JOURNAL OF COMBINATORIAL THEORY, Series A 71, 316–331 (1995)

The Solution of the Waterloo Problem

K. T. ARASU*

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435

JOHN F. DILLON

National Security Agency, Fort George G. Meade, Maryland 20755-6000

DIETER JUNGNICKEL AND ALEXANDER POTT

Lehrstuhl für Angewandte Mathematik II, Universität Augsburg,
Universitätsstrasse 8, 86135 Augsburg, Germany

Communicated by the Managing Editors

Received March 1, 1994

Let $D(d, q)$ be a classical (v, k, λ)-Singer difference set in a cyclic group G corresponding to the complement of the point–hyperplane design of $\mathrm{PG}(d, q)$ $(d \geqslant 1)$. We characterize those Singer difference sets $D(d, q)$ which admit a "Waterloo decomposition" $D = A \cup B$ such that $(A - B) \cdot (A - B)^{(-1)} = k$ in $\mathbb{Z}G$:

THEOREM. *$D(d, q)$ admits a Waterloo decomposition if and only if d is even.*

1. INTRODUCTION

The investigation of symmetric designs is of central interest in design theory. Another class of important incidence structures are projective and affine geometries. A projective geometry gives rise to two symmetric designs, namely the point–hyperplane designs and their complements. It is a remarkable property of these classical symmetric designs that we will investigate in this paper. For the geometric background that is necessary throughout our investigation, we refer the reader to [11].

* Research partially supported by NSA Grant MDA 904-92-H-3057, NSF Grant NCR-9200265 and by an Alexander-von-Humboldt fellowship. The author thanks the Mathematisches Institut der Universität Giessen for its hospitality during the time of this research. We thank Siu-Lun Ma for his careful reading of the manuscript.

0097-3165/95 $12.00

The projective geometries $\mathrm{PG}(d, q)$ of even dimension d contain subsets of points (*parabolic quadrics*) of the same cardinality as hyperplanes which have just three intersection numbers with hyperplanes. In Section 4 we will use these quadrics to construct a "Waterloo decomposition" of the complement of the symmetric point–hyperplane design of $\mathrm{PG}(d, q)$ if d is even (we will explain this term soon and we will also give some important definitions in Section 2). More precisely, we construct a decomposition of the difference set $D(d, q)$ associated with the design. In the odd dimension case there are no non-degenerate quadrics whose size equals the size of a hyperplane and therefore our construction of the Waterloo decomposition fails. The question arises whether a Waterloo decomposition can exist at all if the dimension d is odd: The answer is no and we will prove this in Section 4. Thus we obtain a complete characterization of the parameters d and q for which the complement of the point-hyperplane design of $\mathrm{PG}(d, q)$ admits a Waterloo decomposition.

At this point the reader might ask about the reason for the names "Waterloo problem" and "Waterloo decomposition." The Waterloo problem (existence question for a Waterloo decomposition) was originally posed in terms of *balanced weighing matrices*. Weighing and balanced weighing matrices have many applications in statistics ("design of experiments") and the connection to these matrices was the reason to study the question whether certain designs admit Waterloo decompositions. The existence of such a decomposition is equivalent to the existence of a *group invariant* balanced weighing matrix (and equivalent to the existence of certain *relative difference sets*). These objects have been studied by several mathematicians in Waterloo (Berman [4], Mullin and Stanton [17], Schellenberg [19]) which is the reason why the problem has been sometimes called the *Waterloo problem*. Indeed, at the "6th Southeastern conference on Combinatorics, Graph Theory and Computing, 1975," Collins, Ron Mullin and Paul Schellenberg all gave talks on their independent attacks on this problem.

Another reason to study the existence question for a Waterloo decomposition of $D(d, q)$ (which is the complement of a classical Singer difference set) is the following. The Singer difference set with parameters $(2^{d+1}-1, 2^d, 2^{d-1})$ corresponds to a primitive linear recursive sequence $\{a_t\}$ over GF(2) which has *almost perfect* autocorrelation properties, i.e.,

$$\sum_{t=0}^{2^{d+1}-2} (-1)^{a_{t+s}+a_t} = \begin{cases} 2^{d+1}-1, & \text{if } s=0 \\ -1, & \text{if } s \neq 0. \end{cases}$$

These sequences have many applications to synchronization problems. A Waterloo decomposition for such difference set turns the binary sequence

$\{a_t\}$ into a ternary (i.e., $(-1, 0, 1)$-valued) sequence $\{A_t\}$ which has *perfect* autocorrelation properties; i.e.,

$$\sum_{t=0}^{2^{d+1}-2} A_{t+s} \cdot A_t = \begin{cases} 2^d, & \text{if } s=0 \\ 0 & \text{if } s \neq 0 \end{cases}$$

(see [9], for instance).

Why do we consider just the complements of the point–hyperplane designs rather than the designs themselves? We can associate balanced weighing matrices with the complements of many of the point–hyperplane designs of PG(d, q) (whenever q is odd or d is even). Therefore the trivial necessary conditions for the existence of a balanced weighing matrix are satisfied in these cases and we need more sophisticated arguments to determine the parameters d and q for which a circulant balanced weighing matrix might exist. Interestingly enough, if d and q are both odd then there are examples of *negacyclic* matrices but (as we can prove) no circulant balanced weighing matrices can exist.

For other classes of symmetric designs (or difference sets) the situation is different. No designs with parameters other than those of the complementary point–hyperplane designs are known which have a Waterloo decomposition. In many cases we can prove that no such decomposition can exist. However, the methods of proof are quite different from the one that we have to use here. Roughly, we have to use more or less elementary number theory to check that certain (almost trivial) necessary conditions on the parameters of the symmetric designs are not satisfied. We have therefore decided not to include our non-existence results for other symmetric designs in this paper; see Section 5. What is known to us is summarized in [1].

2. The Main Result

A *weighing matrix* $W(k, v)$ is a square $(0, -1, +1)$-matrix $M=(m_{ij})$ of size v which satsfies $M \cdot M^t = k \cdot I_v$ (where I_v is the $(v \times v)$-identity matrix and M^t denotes the transpose of M). Note that M has to have exactly k non-zero entries in each row. Let $N=(|m_{ij}|)$ be the corresponding $(0, 1)$-matrix. If N is the incidence matrix of a symmetric (v, k, λ)-design then the weighing matrix is called a *balanced weighing matrix*: A symmetric (v, k, λ)-design is an incidence structure consisting of v points and v blocks of size k (we consider blocks as subsets of the set of points) such that any two distinct points are joined by exactly λ blocks. For background from Design Theory, we refer to [5]. We note that an easy counting argument shows that the parameter λ is determined by v and k through the equation

$\lambda \cdot (v-1) = k \cdot (k-1)$. An incidence matrix F of a symmetric (v, k, λ)-design is a $(v \times v)$-matrix, where the rows are labelled by the points and the columns by the blocks. The (p, B)-entry of F is 1 if $p \in B$ and 0 otherwise. Then F satisfies $F \cdot F^t = (k-\lambda) \cdot I_v + \lambda \cdot J_v$ (where J_v is the $(v \times v)$-matrix whose entries are all 1). The parameter $k - \lambda$ is called the *order* of the design.

Examples of balanced weighing matrices include *Hadamard matrices* $W(m, m)$ and *conference matrices* $W(m-1, m)$. The corresponding designs are trivial (m, m, m)-designs (in the case of Hadamard matrices) and $(m, m-1, m-2)$-designs (in the conference matrix case). If M is a balanced weighing matrix we can decompose the incidence matrix $N = (|m_{ij}|)$ of the underlying design $N = A + B$, where A and B are $(0, 1)$-matrices and $M = A - B$. Conversely, we can start with the incidence matrix N of a symmetric (v, k, λ)-design and we can try to find a decomposition $N = A + B$ such that $A - B$ is a (balanced) weighing matrix. From now on we restrict ourselves to *group invariant* balanced weighing matrices $M = (m_{ij})$: We assume that a group $G \leqslant S_n$ (the symmetric group on n letters) acts sharply transitively on $\{1, ..., n\}$ such that $m_{g(i), g(j)} = m_{i,j}$ for all $g \in G$. We call the matrix *circulant* if G is cyclic. Now we can formulate a very general version of the Waterloo problem.

Problem A. Find necessary and sufficient conditions for the existence of group invariant balanced weighing matrices.

If M is group invariant, then the matrices A, B, and N are group invariant, too. (But if only N is group invariant, it is not necessarily true that M, A, and B are group invariant.) In particular, the symmetric design $\mathscr{D}$ defined by the incidence matrix N admits an automorphism group G that acts sharply transitively on the points and blocks of $\mathscr{D}$ (points and blocks "are" the row and column indices of N).

The set of group invariant matrices (over a ring R) is isomorphic to the group ring RG via the isomorphism

$$\psi(M) = \sum_{g \in G} m_{g(1), 1}\, g.$$

Note that $\psi(M^t) = \sum m_{g(1), 1}\, g^{-1} = \psi(M)^{(-1)}$, where $X^{(-1)} = \sum x_g g^{-1}$ for $X = \sum x_g g$ in RG. Therefore, the existence of a group invariant balanced weighing matrix M implies the existence of group ring elements D, A, and B in $\mathbb{Z}G$ such that

$$D \cdot D^{(-1)} = (k - \lambda) + \lambda \cdot G$$

and

$$(A - B) \cdot (A - B)^{(-1)} = k,$$

where $D = A + B$ and D, A, and B are group ring elements with $(0, 1)$-coefficients. Moreover, $k - \lambda$ and k denote the group ring elements $(k - \lambda) \cdot e_G$ and $k \cdot e_G$, where e_G is the identity element of G. Note that $\psi^{-1}(D)$ is the incidence matrix of a symmetric (v, k, λ)-design. The set of group elements $\{d_1, ..., d_k\}$ with coefficient 1 in D is a *(v, k, λ)-difference set* in G: Every element $g \neq e_G$ in G has exactly λ representations as a quotient ("difference") $d_i \cdot d_j^{-1}$. It is not difficult to see from this discussion that any (v, k, λ)-difference set D gives rise to a symmetric (v, k, λ)-design defined via the incidence matrix $\psi^{-1}(D)$, where $D = \sum_{d \in D} d$. We shall identify a subset T of G with the group ring element $\sum_{g \in T} g$ which we also denote by T. Using this identification, the existence of a group invariant balanced weighing matrix $W(k, v)$ is equivalent to the existence of a decomposition of a (v, k, λ)-difference set and it is this decomposition that we call the *Waterloo decomposition*. For more background on difference sets we refer the reader to [5] or the recent survey [15] which includes a list of the (infinite) series of difference sets known theretofore. Two more series have been constructed since then; see [21, 22]. The surprising discovery of these difference sets indicates that it might be very difficult to determine all the difference sets or at least their parameters and it seems impossible to get a satisfactory answer regarding Problem A in full generality. It is more promising to restrict attention to some subclasses of difference sets. In this paper we will concentrate on the complements of the point–hyperplane designs of projective spaces.

Result 2.1. The point–hyperplane design of PG(d, q) admits a cyclic automorphism group acting sharply transitively on points and hyperplanes. In other words, there exist cyclic difference sets with parameters

$$\left(\frac{q^{d+1}}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$$

whose corresponding design is the point–hyperplane design of PG(d, q).

(A difference set in G is called cyclic if the group G is cyclic.) A proof of this result (which is due to Singer [20]) can be found in [5, Theorem III.6.2]. The difference set can be constructed as follows: Identify the vector space $\mathrm{GF}(q)^{d+1}$ with the field $\mathrm{GF}(q^{d+1})$ and the set of one-dimensional subspaces with $\mathrm{GF}(q^{d+1})^*/\mathrm{GF}(q)^*$. The cyclic group $\mathrm{GF}(q^{d+1})^*/\mathrm{GF}(q)^*$ induces an automorphism group of PG(d, q) which acts sharply transitively on points and hyperplanes. The hyperplanes of PG(d, q) are the sets $\pi(E_z)$, where $E_z = \{x\colon \mathrm{trace}(z \cdot x) = 0\}$ in $\mathrm{GF}(q^{d+1})^*$ and where π is the canonical epimorphism $\mathrm{GF}(q^{d+1})^* \to \mathrm{GF}(q^{d+1})^*/\mathrm{GF}(q)^*$. The trace function is the usual trace function of the Galois extension $\mathrm{GF}(q^{d+1})/\mathrm{GF}(q)$. The sets $\pi(E_z)$ are the *classical Singer difference* *sets*. In this paper we will not really distinguish the set $\pi(E_z)$ and E_z; however, the reader should keep in mind that a hyperplane of PG(d, q) is not, for instance, the set of elements with trace 0 but the image of this set under the projection π. It is important to note that *any* cyclic sharply transitive automorphism group of PG(d, q) arises in this way; see 1.4.17 in [7]. Alternatively, any two cyclic difference sets D and E in G corresponding to PG(d, q) are *equivalent*; i.e., there is an automorphism φ of G such that $\varphi(D) = E \cdot g$. The property of a difference set to admit a Waterloo decomposition is obviously invariant under this equivalence.

It is easy to see that the complement of a (v, k, λ)-difference set is a $(v, v-k, v-2k+\lambda)$-difference set and we say that $D(d, q)$ denotes the complement of "the" classical Singer difference set of Result 2.1. This difference set has the parameters $((q^{d+1}-1)/(q-1),\ q^d,\ q^d-q^{d-1})$.

PROBLEM B. Determine the difference sets $D(d, q)$ which have a Waterloo decomposition.

It will become clear very soon why this class of difference sets is most interesting in connection with Problem A (see the remarks in Section 1). We note that the balanced weighing matrix associated with $D(d, q)$ is a balanced weighing matrix $W(q^d, (q^{d+1}-1/(q-1))$. But first, we will formulate our main theorem.

Main Result. The difference set $D(d, q)$ has a decomposition $D(d, q) = A \cup B$ such that $(A-B) \cdot (A-B)^{(-1)} = q^d$ in $\mathbb{Z}G$ if and only if d is even.

Now we want to describe another approach to the Waterloo problem using relative difference sets. It is this approach that we will use to prove the necessary condition in our main theorem. A *relative* (m, n, k, λ)-*difference set* in a group G of order $m \cdot n$ is a k-subset R of G with the following property: Every element in $G-N$ has exactly λ representations $r \cdot r'^{-1}$ as a quotient with elements r, r' from R and no non-identity element in N has such a representation, where N is a normal subgroup of G of order n. We say that R is a difference set *relative* to N. In group ring notation, this means

$$R \cdot R^{(-1)} = k + \lambda \cdot (G-N) \qquad \text{in} \quad \mathbb{Z}G.$$

If U is a normal subgroup of G contained in N and if π denotes the canonical epimorphism $G \to G/U$ it is easy to see that $\pi(R) \cdot (\pi(R))^{(-1)} = k + \lambda\,|U| \cdot (G/U - N/U)$ in $\mathbb{Z}(G/U)$. The coefficients of $\pi(R)$ are still 0 and 1 and therefore $\pi(R)$ is a relative $(m, n/|U|, k, \lambda\,|U|)$-difference set. If $U = N$, then $\pi(R)$ is a $(m, k, n\lambda)$-difference set, see [8], where this argument has been used for the first time. In view of this projection argument we can think of a relative difference set as a *lifting* of a difference set in the usual sense. Moreover, in the same way as symmetric designs with a group G

acting sharply transitively on points and blocks correspond to difference sets, the incidence structure corresponding to a relative difference set is a (symmetric) *group divisible design*; see [13].

We say that R is a *splitting* relative difference set in G relative to N if $G = H \times N$. If $n = 2$, say $N = \{1, t\}$, and if R is splitting, we can write $R = A + B \cdot t$ in $\mathbb{Z}G$, where A and B are elements in $\mathbb{Z}H$. Since t has no representation as a quotient with elements from R, we have $A \cap B = \emptyset$, where A and B are interpreted as subset of H. We obtain immediately

$$A \cdot A^{(-1)} + B \cdot B^{(-1)} = k + \lambda \cdot (H - e_H)$$

and

$$A \cdot B^{(-1)} + B \cdot A^{(-1)} = \lambda \cdot (H - e_H),$$

where e_H denotes the identity element of H. This implies

$$(A - B) \cdot (A - B)^{(-1)} = k \tag{2.1}$$

and it shows that the existence of a splitting relative $(m, 2, k, \lambda)$-difference set gives rise to a Waterloo decomposition of the underlying $(m, k, 2\lambda)$-difference set and hence the existence of a group invariant balanced weighing matrix, see [17]. Conversely, the existence of a Waterloo decomposition of a (m, k, μ)-difference set D in H implies the existence of a splitting $(m, 2, k, \mu/2)$-relative difference set in $H \times N$ (put $R = A + B \cdot t$); see [17]. This gives a first necessary condition for the existence of a group invariant balanced weighing matrix $W(k, m)$: The λ-value of the underlying symmetric design (which is determined by k and m) has to be even. Moreover, k has to be a square (for proof, simply take the sum of the coefficients on both sides of (2.1) or, in terms of characters, apply the principal character to (2.1); see Section 3). For future reference, we state these conditions in the following proposition.

Proposition 2.2. ("trivial necessary conditions"). *If a group invariant balanced weighing matrix $W(k, m)$ exists, then k is a square and $\lambda = k \cdot (k-1)/(m-1)$ is even.*

If G is not of the form $H \times N$, i.e., if the relative difference set is non-splitting, we cannot construct a group invariant balanced weighing matrix. But it is still possible to construct a weighing matrix $W(k, m)$ as we will describe now: Let $g_1, ..., g_m$ be distinct coset representatives of the cosets of $N = \{1, t\}$ in G. We define $M = (m_{ij})$ through

$$m_{i,j} = \begin{cases} +1 & \text{if } \ g_i \cdot g_j^{-1} \in R \\ -1 & \text{if } \ t \cdot g_i \cdot g_j^{-1} \in R, \\ 0 & \text{otherwise.} \end{cases}$$

It is not difficult to check that M is a balanced weighing matrix $W(k, m)$, where the underlying incidence matrix $M^* := (|m_{i,j}|)$ is a group invariant matrix corresponding to the difference set $\pi(R)$ in G/N. If G is cyclic, say $G = \mathbb{Z}_{2m}$, and if $g_i = i$ in G, we obtain

$$\begin{aligned} m_{i,j} &= -m_{i',j'} && \text{if} \quad i - j = m + i' - j' \\ m_{i,j} &= m_{i',j'} && \text{if} \quad i - j = i' - j'. \end{aligned}$$

Matrices with these properties are called *negacyclic* (see [6]) and from negacyclic balanced weighing matrices it is possible to construct cyclic relative difference sets [6]. Let us summarize the foregoing discussion in the following theorem.

THEOREM 2.3. *The existence of a relative $(m, 2, k, \lambda)$-difference set R in G relative to N implies the existence of a balanced weighing matrix $W(k, m)$, say M. The underlying incidence matrix is invariant under the group G/N. If G is cyclic, then M is negacyclic, and if R is splitting, then M is group invariant with group G/N. Moreover, any negacyclic balanced weighing matrix $W(k, m)$ gives rise to a cyclic $(m, 2, k, \lambda)$-relative difference set and any group invariant balanced weighing matrix produces a splitting difference set.*

Some remarks are in order. If G is cyclic and m is odd we can construct both a negacyclic and a cyclic balanced weighing matrix out of the relative difference set. The notion of a balanced weighing matrix can be extended to generalized (balanced) weighing matrices M where the entries of M are elements of a group N. Again, difference sets relative to N give rise to generalized balanced weighing matrices. If the relative difference set is splitting then the generalized balanced weighing matrix is group invariant, too, and in the case of a cyclic relative difference set the balanced weighing matrix is ω-circulant; see [4, 13].

Theorem 2.3 suggests how we can try to construct balanced weighing matrices: We must look for relative difference sets with $n = 2$. We restrict to the case that the underlying symmetric design is the complement of the point–hyperplane design of PG(d, q). (If $d = 1$ this design is a trivial $(q + 1, q, q - 1)$-design since in this case points are just the same as hyperplanes.) The good news is that such a relative difference set always exists if q is odd.

Result 2.4. For any prime power q and any integer $d \geqslant 1$ there exists a cyclic relative difference set with parameters

$$\left(\frac{q^{d+1} - 1}{q - 1}, q - 1, q^d, \frac{q^d - q^{d-1}}{q - 1}\right)$$

such that underlying cyclic difference set is $D(d, q)$.

These difference sets are called the *classical affine difference sets.* For proof of Result 2.3, we refer to [13]. From that construction it is easy to see that the relative difference set projects onto $D(d, q)$. If q is odd, a projection argument yields cyclic

$$\left(\frac{q^{d+1}-1}{q-1}, 2, q^d, \frac{(q^d-q^{d-1})}{2}\right)\text{-relative difference sets.}$$

These examples are splitting if and only if d is even.

COROLLARY 2.5. *If q is odd, there exists a balanced weighing matrix $W(q^d, (q^{d+1}-1)/(q-1))$. This matrix can be constructed as a negacyclic matrix if d is odd and it can be circulant if d is even.*

If $d=1$ in the corollary above, we can say more.

Result 2.6 (Jungnickel [14]). Circulant balanced weighing matrices $W(m, m+1)$ do not exist, hence if $d=1$ in Corollary 2.5, there is no circulant balanced weighing matrix $W(q, q+1)$.

In view of Corollary 2.5, the main theorem in this paper is remarkable: There are always balanced weighing matrices $W(q^d, (q^{d+1}-1)/(q-1))$ with q odd no matter whether d is even or odd. The construction using projections of the classical affine difference sets produces not arbitrary balanced weighing matrices but negacyclic (d odd) and circulant (d even) matrices. Hence the proof of the main theorem has to use the fact that the weighing matrix is circulant (resp. the corresponding relative difference set is splitting) crucially. Moreover, we still have to find a construction for circulant balanced weighing matrices if q and d are both even in order to prove the theorem. In Section 4, we will give a construction that works for the q even and odd cases simultaneously.

3. PRELIMINARIES

In this section we will summarize several tools which are needed in the proof of our main theorem. We assume that G is an abelian group of exponent w. Let K be a field containing a primitive wth root of unity. Then there are exactly $|G|$ homomorphisms $G \rightarrow K^*$. These so called *characters* form the character group $\text{char}(G) \cong G$. Characters can be extended by linearity to homomorphisms from the group algebra KG into K. The importance of characters lies in the inversion formula.

Result 3.1 ("Inversion formula"). Let G be an abelian group of exponent w and K a field whose characteristic does not divide $|G|$ (i.e., the group algebra KG is semi-simple). If $A=\sum a_g g \in KG$ and K contains a primitive wth root of unity, then

$$a_g=\frac{1}{|G|}\cdot \sum_{\chi \in \operatorname{char}(G)} \chi(A)\cdot\chi(g^{-1}),$$

where $\operatorname{char}(G)$ denotes the group of complex characters of G.

This formula shows that the character values completely determine a group algebra element A and that there is an easy formula to recover A from its character values. Let us consider the following situation. The field K is $\mathbb{Q}(\zeta_w)$, where ζ_w is a primitive wth rooth of unity. The element $\chi(R)$ is an algebraic integer in $\mathbb{Q}(\zeta_w)$ and $\chi(R^{(-1)})=\overline{\chi(R)}$, where $^{-}$ denotes complex conjugation. Therefore an equation like $\chi(R)\cdot\overline{\chi(R)}=x$ can be interpreted as an equation for ideals

$$(\chi(R))(\overline{\chi(R)})=(x)$$

in the ring $\mathbb{Z}[\zeta_w]$ of algebraic integers of $\mathbb{Q}(\zeta_w)$ (for the necessary background from algebraic number theory we refer to [12]). If $M=A-B$ is the Waterloo decomposition of a (v, k, λ)-difference set in G, then we have

$$\chi(M)\,\overline{\chi(M)}=k. \tag{3.1}$$

The question is whether we can get any information about $\chi(M)$ from (3.1). This is the case if p^{2a} is the exact divisor of k (i.e., p^{2a+1} does not divide k) for some prime p which satisfies $p^f\equiv -1 \pmod{w}$ for a suitable $f\in\mathbb{Z}$ (in particular, p is relatively prime to w). In this case we say that p is *self-conjugate* modulo w. Using some arguments from number theory (see [18], for instance), we can conclude

$$\chi(M)\equiv 0 \qquad (\text{mod } p^a) \text{ in } \mathbb{Z}[\zeta_w].$$

Then Result 3.1 shows

$$M=p^aX$$

for a suitable element $X\in\mathbb{Z}G$, since $(p, w)=1$. Let us summarize this in the following result.

Result 3.2. Let G be an abelian group of exponent w and let p be a prime which is self-conjugate modulo w. If $A=\sum a_g g\in\mathbb{Z}G$ and

$$\chi(A)\,\overline{\chi(A)}\equiv 0 \qquad (\text{mod } p^{2a}) \text{ in } \mathbb{Z}[\zeta_w]$$

for all complex characters of G then $a_g\equiv 0 \pmod{p^a}$ for all $g\in G$.

For a direct proof of this result which avoids the use of algebraic number theory we refer to [15].

We finish this section with a result which is useful in order to construct circulant balanced weighing matrices. A proof (of a more general result) can be found in [9].

Result 3.3. Let Q be a non-degenerate quadric in $PG(d, q)$ with $d=2f$ and $|Q|=(q^d-1)/(q-1)$. Then the hyperplanes of $PG(d, q)$ intersect Q in sets of three sizes a, b, and c with respective multiplicities A, B, and C:

$$a=\frac{q^{2f-1}-1}{q-1}, \qquad A=\frac{q^{2f}-1}{q-1},$$

$$b=a-q^{f-1}, \qquad B=\frac{q^{2f}-q^f}{2},$$

$$c=a+q^{f-1}, \qquad C=\frac{q^{2f}+q^f}{2}.$$

The A hyperplanes with intersection size a are the tangent hyperplanes.

4. Proof of the Main Theorem

We begin the proof of our main result with a proof of the sufficiency of our condition. Hence we have to construct appropriate relative difference sets with $n=2$ or Waterloo decompositions of $PG(d, q)$ with d even.

Theorem 4.1. *Let q be a prime power and d an even integer $d \geqslant 2$. Then there exists a circulant balanced weighing matrix $W(q^d, (q^{d+1}-1)/(q-1))$ such that the corresponding symmetric design is the complement of the point–hyperplane design of* $PG(d, q)$. *Equivalently, the difference set $D(d, q)$ admits a Waterloo decomposition.*

Proof. We will construct the Waterloo decomposition of the complement of the difference set E which "consists" of the non-zero elements z of trace 0 in the Galois extension $GF(q^{d+1})/GF(q)$. More precisely, the difference set E consist of elements in the quotient group $GF(q^{d+1})^*/GF(q)^*$; see the remarks following Result 2.1. First of all, we show that the following sets are non-degenerate quadrics in $PG(d, q)$:

$$Q_e=\{z \in GF(q^{d+1})^* : \text{trace}(z^{q+1})=0\} \qquad \text{if } q \text{ is even},$$

$$Q_o=\{z \in GF(q^{d+1})^* : \text{trace}(z^2)=0\} \qquad \text{if } q \text{ is odd}.$$

It is obvious that the elements in Q_o satisfy a quadratic equation. The same is true for the elements in Q_e: We choose a normal basis $\{\alpha^{q^i}: i=0, ..., d\}$ of $\mathrm{GF}(q^{d+1})/\mathrm{GF}(q)$. If $z=\sum a_i\alpha^{q^i}$ we get

$$\begin{aligned} \operatorname{trace}(z^{q+1}) &= \operatorname{trace}\left[\left(\sum a_i\alpha^{q^i}\right)\cdot\left(\sum a_i\alpha^{q^{i+1}}\right)\right] \\ &= \operatorname{trace}\left(\sum b_{i,j}\alpha^{q^i}\alpha^{q^j}\right) \\ &= \sum (b_{i,j}\operatorname{trace}(\alpha^{q^{\mu i}}\alpha^{q^j})], \end{aligned}$$

where the $b_{i,j}$'s are quadratic expressions in the a_i's. In order to prove that the quadrics Q are non-degenerate we have to show that there is no point $z\in Q$ with the property

$$x\in Q \Rightarrow (z+x)\in Q \qquad (\text{for all } x\in Q)$$

since in this case each line through z would intersect the quadric either in only one point or the line would be contained in Q (and Q would be degenerate).

Let us first consider the q *even* case and assume that $z\in Q_e$ satisfies for all $x\in Q_e$:

$$\begin{aligned} 0 &= \operatorname{trace}(z+x)^{q+1} \\ &= \operatorname{trace}(z^{q+1})+\operatorname{trace}(x^{q+1})+\operatorname{trace}(z^qx)+\operatorname{trace}(x^qz) \\ &= \operatorname{trace}(z^qx)+\operatorname{trace}(x^qz). \end{aligned}$$

But then $\operatorname{trace}(x\cdot(z^q+z^{q^{-1}}))=0$ for all $x\in Q_e$. In other words: If $z^q+z^{q^{-1}}\neq 0$ the quadric Q_e would be (for reasons of cardinality) the hyperplane $\{x: \operatorname{trace}(x\cdot(z^q+z^{q^{-1}}))=0\}$. But Q_e is not a hyperplane since $q+1$ is never a multiplier of a Singer difference set (see [3]), thus $z^q+z^{q^{-1}}$ has to be 0, equivalently $z^{q^2}=z$ (note that q is even). This shows that $z\in\mathrm{GF}(q)$ since there is no quadratic extension of $\mathrm{GF}(q)$ in $\mathrm{GF}(q^{d+1})$ (since $d+1$ is odd). But we have $\operatorname{trace}(y)=y$ for elements in $\mathrm{GF}(q)$, therefore $\operatorname{trace}(z)\neq 0$, contradicting $z\in Q_e$.

The case q *odd* is similar: $\operatorname{trace}(z+x)^2=2\cdot\operatorname{trace}(zx)$ (if $\operatorname{trace}(z^2)=\operatorname{trace}(x^2)=0$) and hence the quadric Q_o would again be a hyperplane which is absurd since 2 is not a multiplier (see [3]).

It is known that there is exactly one tangent hyperplane T_z through each point z of a non-degenerate quadric. The hyperplane T_z is defined via the property that a line through z (in T_z) that meets the quadric Q in a point different from z is contained in Q. We consider the case q *even* first: the points x in $T_z\cap Q_e$ must satisfy $\operatorname{trace}(z^qx)+\operatorname{trace}(x^qz)=0$. This holds for

$T_z := \{x\colon \mathrm{trace}(x \cdot (z^q + z^{q^{-1}})) = 0\}$. Since $\mathrm{trace}(z^q) = \mathrm{trace}(z^{q^{-1}})$ we have $\mathrm{trace}(z^q + z^{q^{-1}}) = 0$; therefore $\{z^q + z^{q^{-1}}\colon z \in Q_e\} = \{z\colon \mathrm{trace}(z) = 0\}$. Note that $T_z \neq T_{z'}$ for $z \neq z'$; hence the set on the left-hand side of the equation above has the same cardinality as the "trace 0"-hyperplane E. Using this difference set E we can say that the set of tangent hyperplanes are $\{E \cdot z^{-1}\colon z \in E\}$.

Now we have to use the following observation: Let A and B denote group ring elements (over the integers) corresponding to subsets of a group G, then $|A \cdot x^{-1} \cap B| = (A \cdot B^{(-1)})_x$ (coefficient of x in $A \cdot B^{(-1)}$). We obtain the equation in $\mathbb{Z}G$ using Result 3.3 (with $d = 2f$),

$$E \cdot Q_e^{(-1)} = a \cdot G + q^{f-1} \cdot (A - B) = X, \qquad \text{say},$$

where A and B denote two disjoint subsets with $A \cup B = G - E = D(d, q)$ and E is the "trace 0"-hyperplane. We will show $(A - B) \cdot (A - B)^{(-1)} = q^{2f}$ by computing $X \cdot X^{(-1)}$ (here $n = q^{2f-1}$ is the order of the point–hyperplane design):

$$\begin{aligned} X \cdot X^{(-1)} &= (n + a \cdot G) \cdot (n + a \cdot G) = n^2 + t \cdot G \\ &= s \cdot G + q^{(2f-2)} \cdot (A - B) \cdot (A - B)^{(-1)} \\ &\qquad \text{for suitable} \quad s, t \in \mathbb{Z}. \end{aligned}$$

We have $t = 2na + a^2 v$ and $s = a^2 v + 2aq^{f-1}q^f$ and therefore $s = t$. This shows that the complement $D(d, q)$ $(d = 2f)$ of the classical Singer difference set in $\mathrm{PG}(2f, q)$ with q even admits a Waterloo decomposition $D(d, q) = A \cup B$.

The case q *odd* needs some modification: The tangent hyperplane through $z \in Q_o$ is $\{x\colon \mathrm{trace}(xz) = 0\} = E \cdot z^{-1}$, where $E = \{x\colon \mathrm{trace}(x) = 0\}$. We obtain the equation

$$E \cdot Q_o^{(-1)} = a \cdot G + q^{f-1} \cdot (A - B),$$

but now $A \cup B = G - Q_o$ and we would get a decomposition of the complement of Q_o. But Q_o itself is a difference set equivalent to E and that is enough to prove our theorem. ▌

Two balanced weighing matrices M_1 and M_2 are said to be *equivalent* if two generalized permutation matrices exist such that $P \cdot M_1 \cdot Q = M_2$. A matrix $P = (p_{i,j})$ is a *generalized permutation matrix* if P is a $(0, -1, +1)$-matrix and $(|p_{i,j}|)$ is a permutation matrix. In other words: We can obtain M_2 from M_1 via a row and column permutation and (possibly) multiplication of some rows and columns with -1. In terms of the corresponding group divisible designs, this means that the designs are isomorphic. The question arises how many equivalence classes of balanced weighing matrices corresponding to $D(d, q)$ exist. There are at least two constructions for these matrices: The one which we have just presented and those coming via projection from the classical affine difference sets (see remarks following Result 2.4). In some small cases ($D(2, 3)$ and $D(2, 5)$) we have checked that our two constructions yield isomorphic designs. However, the table in [16] shows that there is in general more than just one equivalence class, in particular there are other matrices corresponding to $D(2, 3)$ and $D(2, 5)$. (We note that the relative difference sets with parameters $(13, 2, 9, 3)$ and $(31, 2, 25, 10)$ in [16] are liftings of $D(2, 3)$ and $D(2, 5)$.). This is in contrast to the case of negacyclic conference matrices (which are negacyclic matrices where the underlying design is a $(q+1, q, q-1)$-design). The authors of [6] conjecture that there is just one equivalence class of balanced weighing matrices $W(q, q+1)$ with q (necessarily) an odd prime power (constructed via projection from the classical affine $(q+1, q-1, q, 1)$-difference sets). This problem and the question whether q *has* to be a prime power is still open.

We are now going to prove the necessary condition in our main theorem.

THEOREM 4.2. *Let q be a prime power and let d be an odd integer, $d \geqslant 1$. Then no circulant balanced weighing matrix $W(q^d, (q^{d+1}-1)/(q-1))$ exists; equivalently, no splitting relative $((q^{d+1}-1)/(q-1), 2, q^d, (q^d-q^{d-1})/2)$-difference set exists.*

Proof. Let M be the Waterloo decomposition of a cyclic $((q^{d+1}-1)/(q-1), q^d, q^d-q^{d-1})$-difference set where d is odd. We write $d=2a-1$ and denote by p the prime satisfying $q=p^\alpha$ for some α. Since the k-value of the difference set must be a square (Proposition 2.2), α is even. We may select a subgroup U of H of order $(q^a-1)/(q-1)$ and index $u=q^a+1$ in H. We extend the natural epimorphism from H onto $K=H/U$ to $\mathbb{Z}H$, and let the image of M under this map be $\bar{M}$. We obtain

$$\bar{M} \cdot \bar{M}^{(-1)} = q^d.$$

But p is self-conjugate modulo u, hence we can apply Result 3.2 to show that the coefficients of $\bar{M}$ are divisible by $q^{d/2}$. But on the other hand, the coefficients are bounded by $|U|$, since M has only coefficients 0 and ± 1. The easy inequality

$$q^{d/2} = q^{(2a-1)/2} > (q^a-1)/(q-1) = |U| \qquad \text{for} \quad q \geqslant 3$$

implies $\bar{M}=0$. But this contradicts $\bar{M} \cdot \bar{M}^{(-1)} = q^d$ and proves the theorem. ▌

It is worthwhile to mention that we did not need the fact that the underlying design of the putative balanced weighing matrix is the complementary point–hyperplane design. Moreover, the proof shows that no abelian difference set with the parameters stated in Theorem 4.2 admits a Waterloo decomposition and not just the cyclic ones (although the only known abelian difference sets with these parameters are cyclic).

5. Remarks

We have already indicated in the Introduction why we have restricted ourselves to the case of the complementary Singer difference sets $D(d, q)$. A systematic investigation of other series of difference sets and their possible liftings is in [1]. Let us mention only the following result from [1].

Result 5.1. There are no splitting relative difference sets with $n=2$ which are liftings of difference sets with parameters

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right).$$

There are cyclic difference sets with parameters $((q^{d+1}-1)/(q-1), q^d, q^d-q^{d-1})$ whose corresponding design is *not* the complement of the point–hyperplane design of $\mathrm{PG}(d, q)$; see [3]. There are an infinite series due to Gordon, Mills, and Welch [10] and several sporadic examples. What can we say about "liftings" of these difference sets? Let us begin with the sporadic examples in Baumert's table. We have checked that only one of the six inequivalent (127, 64, 32)-difference sets admits a lifting with $n=2$, namely $D(6, 2)$: There are four inequivalent circulant balanced weighing matrices $W(64, 127)$ corresponding to $D(6, 2)$. There are altogether six inequivalent circulant balanced weighing matrices $W(81, 121)$ corresponding to the four inequivalent (121, 81, 54)-difference sets in [3] (here $d=4$ and $q=3$). The difference sets $\#A$ (classical Singer difference set) and $\#D$ each give rise to inequivalent circulant balanced weighing matrices.

A construction in [2] shows that the GMW-difference sets with d even and q odd admit liftings to splitting relative difference sets with $n=2$. The situation is quite similar to the classical case: One can generalize the construction of Gordon, Mills, and Welch [10] to relative difference sets and the result just mentioned follows by a projection argument. There are negacyclic balanced weighing matrices corresponding to GMW-difference sets whenever q is odd (as in the case of the classical Singer difference sets). The more interesting question whether the GMW-difference sets with d even and q even admit splitting liftings with $n=2$ is still open.

ACKNOWLEDGMENT

The authors thank the referee for pointing out a simplified proof of Theorem 4.2.

REFERENCES

1. K. T. ARASU, D. JUNGNICKEL, S. L. MA, AND A POTT, Relative difference sets with $n = 2$, *Discrete Math.*, in press.
2. K. T. ARASU AND A. POTT, Sequences derived from GMW-sequences, in preparation.
3. L. D. BAUMERT, "Cyclic Difference Sets," Lecture Notes, Vol. 182, Springer-Verlag, Berlin/Heidelberg/New York, 1971.
4. G. BERMAN, Families of generalized weighing matrices, *Canad. J. Math.* **30** (1978), 1016–1028.
5. T. BETH, D. JUNGNICKEL, AND H. LENZ, "Design Theory," Cambridge Univ. Press, Cambridge, 1986.
6. P. DELSARTE, J. M. GOETHALS, AND J. J. SEIDEL, Orthogonal matrices with zero diagonal II, *Canad. J. Math.* **23** (1971), 816–832.
7. P. DEMBOWSKI, "Finite Geometries," Springer-Verlag, Berlin/Heidelberg/New York, 1968.
8. J. E. H. ELLIOTT AND A. T. BUTSON, Relative difference sets, *Illinois J. Math.* **10** (1966), 517–531.
9. R. A. GAMES, The geometry of quadrics and correlations of sequences, *IEEE Trans. Inform. Theory* **32** (1986), 423–426.
10. B. GORDON, W. H. MILLS, AND L. R. WELCH, Some new difference sets, *Canad. J. Math.* **14** (1962), 614–625.
11. J. W. P. HIRSCHFELD, "Projective Geometries over Finite Fields," Oxford Univ. Press, Oxford, 1979.
12. L. K. HUA, "Introduction to Number Theory," Springer-Verlag, Berlin/Heidelberg/New York, 1982.
13. D. JUNGNICKEL, On automorphism groups of divisible designs, *Canad. J. Math.* **24** (1982), 257–297.
14. D. JUNGNICKEL, On automorphism groups of divisible designs. II. Group invariant generalised conference matrices, *Arch. Math.* **54** (1990), 200–208.
15. 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.
16. C. W. H. LAM, On relative difference sets, *in* "Proceedings, 7th Manitoba Conference on Number Math. and Computing, 1977," pp. 445–474.
17. R. C. MULLIN AND R. G. STANTON, Group matrices and balanced weighing designs, *Utilitas Math.* **8** (1975), 277–301.
18. A. POTT, "Finite Geometry and Character Theory," Berlin/Heidelberg/New York, Lecture Notes 1601, Springer-Verlag, 1995.
19. P. J. SCHELLENBERG, A computer construction for balanced orthogonal matrices, *in* "Proceedings, 6th Southeastern Conference on Combinatorics, Graph Theory and Computing, 1975," pp. 513–522.
20. J. SINGER, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. soc.* **43** (1938), 377–385.
21. K. SMITH, Non-abelian Hadamard difference sets, *J. Comb. Theory Ser. A* **70** (1995), 144–156.
22. M.-Y. XIA, Some infinite classes of special Williamson matrices and difference sets, *J. Combin. Theory Ser. A* **61** (1992), 230–242.