UNIVERSITÀ DEGLI STUDI DI ROMA
"LA SAPIENZA"

Balanced Generalized Weighing Matrices and Related Structures

Dieter Jungnickel

Quaderni Elettronici del Seminario di Geometria Combinatoria
16E (Febbraio 2005)

http://www.mat.uniroma1.it/~combinat/quaderni

Dipartimento di Matematica "Guido Castelnuovo"
P.le Aldo Moro, 2 - 00185 Roma - Italia

Balanced Generalized Weighing Matrices and Related Structures

Dieter Jungnickel
Lehrstuhl für Diskrete Mathematik, Optimierung
und Operations Research
Universität Augsburg
D–86135 Augsburg
Germany
jungnickel@math.uni-augsburg.de

Abstract

Balanced generalized weighing matrices include well-known classical combinatorial objects such as Hadamard matrices and conference matrices; moreover, particular classes of BGW-matrices are equivalent to certain relative difference sets. BGW-matrices admit an interesting geometrical interpretation, and in this context they generalize notions like projective planes admitting a full elation or homology group. After explaining these basic connections in detail, we will restrict attention to proper BGW-matrices; thus we will not give any systematic treatment of generalized Hadamard matrices, which are the subject of a large area of research in their own right.

In particular, we will discuss what is usually called the *classical* parameter series. Here the nicest examples are closely related to perfect codes and to some classical relative difference sets associated with affine geometries; moreover, the matrices in question can be characterized as the unique (up to equivalence) BGW-matrices for the given parameters with minimum q-rank. One can also obtain a wealth of monomially inequivalent examples and determine the q-ranks of all these matrices by exploiting a connection with linear shift register sequences.

There are also many applications of BGW-matrices to constructions of designs and graphs; we will restrict ourselves to just one construction method for symmetric designs due to Yury Ionin, for which we will work out an example in detail.

1 Basic facts

We will assume familiarity with some basic facts and notions from coding theory and combinatorial design theory; see, for instance, [7] and [61]. Moreover, we will also require some background concerning finite fields and shift register sequences; for this we refer to [49] and [42].

We start with the definition of a *partial difference matrix* introduced in 1982 by the author [41], using additive notation. In view of the examples we shall concentrate on later, we prefer to switch to multiplicative notation here. In addition, our notation differs in a further aspect from that in [41]: there we used the parameter $\lambda = \mu/|G|$ instead of μ; the change has been made to be consistent with the standard terminology for the special case of BGW-matrices.

Definition 1.1 Let G be a multiplicatively written group, and let 0 be a symbol not contained in G. A *partial difference matrix* $PDM(m, k, \mu)$ over G is an $m \times \beta$ matrix[1] $D = (d_{ij})$ with entries from $\overline{G} = G \cup \{0\}$ satisfying the following two conditions:

- Each column of D contains exactly k nonzero entries.
- For all $a, b \in \{1, \ldots, m\}$ with $a \neq b$, the multiset

$$\left\{d_{ai}d_{bi}^{-1} \colon 1 \leq i \leq \beta,\ d_{ai}, d_{bi} \neq 0\right\}$$

  contains exactly $\mu/|G|$ copies of each element of G.

If there are no entries 0 (that is, for $k = m$) one speaks of a *difference matrix*. Such matrices are an extremely important tool for constructing sets of mutually orthogonal Latin squares; see [7, §VIII.3].

Partial difference matrices are usually called *generalized Bhaskar Rao designs*, as the special case of *Bhaskar Rao designs* (where G is the cyclic group of order 2) goes back to Bhaskar Rao [8, 9]. The more general concept was introduced in 1982 by Seberry [58]; in the same year [41] finally appeared, after having been submitted at the end of 1979.

We mention the following simple but useful observation [41, Lemma 6.6]:

Proposition 1.2 *Let D be a $PDM(m, k, \mu)$ over G, and let H be a normal subgroup of G of order s. Then there also exists a $PDM(m, k, \mu)$ over G/H.*

[1] We have not included β into the list of parameters, since its value can be computed from the remaining parameters – as we will see below.

Proof. Write $D = (d_{ij})$, and replace each non-zero entry d_{ij} by its coset $d_{ij}H$. $\square$

Corollary 1.3 *The existence of a $PDM(m,k,\mu)$ over some group G of order m implies that of an (m,k,μ)-design.*

Proof. Take $H = G$ in 1.2 – that is, replace each non-zero entry of the given $PDM(m,k,\mu)$ by 1 – to obtain the incidence matrix of the desired design. $\square$

The preceding corollary immediately yields the following two additional properties of BGW-matrices, where we write $n = |G|$:

- Each row of D contains exactly $r = \mu(m-1)/(k-1)$ nonzero entries.
- D has exactly $\beta = \mu m(m-1)/k(k-1)$ columns.

In case $r > \mu = n\lambda$, Fisher's inequality applied to $\boldsymbol{\mathcal{D}}$ yields $\beta \geq m$; and for $r = \mu = n\lambda$, we get $k = m$, and then a well-known result on difference matrices gives the same conclusion; see [39] or [7, Corollary VIII.3.7]. As usual, the case of equality is of particular interest:

Definition 1.4 Let G be a multiplicatively written group. A partial difference matrix $PDM(m,k,\mu)$ over G satisfying $\beta = m$ is called a *balanced generalized weighing matrix* $BGW(m,k,\mu)$ over G. If there are no entries 0 (that is, for $k = m = \beta$) one speaks of a *generalized Hadamard matrix* of order m over G and uses the notation $GH(n,\lambda)$, where $n = |G|$ and $\lambda = m/n$. Finally, any $BGW(n+1,n,n-1)$ is called a *generalized conference matrix.*

Let us choose G as the cyclic group of order 2, written as $G = \{1,-1\}$. Then the three notions above reduce to balanced weighing matrices [54], Hadamard matrices, and conference matrices, respectively, which explains the preceding terminology; we refer the reader to the relevant sections in [12] and the references given there for more on these objects. We now give two small examples over the cyclic group of order 3, written as $G = \{1,\omega,\omega^2\}$:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & 1 & \omega^2 & 1 & \omega \\ \omega & 1 & \omega^2 & \omega^2 & \omega & 1 \\ 1 & \omega^2 & \omega^2 & 1 & \omega & \omega \\ \omega^2 & \omega^2 & 1 & \omega & \omega & 1 \\ \omega^2 & 1 & \omega^2 & \omega & 1 & \omega \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & \omega & \omega & 1 \\ 1 & 0 & 1 & \omega & \omega \\ \omega & 1 & 0 & 1 & \omega \\ \omega & \omega & 1 & 0 & 1 \\ 1 & \omega & \omega & 1 & 0 \end{pmatrix}$$

are a generalized Hadamard and a generalized conference matrix, respectively, namely a $GH(3,2)$ and a $BGW(5,4,3)$ over G.

The following important result is due to [11] (using different language). We write $D^{(-1)}$ for the matrix arising from D by replacing each group element g by its inverse g^{-1}, and we denote the transpose of $D^{(-1)}$ by D^*.

Theorem 1.5 *Let G be a finite group. If D is a $BGW(m,k,\mu)$ over G, then so is D^*.* □

Theorem 1.5 may be proved algebraically by using group rings; see [38]. We shall give a combinatorial proof taken from [40]; as this will require some preparations, we postpone the proof of Theorem 1.5 to Section 4. Actually, we shall prove a somewhat stronger result; see Theorem 4.2.

At this point, we mention two non-existence results due to [16]; their proof needs the machinery of group rings and will therefore not be included.

Theorem 1.6 *Suppose the existence of a $BGW(m,k,\mu)$ over a group G of order n. Then we have the following restrictions:*

- *If m is odd and n is even, k must be a square.*
- *If G admits an epimorphism onto a cyclic group of odd prime order p and if h is an integer which divides the squarefree part of k but is not a multiple of p, then the order of h modulo p must be odd.* □

In view of Corollary 1.3 it is a natural to ask if a given (m,k,μ)-design can be obtained from some $PDM(m,k,\mu)$ over a suitable group G of order n, preferably for as large a value of n as possible. In other words, given the incidence matrix M of an (m,k,μ)-design $\boldsymbol{\mathcal{D}}$ and a group G of order n, we would like to know if it is possible to obtain a $PDM(m,k,\mu)$ by replacing all entries 1 in M in a suitable manner with elements of G. In view of the seminal case of the cyclic group of order 2, written as $G=\{1,-1\}$, this process is often referred to as *signing* M (or, by abuse of language, $\boldsymbol{\mathcal{D}}$). Hence the existence problem for partial difference matrices – and, in particular, for balanced generalized weighing matrices – can be viewed as the problem of determining which designs – in particular, which symmetric designs – are *signable* over which groups.

Indeed, BGW-matrices (and generalized Bhaskar Rao designs) have often been studied from the point of view just outlined (compare, for instance, the title of [26]); see the relevant sections in [12] for further references. We shall discuss this problem for a particular parameter series in some detail in Section 7. Quite often, one also requires additional conditions: for instance, if the given incidence matrix is circulant, one might want a signing which retains this property. The rather well-known *Waterloo problem* falls into this category; see [54, 2, 3].

2 Related geometries, I: Class regular divisible designs

We now turn our attention to connections between balanced generalized weighing matrices (and, more generally, partial difference matrices) and finite geometries. The most fundamental one of these is the equivalence of partial difference matrices to certain divisible designs. Recall that a *divisible design* $\boldsymbol{\mathcal{D}}$ with parameters (m, n, k, λ) is an incidence structure consisting of $v = mn$ points, partitioned into m classes of n points each, together with a set of blocks of size k each such that

- each block meets each point class at most once;
- any two points in distinct classes are on exactly λ common blocks.[2]

Standard counting arguments establish the following additional two properties:

- each point of $\boldsymbol{\mathcal{D}}$ is on exactly $r = \lambda(m-1)n/(k-1)$ blocks;
- the total number of blocks is $b = \lambda m(m-1)n^2/k(k-1)$.

A *square* divisible design has $b = mn$; if $\boldsymbol{\mathcal{D}}$ is actually isomorphic to its dual design $\boldsymbol{\mathcal{D}}^*$ (which is, as usual, obtained by interchanging the roles of points and blocks), one speaks of a *symmetric* divisible design.

One calls a divisible design *class regular* if it admits an automorphism group G which acts regularly on each point class. The following observation is [41, Lemma 6.2].

Lemma 2.1 *Let $\boldsymbol{\mathcal{D}}$ be a class regular divisible design (with respect to G). Then G acts semiregularly on the block set of $\boldsymbol{\mathcal{D}}$. Moreover, the blocks in any given orbit of G are pairwise disjoint.*

[2]There is a more general notion of divisible design or GDD where points in the same class are joined by a constant number λ' of blocks; see [7]. For our purposes, the special case given here (where $\lambda' = 0$) suffices.

Proof. Assume $B = B^\sigma$ for some block B of $\boldsymbol{\mathcal{D}}$ and some $\sigma \in G$. Choose a point $p \in B$; then p, $p^\sigma \in B^\sigma$. As each block B meets each point class of $\boldsymbol{\mathcal{D}}$ at most once, we conclude $p = p^\sigma$. By the class regularity of $\boldsymbol{\mathcal{D}}$, we have $\sigma = 1$. Thus G acts semiregularly on the block set.

Now consider two blocks in the same orbit, say B and B^σ. If these two blocks intersect in a point p, the same argument as before again shows $p = p^\sigma$ and then $\sigma = 1$. In other words, each block orbit constitutes a partial parallel class for $\boldsymbol{\mathcal{D}}$. □

We now prove the following simple but fundamental result also established in [41]:

Theorem 2.2 *The existence of a $PDM(m, k, \mu)$ over a group G of order n is equivalent to that of a divisible design with parameters (m, n, k, λ) admitting G as a class regular automorphism group, where $\lambda = \mu/n$.*

Proof. Let $D = (d_{ij})$ be a $PDM(m, k, \mu)$ over G (with β columns) and define $\boldsymbol{\mathcal{D}}$ as follows. The point set of $\boldsymbol{\mathcal{D}}$ is the union of the classes

$$V_i \;=\; \{(i, x) \colon\, x \in G\} \qquad (i = 1, \ldots, m),$$

and the blocks are the sets B_{jg} ($j = 1, \ldots, \beta$; $g \in G$), where

$$B_{jg} \;=\; \{(i, d_{ij}g) \colon\, i = 1, \ldots, m,\ d_{ij} \neq 0\}.$$

Clearly, each block meets each point class at most once. As each column of D contains exactly k nonzero entries, all blocks have size k. Now let (h, x), (i, y) with $h \neq i$ be given. Then (h, x), $(i, y) \in B_{jg}$ iff $x = d_{hj}g$ and $y = d_{ij}g$, that is iff $xy^{-1} = d_{hj}d_{ij}^{-1}$ and $g = d_{hj}^{-1}x$. Hence the number of blocks through (h, x) and (i, y) is the number of indices j with $d_{hj}d_{ij}^{-1} = xy^{-1}$ and, hence, equals $\lambda = \mu/n$, as required. Moreover, the divisible design $\boldsymbol{\mathcal{D}}$ is clearly class regular with respect to G if we let $y \in G$ act by

$$(i, x) \mapsto (i, xy), \quad B_{jg} \mapsto B_{j,gy}.$$

Conversely, let $\boldsymbol{\mathcal{D}}$ be a divisible design with parameters (m, n, k, λ) admitting G as a class regular automorphism group. By definition, G acts regularly on each point class of $\boldsymbol{\mathcal{D}}$; hence we may choose a *base point* p_i in each point class V_i ($i = 1, \ldots, m$) and label the point p_i^x as (i, x) (for $x \in G$). By Lemma 2.1, G acts semiregularly on the block set of $\boldsymbol{\mathcal{D}}$; thus the block set splits into β block orbits $\boldsymbol{\mathcal{B}}_1, \ldots, \boldsymbol{\mathcal{B}}_\beta$, where $\beta = b/n = \lambda m(m-1)n/k(k-1)$, and G acts regularly on each of these orbits. Hence we may choose a *base block* $B_j \in \boldsymbol{\mathcal{B}}_j$

(for $j = 1, \ldots, \beta$) and label the block B_j^g as B_{jg} (for $g \in G$). We now define an $m \times \beta$ matrix $D = (d_{ij})$ over $\overline{G} = G \cup \{0\}$ by putting

$$d_{ij} = x \in G \quad \Longleftrightarrow \quad (i, x) \in B_j = B_{j1},$$

and $d_{ij} = 0$ otherwise. Similar arguments as in the first part of the proof show that D is the desired $PDM(m, k, \mu)$ over G. $\square$

3 A detour: Square divisible designs with disjoint blocks

In view of Lemma 2.1, it is interesting to study the properties of disjoint blocks in square divisible designs. The subsequent results are due to the author [40], generalizing previous work of Hine and Mavron [27] for the special case of transversal designs (that is, divisible designs for which each block meets each point class).

In what follows, we shall write $[p, q]$ to denote the number of blocks joining two distinct points p and q; similarly, $[B, C]$ denotes the number of points shared by two distinct blocks B and C. The fundamental fact we need is as follows:

Lemma 3.1 *Let B and C be two disjoint blocks of a square divisible design $\boldsymbol{\mathcal{D}}$ with parameters (m, n, k, λ). Then B and C meet the same point classes. Moreover, $[B, X] = [C, X]$ for each block $X \neq B, C$.*

Proof. We use the abbreviations $\beta_X = [B, X]$ and $\gamma_X = [C, X]$. Counting the double flags (p, q, X) with $p \in B$ and $q \in C$ yields

$$\sum_X \beta_X \gamma_X \ = \sum_{p \in B, q \in C} [p, q], \tag{1}$$

where X runs over all blocks distinct from B and C. As each block meets each point class at most once, at most one point $q \in C$ can be in the same class as a given point $p \in B$, and thus at least $k - 1$ points of C have to be joined to p. Hence equation (1) implies the inequality

$$\sum_X \beta_X \gamma_X \ \geq \ \lambda k(k-1), \tag{2}$$

and equality holds if and only if B and C meet exactly the same point classes. Thus it will suffice to establish the reverse inequality to prove the first assertion.

Counting the flags and double flags containing a specified block yields the equations

$$\sum_X \beta_X \;=\; \sum_X \gamma_X \;=\; k(k-1) \tag{3}$$

and

$$\sum_X \beta_X(\beta_X - 1) \;=\; \sum_X \gamma_X(\gamma_X - 1) \;=\; (\lambda-1)k(k-1), \tag{4}$$

respectively, and hence

$$\sum_X \beta_X^2 \;=\; \sum_X \gamma_X^2 \;=\; \lambda k(k-1). \tag{5}$$

Hence

$$0 \;\leq\; \sum_X (\beta_X - \gamma_X)^2 \;=\; 2\lambda k(k-1) - 2\sum_X \beta_X\gamma_X, \tag{6}$$

which is the desired reverse inequality of (2). Then we also have equality in (6), which establishes the second assertion. □

Let us call two blocks B and C *equivalent*, written $B \sim C$, provided that either $B = C$ or $[B, C] = 0$. Lemma 3.1 immediately implies the following result.

Corollary 3.2 *Let $\boldsymbol{\mathcal{D}}$ be a square divisible design. Then $\sim$ is an equivalence relation on the block set of $\boldsymbol{\mathcal{D}}$, and the intersection number of any two blocks only depends on their equivalence classes.* □

We also need a bound on the size of the equivalence classes:

Lemma 3.3 *Let $\boldsymbol{\mathcal{D}}$ be a square divisible design with parameters (m, n, k, λ). Then any equivalence class of blocks has at most size n, and equality holds if and only if every block not contained in the given class meets all blocks of the class in exactly λ points.*

Proof. Let us consider the equivalence class of a specified block B. We will use some of the equations obtained in the proof of Lemma 3.1, but restrict the summations to those blocks X which meet B; let d be the number of such X. Using equations (3) and (5), we obtain

$$0 \;\leq\; \sum_X (\beta_X - \lambda)^2 \;=\; \lambda k(k-1) - 2\lambda k(k-1) + \lambda^2 d. \qquad (7)$$

By definition, a square divisible design has $v = b$ and hence also $k = r$, so that the standard equation for r given in the previous section becomes $k(k-1) = \lambda(m-1)n$. Then inequality (7) simplifies to $d \geq (m-1)n$, and hence there are at most $n-1$ blocks disjoint from B; in other words, the equivalence class of B has size at most n. By (7), equality holds if and only if each block intersecting B does so in exactly λ points. □

Combining Corollary 3.2 and Lemma 3.3, we obtain the following useful characterization of symmetric divisible designs. In later sections, we will see two applications of this result.

Theorem 3.4 *Let $\boldsymbol{\mathcal{D}}$ be a square divisible design with parameters (m, n, k, λ). Then the following statements are equivalent:*

- *$\boldsymbol{\mathcal{D}}$ is symmetric.*
- *All block classes of $\boldsymbol{\mathcal{D}}$ have size n.*
- *Any two blocks of $\boldsymbol{\mathcal{D}}$ are either disjoint or intersect in precisely λ points.*

It should be noted that a celebrated result of Connor [13] guarantees that *every* square divisible design is actually symmetric provided that $k \neq m$ and that k and λ are coprime. However, there are infinite families of square divisible designs (both with $k \neq m$ and with $k = m$) which are not symmetric; see [46]. As we shall see later, in our context Theorem 3.4 is just what is needed.

4 Related geometries, II: Back to class regular divisible designs

We now return to class regular divisible designs. Using the results of the previous sections, we can prove the following theorem of [41]:

Theorem 4.1 *Let $\boldsymbol{\mathcal{D}}$ be a class regular divisible design with parameters (m,n,k,λ) and b blocks. Then $b \geq v$; and if $\boldsymbol{\mathcal{D}}$ is square, then it is in fact symmetric.*

Proof. By Theorem 2.2, $\boldsymbol{\mathcal{D}}$ corresponds to a $PDM(m,k,n\lambda)$. As we have seen in Section 1, any PDM satisfies $\beta \geq m$, and thus $b = n\beta \geq nm = v$.

Now assume that D is actually square, and denote the given class regular group by G. By Lemma 2.1, each block orbit under G consists of pairwise disjoint blocks. Hence the orbit of a specified block B is contained in the equivalence class $\boldsymbol{\mathcal{B}}$ of B with respect to $\sim$. By Lemma 3.3, $\boldsymbol{\mathcal{B}}$ has size at most n. On the other hand, Lemma 2.1 states that G is semiregular on blocks. Hence the orbit of B has size n, and therefore it coincides with the equivalence class $\boldsymbol{\mathcal{B}}$. Thus all block classes of $\boldsymbol{\mathcal{D}}$ have size n, so that $\boldsymbol{\mathcal{D}}$ is indeed symmetric, by Theorem 3.4. □

Following [40], we can now give the promised proof of Theorem 1.5. Thus let D be a $BGW(m,k,\mu)$ over a group G of order n. By Theorem 2.2, D gives rise to a class regular square divisible design $\boldsymbol{\mathcal{D}}$ with parameters (m,n,k,λ), where $\lambda = \mu/n$. As we have just seen in Theorem 4.1, $\boldsymbol{\mathcal{D}}$ is actually symmetric. Using the explicit description of $\boldsymbol{\mathcal{D}}$ in Theorem 2.2, we may translate the fact that any two non-equivalent blocks intersect in precisely λ points into a statement about the matrix D. Thus consider two blocks from different classes, say B_{jg} and B_{kh}, where $j \neq k$. Now a point (i,x) is on both these blocks if and only if

$$x = d_{ij}g = d_{ik}h, \quad \text{hence} \quad d_{ik}^{-1}d_{ij} = hg^{-1};$$

thus there are exactly λ indices i such that $d_{ik}^{-1}d_{ij} = hg^{-1}$ holds. Using the definition of D^*, this means that there are exactly λ indices i such that

$$d_{ki}^{*}\left(d_{ji}^{*}\right)^{-1} = hg^{-1}$$

holds. This proves that D^* is indeed a $BGW(m,k,\mu)$.

The preceding arguments establish more than we have originally claimed, and we may actually strengthen Theorem 1.5 as follows:

Theorem 4.2 *Let D be a $BGW(m,k,\mu)$ over a group G of order n, and let $\boldsymbol{\mathcal{D}}$ be the associated class regular square divisible design with parameters (m,n,k,λ), where $\lambda = \mu/n$. Then D^* is likewise a $BGW(m,k,\mu)$, and $\boldsymbol{\mathcal{D}}$ is actually symmetric. Moreover, the dual divisible design $\boldsymbol{\mathcal{D}}^*$ is also class regular, and it is associated with the BGW-matrix D^*.* □

5 Related geometries, III: Projective planes

In this short section, we provide two further interesting consequences of Theorem 2.2 (established in [39, 41]), which show that the notion of class regularity is a generalization of the concept of (p, L)-transitivity for projective planes. Let us briefly recall the definitions; we refer the reader to [28] for more background on finite projective planes.

A projective plane is said to be (∞, L_∞)-*transitive* for a point-line pair (∞, L_∞) provided that, given any two points $p, p' \notin L_\infty$ on a line through ∞, there is a *central collineation* with *center* ∞ and *axis* L_∞ moving p to p': a collineation φ fixing L_∞ pointwise and ∞ linewise, and satisfying $\varphi(p) = p'$. If (∞, L_∞) is a *flag* (that is, if ∞ is on L_∞), one speaks of an *elation*; otherwise, if (∞, L_∞) is an *antiflag*, of a *homology.*

Theorem 5.1 *The existence of a generalized Hadamard matrix $GH(n, 1)$ over a group G is equivalent to that of a finite projective plane of order n which admits G as the group of all (p, L)-elations for some flag (p, L).*

Proof. Let D be a $GH(n, 1)$ over G, and let $\boldsymbol{\mathcal{D}}$ be the associated class regular divisible design with parameters $(n, n, n, 1)$. We first note that $\boldsymbol{\mathcal{D}}$ is resolvable: the line orbits of G on $\boldsymbol{\mathcal{D}}$ define the desired parallelism. (Of course, we speak of *lines* instead of *blocks* in this geometric context.) Now we let all the lines in one of these orbits intersect in a new point. In this way, we add a further point class to $\boldsymbol{\mathcal{D}}$ and obtain a divisible design $\boldsymbol{\mathcal{A}}$ with parameters $(n + 1, n, n, 1)$, that is, the dual of an affine plane of order n. Finally, we interpret the point classes as a further set of $n + 1$ lines, and let them intersect in a new point ∞. This gives a projective plane $\boldsymbol{\mathcal{P}}$ of order n. It is now easily checked that $\boldsymbol{\mathcal{P}}$ is (∞, L_∞)-transitive with G as the corresponding elation group, where L_∞ is the line formed by all the points which have been adjoined. Moreover, this construction may be reversed; the details are left to the reader. $\square$

In a completely analogous way, one also obtains the following result:

Theorem 5.2 *The existence of some generalized conference matrix $BGW(n+1, n, n-1)$ over G is equivalent to that of a finite projective plane of order n which admits G as the group of all (p, L)-homologies for some antiflag (p, L).* $\square$

6 The relation to relative difference sets

There is a close connection between BGW-matrices and another concept of considerable interest in design theory, namely relative difference sets. Let us recall the required definition; for more background, the reader is referred to [7, 55].

Definition 6.1 Let G be a multiplicatively written group of order $v = mn$, and let N be a normal subgroup of order n and index m of G. A k-element subset R is called a *relative difference set* with parameters (m, n, k, λ) if the list of differences $(rs^{-1}\colon r, s \in R, r \neq s)$ contains no element of N and covers every element in $G \backslash N$ exactly λ times. One calls N the *forbidden subgroup.* A relative difference set is called *cyclic* or *abelian*, if G has the respective property. We also simplify notation by speaking of an (m, n, k, λ)-RDS; and in the special case $n = 1$, one simply speaks of a (v, k, λ)-*difference set.*

Like BGW-matrices, relative difference sets admit a nice geometric interpretation in terms of divisible designs. We need some definitions. As usual, a *Singer group* of a square divisible design $\boldsymbol{\mathcal{D}}$ is an automorphism group which acts regularly both on the point set and on the block set. Given a subset R of a group G, we define an incidence structure $\operatorname{dev} R$, the *development* of R, as follows:

$$\operatorname{dev} R \;=\; (G, \boldsymbol{\mathcal{B}}, \in) \qquad \text{with} \quad \boldsymbol{\mathcal{B}} \;=\; \{Rg\colon g \in G\}.$$

The following result is due to [41]; see also [55, §1.1] for a proof. Since we already have Theorem 4.1 at our disposal, we will be able to give yet another proof, which is shorter than the usual ones.

Theorem 6.2 *Let G be a group with a normal subgroup N of order n and index m, and let R be an (m, n, k, λ)-difference set in G relative to N. Then* $\operatorname{dev} R$ *is a symmetric divisible design with parameters (m, n, k, λ) admitting G as a Singer group for which the subgroup N is class regular. Conversely, every symmetric divisible design which admits a Singer group with a class regular subgroup can be represented in this way.*

Proof. Clearly, all blocks of $\boldsymbol{\mathcal{D}} = \operatorname{dev} R$ have cardinality k. Now let x and y be any two points of $\boldsymbol{\mathcal{D}}$, and B any block, say $B = R + u$ for some $u \in G$. We have $x, y \in B$ if and only if

$$x = du \text{ and } y = eu \quad \text{for some } d, e \in R,$$

which is equivalent to the conditions

$$xy^{-1} = de^{-1} \text{ and } x = du \quad \text{for some } d, e \in R.$$

Thus the number $[x, y]$ of blocks joining x and y in $\boldsymbol{\mathcal{D}}$ equals the number of occurrences of xy^{-1} as a difference de^{-1} with $d, e \in R$. Hence $[x, y] = 0$ for $xy^{-1} \in N$, and $[x, y] = \lambda$ otherwise. This already shows that $\boldsymbol{\mathcal{D}}$ is a square divisible design with parameters (m, n, k, λ), where the point classes are the right cosets of N. Clearly, G acts as a Singer group of $\boldsymbol{\mathcal{D}}$ by right translation. As N is a normal subgroup of G, it acts (regularly) on each right coset by right translation, and thus N is indeed class regular. Now Theorem 4.1 implies that $\boldsymbol{\mathcal{D}}$ has to be symmetric.

Conversely, let $\boldsymbol{\mathcal{D}}$ be a symmetric divisible design with parameters (m, n, k, λ) which admits G as a Singer group. As in the proof of Theorem 2.2, we may choose a base point and identify the points with the elements of G; then we may choose a base block R so that $\boldsymbol{\mathcal{D}} = \operatorname{dev} R$. The arguments used in the first part of the proof show that R is an (m, n, k, λ)-difference set in G relative to the given class regular subgroup N. Finally, the class regularity of N ensures that N is actually a normal subgroup of G. $\square$

The reader may consult Ghinelli [20, 21, 22, 23], Jungnickel [41] and Pott [55] for more details on symmetric divisible designs and relative difference sets. In particular, a few examples with respect to non-normal subgroups are in [41].

Combining Theorems 6.2 and 2.2, we have the following interesting result due to [41].

Theorem 6.3 *Let G be a group with a normal subgroup N of order n and index m, and assume the existence of an (m, n, k, λ)-difference set in G relative to N. Then there also exists a $BGW(m, k, n\lambda)$ over N.* $\square$

It is, of course, possible to describe the BGW-matrices of Theorem 6.3 explicitly. The following result is [38, Theorem 10.3.1], generalizing two important special cases studied in [41]. We will give a different proof elaborating the geometric approach just used to obtain Theorem 6.3.

Proposition 6.4 *Let G be a group with a normal subgroup N of order n and index m, and let R be an (m, n, k, λ)-difference set in G relative to N. In addition, let $x_1, x_2, \ldots, x_m$ be a system of coset representatives for N in G, and let $W = (w_{ij})$ be the $m \times m$ matrix with entries from $N \cup \{0\}$ defined by*

$$w_{ij} = \begin{cases} 0 & \text{if } x_i N \cap R x_j = \emptyset \\ \alpha & \text{if } x_i N \cap R x_j = \{x_i \alpha\}. \end{cases}$$

Then W is a $BGW(m, k, n\lambda)$ over N.

Proof. Let $\boldsymbol{\mathcal{D}} = \operatorname{dev} R$ be the symmetric divisible design determined by the relative difference set R. We may associate the point class of x_i with the row i of W in the manner used in the proof of Theorem 2.2 by identifying the point $x_i\alpha$ of $\boldsymbol{\mathcal{D}}$ with the pair (i, α), where $\alpha \in N$. Similarly, we associate the block class of Rx_j with the column j of W by considering the block $Rx_j\beta$ of $\boldsymbol{\mathcal{D}}$, where $\beta \in N$, as the image of the base block $B_j = Rx_j$ under right translation by β; we may then denote this block by $B_{j\beta}$, as in the proof of Theorem 2.2. As N is class regular by Theorem 6.2, the proof of Theorem 2.2 implies the assertion. $\square$

One of the two special cases already alluded to concerns cyclic relative difference sets, while the second one deals with *splitting* relative difference sets: the case where N is a direct factor of G, so that G splits as $G = H \times N$. We will present two fundamental results from [41]; purely computational proofs may also be found [38, §10.3]. We require two more definitions.

A matrix $A = (a_{g,h})$ whose rows and columns are indexed by the elements of a (multiplicatively written) group H is called *H-invariant* provided that

$$a_{g,h} \;=\; a_{gk,hk} \qquad \text{for all } \; g, h, k \in H.$$

Note that A is *circulant* if and only if it is H-invariant for a cyclic group H.

An *ω-circulant* matrix X is defined by the following property: each row of X is obtained from the preceding row by shifting every entry but the one in the final column one position to the right, whereas the entry in the final column is first multiplied by ω, and then the result is put in the first position of the shifted row. Formally, for $i = 1, \ldots, m-1$,

$$x_{i,j} = x_{i+1,j+1} \;\text{ for }\; j = 1, \ldots, m-1 \;\text{ and }\; x_{i+1,1} = \omega x_{i,m}. \tag{8}$$

Note that the special case $\omega = 1$ again yields the well-known *circulant* matrices; for $\omega = -1$ one speaks of *negacyclic* matrices.

Theorem 6.5 *Let H and N be groups of orders m and n, respectively, and put $G = H \times N$. Then the existence of an H-invariant $BGW(m, k, \mu)$ over N is equivalent to the existence of an (m, n, k, λ)-difference set in G relative to N, where $\lambda = \mu/n$.*

Proof. First let R be an (m, n, k, λ)-difference set in G relative to N. As H is a complement of N in G, we may take H as the system of coset representatives of N required in Proposition 6.4; let W be the associated BGW-matrix which we may then consider to be indexed by H (with respect to some specified ordering of the elements of H). Thus

$$w_{g,h} = \begin{cases} 0 & \text{if } gN \cap Rh = \emptyset \\ \alpha & \text{if } gN \cap Rh = \{g\alpha\}. \end{cases}$$

As the elements of H and N commute, we may just multiply these conditions by any given $k \in H$ to see that W is indeed H-invariant.

Conversely, let W be an H-invariant $BGW(m,k,\mu)$ over N. We may assume that the first row and column of W is indexed by the identity 1 of H. By Theorem 2.2, the first base block B_1 of the associated symmetric divisible design $\boldsymbol{\mathcal{D}}$ consists of all elements $(h, w_{h,1})$ with $w_{h,1} \neq 0$. Let us view B_1 as a subset R of $G = H \times N$. As W is H-invariant, the base block defined by the column indexed with $k \in H$ is the right translate $B_k = Rk$ of R. It is now easily seen that G acts as a Singer group of $\boldsymbol{\mathcal{D}}$, so that the assertion follows from Theorem 6.2. □

In a similar (though somewhat more involved) manner we also prove the corresponding result for ω-circulant matrices:

Theorem 6.6 *Let N be a cyclic group of order n, and let ω be some generator of N. Then the existence of an ω-circulant $BGW(m,k,\mu)$ over N is equivalent to the existence of an (m,n,k,λ)-difference set in the cyclic group G of order $v = mn$ relative to the unique subgroup of order n (which may, of course, be identified with N), where $\lambda = \mu/n$.*

Proof. First let R be an (m,n,k,λ)-difference set in G relative to N. Without loss of generality, we may choose $\omega = \beta^{-m}$, where β is a specified generator of G. Also, we shall use the powers $1, \beta, \ldots, \beta^{m-1}$ as the coset representatives of N required in Proposition 6.4. Let X be the associated BGW-matrix, which we may then consider to be indexed by $0, 1, \ldots, m-1$. The definition of X can be written as follows:

> If there is a (necessarily unique) element g of $R\beta^j$ in the coset $N\beta^i$, then set $x_{ij} = \beta^{-i}g$, and otherwise set $x_{ij} = 0$.

It is now rather easy to check that X is ω-circulant: just note that the condition $g \in R\beta^j \cap N\beta^i$ is equivalent to $g\beta \in R\beta^{j+1} \cap N\beta^{i+1}$. Thus, for $i = 0, \ldots, m-2$,

$$x_{i+1,j+1} = \beta^{-(i+1)}(g\beta) = \beta^{-i}g = x_{i,j} \quad \text{if } j \neq m-1.$$

For $j = m-1$, we first note $g\beta \in R\beta^m \cap N\beta^{i+1} = R\omega^{-1} \cap N\beta^{i+1}$ and hence $g\beta\omega \in R\beta^0 \cap N\beta^{i+1}$, which yields

$$x_{i+1,0} = \beta^{-(i+1)}(g\beta\omega) = \omega\left(\beta^{-i}g\right) = \omega x_{i,m-1}.$$

Finally, the case of zero entries is dealt with in the same manner.

Conversely, let X be an ω-circulant $BGW(m,k,\mu)$ over N, where we use $0,\ldots,m-1$ as row and column indices, and let $\boldsymbol{\mathcal{D}}$ be the associated symmetric divisible design according to Theorem 2.2. We may describe N and G as in the first part of the proof, using generators β and ω satisfying $\omega=\beta^{-m}$. Now we identify the point (i,x) of $\boldsymbol{\mathcal{D}}$ with the element $\beta^i x$ of G, so that the jth base block becomes

$$B_j \;=\; \left\{\beta^i x_{i,j}\colon\, i=0,\ldots,m-1;\; x_{i,j}\neq 0\right\}.$$

As in the proof of Theorem 6.5, we consider the first base block B_0 as a subset R of G and claim that R is the desired relative difference set. In view of Theorem 6.2, it will suffice to show that multiplication by β induces an automorphism of $\boldsymbol{\mathcal{D}}$. Using the fact that X is ω-circulant, one easily obtains the following condition complementing the relations given in (8):

$$x_{0,j+1}=\omega x_{m-1,j} \quad \text{for } j=0,\ldots,m-2. \tag{9}$$

Using (8), (9), it is not difficult to check $B_j\beta = B_{j+1}$ for $j=0,...,m-2$ and $B_{m-1}\beta = B_0\omega^{-1}$, which implies the assertion. We leave the details to the reader, as they are similar to the arguments used in the first part of the proof. □

7 Existence results

In this section, we collect information about the known parameters for BGW-matrices. We generally exclude the case where G is the group of order 2; in particular, we do not consider ordinary Hadamard matrices and conference matrices. The reader is referred to the relevant sections in [12] (and the references given there) for these topics.

We begin with a very simple observation regarding generalized Hadamard matrices. In what follows, we shall use the notation $EA(q)$ to denote the elementary abelian group of order q, which we will usually realize as the additive group of the finite field $GF(q)$.

Proposition 7.1 *For each prime power q, there exists a $GH(q,1)$ over the elementary abelian group $EA(q)$.*

Proof. The multiplication table of $F=GF(q)$ gives the desired matrix in the additive group of F. □

Combining Propositions 7.1 and 1.2 yields a wealth of GH-matrices over elementary abelian groups. As a general policy, we will not state parameters which can be obtained by taking homomorphic images of matrices over larger groups.

In connection with Propositions 7.1 we want to digress briefly to discuss the existence problem for abelian group invariant $GH(n,1)$-matrices.

Theorem 7.2 *Let G and H be abelian groups of order n. Then an H-invariant $GH(n,1)$ over G exists if and only if n is an odd prime power. Examples are known whenever G and H are both elementary abelian.*

Proof. By Theorem 6.5, an H-invariant $GH(n,1)$ over G is equivalent to a splitting $(n,n,n,1)$-RDS in $G = H \times N$. By the results of [19] and [10], an abelian relative difference set of this type exists if and only if n is an odd prime power; see also [24, §4] for a detailed exposition of this result. Such relative difference sets are known whenever G is elementary abelian. □

Actually, *all* known abelian $(n,n,n,1)$-RDS of odd order n occur in elementary abelian groups; for instance, every commutative semifield plane of odd order admits a representation by such an RDS, see [24]. On the theoretical side, the results of [10] only guarantee that G has rank at least $b+1$, where $n = p^b$ for the odd prime b. It would be very nice if one could show that G has to be elementary abelian – at least in the splitting case.

Generalized Hadamard matrices have received a lot of attention, and treating them in detail would detract from our main topic, namely *proper* BGW-matrices. We therefore just collect the most interesting general existence results in the following theorem. We refer the reader to [12, §IV.11] both for references and for further results such as recursive constructions and non-existence theorems; let us stress that the existence of generalized Hadamard matrices $GH(s,\lambda)$, where s is not a prime power, is still an open problem.

Theorem 7.3 *Let q be a prime power, and let G be the elementary abelian group of order q. Then a generalized Hadamard matrix $GH(q,\lambda)$ exists in at least the following cases:*

- $\lambda = 1, 2,$ *or* 4*;*
- $\lambda = 8$, *where* $19 < q < 200$ *or where* $q > 19$ *is a prime;*
- λ *the order of a Hadamard matrix and* $q > ((\lambda-2)2^{\lambda-2})^2$.

Now let G be an arbitrary group of order q. Then there exists a $GH(q, q^t)$ over G for every odd positive integer t. □

As announced before, from now on we restrict attention to proper BGW-matrices; here we will also allow the case $n = 2$, as the requirement of balance is a very severe restriction compared to ordinary weighing matrices. The by far most important series of examples has parameters

$$m = \frac{q^d - 1}{q - 1}, \quad k = q^{d-1} \quad \text{and} \quad \mu = q^{d-1} - q^{d-2}, \tag{10}$$

where q is a prime power and $d \geq 2$ an integer; it is usual to refer to these parameters as the *classical parameters*. The most important examples are those defined over the multiplicative group $N = GF(q)^*$ of $GF(q)$ (but there are other examples, see Theorem 7.9). In this case we may identify the extra symbol 0 appearing in the definition of partial difference matrices with $0 \in GF(q)$, so that we can consider any BGW-matrix over N as a matrix over $GF(q)$; this simple observation will lead to rather interesting consequences in Section 8.

The classical examples may be obtained from suitable cyclic relative difference sets; thus we shall first construct the required relative difference sets, usually called the *classical relative difference sets*. This approach to constructing the classical BGW-matrices is actually equivalent to the method used by Berman [6] (who seems to have been the first author to construct BGW-matrices with classical parameters), even though it looks somewhat different. In what follows the term *trace* refers to the relative trace function Tr from $GF(q^d)$ to $GF(q)$ (not the absolute trace to the prime subfield); thus

$$\mathrm{Tr}\, \alpha = \alpha + \alpha^q + \ldots + \alpha^{q^{d-1}} \quad \text{for } \alpha \in GF(q^d).$$

Lemma 7.4 *Let q be a prime power and $d \geq 2$ an integer, and let R denote the set of elements of $GF(q^d)$ of trace 1. Then R is a cyclic relative difference set with parameters*

$$m = \frac{q^d - 1}{q - 1}, \quad n = q - 1, \quad k = q^{d-1} \quad \textit{and} \quad \lambda = q^{d-2} \tag{11}$$

in the multiplicative group $G = GF(q^d)^*$ relative to the forbidden subgroup $N = GF(q)^*$.

Proof. We first check $|R| = q^{d-1}$. Since the trace function is an epimorphism of the additive groups, we have

$$|R| = |\mathrm{kerTr}| = |GF(q^d)|/|\mathrm{imTr}| = q^{d-1}.$$

For $g \in G$, let $A(g)$ denote the number of solutions of $g = x_1 x_2^{-1}$ with $x_1, x_2 \in R$. Thus we have to show $A(g) = 0$ for $g \in N \setminus \{1\}$ and $A(g) = q^{d-2}$ for $g \in G \setminus N$. We note that the sets $H(g) = \{xg : x \in R\}$ with $g \in G$ are distinct hyperplanes when considered as subsets of the affine geometry $AG(d, q)$. Such a hyperplane $H(g)$ is parallel to $R = H(1)$ if and only if $g \in N$. Furthermore, it is easily seen that $A(g)$ is the size of the intersection $|H(g) \cap H(1)|$. Hence indeed $A(g) = 0$ for $g \in N$ and $A(g) = q^{d-2}$ for $g \in G \setminus N$. □

As the proof of Lemma 7.4 shows, G acts as a Singer group of the symmetric divisible design formed by the points of $AG(d, q)$ distinct from the origin and by the hyperplanes not passing through the origin. Now an application of Theorem 6.6 gives the following result:

Theorem 7.5 *Let q be a prime power and $d \geq 2$ an integer, and let ω be a generator of $N = GF(q)^*$. Then there exists an ω-circulant BGW-matrix with parameters (10) over N.* □

Let us also note the analogous result concerning *circulant* BGW-matrices:

Theorem 7.6 *Let q be a prime power and $d \geq 2$ an integer. Then there exists a circulant BGW-matrix with parameters (10) over $GF(q)$ whenever $\left(q-1, \frac{q^{d+1}-1}{q-1}\right) = 1$.*

Proof. The condition $\left(q-1, \frac{q^{d+1}-1}{q-1}\right) = 1$ allows us to write G as the direct product of N with a cyclic group of order $(q^{d+1}-1)/(q-1)$. Thus the assertion is an immediate consequence of Lemma 7.4 and Theorem 6.5. □

We now give an explicit description of the classical BGW-matrices essentially taken from [45].[3] For this purpose, we let β be a primitive element of $GF(q^d)$, so that we may choose $\omega = \beta^{-m}$. As noted in the proof of Theorem 6.6, the ω-circulant BGW-matrix $X = (x_{ij})_{i,j=0,\dots,m-1}$ with entries in $GF(q)$ and parameters (10) obtained from the classical RDS may be obtained as follows:

> If there is a (necessarily unique) element g of $R\beta^j$ in the coset $N\beta^i$, then set $x_{ij} = \beta^{-i} g$, and otherwise set $x_{ij} = 0$.

[3] In [45] and [43], we have always associated the *transpose* of the matrix X defined in Theorem 6.6 with a given cyclic RDS, instead of X itself. Though this makes no essential difference, the proof of Theorem 6.6 shows that it is more natural to proceed as suggested in the present notes. Moreover, this setup agrees with the one used by Ionin and Shrikhande in their book [38].

Now we just have to put the preceding description of X into more explicit terms. It turns out to be more convenient to write down the transpose Y of X first; note that this matrix will be ω^{-1}-circulant, as X is ω-circulant. The description of X gives the following definition of Y:

> If there is a (necessarily unique) element r of $R\beta^i$ in the coset $N\beta^j$, then $y_{ij} = \beta^{-j}r$; and otherwise set $y_{ij} = 0$.

Now we just have to put the preceding description of Y into more explicit terms. As Y is ω^{-1}-circulant, it suffices to consider the first row of Y. Select any coset $N\beta^j$, $j = 0, \ldots, m-1$, and assume first $\operatorname{Tr}\beta^j = 0$. Since $N\beta^j$ consists of the non-zero scalar multiples of β^j, each element of this coset has trace 0; thus $R \cap N\beta^j = \emptyset$ and therefore $y_{0j} = 0 = \operatorname{Tr}\beta^j$ in this case. Now assume $\operatorname{Tr}\beta^j = \alpha \neq 0$. Then $\operatorname{Tr}(\alpha^{-1}\beta^j) = \alpha^{-1}\operatorname{Tr}\beta^j = 1$ and therefore $\alpha^{-1}\beta^j \in R \cap N\beta^j$, which gives $y_{0j} = \alpha^{-1} = (\operatorname{Tr}\beta^j)^{-1}$.

Now we simply have to write down the ω-circulant matrix Y with the first row just computed. In order to avoid case distinctions, it is advisable to write down the matrix $W = Y^{(-1)}$ instead of Y, since then the initial row just consists of the entries $w_{0j} = \operatorname{Tr}\beta^j$; note that W is ω-circulant, as Y is ω^{-1}-circulant. Moreover, a particularly useful (and pleasing) form results, if we also make use of the linearity of the trace function and the relation $\omega = \beta^{-m}$ to re-write all entries of W involving a factor ω as follows:

$$\omega \operatorname{Tr}\beta^j \;=\; \operatorname{Tr}(\omega\beta^j) \;=\; \operatorname{Tr}\beta^{j-m} \;=\; \operatorname{Tr}\beta^{m(q-2)+j}.$$

This gives the following result:

Proposition 7.7 *Let X be the classical ω-circulant BGW-matrix with parameters* (10) *associated with the classical relative difference sets of Lemma 7.4 according to Theorem 6.6. Then $X = W^*$, where, with $v = m(q-1) = q^d - 1$,*

$$W \;=\; \begin{pmatrix} \operatorname{Tr}\beta^0 & \operatorname{Tr}\beta^1 & \operatorname{Tr}\beta^2 & \ldots & \operatorname{Tr}\beta^{m-1} \\ \operatorname{Tr}\beta^{v-1} & \operatorname{Tr}\beta^0 & \operatorname{Tr}\beta^1 & \ldots & \operatorname{Tr}\beta^{m-2} \\ \operatorname{Tr}\beta^{v-2} & \operatorname{Tr}\beta^{v-1} & \operatorname{Tr}\beta^0 & \ldots & \operatorname{Tr}\beta^{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ \operatorname{Tr}\beta^{v-(m-1)} & \operatorname{Tr}\beta^{v-(m-2)} & \ldots & \ldots & \operatorname{Tr}\beta^0 \end{pmatrix}. \quad \square$$

Clearly, if X is a BGW-matrix over an abelian group, then so is X^*; also, if X is ω-circulant, then X^* is likewise ω-circulant. Hence Proposition 7.7 yields the following consequence, which will be of interest in the next section.

Corollary 7.8 *Let q be a prime power and $d \geq 2$ an integer, let β be a primitive element of $GF(q^d)$, and put $\omega = \beta^{-m}$. Then the $m \times m$ matrix W with entries from $GF(q)$ defined in Corollary 7.7 is an ω-circulant BGW-matrix with parameters (10) over $GF(q)^*$.* □

We shall now provide a complete list of the known parameters for proper BGW-matrices. We will not give proofs, but refer the reader to the original sources as well as to [12, §IV.4] and to [38, Chapter 10] for details and further references. Again, we will refrain from stating parameters which can be obtained by taking homomorphic images of matrices over larger groups.

We will require the notion of nearfields. Recall that a proper nearfield may be thought of as a non-commutative field with only one distributive law. To be precise, a finite *nearfield* is a finite set K on which two operations, addition and multiplication $(\cdot)$, are defined with the following properties:

(N1) $(K, +)$ is an abelian group with identity 0;
(N2) $(K^*, \cdot)$ is a group, where $K^* = K \backslash \{0\}$;
(N3) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in K$;
(N4) $a \cdot 0 = 0$ for all $a \in K$.

The finite nearfields were completely classified by Zassenhaus [64], so that the groups which arise as the multiplicative group of a finite nearfield are known; see also [15, §5.2] and [38, §10.1].

Theorem 7.9 *Let q be a prime power, and let G be a finite group of order n. A $BGW(m, k, \mu)$ over G exists at least in the following cases:*

- *The parameters are classical: $m = (q^d - 1)/(q - 1)$, $k = q^{d-1}$, $\mu = q^{d-2}(q - 1)$, and one of the following occurs:*
  1. *G is the cyclic group of order $n = q - 1$ or, more generally, the multiplicative group of a finite nearfield* [53];
  2. *q is even, d is odd, and G is the cyclic group of order $n = 2(q - 1)$* [4];
  3. *q is even, $d = 7$, and G is the direct product of two cyclic groups of orders $2(q - 1)$ and 2, so that $n = 4(q - 1)$* [48];
  4. *$q = r^2$ is a perfect square, and G is an arbitrary group of order $n = r + 1$* [17];
- *$m = k + 1$, $k = n(2n - 1)$, $\mu = k - 1$ and G the cyclic group of order n, where $n = 2^{d-1} - 1$ and $d \geq 3$ (see* [12]*).*

In addition, the following four sporadic cases are known to occur: a circulant $BGW(13,9,6)$ over the symmetric group S_3 [26, 57]*; a $BGW(15,7,3)$* [5] *and a $BGW(45,12,3)$* [51] *over the cyclic group of order* 3*; and a $BGW(19,9,4)$ over the cyclic group of order* 2 [18, 26]. □

A few comments regarding the examples with classical parameters in Theorem 7.9 are in order. Most of these results have been motivated by the problem of signing symmetric designs with parameters

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

In particular, the problem of signing the complements of the classical point-hyperplane designs defined over finite projective spaces has attracted a lot of interest. As these designs admit a difference set representation, particular attention was given to signings respecting this property; explicitly, Pott [55] had posed the question of how far the complements of the classical Singer difference sets might be *lifted* to cyclic relative difference sets. The examples with $n = 2(q-1)$ constructed by Arasu, Dillon, Leung and Ma [4] (Case 2 in Theorem 7.9) actually do belong to cyclic relative difference sets and, hence, are ω-circulant. Moreover, [4] actually contains the answer to Pott's question, strengthening previous work of [2]:

Theorem 7.10 *Let q be a prime power. A cyclic relative difference set with parameters*

$$m = \frac{q^d-1}{q-1},\quad n,\quad k = q^{d-1} \quad \textit{and} \quad \lambda = \frac{q^{d-2}(q-1)}{n} \tag{12}$$

exists if and only if one of the following cases occurs:

- *q is odd, and n divides $q-1$;*
- *q and d are even, and n divides $q-1$;*
- *q is even, d is odd, and n divides $2(q-1)$.* □

In particular, the complements of the classical point-hyperplane designs cannot be lifted to a cyclic RDS with $n = 4(q-1)$. Nevertheless, the examples of BGW-matrices with $n = 4(q-1)$ given in [48] (Case 3 in Theorem 7.9) actually also belong to relative difference sets with classical parameters; however, here the underlying group is the direct product of two cyclic groups, one of which has order 2.

In the language of signings, the result of [53] concerning *BGW*-matrices over finite nearfields (Case 1 in Theorem 7.9) shows that the complement of the symmetric $\big((q^d-1)/(q-1),\, (q^{d-1}-1)/(q-1),\, (q^{d-2}-1)/(q-1)\big)$-design $F[t]$ constructed by Mavron [52] is signable over every quotient group of F^*, where F is any finite right nearfield. To the author's knowledge, this provides the only known infinite series of non-classical symmetric designs which have been proved to be signable.

There has also been considerable interest in the existence of special types of *BGW*-matrices, namely *symmetric* and *skew* matrices, as these are very useful in the context of applications to the construction of designs and graphs. These constructions are more difficult and have only been accomplished in recent years; therefore we will not give proofs, but refer the interested reader to the original sources or to the book [38].

We note that the the classical point-hyperplane designs and their complements can be represented by symmetric incidence matrices, as they admit polarities. Thus the problem of constructing symmetric *BGW*-matrices with classical parameters can also be viewed as asking for signings of these matrices respecting the extra property of symmetry.

To use the full strength of balanced generalized weighing matrices for generating strongly regular graphs, one actually requires even more: symmetric *BGW*'s with zero diagonal. Using the classical ω–circulant *BGW*'s, the following recursive construction was established by Kharaghani [47]:

Theorem 7.11 *Let C_n be a cyclic group of order n, let q be a prime power, and let t and m be positive integers. If there exists a symmetric balanced generalized weighing matrix with parameters*

$$v = 1 + q^{m+1} + q^{2(m+1)} + \cdots + q^{t(m+1)},\ k = q^{t(m+1)},\ \mu = q^{(t-1)(m+1)}(q^{m+1}-1)$$

with zero diagonal over the cyclic group of order $n(1+q+\cdots+q^m)$, then there also exists a symmetric

$$BGW\,\big((1+q+q^2+\cdots+q^m)v,\, kq^m,\, q^{t(m+1)}(q^m-q^{m-1})\big)$$

with zero diagonal over the cyclic group C_n. $\square$

It is clear from the preceding theorem that there is a need for an initial symmetric balanced generalized weighing matrix with zero diagonal. Fortunately, a construction method of Gibbons and Mathon [25] always provides a symmetric $BGW(1+p,p,p-1)$ with zero diagonal over the cyclic group of order n, where p is a prime and where n is a divisor of $p-1$ for which

$(p-1)/n$ is even. (It is interesting to note that the condition on $(p-1)/n$ is actually necessary: otherwise, there is no symmetric $BGW(1+p, p, p-1)$ with zero diagonal over C_n.) These initial matrices lead to the following infinite series:

Theorem 7.12 *Let q be a prime power, and let n be a divisor of $q-1$ for which $(q-1)/n$ is even. Then, for every positive integer d, there exists a symmetric*

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

with zero diagonal over the cyclic group of order n. □

Finally, we come to skew BGW's. Here a balanced generalized weighing matrix W over a finite group G with a fixed element τ of order 2 is said to be *skew* if $W = (W^{\tau})^T$. Note that the diagonal entries of a skew matrix must be equal to 0. Moreover, if W is a matrix over $GF(q)$, where q is odd, then W is skew if and only if $W = -W^T$. The following result due to Ionin and Kharaghani [35] complements Theorem 7.12.

Theorem 7.13 *Let q be an odd prime power, and let n be a divisor of $q-1$ for which $(q-1)/n$ is odd. Then, for every positive integer d, there exists a skew balanced generalized weighing matrix*

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

over the cyclic group of order n. □

8 More on BGW-matrices with classical parameters

In this section, we will summarize the work of [44, 45] concerning BGW-matrices with classical parameters (10), where G is the cyclic group of order $n = q-1$; as noted before, we can view such examples as matrices over $GF(q)$. In particular, we may consider the rank of such a matrix W over $GF(q)$; noting that the rows of W and their nonzero multiples constitute $q^d - 1$ distinct nonzero vectors in the row space of W over $GF(q)$ gives the following basic result.

Lemma 8.1 *Let W be any balanced generalized weighing matrix with classical parameters* (10) *over $GF(q)^*$. Then* $\operatorname{rank}_q M \geq d$. $\square$

In fact, we have already met an example realizing this bound, as the following strengthening of Corollary 7.8 shows.

Theorem 8.2 *Let q be a prime power and $d \geq 2$ an integer, let β be a primitive element of $GF(q^d)$, and put $\omega = \beta^{-m}$. Then the ω-circulant matrix W over $GF(q)$ defined in Proposition 7.7 is a BGW-matrix with parameters (10) satisfying* $\operatorname{rank}_q W = d$.

Proof. It remains to show that the matrix W has q-rank d. Note that W is the submatrix formed by the first m rows and the first m columns of the circulant $v \times v$ matrix C with first row

$$\mathbf{c} \;=\; (\operatorname{Tr}\beta^0 \; \operatorname{Tr}\beta^1 \; \ldots \; \operatorname{Tr}\beta^{v-1}) \;=\; (\mathbf{w} \; \theta\mathbf{w} \; \ldots \; \theta^{q-2}\mathbf{w}),$$

where $\mathbf{w}$ denotes the first row of W and where $\theta = \omega^{-1} = \beta^m$. Now $\mathbf{c}$ is a well-known object, namely the first period of an *m-sequence* (that is, a linear shift register sequence of maximal period), as β was chosen to be a primitive element for $GF(q^d)$; see, for instance, [42, Theorem 6.3.9]. More precisely, the linear feedback shift register of length d with characteristic polynomial the minimal polynomial of β will produce the periodic sequence defined by $\mathbf{c}$. But this implies that the circulant matrix C formed by the v shifts of the first row $\mathbf{c}$ has q-rank d, see [42, Corollary 6.6.4]. Trivially, W then has q-rank at most d, so that the assertion follows from Lemma 8.1. $\square$

BGW-matrices of minimal q-rank can also be described in coding theoretic terms; moreover, these matrices are essentially unique. To make this precise, we need to recall the following concept: two matrices over $G \cup \{0\}$ are said to be *monomially equivalent* if one is obtainable from the other by permutations of rows and columns and by multiplying rows (on the left) and columns (on the right) by elements from G. It is easy to check that any matrix which is monomially equivalent to a *BGW*-matrix is again a *BGW*-matrix. In particular, every *BGW*-matrix is monomially equivalent to a *normalized* matrix, that is, a matrix which has all nonzero entries in the first row and in the first column equal to 1, and all zeros preceding ones.

We shall also require a bit of coding theory. Recall that the q-ary *simplex code* $S_d(q)$ of length $\frac{q^d-1}{q-1}$, where $d \geq 2$ and q is a prime power, is defined as a linear code over $GF(q)$ with a generator matrix having as columns representatives of all distinct 1-dimensional subspaces of the d-dimensional vector space $GF(q)^d$. In other words, S_d is the dual code of the unique linear perfect single-error-correcting code of length $\frac{q^d-1}{q-1}$ over $GF(q)$, that is, of the q-ary analogue of the Hamming code. The reader is referred to MacWilliams and Sloane [50] or to Tonchev [62] for the required background. In particular, we need the following two facts, the first of which is well-known:

Lemma 8.3 *Each non-zero vector in $S_d(q)$ has Hamming weight q^{d-1}. Moreover, the supports of all these vectors form the blocks of a symmetric $(\frac{q^d-1}{q-1}, q^{d-1}, q^{d-1} - q^{d-2})$ design which is isomorphic to the complement of the classical point-hyperplane design in the projective space $PG(d-1, q)$.* $\square$

The characterization of the classical design given in the preceding lemma is due to Tonchev [63]. We can now prove the following major result established in [44]:

Theorem 8.4 *Any $m \times m$ matrix M with rows a set of representatives of the $m = (q^d - 1)/(q - 1)$ distinct 1-dimensional subspaces of $S_d(q)$ is a balanced generalized weighing matrix with parameters (10) and q-rank d over $GF(q)$. Moreover, any BGW-matrix over $GF(q)$ with parameters (10) and q-rank d is monomially equivalent to such a matrix.*

Proof. Let $x = (x_1, x_2, \dots, x_m)$ be a row of M. By Lemma 8.3, if $y = (y_1, y_2, \dots, y_m)$ is any other row of M, there are exactly $q^{d-1} - q^{d-2}$ indices i such that $x_i \neq 0$ and $y_i \neq 0$. We need to show that the multiset

$$S \;=\; \{x_i y_i^{-1}\colon\; y_i \neq 0\}$$

contains every nonzero element of $GF(q)$ exactly q^{d-2} times. Note that multiplication of any column or row of M by a nonzero element of $GF(q)$ preserves the set of frequencies of the elements in S. Therefore, multiplying the ith column of M by y_i^{-1} for all i such that $y_i \neq 0$ transforms M into a matrix M' for which x is transformed into $x' = (\dots x_i y_i^{-1} \dots)$, whereas y becomes a $(0, 1)$-vector y'. By Lemma 8.3, $d(x', y') = d(x, y) = q^{d-1}$, where d denotes the Hamming distance. Let

$$I \;=\; \{i\colon\; x'_i \neq 0 \text{ and } y'_i \neq 0\}.$$

In order for M' (and therefore M) to be a balanced generalized weighing matrix, the multiset $S' = \{x'_i \mid i \in I\}$ has to contain each of the $q - 1$ nonzero elements of $GF(q)$ the same number of times, that is, q^{d-2} times. Note that $q^{d-2} = (q^{d-1} - q^{d-2})/(q - 1)$ is the average frequency of an element in S'. Assume there is some $\beta \in GF(q)$, $\beta \neq 0$ which occurs more than q^{d-2}

times in S'. Then multiplying the vector x' by β^{-1} gives a vector x'' such that $d(x'', y') < q^{d-1}$, contradicting Lemma 8.3. $\square$

It may come as a surprise to hear that the BGW-matrices of minimal q-rank are *not* the classical BGW-matrices obtained from the classical relative difference sets. Nevertheless, as we have seen, the relationship is simple enough: the classical matrix X described in Proposition 7.7 satisfies $X = W^*$, that is, it arises from the minimal rank BGW-matrix W of Theorem 8.2 by transposing and replacing each non-zero entry by its inverse. Note that the minimal rank matrix W describes the dual of the classical symmetric divisible design $\boldsymbol{\mathcal{D}}$ associated with X; see Theorem 4.2. Of course, $\boldsymbol{\mathcal{D}}$ is isomorphic to its dual, as it actually admits an abelian Singer group and, hence, a polarity (cf. [7, Proposition I.4.11]); nevertheless, this does not imply that the associated BGW-matrices have to be monomially equivalent.

The preceding remarks immediately raise the problem of determining the q-rank of the classical BGW-matrix X, or, equivalently, that of $X^T = W^{(-1)}$. It is rather obvious that inversion of elements will, in general, change the q-rank, with a few obvious exceptions. Indeed the q-rank will stay the same for $q \leq 4$; this is trivial if $q = 2$ or $q = 3$, and for $q = 4$ it follows from the observation that inversion here equals squaring, which is a field automorphism of $GF(4)$ and hence respects the 4-rank. Actually, one may solve a more general problem and determine the q-rank of all matrices of the form $W^{(t)}$, where $W^{(t)}$ is the matrix arising from W by replacing each entry g in W with its tth power g^t.

Theorem 8.5 *Let W be the balanced generalized weighing matrix with parameters (10) of q-rank d defined in Proposition 7.7, and let t be a positive integer in the range $1 \leq t \leq q-2$. Write $q = p^r$, where p is prime, and let $\sum_{i=0}^{r-1} t_i p^i$ be the p-ary expansion of t (thus $0 \leq t_i < p$ for all i). Then*

$$\mathrm{rank}_q W^{(t)} \;=\; \prod_{i=0}^{r-1} \binom{d-1+t_i}{d-1}. \tag{13}$$

Proof. As in the proof of Theorem 8.2, the key observation is that the ω-circulant matrix $W^{(t)}$ is a submatrix of a larger circulant matrix: applying the power mapping $x \mapsto x^t$ to the entries of the matrix C defined there, we see that $W^{(t)}$ is the submatrix formed by the first m rows and the first m columns of the circulant matrix $C^{(t)}$ with first row

$$\mathbf{c}^{(t)} \;=\; \left((\mathrm{Tr}\,\beta^0)^t\ (\mathrm{Tr}\,\beta^1)^t\ \ldots\ (\mathrm{Tr}\,\beta^{v-1})^t\right).$$

The periodic sequences with first period $\mathbf{c}^{(t)}$ – which can be thought of as twisted versions of m-sequences – were studied by Antweiler and Bömer [1] who determined their *linear complexity* $L(\mathbf{c}^{(t)})$, that is, the shortest length of a linear feedback shift register capable of producing the sequence $\mathbf{c}^{(t)}$, which agrees with the q-rank of the circulant matrix $C^{(t)}$. Their result is as follows; see also [42, Thm. 6.8.3] or [55, Thm. 3.2.8] for proofs.

$$L(\mathbf{c}^{(t)}) \;=\; \prod_{i=0}^{r-1} \binom{d-1+t_i}{d-1}. \tag{14}$$

Thus we may establish (13) by proving $\mathrm{rank}_q W^{(t)} = L(\mathbf{c}^{(t)})$. We proceed as before and note that the circulant matrix $C^{(t)}$ formed by the v shifts of the first row $\mathbf{c}^{(t)}$ has q-rank $L(\mathbf{c}^{(t)})$, see [42, Cor. 6.6.4]. Trivially, this implies $\mathrm{rank}_q W^{(t)} \le L(\mathbf{c}^{(t)})$. Now we need another result about the linear complexity which asserts that $L(\mathbf{c}^{(t)})$ also equals the maximum number of linearly independent vectors among the *state vectors*

$$\left(c_h^{(t)}, c_{h+1}^{(t)}, \dots, c_{h+L-1}^{(t)}\right),$$

where $L = L(\mathbf{c}^{(t)})$; see, for instance [42, Thm. 6.6.2]. An easy estimate using (14) establishes

$$L \;=\; \prod_{i=0}^{r-1} \binom{d-1+t_i}{d-1} \;\le\; \binom{d+p-2}{d-1}^r \;\le\; p^{r(d-1)} \;<\; m.$$

This implies that the state vectors $(c_h^{(t)}, c_{h+1}^{(t)}, \dots, c_{h+L-1}^{(t)})$ are initial subvectors of the rows of $W^{(t)}$ and their scalar multiples. Hence $L(\mathbf{c}^{(t)})$ is at most equal to the maximum number of linearly independent vectors among the rows of $W^{(t)}$, establishing the converse inequality $\mathrm{rank}_q W^{(t)} \ge L(\mathbf{c}^{(t)})$. □

We now obtain the following rank formula for the classical BGW-matrices:

Corollary 8.6 *Let $X = W^*$ be the classical balanced generalized weighing matrix with parameters (10) defined in Proposition 7.7. Then, with $q = p^r$,*

$$\mathrm{rank}_q\, X \;=\; \binom{d+p-3}{d-1}\binom{d+p-2}{d-1}^{r-1}.$$

Proof. Note $X^T = W^{(-1)} = W^{(q-2)}$. Specializing Theorem 8.5 to the case $t = q-2$, where $q \ne 2$, gives the desired formula. □

In particular, the classical BGW-matrix has $\mathrm{rank}_q\, X \ne d$ whenever $q \ge 5$ and is therefore not monomially equivalent to the matrix coming from the simplex code construction. Theorem 8.5 also shows that this construction combined with the application of a power map gives a wealth of monomially inequivalent BGW-matrices with parameters (10) which are distinguishable by their q-ranks. The simplex code construction allows one to do so in an extremely simple way which only uses trivial manipulations over the underlying field $GF(q)$. In contrast, our proofs and the standard version of the classical construction via relative difference sets as well as the explicit trace description all require the use of the extension field $GF(q^d)$ and, in fact, even a primitive element for this field. We note that the construction of primitive elements (or, equivalently, primitive polynomials) is a non-trivial problem; in fact, no polynomial algorithm achieving this is known. Also, the computations required by either the trace description or the RDS-construction are considerably more involved than the simplex code construction, even after a primitive polynomial has been specified.

We also point out that there exist further examples of inequivalent BGW-matrices with parameters (10). For instance, there is an example with parameters (85,64,48) and rank 16 over $GF(4)$, see [44]. Clearly such a matrix is not equivalent to one of the matrices constructed here, since all automorphisms of the group $GF(4)^*$ are actually automorphisms of the field $GF(4)$. It would be interesting to construct further families of monomially inequivalent matrices by using other, more elaborate methods.

9 An application

We conclude this survey with an application of BGW-matrices to the construction of symmetric designs. While Rajkundlia [56] provided the first example of such a construction, the systematic approach to this topic is due to Yury Ionin who showed how one can multiply the parameters of symmetric designs by the cyclotomic numbers. Besides the zero entry all other entries of a balanced generalized matrix W belong to a group. In Ionin's work, this group consists of bijections σ acting on a class $\mathcal{M}$ of matrices which contains the incidence matrix of a symmetric design and satisfies a number of properties. This is explained in the following result of Ionin [30] (which is a modified version of an earlier lemma in [29]).

Lemma 9.1 *Let $v > k > \lambda \geq 0$ be integers. Let $\mathcal{M}$ be a set of $v \times v$ 0-1-matrices, and let G be a finite group of bijections $\mathcal{M} \to \mathcal{M}$ satisfying the following conditions:*

(i) $\mathcal{M}$ contains the incidence matrix M of a symmetric (v, k, λ)-design;

(ii) for all $P, Q \in \mathcal{M}$ and $\sigma \in G$, $(\sigma P)(\sigma Q)^T = PQ^T$;

(iii) $\sum_{\sigma\in G}\sigma M = \frac{k|G|}{v}J$*, where* J *is a matrix with entries* 1 *only;*

(iv) $q = k^2/(k-\lambda)$ *is a prime power;*

(v) G *is cyclic and* $|G|$ *divides* $q-1$.

Then, for every positive integer m*, there exists a symmetric* $(vw, kq^m, \lambda q^m)$*-design, where* $w = (q^{m+1}-1)/(q-1)$.

Proof. Let $W = (\omega_{ij})$ be a $BGW(w, q^m, q^m - q^{m-1})$ over G. We claim that $W \otimes M$ is the incidence matrix of a symmetric $(vw, kq^m, \lambda q^m)$-design. Here the Kronecker product notation $W \otimes M$ is to be read as follows: $W \otimes M$ is a block matrix with block entries $\omega_{ij}M$, where $\omega_{ij}M$ is the image of the matrix M under the bijection $\omega_{ij} \in G$. Thus we need to check

$$\sum_{j=1}^{w}(\omega_{ij}M)(\omega_{hj}M)^T = \begin{cases}(k-\lambda)q^mI + \lambda q^mJ & \text{if } i = h\\ \lambda q^mJ & \text{if } i \neq h\end{cases}$$

(for $i, h = 1, 2, \ldots, w$). If $i = h$, we have for some $\sigma_j \in G$,

$$\sum_{j=1}^{w}(\omega_{ij}M)(\omega_{hj}M)^T = \sum_{j=1}^{q^m}(\sigma_jM)(\sigma_jM)^T = \sum_{j=1}^{q^m}MM^T = (k-\lambda)q^mI + \lambda q^mJ;$$

and if f $i \neq h$, we have for some $\sigma_j, \tau_j \in G$,

$$\begin{aligned}\sum_{j=1}^{w}(\omega_{ij}M)(\omega_{hj}M)^T &= \sum_{j=1}^{q^m-q^{m-1}}(\sigma_jM)(\tau_jM)^T = \sum_{j=1}^{q^m-q^{m-1}}(\tau_j^{-1}\sigma_jM)M^T\\ &= \frac{q^m-q^{m-1}}{|G|}\big(\sum_{\sigma\in G}\sigma M\big)M^T = \frac{k(q^m-q^{m-1})}{v}JM^T\\ &= \frac{k^2(q^m-q^{m-1})}{v}J = \lambda q^mJ. \qquad \square\end{aligned}$$

Ionin calls the group G in Lemma 9.1 the *group of symmetry*; finding such a group is by far the hardest part of his construction. In order to give a concrete illustration of the method, we shall now present Ionin's detailed discussion of the case of symmetric designs associated with $(36, 15, 6)$- and $(36, 21, 12)$-difference sets given in [30].

Example 9.2 We start with a brief description of a $(36, 15, 6)$-difference set, which is the smallest member in the family of difference sets constructed by Spence [60]. Let $\Gamma = \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4$; that is, Γ is the set of triples (x_1, x_2, x_3), where $x_1, x_2 \in \{0,1,2\}$ and $x_3 \in \{0,1,2,3\}$ with the mod 3 and the mod 4 addition, respectively. We shall consider $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ as a 2-dimensional vector space over the field GF(3), and denote its four 1-dimensional subspaces by

$$L_1 = \{(x,0)\colon x = 0,1,2\}, \quad L_2 = \{(0,x)\colon x = 0,1,2\},$$

$$L_3 = \{(x,x)\colon x = 0,1,2\} \quad \text{and} \quad L_4 = \{(x,-x)\colon x = 0,1,2\}.$$

Now we put

$$D_1 \; = \; \{(x_1,x_2,0) \in \Gamma\colon \; (x_1,x_2) \notin L_1\}$$

and, for $i = 2,3,4$,

$$D_i \; = \; \{(x_1,x_2,i-1) \in \Gamma\colon \; (x_1,x_2) \in L_i\}.$$

Then $D = D_1 \cup D_2 \cup D_3 \cup D_4$ is a $(36,15,6)$-difference set in Γ; see, for instance, [7, Theorem VI.9.3]. (Of course, this may be verified directly, if so desired.) In order to specify an incidence matrix for the corresponding symmetric symmetric $(36,15,6)$-design, we first select an order on Γ:

> (x_1,x_2,x_3) precedes (y_1,y_2,y_3) if and only if $x_i < y_i$ and $x_j = y_j$ whenever $j > i$ (for some index i).

Let M be the $(0,1)$-matrix of order 36 whose rows and columns are indexed by elements of Γ in this order, with (x,y)-entry equal to 1 if and only if $y - x \in D$. In order to write down M more explicitly (and to make use of its structural properties, which are needed in what follows), we introduce an operation ρ on the set of 3×3 block matrices: let $P = (P_{ij})$ be a 3×3 block matrix with square blocks; in particular, P can be a 3×3 matrix. Denote by ρP the matrix obtained by cyclically permuting the columns of P, i.e.,

$$\rho \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} \; = \; \begin{pmatrix} P_{13} & P_{11} & P_{12} \\ P_{23} & P_{21} & P_{22} \\ P_{33} & P_{31} & P_{32} \end{pmatrix}.$$

It is easily seen that our matrix M may be written as a circulant 4×4 block matrix:

$$M \; = \; \begin{pmatrix} M_1 & M_2 & M_3 & M_4 \\ M_4 & M_1 & M_2 & M_3 \\ M_3 & M_4 & M_1 & M_2 \\ M_2 & M_3 & M_4 & M_1 \end{pmatrix},$$

where each M_i is a 9×9 matrix. Moreover, each M_i in turn is a circulant 3×3 block matrix:

$$M_i = \begin{pmatrix} M_{i1} & M_{i2} & M_{i3} \\ M_{i3} & M_{i1} & M_{i2} \\ M_{i2} & M_{i3} & M_{i1} \end{pmatrix}.$$

The reader may check $M_{11} = 0$, $M_{12} = M_{13} = J$, $M_{21} = M_{22} = M_{23} = M_{31} = M_{41} = I$, $M_{32} = M_{43} = \rho I$, and $M_{33} = M_{42} = \rho^2 I$.

We choose $\mathcal{M}$ as the set of all block matrices $P = (P_{ij})$, $i, j = 1, 2, 3, 4$, where each P_{ij} is in turn a block matrix $P_{ij} = (P_{ijkl})$, $k, l = 1, 2, 3$, satisfying the following two conditions:

- each P_{ijkl} is a 3×3 $(0,1)$-matrix;
- for $i = 1, 2, 3, 4$, there is a unique $h_i = h_i(P) \in \{1, 2, 3, 4\}$ such that
  1. $(P_{ijk1}, P_{ijk2}, P_{ijk3})$ is a permutation of(O, J, J) for $j = h_i$ and all k
  2. $P_{ijkl} \in \{I, \rho I, \rho^2 I\}$ for $j \neq h_i$ and all k, l.

Note that the incidence matrix M constructed above belongs to $\mathcal{M}$. Now let us define a bijection $\sigma\colon \mathcal{M} \to \mathcal{M}$ by $\sigma P = P'$, where

- for $i = 1, 2, 3, 4$ and $j = 2, 3, 4$, $P'_{ij} = P_{i,j-1}$;
- for $i = 1, 2, 3, 4$, if $h_i = 4$, then $P'_{i1} = \rho P_{i4}$;
- for $i = 1, 2, 3, 4$, if $h_i \neq 4$, then $P'_{i1kl} = \rho P_{i4kl}$ for all k, l.

Then the cyclic group G generated by σ has order 12. Let us verify the condition $(\sigma P)(\sigma Q)^T = PQ^T$ for all $P, Q \in \mathcal{M}$; write $P' = \sigma P$ and $Q' = \sigma Q$. It suffices to show that, for $i = 1, 2, 3, 4$,

$$P'_{i1} Q'^T_{i1} = P_{i4} Q^T_{i4}. \tag{15}$$

If $h_i(P) = h_i(Q) = 4$ or $h_i(P) \neq 4$ and $h_i(Q) \neq 4$, then P'_{i1} is obtained from P_{i4} by the same permutation of columns as Q'_{i1} from Q_{i4}, so (15) is clear. Suppose $h_i(P) = 4$ and $h_i(Q) \neq 4$. Then $(P_{i4k1}, P_{i4k2}, P_{i4k3})$ is a permutation of (O, J, J) and the matrices $Q_{i4k1}, Q_{i4k2}, Q_{i4k3}$ have the same row sum (equal to 1). Therefore

$$\sum_{l=1}^{3} P'_{i1kl} Q'^T_{i1kl} = \sum_{l=1}^{3} P_{i4kl} Q^T_{i4kl} = 2J,$$

and (15) follows.

Next, one readily verifies $\sum_{n=0}^{11} \sigma^n M = 5J$. Thus the set $\mathcal{M}$, the matrix M, and the group G satisfy the assumptions of Lemma 9.1 for $(v, k, \lambda) = (36, 15, 6)$ with $q = 25$ and $|G| = 12$. Note that the sum of the entries of any row of any matrix $P \in \mathcal{M}$ is equal to 15.

Finally, let $\overline{M} = J - M$ and $\overline{\mathcal{M}} = \{J - P\colon P \in \mathcal{M}\}$. Then the same group G and the set of matrices $\overline{\mathcal{M}}$ satisfy the assumptions of Lemma 9.1 for $(v, k, \lambda) = (36, 21, 12)$ with $q = 49$, where now the sum of the entries of any row of any matrix $P \in \overline{\mathcal{M}}$ equals 21.

Applying Lemma 9.1, we obtain two infinite series of symmetric designs, namely with parameters

$$v = 3(5^{2m+2} - 1)/2, \quad k = 3 \cdot 5^{2m+1}, \quad \lambda = 6 \cdot 5^{2m}$$

and

$$v = 3(7^{2m+2} - 1)/4, \quad k = 3 \cdot 7^{2m+1}, \quad \lambda = 12 \cdot 7^{2m}. \quad \square$$

Despite of the difficult problem of determining a suitable group of symmetry, in a series of papers [29, 30, 31, 32, 33] Ionin was able to construct several infinite classes of symmetric designs with new parameters. We will briefly discuss some of these classes now.

In [29], it is shown that the designs corresponding to some McFarland and Spence difference sets can serve as starter designs. In [30], by using the $(36, 15, 6)$- and $(36, 21, 12)$-difference sets discussed in Example 9.2 together with a product construction, an extension of the result in [29] is proved. Later, Ionin made spectacular progress in [32] by exploiting the theory of building blocks of Davis and Jedwab [14] for the construction of difference sets (see also [7] for an exposition of this theory). Applying these results to McFarland difference sets and their complements, Spence difference sets and their complements, Davis–Jedwab difference sets and their complements, and Hadamard difference sets, Ionin obtained seven infinite families of symmetric designs, which we will list below.

Ionin's constructions may also be viewed in terms of the theory of decompositions of symmetric designs introduced by Ionin and Shrikhande in [37]. The method of global decomposition produces an incidence matrix of a symmetric design as a block matrix, with each block being a zero matrix or an incidence matrix of a smaller symmetric design. The method of local decomposition represents incidence matrices of a residual and a derived design of a symmetric design as block matrices, with each block being a zero matrix or an incidence matrix of a smaller residual or derived design, respectively. We refer the reader to the monograph [38] for details, including a complete proof of the following result.

Theorem 9.3 *There exist symmetric (v,k,λ)-designs with the following parameters, where d and m denote positive integers, where p is any prime power, and where q is a prime power defined in terms of p and/or d:*

$$v = \frac{p^{d+1}(q^{2m}-1)}{q-1},\ \ k = q^{2m-1}p^d,\ \ \lambda = (q-1)q^{2m-2}p^{d-1},\ \ q = \frac{p^{d+1}-1}{p-1};$$

$$v = \frac{p^d(q^{2m}-1)}{(p-1)(p^d+1)},\ \ k = p^d q^{2m-1},\ \ \lambda = p^d(p^d+1)(p-1)q^{2m-2},\ \ q = p^{d+1}+p-1;$$

$$v = \frac{2\cdot 3^d(q^{2m}-1)}{3^d+1},\ \ k = 3^d q^{2m-1},\ \ \lambda = \frac{3^d(3^d+1)q^{2m-2}}{2},\ \ q = \frac{3^{d+1}+1}{2};$$

$$v = \frac{3^d(q^{2m}-1)}{2(3^d-1)},\ \ k = 3^d q^{2m-1},\ \ \lambda = 2\cdot 3^d(3^d-1)q^{2m-2},\ \ q = 3^{d+1}-2;$$

$$v = \frac{2^{2d+3}(q^{2m}-1)}{q+1},\ \ k = 2^{2d+1}q^{2m-1},\ \ \lambda = 2^{2d-1}(q+1)q^{2m-2},\ \ q = \frac{2^{2d+3}+1}{3};$$

$$v = \frac{2^{2d+3}(q^{2m}-1)}{3(q-1)},\ \ k = 2^{2d+1}q^{2m-1},\ \ \lambda = 3\cdot 2^{2d-1}(q-1)q^{2m-2},\ \ q = 2^{2d+3}-3;$$

and

$$v = \frac{h((2h-1)^{2m}-1)}{h-1},\ \ k = h(2h-1)^{2m-1},\quad \lambda = h(h-1)(2h-1)^{2m-2},$$

where $h = \pm 3\cdot 2^d$ and $|2h-1|$ is a prime power.

In [33], Ionin generalized Lemma 9.1 to not necessarily symmetric designs. In particular, he used these methods to construct certain quasi-residual and quasi-derived designs; moreover, he gave a sufficient condition for combining these designs into a symmetric design. In this way, he obtained the following infinite family of (in most cases new) symmetric designs; the same approach also yields the symmetric designs in the Wilson–Brouwer family (Family 11 in [12]).

Theorem 9.4 *Let q and $r = (q^d - 1)/(q-1)$ be prime powers. Then, for every nonnegative integer m, there exists a symmetric design with parameters*

$$\left(1 + \frac{qr(r^{m+1}-1)}{r-1}, r^{m+1}, \frac{r^m(r-1)}{q}\right). \qquad \square$$

For a wealth of further constructions of designs and graphs with the aid of BGW-matrices, we refer the reader to the survey [43] and the references given there.

Acknowledgement. This paper contains the notes to a *minicorso* given at the Università di Roma "La Sapienza" in the framework of an Erasmus/Socrates program; the author gratefully acknowledges the hospitality and financial support extended to him.

The present notes are based to some extent on the author's previous survey [43], though the treatment differs substantially: first of all, there are more (and also more detailed) proofs; second, the algebraic machinery of group rings has been avoided; third, a thorough treatment of square divisible designs with disjoint blocks has been included; and, finally, the extensive survey of applications has been replaced by discussing one example in considerable detail.

References

[1] M. Antweiler and A. Bömer: Complex sequences over $GF(p^m)$ with a two-level autocorrelation function and a large linear span. *IEEE Trans. Inf. Th.* **38** (1992), 120–130.

[2] K.T. Arasu, J.F. Dillon, D. Jungnickel and A. Pott: The solution of the Waterloo problem. *J. Comb. Th. (A)* **71** (1995), 316–331.

[3] K.T. Arasu, J.F. Dillon, D. Jungnickel and A. Pott: Relative difference sets with $n = 2$. *Discr. Math.* **147** (1995), 1–17.

[4] K.T. Arasu, J.F. Dillon, K.H. Leung and S.L. Ma: Cyclic relative difference sets with classical parameters. *J. Comb. Th. (A)* **94** (2001), 118–126.

[5] R.D. Baker: Elliptic semi-planes I: existence and classification. *Congr. Numer.* **19** (1977), 61–73.

[6] G. Berman: Families of generalized weighing matrices. *Canadian J. Math.* **30** (1978), 1016–1028.

[7] T. Beth, D. Jungnickel and H. Lenz: *Design Theory (2nd edition).* Cambridge University Press, Cambridge (1999).

[8] M. Bhaskar Rao: Group divisible family of PBIB designs. *J. Indian Stat. Ass.* **4** (1966), 14–28.

[9] M. Bhaskar Rao: Balanced orthogonal designs and their application in the construction of some BIB and group divisible designs. *Sankhyā (A)* **32** (1970), 439–448.

[10] A. Blokhuis, D. Jungnickel and B. Schmidt: Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2. *Proc. Amer. Math. Soc.* **130** (2002), 1473–1476.

[11] P.J. Cameron, P. Delsarte and J.-M. Goethals: Hemisystems, orthogonal configurations, and dissipative conference matrices. *Philips J. Res.* **34** (1979), 147–162.

[12] C. J. Colbourn and J. H. Dinitz: *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton (1996).

[13] W.S. Connor: Some relations among the blocks of symmetric group divisible designs. *Ann. Math. Stat.* **23** (1952), 602–609.

[14] James A. Davis and Jonathan Jedwab: A unifying construction of difference sets. *J. Comb. Th. (A)* **80** (1997), 13–78.

[15] P. Dembowski: *Finite geometries.* Springer, Berlin (1968, Reprint 1997).

[16] W. de Launey: On the non-existence of generalized weighing matrices. *Ars Comb.* **17-A** (1984), 117–132.

[17] W. de Launey: Some constructions for square GBRD's and some new infinite families if generalised Hadamard matrices. Manuscript (1989)

[18] W. de Launey and D.G. Sarvate: Non-existence of certain GBRD's. *Ars Comb.* **18**, 5–20 (1984).

[19] M.J. Ganley: On a paper of Dembowski and Ostrom. *Arch. Math.* **27** (1976), 93–98.

[20] D. Ghinelli(-Smit): *Nonexistence theorems for automorphism groups of divisible square designs.* Ph.D. Thesis, University of London (1983).

[21] D. Ghinelli(-Smit): Automorphisms and generalized incidence matrices of point-divisible designs. *Ann. Discr. Math.* **18** (1983), 377–400.

[22] D. Ghinelli(-Smit): Hall-Ryser type theorems for relative difference sets. *Ann. Discr. Math.* **37** (1988), 189–194.

[23] D. Ghinelli: A rational congruence for a standard orbit decomposition. *European J. Combin.* **11** (1990), 105–113.

[24] D. Ghinelli and D. Jungnickel: Finite projective planes with a large abelian group. In: *Surveys in Combinatorics 2003* (Ed. C.D. Wensley), pp. 175–237. Cambridge University Press, Cambridge (2003).

[25] P. Gibbons and R. Mathon: Construction methods for Bhaskar Rao and related designs. *J. Austral. Math. Soc. (A)* **42** (1987), 5–30.

[26] P. Gibbons and R. Mathon: Group signings of symmetric balanced incomplete block designs. *Ars Comb.* **23-A** (1987), 123–134.

[27] T.C. Hine and V.C.Mavron: Embeddable transversal designs. *Discr. Math.* **29** (1980), 191–200.

[28] D.R. Hughes and F.C. Piper: *Projective Planes (2nd edition)*. Springer (1982).

[29] Y.J. Ionin: A technique for constructing symmetric designs. *Designs, Codes and Cryptography* **14** (1997), 147–158.

[30] Y.J. Ionin: New symmetric designs from regular Hadamard matrices. *Electronic J. Comb.* **5** (1998), R1.

[31] Y.J. Ionin: Symmetric subdesigns of symmetric designs. *J. Comb. Math. Comb. Comput.* **29** (1999), 65–78.

[32] Y.J. Ionin: Building symmetric designs with building blocks. *Designs, Codes and Cryptography* **17** (1999), 159–175.

[33] Y.J. Ionin: Applying balanced generalized weighing matrices to construct block designs. *Electronic J. Comb.* **8** (2001), R12.

[34] Y.J. Ionin: *Regular Hadamard matrices generating infinite families of symmetric designs. Designs, Codes and Cryptography* **32** (2004), 227–233.

[35] Y.J. Ionin and H. Kharaghani: Doubly regular digraphs and symmetric designs. *J. Comb. Th. (A)* **101** (2003), 35–48.

[36] Y.J. Ionin and K. Mackenzie-Fleming: A technique for constructing non–embeddable quasi–residual designs. *J. Comb. Des.* **10** (2002), 160–172.

[37] Y.J. Ionin and Mohan S. Shrikhande: Decomposable symmetric designs. *Discr. Math.*, to appear.

[38] Y.J. Ionin and Mohan S. Shrikhande: *Combinatorics of Symmetric Designs.* Cambridge University Press, Cambridge (to appear).

[39] D. Jungnickel: On difference matrices, resolvable transversal designs and generalized Hadamard matrices. *Math. Z.* **167** (1979), 49–60.

[40] D. Jungnickel: A note on square divisible designs. *J. Geom.* **15** (1980), 153–157.

[41] D. Jungnickel: On automorphism groups of divisible designs. *Canadian J. Math.* **34** (1982), 257–297.

[42] D. Jungnickel: *Finite Fields: Structure and Arithmetics.* Bibliographisches Institut, Mannheim (1993).

[43] D. Jungnickel and H. Kharaghani: Balanced generalized weighing matrices and their applications. *Le Matematiche,* submitted.

[44] D. Jungnickel and V.D. Tonchev: Perfect codes and generalized balanced weighing matrices. *Finite Fields Appl.* **5** (1999), 294–300.

[45] D. Jungnickel and V.D. Tonchev: Perfect codes and generalized balanced weighing matrices, II. *Finite Fields Appl.* **8** (2002), 155–165.

[46] D. Jungnickel and K. Vedder: Square divisible designs with $k = (n+1)\mu$. *Archiv Math.* **43** (1984), 275–284.

[47] H. Kharaghani: On a class of symmetric balanced generalized weighing matrices. *Designs, Codes and Cryptography* **30** (2003), 139–149.

[48] K.H. Leung, S.L. Ma and B.Schmidt: Constructions of relative difference sets with classical parameters and circulant weighing matrices. *J. Comb. Th. (A)* **99** (2002), 111–127.

[49] R. Lidl and H. Niederreiter: *Finite fields.* Addison-Wesley, Reading, Mass. (1983).

[50] F.J. MacWilliams and N.J.A. Sloane: *The theory of error-correcting codes.* North-Holland, Amsterdam (1977).

[51] R. Mathon: On a new divisible semiplane. Announcement at the 11th British Combinatorial Conference (1987).

[52] V.C. Mavron: A class of symmetric designs. *Geom. Ded.* **1** (1983), 468–476.

[53] V.C. Mavron, T.P. McDonough and C.A. Pallikaros: A difference matrix construction and a class of balanced generalized weighing matrices. *Arch. Math.* **76** (2001), 259–264.

[54] R.C. Mullin and R.G. Stanton: Group matrices and balanced weighing designs. *Util. Math.* **8** (1975), 303–310.

[55] A. Pott: *Finite Geometry and Character Theory.* Lecture Notes in Mathematics **1601**, Springer, Berlin (1995).

[56] D.P. Rajkundlia: Some techniques for constructing infinite families of BIBDs. *Discr. Math.* **44** (1983), 61–96.

[57] J. Seberry: Some remarks on generalized Hadamard matrices and theorems of Rajkundlia on SBIBDS. *Lect. Notes Math.* **748**, 154–164. Springer (1979).

[58] J. Seberry: Some families of partially balanced incomplete block designs. In: *Combinatorial mathematics IX*. Lect. Notes Math. **952**, 378–386. Springer (1982)

[59] J. Seberry and A.L. Whiteman: New Hadamard matrices and conference matrices obtained via Mathon's construction. *Graphs Comb.* **4** (1988), 355–377.

[60] E. Spence: A family of difference sets in non-cyclic groups. *J. Comb. Th. (A)* **22** (1977), 103–106.

[61] V.D. Tonchev: *Combinatorial Configurations*. Longman-Wiley, New York (1988).

[62] V.D. Tonchev: Codes. In: *The CRC Handbook of Combinatorial Designs* (Eds. C.J. Colbourn and J.H. Dinitz). CRC Press, Boca Raton (1996), pp. 517–543.

[63] V.D. Tonchev: Linear perfect codes and a characterization of the classical designs. *Designs, Codes and Cryptography* **17** (1999), 121–128.

[64] H. Zassenhaus: Über endliche Fastkörper. *Abh. Math. Sem. Hamburg* **11** (1935), 187–220.