Math. Z. 167, 49–60 (1979)

Mathematische Zeitschrift

On Difference Matrices, Resolvable Transversal Designs and Generalized Hadamard Matrices

Dieter Jungnickel

Fachbereich Mathematik der Technischen Universität Berlin,
Straße des 17. Juni 135, D-1000 Berlin 12, Federal Republic of Germany

To my teacher Professor Hanfried Lenz

0. Introduction

In this paper we are concerned with $(s, r; \lambda, G)$-difference matrices. Here G is a group of order s and D an $(r \times s\lambda)$-matrix with entries from G such that the sequence $d_{ik} - d_{jk}$ of differences of rows i and j of D contains each element of G exactly λ times whenever $i \neq j$. (We will use additive notation but G may be non-abelian.) Such matrices have been used by Bose and Bush [1] and by Shrikhande [15] (in the abelian case) for the construction of orthogonal arrays. The author has studied the special case $\lambda = 1$ in [10]. Recently, Drake [4] introduced the notion of a generalized Hadamard matrix over any finite group G (Drake's definition is in general stronger than that of Butson [2] and Shrikhande [15] where only cyclic groups have been investigated). Such a matrix is just a square matrix H such that both H and H^T are difference matrices. This immediately poses the problem of characterizing the generalized Hadamard matrices among the difference matrices. We will show that for any difference matrix $r \leqq s\lambda$ and that the complete difference matrices (i.e., $r = s\lambda$) coincide with the generalized Hadamard matrices. Hence in particular the two axioms of Drake (on H and H^T) are equivalent.

These results are in fact corollaries of more general results on transversal designs (TD's). We first prove that difference matrices and regular resolvable TD's are equivalent, thus giving a geometric interpretation of difference matrices (here regularity means the existence of a particularly pleasant collineation group). For the case $\lambda = 1$ we obtain a connection to projective planes of Lenz type at least II. We then show that the existence of just one parallel class in an $(s, r; \lambda)$-TD forces $r \leqq s\lambda$ (the general bound being $(s^2\lambda - 1)/(s - 1)$, see e.g. Hanani [7]) and that resolvable TD's with $r = s\lambda$ are in fact symmetric (i.e., the dual is also a TD). Finally, we mention some constructions which in particular yield a new class of GH-matrices.

This paper should be more or less self-contained. For the general background, the reader might consult the referenced books by Hall, Dembowski and Raghavarao. We will in general use the notation of Dembowski; e.g., points are

0025-5874/79/0167/0049/$02.40

always denoted by lower case and lines by upper case letters, $[p, q]$ is the number of blocks through points p and q, etc. All structures considered are assumed to be finite.

1. Difference Matrices and Regular TD's

Definition 1.1 (Bose, Bush; see also [10]). Let G be a group of order s and $D = (d_{ik})$ $(i = 1, \ldots, r;\ k = 1, \ldots, s\lambda)$ a matrix with entries from D. D is called an $(s, r; \lambda, G)$-*difference matrix* if it satisfies the following condition:

(1.1) The sequence of differences $(d_{ik} - d_{jk})_{k=1,\ldots,s\lambda}$ contains each element of G exactly λ times (for all i, j with $i \neq j$ and $i, j = 1, \ldots, r$).

We warn the reader that what we just defined to be an $(s, r; 1, G)$-difference matrix has been called an $(s, r-1; G)$-difference matrix in [10], [11] and [12]; the reason was that an $(s, r; G)$-difference matrix as defined here corresponds to a G-regular set of $r-1$ mutually orthogonal Latin squares which was the point of view of [10].

Definition 1.2 (Hanani). Let $\Sigma = (\mathbf{P}, \mathbf{B}, \mathrm{I})$ be an incidence structure and assume that the relation $\sim$ defined by

(1.2) $p \sim q$ if and only if $p = q$ or $[p, q] = 0$

is an equivalence relation on $\mathbf{P}$. The equivalence classes will be called *point classes*. (We avoid the generally used term "groups" as we will encounter real groups acting on the "groups" later.) Σ is called a *transversal design* of *order* s, *degree* r and *index* λ or briefly an $(s, r; \lambda)$-TD if the following axioms are satisfied:

(1.3) Each block meets each point class.

(1.4) $p \not\sim q$ implies $[p, q] = \lambda$.

(1.5) There are $r \geqq 3$ point classes and some point class has precisely $s \geqq 2$ points.

The dual structure of an $(s, r; \lambda)$-TD is called an $(s, r; \lambda)$-*net* (Drake and Jungnickel [5]). A TD is said to be *symmetric* if the dual structure is also a TD with the same parameters (Drake [4]). A TD is *resolvable* if its blocks can be partitioned into parallel classes where the blocks in any parallel class partition the point set.

Proposition 1.3 (Bose, Hanani, Drake, Jungnickel). *Let Σ be an $(s, r; \lambda)$-TD. Then each point class has s points, there are $b := s^2\lambda$ blocks, each point is on $s\lambda$ blocks and each block contains r points. Furthermore $r \leqq (s^2\lambda - 1)/(s-1)$. In the case of equality, Σ is said to be complete. A* TD *is complete iff any two blocks intersect in precisely $(s\lambda - 1)/(s-1)$ points; then the dual structure is an affine resolvable block design* (ARBD).

The proofs may be found in [5, Section 5]. A survey on ARBD's is in [16].

Definition 1.4. Let Σ be an $(s, r; \lambda)$-TD and G a group of order s. Σ is called *G-regular* if G acts as a collineation group of Σ which is regular on each point class and semiregular on the set of blocks.

Theorem 1.5. *Let $D=(d_{ik})$ be an $(s, r; \lambda, G)$-difference matrix and define an incidence structure $\Sigma(D)=(\mathbf{P}(D), \mathbf{B}(D), \in)$ as follows:*

$$\mathbf{P}(D) := \bigcup_{i=1}^{r} \mathbf{P}_i \quad \text{with} \quad \mathbf{P}_i := \{(i, x): x \in G\};$$

$$\mathbf{B}(D) := \{B_{jx}: j=1, \ldots, s\lambda;\ x \in G\}$$

where

$$B_{jx} := \{(i, d_{ij}+x): i=1, \ldots, r\}.$$

Then $\Sigma(D)$ is a resolvable G-regular $(s, r; \lambda)$-TD. Conversely, every G-regular TD *is resolvable and may be described in this way.*

Proof. First let D be a difference matrix and $\Sigma(D)$ be defined as above. Clearly any two points in the same $\mathbf{P}_i$ are not joined. Consider two points (i, x) and (j, y) with $i \neq j$. Then there are precisely λ indices k with $d_{ik}-d_{jk}=x-y$. But then (i, x), $(j, y) \in B_{k,\, -d_{ik}+x}$ for all these k. Conversely, (i, x), $(j, y) \in B_{ku}$ implies $d_{ik}+u=x$ and $d_{jk}+u=y$, hence $d_{ik}-d_{jk}=x-y$. Thus $[(i, x), (j, y)]=\lambda$. Hence $\Sigma(D)$ is an $(s, r; \lambda)$-TD; as the sets $\mathbf{B}_j := \{B_{jx}: x \in G\}$ obviously are parallel classes, $\Sigma(D)$ is resolvable. Finally, $\Sigma(D)$ is G-regular: let $g \in G$ act on $\Sigma(D)$ by $(i, x) \to (i, x+g)$ and $B_{jx} \to B_{j,\, x+g}$.

Now let Σ be any G-regular $(s, r; \lambda)$-TD. In each point class $\mathbf{P}_i$, choose a "base point" p_i arbitrarily and coordinatize the point $q \in \mathbf{P}_i$ as (i, g) if and only if the image of p_i under $g \in G$ is q; this is well-defined because of the regularity of G on each point class. As G is semiregular on the block set, there will be $s\lambda$ orbits $\mathbf{B}_1, \ldots, \mathbf{B}_{s\lambda}$ of s blocks each. In each orbit $\mathbf{B}_j$ choose a "base block" $B_{j0} = \{(i, d_{ij}): i=1, \ldots, r\}$ arbitrarily. Then Σ has been represented in the form $\Sigma(D)$, where $D=(d_{ik})$ $(i=1, \ldots, r;\ k=1, \ldots, s\lambda)$. So clearly Σ is resolvable (the $\mathbf{B}_i$ being the parallel classes). As we have $[(i, x), (j, 0)]=\lambda$ for all $x \in G$ and all i, j with $i \neq j$, it is easily seen that D is an $(s, r; \lambda, G)$-difference matrix.

The case $\lambda=1$ of the previous theorem and the following proposition have been stated as a remark in [10] (without proof).

Proposition 1.6. *Let $s \geqq 3$ and G a group of order s. Then the existence of an $(s, s; 1, G)$-difference matrix is equivalent to the existence of a projective plane of order s and Lenz type at least II which has G as the group of all (p, L)-elations for some flag (p, L).*

Proof. First let the difference matrix be given and construct $\Sigma(D)$ as in Theorem 1.5. To each parallel class $\mathbf{B}_i (i=1, \ldots, s)$ adjoin a point ∞_i; this yields the dual of an affine plane of order s with another point class $\mathbf{P}_0 := \{\infty_1, \ldots, \infty_s\}$. Now take all point classes as the lines of another parallel class $\mathbf{B}_0$ and adjoin to $\mathbf{B}_0$ a new point ∞_0. The result is a projective plane of order s which is obviously $(\infty_0, \mathbf{P}_0)$-transitive with G as the corresponding group of elations.

Conversely, given a projective plane of order s with G as group of (p, L)-elations, discard the line L with all its points and consider the lines through p as point classes. This yields a G-regular $(s, s; 1)$-TD and the assertion follows by Theorem 1.5.

2. Generalized Hadamard Matrices

Clearly difference matrices are generalizations of the generalized Hadamard matrices of Drake [4] (in additive notation). In our terminology, Drake's definition reads as follows.

Definition 2.1 (Drake). Let G be a group of order s and H an $(s\lambda \times s\lambda)$-matrix with entries from G. Then H is called a *generalized Hadamard matrix* or briefly an $(s; \lambda)$-GH-matrix iff both H and H^T are $(s, s\lambda; \lambda, G)$-difference matrices. (The choice of name is motivated by (2.1) below.)

We warn the reader that this definition coincides with Butson's [2] only in the case of the cyclic groups C_p, p a prime (see [4, Remarks 1.3]). The definition also gives rise to the problem of characterizing the GH-matrices among the difference matrices. The answer is

Theorem 2.2. *Let D be an $(s, r; \lambda, G)$-difference matrix. Then necessarily $r \leqq s\lambda$ and equality holds if and only if D is an $(s; \lambda)$-GH-matrix over G. Hence in particular the conditions on H and H^T in Definition* 2.1 *(i.e. Drake's axioms* (i) *and* (ii) *in* [4, *Definition* 1.1]) *are equivalent.*

This generalizes the classical result that $HH^T = nI$ is equivalent to $H^T H = nI$ for ordinary Hadamard matrices.

We could give a direct proof of Theorem 2.2 but we prefer to obtain this result as a corollary of Theorem 1.5 and results on TD's in general. This will be done in Section 3. We now list the known existence results on GH-matrices as first examples for difference matrices.

Proposition 2.3 (Butson, Drake). *An $(s; \lambda)$-GH-matrix over G and thus an $(s, s\lambda; \lambda, G)$-difference matrix exists in all of the following cases:*

(2.1) $s = 2$, $G = C_2$: *Here an ordinary Hadamard matrix of order 4λ is a $(2; 2\lambda)$-GH-matrix.* The existence problem has been studied extensively and existence is conjectured for all values of λ but this has not been proved up to now. The reader should consult [17].

(2.2) $s = p$, $G = C_p$, $\lambda = 2^m p^k$, *where m, k are non-negative integers with $m \leqq k + 1$ and where p is a prime* (Butson [2], see also Drake [4, Theorem 1.4]).

(2.3) $s = p^i$; $G = \mathrm{EA}(p^i)$, $\lambda = p^j$, *where p is a prime, i, j are non-negative integers with $i \neq 0$ and $\mathrm{EA}(p^i)$ denotes the elementary abelian group of order p^i* (Drake [4, Corollary 1.9]).

We conclude this section by generalizing Butson's result to arbitrary odd prime powers. This simultaneously yields an alternative considerably simpler proof of his theorem.

Theorem 2.4. *Let q be an odd prime power. Then there exists a $(q; 2)$-GH-matrix over $\mathrm{EA}(q)$.*

Proof. Consider $\mathrm{EA}(q)$ as the additive group of the Galois field $\mathrm{GF}(q)$ and define matrices $A_i=(a^i_{xy})$ $(x, y\in \mathrm{GF}(q); i=1, \ldots, 4)$ by

$$a^1_{xy}:=xy+(x^2/4); \qquad a^2_{xy}:=xy+(nx^2/4);$$
$$a^3_{xy}:=xy-y^2-(x^2/4); \qquad a^4_{xy}:=(xy-y^2-(x^2/4))/n$$

where n is any non-square of $\mathrm{GF}(q)$. Then put

$$D:=\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}.$$

We claim that D is the desired GH-matrix. In view of Theorem 2.2 it will be sufficient to verify (1.1) for D. Note that each A_i is a $(q; 1)$-GH-matrix over $\mathrm{EA}(q)$: certainly $A=(xy)$ (the multiplication table of $\mathrm{GF}(q)$) is a $(q; 1)$-GH-matrix and the A_i's are obtained from A by adding suitable elements to the rows and columns of A which obviously leaves property (1.1) invariant. Thus (1.1) is clearly satisfied (with $\lambda=2$) if we consider two rows of D which both belong to $(A_1\, A_2)$ respectively to $(A_3\, A_4)$. Now let x, x' be arbitrary and consider rows x of $(A_1\, A_2)$ and x' of $(A_3\, A_4)$. The differences arising from A_1 and A_3 then are the elements

$$y^2+y(x-x')+(x^2+x'^2)/4=(y+(x-x')/2)^2+(xx'/2)(y\in \mathrm{GF}(q)).$$

But these elements contain $xx'/2$ once and every element of the form $s+(xx'/2)$ with s a square twice. Similarly, the differences arising from A_2 and A_4 are the elements

$$(y^2+y(nx-x')+(n^2x^2+x'^2)/4)/n=(y+(nx-x')/2)^2/n+(xx'/2)$$

which yields $xx'/2$ a second time and all elements of the form $u+(xx'/2)$ with u a non-square twice. This completes the proof.

Using the matrices just constructed and (2.3) in the well-known Kronecker product construction (which of course has to be written additively here, see Proposition 4.3 below) we obtain

Corollary 2.5. *Let $q=p^i$ be an odd prime power. Then there exist $(q; 2^m q^{m-1})$- and $(q; 2^m q^m p^j)$-GH-matrices over $\mathrm{EA}(q)$ for all natural numbers m and all non-negative integers j.*

3. Resolvable TD's

We now study TD's with parallel classes. One first has

Proposition 3.1. *Let Σ be an $(s, r; \lambda)$-TD which has at least one parallel class. Then necessarily $r\leqq s\lambda$.*

Proof. Let $\mathbf{C}$ be a parallel class of Σ and choose any block B of $\mathbf{C}$. By Proposition 1.3, $\mathbf{C}$ consists of s blocks. Label the remaining $m := s(s\lambda - 1)$ blocks of Σ as $G_1, \ldots, G_m$ and let $x_i := [B, G_i]$ for $i = 1, \ldots, m$. Counting the flags (p, G_i) with $p \mathrm{I} B$ one obtains by 1.3

$$(3.1) \quad \sum_{i=1}^{m} x_i = r(s\lambda - 1).$$

Similarly, counting all double flags (p, q, G_i) with $p, q \mathrm{I} B, G_i$ for a fixed point p ($q = p$ is allowed, too) one has

$$\sum_{G_i \mathrm{I} p} x_i = s\lambda - 1 + (r-1)(\lambda - 1);$$

summation over all points $p \mathrm{I} B$ then yields

$$(3.2) \quad \sum_{i=1}^{m} x_i^2 = r(s\lambda - 1 + (r-1)(\lambda - 1)).$$

But using the well-known inequality $\left(\sum_{i=1}^{m} x_i\right)^2 \leqq m \left(\sum_{i=1}^{m} x_i^2\right)$ (see e.g. [8, p. 245]), a short computation gives $r \leqq s\lambda$ from (3.1) and (3.2).

We remark that it is also well-known that equality holds in the above argument if and only if all x_i coincide; thus $r = s\lambda$ if and only if $x_i = \lambda$ for all i (by (3.1)). Using this observation we obtain:

Theorem 3.2. *Let Σ be an $(s, s\lambda; \lambda)$-TD. Then the following assertions are equivalent:*

(i) *Σ is resolvable.*
(ii) *Σ is symmetric* (see Definition 1.2).
(iii) *Any two blocks of Σ intersect in either 0 or λ points.*

(The dual of such a TD has been called an affine resolvable partial plane in [5] and [4].)

Proof. Trivially, (ii) implies (i). Now suppose the validity of (i). Since $r = s\lambda$, our remarks above show that the dual of Σ satisfies (1.4) and (trivially) (1.3) and (1.5), i.e. Σ is symmetric. So (i) and (ii) are equivalent. But (ii) and (iii) are equivalent by Drake [4, Lemma 2.4] where the dual assertion has been proved.

In view of these results we will call a resolvable TD with $r = s\lambda$ *completely resolvable.* The proof given resembles [5, 5.3]. Theorem 2.2 is now an easy corollary to the results just obtained. By Theorem 1.5 and Proposition 3.1, $r \leqq s\lambda$ for any $(s, r; \lambda, G)$-difference matrix D. If actually $r = s\lambda$, then $\Sigma(D)$ is resolvable and thus by Theorem 3.2 the dual of $\Sigma(D)$ is also a TD; clearly this TD is also G-regular by the construction in Theorem 1.5. As in $\Sigma(D)$ $(i, y) \mathrm{I} B_{jx}$ iff $y - x = d_{ij}$ iff $x - y = -d_{ij}$ we see that the dual of Σ can be described by $-D^T$ and therefore $-D^T$ and hence D^T are difference matrices which completes the proof of Theorem 2.2. We also have proven

Corollary 3.3. *Let Σ be a complete resolvable (and hence symmetric)* TD. *Then Σ is G-regular if and only if its dual is G-regular. If Σ is described by the difference matrix D, then its dual may be described by $-D^T$.*

Our next result is a generalization of Shrikhande [15, Theorem 2] where the special case $s=p$ a prime, $t=2$ has been proved in the language of orthogonal arrays. Our proof is essentially the same.

Theorem 3.4. *Assume the existence of the series of complete resolvable* TD's *with parameters s and $\lambda=ts^n$, n a nonnegative integer. Then there exists an $(s, ts^{n+1}+ts^n+\ldots+ts+1; ts^n)$-*TD *for each n.*

Proof. We use induction on n. For $n=0$, the resolvable $(s, ts; t)$-TD can be embedded into an $(s, ts+1; t)$-TD by adding one point class and adjoining each of the new points to the blocks of t distinct parallel classes (see [7, Lemma 6]). Now suppose that the theorem is true for a particular value of n and consider $n+1$. Let Σ be a resolvable $(s, ts^{n+2}; ts^{n+1})$-TD and Δ an $(s, ts^{n+1}+\ldots+ts+1; ts^n)$-TD. Then there is a $1-1$-correspondence between the ts^{n+2} parallel classes of Σ and the blocks of Δ. Define the desired TD on the disjoint union of the point classes of Σ and Δ by adjoining to each block of any given parallel class of Σ all points of the corresponding line of Δ. It is easily checked that the result is in deed an $(s, ts^{n+2}+ts^{n+1}+\ldots+ts+1; ts^{n+1})$-TD.

Corollary 2.5 and Theorem 1.5 yield series of complete resolvable TD's. Using these in the above construction, we obtain:

Corollary 3.5. *Let p be an odd prime, s any power of p and $t=2^m s^{m-1}$ (m a natural number) or $t=2^m p^j s^m$ (m a natural number, j any nonnegative integer). Then there exists an $(s, ts^{n+1}+ts^n+\ldots+ts+1; ts^n)$-*TD *for each nonnegative integer n.*

We remark that the case $t=2$ has been obtained by other, much more involved methods by Kempthorne and Addelman [13] and that these examples meet the Bose-Bush bound which improves the inequality of Proposition 1.3 when $s-1$ does not divide $\lambda-1$ (see [1] or [4]) and thus have maximum possible r.

4. Some Constructions

In this section we collect some constructions of difference matrices. But first we state a non-existence result due to Drake [4, Theorem 1.10] which generalizes the well-known theorem of Hall and Paige on complete mappings:

Theorem 4.1 (Drake). *Let G be any group of even order s with a cyclic Sylow 2-subgroup. Then there is no $(s, r; \lambda, G)$-difference matrix with $r \geqq 3$ whenever λ is odd.*

We now list some quite trivial constructions.

Proposition 4.2. *The existence of an $(s, r; \lambda, G)$-difference matrix implies the existence of an $(s, r; n\lambda, G)$-difference matrix for every natural number n. The existence of both $(s, r; \lambda, G)$- and $(s, r; \lambda', G)$-difference matrices implies the existence of an $(s, r; \lambda+\lambda', G)$-difference matrix.*

For example, the existence of (9, 18; 2, EA(9))- and (9, 27; 3, EA(9))-difference matrices (by Theorem 2.4 and (2.3)) implies the existence of (9, 18; λ, EA(9))-difference matrices for every $\lambda \geqq 2$ (for $\lambda = 1$ the maximum value of r is 9).

Proposition 4.3 (Shrikhande). *The existence of $(s, r; \lambda, G)$- and of $(s, r'; \lambda', G)$-difference matrices implies the existence of an $(s, rr'; s\lambda\lambda', G)$-difference matrix.*

Proof. Let D and D' be the given difference matrices and form the Kronecker product (written additively) of D and D', i.e. put $A = (A_{ik})$ with $A_{ik} = d_{ik} + D'$ $(i = 1, \ldots, r;\ k = 1, \ldots, s\lambda)$. For the details, see [15, Theorem 3].

Proposition 4.3 has already been used in the proof of Corollary 2.5 (it is clear that the Kronecker product of complete difference matrices is complete). Another example: the existence of a (9, 9; 1, EA(9))- and of (9, 18; λ, EA(9))-difference matrices for every $\lambda \geqq 2$ shown above implies the existence of a (9, 162; 9λ, EA(9))-difference matrix for every $\lambda \geqq 2$. In analogy to the proof of Theorem 3.4 this implies the existence of (9, 181; 9λ)-TD's for all $\lambda \geqq 2$. Whereas the two previous constructions produced new difference matrices over the same group, the next ones will yield matrices over another group.

Proposition 4.4. *Let D be an $(s, r; \lambda, G)$-difference matrix and $\psi: G \to G'$ be a group epimorphism with $|G'| = s'$ and $|\ker \psi| = t$ (so $s't = s$). Then D^{ψ} is an $(s', r; \lambda t, G')$-difference matrix.*

For example, the well-known existence of a (12, 6; 1, EA(4)$\oplus C_3$)-difference matrix (see [9]) implies the existence of (6, 6; 2, C_6)-, (4, 6; 3, EA(4))- and (3, 6; 4, C_3)-difference matrices. In view of Theorem 4.1, the first of these results seems particularly interesting. The last example may also be obtained by Theorem 2.4 and Proposition 4.2. Proposition 4.4 also yields the proof of (2.3) by applying it to a $(p^{i+j}, p^{i+j}; 1, \mathrm{EA}(p^{i+j}))$-difference matrix for which we may take a multiplication table of $\mathrm{GF}(p^{i+j})$ (this is due to Drake [4, Corollary 1.9]).

Proposition 4.5. *The existence of $(s, r; \lambda, G)$ and $(s', r; \lambda', G')$-difference matrices implies the existence of an $(ss', r; \lambda\lambda', G \oplus G')$-difference matrix.*

Proof. Let D and D' be the given difference matrices and form the matrix

$$D \oplus D' := \begin{pmatrix} (d_{11}, d'_{11}) \ldots (d_{11}, d'_{1, s'\lambda'}) \ldots (d_{1, s\lambda}, d'_{11}) \ldots (d_{1, s\lambda}, d'_{1, s'\lambda'}) \\ \vdots \qquad\qquad\qquad\qquad\qquad\qquad \vdots \\ (d_{r1}, d'_{r1}) \ldots (d_{r1}, d'_{r, s'\lambda'}) \quad \ldots (d_{r, s\lambda}, d'_{r1}) \ \ldots (d_{r, s\lambda}, d'_{r, s'\lambda'}) \end{pmatrix}.$$

It is easily checked that $D \oplus D'$ is the desired $(ss', r; \lambda\lambda', G \oplus G')$-difference matrix. (This generalizes [10, Theorem 12].)

For example, using a (6, 6; 2, C_6)- and a (5, 6; 1, C_5)-difference matrix, we obtain a (30, 6; 2, C_{30})-difference matrix. In our next constructions, we do not have to know difference matrices already; the ingredients here will be TD's in general and difference families.

Theorem 4.6. *Let $(G, +, \cdot)$ be a ring of order s and let $\{x_1, \ldots, x_t\}$ be a set of units of G such that $x_i - x_j$ is a unit too whenever $i \neq j$. Then the existence of an $(s, r; \lambda)$-TD implies the existence of an $(s, rt+1; \lambda s, G)$-difference matrix.*

Proof. It is well known that the existence of an $(s, r; \lambda)$-TD is equivalent to the existence of an orthogonal array $(s^2\lambda, r, s, 2)$ (see e.g. [4, Proposition 3.2]). We recall that such an array is an $(r \times s^2\lambda)$-matrix with entries from a symbol set of s elements such that each $(2 \times s^2\lambda)$-submatrix contains each possible column vector (x, y) precisely λ times. Thus let A be an $(s^2\lambda, r, s, 2)$-orthogonal array with symbols from G. Then clearly A is an $(s, r; s\lambda, G)$-difference matrix. Now put

$$D := \begin{pmatrix} x_1 A \\ \vdots \\ x_t A \\ 0 \end{pmatrix}$$

where 0 is a row of 0's. We have to verify (1.1) for D. As each element of G appears in each row of A exactly $s\lambda$ times and as each x_i is a unit, (1.1) holds for row 0 and any other row of D. As A is a difference matrix, (1.1) holds for any two rows within the same $x_i A$. Now let $i \neq j$ and consider rows k and 1 of $x_i A$ and $x_j A$. If $k=1$, we obtain differences of the form $(x_i - x_j)y$; as y appears exactly $s\lambda$ times in row k of A and as $x_i - x_j$ is a unit, this yields each element of G exactly $s\lambda$ times. Finally let $k \neq 1$. Let y and z be any two elements of G. Then by the orthogonality property of A, we obtain the pair $(x_i y, x_j z)$ precisely λ times. But it is clear that precisely s pairs (y, z) will satisfy the equation $x_i y - x_j z = c$ for any given $c \in G$.

For the application of Theorem 4.6 one needs enough units in G. The best one can do is obviously taking a finite field $GF(s)$. This sometimes allows to improve results we could get with the previous methods. For example, the existence of $(4, 9; \lambda)$- and of $(5, 8; \lambda)$-TD's for all $\lambda \geqq 2$ (see Hanani [7, (3.3) and (3.4)]) implies the existence of $(4, 28; 4\lambda, EA(4))$- and of $(5, 33; 5\lambda, C_5)$-difference matrices for all $\lambda \geqq 2$. The previous results only yield (for $\lambda = 3$) $(4, 24; 12, EA(4))$- and $(5, 25; 15, C_5)$-difference matrices. Next consider some non prime power examples: e.g. there are $(15, 6; 1)$-, $(12, 7; 1)$- and $(20, 5; 1)$-TD's which yields the existence of $(15, 13; 15, C_{15})$-, $(12, 15; 12, EA(4) \oplus C_3)$- and $(20, 16; 20, EA(4) \oplus C_5)$-difference matrices. (For 12, we can do better: the Kronecker product of a $(12, 6; 1, EA(4) \oplus C_3)$-difference matrix with itself yields $(12, 36; 12, EA(4) \oplus C_3)$).) These last examples are easily generalized to give

Corollary 4.7. *Let $s = q_1 \ldots q_n$ be the prime power factorization of s and put $q := \min\{q_i : i = 1, \ldots, n\}$. Then the existence of an $(s, r; 1)$-TD implies the existence of an $(s, r(q-1)+1; s, EA(q_1) \oplus \ldots \oplus EA(q_n))$-difference matrix.*

Of course, $r = q+1$ is always possible by the theorem of McNeish; but this yields only q^2 rows which we can also obtain from the Kronecker product of an $(s, q; 1, EA(q_1) \oplus \ldots \oplus EA(q_n))$-difference matrix with itself. Such a matrix always exists by (2.3) and Proposition 4.5 (due to [10, Corollary 14]). So Corollary 4.7 is interesting only if we know better values than the McNeish bound. The next

corollary supposes the existence of a complete $(s, r; t)$-TD, i.e. $r=(s^2t-1)/(s-1)$ or equivalently of an ARBD with parameters s and $\mu=t$ (cf. Drake and Jungnickel [5, Propositions 5.6 and 5.7]). The special case of s a prime was proved by Shrikhande [15, Theorem 1(ii)]. Using $r=(s^2t-1)/(s-1)$ and Theorem 2.2 we have

Corollary 4.8. *Let s be a prime power and assume the existence of an* ARBD *with parameters s and $\mu=t$. Then there exists an $(s; st)$-GH-matrix over* EA(s).

Unfortunately, this does not yield any new GH-matrices as the only known series of ARBD's have parameters s a prime power and $t=s^n$ respectively $s=2$ and $4t$ the order of an (ordinary) Hadamard matrix (see [16]). We mention one more corollary to Theorem 4.6 which follows by the first part of the proof and gives some examples for the non-abelian case too.

Proposition 4.9. *Let G be any group of order s and assume the existence of an $(s, r; \lambda)$-TD. Then there exists an $(s, r; \lambda s, G)$-difference matrix.*

Using the ARBD's mentioned above we obtain $(s, s^n+\ldots+s+1; s^n, G)$-difference matrices for any group G of order s (s a prime power). Our last construction uses difference families. Recall that a (v, k, λ)-difference family over a group G of order v is a family $D_1, \ldots, D_n$ of subsets D_i of cardinality k of G such that the list of differences $x-y$ (where x and y are distinct elements of the same D_i) contains each nonzero element of G exactly λ times (see e.g. [6]). We now generalize [10, Theorem 19] and obtain

Theorem 4.10. *Assume the existence of a (v, k, λ)-difference family over G and of a $(k, r; 1)$-TD with a parallel class. Then there exists a $(v, r; \lambda, G)$-difference matrix.*

Proof. From the $(k, r; 1)$-TD with parallel class $\mathbf{C}$ form an orthogonal array $(k^2, r, k, 2)$ on the symbols $\{1, \ldots, k\}$ s.t. the last k columns are the vectors $(x, \ldots, x)^T$, $x \in \{1, \ldots, k\}$. (This may be done by taking the blocks of $\mathbf{C}$ to correspond to the last k columns and by labelling each point on the x'th block of $\mathbf{C}$ as x.) Discard these last k columns and replace each entry i by the i'th element of the set D_j of the given difference family (j fixed); this yields an $(r \times k(k-1))$-matrix A_j over G. Then put

$$D := (A_1 A_2 \ldots A_n 0)$$

where 0 denotes an $(r \times \lambda)$-zero matrix. Using the orthogonality property of the array and the fact that $\{D_1, \ldots, D_n\}$ was a (v, k, λ)-difference family one may check that D is a $(v, r; \lambda, G)$-difference matrix.

This construction yields e.g. the existence of $(40, 13; 4, C_{40})$-, $(15, 7; 3, C_{15})$-, $(21, 5; 1, C_{21})$- and $(57, 8; 1, C_{57})$-difference matrices. (The corresponding difference families may be found in [6] and the existence of TD's with one more point class than the value of r given above implies the existence of resolvable TD's with the value stated.) Application of Proposition 4.4 then yields e.g. $(20, 13; 8, C_{40})$- and $(10, 13; 16, C_{40})$-difference matrices. Unfortunately it is in general not possible to give a similar construction for (say resolvable) $(k, r; \mu)$-TD's with $\mu \neq 1$ as we can not assume that all pairs (x, x) occur in the last columns. (This would clearly force $r \leqq k$.) Using one parallel class one may again obtain the last

k columns as $(x, \ldots, x)^T$. The construction above then yields a matrix (no zero columns added up to now) which yields every nonzero element of G $\lambda\mu$ times as a difference and 0 $k(\mu-1)$ times (for any two distinct rows). So we may get the desired result by adding zero columns provided that $k(\mu-1) \leqq \lambda\mu$. Thus we have

Proposition 4.11. *Assume the existence of a (v, k, λ)-difference family over G with $k(\mu-1) \leqq \lambda\mu$ and of a $(k, r; \mu)$-TD with a parallel class. Then there exists a $(v, r; \lambda\mu, G)$-difference matrix.*

We may apply Proposition 4.11 for $\mu \leqq k$ and the trivial $(k+1, k, k-1)$-difference family which exists in any group G. For k a prime power and $\mu = k$ resp. $\mu = 2$ (by (2.3) and Theorem 2.4 in conjunction with Theorem 1.5) we obtain

Corollary 4.12. *Let q be a prime power and G be any group of order $q+1$. Then there exist both $(q+1, q^2; q(q-1), G)$- and $(q+1, 2q; 2(q-1), G)$-difference matrices.*

E.g., we obtain $(6, 25; 20, C_6)$- and $(6, 10; 8, C_6)$-difference matrices. Similarly, application of Theorem 4.10 to the trivial difference families yields a $(6, 5; 4, C_6)$-, a $(10, 9; 8, C_{10})$- and a $(14, 13; 12, C_{14})$-difference matrix. In general, one has

Corollary 4.13. *Let q be a prime power and G be any group of order $q+1$. Then there exists a $(q+1, q; q-1, G)$-difference matrix.*

We just used difference families in the construction of difference matrices. It should be remarked that the converse is possible too. This has been done (for $\lambda = 1$) in [11, Theorem 4.1]. This result is easily generalized to the following result (the term $(v, k, \lambda; s)$-difference family is explained in [11, Definition 2.3]):

Theorem 4.14. *Assume the existence of a $(v, k, \lambda; s)$-difference family in G and of a $(t, k; \lambda', G')$-difference matrix. Then there also is a $(tv, k, \lambda\lambda'; st)$-difference family in $G \oplus G'$. Furthermore, if the $(v, k, \lambda; s)$-family is maximal (i.e. an ordinary difference family) and if there also is an ordinary $(t, k, \lambda\lambda')$-difference family in G', then there exists an ordinary $(tv, k, \lambda\lambda')$-difference family in $G \oplus G'$.*

We leave the proof to the reader (cf. [11]) and give some numerical examples instead. Take a $(91, 10, 1)$-difference family in C_{91}; the existence of $(13, 13; 1, C_{13})$- and of $(7, 14; 2, C_7)$-difference matrices implies the existence of a $(91, 10; 2, C_{91})$-difference matrix. Then we obtain $(91^n, 10, 2^{n-1})$-difference families in $C_{91} \oplus \ldots \oplus C_{91}$ for all natural numbers n. Similarly, one obtains $(133^n, 12, 2^{n-1})$-difference families in $C_{133} \oplus \ldots \oplus C_{133}$ for all n. Note that [11, Theorem 3.1] cannot be applied in these cases. Or take $(16, 6, 2)$- and $(31, 6, 1)$-difference families in EA(16) resp. C_{31}. We then obtain $(16^k 31^n, 6, 2^k)$-difference families in $\mathrm{EA}(16^k) \oplus \mathrm{EA}(31^n)$ for all k and n (not both 0).

References

1. Bose, R.C., Bush, K.A.: Orthogonal arrays of strength two. Ann. Math. Statist. **23**, 508–524 (1952)
2. Butson, A.T.: Generalized Hadamard matrices. Proc. Amer. Math. Soc. **13**, 894–898 (1962)
3. Dembowski, P.: Finite geometries. Berlin-Heidelberg-New York: Springer 1968

4. Drake, D.A.: Partial λ-geometries and generalized Hadamard matrices over groups. Canadian J. Math. (to appear)
5. Drake, D.A., Jungnickel, D.: Klingenberg structures and partial designs II. Regularity and uniformity. Pacific J. Math. **77**, 389–415 (1978)
6. Hall, M., Jr.: Combinatorial theory. Waltham: Blaisdell 1967
7. Hanani, H.: On transversal designs. In: Proceedings of the Advanced Study Institute on Combinatorics (Breukelen 1974), pp. 42–52. Mathematical Centre tracts **55**. Amsterdam: Mathematisch Centrum 1974
8. Hughes, D.R., Piper, F.C.: Projective planes. Berlin-Heidelberg-New York: Springer 1973
9. Johnson, D.M., Dulmage, A.K., Mendelsohn, N.S.: Orthomorphisms of groups and orthogonal Latin squares. Canadian J. Math. **13**, 356–372 (1961)
10. Jungnickel, D.: On difference matrices and regular Latin squares. Abh. Math. Sem. Univ. Hamburg (to appear)
11. Jungnickel, D.: Composition theorems for difference families and regular planes. Discrete Math. **23**, 151–158 (1978)
12. Jungnickel, D.: On TD-structures. Arch. Math. (Basel) **31**, 403–413 (1978)
13. Kempthorne, O., Adelman, S.: Some main effect plans and orthogonal arrays of strength two. Ann. Math. Statist. **32**, 1167–1178 (1961)
14. Raghavarao, D.: Constructions and combinatorial problems in design of experiments. New York: Wiley 1971
15. Shrikhande, S.S.: Generalized Hadamard matrices and orthogonal arrays of strength two. Canadian J. Math. **16**, 736–740 (1964)
16. Shrikhande, S.S.: Affine resolvable balanced incomplete block designs: A survey. Aequationes Math. **14**, 251–269 (1976)
17. Wallis, W.D., Street, A.P., Wallis, J.S.: Combinatorics: Room squares, sum-free sets, Hadamard matrices, pp. 273–489. Berlin-Heidelberg-New York: Springer 1972

Received October 2, 1978