth root of unity. A sequence $f(\alpha^t)$ is said to have ideal autocorrelation property if the autocorrelation function takes the values given by

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

Recently, Helleseth and Gong introduced new p-ary sequences of period $p^n - 1$ with ideal autocorrelation property [10], which include the ternary HKM sequences [11] as a special case as in the following theorem.

Theorem 3: (Helleseth and Gong [10]): Let p be an odd prime, $q = p^k$, and α be a primitive element in F_{p^n}. Let $n = (2m+1)k$ and s, $1 \le s \le 2m$, be an integer such that $\gcd(s, 2m+1) = 1$. Define $b_0 = 1$, $b_{is} = (-1)^i$, and $b_i = b_{2m+1-i}$ for $i = 1, 2, \ldots, m$. Let $u_0 = \frac{b_0}{2}$, $u_i = b_{2i}$ for $i = 1, 2, \ldots, m$. Define

$$g(x) = \sum_{i=0}^{m} u_i x^{\frac{q^{2i}+1}{2}}. \tag{6}$$

Then the p-ary sequences of period $p^n - 1$ defined by

$$f(\alpha^t) = \mathrm{tr}_p^{p^n}(g(\alpha^t)) \tag{7}$$

have ideal autocorrelation property. □

The following lemma shows that the function $f(\alpha^t)$ in (7) is a 1-homogeneous function with difference-balanced property.

Lemma 4: Let $f(x)$ be the function defined by

$$f(x) = \mathrm{tr}_p^{p^n}(g(x)) = \sum_{i=0}^{m} u_i \mathrm{tr}_p^{p^n}\left(x^{\frac{q^{2i}+1}{2}}\right) \tag{8}$$

where $g(x)$ and u_i's are defined in Theorem 3. Then $f(x)$ is a 1-homogeneous function on $F_{p^n}^*$ over F_p with difference-balanced property.

Proof: See Appendix I. □

Let l be a positive integer such that $l|k$. Then the function $f(x)$ in (8) can be rewritten as

$$f(x) = \mathrm{tr}_p^{p^l}\left\{\sum_{i=0}^{m} u_i \mathrm{tr}_{p^l}^{p^n}\left(x^{\frac{q^{2i}+1}{2}}\right)\right\} \tag{9}$$

where $u_i \in F_p$. The next theorem shows that the inner sum in (9) is a 1-homogeneous function from $F_{p^n}^*$ to F_{p^l} with difference-balanced property.

Theorem 5: Let l be a positive integer such that $l|k$ and $h(x)$ be the function defined by

$$h(x) = \sum_{i=0}^{m} u_i \mathrm{tr}_{p^l}^{p^n}\left(x^{\frac{q^{2i}+1}{2}}\right) \tag{10}$$

where n, m, k, and u_i's are those of Theorem 3. Then $h(x)$ is a 1-homogeneous function from $F_{p^n}^*$ onto F_{p^l} with difference-balanced property.

Proof: See Appendix II. □

Using the 1-homogeneous function $h(x)$ with difference-balanced property in (10) and the main theorem, a 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 $h(x)$ be the function defined in (10). Then, the set

$$D = \left\{x \mid h(x) = 1, x \in F_{p^n}^*\right\}$$

is a cyclic relative difference set in $F_{p^n}^*$ relative to $F_{p^l}^*$ with parameters

$$\left(\frac{p^n-1}{p^l-1}, p^l-1, p^{n-l}, p^{n-2l}\right). \quad \square$$

It is clear that the cyclic relative difference sets in Theorem 6 include the cyclic relative difference sets by Chandler and Xiang [4] as a special case of $p = 3$ and $m = 1$.

For $p = 5$, $m = 1$, and $k = 2$, an example of relative difference set in $F_{5^6}^*$ relative to $F_{5^2}^*$ is given as follows.

Example 7: Let $h(x)$ be the function from $F_{5^6}^*$ to F_{5^2} given by

$$\begin{aligned} h(x) &= \sum_{i=0}^{1} u_i \mathrm{tr}_{5^2}^{5^6}\left(x^{\frac{5^{4i}+1}{2}}\right) \\ &= 2\mathrm{tr}_{5^2}^{5^6}(x) + \mathrm{tr}_{5^2}^{5^6}(x^{313}). \end{aligned}$$

Then, the set

$$D = \{x \mid h(x) = 1, x \in F_{5^6}^*\} \tag{11}$$

is a cyclic relative difference set in $F_{5^6}^*$ relative to $F_{5^2}^*$ with parameters

$$\left(\frac{5^6-1}{5^2-1}, 5^2-1, 5^4, 5^2\right). \quad \square$$

So far, the only known cyclic relative difference set with parameters $(\frac{5^6-1}{5^2-1}, 5^2-1, 5^4, 5^2)$ is

$$D = \left\{x \mid \mathrm{tr}_{5^2}^{5^6}(x) = 1, x \in F_{5^6}^*\right\}. \tag{12}$$

From the computer simulation, it turns out that the cyclic relative difference sets given in (11) and (12) are inequivalent, which means that the cyclic relative difference set in (11) is new.

From the construction method of the cyclic difference sets in [18], it is easy to show that the set of elements

$$D = \left\{x \mid h(x) = 0, x \in F_{p^n}^*/F_{p^l}^*\right\}$$

becomes a cyclic difference set with Singer parameters

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

because $h(x)$ is a 1-homogeneous function with difference-balanced property.

No introduced the p-ary d-form sequences by applying a lifting idea to p-ary sequences as follows.

Theorem 8: (No [17]) Let p be a prime and l, n integers such that $l|n$. Let $e = d \bmod p^l - 1$ for all e in some index set I, where d is relatively prime to $p^l - 1$. Assume that the p-ary sequence of period $p^n - 1$

$$s(t) = \sum_{e \in I} u_e \mathrm{tr}_p^{p^n}(\alpha^{et}), \qquad u_e \in F_p^*$$

has ideal autocorrelation property. Then, for an integer r relatively prime to $p^l - 1$ and $1 \le r < p^l - 1$, the p-ary d-form sequences $s_d(t)$ of period $p^n - 1$ defined by

$$s_d(t) = tr_p^{p^l}\left(\left[\sum_{e \in I} u_e \mathrm{tr}_{p^l}^{p^n}(\alpha^{et})\right]^r\right)$$

has ideal autocorrelation property. □

Using Theorem 8, we can construct the p-ary d-form sequences with ideal autocorrelation property from HG sequences [10]. Let l_1 and l_2 be positive integers such that $l_1|l_2|k$. Then the function in (9) can be rewritten as

$$f(x) = \mathrm{tr}_p^{p^{l_2}}\left\{\sum_{i=0}^{m} u_i \mathrm{tr}_{p^{l_2}}^{p^n}(x)\right\}.$$

Let r be an integer relatively prime to $p^{l_2} - 1$, $1 \le r < p^{l_2} - 1$, and replace x with α^t. Then a p-ary d-from sequence with ideal autocorrelation property is constructed as

$$f_d(\alpha^t) = \mathrm{tr}_p^{p^{l_2}}\left\{\left[\sum_{i=0}^{m} u_i \mathrm{tr}_{p^{l_2}}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right]^r\right\}$$

which can be rewritten as

$$f_d(\alpha^t) = \mathrm{tr}_p^{p^{l_1}}\left\{\mathrm{tr}_{p^{l_1}}^{p^{l_2}}\left\{\left[\sum_{i=0}^{m} u_i \mathrm{tr}_{p^{l_2}}^{p^n}\left(\alpha^{\frac{q^{2i}+1}{2}t}\right)\right]^r\right\}\right\}.$$

Let $h_d(x)$ be the function given by

$$h_d(x) = \mathrm{tr}_{p^{l_1}}^{p^{l_2}}\left\{\left[\sum_{i=0}^{m} u_i \mathrm{tr}_{p^{l_2}}^{p^n}\left(x^{\frac{q^{2i}+1}{2}}\right)\right]^r\right\}. \tag{13}$$

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

$$r = r' \bmod p^{l_1} - 1.$$

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 9: Let $n = (2m+1)k$ and l_1 and l_2 be positive integers such that $l_1|l_2|k$. Let $h_d(x)$ be the function defined in (13). Then the set

$$D = \left\{x \mid h_d(x) = 1, x \in F_{p^n}^*\right\}$$

is a cyclic relative difference set in $F_{p^n}^*$ relative to $F_{p^{l_1}}^*$ with parameters

$$\left(\frac{p^n-1}{p^{l_1}-1}, p^{l_1}-1, p^{n-l_1}, p^{n-2l_1}\right). \quad \square$$

From the construction method in [18], it is easy to show that the set

$$D = \left\{x \mid h_d(x) = 0, x \in F_{p^n}^*/F_{p^l}^*\right\}$$

is a cyclic difference set with Singer parameters

$$\left(\frac{p^n-1}{p^{l_1}-1}, \frac{p^{n-l_1}-1}{p^{l_1}-1}, \frac{p^{n-2l_1}-1}{p^{l_1}-1}\right)$$

because $h_d(x)$ is an r'-homogeneous function with difference-balanced property. Using the construction method of unified sequences [17] and the HG sequences [10], the cyclic difference sets with Singer parameters and cyclic relative difference sets with classical parameters can also be constructed.

Up to now, m-sequences, Gordon–Mills–Welch (GMW) sequences, HG sequences, and unified sequences have been the only known and proven p-ary ($p \geq 3$) sequences with ideal autocorrelation property. Other than these sequences, a ternary sequence is conjectured by Lin to have ideal autocorrelation property.

Conjecture 10: (Lin [16]) Let $n = 2m+1$ and $d = 2 \cdot 3^m + 1$. Let α be a primitive element in F_{3^n}. Then the ternary sequence of period $3^n - 1$ defined by

$$f(\alpha^t) = \mathrm{tr}_3^{3^n}(\alpha^t) + \mathrm{tr}_3^{3^n}(\alpha^{dt}) \tag{14}$$

has ideal autocorrelation property. □

Lin verified his conjecture up to $n = 13$. Chandler and Xiang [4] conjectured that new relative difference sets can be constructed from the Lin sequence and verified up to $n = 11$. But our main theorem tells that the verification of this conjecture is equivalent to that of the Lin conjecture, since any ternary sequence with ideal autocorrelation is difference-balanced.

IV. p-Rank and Trace Representation of Characteristic Sequences of Cyclic Relative Difference Sets

The p-rank of a (relative) difference set is defined as the rank over Z_p of the incidence matrix of the (relative) difference set. When the characteristic sequence of a cyclic (relative) difference set is expressed as a sum of trace representation, the p-rank is simply the number of terms in the trace expression. Especially when a cyclic difference set has Singer parameters

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

the p-rank receives the special interest since the only prime dividing the order of the difference set is p.

The p-ranks of cyclic relative difference sets are often used to verify their inequivalence. The 3-ranks and characteristic polynomials of the cyclic difference sets constructed from HKM sequences and Lin sequences are obtained in [19]. Chandler and Xiang [4] found the 3-ranks of their new cyclic relative difference set, which corresponds to the one in Theorem 6 for the case when $p = 3$ and $m = 1$. At this time it does not seem easy to derive the general formula for p-ranks of the cyclic relative difference sets in Theorems 6 and 9. But we can derive the 3-ranks of the case that $p = 3$, $m = 2$, and $l = 1$ in Theorem 6 and those of Lin relative difference sets by identifying the trace representation of the corresponding characteristic sequences.

Theorem 11: Let $p = 3$, $m = 2$, $n = (2m+1)k = 5k$, and $q = 3^k$. There exist two HG sequences given by

$$f_1(x) = 2\mathrm{tr}_3^{3^n}(x) + \mathrm{tr}_3^{3^n}(x^{d_1}) + 2\mathrm{tr}_3^{3^n}(x^{d_2})$$
$$f_2(x) = 2\mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^{d_1}) + \mathrm{tr}_3^{3^n}(x^{d_2})$$

where $d_1 = \frac{3^{2k}+1}{2}$ and $d_2 = \frac{3^{4k}+1}{2}$. Let D_1 and D_2 be cyclic relative difference sets defined by

$$D_1 = \{x \mid f_1(x) = 1, x \in F_{3^n}^*\}$$
$$D_2 = \{x \mid f_2(x) = 1, x \in F_{3^n}^*\}.$$

Then, for $n = 2e+1 \geq 15$, the trace representations of the characteristic sequences of D_1 and D_2 are

$$\begin{aligned}
c_1(x) = {} & 2\mathrm{tr}_3^{3^n}(x^2) + 2\mathrm{tr}_3^{3^n}(x^{(1+3^{2k})d_1}) + \mathrm{tr}_3^{3^n}(x^{d_1+3^{3k}}) \\
& + \mathrm{tr}_3^{3^n}(x^{d_1+3^{4k}}) + \mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^{d_1}) \\
& + \mathrm{tr}_3^{3^n}(x^{d_2}) + \sum_{i=1, i\neq k, 2k}^{e} \mathrm{tr}_3^{3^n}(x^{1+3^i}) \\
& + \sum_{i=1, i\neq k, 2k}^{e} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) + \sum_{i=1, i\neq k}^{e} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\
& + 2\sum_{i=0, i\neq k, 3k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_1+3^i}) + \sum_{i=0, i\neq 2k, 3k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\
& + 2\sum_{i=1, i\neq k, 2k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i d_1}) \\
c_2(x) = {} & 2\mathrm{tr}_3^{3^n}(x^2) + 2\mathrm{tr}_3^{3^n}(x^{(1+3^k)d_2}) + \mathrm{tr}_3^{3^n}(x^{d_2+3^{3k}}) \\
& + \mathrm{tr}_3^{3^n}(x) + \mathrm{tr}_3^{3^n}(x^{d_1}) + 2\mathrm{tr}_3^{3^n}(x^{d_2}) \\
& + \sum_{i=1, i\neq k, 2k}^{e} \mathrm{tr}_3^{3^n}(x^{1+3^i}) + \sum_{i=1, i\neq k, 2k}^{e} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\
& + \sum_{i=1, i\neq k}^{e} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) + \sum_{i=0, i\neq k, 3k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\
& + 2\sum_{i=0, i\neq 2k, 3k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\
& + \sum_{i=1, i\neq k, 2k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i d_1})
\end{aligned}$$

and for $n = 2e \geq 10$

$$\begin{aligned}
c_1(x) = {} & 2\mathrm{tr}_3^{3^n}(x^2) + \mathrm{tr}_3^{3^n}(x^{d_1+3^{3k}}) + \mathrm{tr}_3^{3^n}(x^{d_1+3^{4k}}) \\
& + \mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^{d_1}) + \mathrm{tr}_3^{3^n}(x^{d_2}) \\
& + 2\mathrm{tr}_3^{3^n}(x^{(1+3^{2k})d_1}) + \mathrm{tr}_3^{3^e}(x^{1+3^e}) \\
& + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}) \\
& + \sum_{i=1, i\neq k, 2k}^{e-1} \mathrm{tr}_3^{3^n}(x^{1+3^i}) \\
& + \sum_{i=1, i\neq k, 2k}^{e-1} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) + \sum_{i=1, i\neq k}^{e-1} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\
& + 2\sum_{i=1, i\neq k, 2k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i d_1}) \\
& + 2\sum_{i=0, i\neq k, 3k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_1+3^i}) + \sum_{i=0, i\neq 2k, 3k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\
c_2(x) = {} & 2\mathrm{tr}_3^{3^n}(x^2) + 2\mathrm{tr}_3^{3^n}(x^{(1+3^k)d_2}) + \mathrm{tr}_3^{3^n}(x^{d_2+3^{3k}}) \\
& + \mathrm{tr}_3^{3^n}(x) + \mathrm{tr}_3^{3^n}(x^{d_1}) + 2\mathrm{tr}_3^{3^n}(x^{d_2}) \\
& + \mathrm{tr}_3^{3^e}(x^{1+3^e}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}) \\
& + \sum_{i=1, i\neq k, 2k}^{e-1} \mathrm{tr}_3^{3^n}(x^{1+3^i}) + \sum_{i=1, i\neq k, 2k}^{e-1} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\
& + \sum_{i=1, i\neq k}^{e-1} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) + \sum_{i=0, i\neq k, 3k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\
& + 2\sum_{i=0, i\neq 2k, 3k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i}) + \sum_{i=1, i\neq k, 2k, 4k}^{n-1} \mathrm{tr}_3^{3^n}(x^{d_2+3^i d_1}).
\end{aligned}$$

And the 3-ranks L_1 and L_2 of D_1 and D_2, respectively, are given as

$$L_1 = \begin{cases} 45, & \text{for } k = 1 \\ \frac{1}{2}(9n^2 - 17n), & \text{for } k \geq 2 \end{cases}$$
$$L_2 = \begin{cases} 40, & \text{for } k = 1 \\ \frac{1}{2}(9n^2 - 19n), & \text{for } k \geq 2. \end{cases}$$

Proof: See Appendix III. □

Theorem 12: Let $f(x)$ be the function defined in (14). Assume that D given by

$$D = \{x | f(x) = 1, x \in F_{3^n}^*\} \tag{15}$$

is a cyclic relative difference set in $F_{3^n}^*$ relative to F_3. The trace representation of the characteristic sequence of D is

$$\begin{aligned} c(x) = {} & 2\mathrm{tr}_3^{3^n}(x^{1+1}) + \sum_{i=1}^{m-1} \mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ & + 2\mathrm{tr}_3^{3^n}(x^{1+3^m}) + \sum_{i=1}^{m} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d}) \\ & + \sum_{i=0, i\neq m}^{n-2} \mathrm{tr}_3^{3^n}(x^{d+3^i}) + 2\mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^d) \end{aligned}$$

and the 3-rank L of D is

$$L = \begin{cases} 12, & \text{for } n = 3 \\ 2n^2, & \text{for } n \geq 5. \end{cases}$$

Proof: See Appendix IV. □

Appendix I
Proof of Lemma 4

Since

$$\frac{q^{2i}+1}{2} = \frac{q^i+1}{2}(q^i - 1) + 1 = 1 \bmod p - 1$$

we have

$$\mathrm{tr}_p^{p^n}\left((ax)^{\frac{q^{2i}+1}{2}}\right) = a\mathrm{tr}_p^{p^n}\left(x^{\frac{q^{2i}+1}{2}}\right), \qquad \text{for any } a \in F_p$$

which implies $f(x)$ is a 1-homogeneous function from $F_{p^n}^*$ onto F_p.

For the proof of difference-balancedness of $f(\alpha^t)$, let us define the autocorrelation polynomial $R(y, \tau)$ of $f(\alpha^t)$ as

$$\begin{aligned} R(y,\tau) &\doteq \sum_{t=0}^{p^n-2} y^{f(\alpha^{t+\tau}) - f(\alpha^t)} \\ &= \sum_{k=0}^{p-1} r_k y^k \end{aligned}$$

where r_k stands for the number of occurrences of $f(\alpha^{t+\tau}) - f(\alpha^t) = k$ as t runs from 0 to $p^n - 2$. The ideal autocorrelation property of the sequences $f(\alpha^t)$ gives us that

$$1 + R(w, \tau) = 0, \qquad \forall\, \tau \neq 0$$

which implies that $1 + R(y, \tau)$ is some multiple of the minimal polynomial of w in $Z[y]$, i.e., $1 + y + y^2 \cdots + y^{p-1}$. Then we have

$$1 + R(y,\tau) = (1 + y + y^2 \cdots + y^{p-1})m(y) = \sum_{k=0}^{p-1} r_k y^k$$

where $m(y)$ is a nonzero polynomial in $Z[y]$. Since $\sum_{k=0}^{p-1} r_k = p^n - 1$, we have

$$r_0 + 1 = r_1 = \cdots = r_{p-1} = p^{n-1}.$$

Thus, $f(x)$ is difference-balanced. □

Appendix II
Proof of Theorem 5

Let $T = \frac{p^n-1}{p^l-1}$. Then α^T is a primitive element in F_{p^l}. It is clear that for an integer i, $0 \leq i \leq m$, we have

$$\frac{q^{2i}+1}{2} = \frac{q^i+1}{2}(q^i - 1) + 1 = 1 \bmod p^l - 1$$

where $q = p^k$ and $l|k$. Thus, for any $g \in F_{p^l}^*$, it is obvious that

$$g^{\frac{q^i+1}{2}(q^i-1)+1} = g$$

and therefore,

$$h(gx) = gh(x)$$

which means that $h(x)$ is a 1-homogeneous function on $F_{p^n}^*$ over F_{p^l}.

Replacing x with α^t in (9), we have the associated sequence $f(\alpha^t)$. Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 T + t_2, 0 \leq t_1 \leq p^l - 2, 0 \leq t_2 \leq T - 1$. The two-dimensional representation of the sequence $f(\alpha^t)$ can be expressed as

$$\begin{aligned} f(\alpha^t) &= \mathrm{tr}_p^{p^l}(h(\alpha^{t_1 T + t_2})) \\ &= \mathrm{tr}_p^{p^l}(\alpha^{t_1 T} h(\alpha^{t_2})) \end{aligned}$$

where the subsequence of $f(\alpha^t)$ for a fixed value $t_2, 0 \leq t_2 \leq T - 1$, is either an all-zero sequence of period $p^l - 1$ if $h(\alpha^{t_2}) = 0$ or a cyclic shift of m-sequence of period $p^l - 1$, $\mathrm{tr}_p^{p^l}(\alpha^{t_1 T})$, otherwise. The difference of $f(\alpha^t)$ can be written as

$$\begin{aligned} f(\alpha^{t+\tau}) - f(\alpha^t) &= \mathrm{tr}_p^{p^l}(\alpha^{t_1 T} h(\alpha^{t_2+\tau})) - \mathrm{tr}_p^{p^l}(\alpha^{t_1 T} h(\alpha^{t_2})) \\ &= \mathrm{tr}_p^{p^l}(\alpha^{t_1 T}[h(\alpha^{t_2+\tau}) - h(\alpha^{t_2})]) \end{aligned}$$

where the subsequence of $f(\alpha^{t+\tau}) - f(\alpha^t)$ for a fixed value t_2, $0 \leq t_2 \leq T - 1$, is also either an all-zero sequence of period $p^l - 1$ if $h(\alpha^{t_2+\tau}) = h(\alpha^{t_2})$ or a cyclic shift of m-sequence of period $p^l - 1$, $\mathrm{tr}_p^{p^l}(\alpha^{t_1 T})$, otherwise. It is known that the element "0" appears $p^{l-1} - 1$ times and each nonzero element in F_p appears p^{l-1} times in one period of the subsequence $\mathrm{tr}_p^{p^l}(\alpha^{t_1 T})$. Assume that as t_2 varies over $0 \leq t_2 \leq T - 1$, $h(\alpha^{t_2+\tau}) = h(\alpha^{t_2})$ occurs B times and $h(\alpha^{t_2+\tau}) \neq h(\alpha^{t_2})$ occurs $T - B$ times. Then the element "0" appears $(p^l - 1)B + (p^{l-1} - 1)(T - B)$ times and each nonzero element in F_p appears $p^{l-1}(T - B)$ times in one period of the difference of $f(\alpha^t)$. From Lemma 4, the function $f(x)$ is difference-balanced and thus we have

$$\begin{aligned} (p^l - 1)B + (p^{l-1} - 1)(T - B) &= p^{n-1} - 1 \\ p^{l-1}(T - B) &= p^{n-1} \end{aligned}$$

and thus, B is computed as $\frac{p^{n-l}-1}{p^l-1}$ and $T - B = p^{n-l}$. And we have the relation as

$$h(\alpha^{t_1 T + t_2 + \tau}) - h(\alpha^{t_1 T + t_2}) = \alpha^{t_1 T}\{h(\alpha^{t_2+\tau}) - h(\alpha^{t_2})\}.$$

For a fixed t_2 such that

$$h(\alpha^{t_2+\tau}) - h(\alpha^{t_2}) \neq 0$$

$h(\alpha^{t_1T+t_2+\tau})-h(\alpha^{t_1T+t_2})$ takes all nonzero elements in F_{p^l} exactly once as t_1 varies over $0 \le t_1 \le p^l-2$. Therefore, as t varies over $0 \le t \le p^n-2$, the element "0" appears

$$(p^l-1)B = p^{n-l}-1$$

times and each nonzero element in F_{p^l} appears

$$T-B = p^{n-l}$$

times in the difference $h(\alpha^{t+\tau})-h(\alpha^t)$, which proves the difference-balanced property of $h(x)$. □

Appendix III
Proof of Theorem 11

Case 1) 3-rank of D_1:

Let $c_1(x)$ be the characteristic sequence of the relative difference set D_1. Then, $c_1(x)$ is given as

$$\begin{aligned} c_1(x) &= 1+2[f_1(x)+2]^2 = 2f_1(x)^2+2f_1(x) \\ &= 2\left[\mathrm{tr}_3^{3^n}(x)\right]^2+2\left[\mathrm{tr}_3^{3^n}(x^{d_1})\right]^2 \\ &\quad +2\left[\mathrm{tr}_3^{3^n}(x^{d_2})\right]^2+2\mathrm{tr}_3^{3^n}(x)\mathrm{tr}_3^{3^n}(x^{d_1}) \\ &\quad +\mathrm{tr}_3^{3^n}(x)\mathrm{tr}_3^{3^n}(x^{d_2})+2\mathrm{tr}_3^{3^n}(x^{d_1})\mathrm{tr}_3^{3^n}(x^{d_2}) \\ &\quad +\mathrm{tr}_3^{3^n}(x)+2\mathrm{tr}_3^{3^n}(x^{d_1})+\mathrm{tr}_3^{3^n}(x^{d_2}). \end{aligned}$$

i) $n=2e+1$:

For $k=1$, the 3-rank is easily computed as 45. For $k \ge 2$, the square of the trace function can be expanded as

$$\begin{aligned} \left[\mathrm{tr}_3^{3^n}(x)\right]^2 &= \mathrm{tr}_3^{3^n}(x)\mathrm{tr}_3^{3^n}(x) \\ &= \sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &= \mathrm{tr}_3^{3^n}(x^{1+1})+\sum_{i=1}^{n-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &= \mathrm{tr}_3^{3^n}(x^{1+1})+2\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{1+3^i}). \end{aligned} \tag{16}$$

Similarly

$$\begin{aligned} \left[\mathrm{tr}_3^{3^n}(x^{d_1})\right]^2 &= \mathrm{tr}_3^{3^n}(x^{(1+1)d_1})+2\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\ \left[\mathrm{tr}_3^{3^n}(x^{d_2})\right]^2 &= \mathrm{tr}_3^{3^n}(x^{(1+1)d_2})+2\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}). \end{aligned} \tag{17}$$

Using (16) and (17), $c_1(x)$ can be rewritten as

$$\begin{aligned} c_1(x) &= 2\mathrm{tr}_3^{3^n}(x^2)+\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad +2\mathrm{tr}_3^{3^n}(x^{2d_1})+\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\ &\quad +2\mathrm{tr}_3^{3^n}(x^{2d_2})+\sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\ &\quad +2\sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i})+\sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\ &\quad +2\sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1})+\mathrm{tr}_3^{3^n}(x) \\ &\quad +2\mathrm{tr}_3^{3^n}(x^{d_1})+\mathrm{tr}_3^{3^n}(x^{d_2}). \end{aligned} \tag{18}$$

This can be reduced to

$$\begin{aligned} c_1(x) &= 2\mathrm{tr}_3^{3^n}(x^2)+\sum_{i=1,i\neq k,2k}^{e}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad +\sum_{i=1,i\neq k,2k}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1})+2\mathrm{tr}_3^{3^n}(x^{(1+3^{2k})d_1}) \\ &\quad +\sum_{i=1,i\neq k}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\ &\quad +2\sum_{i=0,i\neq k,3k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\ &\quad +\mathrm{tr}_3^{3^n}(x^{d_1+3^{3k}})+\mathrm{tr}_3^{3^n}(x^{d_1+3^{4k}}) \\ &\quad +\sum_{i=0,i\neq 2k,3k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\ &\quad +2\sum_{i=1,i\neq k,2k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1}) \\ &\quad +\mathrm{tr}_3^{3^n}(x)+2\mathrm{tr}_3^{3^n}(x^{d_1})+\mathrm{tr}_3^{3^n}(x^{d_2}) \end{aligned} \tag{19}$$

because

$$\begin{aligned} \mathrm{tr}_3^{3^n}(x^{2d_1}) &= \mathrm{tr}_3^{3^n}(x^{1+3^{2k}}) \\ \mathrm{tr}_3^{3^n}(x^{2d_2}) &= \mathrm{tr}_3^{3^n}(x^{1+3^k}) \\ \mathrm{tr}_3^{3^n}(x^{(1+3^k)d_1}) &= \mathrm{tr}_3^{3^n}(x^{d_2+3^kd_1}) \\ \mathrm{tr}_3^{3^n}(x^{(1+3^{2k})d_1}) &= \mathrm{tr}_3^{3^n}(x^{d_2+3^{2k}}) \\ \mathrm{tr}_3^{3^n}(x^{(1+3^k)d_2}) &= \mathrm{tr}_3^{3^n}(x^{d_1+3^k}) \\ \mathrm{tr}_3^{3^n}(x^{d_1+3^{3k}}) &= \mathrm{tr}_3^{3^n}(x^{d_2+d_1}) \\ \mathrm{tr}_3^{3^n}(x^{d_1+3^{4k}}) &= \mathrm{tr}_3^{3^n}(x^{d_2+3^{2k}d_1}) \\ \mathrm{tr}_3^{3^n}(x^{d_2+3^{3k}}) &= \mathrm{tr}_3^{3^n}(x^{d_2+3^{4k}d_1}). \end{aligned}$$

The preceding equivalences of trace functions can be checked by examining the p-adic expansions of exponents of x in trace functions. Now, we have to prove that all the exponents of x in (19) belong to different cosets of size n in F_{3^n}. It is easy to check that if a^2 and b^2 belong to different cosets of size n in F_{3^n}, so do a and b. In order to prove that all the exponents of x in (19) belong to different cyclotomic cosets in F_{3^n}, we had better examine two times all the exponents of x, which are given as

$$\begin{aligned} 2\cdot 2 &= 4 = 1+3 \\ 2(1+3^i), &\quad 1 \le i \le e,\ i \neq k,\ 2k \\ (1+3^i)(1+3^{2k}) &= 1+3^i+3^{2k}+3^{2k+i}, \\ &\quad 1 \le i \le e,\quad i \neq k,\ 2k \\ (1+3^{2k})(1+3^{2k}) &= 1+2\cdot 3^{2k}+3^{4k} \\ (1+3^i)(1+3^{4k}) &= 1+3^i+3^{4k}+3^{4k+i} \\ &\Rightarrow 1+3^k+3^i+3^{k+i}, \\ &\quad 1 \le i \le e,\ i \neq k \\ 1+3^{2k}+2\cdot 3^i, &\quad 0 \le i \le n-1,\ i \neq k,\ 3k,\ 4k \\ 1+3^{2k}+2\cdot 3^{3k} &\Rightarrow 1+2\cdot 3^k+3^{3k} \\ 1+3^{2k}+2\cdot 3^{4k} &\Rightarrow 2+3^k+3^{3k} \\ 1+3^{4k}+2\cdot 3^i, &\quad 0 \le i \le n-1,\ i \neq 2k,\ 3k \\ 1+3^i+3^{2k+i}+3^{4k} &\Rightarrow 1+3^k+3^{k+i}+3^{4k+i}, \\ &\quad 1 \le i \le n-1,\ i \neq k,\ 2k,\ 4k \end{aligned}$$

$$2,\quad 1+3^{2k},\quad 1+3^{4k}.$$

It is easy to check that all the exponents listed above belong to different cyclotomic cosets of size n in F_{3^n}. Then, so do all the exponents in (19), which proves the trace representation of the characteristic sequence of D_1. Thus, the 3-rank of D_1 is computed as

$$\begin{aligned}L_1 &= n + n\left(\frac{n-1}{2}-2\right) + n\left(\frac{n-1}{2}-2\right) + n \\ &\quad + n\left(\frac{n-1}{2}-1\right) + n(n-3) + 2n \\ &\quad + n(n-2) + n(n-4) + 3n \\ &= \frac{1}{2}(9n^2 - 17n).\end{aligned}$$

ii) $n = 2e$:

For even n, the squares of the trace functions can be expanded as

$$\begin{aligned}\left[\mathrm{tr}_3^{3^n}(x)\right]^2 &= \mathrm{tr}_3^{3^n}(x^{1+1}) + 2\sum_{i=1}^{e-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad + 2\mathrm{tr}_3^{3^e}(x^{1+3^e}) \\ \left[\mathrm{tr}_3^{3^n}(x^{d_1})\right]^2 &= \mathrm{tr}_3^{3^n}(x^{(1+1)d_1}) + 2\sum_{i=1}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\ &\quad + 2\mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) \\ \left[\mathrm{tr}_3^{3^n}(x^{d_2})\right]^2 &= \mathrm{tr}_3^{3^n}(x^{(1+1)d_2}) + 2\sum_{i=1}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\ &\quad + 2\mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}).\end{aligned}$$

Using the preceding expansion of trace functions, $c_1(x)$ is given as

$$\begin{aligned}c_1(x) &= 2\mathrm{tr}_3^{3^n}(x^2) + \sum_{i=1}^{e-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad + \mathrm{tr}_3^{3^e}(x^{1+3^e}) + 2\mathrm{tr}_3^{3^n}(x^{2d_1}) + \sum_{i=1}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) \\ &\quad + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) + 2\mathrm{tr}_3^{3^n}(x^{2d_2}) \\ &\quad + \sum_{i=1}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}) \\ &\quad + 2\sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i}) + \sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\ &\quad + 2\sum_{i=0}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1}) + \mathrm{tr}_3^{3^n}(x) \\ &\quad + 2\mathrm{tr}_3^{3^n}(x^{d_1}) + \mathrm{tr}_3^{3^n}(x^{d_2}).\end{aligned}$$

Similarly to the previous case, it can be reduced to

$$\begin{aligned}c_1(x) &= 2\mathrm{tr}_3^{3^n}(x^2) + \sum_{i=1,i\neq k,2k}^{e-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad + \sum_{i=1,i\neq k,2k}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) + 2\mathrm{tr}_3^{3^n}(x^{(1+3^{2k})d_1}) \\ &\quad + \sum_{i=1,i\neq k}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\ &\quad + 2\sum_{i=0,i\neq k,3k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\ &\quad + \mathrm{tr}_3^{3^n}(x^{d_1+3^{3k}}) + \mathrm{tr}_3^{3^n}(x^{d_1+3^{4k}}) \\ &\quad + \sum_{i=0,i\neq 2k,3k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) \\ &\quad + 2\sum_{i=1,i\neq k,2k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1}) \\ &\quad + \mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^{d_1}) + \mathrm{tr}_3^{3^n}(x^{d_2}) + \mathrm{tr}_3^{3^e}(x^{1+3^e}) \\ &\quad + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}). \qquad (20)\end{aligned}$$

Therefore, the 3-rank of D_1 is computed as

$$\begin{aligned}L_1 &= n + n(e-3) + n(e-3) + n + n(e-2) + n(n-3) \\ &\quad + 2n + n(n-2) + n(n-4) + 3n + 3e \\ &= \frac{1}{2}(9n^2 - 17n).\end{aligned}$$

Case 2) 3-rank of D_2:

For $k = 1$, the rank can be easily computed as 40. Similarly to Case 1), for odd $n = 2e+1$, the reduced form of the trace representation of characteristic sequence can be derived as

$$\begin{aligned}c_2(x) &= 2\mathrm{tr}_3^{3^n}(x^2) + \sum_{i=1,i\neq k,2k}^{e}\mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ &\quad + \sum_{i=1,i\neq k,2k}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) + \sum_{i=1,i\neq k}^{e}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) \\ &\quad + 2\mathrm{tr}_3^{3^n}(x^{(1+3^k)d_2}) + \sum_{i=0,i\neq k,3k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\ &\quad \times 2\sum_{i=0,i\neq 2k,3k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) + \mathrm{tr}_3^{3^n}(x^{d_2+3^{3k}}) \\ &\quad + 2\sum_{i=1,i\neq k,2k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1}) + \mathrm{tr}_3^{3^n}(x) \\ &\quad + \mathrm{tr}_3^{3^n}(x^{d_1}) + 2\mathrm{tr}_3^{3^n}(x^{d_2}) \qquad (21)\end{aligned}$$

and for even $n = 2e$

$$\begin{aligned}c_2(x) &= 2\mathrm{tr}_3^{3^n}(x^2) + \sum_{i=1,i\neq k,2k}^{e-1}\mathrm{tr}_3^{3^n}(x^{1+3^i}) + \mathrm{tr}_3^{3^e}(x^{1+3^e}) \\ &\quad + \sum_{i=1,i\neq k,2k}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_1}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_1}) \\ &\quad + \sum_{i=1,i\neq k}^{e-1}\mathrm{tr}_3^{3^n}(x^{(1+3^i)d_2}) + \mathrm{tr}_3^{3^e}(x^{(1+3^e)d_2}) \\ &\quad + 2\mathrm{tr}_3^{3^n}(x^{(1+3^k)d_2}) + \sum_{i=0,i\neq k,3k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_1+3^i}) \\ &\quad + 2\sum_{i=0,i\neq 2k,3k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^i}) + \mathrm{tr}_3^{3^n}(x^{d_2+3^{3k}}) \\ &\quad + 2\sum_{i=1,i\neq k,2k,4k}^{n-1}\mathrm{tr}_3^{3^n}(x^{d_2+3^id_1}) + \mathrm{tr}_3^{3^n}(x) \\ &\quad + \mathrm{tr}_3^{3^n}(x^{d_1}) + 2\mathrm{tr}_3^{3^n}(x^{d_2}). \qquad (22)\end{aligned}$$

Thus, we have

$$L_2 = \begin{cases} 40, & \text{for } k = 1 \\ \frac{1}{2}(9n^2 - 19n), & \text{for } k \geq 2. \end{cases}$$

□

APPENDIX IV
PROOF OF THEOREM 12

For $n = 3$, it is easy to compute the 3-rank of D. For $n \geq 5$, the characteristic sequence of D is

$$c(x) = 1 - \left[\mathrm{tr}_3^{3^n}(x) + \mathrm{tr}_3^{3^n}(x^d) - 1\right]^2. \tag{23}$$

$c(x)$ can be rewritten as

$$c(x) = 2\left[\mathrm{tr}_3^{3^n}(x)\right]^2 + 2\left[\mathrm{tr}_3^{3^n}(x^d)\right]^2 + \mathrm{tr}_3^{3^n}(x)\mathrm{tr}_3^{3^n}(x^d) + 2\mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^d).$$

Expanding the squares of the trace functions, it can be rewritten as

$$\begin{aligned} c(x) = {} & 2\mathrm{tr}_3^{3^n}(x^{1+1}) + \sum_{i=1}^{m} \mathrm{tr}_3^{3^n}(x^{1+3^i}) \\ & + 2\mathrm{tr}_3^{3^n}(x^{(1+1)d}) + \sum_{i=1}^{m} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d}) \\ & + \sum_{i=0}^{n-1} \mathrm{tr}_3^{3^n}(x^{d+3^i}) + 2\mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^d). \end{aligned} \tag{24}$$

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

$$\mathrm{tr}_3^{3^n}(x^{d+3^m}) = \mathrm{tr}_3^{3^n}(x^{1+3^m})$$

and

$$\begin{aligned} \mathrm{tr}_3^{3^n}(x^{d+3^{n-1}}) &= \mathrm{tr}_3^{3^n}(x^{2\cdot 3^{m+1}+3+1}) = \mathrm{tr}_3^{3^n}(x^{2(3^{m+1}+2)}) \\ &= \mathrm{tr}_3^{3^n}(x^{2(1+2\cdot 3^m)}) = \mathrm{tr}_3^{3^n}(x^{(1+1)d}). \end{aligned}$$

Then (24) can be reduced to

$$\begin{aligned} c(x) = {} & 2\mathrm{tr}_3^{3^n}(x^{1+1}) + \sum_{i=1}^{m-1} \mathrm{tr}_3^{3^n}(x^{1+3^i}) + 2\mathrm{tr}_3^{3^n}(x^{1+3^m}) \\ & + \sum_{i=1}^{m} \mathrm{tr}_3^{3^n}(x^{(1+3^i)d}) + \sum_{i=0, i\neq m}^{n-2} \mathrm{tr}_3^{3^n}(x^{d+3^i}) \\ & + 2\mathrm{tr}_3^{3^n}(x) + 2\mathrm{tr}_3^{3^n}(x^d). \end{aligned} \tag{25}$$

For $n \geq 5$, all the exponents of x in (25) belong to different cosets of size n in F_{3^n}. Thus, the trace representation of the characteristic sequences of D is proved. And the 3-rank of the relative difference set D is computed as

$$n + (m-1)n + n + mn + (n-2)n + 2n = 2n^2. \qquad \square$$

REFERENCES

[1] L. D. Baumert, *Cyclic Difference Sets (Lecture Notes in Mathematics)*. Berlin/Heidelberg/New York: Springer-Verlag, 1971, vol. 182.

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1999, vol. 1.

[3] A. T. Butson, "Relations among generalized Hadamard matrices, relative difference sets and maximal length linear recurring sequences," *Canad. J. Math.*, vol. 15, pp. 42–48, 1963.

[4] D. Chandler and Q. Xiang, "Cyclic relative difference sets and their p-ranks," *Des., Codes, Cryptogr.*, vol. 30, pp. 325–343, Nov. 2003.

[5] F. R. K. Chung, J. A. Salehi, and V. K. Wei, "Optical orthogonal codes: Design, analysis, and applications," *IEEE Trans. Inf. Theory*, vol. 35, no. 3, pp. 595–604, May 1989.

[6] J. F. Dillon and H. Dobbertin, "Cyclic difference sets with singer parameters," preprint, 1999.

[7] J. E. H. Elliott and A. T. Butson, "Relative difference sets," *Illinois J. Math.*, vol. 10, pp. 517–531, 1966.

[8] R. Evans, H. Hollmann, C. Krattenthaler, and Q. Xiang, "Gauss sums, Jacobi sums and p-ranks of cyclic difference sets," *J. Combin. Theory (A)*, vol. 87, pp. 74–119, 2000.

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

[10] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2868–2872, Nov. 2002.

[11] T. Helleseth, P. V. Kumar, and H. M. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation," *Des., Codes, Cryptogr.*, vol. 23, pp. 157–166, 2001.

[12] D. Jungnickel, "Difference sets," in *Contemporary Design Theory: A Collection of Surveys*, J. Dinitz and D. Stinson, Eds. New York: Wile, 1992, pp. 241–324.

[13] D. Jungnickel and A. Pott, "Difference sets: An introduction," in *Difference Sets, Sequences and their Correlation Properties*, A. Pott, P. Kumar, T. Helleseth, and D. Jungnickel, Eds. Amsterdam, The Netherlands: Kulwer, 1999, pp. 259–295.

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

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

[16] H. A. Lin, "From cyclic Hadamard cyclic difference sets to perfectly balanced sequences," Ph.D. dissertation, USC, Los Angeles, CA, 1988.

[17] J. S. No, "p-ary unified sequences: p-ary extended d-form sequences with ideal autocorrelation property," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2540–2546, Sep. 2002.

[18] ——, "New cyclic difference sets with Singer parameters constructed from d-homogeneous function," *Des., Codes, Cryptogr.*, vol. 33, pp. 199–213, Nov. 2004.

[19] J. S. No, D. J. Shin, and T. Helleseth, "On the p-ranks and characteristic polynomials of cyclic difference sets," *Des., Codes, Cryptogr.*, vol. 33, pp. 23–37, Aug. 2004.

[20] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.

[21] E. Spence, "Hadamard matrices from relative difference sets," *J. Combin. Theory 19*, pp. 287–300, 1975.

[22] M. Yamada, "On a relation between a cyclic relative difference sets associated with the quadratic extensions of a finite field and the szekeres difference sets," *Combinatorica 8*, pp. 207–216, 1988.

Unimodular Perfect Sequences of Length p^s

Ernst M. Gabidulin and Vitaly V. Shorin

***Abstract*—A new class of unimodular perfect sequences of length p^s, where p is a prime, is proposed. An explicit secondary construction is provided. This construction includes most of the previously known unimodular perfect sequences of length p^s as special cases. Also the proposed construction is extended to sequences with autocorrelation over $\mathbb{Z}_{p^k}^s$, $V_{m_2} \times \mathbb{Z}_{p^{m_1}}$, V_k.**

***Index Terms*—Correlation, generalized bent, generalized unimodular perfect sequence, phase-shift keyed (PSK), unimodular perfect sequence.**

I. INTRODUCTION

Perfect sequences with unit magnitude have been extensively studied since the middle of the twentieth century. They have been

Manuscript received May 5, 2003; revised September 2, 2004.

E. M. Gabidulin is with the Moscow Institute of Physics and Technology (State University), 141700 Dolgoprudny, Moscow Region, Russia (e-mail: gab@pop3.mipt.ru).

V. V. Shorin is with École Nationale Supérieure de Techniques Avancées, 75739 Paris Cedex 15, France (e-mail: shorin@dgap.mipt.ru).

Communicated by K. G. Paterson, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2004.842720