To appear in DCC

Concerning difference matrices

Charles J. Colbourn*
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

Donald L. Kreher†
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

Abstract Several new constructions for difference matrices are given. One class of constructions uses pairwise balanced designs to develop new difference matrices over the additive group of GF(q). A second class of constructions gives difference matrices over groups whose orders are not (necessarily) prime powers.

1 Introduction

We employ definitions from design theory consistent with [2]. An *orthogonal array* $\mathrm{OA}_\lambda(k,n)$ is a k by λn^2 array A whose entries come from an n-element set X, so that for any $1 \le i_1 < i_2 \le k$, and any $\alpha, \beta \in X$, there are exactly λ columns in the set $\{j : A[i_1,j] = \alpha \text{ and } A[i_2,j] = \beta\}$. The orthogonal array is said to have *order* n, *degree* k and *index* λ.

A $(s,v;\lambda)$–*difference matrix* over the group $(G,*)$ of order s is a v by $s\lambda$ matrix D with entries from G such that the multiset

$$\{D[i_1,j] * D[i_2,j]^{-1} : j = 1,2,\ldots s\lambda\}$$

for any pair of rows (i_1,i_2) contains every element of G exactly λ times. If the base group G is abelian, additive notation is often used. If D is a $(s,v;\lambda)$–difference matrix expressed multiplicatively over the group $G = \{g_1,\ldots,g_s\}$, then

$$[Dg_1, Dg_2, Dg_3, \ldots, Dg_s]$$

is an $\mathrm{OA}_\lambda(v,s)$.

Difference matrices have been studied primarily as a consequence of their uses in the construction of orthogonal arrays (see, for example, [2] and [6]). In fact, an orthogonal

*Research supported by NSERC Canada grant A0579.
†Research supported by National Security Agency grant MDA904–92–H–3036.

array $\mathrm{OA}_\lambda(v,s)$ that admits an automorphism group G acting regularly on the symbols is equivalent to a $(s,v;\lambda)$–difference matrix [7].

Jungnickel [7] established that a $(s,v;\lambda)$–difference matrix satisfies $v \leq s\lambda$. Most previous research on difference matrices has concentrated on constructions with a "large" number of rows (close or equal to $s\lambda$). However, for many selections of s and λ, no constructions of this type are available. In these cases, often the best bound is obtained by using the observations that given a $(s_1,v_1;\lambda_1)$–difference matrix and a $(s_2,v_2;\lambda_2)$–difference matrix, one can produce a $(s_1,\min(v_1,v_2);\lambda_1+\lambda_2)$–difference matrix if $s_1 = s_2$, and a $(s_1s_2,\min(v_1,v_2);\lambda_1\lambda_2)$–difference matrix. These simple "addition" and "multiplication" constructions typically yield a number of rows far from the upper bound.

Hence it is of substantial interest to improve the lower bounds on the numbers of rows in difference matrices. We develop two types of constructions here, and demonstrate that they improve some of the lower bounds implied by the known constructions.

2 A PBD construction

In this section we give a construction for $(s,v;\lambda)$–difference matrices over the additive group of $\mathrm{GF}(s)$.

A pairwise balanced design of order v and index λ is a pair $(X,\mathcal{B})$ where X is a v–element set of *points* and $\mathcal{B}$ is a family of (not necessarily distinct) subsets of X called *blocks* such that every pair of points is in precisely λ blocks. We denote a pairwise balanced design of order v and index λ by $\mathrm{PBD}(v,\lambda)$. Blocks of size one and two *are permitted.*

Let $(X,\mathcal{B})$ be a $\mathrm{PBD}(v,\lambda)$. A collection $\mathcal{P}$ of n disjoint blocks in $\mathcal{B}$ that contain all of the points of X is a *parallel class of width* n. A $\mathrm{PBD}(v,\lambda)$ is *resolvable* if it can be partitioned into parallel classes.

An ℓ by w $\mathrm{PBD}(v,\lambda)$ is a $\mathrm{PBD}(v,\lambda)$ whose blocks can be partitioned into ℓ parallel classes of maximum width w. For example, developing the parallel class

$$\{0\},\{1,2,4\},\{3,5,6\}$$

modulo 7 constructs a 7 by 3 $\mathrm{PBD}(7,2)$. Developing the parallel class

$$\{0\},\{3\},\{5\},\{6\},\{1,2,4\}$$

modulo 7 constructs a 7 by 5 $\mathrm{PBD}(7,1)$.

LEMMA **2.1** *If there is a $(s,v;\lambda)$–difference matrix then there exists an $s\lambda$ by s PBD(v,λ).*

Proof. Let D be a $(s,v;\lambda)$–difference matrix over the group $(G,*)$. Let X be the set of rows of D; for each column j of D and element g of G, define $B_{j,g}$ by

$$B_{j,g} = \{x \in X : D[x,j] = g\}$$

Let $\mathcal{B} = \{B_{j,g} : j \text{ is a column of } D \text{ and } g \in G\}$. For any pair of rows (i_1, i_2) of D, the multiset

$$\{D[i_1, j] * D[i_2, j]^{-1} : j = 1, 2, \ldots s\lambda\}$$

contains the identity of G exactly λ times; hence every pair of elements of X is in exactly λ of the $\{B_{j,g}\}$. Consequently, $(X, \mathcal{B})$ is a PBD(v, λ). Since $\mathcal{P}_j = \{B_{j,g} : g \in G\}$ is a parallel class, $(X, \mathcal{B})$ is $s\lambda$ by s. □

We establish a partial but important converse to Lemma 2.1. A definition is required. Let $(X, \mathcal{B})$ be an ℓ by w PBD(v, λ) and let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_\ell$ be its partition into ℓ parallel classes of maximum width w. Let G be a group of order $s \geq w$ and for each $j = 1, 2, \ldots \ell$ select an injection $\Phi_j : \mathcal{P}_j \to G$. The parallel class

$$\mathcal{P}_j = \{S_{1,j}, S_{2,j}, \ldots, S_{n,j}\}$$

describes the j-th column of an v by ℓ matrix M with entries in G by setting

$$M[k, j] = \Phi_j(S_{i,j}) \text{ if } k \in S_{ij} \in \mathcal{P}_j.$$

We say that M is a *matrix over G belonging to the ℓ by w PBD(v, λ)* $(X, \mathcal{B})$. For any pair of rows (i_1, i_2), the multiset

$$\{M[i_1, j] * M[i_2, j]^{-1} : j = 1, 2, \ldots s\lambda\}$$

contains the identity element of G exactly λ times. If M has the additional property that, for any $\alpha, \beta \in G$ and any two rows i_1, i_2,

$$| \{j : M[i_1, j] = \alpha \text{ and } M[i_2, j] = \beta\} | = | \{j : M[i_1, j] = \beta \text{ and } M[i_2, j] = \alpha\} |,$$

we say that the PBD has an *obverse matrix M* over G.

THEOREM **2.2** *Let s be a prime power. If there is an ℓ by w PBD(v, λ) with $w \leq s \leq \lfloor \frac{\ell}{\lambda} \rfloor$, then there exists a $(s, v; \ell - \lambda)$–difference matrix over the additive group of GF(s).*

Proof. Let $(X, \mathcal{B})$ be an ℓ by w PBD(v, λ) and let M, over the additive group of $GF(s)$, be any matrix belonging to $(X, \mathcal{B})$. Choose a primitive root α of GF(s) and set $D' = [M, \alpha M, \alpha^2 M, \ldots, \alpha^{s-2} M]$. If in rows i_1, i_2 of column j of M the difference is nonzero, then every nonzero difference occurs in rows i_1, i_2 in column j of exactly one $\alpha^h M$. Hence the vector difference of any pair of rows of D' contains each nonzero element of GF(s) exactly $\ell - \lambda$ times and 0 exactly $\lambda(s-1)$ times. The conditions guarantee that $\ell - \lambda \geq \lambda(s-1)$. Thus $m = \ell - \lambda s = \ell - \lambda - \lambda(s-1) \geq 0$ and we set Z to be the v by m zero matrix. Therefore

$$D = [M, \alpha M, \alpha^2 M, \ldots, \alpha^{s-2} M, Z]$$

is a $(s, v; \ell - \lambda)$–difference matrix over the additive group of GF(s). □

For example, the 7 by 3 PBD$(7, 2)$ given above yields a $(3, 7; 5)$–difference matrix over $\mathbb{Z}_3$ and the 7 by 5 PBD$(7, 1)$ yields a $(5, 7; 6)$–difference matrix.

LEMMA **2.3** *Let $v = 1 + nk$ be a prime power. Then*

(i) *there is v by $n+1$ PBD$(v, k-1)$ $(X, \mathcal{B})$;*

(ii) *if $v = 2^m$ for some m the PBD in* (i) *has an obverse matrix over any group G of order $s \geq n+1$; and*

(iii) *if v is odd and k is even the PBD$(v, k-1)$ in* (i) *has an obverse matrix over any group G of order $s \geq n+1$.*

Proof. Let f be a primitive element of GF(v) and set $g = f^n$. $K = \{1, g, g^2, \ldots, g^{k-1}\}$ is a subgroup of GF$(v)^*$ of order k. Let $\mathcal{P}$ be the parallel class consisting of $\{0\}$ and the n cosets of K in GF$(v)^*$ and define for all $x \in$ GF(v) the parallel class $\mathcal{P}_x$ by

$$\mathcal{P}_x = \mathcal{P} + x = \{B + x : B \in \mathcal{P}\}.$$

Then $\mathcal{B} = \cup_{x \in GF(v)} \mathcal{P}_x$ is preserved by the 2-transitive group $\{x \mapsto \alpha x + \beta : \alpha, \beta \in$ GF$(v), \alpha \neq 0\}$. $\mathcal{B}$ is a v by $n+1$ PBD$(v, k-1)$.

Let G be a group of order $s \geq n+1$ and fix any injection $\Phi : \mathcal{P} \to G$ such that $\Phi(\{0\}) = e$, the identity of G. For each $x \in$ GF(v) and $B \in \mathcal{P}$ define $\Phi_x(B + x) = \Phi(B)$ and construct the v by $n+1$ matrix $M = M_k$ as in the definition. That is, the $[i, j]$–entry of M_k is $\Phi_j(B + j)$ where $j \in$ GF(v) and $i \in B \in \mathcal{P}$.

We claim that, subject to the conditions of (ii) and (iii), M_k is an obverse matrix. For (ii), the matrix M_1 as defined above is just the addition table of the field GF(2^m) and an easy induction on m shows that it is obverse. Consequently, because M_k is a refinement of M_1 (i.e. if $M_1[i_1, x] = M_1[i_2, x]$, then $M_k[i_1, x] = M_k[i_2, x]$), M_k is obverse.

For (iii), when $k = 2$ the parallel classes of the PBD form a one factorization of the complete graph K_v and thus the matrix M_2 is obverse. Again any refinement of M_2 to a matrix M_{2h} is also obverse and so for k even the PBD has an obverse matrix M_k. If k is odd, a simple parity argument shows that the PBD cannot possibly have an obverse matrix. □

THEOREM **2.4** *If the ℓ by w PBD(v, λ) has an obverse matrix M over the additive group of GF(s) where s is an odd prime power such that $w \leq s \leq \lfloor \frac{\ell}{\lambda} \rfloor$, then there exists a $(s, v; \frac{\ell - \lambda}{2})$–difference matrix over $(GF(s), +)$.*

Proof. Choose a primitive root α of GF(s) and set

$$D' = [M, \alpha M, \alpha^2 M, \ldots, \alpha^{\frac{s-1}{2}-1} M]$$

Consider the pair of rows i_1, i_2 of M and let π be a permutation of order two on the ℓ columns of M such that if (a, b) occurs in column j on these rows, then (b, a) occurs in column $\pi(j)$ whenever $a \neq b$. If $a = b$, then $\pi(j) = j$. Now in column j of M, if the difference is a nonzero element $x \in$ GF(s), then every nonzero difference occurs in rows i_1, i_2 in column j or $\pi(j)$ of exactly one $\alpha^h M$. Hence the vector difference of any pair of rows of D' contains each nonzero element of GF(s) exactly $(\ell - \lambda)/2$ times and 0

exactly $\lambda(s-1)/2$ times. The conditions guarantee that $(\ell-\lambda)/2 \geq \lambda(s-1)/2$. Thus $m = (\ell-\lambda s)/2 = (\ell-\lambda)/2 - \lambda(s-1)/2 \geq 0$ and we set Z to be the v by m zero matrix. Therefore

$$D = [M, \alpha M, \alpha^2 M, \ldots, \alpha^{\frac{s-1}{2}-1} M, Z]$$

is a $(s, v; \frac{\ell-\lambda}{2})$–difference matrix over the additive group of GF(s). □

COROLLARY **2.5** *Let $v = 1 + nk$ and s be prime powers, with $n+1 \leq s \leq \lfloor \frac{v}{k-1} \rfloor$. Then there exist a $(s, v; v-k+1)$–difference matrix over $(GF(s), +)$ and there also exists a $(s, v; \frac{v-k+1}{2})$–difference matrix over $(GF(s), +)$ if v or k is even, and s is odd.*

Proof. Apply Theorems 2.2 and 2.4 to Lemma 2.3. □

In particular Corollary 2.5 settles the existence of a $(3, 7; 5)$–difference matrix and of a $(4, 13; 10)$–difference matrix.

The PBD$(v, k-1)$ used in Corollary 2.5 is a special kind of nearly resolvable design. In general a *nearly resolvable design* with parameters NRB(v, k) is a v by $1 + (v-1)/k$ PBD$(v, k-1)$ in which every nonsingleton block has exactly k points and $v = 1 + nk$ for some n. In [5] it is reported that:

- An NRB$(v, 3)$ exists if and only if $v \equiv 1 \bmod 3$.
- An NRB$(v, 4)$ exists if and only if $v \equiv 1 \bmod 4$.
- An NRB$(v, 5)$ exists for $v \equiv 1 \bmod 5$, except possibly for v in $\{46, 51, 141, 201\}$
- An NRB$(v, 6)$ exists for $v \equiv 1 \bmod 6$, except possibly for v in $\{55, 145\}$.

Applying Theorem 2.2 with s equal to the width, we get:

COROLLARY **2.6** *For every prime power s and integer $3 \leq k \leq 6$, there is a $(s, 1 + (s-1)k; 2 + (s-2)k)$–difference matrix over $(GF(s), +)$ except possibly for $(s, k) = (11, 5)$, $(29, 5)$, $(41, 5)$, or $(25, 6)$.*

Actually, more can be obtained because we can employ any prime power s in the range $1 + \frac{v-1}{k} \leq s \leq \frac{v-1}{k} + \frac{v}{k(k-1)}$.

We can also use resolvable designs:

COROLLARY **2.7** *There is $(s, 3s; 3(s-1)/2)$–difference matrix over the additive group of $GF(s)$ for all odd prime powers s.*

Proof. Let s be an odd prime power and set $n = (s-1)/2$. Then there is a Kirkman triple system of order $3s = 3 + 6n$ (see [2]). This is a $1 + 3n$ by $1 + 2n$ PBD$(3s, 1)$. Hence by Theorem 2.2 the result follows. □

For example using Corollary 2.7 a $(5, 15; 6)$–difference matrix can be constructed; this improves the bound on the number of rows v of a $(5, v; 6)$–difference matrix from $10 \leq v \leq 30$ to $15 \leq v \leq 30$.

COROLLARY **2.8** *If there is a resolvable BIBD with parameters (b, v, r, k, λ), with $\frac{v}{k}$ a prime power, then there is a $(\frac{v}{k}, v; r - \lambda)$–difference matrix.*

Proof. A resolvable BIBD is an r by v/k PBD(v, λ). Now

$$\frac{r}{\lambda} = \frac{v-1}{k-1} \geq \frac{v}{k}$$

since in a BIBD $v > k$ and $\lambda(v-1) = r(k-1)$. Therefore by Theorem 2.2 a $(\frac{v}{k}, v; r - \lambda)$–difference matrix exists. □

Several resolvable BIBD exist with which new difference matrices can be constructed using Corollary 2.8. Some examples are given in Table 1.

Table 1: Some resolvable (v, b, r, k, λ) designs that give new $(\frac{v}{k}, v; r - \lambda)$–difference matrices

No. in [8]	(v, b, r, k, λ)	$(\frac{v}{k}, v; r - \lambda)$–difference matrix
14	(15,35,7,3,1)	$(5, 15; 6)$–difference matrix
151	(65,208,16,5,1)	$(13, 65; 15)$–difference matrix
219	(39,247,19,3,1)	$(13, 39; 18)$–difference matrix
279	(85,357,21,5,1)	$(17, 85; 20)$–difference matrix

3 Two constructions

In this section we describe two constructions which produce difference matrices over arbitrary groups.

THEOREM **3.1** *If an $OA_\lambda(k, n)$ exists with at least λ constant columns, then, over any group G of order $n + 1$, a $(n + 1, k; \lambda(n - 1))$–difference matrix exists.*

Proof. Let G be any group of order $n+1$ with identity element e. Let A be an $\mathrm{OA}_\lambda(k, n)$, with entries from $X = G \setminus \{e\}$. In this array every ordered pair of symbols of X occurs λ times in each ordered pair of rows. Hence in the multiset

$$\{A[i_1, j] * A[i_2, j]^{-1} : j = 1, 2, \ldots s\lambda\}$$

for any pair of rows (i_1, i_2) e occurs λn times and each nonidentity element of G occurs $\lambda(n - 1)$ times. Deleting λ of the constant columns constructs the desired difference matrix. □

A $(10, 27; 24)$–difference matrix exists by Theorem 3.1, using an $\mathrm{OA}_3(27, 9)$.

THEOREM **3.2** *If v is a prime power and $v = 1 + nk$ for nonnegative integers n and k with $n \geq k-2 \geq 0$, then for any group G of order $n+1$ there is a $(n+1, v; 2+(n-1)k)$–difference matrix over G.*

Proof. Let f be a primitive element of GF(v) and set $g = f^n$. Then the order of g in GF(v)* is k. Hence, $B = \{g^j : 0 \leq j < k\}$ is a subgroup of GF(v)* of order k and $B_i = f^{i-1}B$, $i = 1, 2, 3, \ldots, n$ is a complete set of cosets. Let $B_0 = \{0\}$. Define the v by v matrix M indexed by GF(v) and with entries in $G = \{a_0 = e, a_1, a_2, \ldots a_n\}$ by:

$$M[\alpha, \beta] = a_i \text{ if and only if } \alpha + \beta \in B_i.$$

Now set π to be the permutation of the elements of G given by $\pi = (e)(a_1, a_2, a_3, \ldots, a_n)$ and define $\pi(M)$ to be the v by v matrix with $[i, j]$–th entry $\pi(M[i, j])$. Finally set Z to be the v by $(n - k + 2)$ constant matrix containing e and define the v by $(nv + n - k + 2)$ matrix D to be

$$D = [M, \pi(M), \pi^2(M), \cdots, \pi^{n-1}(M), Z]$$

We claim that D is difference matrix over G. Let $\alpha, \beta \in$ GF(v), $\alpha = f^\ell$ $(1 \leq \ell \leq n-1)$, and consider any $i, j \in$ GF(v). If $a_u = M[\alpha \cdot i + \beta, \alpha \cdot j - \beta]$, then $f^\ell(i + j) = \alpha(i + j) = \alpha \cdot i + \beta + \alpha \cdot j - \beta \in B_u = f^{u-1}B$. Hence $i + j \in f^{u-\ell-1}B = B_{u-\ell}$, which implies $M[i, j] = \pi^{-\ell}(a_u)$. Now fix a pair of rows i_0, i_0' of M and consider any other two rows i_1, i_1'. Since the group $H = \{x \mapsto \alpha x + \beta : \alpha, \beta \in \text{GF}(v)\}$ acts sharply 2–transitively on GF(v), there is a unique $\alpha, \beta \in$ GF(v) such that $\alpha \cdot i_0 + \beta = i_1$ and $\alpha \cdot i_0' + \beta = i_1'$. The above argument shows that the pair $(M[i_1, \alpha \cdot j - \beta], M[i_1', \alpha \cdot j - \beta]) = \pi^\ell(M[i_0, j], M[i_0', j])$ Hence $(M[i_1, \alpha \cdot j - \beta], M[i_1', \alpha \cdot j - \beta])$ and $(M[i_0, j], M[i_0', j])$ belong to the same orbit of π on ordered pairs. In particular if the orbit of (a_i, a_j) under π is represented $N_{i,j}$ times in some ordered pair of rows of M it is represented exactly $N_{i,j}$ times in every pair of rows. The value of $N_{i,j}$ can now be calculated. Let (x, y) be in the orbit of (a_i, a_j) under π.

Case 1. $i \neq 0$, $j \neq 0$.

In this case there are in column α of M exactly k^2 ordered pairs of rows that have (x, y). The length of the orbit of (a_i, a_j) under π is n and so in column α there are exactly nk^2 ordered pairs of rows that have an orbit representative of the orbit of (a_i, a_j) under π. Summing over all columns and dividing by the number of ordered pairs of rows, we find $N_{i,j} = k$.

Case 2. $i = 0$, $j \neq 0$ or $i \neq 0$, $j = 0$.

In this case there are in column α of M exactly k ordered pairs of rows that have (x, y). Following exactly the same argument as in case 1 we have in this case $N_{i,j} = 1$.

This regularity on M shows that in any pair of rows in D every ordered pair (a_i, a_j) occurs k times if neither i nor j is 0 and occurs once otherwise. Hence in any pair of rows each nonidentity difference occurs $k(n-1)+2$ times. A pair (a_i, a_j) has difference e if and only if $i = j$. If the pair is in column α and rows (β_1, β_2) of M this means that $\beta_1, \beta_2 \in B_i - \alpha$. But $\{B_i + \gamma : \gamma \in \text{GF}(v)\}$ is a set system invariant under the 2-transitive group H and is hence a 2–$(v, k, k-1)$ design. So the identity of G occurs as a difference in any particular pair of rows of D exactly $n(k-1) + n - k + 2 = k(n-1) + 2$ times. □

Some examples of this construction appear in Table 2.

Table 2: Some new difference matrices over arbitrary groups

A $(6, 11; 10)$–difference matrix over the group $\mathcal{A} = \{a_0 = e, a_1, \ldots, a_5\}$ is constructed by cyclically shifting the following five columns (shown transposed) into 55 columns and appending five columns of all zeros.

$$\begin{array}{ccccccccccc}
a_0 & a_1 & a_2 & a_4 & a_3 & a_5 & a_5 & a_3 & a_4 & a_2 & a_1 \\
a_0 & a_2 & a_3 & a_5 & a_4 & a_1 & a_1 & a_4 & a_5 & a_3 & a_2 \\
a_0 & a_3 & a_4 & a_1 & a_5 & a_2 & a_2 & a_5 & a_1 & a_4 & a_3 \\
a_0 & a_4 & a_5 & a_2 & a_1 & a_3 & a_3 & a_1 & a_2 & a_5 & a_4 \\
a_0 & a_5 & a_1 & a_3 & a_2 & a_4 & a_4 & a_2 & a_3 & a_1 & a_5
\end{array}$$

A $(4, 13; 10)$–difference matrix over the group $\mathcal{A} = \{a_0 = e, a_1, a_2, a_3\}$ is constructed by cyclically shifting the following three columns (shown transposed) into 39 columns and appending one column of all zeros.

$$\begin{array}{ccccccccccccc}
a_0 & a_1 & a_2 & a_2 & a_3 & a_1 & a_3 & a_3 & a_1 & a_3 & a_2 & a_2 & a_1 \\
a_0 & a_2 & a_3 & a_3 & a_1 & a_2 & a_1 & a_1 & a_2 & a_1 & a_3 & a_3 & a_2 \\
a_0 & a_3 & a_1 & a_1 & a_2 & a_3 & a_2 & a_2 & a_3 & a_2 & a_1 & a_1 & a_3
\end{array}$$

4 Concluding Remarks

We have developed a number of constructions here for difference matrices, but the number of rows obtained is relatively small. Nevertheless, the results obtained often improve upon the best available results in the literature. To see what effect the results developed have upon the bounds on the number of rows, we tabulate in Tables 3 and 4 the best lower bounds on the number v of rows in a $(s, v; \lambda)$–difference matrix for $1 \leq s \leq 32$ and $1 \leq \lambda \leq 30$. A key is provided to interpret the authority for each entry, which is given as a single letter superscript on the entry. When the superscript is omitted, the entry is obtained by the addition or multiplication construction stated in the introduction.

Key For Table 3 and 4	
blank	obtained by addition or multiplication
d	de Launey [4]
g	generalized Hadamard matrix; see [3]
h	Hadamard matrix; see [2]
j	Jungnickel [7]
m	Theorem 3.2
n	Theorem 3.1
p	Theorem 2.2
q	Theorem 2.4
s	sporadic example; see [1] and [2]
t	tensor product; see [9]

We do not include the upper bounds, as for the most part they can be calculated easily. When $s \equiv 2 \pmod 4$ and $\lambda \equiv 1 \pmod 2$, a $(s, v; \lambda)$–difference matrix exists only for $v \leq 2$ (see, for example, [2]). In the remaining cases, $v \leq s\lambda$ always provides an upper bound [7]; when equality holds, the difference matrix is a *generalized Hadamard matrix*. Nonexistence of generalized Hadamard matrices for certain choices of s and λ (see, for example, [3]) reduces the upper bound to $v \leq s\lambda - 1$.

Acknowledgments

This work was completed while the authors held Raybould Fellowships at the University of Queensland, Australia. Special thanks to Anne Street, Liz Billington and the other members of the Department of Mathematics there. The authors were also supported in part by NSF grant DMS-9402637. We especially thank Neil Sloane for suggesting the problem and for his encouragement, and Dieter Jungnickel for some very helpful comments.

References

[1] R.J.R. Abel and Y.W. Cheng, Some new MOLS of order $2^n p$ for p a prime power, *Austral. J. Combin.* 10 (1994), 175–186.

[2] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, 1986.

[3] W. de Launey, A survey of generalized Hadamard matrices and difference matrices $D(k, \lambda; G)$ with large k, *Util. Math.* 30 (1986), 5–29.

[4] W. de Launey, On difference matrices, transversal designs, resolvable transversal designs, and large sets of mutually orthogonal F-squares, *J. Stat. Plan. Infer.* 16 (1987), 107–125.

[5] S. Furino, Existence results for near resolvable designs, *J. Comb. Designs*, to appear.

[6] A.S. Hedayat, N.J.A. Sloane and J. Stufken, *Orthogonal Arrays*, to appear.

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

[8] R. Mathon and A. Rosa, Tables of parameters of BIBDs with $r \leq 41$ including Existence, Enumeration, and Resolvability Results, *Ann. Disc. Math.* **26**(1985) 275-308.

[9] S.S. Shrikhande, Generalized Hadamard matrices and orthogonal arrays of strength 2, *Canad. J. Math.* **16** (1964), 131–141.

Table 3: Lower Bounds on Numbers of Rows in $(s, k; \lambda)$–difference matrix

$s \setminus \lambda$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2^g	4^h	2	8^h	2	12^h	2	16^h	2	20^h	2	24^h	2	28^h	2
3	3^g	6^g	9^g	12^g	7^m	18^g	9	24^g	27^g	30^g	9	36^g	12	18	21^d
4	4^g	8^g	12^g	16^g	8	12	12	32^g	36^g	13^m	12	28^j	16	56^g	12
5	5^g	10^g	7^q	20^g	25^g	15^p	17^q	20	20	50^g	17	25^d	20	20	33^j
6	2	6^s	2	6	2	6	2	10^j	2	11^m	2	8	2	16^m	2
7	7^g	14^g	7	28^g	11^q	15^p	49^g	28	28^d	15	28	28	28	98^g	28
8	8^g	16^g	8	32^g	8	16	56^g	64^g	21^p	16	32	32	21	56	56
9	9^g	18^g	27^g	36^g	18	54^g	27	72^g	81^g	36	27	108^g	36	54	54
10	2	4	2	8^s	2	5	2	10^s	2	5	2	10	2	5	2
11	11^g	22^g	11	44^g	11	22	11	44	19^q	22	121^g	44	22	22	44
12	6^s	6	6	6	6	8	6	8	9	11^j	6	15^j	6	8	8
13	13^g	26^g	13	52^g	13	26	13	52	19^q	26	23^q	52	169^g	27^p	65^p
14	2	5^s	2	7	2	7	2	8	2	7	2	13^j	2	7	2
15	5^s	7^s	7^j	7	7	9	7	10	7	7	7	10	7	9	13^j
16	16^g	32^g	16	64^g	16	32	16	128^g	16	32	16	64	16	32	65^p
17	17^g	34^g	17	68^g	17	34	17	68	19^q	34	23^q	68	27^q	34	31^q
18	2	6^s	2	8	2	9	2	9	2	9	2	12	2	9	2
19	19^g	38^g	19	76^g	19	38	19	76	19	38	23^q	76	27^q	38	31^q
20	4	8^s	5	10^s	5	10	5	13^j	7	10	7	12	7	10	12
21	6^s	6	7	7	7	9	7	12	7	7	7	14	7	9	9
22	2	4	2	8	2	11	2	11	2	11	2	12	2	11	2
23	23^g	46^g	23	92^g	23	46	23	92	23	46	23	92	27^q	46	31^q
24	6^s	6	8	8	7	9	8	12	8	8	8	16	8	9	8
25	25^g	50^g	25	100^g	125^g	50	50	100	100	125	50	100	100	100	125
26	2	4	2	8	2	12	2	13	2	13	2	13	2	13	2
27	27^g	54^g	81^g	108^g	54	162^g	81	108	243^g	108	81	324^g	108	108	162
28	5^s	7	7	8	7	12	7	14	7	8	7	12	7	12	11
29	29^g	58^g	29	116^g	29	58	29	116	29	58	29	116	29	58	31^q
30	2	5	2	6	2	6	2	7	2	6	2	8	2	6	2
31	31^g	62^g	31	124^g	31	62	31	124	31	62	31	124	31	62	31
32	32^g	64^g	32	128^g	32	64	32	256^g	32	64	32	128	32	64	32

Table 4: Lower Bounds on Numbers of Rows in $(s, k; \lambda)$–difference matrix (cont'd)

s \ λ	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
2	32^h	2	36^h	2	40^h	2	44^h	2	48^h	2	52^h	2	56^h	2	60^h
3	48^g	24	54^g	27	30	27	30	21	72^g	27	30	81^g	42^d	27	90^t
4	64^g	32	36	13	28	28	32	36	36^t	36	32	108^g	56	28	56
5	80^g	35^d	90^g	20	100^g	25	25	25	60^d	125^g	50	35	50	25	75^t
6	20^j	2	10	2	25^j	2	10	2	15^j	2	31^m	2	16	2	16
7	37^q	28	63^d	28	28	49	28	37	28	49	182^g	31^m	196^g	28	91^d
8	128^g	21	32	32	32	56	56	56	64	32	32	32	56	56	99^d
9	72	72	162^g	36	72	81	54	54	108	72	72	243^g	72	72	108
10	18^j	2	19^m	2	10	2	8	2	27^n	2	10	2	10	2	12
11	44	37^q	22	44	44	37	242^g	44	121^d	37	44	44	61^q	37	44
12	12	8	12	9	22^j	9	23^m	8	16	9	11	12	12	9	12
13	52	52	39^p	52	52	52	39	52	52	52	338^g	52	169^d	52	65
14	14	2	7	2	14	2	7	2	26^j	2	27^m	2	14	2	11
15	12	7	10	7	12	9	9	10	18	7	10	10	29^m	9	18
16	256^g	33^p	39^p	64	64	45^p	39	65	128	45	39	64	64	45	65
17	272^g	289^g	39^p	34	85^p	68	39	34	68	68	39	34	68	68	39
18	17^j	2	12	2	18	2	9	2	18	2	9	2	18	2	20
19	76	31	39^p	361^g	85^p	45^p	39	76	76	45	39	76	76	61^q	39
20	16	8	19^j	10	19^j	12	10	12	15	10	13	12	16	12	12
21	14	7	14	7	14	15^j	9	9	18	7	12	9	14	12	14
22	16	2	11	2	20	2	11	2	22	2	11	2	22	2	11
23	92	31	46	31	92	43^q	46	529^g	92	46	46	92	92	46	63^p
24	16	8	16	8	16	9	23^j	8	18	8	12	9	16	9	16
25	100	100	100	100	125	100	100	100	100	625^g	100	100	100	100	125
26	16	2	13	2	20	2	13	2	25^j	2	13	2	26	2	13
27	108	108	243	108	108	243	108	108	324	108	108	729^g	108	108	243
28	16	7	14	8	13	12	12	11	15	8	27^j	12	19^j	12	12
29	116	31	58	31	116	43^q	58	47^q	116	47	58	47	116	841^g	63^p
30	10	2	7	2	10	2	6	2	9	2	7	2	29^j	2	7
31	124	31	62	31	124	43^q	62	47^q	124	47	62	47	124	59^q	63^p
32	512^g	32	64	32	128	32	64	32	256	32	64	32	128	32	64

Concerning difference matrices

Charles J. Colbourn[‡]
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

Donald L. Kreher[§]
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

keywords

difference matrices, pairwise balanced designs, orthogonal arrays

[‡]Research supported by NSERC Canada grant A0579.
[§]Research supported by National Security Agency grant MDA904–92–H–3036.

Concerning difference matrices

Charles J. Colbourn[¶]
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

Donald L. Kreher[‖]
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

mailing address for proofs

Professor Donald L. Kreher
Department of Mathematical Sciences
Michigan Technological University
1400 Townsend Drive
Houghton, Michigan
U.S.A. 49931-1295

[¶]Research supported by NSERC Canada grant A0579.
[‖]Research supported by National Security Agency grant MDA904–92–H–3036.

Concerning difference matrices

Charles J. Colbourn[**]
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, CANADA N2L 3G1

Donald L. Kreher[††]
Department of Mathematical Sciences, Michigan Technological University, Houghton, Michigan, U.S.A. 49931–1295

[**]Research supported by NSERC Canada grant A0579.
[††]Research supported by National Security Agency grant MDA904–92–H–3036.