LE MATEMATICHE
Vol. LIX (2004) – Fasc. I–II, pp. 225–261

# BALANCED GENERALIZED WEIGHING MATRICES AND THEIR APPLICATIONS

DIETER JUNGNICKEL - H. KHARAGHANI

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 surveying these basic connections, we will focus attention on 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 might be 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.

The final section of this survey will consider applications to constructions of designs and graphs. We will divide this section into six parts. The first of these will deal with the work of Ionin. The second part will be devoted to Bush–type Hadamard matrices and twin designs. In the third part we will

*Keywords*: Balanced generalized weighing matrix, Relative difference set, Simplex code, Symmetric design, Regular Hadamard matrix, Productive regular Hadamard matrix, Bush–type Hadamard matrix

discuss the productive regular Hadamard matrices and symmetric designs. In the fourth part applications to constructing strongly regular graphs are given. The fifth part concerns doubly regular digraphs, and the final part deals with some newly emerging applications.

## 1. Basic facts.

We will assume familiarity with some basic facts and notions from coding theory and combinatorial design theory; see, for instance, [6] and [70]. Moreover, we will also require some background concerning finite fields and shift register sequences; for this we refer to [58] and [46]. Group rings will also appear from time to time; see [6] for the required background.

We shall start with the definition of a *partial difference matrix* introduced in 1982 by the first author [45] (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 [45]: there we used the parameter $\lambda = \mu/|G|$ instead of $\mu$; 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
$$\{d_{ai}d_{bi}^{-1} : 1 \leq i \leq \beta, d_{ai}, d_{bi} \neq 0\}$$
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 [6], 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 [7], [8]. The more general concept was introduced in 1982 by Seberry [67]; in the same year [45] finally appeared, after having been submitted at the end of 1979.

We mention the following simple but useful observation [45], Lemma 6.6:

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

**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 $G/H$.*

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

In particular, if we replace each non-zero entry of a $PDM(m, k, \mu)$ $D$ by 1, we obviously obtain the incidence matrix of an $(m, k, \mu)$-design $\mathcal{D}$. This observation immediately gives the following two additional properties, 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 $r > n\lambda$, Fisher's inequality applied to $\mathcal{D}$ yields $\beta \geq m$; and for $r = n\lambda$, we get $k = m$, and then a well-known result on difference matrices gives the same conclusion; see [43] or [6], Corollary VIII.3.7. As usual, the case of equality is of particular interest:

**Definition 1.3.** 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 [63], Hadamard matrices, and conference matrices, respectively, which explains the preceding terminology; we refer the reader to the relevant sections in [13] 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: a $GH(3, 2)$ and a $BGW(5, 4, 3)$ over $G$.

The following important result is due to [12] (using different language). An alternative combinatorial proof can be found in [44]. 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 1.4.** *Let $G$ be a finite group. If $D$ is a $BGW(m, k, \mu)$ over $G$, then so is $D^*$.*

Theorem 1.4 may also be proved using group rings; see [37]. Recall that the integral *group ring*

$$\mathbb{Z}G = \{\sum_{g\in G} a_g g : a_g \in \mathbb{Z}\}$$

is the free $\mathbb{Z}$-module with $G$ as basis, equipped with the multiplication

$$(\sum_{g\in G} a_g g)\cdot(\sum_{h\in G} b_h h) = \sum_{g,h\in G} a_g b_h gh.$$

We will use the following standard conventions. For $X = \sum a_g g \in \mathbb{Z}G$ and $t \in \mathbb{Z}$ we write $X^{(t)} = \sum a_g g^t$; for $r \in \mathbb{Z}$ we write $r$ for the group ring element $r \cdot 1$; and for $S \subseteq G$ we write – by abuse of notation – $S$ instead of $\sum_{g\in S} g$, so that $S^{(-1)} = \sum_{g\in S} g^{-1}$. Group rings are a standard tool in the theory of difference sets and related objects; see [6].

Clearly, any partial difference matrix $D$ may be viewed as a matrix over the group ring $\mathbb{Z}G$ with all entries coming from the set $G\cup\{0\}$. We may characterize balanced generalized weighing matrices in terms of a matrix equation over the integral group ring:

**Lemma 1.5.** *Let $G$ be a finite group. A matrix $D$ of order $m$ with entries from the set $G \cup \{0\}$ is a $BGW(m, k, \mu)$ over $G$ if and only if the following matrix equation holds over the group ring $\mathbb{Z}G$:*

$$DD^* = \Big(k - \frac{\mu}{|G|}G\Big)I + \frac{\mu}{|G|}GJ, \tag{1}$$

*where $J$ denotes the matrix with all entries* 1.

*Proof.* Equation (1) just re-formulates the following two basic facts defining $BGW$-matrices:

- Each row of $D$ contains exactly $k$ nonzero entries, so that the multiset $\{d_{ai}d_{ai}^{-1} : 1 \le i \le \beta, d_{ai} \neq 0\} = k \cdot 1$.
- For all $a, b \in \{1, \dots, m\}$ with $a \neq b$, $\{d_{ai}d_{bi}^{-1} : 1 \le i \le \beta,\ d_{ai}, d_{bi} \neq 0\} = \mu G/|G|$. □

Finally, we introduce one more 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.

## 2. Related geometries.

We first show that partial difference matrices are equivalent to certain divisible designs. Recall that a *divisible design* $\mathcal{D}$ with parameters $(m, n, k, \lambda)$ is an incidence structure which consists of $mn$ points split 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 $\lambda$ common blocks. [2]

We note that each point of $\mathcal{D}$ is on exactly $r = \lambda(m-1)n/(k-1)$ blocks, and that the total number of blocks is $b = \lambda m(m-1)n^2/k(k-1)$. A *square* divisible design has $b = mn$; if $\mathcal{D}$ is actually isomorphic to its dual design $\mathcal{D}^*$ (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 [45, Lemma 6.2].

**Lemma 2.1.** *Let $\mathcal{D}$ be a class regular divisible design (with respect to $G$). Then $G$ acts semiregularly on the block set of $\mathcal{D}$.*

*Proof.* Assume $B = B^\sigma$ for some block $B$ of $\mathcal{D}$ 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 $\mathcal{D}$ at most once, we conclude $p = p^\sigma$. By the class regularity of $\mathcal{D}$, we have $\sigma = 1$. Thus $G$ acts semiregularly on the block set. □

We now prove the following simple but fundamental result also established in [45]:

[2] There is a more general notion of divisible design or GDD where points in the same class are joined by a constant number $\lambda'$ of blocks; see [6]. For our purposes, the special case given here (where $\lambda' = 0$) suffices.

**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 $(m, n, k, \lambda)$ 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 $\beta$ columns) and define $\mathcal{D}$ as follows. The point set of $\mathcal{D}$ is the union of the classes

$$V_i = \{(i, x) : x \in G\} \qquad (i = 1, \dots, m),$$

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

$$B_{jg} = \{(i, d_{ij}g) : d_{ij} \neq 0,\ i = 1, \dots, m\}.$$

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 $\mathcal{D}$ 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 $\mathcal{D}$ be a divisible design with parameters $(m, n, k, \lambda)$ admitting $G$ as a class regular automorphism group. By definition, $G$ acts regularly on each point class of $\mathcal{D}$; hence we may choose a *base point* $p_i$ in each point class $V_i$ $(i = 1, \dots, m)$ 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 $\mathcal{D}$; thus the block set splits into $\beta$ block orbits $\mathcal{B}_1, \dots, \mathcal{B}_\beta$, 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* $B_j \in \mathcal{B}_j$ (for $j = 1, \dots, \beta$) 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 $G$ by putting

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

Similar arguments as in the first part of the proof show that $D$ is the desired $PDM(m, k, \mu)$ over $G$. □

Using the results of the previous section, we have the following consequence of Theorem 2.2 also noted in [45]:

**Corollary 2.3.** *Let $\mathcal{D}$ be a class regular divisible design with parameters $(m, n, k, \lambda)$ and $b$ blocks. Then $b \geq mn$; and if $\mathcal{D}$ is square, then it is in fact symmetric.*

We mention another interesting consequence of Theorem 2.2 which shows that the notion of class regularity is a generalization of the concept of $(p, L)$-transitivity for projective planes; we refer the reader to [24] for the necessary background on finite projective planes. The following result was established in [43], [45].

**Theorem 2.4.** *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 $(p, L)$. The existence of a 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 $(p, L)$.*

*Proof.* We shall merely sketch the proof of the first assertion; the second claim follows in a similar manner. Let $D$ be a $GH(n, 1)$ over $G$, and let $\mathcal{D}$ be the associated class regular divisible design with parameters $(n, n, n, 1)$. We first note that $\mathcal{D}$ is resolvable: the line orbits of $G$ on $\mathcal{D}$ 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 $\mathcal{D}$ and obtain a divisible design $\mathcal{A}$ 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 $\infty$. This gives a projective plane $\mathcal{P}$ of order $n$. It is now easily checked that $\mathcal{P}$ is $(\infty, L_\infty)$-transitive with $G$ as the corresponding elation group, where $L_\infty$ is the line formed by all the points which have been adjoined. Moreover, this construction may be reversed. □

## 3. The relation to relative difference sets.

There is a close connection between $BGW$-matrices and relative difference sets. Let us recall the required definition; for more background, the reader is referred to [6], [64].

**Definition 3.1.** 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 $(m, n, k, \lambda)$, if the list of differences $(rs^{-1} : r, s \in R, r \neq s)$ contains no element of $N$ and covers every element in $G/N$ exactly $\lambda$ 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 $(m, n, k, \lambda)$-RDS; and in the special case $n = 1$, one simply speaks of a $(v, k, \lambda)$-*difference set.*

As for $BGW$-matrices, this definition can be re-formulated in terms of group rings:

**Lemma 3.2.** *Let $G$ be a group with a normal subgroup $N$ of order $n$ and index $m$. Then an element $R \in \mathbb{Z}G$ is an $(m, n, k, \lambda)$-difference set in $G$ relative to $N$ if and only if the following equation holds in $\mathbb{Z}G$:*

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

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 $\mathcal{D}$ is an automorphism group which acts regularly both on the point set and the block set. Given a subset $R$ of a group $G$, we define an incidence structure dev $R$, the *development* of $R$, as follows:

$$\text{dev}R = (G, \mathcal{B}, \in) \qquad \text{with} \qquad \mathcal{B} = \{Rg : g \in G\}.$$

The following result is due to [45]; see also [64], 1.1 for a proof.

**Theorem 3.3.** *Let $G$ be a group with a normal subgroup $N$ of order $n$ and index $m$, and let $R$ be an $(m, n, k, \lambda)$-difference set in $G$ relative to $N$. Then* dev *$D$ is a symmetric divisible design with parameters $(m, n, k, \lambda)$ which admits $G$ 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 normal subgroup can be represented in this way.*

Combining Theorems 3.3 and 2.2, we have the following interesting result due to [45].

**Theorem 3.4.** *Let $G$ be a group with a normal subgroup $N$ of order $n$ and index $m$, and assume the existence of an $(m, n, k, \lambda)$-difference set in $G$ relative to $N$. Then there also exists a $BGW(m, k, n\lambda)$ over $N$.*

It is, of course, possible to describe the $BGW$-matrices of Theorem 3.4 explicitly. The following result is [37], Theorem 10.3.1, generalizing two important special cases given in [45].

**Proposition 3.5.** *Let $G$ be a group with a normal subgroup $N$ of order $n$ and index $m$, and let $R$ be an $(m, n, k, \lambda)$-difference set in $G$ relative to $N$. In addition, let $x_1, x_2, \ldots, x_m$ be representatives of all distinct cosets of $N$ in $G$, and let $W = (w_{ij})$ be the $m \times m$ matrix with entries from $N \cup \{0\}$ defined by*

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

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

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 now quote two fundamental results from [45]; for proofs, see also [37], 10.3. We require two more definitions.

An *$\omega$-circulant* matrix $W$ is defined by the following property: each row of $W$ 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 $\omega$ and then the result is put in the first position of the shifted row. Formally,

$$w_{i,j} = w_{i+1,j+1} \text{ for } j = 1, \dots, m-1 \text{ and } w_{i+1,1} = \omega w_{i,m}.$$

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

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

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

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

**Theorem 3.6.** *Let $N$ be a cyclic group of order $n$, and let $\omega$ be a generator of $N$. Then the existence of an $\omega$-circulant $BGW(m, k, \mu)$ over $N$ is equivalent to the existence of an $(m, n, k, \lambda)$-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 $\lambda = \mu/n$.*

**Theorem 3.7.** *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 $(m, n, k, \lambda)$-difference set in $G$ relative to $N$, where $\lambda = \mu/n$.*

## 4. 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 [13] (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 4.1.** *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 4.1 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 4.1 we want to discuss the existence problem for abelian group invariant $GH(n, 1)$-matrices; this just combines known results but has – to our knowledge – not been stated explicitly before. As it fits nicely into our topic, it seems worthwhile to do so now.

**Theorem 4.2.** *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 3.7, 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 [20] and [9], an abelian relative difference set of this type exists if and only if $n$ is an odd prime power; see also [21], 4, for an exposition of this result. Such relative difference sets are known whenever $G$ is elementary abelian. □

Actually, *all* known abelian $(n, n, n, 1)$-RDS occur in elementary abelian groups; for instance, every commutative semifield plane admits a representation by such an RDS, see [21]. On the theoretical side, the results of [9] only guarantee that $G$ has rank at least $b + 1$, where $n = p^b$ for the odd prime $p$. 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: *proper $BGW$-matrices*. We therefore just collect the most interesting general existence results in the following theorem. We refer the reader to [13], IV.11, both for references and for further results such as recursive constructions and nonexistence theorems; we stress that the existence of generalized Hadamard matrices $GH(s, \lambda)$, where $s$ is not a prime power, is still an open problem.

**Theorem 4.3.** *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;*
- $\lambda$ *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 $t$.*

We now turn our 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

$$(2) \qquad m = \frac{q^d - 1}{q - 1}, \quad k = q^{d-1} \quad \text{and} \quad \mu = q^{d-1} - q^{d-2},$$

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 4.9). 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 5.

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 [5] (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* means the relative trace function Tr from $GF(q^d)$ to $GF(q)$ (not the absolute trace to the prime subfield); thus

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

**Lemma 4.4.** *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*

$$(3) \qquad m = \frac{q^d - 1}{q - 1}, \quad n = q - 1, \quad k = q^{d-1} \quad \textit{and} \quad \lambda = q^{d-2}$$

*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

$$|R| = |\ker \mathrm{Tr}| = |GF(q^d)|/|\mathrm{im}\,\mathrm{Tr}| = q^{d-1}.$$

For $g \in G$, let $A(g)$ denote the number of solutions of $g = x_1x_2^{-1}$ 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 $g \in G \setminus N$. □

We may rephrase Lemma 4.4 as follows: $G$ 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 3.6 gives the following result:

**Theorem 4.5.** *Let $q$ be a prime power and $d \geq 2$ an integer, and let $\omega$ be a generator of $N = GF(q)^*$. Then there exists an $\omega$-circulant BGW-matrix with parameters (2) over $N$.*

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

**Theorem 4.6.** *Let $q$ be a prime power and $d \geq 2$ an integer. Then there exists a circulant BGW-matrix with parameters (2) over $GF(q)$ whenever $(q-1,\ \frac{q^{d+1}-1}{q-1}) = 1$.*

*Proof.* The condition $(q-1,\ \frac{q^{d+1}-1}{q-1}) = 1$ 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 4.4 and Theorem 3.7. □

We now give an explicit description of the classical $BGW$-matrices taken from [49]. For this purpose, we let $\beta$ be a primitive element of $GF(q^d)$, so that we may take $\omega = \beta^m$. By Proposition 3.5, the $\omega$-circulant $BGW$-matrix $X = (x_{ij})_{i,j=0,\dots,m-1}$ with entries in $GF(q)$ and parameters (2) obtained from the classical RDS looks as follows: if there is a (necessarily unique) element $r$ of $R\beta^i$ in the coset $N\beta^j$, then $x_{ij} = \beta^{-j}r$; and otherwise $x_{ij} = 0$.

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

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

$$\omega^{-1}\mathrm{Tr}\,\beta^j = \mathrm{Tr}(\omega^{-1}\beta^j) = \mathrm{Tr}\beta^{j-m} = \mathrm{Tr}\beta^{m(q-2)+j}.$$

This gives the following result:

**Proposition 4.7.** *Let $X$ be the classical $\omega$-circulant $BGW$-matrix with parameters (2) associated with the classical relative difference sets constructed in Lemma 1.4. Then $X = W^{(-1)}$, where, with $v = m(q-1) = q^d - 1$,*

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

Clearly, if $X$ is a $BGW$-matrix over an abelian group, then so is $X^{(-1)}$. Hence Proposition 4.7 yields the following consequence, which will be of interest in the next section.

**Corollary 4.8.** *Let $q$ be a prime power and $d \geq 2$ an integer, let $\beta$ be a primitive element of $GF(q^d)$, and put $\theta = \beta^{-m}$. Then the $m \times m$ matrix $W$ with entries from $GF(q)$ defined in Corollary 4.7 is a $\theta$-circulant BGW-matrix with parameters (2) 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 [13], IV.4, and to [37], 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 [71], so that the groups which arise as the multiplicative group of a finite nearfield are known; see also [15], 5.2 and [37], 10.1.

**Theorem 4.9.** *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* [60]*;*
    2. *$q$ is even, $d$ is odd, and $G$ is the cyclic group of order $n = 2(q-1)$* [2]*;*
    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 $n = 4(q-1)$* [57]*;*
    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* [13]*).*

*In addition, the following four sporadic cases are known to occur: a circulant $BGW(13, 9, 6)$ over the symmetric group $S_3$* [23], [66]*; a $BGW(15, 7, 3)$* [3] *and a $BGW(45, 12, 3)$* [59] *over the cyclic group of order 3; and a $BGW(19, 9, 4)$ over the cyclic group of order 2* [18], [23].

A few comments regarding the more recent examples in the cases 2. and 3. of Theorem 4.9 are in order. The examples constructed in [2] actually belong to cyclic relative difference sets and, hence, are $\omega$-circulant. In fact, [2] contains a considerably stronger result:

**Theorem 4.10.** *Let $q$ be a prime power. A cyclic relative difference set with parameters*

$$m = \frac{q^d - 1}{q - 1}, \quad n, \; k = q^{d-1} \quad \textit{and} \quad \lambda = \frac{q^{d-2}(q-1)}{n} \tag{4}$$

*exists if and only if one of the following 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 classical parameters cannot be realized over a cyclic group for the case $n = 4(q - 1)$; nevertheless, the examples of [57] also belong to relative difference sets with classical parameters, but here the underlying group is the direct product of two cyclic groups, one of which has order 2.

The existence of special types of $BGW$-matrices, namely *symmetric* and *skew* matrices, will be discussed later in the context of applications to the construction of designs; see Theorems 6.17 and 6.20.

We conclude this section with two non-existence results due to [16]; the proof ultimately relies on Lemma 1.5 and requires a careful analysis of equation (1).

**Theorem 4.11.** *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.*

## 5. $BGW$-matrices with classical parameters.

In this section, we will summarize the work of [48, 49] concerning $BGW$-matrices with classical parameters (2), 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 5.1.** *Let $W$ be any balanced generalized weighing matrix with classical parameters (2) over $GF(q)^*$. Then* $\text{rank}_q M \geq d$.

In fact, we have already met an example realizing this bound, as the following strengthening of Corollary 4.8 shows.

**Theorem 5.2.** *Let $q$ be a prime power and $d \geq 2$ an integer, let $\beta$ be a primitive element of $GF(q^d)$, and put $\theta = \beta^{-m}$. Then the $\theta$-circulant matrix $W$ over $GF(q)$ defined in Proposition 1.7 is a BGW-matrix with parameters (2) satisfying* $\operatorname{rank}_q W = d$.

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

$$\mathbf{c} = (\mathrm{Tr}\,\beta^0, \mathrm{Tr}\beta^1, \dots, \mathrm{Tr}\,\beta^{v-1}) = (\mathbf{w}, \omega\mathbf{w}, \dots, \omega^{q-2}\mathbf{w}),$$

where $\mathbf{w}$ denotes the first row of $W$ and where $\omega = \theta^{-1} = \beta^m$. 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 $\beta$ was chosen to be a primitive element for $GF(q^d)$; see, for instance, [46, Theorem 6.3.9]. More precisely, the linear feedback shift register of length $d$ with characteristic polynomial the minimal polynomial of $\beta$ 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 [46], Corollary 6.6.4. Trivially, $W$ then has $q$-rank at most $d$, so that the assertion follows from Lemma 5.1. □

The $BGW$-matrices of minimal $q$-rank can also be described in coding theoretic terms; moreover, they are unique up to monomial equivalence. 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. Using properties of the simplex code and of the classical affine spaces, one can prove the following major result; see [48].

**Theorem 5.3.** *Any $m \times m$ matrix 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 (2) and $q$-rank $d$ over $GF(q)$. Moreover, any BGW-matrix $M$ over $GF(q)$ with parameters (2) satisfying $\mathrm{rank}_q M = d$ is monomially equivalent to such a matrix.*

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 4.7 arises from the minimal rank $BGW$-matrix $W$ of Theorem 5.2 by replacing each non-zero entry of $W$ by its inverse. This observation immediately raises the problem of determining the $q$-rank of the classical $BGW$-matrix $X = W^{(-1)}$. It is rather obvious that inversion of elements will, in general, change the $q$-rank, with a few simple 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 $W^{(t)}$.

**Theorem 5.4.** *Let $W$ be the balanced generalized weighing matrix with parameters (2) of $q$-rank $d$ defined in Proposition 4.7, 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*

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

*Proof.* We will merely sketch the proof. As in the proof of Theorem 5.2, the key observation is that the $\theta$-circulant matrix $W^{(t)}$ is a submatrix of a larger circulant matrix: applying the power mapping $x \mapsto x^t$ to the entries of $W$, 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

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

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 $C^{(t)}$. Using the result of [1] together with some facts concerning the linear complexity establishes the assertion; see [49] for details. □

Specializing Theorem 5.4 to the case $t = q-2$, where $q \neq 2$, we obtain the following rank formula for the classical $BGW$-matrices:

**Corollary 5.5.** *Let $X = W^{(-1)} = W^{(q-2)}$ be the classical balanced generalized weighing matrix with parameters (2) defined in Proposition 4.7. Then, with $q = p^r$,*

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

In particular, the classical $BGW$-matrix has $\text{rank}_q X \neq d$ whenever $q \geq 5$ and is therefore not monomially equivalent to the matrix coming from the simplex code construction. Theorem 5.4 also shows that this construction combined with the application of a power map gives a wealth of monomially inequivalent $BGW$-matrices with parameters (2) 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 (2). For instance, there is an example with parameters (85,64,48) and rank 16 over $GF(4)$, see [48]. 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.

## 6. Applications.

We conclude this survey with applications of $BGW$-matrices to the construction of designs and graphs. This section is divided into six parts, the first of which will deal with the work of Ionin. The second part will be devoted to Bush–type Hadamard matrices and twin designs. In the third part we will discuss the productive regular Hadamard matrices and symmetric designs. In the fourth part applications to constructing strongly regular graphs are given. The fifth part concerns doubly regular digraphs, and the final part deals with some newly emerging applications.

### 6.1 The work of Ionin

We begin this section by giving credit to Rajkundlia [65] for being the first to realize the use of balanced generalized weighing matrices in generating symmetric designs. Credit also goes to Brouwer [10] and Fanning [19].

However, it was Yury Ionin who systematically studied the construction of symmetric designs via balanced generalized weighing matrices and effectively 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 $\sigma$ 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 lemma [26] which is a modified version of his earlier lemma in [25].

**Lemma 6.1.** *Let $v > k > \lambda \geq 0$ be integers. Let $\mathcal{M}$ be a set of matrices of order $v$ and $G$ 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 $(v, k, \lambda)$-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. Thus we need to check

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

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

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

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

$$\sum_{j=1}^{w} (\omega_{ij} M)(\omega_{hj} M)^T = \sum_{j=1}^{q^m - q^{m-1}} (\sigma_j M)(\tau_j M)^T = \sum_{j=1}^{q^m - q^{m-1}} (\tau_j^{-1} \sigma_j M) M^T$$

$$= \frac{q^m - q^{m-1}}{|G|} \Big( \sum_{\sigma \in G} \sigma M \Big) M^T = \frac{k(q^m - q^{m-1})}{v} J M^T$$

$$= \frac{k^2(q^m - q^{m-1})}{v} J = \lambda q^m J. \qquad \square$$

Ionin calls the group $G$ in Lemma 6.1 the *group of symmetry*; finding such a group is the hardest part of his construction. For a good illustration of the method, the reader should look at the detailed discussion of the case of symmetric designs associated with (36, 15, 6)- and (36, 21, 12)-difference sets given in [26].

Despite of the difficulty in determining the group of symmetry, in a series of papers Ionin was able to construct a considerable number of infinite classes of symmetric designs with new parameters in [25], [26], [27], [28], [29]. We will briefly discuss some of these classes now.

In [25], it is shown that the designs corresponding to some McFarland and Spence difference sets can serve as starter designs. In [26], by using the Spence (36, 15, 6)- and (36, 21, 12)-difference sets mentioned above and by devising a product theorem, an extension of a result in [25] is proved.

Spectacular progress was made in [28] by exploiting the theory of building blocks of Davis and Jedwab [14] for the construction of difference sets (see also [6] 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 with the following parameters $(v, k, \lambda)$, where $d$ and $m$ are positive integers, $p$ is any prime power, and $q$ 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

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

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

In [29], Ionin generalized Lemma 6.1 to not necessarily symmetric designs. He applied this result to the non-embeddable quasi-residual designs with parameters $(r+1, 2r, r, (r+1)/2, (r-1)/2)$ constructed in [61], [62], where $r \geq 11$ is of the form $2^d - 1$, $3 \cdot 2^d - 1$ or $5 \cdot 2^d - 1$; if $r$ is a prime power, he obtained a non-embeddable quasi-residual design with parameters

$$((r+1)(r^m-1)/(r-1), 2r(r^m-1)/(r-1), r^m, (r+1)r^{m-1}/2, (r-1)r^{m-1}/2)$$

for every positive integer $m$.

He also used these methods to construct certain quasi-residual and quasi-derived designs and gave a sufficient condition for combining these designs into a symmetric design. In this way, Ionin [29] 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 [13]).

**Theorem 6.2.** *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*

$$\Big(1 + \frac{qr(r^{m+1}-1)}{r-1}, r^{m+1}, \frac{r^m(r-1)}{q}\Big).$$

### 6.2. Bush–type Hadamard matrices

One of the most interesting class of Hadamard matrices, if not the most interesting class, undoubtedly is that of Bush–type Hadamard matrices.

**Definition 6.3.** A regular Hadamard matrix $H = \big(H_{ij}\big)$ of order $4n^2$, where $H_{ij}$ are $2n \times 2n$ block matrices, is said to be of *Bush–type* if $H_{ii} = J_{2n}$ and $H_{ij}J_{2n} = J_{2n}H_{ij} = 0$, for $i \neq j$, $i \leq i, j \leq 2n$, where $J$ is the matrix of all ones.

Bush [11] showed that the existence of a projective plane of order $2n$ implies the existence of a symmetric Bush–type Hadamard matrix of order $4n^2$. The following result is in [51]:

**Proposition 6.4.** *The existence of a Hadamard matrix of order* $4n$ *implies the existence of a Bush–type Hadamard matrix of order* $16n^2$.

*Proof.* Let $K$ be a normalized Hadamard matrix of order $4n$. Denote the row vectors of $K$ by $r_1, r_2, \dots, r_{4n}$, and let $C_i = r_i^T r_i$ for $i = 1, 2, \dots, 4n$. Then it is easy to see that:

1. $C_i^T = C_i$, for $i = 1, 2, \dots, 4n$;
2. $C_1 = J_{4n}$, $C_i J_{4n} = J_{4n} C_i = 0$, for $i = 2, \dots, 4n$;
3. $C_i C_j^T = 0$, for $i \neq j$, $1 \leq i, j \leq 4n$;
4. $\sum_{i=1}^{4n} C_i C_i^T = 16n^2 I_{4n}$.

Now the block circulant matrix with first row $C_1\ C_2\ \dots\ C_{4n}$ is a Bush-type Hadamard matrix of order $16n^2$. □

Let us illustrate the preceding construction with the case $n = 4$. Starting with a normalized Hadamard matrix $K$ of order 4,

$$K = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

we construct four $4 \times 4$ matrices of rank one as follows: we put

$$\begin{aligned} r_1 &= \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}, \\ r_2 &= \begin{pmatrix} 1 & 1 & -1 & -1 \end{pmatrix}, \\ r_3 &= \begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}, \\ r_4 &= \begin{pmatrix} 1 & -1 & -1 & 1 \end{pmatrix}, \end{aligned}$$

and define

$$C_1 = r_1^T r_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$C_2 = r_2^T r_2 = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$$

$$C_3 = r_3^T r_3 = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

$$C_4 = r_4^T r_4 = \begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Now let $L$ be any Latin square on the symbols $1, 2, 3, 4$ with constant diagonal 1, and replace each entry $i$ with $C_i$. The result is a Bush–type Hadamard matrix of order 16. If the Latin square $L$ is chosen to be symmetric, then the resulting Bush–type Hadamard matrix is also symmetric.

It was Bush–type Hadamard matrices that led to the introduction of the so-called twin designs in [52]:

**Definition 6.5.** A $(0, \pm 1)$-matrix is said to be the incidence matrix of *twin designs*, if by changing either all entries 1 or all entries $-1$ to 0 a design is obtained.

**Lemma 6.6.** *Every Bush–type Hadamard matrix of order* $4n^2$ *contains the incidence matrix of twin symmetric* $(4n^2, 2n^2 - n, n^2 - n)$*-designs.*

*Proof.* Change all the diagonal block entries of the given Bush–type $H$ matrix to 0. The row sums of $H$ are all $2n$. Thus the negative entries form the incidence matrix of a symmetric $(4n^2, 2n^2 - n, n^2 - n)$-design; the same argument applies to the positive entries. □

To give an example, let $C_2$, $C_3$, $C_4$ be the matrices of the previous example. Then $M = \mathrm{circ}(0, C_2, C_3, C_4)$ is the matrix of twin symmetric (16, 6, 2)-designs, where we write $-$ instead of $-1$:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 1 & 1 & - & - & 1 & - & 1 & - & 1 & - & - & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & - & - & - & 1 & - & 1 & - & 1 & 1 & - \\
0 & 0 & 0 & 0 & - & - & 1 & 1 & 1 & - & 1 & - & - & 1 & 1 & - \\
0 & 0 & 0 & 0 & - & - & 1 & 1 & - & 1 & - & 1 & 1 & - & - & 1 \\
1 & - & - & 1 & 0 & 0 & 0 & 0 & 1 & 1 & - & - & 1 & - & 1 & - \\
- & 1 & 1 & - & 0 & 0 & 0 & 0 & 1 & 1 & - & - & - & 1 & - & 1 \\
- & 1 & 1 & - & 0 & 0 & 0 & 0 & - & - & 1 & 1 & 1 & - & 1 & - \\
1 & - & - & 1 & 0 & 0 & 0 & 0 & - & - & 1 & 1 & - & 1 & - & 1 \\
1 & - & 1 & - & 1 & - & - & 1 & 0 & 0 & 0 & 0 & 1 & 1 & - & - \\
- & 1 & - & 1 & - & 1 & 1 & - & 0 & 0 & 0 & 0 & 1 & 1 & - & - \\
1 & - & 1 & - & - & 1 & 1 & - & 0 & 0 & 0 & 0 & - & - & 1 & 1 \\
- & 1 & - & 1 & 1 & - & - & 1 & 0 & 0 & 0 & 0 & - & - & 1 & 1 \\
1 & 1 & - & - & 1 & - & 1 & - & 1 & - & - & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & - & - & - & 1 & - & 1 & - & 1 & 1 & - & 0 & 0 & 0 & 0 \\
- & - & 1 & 1 & 1 & - & 1 & - & - & 1 & 1 & - & 0 & 0 & 0 & 0 \\
- & - & 1 & 1 & - & 1 & - & 1 & 1 & - & - & 1 & 0 & 0 & 0 & 0
\end{pmatrix}$$

One can also see that by replacing all the $-1$ entries in a Bush–type Hadamard matrix by zero, or by changing all the diagonal block entries to $-1$ and all entries 1 to 0 one gets the incidence matrices of two symmetric $(4n^2, 2n^2 + n, n^2 + n)$-designs. Note that the two incidence matrices now share all the diagonal block entries. This is called a *Siamese twin design* in [53].

It is noted in [52], [53] that the group of symmetries for Bush–type Hadamard matrices is trivial. In these papers an elementary technique is used to show that the existence of a Hadamard matrix of order 2 or $4n$ implies that of twin symmetric designs with Ionin-type parameters.

**Theorem 6.7.** *Let $4n^2$ be the order of a Bush-type Hadamard matrix, and assume that $q = (2n - 1)^2$ is a prime power. Then there exist twin symmetric designs with parameters*

$$v = 4(q^m + q^{m-1} + \cdots + q + 1)n^2, \quad k = q^m(2n^2 - n), \quad \lambda = q^m(n^2 - n)$$

*for every positive integer $m$.*

*Proof.* Let $U$ be the circulant shift permutation matrix of order $2n$ (that is, the circulant matrix of order $2n$ with first row $0\ 1\ 0\ \ldots\ 0$), and let $N$ be the diagonal matrix of order $2n$ with $-1$ at the $(1, 1)$-position and 1 elsewhere on the diagonal. Let $E = UN$ and $\gamma = E \otimes I_{2n}$, where $I_{2n}$ denotes the identity matrix of order $2n$. Also, let

$$G_{4n} = \{\gamma^i = E^i \otimes I_{2n} : i = 1, 2, \ldots, 4n\} = \langle\ \gamma\ \rangle$$

be the cyclic subgroup of all signed permutation matrices of order $4n^2$ generated by $\gamma$. Then the cyclic group $G_{4n}$ is of order $4n$. Let $H$ be a twin $(4n^2, 2n^2 - n, n^2 - n)$-design obtained from the Bush–type Hadamard matrix, and let $W = (w_{i,j})$ be a $BGW(1 + q + q^2 + \ldots + q^m, q^m, q^m - q^{m-1})$ over $G_{4n}$. (Note that $4n$ is a divisor of $q - 1$ and apply Theorem 4.5 together with Proposition 1.2.) Then the block matrix $(Hw_{i,j})$ is the incidence matrix of twin symmetric designs with the Ionin–type parameters

$$v = 4(q^m + q^{m-1} + \cdots + q + 1)n^2, \quad k = q^m(2n^2 - n), \quad \lambda = q^m(n^2 - n)$$

for every positive integer $m$. See [52] for details. □

The analogue of this result, where Siamese twin symmetric designs with parameters $(4n^2, 2n^2 + n, n^2 + n)$ are used, appeared in [53]:

**Theorem 6.8.** *Let $4n^2$ be the order of a Bush-type Hadamard matrix, and assume that $q = (2n + 1)^2$ is a prime power. Then there exist Siamese twin symmetric designs with parameters*

$$v = 4(q^m + q^{m-1} + \cdots + q + 1)n^2,\ k = q^m(2n^2 + n), \lambda = q^m(n^2 + n)$$

*and*

$$v = 16(q^m + q^{m-1} + \cdots + q + 1)n^2,\ k = q^m(8n^2 + 2n), \lambda = q^m(4n^2 + 2n)$$

*for every positive integer $m$.*

In [50], a new method of construction for Bush–type Hadamard matrices is given from which at least one new infinite class of Siamese twin symmetric designs arises. These have parameters

$$v = 4p^2(1 + q + \cdots + q^{m+1}),\ k = (2p^2 + p)q^{m+1}, \lambda = (p^2 + p)q^{m+1},$$

where $p = 53208$, $q = 106417$, and exist for each positive integer $m$.

Bush–type Hadamard matrices of order $4n^2$, where $n$ is odd, seem pretty hard to construct. Examples are known for $n = 3$, $n = 5$, and $n = 9$ (see [38], [40], and [41], respectively); all other cases are open.

### 6.3. Productive regular Hadamard matrices

The group of symmetries depends very much on the block structure of regular Hadamard matrices. A prime example of this can be seen in [33], where a recursive method is used to construct an infinite class of regular Hadamard matrices and a corresponding group of symmetries.

**Theorem 6.9.** *Let $h = \pm 3^n$ and assume that $q = (2h - 1)^2$ is a prime power. Then there exists a symmetric design with parameters*

$$\Big(\frac{h(q^{m+1} - 1)}{h - 1}, h(2h - 1)^{2m+1}, h(h - 1)(2h - 1)^{2m}\Big)$$

*for every nonnegative integer $m$.*

Recently, Ionin [30] has introduced a new class of regular Hadamard matrices:

**Definition 6.10.** A regular Hadamard matrix $H$ with row sum $2h$ is called *productive* if there is a set $\mathcal{H}$ of matrices with row sum $2h$ and a cyclic group $G = \langle \sigma \rangle$ where $\sigma : \mathcal{H} \to \mathcal{H}$ is a bijection, such that

(i) $H \in \mathcal{H}$;
(ii) for all $H_1, H_2 \in \mathcal{H}$, $(\sigma H_1)(\sigma H_2)^T = H_1 H_2^T$;
(iii) $|G| = 4|h|$;
(iv) $\sum_{\sigma \in G} \sigma H = 2\frac{h}{|h|} J$.

Ionin proved that the existence of a productive regular Hadamard matrix with row sum $2h$, where $q = (2h - 1)^2$ is a prime power, allows one to apply his methods. The group $G$ here acts on regular Hadamard matrices and replaces the group of symmetries in his earlier work.

**Theorem 6.11.** *If there exists a productive regular Hadamard matrix with row sum $2h$ such that $q = (2h - 1)^2$ is a prime power, then, for every nonnegative integer $m$, there exists a symmetric design with parameters*

$$\left(\frac{4h^2(q^{m+1} - 1)}{q - 1}, (2h^2 - h)q^m, (h^2 - h)q^m\right). \tag{5}$$

In the same paper, Ionin also obtained a recursive construction for productive regular Hadamard matrices:

**Theorem 6.12.** *If $B$ is a regular Hadamard matrix of Bush type, and if $H$ is a productive regular Hadamard matrix, then $B \otimes H$ is a productive regular Hadamard matrix.*

In this new terminology, all Bush–type Hadamard matrices are productive. Using Mathon–Seberry–Whiteman [68] matrices, another class of productive regular Hadamard matrices is constructed in [4]:

**Theorem 6.13.** *Let $m = 8n^2 - 1$ be a prime, and assume that $4n$ is the order of a Hadamard matrix. Then there exists a productive Hadamard matrix of order $16n^2m^2$.*

Ionin and Kharaghani [33] proposed the following conjecture, which is given some evidence by the results on Bush–type and on productive regular Hadamard matrices that we have discussed:

**Conjecture 6.14.** *For all integers $h \neq 0$ and $m \geq 0$, if $q = (2h - 1)^2$ is a prime power, then there exists a symmetric design with parameters (5).*

### 6.4. Strongly regular graphs

The fact that the action of the group of symmetries for Bush–type Hadamard matrices can be expressed as a simple multiplication from the left by certain block negacyclic matrices was the main motivation to explore the possibility of having the incidence matrix of the twin designs to be symmetric with constant diagonal. This led to a search for block negacyclic Bush–type Hadamard matrices of order 36 in [39]. Here a *block negacyclic Bush-type Hadamard matrix* of order $4n^2$ is a Bush-type Hadamard matrix which has symmetric blocks and is block negacyclic. (Recall that *negacyclic* matrices are, by definition, simply $-1$-circulant matrices).

As no other block negacyclic Bush–type Hadamard matrix of order $4n^2$ for $n$ odd is known, we will now describe the example of [39]. It is a block matrix of the form

$$H = \begin{pmatrix} J & A & B & C & D & E \\ -E & J & A & B & C & D \\ -D & -E & J & A & B & C \\ -C & -D & -E & J & A & B \\ -B & -C & -D & -E & J & A \\ -A & -B & -C & -D & -E & J \end{pmatrix}$$

where all the blocks are symmetric. Here $J$ is the all one matrix (as usual), and the remaining blocks are as follows:

$$A = \begin{pmatrix} 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

$$B = \begin{pmatrix} -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 \end{pmatrix}$$

$$C = \begin{pmatrix} -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

$$D = \begin{pmatrix} -1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}$$

$$E = \begin{pmatrix} -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 \end{pmatrix}.$$

This example led to two very interesting new strongly regular graphs. Let us recall the definition:

**Definition 6.15.** A *strongly regular graph* with parameters $(v, k, \lambda, \mu)$ –for short, an $SRG(v, k, \lambda, \mu)$ – is a simple graph $\Gamma$ with $v$ vertices, not complete or null, in which the number of common neighbors of vertices $x$ and $y$ is $k$, $\lambda$, or $\mu$ according as $x$ and $y$ are equal, adjacent, or non-adjacent, respectively.

It is well-known that the incidence matrix $M$ of a symmetric $(v, k, \lambda)$-design can be interpreted as the adjacency matrix of an $SRG(v, k, \lambda, \lambda)$ provided that $M$ is symmetric and has diagonal entries 0. (Another way to phrase this is to say that the symmetric design should admit a polarity without absolute points; see [6], 2.9.) If this phenomenon happens for the incidence matrices of a pair of (Siamese) twin designs, one speaks of *(Siamese) twin strongly regular graphs.*

Using the block negacyclic Bush-type Hadamard matrix of order 36, twin strongly regular graphs with parameters $(936, 375, 150, 150)$ and also Siamese twin strongly regular graphs with parameters $(1800, 1029, 588, 588)$ were constructed.

To use the full strength of balanced generalized weighing matrices for generating strongly regular graphs, there was a need for symmetric balanced generalized weighing matrices with zero diagonal. Using the classical $\omega$–circulant balanced generalized weighing matrices, the following recursive construction for symmetric balanced generalized weighing matrices with zero diagonal was established in [54]:

**Theorem 6.16.** *Let $C_n$ be a cyclic group of order $n$, and let $q$ be a prime power and $t$ and $m$ be positive integers. If there exists a symmetric balanced generalized weighing matrix with parameters*

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

*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 $C_n$.*

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 [22] 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 necessary here: otherwise, there is no symmetric $BGW(1+p, p, p-1)$ with zero diagonal over $C_n$). These initial matrices lead to the following series:

**Theorem 6.17.** *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*

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

*with zero diagonal over the cyclic group of order $n$.*

Using the block negacyclic Bush-type Hadamard matrix of order 36 and Theorem 6.17, the existence of two families of twin strongly regular graphs, which embed the previously discussed examples of [39] into infinite families, is shown in [54].

The existence of four further new infinite classes of strongly regular graphs was shown in [31]; the methods used there are considerably more involved. First, one needs a modification of the construction in [54] to obtain a slight generalization of Theorem 6.17: the condition that $(q-1)/n$ is even may be relaxed to the requirement that $q(q-1)/n$ is even. Next, it is shown there that every finite abelian group can be equipped with a *symmetric ordering*. This was essential in order to establish that the starting symmetric designs can be selected in a way to have symmetric incidence matrices. It is then shown that this may indeed be achieved for designs with the parameters of McFarland and Spence difference sets. We only mention one of the four new classes of SRG's here:

**Theorem 6.18.** *Let $q$ be an odd prime power and $d$ a positive integer. If $r = (q^{d+1}-1)/(q-1)$ is a prime power, then, for every positive integer $m$, there exists a strongly regular graph with parameters*

$$\Big(\frac{q^{d+1}(r^{4m}-1)}{r-1},\ q^d r^{4m-1},\ q^{d-1}r^{4m-2}(r-1),\ q^{d-1}r^{4m-2}(r-1)\Big).$$

### 6.5. Doubly regular digraphs

A *digraph* is a pair $\Gamma = (V, E)$, where $V$ is a finite nonempty set of *vertices* and $E$ is a set of ordered pairs (*arcs*) $(x, y)$ with $x, y \in V$ and $x \neq y$. If $(x, y)$ is an arc, we will say that $x$ *dominates* $y$ or that $y$ *is dominated by* $x$. A digraph $\Gamma$ is called *regular of degree* $k$ if each vertex of $\Gamma$ dominates exactly $k$ vertices and is in turn dominated by exactly $k$ vertices. A digraph $\Gamma$ on $v$ vertices is said to be *doubly regular with parameters* $(v, k, \lambda)$ if the following three conditions hold:

- $\Gamma$ is regular of degree $k$;
- for all pairs of distinct vertices $x$ and $y$, the number of vertices $z$ that dominate both $x$ and $y$ is equal to $\lambda$;
- for all pairs of distinct vertices $x$ and $y$, the number of vertices $z$ that are dominated by both $x$ and $y$ is equal to $\lambda$.

Now let $N$ be an incidence matrix for a symmetric design, and assume that $N + N^T$ is a (0, 1) matrix. Then $N$ is the adjacency matrix of a doubly regular asymmetric digraph, and vice versa. A doubly regular asymmetric digraph with parameters $(v, k, \lambda)$ is denoted by $DRAD(v, k, \lambda)$. For more information on these (and also on more general) digraphs see Jørgensen [42].

One well known example of the above relation between symmetric designs and digraphs is provided by the so-called *Hadamard tournaments*: a Hadamard tournament is a $DRAD(4n - 1, 2n - 1, n - 1)$, and such a tournament exists if and only if there exists a skew Hadamard matrix of order $4n$. More interesting in our context is the following connection to twin designs: if $\Gamma$ is a $DRAD(v, k, \lambda)$ and if $\Gamma'$ denotes the digraph obtained by reversing the direction of every arc of $\Gamma$, then the corresponding symmetric designs are twins. Such digraphs are studied in [32] and several parametrically new infinite families constructed; three of these families are obtained from direct constructions using well known symmetric designs. Actually, one of them fits nicely into our topic, and hence we will mention it explicitly. Returning to the construction method in Proposition 6.4, one can see that the Bush–type Hadamard matrices of order $16n^2$ can be selected in a special way, so that one obtains doubly regular asymmetric digraphs:

**Theorem 6.19.** *If $h$ is a positive integer such that there exists a Hadamard matrix of order $2h$, then there exists a $DRAD(4h^2, 2h^2 - h, h^2 - h)$.*

To carry out some further constructions, the authors first obtained an infinite family of skew balanced generalized weighing matrices. Here a balanced generalized weighing matrix $W$ over a finite group $G$ with a fixed element $\tau$ of order 2 is said to be *skew* if $W^T = \tau W$. 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 $W^T = -W$. The following result should be compared to Theorem 6.17.

**Theorem 6.20.** *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*

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

*over the cyclic group of order $n$.*

Using the $DRAD(4h^2, 2h^2-h, h^2-h)$ together with skew balanced generalized weighing matrices, the following large class of doubly regular asymmetric digraphs was constructed in [32]:

**Theorem 6.21.** *Let $h$ be a positive integer such that there exists a Hadamard matrix of order $2h$. If $q=(2h-1)^2$ is a prime power, then there exists a*

$$DRAD\Big(\frac{h(q^{2d}-1)}{h+1},\ hq^{2d},\ h(h+1)q^{2d-1}\Big)$$

*for every positive integer $d$.*

As in the case of strongly regular graphs, it was much harder to show that the symmetric designs with parameters of the McFarland difference sets also can be selected to have skew incidence matrices. Nevertheless, the following result could be obtained:

**Theorem 6.22.** *Let $q=2^t$ and let $d$ be a positive integer. If $r=(q^{d+1}-1)/(q-1)$ is a prime power, then there exists a*

$$DRAD\Big(\frac{q^{d+1}(r^{4m}-1)}{r-1},\ q^d r^{4m-1},\ q^{d-1}r^{4m-2}(r-1)\Big)$$

*for every positive integer $d$.*

### 6.6. Further applications

Balanced generalized weighing matrices are also used to construct $BIBD$s; see, for example, [29] and [55]; the construction method of [34] for non-embeddable quasi-residual designs was already mentioned before. One may also used balanced generalized weighing matrices to construct strongly regular graphs from designs with three intersection numbers, see [35]. We quote a corollary here:

**Corollary 6.23.** *Let $2^n - 1$ be a prime, put $q = 2^n$, and let $m$ be a positive integer. Then there exists a BIBD with parameters*

$$v = (q^{m+1} - 1) \cdot (2^n - 1),\ b = (q^{m+1} - 1) \cdot 2^n,\ r = q^m \cdot 2^{2n-1},$$

$$k = q^m \cdot 2^{n-1}(2^n - 1) \quad \textit{and} \quad \lambda = q^m \cdot 2^{n-2}(2^n + 1)$$

*and with intersection numbers $\rho_1 = k^2 q^m / v$, $\rho_2 = (k + \lambda - r) \cdot q^m$, and $\rho_3 = v\lambda q^m / b$ which admits a nearly affine decomposition.*

Finally, we mention a graph decomposition result given in [56] by exploiting balanced generalized weighing matrices:

**Corollary 6.24.** *For every prime power $q$, the complete graph on $1+q+q^2+q^3$ vertices can be written as the union of $1 + q$ Siamese twin*

$$SRG(1 + q + q^2 + q^3,\ q + q^2,\ q - 1,\ q + 1)$$

*which share $1 + q^2$ disjoint cliques of size $1 + q$.*

**Note.** We refer the reader to [47] for an alternative, more ‘didactic’ approach to the material covered here, which should be useful for class room use in an advanced course on design theory and/or finite geometry. The treatment given there differs substantially: first of all, there are many more (and also more detailed) proofs; second, the algebraic machinery of group rings has been avoided; third, a thorough study of square divisible designs with disjoint blocks has been included; and, finally, the extensive survey of applications given here has been replaced with discussing just one example in considerable detail.

**Note added in proof.** There has been considerable progress regarding the problem mentioned at the end of Section 6.2; see M. Muzychuk and Q. Xiang *Symmetric Bush–type Hadamard matrices of order $4m^4$ exist for all odd $m$*, preprint

**Acknowledgement.** The authors thank Yuri Ionin for providing them with a draft of Chapters 10 and 11 of [37]. The second author was supported by a research grant from IPM and a discovery grant from NSERC.

## REFERENCES

[1] M. Antweiler - 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), pp. 120–130.

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

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

[4] M. Behbahani - H. Kharaghani, *On a new productive class of regular Hadamard matrices,* Preprint.

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

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

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

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

[9] A. Blokhuis - D. Jungnickel - 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), pp. 1473–1476.

[10] A.E. Brouwer, *An infinite series of symmetric designs,* Math. Centrum Amsterdam Report, ZW 136/80 (1983).

[11] K.A. Bush, *Unbalanced Hadamard matrices and finite projective planes of even order,* J. Comb. Th., 11 (1971), pp. 38–44.

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

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

[14] J.A. Davis - J. Jedwab, *A unifying construction of difference sets,* J. Comb. Th. (A), 80 (1997), pp. 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), pp. 117–132.

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

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

[19] J.D. Fanning, *A family of symmetric designs,* Discr. Math., 146 (1995), pp. 307–312.

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

[21] D. Ghinelli - 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).

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

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

[24] D.R. Hughes - F.C. Piper, *Projective Planes (2nd edition),* Springer, 1982.

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

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

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

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

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

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

[31] Y.J. Ionin - H. Kharaghani, *New families of strongly regular graphs,* J. Comb. Des., 11 (2003), pp. 208–217.

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

[33] Y.J. Ionin - H. Kharaghani, *A recursive construction for new symmetric designs,* Designs, Codes and Cryptography, 35 (2005), pp. 303–310.

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

[35] Y.J. Ionin - M.S. Shrikhande, *Strongly regular graphs and designs with three intersection numbers,* Designs, Codes and Cryptography 21 (2000), pp. 113–125.

[36] Y.J. Ionin - M.S. Shrikhande, *On classification of two class partially balanced designs,* J. Statist. Plann. Inference 95 (2001), pp. 209–228.

[37] Y.J. Ionin - M.S. Shrikhande, *Combinatorics of Symmetric Designs,* Cambridge University Press, Cambridge (to appear).

[38] Z. Janko, *The existence of a Bush-type Hadamard matrix of order* 36 *and two new infinite classes of symmetric designs,* J. Comb. Th. (A), 95 (2001), pp. 360–364.

[39] Z. Janko - H. Kharaghani, *A block negacyclic Bush–type Hadamard matrix and two strongly regular graphs,* J. Comb. Th. (A), 98 (2002), pp. 118–126.

[40] Z. Janko - H. Kharaghani - V.D. Tonchev, *A Bush–type Hadamard matrix of order* 100 *and two new infinite classes of symmetric designs,* Designs, Codes and Cryptography, 24 (2001), pp. 225–232.

[41] Z. Janko - H. Kharaghani - V.D. Tonchev, *The existence of a Bush–type Hadamard matrix of order* 324 *and two new infinite classes of symmetric designs,* J. Comb. Des., 9 (2001), pp. 72–78.

[42] L. Jörgensen, *On normally regular digraphs,* Preprint R-94-2023, Institute for Electronic Systems, Aalborg University (1994).

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

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

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

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

[47] D. Jungnickel, *Balanced generalized weighing matrices and related structures,* Quaderni elettronici del Seminario di Geometria Combinatoria, 16 E (Febbraio 2005), pp. 1–39.

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

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

[50] F. Kamali - H. Kharaghani - G.B. Khosrovshahi, *Some Bush-type Hadamard matrices,* J. Statist. Plann. Inference, 113 (2003), pp. 375–384.

[51] H. Kharaghani, *New classes of weighing matrices,* Ars Combinatoria, 19 (1985), pp. 69–72.

[52] H. Kharaghani, *On the twin designs with the Ionin–type parameters,* Electronic J. Comb., 7 (2000), R1.

[53] H. Kharaghani, *On the Siamese twin designs,* In: Finite Fields and Applications (Eds. D. Jungnickel and H. Niederreiter), pp. 303–312, Springer–Verlag, Berlin (2001).

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

[55] H. Kharaghani - V.D. Tonchev, *On a class of twin balanced incomplete block designs,* In: Codes and designs (Eds. K.T. Arasu und A. Seress), pp. 157–163. Walter de Gruyter, Berlin, 2002.

[56] H. Kharaghani - R. Torabi, *On a decomposition of complete graphs,* Graphs Comb., 19 (2003), pp. 519–526.

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

[58] R. Lidl - H. Niederreiter, *Finite fields,* Addison-Wesley, Reading, Mass., 1983.

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

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

[61] K. Mackenzie-Fleming, *An infinite family of non-embeddable Hadamard designs,* Electronic J. Comb., 6 (1999), R24.

[62] K. Mackenzie-Fleming, *An infinite family of non-embeddable quasi-residual Hadamard designs,* J. Geom., 67 (2000), pp. 173–179.

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

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

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

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

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

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

[69] G. Szekeres, *Tournaments and Hadamard matrices,* Enseignement Math., 15 (1969), pp. 269–278.

[70] V.D. Tonchev, *Combinatorial Configurations,* Longman-Wiley, New York, 1988.

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

*D. Jungnickel*
*Lehrstuhl für Diskrete Mathematik,*
*Optimierung und Operations Research,*
*Universität Augsburg,*
*D–86135 Augsburg (GERMANY)*
*e-mail:* jungnickel@math.uni-augsburg.de

*H. Kharaghani*
*Department of Mathematics and Computer Science,*
*University of Lethbridge,*
*Lethbridge, Alberta, T1K 3M4 (CANADA)*
*e-mail:* kharaghani@uleth.ca