Journal of Combinatorial Theory, Series A **94**, 118–126 (2001)
doi:10.1006/jcta.2000.3137, available online at http://www.idealibrary.com on IDEAL®

Cyclic Relative Difference Sets with Classical Parameters

K. T. Arasu[1]

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435
E-mail: karasu@math.wright.edu

J. F. Dillon

National Security Agency, Fort George G. Meade, Maryland 20755
E-mail: jfdillon@afterlife.ncsc.mil

and

Ka Hin Leung and Siu Lun Ma[2]

Department of Mathematics, National University of Singapore, Kent Ridge,
Singapore 119260, Republic of Singapore
E-mail: matlkh@nus.edu.sg, matmasl@nus.edu.sg

Communicated by William M. Kantor

Received June 16, 2000

We investigate the existence of cyclic relative difference sets with parameters $((q^d-1)/(q-1), n, q^{d-1}, q^{d-2}(q-1)/n)$, q any prime power. One can think of these as "liftings" or "extensions" of the complements of Singer difference sets. When q is odd or d is even, we find that relative difference sets with these parameters exist if and only if n is a divisor of $q-1$. In case q is even and d is odd, relative difference sets with these parameters exist if and only if n is a divisor of $2(q-1)$. © 2001 Academic Press

1. INTRODUCTION

Let G be a finite group of order mn and N a normal subgroup of G of order n. A k-element subset D of G is called an (m, n, k, λ)-*relative difference set* in G relative to N if every element in $G\backslash N$ has exactly λ representations $r_1 r_2^{-1}$ (or $r_1 - r_2$ if G is additive) with $r_1, r_2 \in D$ and no

[1] The work was partially supported by NSA Grant MDA 904-97-1-0012, by AFOSR Grant F49620-96-1-0328, and by NSF Grant CCR-9814106.

[2] The work was partially done when the author visited Wright State University.

0097-3165/01 $35.00

non-identity element in N has such a representation. When $n=1$, D is an (m, k, λ)-*difference set* in the usual sense. A difference set or relative difference set is called *cyclic* if the group is cyclic. We refer the reader to [7, 9] for the background on both difference sets and relative difference sets. The following is a well-known result in the study of relative difference sets.

Proposition 1.1 (Elliott and Butson [5]). *Let D be an (m, n, k, λ)-relative difference set in G relative to N. If U is a normal subgroup of G of order u contained in N and if $\rho\colon G \to G/U$ is the natural epimorphism, then $\rho(D)$ is an $(m, n/u, k, \lambda u)$-relative difference set in G/U relative to N/U. In particular, if $U=N$, then $\rho(D)$ is an $(m, k, \lambda n)$-difference set in G/N.*

In view of Proposition 1.1, we may think of relative difference sets as "liftings" or "extensions" of difference sets. Among difference sets which can be lifted, the complements of Singer difference sets have attracted most of the attention because of their relationship with finite projective geometry. The parameters of the relative difference sets lifted from them are of the form

$$(m, n, k, \lambda)=\left(\frac{q^d-1}{q-1}, n, q^{d-1}, \frac{q^{d-2}(q-1)}{n}\right), \tag{1}$$

where q is a prime power. These parameters are called the *classical* parameters in [9]. There are some known results on cyclic relative difference sets with these parameters:

Result 1. Let G be the multiplicative group of $\mathbb{F}_{q^d}$. If we regard $\mathbb{F}_{q^d}$ as a linear space over $\mathbb{F}_q$, then an affine hyperplane in $\mathbb{F}_{q^d}$ not through the origin forms a cyclic $((q^d-1)/(q-1), q-1, q^{d-1}, q^{d-2})$-relative difference set in G. For more details please consult [4, 5]. By Proposition 1.1, we can then construct cyclic $((q^d-1)/(q-1), n, q^{d-1}, q^{d-2}(q-1)/n)$-relative difference sets for all divisors n of $q-1$. Indeed, this family is one of the earliest known families of relative difference sets; the difference sets corresponding to $n=1$ and their complements are called Singer difference sets [10].

Result 2. In [1], Arasu *et al.* gave a construction of cyclic $((q^d-1)/(q-1), 2, q^{d-1}, q^{d-2}(q-1)/2)$-relative difference sets for odd d. When q is even, the parameters of the relative difference sets constructed are new. In the same paper, they also proved that if q and d are both even, then no cyclic $((q^d-1)/(q-1), 2, q^{d-1}, q^{d-2}(q-1)/2)$-relative difference set exists. By Result 1, we deduce that when both q and d are even, cyclic relative difference sets with parameters (1) exist if and only if n is a divisor of $q-1$.

Result 3. By a computer search, Lam [8] found a (21, 6, 16, 2)-relative difference set in a cyclic group of order 126. Note that $q=4$, $d=3$ and $n=2(q-1)$.

In view of the constructions above, Pott [9] asked if there exists an (m, n, k, λ)-relative difference set whose projection is a difference set with parameters $((q^d-1)/(q-1), q^{d-1}, q^{d-2}(q-1))$, where $n \neq 2$ and n is not a divisor of $q-1$ (see [9, Problem 7, p. 48]). In this paper, we give a complete answer to his question for the case of cyclic relative difference sets. In fact, we shall prove the following:

THEOREM 1.2. *Let q be a prime power. A cyclic relative difference set with parameters* (1) *exists if and only if n is a divisor of $q-1$ when q is odd or d is even*; *and n is a divisor of* $2(q-1)$ *when q is even and d is odd.*

2. NONEXISTENCE RESULTS

In this section, we will prove two nonexistence results on relative difference sets. Using those results on cyclic relative difference sets with parameters (1), we deduce that n must be a divisor of $q-1$ if q is odd; and n must be a divisor of $2(q-1)$ if q is even. Together with Results 1 and 2 mentioned earlier, we easily deduce Theorem 1.2 in case q is odd or d is even.

To facilitate the study of relative difference sets, we often represent a relative difference set by an element in the group ring $\mathbb{Z}G$. A subset D of G is an (m, n, k, λ)-relative difference set relative to N if and only if

$$DD^{(-1)} = k + \lambda(G-N).$$

Here, for any subset A of G, we denote the element $\sum_{g \in A} g$ in $\mathbb{Z}G$ by A, and the set $\{g^{-1} \mid g \in A\}$ by $A^{(-1)}$. When G is abelian, one often uses character values to characterize a relative difference set D. In fact, a k-element subset D of an abelian group G is an (m, n, k, λ)-relative difference set relative to N if and only if for every nonprincipal character χ of G,

$$\chi(D)\,\overline{\chi(D)} = \begin{cases} k & \text{if } \chi \text{ is nonprincipal on } N \\ k-\lambda n & \text{if } \chi \text{ is principal on } N. \end{cases}$$

Readers are referred to [9] for a more detailed discussion of this approach.

In the following, we denote the complex wth root of unity $e^{2\pi i/w}$ by ζ_w. For $y=\sum_{g \in G} a_g g \in \mathbb{C}G$ where $a_g \in \mathbb{C}$, we define $y^{(t)} = \sum_{g \in G} a_g g^t$. First, we recall a lemma from [3, Lemma 1]. Note that we have modified the lemma in [3] slightly by changing ζ_v to ζ_{uw}. The proof of our lemma is exactly the same as in [3].

LEMMA 2.1. *Let $G = \langle \alpha \rangle \times H$ be an abelian group of exponent $v = uw$ where $u = o(\alpha)$, $w = \exp(H)$ and $\text{g.c.d.}(u, w) = 1$. Suppose $y \in \mathbb{Z}G$, n is an integer relatively prime to w and $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{uw})/\mathbb{Q})$ such that for every character χ of G satisfying $\chi(\alpha) = \zeta_u$,*

(i) *$\chi(y)\,\overline{\chi(y)} = n$; and*

(ii) *σ fixes every prime ideal divisor of $\chi(y)\,\mathbb{Z}[\zeta_{uw}]$.*

If $\sigma(\zeta_{uw}) = \zeta_{uw}^t$ for some integer t, then

$$y^{(t)} = \pm \beta y + \sum_{i=1}^{r} \langle \alpha^{u/p_i} \rangle x_i, \tag{2}$$

where $\beta \in G$, $x_1, x_2, ..., x_r \in \mathbb{Z}G$ and $p_1, p_2, ..., p_r$ are all prime divisors of u. Furthermore, if u is even, then the sign in (2) can be chosen to be positive.

THEOREM 2.2. *Suppose G is an abelian group of order $4w$, where w is odd and $w > 1$, such that the Sylow 2-subgroup of G is cyclic. Then there are no $(2w, 2, 2^s, \lambda)$ or $(w, 4, 2^s, \lambda)$-relative difference sets in G.*

Proof. Assume there exists a relative difference set D in G with one of the given parameter sets. Let t be an integer with $t \equiv -1 \bmod 4$ and $t \equiv 1 \bmod w^*$ where $w^* = \exp(G)/4$. Let σ be the automorphism that maps ζ_{4w^*} to $\zeta_{4w^*}^t$. As σ fixes every prime ideal divisor of $2\mathbb{Z}[\zeta_{4w^*}]$ (see [9, Result 1.2.7]), we conclude from Lemma 2.1 that there exist $x \in \mathbb{Z}G$ and $\alpha, \beta \in G$ such that $o(\alpha) = 2$ and

$$D^{(t)} = \beta D + \langle \alpha \rangle\, x.$$

Let $\rho: G \to G/\langle \alpha \rangle$ be the natural epimorphism. Then $\rho(D) = \rho(D^{(t)}) = \rho(\beta)\,\rho(D) + 2\rho(x)$ and hence

$$\rho(D)[1 - \rho(\beta)] = 2\rho(x).$$

Since $|D \cap \langle \alpha \rangle\, \gamma| \leqslant 1$ for all $\gamma \in G$, the coefficients of $\rho(D)$ are 0 and 1. So we can only have $\rho(x) = 0$. As $\chi(\rho(D)) \neq 0$ for all characters χ of $G/\langle \alpha \rangle$, we have $\chi(\rho(\beta)) = 1$ for all characters χ of $G/\langle \alpha \rangle$, i.e. $\rho(\beta) = 1$. Thus $D^{(t)} = D$ or αD. But $|D \cap \langle \alpha \rangle\, \gamma| \leqslant 1$ for all $\gamma \in G$ also. This forces D to be a subset of H or aH where H is the subgroup of order $2w$ in G and a is an element of order 4 in G. This is a contradiction. ▮

THEOREM 2.3. *Let p be an odd prime and let $w > 1$ be an integer relatively prime to p. Then there is no (w, p, p^s, λ)-relative difference set in any abelian group of order wp.*

Proof. Assume there exists a (w, p, p^s, λ)-relative difference set D in an abelian group G of order wp. Let t be an integer such that $t \equiv -1 \bmod p$ and $t \equiv 1 \bmod w^*$ where $w^* = \exp(G)/p$. Let σ be the automorphism that maps ζ_{pw^*} to $\zeta_{pw^*}^t$. Again, σ fixes every prime ideal divisor of $p\mathbb{Z}[\zeta_{pw^*}]$ (see [9, Result 1.2.7]). As before, we conclude from Lemma 2.1 that we have

$$D^{(t)} = \pm \beta D + \langle \alpha \rangle x,$$

where $x \in \mathbb{Z}G$ and $\alpha, \beta \in G$ such that $o(\alpha) = p$. Let $\rho: G \to G/\langle \alpha \rangle$ be the natural epimorphism. Then $\rho(D)[1 \mp \rho(\beta)] = p\rho(x)$. By arguments similar to the proof of Theorem 2.2, we obtain $D^{(t)} = \alpha^i D$, for some integer i, and this forces D to be contained in the subgroup of G of index p, a contradiction. ▮

By Theorems 2.2 and 2.3 and Results 1 and 2 of Section 1, we have the following corollary.

COROLLARY 2.4. *Let q be a prime power.*

(a) *When q is odd or d is even, cyclic relative difference sets with parameters* (1) *exist if and only if n is a divisor of $q-1$.*

(b) *When q is even and d is odd, no cyclic relative difference set with parameters* (1) *exists if n is not a divisor of* $2(q-1)$.

3. A CONSTRUCTION

In this section, we will complete the proof of Theorem 1.2. In view of Corollary 2.4, we need only consider the case when q is even and d is odd. By Proposition 1, it suffices to construct a cyclic $((q^d-1)/(q-1), 2(q-1), q^{d-1}, q^{d-2}/2)$-relative difference set. In particular, when $q=4$ and $d=3$ our construction yields a cyclic (21, 6, 16, 2)-relative difference set as found by Lam. Our strategy is to combine the affine hyperplane construction of $((q^d-1)/(q-1), q-1, q^{d-1}, q^{d-2})$-relative difference sets and the construction of $((q^d-1)/(q-1), 2, q^{d-1}, q^{d-2}(q-1)/2)$-relative difference sets in [1]. Our construction can be regarded as the affine analogue of the construction in [1]. Our proof, like the one in [1], exploits an $\mathbb{F}_2$-quadratic form; but instead of a geometric argument we give here a very simple algebraic argument based on the Hadamard transform.

In [1] the authors define a *Waterloo decomposition* of a (v, k, λ)-difference set D in the group G to be a partition $D = A + B$ with the property that $E = A - B$ satisfies $EE^{(-1)} = k$ in the group ring $\mathbb{Z}G$; and they showed that such a decomposition is equivalent to a $(v, 2, k, \lambda/2)$-relative difference set $R = A + B\theta$ in the group $\mathcal{G} = G \times \langle \theta \rangle$ relative to the subgroup $\langle \theta \rangle$, where θ has order 2. By way of the regular representation of G such an element E corresponds to a G-developed weighing matrix, which, when G is cyclic, is a circulant weighing matrix, denoted $CW(|G|, k)$. The reader is invited to see [2] for a recent survey of these and more general *perfect ternary arrays*. The notion of Waterloo decomposition has the following natural extension to relative difference sets.

THEOREM 3.1. *The following are equivalent*:

(I) *An* (m, n, k, λ)*-relative difference set* R *in* G *with respect to* N *with a "Waterloo decomposition"* $R = A + B$ *for which* $E = A - B$ *satisfies* $EE^{(-1)} = k$ *in the group ring* $\mathbb{Z}G$;

(II) *An* $(m, 2n, k, \lambda/2)$*-relative difference set* $\mathcal{R} = A + B\theta$ *in* $\mathcal{G} = G \times \langle \theta \rangle$ *relative to* $\mathcal{N} = N \times \langle \theta \rangle$, *where* θ *has order* 2.

Proof. The relative difference set $\mathcal{R}$ in (II) is equivalent to the equation in the group ring $\mathbb{Z}\mathcal{G}$

$$k + \frac{\lambda}{2}(\mathcal{G} - \mathcal{N}) = \mathcal{R}\mathcal{R}^{(-1)} = (A + B\theta)(A + B\theta)^{(-1)}$$

$$= (AA^{(-1)} + BB^{(-1)}) + (AB^{(-1)} + BA^{(-1)})\,\theta$$

which is equivalent to the pair of equations in $\mathbb{Z}G$:

(i) $k + \frac{\lambda}{2}(G - N) = AA^{(-1)} + BB^{(-1)}$;

(ii) $\frac{\lambda}{2}(G - N) = AB^{(-1)} + BA^{(-1)}$.

Adding and subtracting these equations gives the equivalent pair

(i') $k + \lambda(G - N) = (A + B)(A + B)^{(-1)}$;

(ii') $k = (A - B)(A - B)^{(-1)}$.

Since θ is in the forbidden subgroup $\mathcal{N} = N \times \langle \theta \rangle$, A and B are disjoint. Thus $A + B$ has coefficients in $\{0, 1\}$ so corresponds to a subset of G; the last pair of equations is now seen to be equivalent to (I). ▮

In light of this result and Result 1 of Section 1 it suffices to exhibit a Waterloo decomposition of the classical affine difference set

$$T_1 = \{x \in \mathbb{F}_{q^d} : \mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_q}(x) = 1\}.$$

We shall prove the

THEOREM 3.2. T_1 *has the Waterloo decomposition* $T_1 = A + B$, *where* $\{A, B\} = \{C_0, C_1\}$ *and*

$$C_\varepsilon = \{1 + \gamma^q + \gamma^{q^{-1}} : \mathrm{Tr}_{\mathbb{F}_{q^d}/\mathbb{F}_2}(\gamma^{q+1} + \gamma) = \varepsilon\}.$$

Proof. The following notation shall be used in the sequel. q is a power of 2, $F=\mathbb{F}_q$ and $K=\mathbb{F}_{q^d}$, where d is odd. Note that in this case $1=(q+1, q-1)=(q+1, q^d-1)$. For convenience we shall also denote the trace function $\mathrm{Tr}_{K/\mathbb{F}_2}$ more simply by Tr. We define $Q: K\to\mathbb{F}_2$ by $Q(x)=\mathrm{Tr}(x^{q+1})$ for all $x\in K$ and we let $\mathcal{Q}$ denote the real-valued function $(-1)^Q$. Then for all $\alpha\in K$ we have

$$\begin{aligned} q^d\delta_{1,\alpha} &= \sum_{x\in K}(-1)^{\mathrm{Tr}([\alpha^{q+1}+1]\,x)} \\ &= \sum_{x\in K}(-1)^{Q(\alpha x)+Q(x)} \\ &= \sum_{x\in K}\mathcal{Q}(\alpha x)\,\mathcal{Q}(x) \\ &= \sum_{x\in K}\hat{\mathcal{Q}}(\alpha x)\,\hat{\mathcal{Q}}(x), \end{aligned}$$

where, for *any* real-valued function $\mathbf{F}$ on K, $\mathbf{F}\mapsto\hat{\mathbf{F}}$ denotes the orthogonal Fourier (Hadamard) transform given by

$$\hat{\mathbf{F}}(\beta)=q^{-d/2}\sum_{x\in K}\mathbf{F}(x)(-1)^{\mathrm{Tr}(\beta x)} \qquad \forall\beta\in K,$$

and the last equality above follows from Parseval's theorem. Now $\hat{\mathcal{Q}}(0)=0$; and for all $\beta\in K$, $\beta\neq 0$, we have

$$(\hat{\mathcal{Q}}(\beta))^2=q^{-d}\sum_{x\in K}(-1)^{\mathrm{Tr}(x^{q+1}+\beta x)}\sum_{y\in K}(-1)^{\mathrm{Tr}(y^{q+1}+\beta y)},$$

which, on replacement of y by $x+y$ and reversal of the order of summation, becomes

$$\begin{aligned} (\hat{\mathcal{Q}}(\beta))^2 &= q^{-d}\sum_{y\in K}(-1)^{\mathrm{Tr}(y^{q+1}+\beta y)}\sum_{x\in K}(-1)^{\mathrm{Tr}(x^q y+xy^q)} \\ &= q^{-d}\sum_{y\in K}(-1)^{\mathrm{Tr}(y^{q+1}+\beta y)}\sum_{x\in K}(-1)^{\mathrm{Tr}([y^{q^2}+y]\,x^q)}. \end{aligned}$$

The inner sum is 0 unless $y\in\mathbb{F}_{q^2}$ in which case it is q^d. But, since d is odd, $y\in K\cap\mathbb{F}_{q^2}$ iff $y\in\mathbb{F}_q$; and, for any such y, $\mathrm{Tr}(y^{q+1}+\beta y) = \mathrm{Tr}([1+\beta]\,y)$. Thus,

$$(\hat{\mathcal{Q}}(\beta))^2=\sum_{y\in F}(-1)^{\mathrm{Tr}([1+\beta]\,y)}.$$

But for $y \in F$ we have

$$\begin{aligned}\mathrm{Tr}([1+\beta]\, y) &= \mathrm{Tr}_{F/\mathbb{F}_2}(\mathrm{Tr}_{K/F}([1+\beta]\, y)) \\ &= \mathrm{Tr}_{F/\mathbb{F}_2}([\mathrm{Tr}_{K/F}(1+\beta)]\, y) \\ &= \mathrm{Tr}_{F/\mathbb{F}_2}([1+\mathrm{Tr}_{K/F}(\beta)]\, y),\end{aligned}$$

the last equation a consequence of $d = [K: F]$ being odd. Therefore

$$\begin{aligned}(\hat{\mathscr{Q}}(\beta))^2 &= \sum_{y \in F} (-1)^{\mathrm{Tr}_{F/\mathbb{F}2}([1+\mathrm{Tr}_{K/F}(\beta)]\, y)} \\ &= q\delta_{1,\, \mathrm{Tr}_{K/F}(\beta)}.\end{aligned}$$

Thus, the $\{-1, 0, 1\}$-valued function $E = q^{-1/2}\hat{\mathscr{Q}}$ on K has support T_1 and satisfies the equation

$$q^{d-1}\delta_{1,\alpha} = \sum_{x \in K} E(\alpha x)\, E(x) \qquad \forall \alpha \in K,$$

and, since $E(0) = 0$, the equivalent equation

$$q^{d-1}\delta_{1,\alpha} = \sum_{x \in K^\times} E(\alpha x)\, E(x) \qquad \forall \alpha \in K^\times.$$

But this last equation is equivalent to the equation $EE^{(-1)} = q^{d-1}$ in the group ring $\mathbb{Z}K^\times$ so that E defines the desired Waterloo decomposition of T_1. Since d is odd 1 belongs to T_1; and, by the additive Hilbert's Satz 90, we have that

$$T_1 = \{1 + \gamma^{q^2} + \gamma : \gamma \in K\} = \{1 + \gamma^q + \gamma^{q^{-1}} : \gamma \in K\}.$$

Since $\hat{\mathscr{Q}}(1 + \gamma^q + \gamma^{q^{-1}}) = (-1)^{\mathrm{Tr}(\gamma^{q+1} + \gamma)}\, \hat{\mathscr{Q}}(1)$, it follows that the pieces A and B in the Waterloo decomposition of T_1 are given by

$$\{A, B\} = \{C_0, C_1\}, \qquad \text{where } C_\varepsilon = \{1 + \gamma^q + \gamma^{q^{-1}} : \mathrm{Tr}(\gamma^{q+1} + \gamma) = \varepsilon\}. \quad \blacksquare$$

This also completes the proof of Theorem 1.2.

REFERENCES

1. K. T. Arasu, J. F. Dillon, D. Jungnickel, and A. Pott, The solution of the Waterloo problem, *J. Combin. Theory Ser. A* **71** (1995), 316–331.
2. K. T. Arasu and J. F. Dillon, Perfect Ternary arrays, *in* "Difference Sets, Sequences and their Correlation Properties" (A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnicel, Eds.), NATO Sciences Series C, Vol. 542, Kluwer Academic, Dordrecht, 1999.

3. K. T. Arasu and S. L. Ma, Abelian difference sets without self-conjugacy, *Des. Codes Cryptogr.* **15** (1998), 223–230.
4. R. C. Bose, An affine analogue of Singer's theorem, *J. Indian Math. Soc.* **6** (1942), 1–15.
5. J. E. H. Elliott and A. T. Butson, Relative difference sets, *Illinois J. Math.* **10** (1966), 517–531.
6. K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," Springer-Verlag, New York/Heidelberg/Berlin, 1982.
7. D. Jungnickel, Difference sets, *in* "Contemporary Design Theory: A Collection of Surveys" (J. H. Dinitz and D. R. Stinson, Eds.), pp. 241–324, Wiley, New York, 1992.
8. C. W. H. Lam, On relative difference sets, *in* "Proc. 7th Manitoba Conference on Numerical Mathematics and Computing, 1977," pp. 445–474.
9. A. Pott, "Finite Geometry and Character Theory," Lecture Notes in Mathematics, Vol. 1601, Springer-Verlag, Berlin/Heidelberg/New York, 1995.
10. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.