Constructions of Relative Difference Sets with Classical Parameters and Circulant Weighing Matrices

Ka Hin Leung
Department of Mathematics
National University of Singapore
2 Science Drive 2, Singapore 117543
Republic of Singapore
E-mail: *matlkh@nus.edu.sg*

Siu Lun Ma
Department of Mathematics
National University of Singapore
2 Science Drive 2, Singapore 117543
Republic of Singapore
E-mail: *matmasl@nus.edu.sg*

Bernhard Schmidt
Mathematisches Institut
Universitắt Augsburg
Unversitắtsstraße 15, 86135 Augsburg
Germany
E-mail: *bernhard.schmidt@math.uni-augsburg.de*

September 7, 2004

The first two authors was supported by NUS research grant R-146-000-015-112. Also, the research was done when the third author visited the National University of Singapore.

Abstract

In this paper, a new family of relative difference sets with parameters $(m, n, k, \lambda) = ((q^7 - 1)/(q - 1), 4(q - 1), q^6, q^5/4)$ is constructed where q is a 2-power. The construction is based on the technique used in [2]. By a similar method, we also construct some new circulant weighing matrices of order q^{d-1} where q is a 2-power, d is odd and $d \geq 5$.

Correspondence: S.L. Ma
Department of Mathematics
National University of Singapore
2 Science Drive 2, Singapore 117543
Republic of Singapore
E-mail: *matmasl@nus.edu.sg*

Running Head: Relative difference sets with classical parameters

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 $r_1r_2^{-1}$ (or $r_1 - r_2$ if G is additive) with $r_1, r_2 \in D$ and no 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 [3], [7] and [10] for the background of both difference sets and relative difference sets. The following is a well-known result in the studies 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 $\rho : G \to G/U$ 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, 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. In [10], the parameters (1) is called the *classical* parameters.

Pott [10, Problem 7 (p.48)] asked if there exists a relative (m,n,k,λ)-difference set such that its projection is the complement of a Singer difference sets, $n \neq 2$ and n is not a divisor of $q-1$. In [2], the cyclic case was studied. In fact, a new construction of cyclic relative difference sets with classical parameters was found where q is a 2-power, d is odd and $n = 2(q-1)$. This helps us to answer Pott's question when the group is cyclic.

Theorem 1.2 (Arasu, Dillon, Leung and Ma [2]) *Let q be a prime power. A cyclic relative difference sets 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.*

In this paper, we investigate further 'lifting' of the relative difference sets constructed in [2]. We show that under some conditions, n can go up to $4(q-1)$. More specifically, we construct a family of relative difference sets with classical parmeters when q is a 2-power, $d = 7$ and $n = 4(q-1)$. Obviously, in view of Theorem 1.2, the groups where the new relative difference sets lie in are no longer cyclic. In fact, the group concerns is the direct product of an even cyclic group and a copy of $\mathbb{Z}_2$. The main idea of our construction is to combine several relative difference sets constructed in [2].

In the last section, by using the methods developed in constructing relative different sets, we also give a construction of new circulant weighing matrices of weight q^{d-1} where q is a 2-power, d is odd and $d \geq 5$.

Finally, we would like to mention that recently, Chandler and Xiang [4] constructed a new family of relative difference sets with classical parameters when q is a power of 3. However, these relative difference sets are, in general, not 'lifted' from complements of Singer difference sets.

2 Some Quadrics in GF(q^d)

Throughout this paper, q is a 2-power, $F_2 = \mathrm{GF}(2)$, $F = \mathrm{GF}(q)$ and $K = \mathrm{GF}(q^d)$ where d is odd. For any real-value function L on K, let $L \mapsto \hat{L}$ donote the orthogonal Fourier (Hadamard) transform given by

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

for all $\beta \in K$, where for convenience we denote the trace function $\mathrm{Tr}_{F_2}^{K}$ simply by Tr.

Let T denote the classicial affine difference set $\{x \in K^\times : \mathrm{Tr}_F^K(x) = 1\}$ in $K^\times$. For $1 \leq i \leq d-1$, we define $Q_i : K \to F_2$ such that $Q_i(x) = \mathrm{Tr}(x^{q^i+1})$ for all $x \in K$ and we let G_i denote the real-valued function $(-1)^{Q_i}$. Note that the set $\{x \in K^\times : Q_i(x) = 0\}$ is a quadric in the affine space K when i is relatively prime to d.

Proposition 2.1 *Suppose i is relatively prime to d. Then there exist disjoint subsets A_i and B_i such that $T = A_i \cup B_i$ and*

$$\hat{G}_i(\beta) = q^{-d/2} \sum_{x \in K} (-1)^{\mathrm{Tr}(x^{q^i+1}+\beta x)} = \begin{cases} 0 & \text{if } \beta \notin T \\ \sqrt{q} & \text{if } \beta \in A_i \\ -\sqrt{q} & \text{if } \beta \in B_i. \end{cases}$$

Furthermore, $D_i = A_i \cup B_i\theta$ is a $((q^d-1)/(q-1), 2(q-1), q^{d-1}, q^{d-2}/2)$-relative difference set in $K^\times \times \langle\theta\rangle$ relative to $F^\times \times \langle\theta\rangle$, where $o(\theta) = 2$.

Proof Note that for $i = 1$, our proposition is just [2, Theorem 3.2]. In fact, the proof for our proposition is basically the same. Since this result is crucial, we highlight the essential part of the proof. For all $\beta \in K^\times$, we have

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

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

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

The inner sum is 0 unless $y^{q^{2i}} + y = 0$ in which case it is q^d. However, $y^{q^{2i}} + y = 0$ iff $y \in K \cap \mathbb{F}_{q^{2i}}$. Since d is odd and $gcd(i, d) = 1$, $y \in K \cap \mathbb{F}_{q^{2i}}$ iff $y \in \mathbb{F}_q$.

¿From now on, we can apply the arguement used in the proof of [2, Theorem 3.2] to complete the proof. □

Proposition 2.2 *Let i and j be relatively prime to d. Then $\{A_i, B_i\} = \{A_j, B_j\}$ if and only if $i = j$ or $i = d - j$, where A_i, B_i, A_j, B_j are defined as in Propositon 2.1.*

Proof Since $\mathrm{Tr}(x^{(q^i+1)q^{d-i}}) = \mathrm{Tr}(x^{q^{d-i}+1})$ for all $x \in K$, we have $G_i = G_{d-i}$. Thus, $\{A_i, B_i\} = \{A_{d-i}, B_{d-i}\}$. To prove the converse, we may assume $1 \le i < j < d/2$.

Now assume $\{A_i, B_i\} = \{A_j, B_j\}$, i.e. $\hat{G}_i(\beta) = \delta\hat{G}_j(\beta)$ for all $\beta \in K$ where $\delta = \pm 1$. By the property of Fourior tranform, we then have $G_i(x) = \delta G_j(x)$ for all $x \in K$. Note that $\delta = 1$ as $Q_i(0) = Q_j(0) = 0$. Hence, $Q_i(x) + Q_j(x) = 0$ for all $x \in K$. Consequently,

$$\begin{aligned}0 &= Q_i(x+y) + Q_j(x+y) - Q_i(x) - Q_j(x) - Q_i(y) - Q_j(y)\\ &= \mathrm{Tr}(xy^{q^i} + x^{q^i}y + xy^{q^j} + x^{q^j}y) = \mathrm{Tr}([y^{q^{i+j}} + y^{q^{j-i}} + y^{q^{2j}} + y]x^{q^j}).\end{aligned}$$

Thus, $y^{q^{i+j}} + y^{q^{j-i}} + y^{q^{2j}} + y = 0$ for all $y \in K$. Hence $y^{q^{i+j}} + y^{q^{j-i}} + y^{q^{2j}} + y$ is a multiple of the polynomial $y^{q^d} - y$. This is impossible as $2j < d$. □

3 New Relative Difference Sets

Our construction bases on the following simple observation.

Theorem 3.1 *Let G be a group of order mn and N a normal subgroup of order n in G. Furthermore, let $G' = G \times \langle\theta_1\rangle \times \langle\theta_2\rangle$ where $\circ(\theta_1) = \circ(\theta_2) = 2$. Suppose R is an (m, n, k, λ)-relative difference set in G relative to N. Furthermore, for $i = 1, 2, 3$, let $X_i \cup \theta_1 Y_i$, where $X_i \cup Y_i = R$, be $(m, 2n, k, \lambda/2)$-relative difference sets in $G \times \langle\theta_1\rangle$ relative to $N \times \langle\theta_1\rangle$. If*

$$\{X_3, Y_3\} = \{(X_1 \cap X_2) \cup (Y_1 \cap Y_2), (X_1 \cap Y_2) \cup (X_2 \cap Y_1)\},$$

then

$$R' = (X_1 \cap X_2) \,\cup\, (X_2 \cap Y_1)\theta_1 \,\cup\, (X_1 \cap Y_2)\theta_2 \,\cup\, (Y_1 \cap Y_2)\theta_1\theta_2$$

is an $(m, 4n, k, \lambda/4)$-relative difference set in $G \times \langle\theta_1\rangle \times \langle\theta_2\rangle$ relative to $N \times \langle\theta_1\rangle \times \langle\theta_2\rangle$.

Proof It sufficies to show that

$$|\chi(R')| = \begin{cases} k & \text{if } \chi \text{ is nonprincipal on } N \times \langle\theta_1\rangle \times \langle\theta_2\rangle \\ k - \lambda n & \text{if } \chi \text{ is principal on } N \times \langle\theta_1\rangle \times \langle\theta_2\rangle. \end{cases}$$

Suppose χ is principal on $\langle\theta_1\rangle \times \langle\theta_2\rangle$. Then,

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

If χ is nonprincipal on $\langle\theta_1\rangle \times \langle\theta_2\rangle$, we have three possibilities. In each case, we shall prove that $|\chi(R')| = k$.

Case (1) $\chi(\theta_1) = 1, \chi(\theta_2) = -1$. In that case, $|\chi(R')| = |\chi(X_2 - Y_2)|$.

Case (2) $\chi(\theta_1) = -1, \chi(\theta_2) = 1$. In that case, $|\chi(R')| = |\chi(X_1 - Y_1)|$.

Case (3) $\chi(\theta_1) = -1, \chi(\theta_2) = -1$. In that case, $|\chi(R')| = |\chi(X_3 - Y_3)|$.

Since each $X_i \cup \theta_1 Y_i$ is a relative difference sets in $G \times \langle\theta_1\rangle$ relative to $N \times \langle\theta_1\rangle$, $|\chi(X_i - Y_i)| = k$. We have thus shown that R' is a relative difference set. □

It is possible to generalize Theorem 3.1 to construct relative difference sets in $G \times \langle\theta_1\rangle \times \langle\theta_2\rangle \times \cdots \times \langle\theta_r\rangle$ relative to $N \times \langle\theta_1\rangle \times \langle\theta_2\rangle \cdots \times \langle\theta_r\rangle$ where $\circ(\theta_1) = \cdots = \circ(\theta_r) = 2$.

To facilitate the construction, we reconsider the condition required in Theorem 3.1. We first need an easy observation.

Proposition 3.2 *Let S be a set and $\mathbf{S} = \{\{X, Y\} : X \cup Y = S$ and $X \cap Y = \emptyset\}$. Let $*$ be an operation defined on $\mathbf{S}$ such that*

$$\{X, Y\} * \{X', Y'\} = \{(X \cap X') \cup (Y \cap Y'), (X \cap Y') \cup (Y \cap X')\}.$$

Then $(\mathbf{S}, *)$ is an elementary abelian 2-group with identity $\{S, \emptyset\}$.

Let R be as defined in Theorem 3.1 and $\mathbf{R} = \{\{X, Y\} : X \cup Y = R$ and $X \cap Y = \emptyset\}$. In $\mathbf{R}$, $*$ a binary operation as defined before. Let us now consider the condition required in Theorem 3.1. Note that each relative difference set R_i induces a partition of R into two disjoint sets X_i, Y_i. Thus, we may identify R_i as the element $\{X_i, Y_i\}$ in $\mathbf{R}$. For convenience, we also write R for $\{R, \emptyset\}$. Now the condition required in Theorem 3.1 is equivalent to the condition that $\{R, R_1, R_2, R_3\}$ is a subgroup in $\mathbf{R}$.

We can now generalize Theorem 3.1.

Theorem 3.3 *Let G be a group of order mn and N a normal subgroup of order n in G. Furthermore, let $G' = G \times \langle\theta_1\rangle \times \langle\theta_2\rangle \cdots \times \langle\theta_r\rangle$ where $\circ(\theta_1) = \circ(\theta_2) = \cdots = \circ(\theta_r) = 2$. Suppose R is an (m, n, k, λ)-relative difference set in G relative to N. Furthermore, for $i = 1, 2, \ldots, 2^r - 1$, let $R_i = X_i \cup Y_i\theta_1$, where $X_i, Y_i \subset G$, be relative difference sets in $G \times \langle\theta_1\rangle$ relative to $N \times \langle\theta_1\rangle$. Suppose $\{R, R_1, R_2, \ldots, R_{2^r-1}\}$ is a subgroup in $(\mathbf{R}, *)$ and*

$$W(x_1, x_2, \ldots, x_r) = \bigcap_{i=1}^{r} Z_i \text{ such that } Z_i = \begin{cases} X_i & \text{if } x_i = 0 \\ Y_i & \text{if } x_i = 1. \end{cases}$$

Then

$$R' = \bigcup_{(x_1, x_2, \ldots, x_r) \in F_2^r} W(x_1, x_2, \ldots, x_r)\theta_1^{x_1} \cdots \theta_r^{x_r}$$

is an $(m, 2^r n, k, \lambda/2^r)$-relative difference set in $G \times \langle\theta_1\rangle \times \cdots \times \langle\theta_r\rangle$ relative to $N \times \langle\theta_1\rangle \times \cdots \times \langle\theta_r\rangle$.

We skip the proof as it is analogous to the argument used in the proof of Theorem 3.1.

To apply Theorem 3.3 (or Theorem 3.1), we use the relative difference sets constructed in Propositon 2.1. Assume $[K : F]$ is an odd number d and i is an integer relative prime to d. For each i, let R_i be the relative difference set induced by the form $Q_i(x)$. If we can find a subgroup $\{R_{i_j} : j = 1, 2, \ldots, 2^r - 1\} \cup \{R\}$, then we obtain a new relative difference set. As we shall shown later, such a group exists when $r = 2$ and $d = 7$.

¿From now on, we shall follow the notation used in Section 2. Let q be a power of 2, and let $d \geq 7$ be an odd integer. Write $F = \mathrm{GF}(q)$ and $K = \mathrm{GF}(q^d)$. Let $\beta \in K$ and let i be any positive integer coprime to d. Recall that

$$\begin{aligned}
\hat{G}_i(\beta) &= q^{-d/2} \sum_{x \in K} (-1)^{\mathrm{Tr}(x^{q^i+1}+\beta x)}, \\
A_i &= \{\beta \in K : \hat{G}_i(\beta) = \sqrt{q}\}, \\
B_i &= \{\beta \in K : \hat{G}_i(\beta) = -\sqrt{q}\}, \\
T &= \{\beta \in K : \mathrm{Tr}_F^K(\beta) = 1\}.
\end{aligned}$$

Theorem 3.4 *Let $G = K^\times \times \langle\theta_1\rangle \times \langle\theta_2\rangle$ where θ_1 and θ_2 are of order 2. Let $a, b, c \in \{1, ..., (d-1)/2\}$ be distinct integers coprime to d and define $R \subset G$ by*

$$R = (A_a \cap A_b) \cup (A_b \cap B_a)\theta_1 \cup (A_a \cap B_b)\theta_2 \cup (B_a \cap B_b)\theta_1\theta_2.$$

If $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$, then R is a $((q^d-1)/(q-1), 4(q-1), q^{d-1}, q^{d-2}/4)$ difference set in G relative to $F^\times \times \langle\theta_1\rangle \times \langle\theta_2\rangle$.

Proof If $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$, then

$$\{(A_a \cap A_b) \cup (B_a \cap B_b), (A_a \cap B_b) \cup (A_b \cap B_a)\} = \{A_c, B_c\}$$

and thus Theorem 3.1 implies the assertion. $\square$.

In view of Theorem 3.4, it is very interesting to determine all values of q, d, a, b, c for which $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$. This is done in our following main result.

Theorem 3.5 *Let q be a power of 2, let $d \geq 7$ be odd, and let $a, b, c \in \{1, ..., (d-1)/2\}$ be distinct integers coprime to d. Then $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for $x \in T$ if and only if $d = 7$ and $\{a, b, c\} = \{1, 2, 3\}$.*

Corollary 3.6 *Let q be a power of 2. Then there is a $((q^7-1)/(q-1), 4(q-1), q^6, q^5/4)$ difference set in $K^\times \times \langle\theta_1\rangle \times \langle\theta_2\rangle$ relative to $F^\times \times \langle\theta_1\rangle \times \langle\theta_2\rangle$.*

The proof of Theorem 3.5 is quite long and we need several lemmas. First we reduce the problem to evaluating a sum involving a quadratic form.

Lemma 3.7 *The product $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$ if and only if*

$$\sum_{x,y\in K}(-1)^{\mathrm{Tr}(x^{q^a+1}+y^{q^b+1}+(x+y)^{q^c+1})} = \pm q^{(3d+1)/2}. \tag{2}$$

Proof Recall that for $(i,d)=1$, $\hat{G}_i(\beta)=\pm\sqrt{q}$ for $\beta\in T$ and $\hat{G}_i(\beta)=0$ for $\beta\in K\setminus T$. Furthermore, $|T|=q^{d-1}$. Thus $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x\in T$ if and only if

$$\sum_{\beta\in K}\hat{G}_a(\beta)\hat{G}_b(\beta)\hat{G}_c(\beta) = \pm q^{d-1}\cdot q^{3/2} = \pm q^{(2d+1)/2}. \tag{3}$$

By definition, (3) is equivalent to

$$\sum_{\beta\in K}\sum_{x,y,z\in K}(-1)^{\mathrm{Tr}((x^{q^a+1}+\beta x)+(y^{q^b+1}+\beta x)+(z^{q^c+1}+\beta x))} = \pm q^{(2d+1)/2}\cdot q^{3d/2} = \pm q^{(5d+1)/2}. \tag{4}$$

Note that

$$\sum_{\beta\in K}(-1)^{\mathrm{Tr}(\beta(x+y+z))} = \begin{cases} 0 & \text{if } x+y+z\neq 0\\ q^d & \text{if } x+y+z=0.\end{cases}$$

Hence

$$\begin{aligned} &\sum_{\beta\in K}\sum_{x,y,z\in K}(-1)^{\mathrm{Tr}((x^{q^a+1}+\beta x)+(y^{q^b+1}+\beta x)+(z^{q^c+1}+\beta x))}\\ = &\sum_{x,y,z\in K}(-1)^{\mathrm{Tr}(x^{q^a+1}+y^{q^b+1}+z^{q^c+1})}\sum_{\beta\in K}(-1)^{\beta(x+y+z)}\\ = &\; q^d\sum_{x,y\in K}(-1)^{\mathrm{Tr}(x^{q^a+1}+y^{q^b+1}+(x+y)^{q^c+1})}. \end{aligned}$$

Thus (4) is equivalent to (2) and this proves the assertion. □

In order to calculate the sum occuring in (2), we need to consider $Q(x,y) := \mathrm{Tr}(x^{q^a+1} + y^{q^b+1} + (x+y)^{q^c+1})$ as a quadratic form over GF(2). For this let B be a fixed basis of K over GF(2). Then, for each $x\in K$, there are unique elements $x_b\in \mathrm{GF}(2)$ with $x=\sum_{b\in B}x_b b$. Hence

$$\begin{aligned} \mathrm{Tr}(x^{q^a+1}) &= \mathrm{Tr}([\sum_{b\in B}x_b b]^{q^a}\sum_{c\in B}x_c c)\\ &= \mathrm{Tr}([\sum_{b\in B}x_b b^{q^a}]\sum_{c\in B}x_c c)\\ &= \sum_{b,c\in B}x_b x_c \mathrm{Tr}(b^{q^a}c). \end{aligned}$$

This shows that $\mathrm{Tr}(x^{q^a+1})$ is a quadratic form of K over GF(2). Similarly, it follows that $Q(x,y)$ is a quadratic form of $K \times K$ over GF(2). The GF(2) vector space

$$D_Q := \{(u,v) \in K \times K : Q(x+u, y+v) = Q(x,y)\ \forall (x,y) \in K \times K\}$$

is called the **degeneracy space** of Q.

Lemma 3.8 *Write $q = 2^r$. Let k denote the dimension of D_Q over* GF(2)*. Then*

$$\sum_{x,y \in K} (-1)^{\mathrm{Tr}(x^{q^a+1}+y^{q^b+1}+(x+y)^{q^c+1})} = \begin{cases} 0 & \text{if } k \text{ is odd,} \\ \pm 2^{rd+k/2} & \text{if } k \text{ is even.} \end{cases}$$

Proof Let V be a complement of D_Q in $K \times K$. Then V is a GF(2) vector space of dimension $2rd - k$ and Q is a nondegenerate quadratic form on V. Let

$$N := |\{(x,y) \in V : Q(x,y) = 0\}|.$$

By [9, Thms. 6.30, 6.32], we have

$$N = \begin{cases} 2^{2rd-k-1} & \text{if } k \text{ is odd,} \\ 2^{2rd-k-1} \pm 2^{(2rd-k-2)/2} & \text{if } k \text{ is even.} \end{cases} \tag{5}$$

Hence

$$\begin{aligned} \sum_{x,y \in K} (-1)^{\mathrm{Tr}(x^{q^a+1}+y^{q^b+1}+(x+y)^{q^c+1})} &= \sum_{x,y \in K} (-1)^{Q(x,y)} \\ &= \sum_{(x,y) \in V} \sum_{(u,v) \in D_Q} (-1)^{Q(x+u,y+v)} \\ &= \sum_{(x,y) \in V} \sum_{(u,v) \in D_Q} (-1)^{Q(x,y)} \\ &= 2^k \sum_{(x,y) \in V} (-1)^{Q(x,y)} \\ &= 2^k (N - (2^{2rd-k} - N)) \\ &= 2^k (2N - 2^{2rd-k}). \end{aligned}$$

Now the assertion follows from (5). □

Corollary 3.9 *The degenaracy space D_Q of the quadratic form Q is a vector space over $F =$ GF(q). Furthermore, the product $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$ if and only if the dimension of D_Q over F is $d+1$.*

Proof The assertion that D_Q is an F vector space follows by a straightforward calculation using the definitions of Q and D_Q. Write $q = 2^r$ and let k respectively k_F be the dimension of D_Q over GF(2) respectively F. Then $k_F r = k$ and by Lemmas 3.7 and 3.8 the product $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$ if and only if $k_F r$ is even and $2^{(3d+1)r/2} = 2^{rd+k_F r/2}$. But since d is odd this is the case if and only if $k_F = d + 1$. $\square$

Convention: In the following, all exponents of q are considered as integers modulo d in $[0, d-1]$. For example, for $a > 0$ the term $x^{q^{-a}}$ is a short notation for $x^{q^{a_1}}$ where a_1 is the unique integer in $[0, d-1]$ with $a_1 \equiv a \bmod d$.

Lemma 3.10 *Let*

$$V' = \{(x, y) \in K \times K : x^{q^a} + x^{q^{-a}} = y^{q^b} + y^{q^{-b}}\}.$$

Then V' is an F vector space of dimension $d + 1$ which contains D_Q. In particular, $\dim_F(D_Q) = d + 1$ if and only if $D_Q = V'$.

Proof The assertion that V' is an F vector space follows directly from its definition. We now show $\dim_F(V') = d + 1$. Let $\phi : K \to K, x \mapsto x^{q^a} + x^{q^{-a}}$ and $\rho : K \to K, y \mapsto y^{q^b} + y^{q^{-b}}$.

Claim 1: $\ker\, \phi = \ker \rho = F$.

Proof of Claim 1: It follows from the definitions that $F \subset \ker\, \phi$ and $F \subset \ker \rho$. Let $x \in \ker\, \phi$ be arbitrary. Then $x^{q^a} = x^{q^{-a}}$ and thus $x^{q^{2a}} = x$. But since $(2a, d) = 1$ the automorphism $x \mapsto x^{q^{2a}}$ generates $G := \mathrm{Gal}(K/F)$. Thus $x \in \mathrm{Fix}(G) = F$. This shows $\ker\phi \subset F$. Similarly, it follows that $\ker\rho \subset F$ and this proves Claim 1.

Claim 2: $\mathrm{Im}\ \phi = \mathrm{Im}\ \rho = \{x \in K : \mathrm{Tr}_F^K(x) = 0\}$.

Proof of Claim 2: Write $W := \{x \in K : \mathrm{Tr}_F^K(x) = 0\}$. From the definitions of ϕ and ρ it follows that $\mathrm{Im}\ \phi \subset W$ and $\mathrm{Im}\ \rho \subset W$. Note $\dim_F W = d - 1$. But Claim 1 implies $\dim_F \mathrm{Im}\ \phi = \dim_F \mathrm{Im}\ \rho = d - 1$. This proves Claim 2.

Now let B be any basis of K over F. By Claim 2, for every $b \in B$ there is a $y_b \in K$ such that $(b, y_b) \in V'$. Define

$$C := \{(b, y_b) : b \in B\} \cup \{(0, 1)\}.$$

Then $C \subset V'$ and C is linearly independent over F. Let $(x,y) \in V'$ be arbitrary and write $x = \sum_{b\in B} x_b b$ with $x_b \in F$. Since $(b, y_b) \in V'$ for all $b \in B$, we have $(x, \sum_{b\in B} x_b y_b) = \sum_{b\in B} x_b(b, y_b) \in V'$. Thus $(0, y - \sum_{b\in B} x_b y_b) \in V'$ which implies $y - \sum_{b\in B} x_b y_b \in \ker \rho = F$. Thus $(x,y) = (\sum_{b\in B} x_b(b, y_b)) + (y - \sum_{b\in B} x_b y_b)(0,1)$ is an F-linear combination of elements of C. In summary, we have shown that C is a basis of V' over F. Thus $\dim_F V' = |C| = d+1$.

It remains to show that V' contains D_Q. Let $(u,v) \in D_Q$ be arbitrary. Then $Q(u,v) = 0$ and for all $x, y \in K$ we have

$$\begin{aligned} 0 &= Q(x+u, y+v) + Q(x,y) + Q(u,v) \\ &= \mathrm{Tr}(x^{q^a}u + xu^{q^a} + y^{q^b}v + yv^{q^b} + (x+y)^{q^c}(u+v) + (x+y)(u+v)^{q^c}) \\ &= \mathrm{Tr}(x^{q^a}u + xu^{q^a} + x^{q^c}(u+v) + x(u+v)^{q^c}) + \\ &\quad \mathrm{Tr}(y^{q^b}v + yv^{q^b} + y^{q^c}(u+v) + y(u+v)^{q^c}). \end{aligned}$$

Using the fact that $\mathrm{Tr}(z^{q^i}) = \mathrm{Tr}(z)$ for all $z \in K$ and all $i \geq 0$ we get

$$\begin{aligned} 0 &= \mathrm{Tr}(x(u^{q^{-a}} + u^{q^a} + (u+v)^{q^{-c}} + (u+v)^{q^c})) + \\ &\quad \mathrm{Tr}(y(v^{q^{-b}} + v^{q^b} + (u+v)^{q^{-c}} + (u+v)^{q^c})) \end{aligned}$$

for all $x, y \in K$. Setting $x = 0$ respectively $y = 0$ we get

$$\begin{aligned} \mathrm{Tr}(y(v^{q^{-b}} + v^{q^b} + (u+v)^{q^{-c}} + (u+v)^{q^c})) &= 0 \quad \forall y \in K, \\ \mathrm{Tr}(x(u^{q^{-a}} + u^{q^a} + (u+v)^{q^{-c}} + (u+v)^{q^c})) &= 0 \quad \forall x \in K. \end{aligned}$$

Since $(r,s) \mapsto \mathrm{Tr}(rs)$ is a nondegenerate bilinear form on $K \times K$ this implies

$$v^{q^{-b}} + v^{q^b} + (u+v)^{q^{-c}} + (u+v)^{q^c} = 0 \tag{6}$$

and

$$u^{q^{-a}} + u^{q^a} + (u+v)^{q^{-c}} + (u+v)^{q^c} = 0. \tag{7}$$

Adding (6) and (7) we see that $(u,v) \in V'$. This shows $D_Q \subset V'$ and concludes the proof. □

Lemma 3.11 *Define $f \in \{1, ..., d-1\}$ by $af \equiv c \bmod d$ and let I be the multiset given by*

$$\begin{aligned} I &= \{-b, b, -c, c\} \cup \{-c-b+(2i+1)a : i = 0, ..., f-1\} \\ &\quad \cup \{-c+b+(2i+1)a : i = 0, ..., f-1\}. \end{aligned}$$

(here all elements of I are chosen in $[0, d-1]$ by reducing modulo d).

If $D_Q = V'$ then all elements of I have even multiplicity in I.

Proof Assume $D_Q = V'$ and let $(x, y) \in V'$ be arbitrary. By definition we have

$$x^{q^a} + x^{q^{-a}} = y^{q^b} + y^{q^{-b}}. \tag{8}$$

Applying suitable automorphisms $z \mapsto z^{q^i}$ of K to (8) we get the following sequence of equations.

$$\begin{aligned} x^{q^{-c}} + x^{q^{-c+2a}} &= y^{q^{a+b-c}} + y^{q^{a-b-c}} \\ x^{q^{-c+2a}} + x^{q^{-c+4a}} &= y^{q^{3a+b-c}} + y^{q^{3a-b-c}} \\ \cdots &= \cdots \\ x^{q^{-c+2a(f-1)}} + x^{q^{-c+2af}} &= y^{q^{(2(f-1)+1)a+b-c}} + y^{q^{2(f-1)+1)a-b-c}}. \end{aligned}$$

Summing up all these equation and using $-c + 2af \equiv c \bmod d$ we obtain

$$x^{q^{-c}} + x^{q^c} = \sum_{j \in J} y^{q^j} \tag{9}$$

where

$$J = \{-c-b+(2i+1)a : i = 0, ..., f-1\} \cup \{-c+b+(2i+1)a : i = 0, ..., f-1\}.$$

Since we are assuming $D_Q = V'$, we have $(x, y) \in D_Q$ and thus

$$y^{q^{-b}} + y^{q^b} + (x+y)^{q^{-c}} + (x+y)^{q^c} = 0 \tag{10}$$

by (6). Combining (9) and (10) we get

$$\sum_{i \in I} y^{q^i} = 0. \tag{11}$$

In summary, we have shown that (11) holds for every $y \in K$ for which there is an $x \in K$ with $(x, y) \in V'$. But by Claim 2 in the proof of Lemma 3.10, for *every* $y \in K$ there is an $x \in K$ with $(x, y) \in V'$. Thus we have shown that (11) holds for every $y \in K$. Now recall that all elements of I are integers in $[0, d-1]$. Thus $f(y) := \sum_{i \in I} y^{q^i}$ is a polynomial of degree $< q^d$ such that $f(y) = 0 \ \ \forall y \in K$. But this implies that $y^{q^d} - y$ divides f. Since deg $f < q^d$, f must be the zero polynomial over GF(2). This implies the assertion. □

Proof of Theorem 3.5

We first prove the necessary part. To avoid some case distinctions, we drop the assumption that $a, b, c \leq (d-1)/2$. Thus let $a, b, c \in [1, d-1]$ be any integers coprime to d such that $a \not\equiv \pm b \bmod d$, $a \not\equiv \pm c \bmod d$ and $b \not\equiv \pm c \bmod d$.

Claim: If $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for $x \in T$ then $d = 7$.

Proof of the Claim: Assume that $\hat{G}_a(x)\hat{G}_b(x)\hat{G}_c(x)$ is constant for all $x \in T$. Then by Corollary 3.9, Lemma 3.10 and Lemma 3.11, the multiset

$$\begin{aligned} I &= \{-b, b, -c, c\} \cup \{-c - b + (2i+1)a : i = 0, ..., f-1\} \\ &\quad \cup \{-c + b + (2i+1)a : i = 0, ..., f-1\} \end{aligned}$$

has only even multiplicities. Recall that all elements of I are considered mod d and that $f \in [1, d-1]$ is defined by $af \equiv c \bmod d$. Since $\hat{G}_c(x) = \hat{G}_{-c}(x)$ we may replace c by $-c$ if necessary so that we can assume $f \in [1, (d-1)/2]$.

Let $a^{-1} \in [1, d-1]$ denote the multiplicative inverse of a mod d. Since I has only even multiplicities if and only if

$$\begin{aligned} I' &= \{-ba^{-1}, ba^{-1}, -ca^{-1}, ca^{-1}\} \cup \{-ca^{-1} - ba^{-1} + (2i+1) : i = 0, ..., f-1\} \\ &\quad \cup \{-ca^{-1} + ba^{-1} + (2i+1) : i = 0, ..., f-1\} \end{aligned}$$

has only even multiplicities, we may assume $a = 1$. Then $f = c$ and $b, c \not\equiv \pm 1 \bmod d$. Set

$$\begin{aligned} A &= \{-b, b, -c, c\}, \\ B &= \{-c - b + 2i + 1 : i = 0, ..., c-1\}, \\ C &= \{-c + b + 2i + 1 : i = 0, ..., c-1\}. \end{aligned}$$

Note that within B and within C no two elements overlap since d is odd. Thus, since $I = A \cup B \cup C$ has only even multiplicities and since $|B| + |C| = 2c$, exactly $c - 2$ elements of B must overlap with elements of C and the remaining four elements of B and C must overlap with the elements of A. Recall that we assume $c = f \in [1, (d-1)/2]$. An overlap of $c - 2$ elements between B and C happens if and only if $-c - b = -c + b - 4$ or $-c - b = -c + b + 4$. In all following multisets, we take all the multiplicities mod 2 and all elements mod d.

Case 1: $-c-b = -c+b-4$. Then $b = 2$ and $B \cup C = \{-c-1, -c+1, c-1, c+1\} = A = \{2, -2, c, -c\}$. Since $c \neq \pm 1$, we have $-c+1 \neq 2$ and $c+1 \neq 2$. Thus $-c-1 = 2$ or $c - 1 = 2$, i.e., $c = \pm 3$. If $c = 3$ then $\{-4, -2, 2, 4\} = \{2, -2, 3, -3\}$ which implies $d = 7$. Similarly, $c = -3$ also implies $d = 7$.

Case 2: $-c-b = -c+b+4$. Then $b = -2$ and $B \cup C = \{c-1, c+1, -c-1, -c+1\} = A = \{-2, 2, -c, c\}$. This implies $d = 7$ exactly as in Case 1.

In summary, we have shown that $d = 7$ in all possible cases. This proves our claim. When $d = 7$, then $\{a, b, c\} = \{1, 2, 3\}$ is forced in Theorem 3.5 since there we assume $a, b, c \in [1, (d-1)/2]$. This concludes the proof of the necessary part of Theorem 3.5. In view of Corollary 3.9 and Lemma 3.10, the proof of the sufficient part of Theorem 3.5 is provided by the following lemma.

Lemma 3.12 *Let $d = 7$ and $\{a, b, c\} = \{1, 2, 3\}$. Then $D_Q = V'$.*

Proof W.l.o.g. let $a = 1$, $b = 2$ and $c = 3$. By Lemma 3.10 we have $D_Q \subset V'$. Thus it suffices to show $V' \subset D_Q$. Let $(x, y) \in V'$ be arbitrary. Then by definition

$$x^q + x^{q^6} = y^{q^2} + y^{q^5}. \tag{12}$$

Claim 1: $\mathrm{Tr}(x^{q+1} + y^{q^2+1} + (x+y)^{q^3+1}) = 0$.

Proof of Claim 1: Applying suitable automorphisms $z \mapsto z^{q^i}$ of K to (12) we get

$$x^{q^3} + x^q = y^{q^4} + y \tag{13}$$

as well as $x + x^{q^2} = y^{q^3} + y^{q^6}$ and $x^{q^2} + x^{q^4} = y^{q^5} + y^q$. Adding up the last two equations we get

$$x + x^{q^4} = y^q + y^{q^3} + y^{q^5} + y^{q^6}. \tag{14}$$

Using (13), (14) and the fact that $\mathrm{Tr}(z^{q^i}) = \mathrm{Tr}(z)$ for all $z \in K$ and all $i \geq 0$ we calculate

$$\begin{aligned}
& \mathrm{Tr}(x^{q+1} + y^{q^2+1} + (x+y)^{q^3+1}) \\
= \; & \mathrm{Tr}(x(x^q + x^{q^3}) + y^{q^2+1} + y^{q^3+1} + xy^{q^3} + x^{q^3}y) \\
= \; & \mathrm{Tr}(x(y + y^{q^4}) + y^{q^2+1} + y^{q^3+1} + xy^{q^3} + x^{q^3}y) \\
= \; & \mathrm{Tr}(y(x + x^{q^3} + x^{q^3} + x^{q^4}) + y^{q^2+1} + y^{q^3+1}) \\
= \; & \mathrm{Tr}(y(y^q + y^{q^3} + y^{q^5} + y^{q^6}) + y^{q^2+1} + y^{q^3+1}) \\
= \; & \mathrm{Tr}(y^{q^6}y + yy^{q^3} + y^{q^2}y + yy^{q^6} + y^{q^2+1} + y^{q^3+1}) \\
= \; & \mathrm{Tr}(0) = 0.
\end{aligned}$$

This proves Claim 1.

The following completes the proof of Lemma 3.12

Claim 2: Let $(x, y) \in V'$ and $(u, v) \in K$ be arbitrary. Then $Q(x+u, y+v) = Q(u, v)$.

Proof of Claim 2: ¿From (14) we get $x^{q^4} + x^q = y^{q^5} + y + y^{q^2} + y^{q^3}$. Adding this equation to (14) we get $x + x^q = y + y^q + y^{q^2} + y^{q^6}$ and hence

$$x^{q^3} + x^{q^4} = y^{q^3} + y^{q^4} + y^{q^5} + y^{q^2}. \tag{15}$$

Using Claim 1, equations (12), (15) and the fact that $\mathrm{Tr}(z^{q^i}) = \mathrm{Tr}(z)$ for all $z \in K$ and all $i \geq 0$ we calculate

$$\begin{aligned}
& Q(x+u, y+v) - Q(u, v) \\
= \; & \mathrm{Tr}(xu^q + x^q u + yv^{q^2} + y^{q^2}v + (x+y)(u+v)^{q^3} + (x+y)^{q^3}(u+v)) \\
= \; & \mathrm{Tr}(u(x^{q^6} + x^q + x^{q^4} + y^{q^4} + x^{q^3} + y^{q^3}) + v(y^{q^5} + y^{q^2} + x^{q^4} + y^{q^4} + x^{q^3} + y^{q^3})) \\
= \; & \mathrm{Tr}(u \cdot 0 + v \cdot 0) = 0.
\end{aligned}$$

This proves Claim 2. □

4 Circulant Weighing Matrices

A *weighing matrix* W, denoted by $W(n,k)$, of order n and weight k is a square matrix of order n with entries from $\{-1,0,+1\}$ such that $WW^t = kI_n$ where I_n is the $n \times n$ identity matrix and W^t is the transpose of W. We refer the reader to [6] for more details on weighing matrices.

Let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order n. Suppose $E = \sum_{i=1}^{n} a_i g_i \in \mathbb{Z}[G]$ satisfies

(i) $a_i = 0, \pm 1$ and

(ii) $EE^{(-1)} = k$ where $E^{(-1)} = \sum_{i=1}^{n} a_i g_i^{-1}$.

Then the group matrix $W = (w_{ij})$, where $w_{ij} = a_k$ if $g_i g_j^{-1} = g_k$, is a $W(n,k)$. A weighing matrix constructed in this way is called a *group weighing matrix* and denoted by $GW(G,k)$. In particular, if G is cyclic, then W is a *circulant weighing matrix* and is denoted by $CW(n,k)$. We refer the reader to [1] for the case when G is abelian.

For the convenience of our study of group weighing matrices using the notation of group rings, we say that $E \in \mathbb{Z}[G]$ is a $GW(G,k)$ ($CW(n,k)$ when G is cyclic) if it satisfies conditions (i) and (ii) above.

Let $E \in \mathbb{Z}[G]$ be a $GW(G,k)$. If the support of E is contained in a coset of a subgoup H of G, we say that E is a *trivial extension* of a $GW(H,k)$. If A is not a trivial extension of a $GW(H,k)$ for any subgroup H ($\neq G$) of G, A is called a *proper* $GW(G,k)$.

Using a similar idea to that of Theorem 3.1, we obtain the following:

Theorem 4.1 *Let G be a finite group. Suppose $E_1, E_2 \in \mathbb{Z}[G]$ are $GW(G,k)$ such that Support(E_1) = Support(E_2). Let*

$$X_i = \{g \in G : \textit{the coefficient of } g \textit{ in } E_i = 1\}$$

and

$$Y_i = \{g \in G : \textit{the coefficient of } g \textit{ in } E_i = -1\}$$

for $i = 1, 2$. Then

$$E = [(X_1 \cap X_2) - (Y_1 \cap Y_2)] + [(X_1 \cap Y_2) - (X_2 \cap Y_1)]\,\theta$$

is a $GW(G \times \langle\theta\rangle, k)$ where $o(\theta) = 2$. Furthermore, if $\{X_1, Y_1\} \neq \{X_2, Y_2\}$, then E is not a trivial extension of a $GW(G,k)$.

The following is a consequence of Propositions 2.1, 2.2 and Theorem 4.1.

Corollary 4.2 *Use the notation in Section 2. If $d \geq 5$ is an odd integer and i, j are two integers relatively prime to d such that $1 \leq i, j \leq d-1$ and $i \neq j, d-j$, then*

$$E = [(A_i \cap A_j) - (B_i \cap B_j)] + [(A_i \cap B_j) - (A_j \cap B_i)]\,\theta$$

is a proper $GW(K^\times \times \langle\theta\rangle, q^{d-1})$, where $o(\theta) = 2$, and hence a proper $CW(2(q^d-1), q^{d-1})$.

Remark 4.3 Note that the support of E in Corollary 4.2 contains at most one element in each coset of $F^\times$. Thus by projecting E onto the subgroup of order $2(q^d-1)/m$, where m is any divisor of $q-1$, we obtain a proper $CW(2(q^d-1)/m, q^{d-1})$. We refer the reader to [8] for a detailed discussion of $CW(n, 2^{2t})$.

References

[1] K.T. Arasu and J.F. Dillon, Perfect ternary arrays: Difference sets, sequences and their correlation properties, *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, vol. 542, Kluwer Acad. Publ., Dordrecht, 1999, 1-15.

[2] K.T. Arasu, J.F. Dillon, K.H. Leung and S.L. Ma, Cyclic relative dIfference sets with classical parameters, *J. Combin. Theory Ser. A*, 94(2001), 118-126.

[3] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Vol. 1, Encyclopedia of Mathematics and its Applications 69, Cambridge University Press, Cambridge, 1999.

[4] D. Chandler and Q. Xiang, Cyclic relative difference sets and their p-ranks, preprint.

[5] J.E.H. Elliott and A.T. Butson, Relative difference sets, *Ill. J. Math.*, 10(1966), 517-531.

[6] A.V. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker, New York-Basel, 1979.

[7] D. Jungnickel, Difference sets, in *Contemporary Design Theory: a Collection of Surveys*, eds. J.H. Dinitz and D.R. Stinson, pp. 241-324, Wiley, New York, 1992.

[8] K.H. Leung and S.L. Ma, Circulant weighing matrices of weight 2^{2t}, preprint.

[9] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997.

[10] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics Vol. 1601, Springer, Berlin/Heidelberg/New York, 1995.