Smallest defining sets of designs associated with $PG(d,2)$

Brenton D. Gray*

Centre for Combinatorics
Department of Mathematics
The University of Queensland
Brisbane 4072 Australia

Abstract

For $d \geq 2$, let D_d be the symmetric block design formed from the points and hyperplanes of the projective space $PG(d,2)$. Let s_d equal the number of blocks in a smallest defining set of D_d. The known results $s_2 = 3$ and $s_3 = 9$ are reviewed and it is shown that $s_4 = 24$ and $52 \leq s_5 \leq 55$. If $\mu_d = s_d/(2^{d+1}-1)$ is the proportion of blocks in a smallest defining set of D_d, then $\mu_2 = 3/7, \mu_3 = 9/15$ and $\mu_4 = 24/31$. The main result of this paper is that $\mu_d \to 1$ as $d \to \infty$.

1 Introduction

A **block design** $D = (V, \mathcal{B})$ is a set V of v elements (points), together with a set $\mathcal{B}$ of b k-subsets (blocks) of V, such that each element of V occurs in precisely r blocks, for some positive integers v, b, r, k. If $k < v$, D is said to be **incomplete**; if all the blocks of $\mathcal{B}$ are distinct, D is said to be **simple**. If every t-subset of V occurs in precisely λ_t blocks of $\mathcal{B}$, then D is a **t-design** with parameters $t-(v,k,\lambda_t)$. Throughout this paper, only simple incomplete t-designs are considered.

If $t = 2$, then the design is said to be **balanced**. Fisher's inequality states that for any balanced incomplete block design (BIBD) $b \geq v$. When equality holds, the design is said to be **symmetric**. For $d \geq 2$, let $D_d = (V_d, \mathcal{B}_d)$ be the symmetric BIBD with parameters $2-(2^{d+1}-1, 2^d-1, 2^{d-1}-1)$ formed from the points and hyperplanes of the **projective space** $PG(d,2)$. These designs are a subfamily of the family of **Hadamard** designs with parameters $2-(4q-1, 2q-1, q-1)$. Also, D_d is a **cyclic** design (see for instance Street and Street [11, page 184]).

Definition 1.1 *Let T_1 be a collection of m blocks of a design D. If there exists a collection T_2 of m k-subsets of V such that T_1 and T_2 contain precisely the same*

*Research supported by Australian Research Council Large Grant A49532477

t-subsets, then T_1 and T_2 are said to be **mutually t-balanced**. *If T_1 and T_2 are disjoint then $T = (T_1, T_2)$ is a (v, k, t)* **trade** *of* **volume** *m. The* **foundation** *of the trade, found(T), is the set of elements of V covered by T_1 or T_2. The single collection T_1 is often referred to as a trade in D.*

Example 1.2 *Let $D_2 = PG(2,2) = (V_2, \mathcal{B}_2)$ be a $2-(7,3,1)$ design, that is, $PG(2,2)$, with $V_2 = \{1,\ldots,7\}$ and $\mathcal{B}_2 = \{124, 235, 346, 457, 561, 672, 713\}$. Each of the seven collections of four blocks from $\mathcal{B}_2$, with an element of V_2 omitted, is a trade of volume four in D_2. For example, $T_1 = \{124, 156, 235, 346\}$ trades with $T_2 = \{125, 146, 234, 356\}$.*

Definition 1.3 (K. Gray [4]) *A set of blocks which is a subset of a unique t-(v, k, λ_t) design D is a* **defining set** *of that design. A defining set is* **minimal** *if it does not properly contain a defining set of D, and* **smallest** *if no defining set of D has fewer blocks.*

There is a strong relationship between defining sets and trades.

Theorem 1.4 ([4]) *Let $D = (V, \mathcal{B})$ be a simple $t-(v, k, \lambda_t)$ design and $S \subseteq \mathcal{B}$. Then S is a defining set of D if and only if $S \cap T \neq \emptyset$ for every trade $T \subseteq \mathcal{B}$.* □

Example 1.5 *In the design D_2 of Example 1.2, any set of three blocks not containing a common element is a smallest defining set of D_2. In particular, $s_2 = 3$.*

Let q be a prime or prime power of the form $q = 4h-1$. Seberry [10] has conjectured that the Hadamard design H cyclically generated from the starter block consisting of the quadratic residues in $GF[q]$ contains a defining set of $2h-1$ blocks; in particular, fewer than half the blocks of H are contained in a smallest defining set. In contrast to Seberry's conjecture, it is shown in this paper that the proportion of blocks in a smallest defining set of the cyclic Hadamard design D_d approaches 1 as $d \to \infty$. This is the first known asymptotic result for the size of a smallest defining set.

2 Asymptotic results for smallest defining sets of designs associated with $PG(d, 2)$

K. Gray [5] showed that the cardinality s of a smallest defining set of a symmetric $2-(v, k, \lambda)$ design D satisfies

$$s \geq \frac{2(v-1)}{k+1}.$$

If in addition, $D = (V, \mathcal{B})$ is a cyclic design, an independent lower bound can be given. The block with x added modulo v to the elements of block B will be denoted $B + x$. Similar notation will also be used to describe sets of blocks.

Theorem 2.1 *Suppose $D = (V, \mathcal{B})$ is a cyclic symmetric $2-(v,k,\lambda)$ design and $T \subseteq \mathcal{B}$ is a trade of volume m. If m does not divide v, then the cardinality s of a smallest defining set of D satisfies*

$$s \geq \frac{v}{m}.$$

Proof. Suppose that $V = \{1, \ldots, v\}$ and $\mathcal{B} = \{B + x \mid x \in V\}$ for some starter block $B \in \mathcal{B}$. If $T \subseteq \mathcal{B}$ is a trade of volume m, then so also is $T + x$ for each $x \in V$. Moreover, if m does not divide v, then there are v distinct trades of the form $T + x \subseteq \mathcal{B}$. Each block of $\mathcal{B}$ is in precisely m of these trades, so by Theorem 1.4, $s \geq v/m$. □

Let S_d be a smallest defining set of design D_d and let $R_d = \mathcal{B}_d \setminus S_d$, $s_d = |S_d|$ and $r_d = |R_d|$. K. Gray's bound implies that $s_d \geq 4$ for $d > 2$. However, it will be shown in Corollary 2.4 that D_d always contains a trade of volume four. As D_d is cyclic, $s_d \geq (2^{d+1} - 1)/4$ by Theorem 2.1. In this section we will improve the lower bound for s_d even further, eventually showing that $s_d \geq 2^{d+1} - 2^{(d/2)+1} - 2$.

To avoid any confusion between vector space and projective dimensions, we shall only refer to the **vector space dimension** of subspaces of $PG(d, 2)$. So for example, the dimension of $PG(d, 2)$ is $d+1$, and d-subspaces of $PG(d, 2)$ are hyperplanes.

It is well known that for each $(d-1)$-subspace Π of $PG(d, 2)$, there exist precisely three distinct blocks (hyperplanes) $B_1, B_2, B_3 \in \mathcal{B}_d$ containing Π. For three such blocks containing a common $(d-1)$-subspace, define the function $\circ$ by $B_1 \circ B_2 = B_3$; so $B_1 \circ B_3 = B_2$ and $B_2 \circ B_3 = B_1$ also. $B_i \circ B_i, i = 1, 2, 3$, is undefined.

Notation: Let $S = \{S_i \mid i = 0, 1, \ldots m\}$ be a collection of mutually disjoint sets. The notation $B = S_0 S_1 \ldots S_m$ is used to represent the block B if $B = S_0 \cup S_1 \ldots \cup S_m$. There should be no confusion with the notation S_d for a smallest defining set of D_d.

Lemma 2.2 (B. Gray [3]) *Distinct blocks $B_1, B_2, B_3, B_4 \in \mathcal{B}_d$ comprise a trade of volume four if and only if $B_1 \circ B_2 = B_3 \circ B_4$. Moreover, B_1, B_2, B_3, B_4 have structure*

$$B_1 = S_0 S_1 S_3 S_5, \quad B_2 = S_0 S_1 S_4 S_6, \quad B_3 = S_0 S_2 S_4 S_5, \quad B_4 = S_0 S_2 S_3 S_6,$$

where $S_i \cap S_j = \emptyset$ when $i \neq j$, and S_0 and $S_0 \cup S_i$ $(i \neq 0)$ are $(d-2)$- and $(d-1)$-subspaces of $PG(d, 2)$ respectively. □

Example 2.3 *In the design D_2, $124 \circ 156 = 235 \circ 346 = 457 \circ 267 = 137$.*

Lemma 2.2 implies the following two simple but useful results. The first corollary relates the structure of trades of volume four in D_d to the $(d-2)$-subspaces of $PG(d, 2)$.

Corollary 2.4 *Any set of five distinct blocks in $\mathcal{B}_d$ that have a common $(d-2)$-subspace contains a trade of volume four. The blocks of a trade of volume four in D_d contain a common $(d-2)$-subspace.* □

Corollary 2.5 *Suppose blocks $B_1, B_2, B_3, B_4 \in \mathcal{B}_d$ where these blocks are not necessarily distinct. Then B_1, B_2, B_3, B_4 comprise a trade of volume four if and only if $B_1 \circ B_2 = B_3 \circ B_4$ and $\{B_1, B_2\} \neq \{B_3, B_4\}$.* □

Theorem 2.6 *For $d \geq 2$, $s_d \geq 2^{d+1} - 2^{(d/2)+1} - 2$.*

Proof. If $\{B_1, B_2\}$ and $\{B_3, B_4\}$ are distinct pairs of blocks in R_d, then $B_1 \circ B_2 \neq B_3 \circ B_4$ or else B_1, B_2, B_3, B_4 comprise a trade of volume four by Corollary 2.5. Thus r_d satisfies the inequality

$$\binom{r_d}{2} \leq 2^{d+1} - 1. \tag{1}$$

Completing the square yields

$$(r_d - \frac{1}{2})^2 \leq 2^{d+2} - 2 + \frac{1}{4} = 2^{d+2} - \frac{7}{4}.$$

This implies

$$r_d \leq \frac{(2^{d+4} - 7)^{1/2}}{2} + \frac{1}{2} \leq \frac{2^{(d/2)+2}}{2} + 1 = 2^{(d/2)+1} + 1 \text{ for } d \geq 2.$$

But $s_d = 2^{d+1} - 1 - r_d$, and the result follows. □

Corollary 2.7 *Let μ_d be the proportion of blocks in the smallest defining set of D_d. Then $\mu_d \to 1$ as $d \to \infty$.*

Proof. By Theorem 2.6,

$$\mu_d = \frac{s_d}{|\mathcal{B}_d|} = 1 - \frac{r_d}{|\mathcal{B}_d|} \geq 1 - \frac{2^{(d/2)+1} + 1}{2^{d+1} - 1} \to 1 \text{ as } d \to \infty.$$ □

Let B be a fixed block in $\mathcal{B}_d$ and define $B_i^* = B_i \setminus B$ for each $B_i \in \mathcal{B}_d$ other than B. Let $\mathcal{B}_d^*$ equal the collection of blocks B_i^*. The design $D_d^* = (V_d \setminus B, \mathcal{B}_d^*)$ is called the **residual design** (see [11]) of D_d with respect to block B. D_d^* has parameters $2 - (2^d, 2^{d-1}, 2^{d-1} - 1)$. The design D_d^* consists of the points and hyperplanes of the **affine space** $AG(d, 2)$ (Hirschfeld [7, page 37]). We say blocks $B_i^*, B_j^* \in \mathcal{B}_d^*$ are a **special pair** if $B_i \circ B_j = B$.

What can be said about trades of volume four in D_d^*?

Lemma 2.8 *Let D_d^* be the residual design of D_d with respect to the fixed block $B \in \mathcal{B}_d$. Suppose that $B_1, B_2, B_3, B_4 \neq B \in \mathcal{B}_d$ comprise a trade of volume four in D_d and B_i^*, B_j^* are not a special pair for $i, j \in \{1, 2, 3, 4\}$. Then $B_1^*, B_2^*, B_3^*, B_4^* \in \mathcal{B}_d^*$ comprise a trade of volume four in D_d^*.*

Proof. By Lemma 2.2, the blocks B_1, B_2, B_3, B_4 have structure

$$B_1 = S_0S_1S_3S_5, \quad B_2 = S_0S_1S_4S_6, \quad B_3 = S_0S_2S_4S_5, \quad B_4 = S_0S_2S_3S_6,$$

where $S_i \cap S_j = \emptyset$ when $i \neq j$. Also, S_0 and $S_0 \cup S_i$ $(i \neq 0)$ are $(d-2)$-and $(d-1)$-subspaces of $PG(d,2)$ respectively. By Hwang's characterisation of basic trades in [8], $B_1^*, B_2^*, B_3^*, B_4^*$ comprise a trade of volume four if B does not contain S_k for some $k \in \{1,\ldots,6\}$. But if B contains S_k for some k, then B contains $S_0 \cup S_k$ as the vector space closure of S_k is $S_0 \cup S_k$. Thus $B_i \circ B_j = B$ for some $i,j \in \{1,2,3,4\}$. But by hypothesis B_i^*,B_j^* are not a special pair. This completes the proof. □

Let S_d^* be a smallest defining set of D_d^*, $R_d^* = \mathcal{B}_d^* \setminus S_d^*$, $s_d^* = |S_d^*|$ and $r_d^* = |R_d^*|$. Lemma 2.8 can be used to give a result similar to Theorem 2.6 for the smallest defining sets of D_d^*.

Theorem 2.9 *For $d \geq 3$, $s_d^* \geq 2^{d+1} - 2^{(d/2)+2} - 4$.*

Proof. Let l be the number of disjoint special pairs with at least one member in R_d^*, so $2l \geq r_d^*$. Choose one block from each of the pairs represented in R_d^* to form the set L. Then $|L| = l$ and by Lemma 2.8,

$$\binom{l}{2} \leq 2^{d+1} - 2.$$

After completing the square,

$$l \leq \frac{(2^{d+4} - 15)^{1/2}}{2} + \frac{1}{2} \leq 2^{(d/2)+1} + 1 \quad \text{for } d \geq 3\,.$$

But $s_d^* = 2^{d+1} - 2 - r_d^* \geq 2^{d+1} - 2 - 2l \geq 2^{d+1} - 2^{(d/2)+2} - 4$. □

Corollary 2.10 *Let μ_d^* be the proportion of blocks in the smallest defining set of D_d^*. Then $\mu_d^* \to 1$ as $d \to \infty$.*

Proof. By Theorem 2.9, for $d \geq 3$,

$$\mu_d^* = \frac{s_d^*}{|\mathcal{B}_d^*|} = 1 - \frac{r_d^*}{|\mathcal{B}_d^*|} \geq 1 - \frac{2^{(d/2)+2} + 2}{2^{d+1} - 2} \to 1 \text{ as } d \to \infty.$$ □

Let L_d denote the $2 - (2^{d+1} - 1, 3, 1)$ design formed from the points and lines of $PG(d,2)$. Let a_d equal the size of a smallest defining set of L_d and $\eta_d = 6a_d/(2^{d+1} - 1)(2^{d+1} - 2)$; so η_d is the proportion of the total number of blocks in a smallest defining set of L_d. It is now shown that the sequence $\{\eta_d\}_{d=2}^{\infty}$ also converges to a limit.

Lemma 2.11 ([4]) *Suppose that D' is a subdesign of D. If S is a defining set of D, then S contains a defining set of D'.* □

Theorem 2.12 *The sequence* $\{\eta_d\}_{d=2}^{\infty}$ *is non-decreasing and bounded above by* 1. *Thus it converges.*

Proof. For $d > 2$, L_d contains $(2^{d+1} - 1)$ L_{d-1} subdesigns. Moreover, each block of L_d is contained in $(2^{d-1} - 1)$ L_{d-1} subdesigns. Thus, by Lemma 2.11

$$a_d \geq \frac{a_{d-1}(2^{d+1} - 1)}{(2^{d-1} - 1)}.$$

This implies that

$$\eta_d = \frac{6a_d}{(2^{d+1} - 1)(2^{d+1} - 2)} \geq \frac{6a_{d-1}}{(2^d - 1)(2^d - 2)} = \eta_{d-1}. \qquad \square$$

Moran [9] has shown that $\eta_3 = 16/35$ and Gower [2] has found a family of minimal defining sets of L_d. However, the limiting value for η_d is unknown to the author.

3 Smallest defining sets of D_3, D_4 and D_5

In this section, we first extend the counting argument of Theorem 2.6 to determine the size and structure of smallest defining sets of D_3 and D_4. Then we determine bounds on the size of a smallest defining set of D_5.

Lemma 3.1 *Suppose* $A \circ B = C$ *and* $D \circ E = F$, *and* $A, B, C, D, E, F \in R_d$. *Then, either* $\{A, B, C\} = \{D, E, F\}$ *or* $\{A, B, C\} \cap \{D, E, F\} = \emptyset$.

Proof. The only case to consider is $|\{A, B, C\} \cap \{D, E, F\}| = 1$. Without loss of generality, suppose that $A = D$. Then $B \circ C = A = E \circ F$ and so by Corollary 2.5, $B, C, E, F \in R_d$ comprise a trade of volume four. This is a contradiction. $\square$

Let j_d equal the number of triples of blocks $\{A, B, C\} \subseteq R_d$ with $A \circ B = C$.

Lemma 3.2 *In* D_d, $3j_d \leq r_d$ *and*

$$\binom{r_d}{2} - 3j_d \leq 2^{d+1} - 1 - r_d. \tag{2}$$

Proof. That $3j_d \leq r_d$ is an immediate consequence of Lemma 3.1. The left hand side of inequality (2) is the number of distinct blocks $X \circ Y \notin R_d$ for $X, Y \in R_d$, and the inequality follows. $\square$

Lemma 3.3 *There is no defining set of* D_3 *consisting of eight blocks.*

Proof. By inequality (1), $r_3 \leq 6$ and thus $s_3 \geq 9$. $\square$

Theorem 3.4 was obtained by K. Gray and Street [6] by directly considering $(d-1)$-subspaces (special triples) of D_3. An alternative approach is presented.

Theorem 3.4 *The smallest defining sets of D_3 are precisely the sets of nine blocks obtained by deleting two disjoint sets of three blocks $\{A, B, C\}$ and $\{D, E, F\}$ where $A \circ B = C$, $D \circ E = F$ and $A \cap B \cap C \cap D \cap E \cap F = \emptyset$.*

Proof. By Lemma 3.3, there is no defining set of D_3 consisting of eight blocks. We now attempt to find a smallest defining set of D_3 consisting of nine blocks and thus assume that $r_3 = 6$. Solving inequality (2) yields $j_3 \geq 2$. But $3j_3 \leq 6$ by Lemma 3.2 and thus $j_3 = 2$. Hence let $R_3 = \{A, B, C, D, E, F\}$ where $A \circ B = C$ and $D \circ E = F$. That $A \cap B \cap C \cap D \cap E \cap F = \emptyset$, and that R_3 does not contain a trade of volume four are both consequences of Corollary 2.4. It is then simple to show that R_3 does not comprise a trade of volume six [6]. Hence we have found a collection $S_3 = \mathcal{B}_3 \setminus R_3$ which is a smallest defining set of D_3 consisting of nine blocks. Moreover, we have demonstrated that such a collection S_3 is unique up to isomorphism with structure as claimed. □

Theorem 3.5 *There is no defining set of D_4 consisting of 23 blocks, that is, $r_4 < 8$.*

Proof. By inequality (1), $r_4 \leq 8$, and if $r_4 = 8$, then $j_4 = 2$ by Lemma 3.2. Thus suppose $X = \{A, B, C, D, E, F\}$ is a collection of six distinct blocks contained in R_4 with $A \circ B = C$ and $D \circ E = F$. $A \cap B \cap C$ is a subspace of $PG(4, 2)$ of dimension three. By the intersection theorem for finite subspaces,

$$dim(A \cap B \cap C) + dim(D \cap E \cap F) - dim(A \cap B \cap C \cap D \cap E \cap F) \leq dim(D_4) = 5.$$

Therefore $1 \leq dim(A \cap B \cap C \cap D \cap E \cap F) \leq 2$ and by Corollary 2.4 this dimension must equal one. Thus the blocks A, B, C, D, E, F contain precisely one common point s, say. The $\binom{6}{2} = 15$ blocks $X_1 \circ X_2$, $X_i \in X$, are distinct by Corollary 2.5 and each contains the element s. Thus nine blocks containing s are excluded from R_4. There are 16 blocks in D_4 which do not contain the element s. At most one of these blocks can belong to R_4. For suppose two of these blocks belong to R_4, call them G and H say. Now $s \in G \circ H$. Thus, either $G \circ H = X_1$ or $G \circ H = X_1 \circ X_2$, where $X_1, X_2 \in X \subset R_4$; either way we obtain a contradiction, for if $G \circ H = X_1$ then $j_4 > 2$ and $G \circ H \neq X_1 \circ X_2$ by Corollary 2.5. Thus at least $9 + 15 = 24$ blocks belong to S_4 which completes the proof. □

To simplify the construction of smallest defining sets of D_4 the following lemmata are helpful.

Lemma 3.6 *Let T be a trade of volume m and $e \in found(T)$. Then the number of occurrences of e in the blocks of T is not equal to 1 or $m - 1$.*

Proof. This is immediate from Definition 1.1. □

The following lemma has been proven independently by Billington and Hoffman in [1].

Lemma 3.7 *Suppose $k > 2$ and $T = (T_1, T_2)$ is a $(v, k, 2)$ trade such that any pair of elements occurs at most once in the blocks of T_1. Then the volume of T is at least $2(k-1)$.*

Proof. Let r_e equal the number of occurrences of the element e in the blocks of T_1. It is simple to show that either $r_x = 2$ for some $x \in found(T)$ or the volume of T is greater than $2(k-1)$. Let $B_1 = xa_1 \dots a_{k-1}$ and $B_2 = xb_1 \dots b_{k-1}$ represent the two distinct blocks in T_1 containing the element x where $r_x = 2$. Let B_1^* and B_2^* represent the two distinct blocks in T_2 also containing x. As T_1 and T_2 are 2−balanced, each of $a_1, \dots, a_{k-1}, b_1, \dots, b_{k-1}$ is contained in precisely one of B_1^*, B_2^*. Let $j_a = |B_1 \cap B_1^* \setminus \{x\}|$, so $1 \leq j_a \leq k-2$. Without loss of generality,

$$B_1^* = xa_1 \dots a_{j_a} b_1 \dots b_{j_b}, B_2^* = xa_{j_a+1} \dots a_{k-1} b_{j_b+1} \dots b_{k-1},$$

where $j_a + j_b = k-1$ and $j_a, j_b \geq 1$. Note that the minimum of the product $j_a j_b$ occurs when $\{j_a, j_b\} = \{1, k-2\}$.

Let $i_1 \in \{1, \dots, j_a\}, i_2 \in \{1, \dots j_b\}, i_3 \in \{j_a+1, \dots, k-1\}, i_4 \in \{j_b+1, \dots, k-1\}$. The pairs $\{a_{i_1}, b_{i_2}\}$ and $\{a_{i_3}, b_{i_4}\}$ occur in T_2 and thus must also occur in T_1. Moreover, each of these pairs must occur in a separate block of T_1. This implies the volume of T is at least $2 + j_a j_b + (k-1-j_a)(k-1-j_b) = 2 + 2j_a j_b \geq 2(k-1)$, with equality if and only if $\{j_a, j_b\} = \{1, k-2\}$. □

Recall that $D_4 = PG(4,2)$ is cyclic. Let $D_4 = (V_4, \mathcal{B}_4)$ where $V_4 = \{1, \dots, 31\}$ and starter block $B = \{1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30\}$ ([11, page 191]) whence $\mathcal{B}_4 = \{B + x \mid x = 1, \dots, 31\}$. D_4 has parameters $2-(31, 15, 7)$. Let block $B+x$ be denoted by B_x; so for example, $B_2 = \{3,4,5,6,8,10,14,17,18,19,25,26,29,31,1\}$ and $B_{31} = B$.

Theorem 3.8 *The smallest defining sets S_4 of D_4 consist of 24 blocks and R_4 is isomorphic to one of the following sets of seven blocks: $R_4^1 = \{B_{25}, B_{26}, B_{27}, B_{28}, B_{29}, B_{30}, B_{31}\}$, or $R_4^2 = \{B_{23}, B_{24}, B_{26}, B_{27}, B_{29}, B_{30}, B_{31}\}$.*

Proof.

(a) $S_4^1 = \mathcal{B}_4 \setminus R_4^1$ and $S_4^2 = \mathcal{B}_4 \setminus R_4^2$ are defining sets of D_4.

(i) R_4^1 and R_4^2 do not contain a trade of volume four.

By Corollary 2.5, it suffices to check that there do not exist four distinct blocks $A, B, C, D \in R_4^i$ such that $A \circ B = C \circ D$. This is demonstrated in Table 1 and Table 2.

(ii) R_4^1 and R_4^2 do not contain a trade of volume seven or six.

R_4^1 is not a trade of volume seven by Lemma 3.6 as the element 29 occurs in all blocks of R_4^1 except B_{29}. Similarly, the only possible trade of volume six contained in R_4^1 is $R_4^1 \setminus B_{29}$. However, these six blocks contain the common element 29 and it is easily verified that they are structurally isomorphic to the

set R_3 of Theorem 3.4. Thus R_4^1 does not contain a trade of volume seven or six.

R_4^2 is not a trade of volume seven by Lemma 3.6 as the element 18 occurs in R_4^2 only in block B_{26}. Again, the only possible trade of volume six contained in R_4^2 is $R_4^2 \setminus B_{26} = Z$, say. The 30 elements other than 18 occurring in $found(Z)$ can be matched into complementary pairs; that is, for any element contained in precisely two blocks of Z, there exists exactly one element contained in precisely four different blocks of Z. For example, the element 9 is contained in the blocks B_{23} and B_{24} whilst the element 2 is contained in B_{27}, B_{29}, B_{30} and B_{31}. Let Z' be the set of six blocks of size five formed from Z by deleting all elements contained in Z precisely four times. It follows that Z is a trade only if Z' is a trade. However, Z' is not a trade by Lemma 3.7. Thus R_4^2 does not contain a trade of volume seven or six.

As R_4^1 and R_4^2 do not contain a trade, S_4^1 and S_4^2 are defining sets of D_4.

(b) By Theorem 3.5, S_4^1 and S_4^2 are smallest defining sets of D_4.

(c) S_1^4 and S_2^4 are the only smallest defining sets of D_4 (up to isomorphism).
There are three cases to consider depending on the value of j_4.

(i) $r_4 = 7$ and $j_4 = 2$.
From the proof of Theorem 3.5, it is clear that R_4 must be isomorphic to the collection R_4^1.

(ii) $r_4 = 7$ and $j_4 = 1$.
It is shown that is impossible to construct a set R_4 satisfying these equations such that $S_4 = \mathcal{B}_4 \setminus R_4$ is a defining set of D_4 unless $R_4 = R_4^2$. Without loss of generality let blocks containing a common $(d-1)$-subspace in R_4 be B_{24}, B_{26} and B_{29}. The next two blocks chosen must not contain a common $(d-2)$-subspace with B_{24}, B_{26} and B_{29} and thus without loss of generality choose blocks B_{23} and B_{27}. These five blocks contain the common element 25. There are two cases to consider:
Case 1: A block containing the element 25 is added to R_4.
The only block containing 25 that does not force a trade of volume four is $B_{23} \circ B_{27}$ but then $j_4 = 2$.
Case 2: A block not containing the element 25 is added to R_4.
Again, without loss of generality, choose first the block B_{30}. The one remaining choice for a block that does not contain 25 and does not force a trade of volume four is B_{31}. Thus $R_4 = R_4^2$.

(iii) $r_4 = 7$ and $j_4 = 0$.
If an element $s \in A \cap B$, then $s \in A \circ B$. Similarly, if $s \notin A \cup B$, then $s \in A \circ B$. Let n be the number of times s occurs in the blocks of R_4. By Corollary 2.5. and also because $j_4 = 0$, the number of distinct blocks containing s is at least $n + \binom{n}{2} + \binom{7-n}{2} = n'$, say. The inequality $n' \leq 15$ yields $n \in \{2, 3, 4\}$. Let n_i equal the number of elements that occur in R_4 i times. Clearly

$$n_2 + n_3 + n_4 = 31. \tag{3}$$

$\circ$	B_{25}	B_{26}	B_{27}	B_{28}	B_{29}	B_{30}	B_{31}
B_{25}	$-$	B_{12}	B_{30}	B_{23}	B_4	B_{27}	B_{21}
B_{26}		$-$	B_{13}	B_{31}	B_{24}	B_5	B_{28}
B_{27}			$-$	B_{14}	B_1	B_{25}	B_6
B_{28}				$-$	B_{15}	B_2	B_{26}
B_{29}					$-$	B_{16}	B_3
B_{30}						$-$	B_{17}
B_{31}							$-$

Table 1: Circle product of blocks in R_4^1

$\circ$	B_{23}	B_{24}	B_{26}	B_{27}	B_{29}	B_{30}	B_{31}
B_{23}	$-$	B_{10}	B_{21}	B_2	B_{19}	B_{14}	B_{12}
B_{24}		$-$	B_{29}	B_{22}	B_{26}	B_{20}	B_{15}
B_{26}			$-$	B_{13}	B_{24}	B_5	B_{28}
B_{27}				$-$	B_1	B_{25}	B_6
B_{29}					$-$	B_{16}	B_3
B_{30}						$-$	B_{17}
B_{31}							$-$

Table 2: Circle product of blocks in R_4^2

Similarly, by counting the total number of elements in R_4 and the total block intersection sizes of R_4, the following standard equations can be obtained.

$$2n_2 + 3n_3 + 4n_4 = 105 = 7.15 , \tag{4}$$

$$n_2\binom{2}{2} + n_3\binom{3}{2} + n_4\binom{4}{2} = 147 = 7.\binom{7}{2}. \tag{5}$$

Solving Equations (3), (4) and (5) yields the solution $n_2 = 18, n_3 = -17, n_4 = 30$ which is clearly impossible. Thus there is no defining set S_4 with $j_4 = 0$. □

It has been shown in Section 2 that the number of blocks s_d in a smallest defining set of D_d is increasing. A similar result also holds for the number of blocks r_d not in a smallest defining set of D_d.

Theorem 3.9 *The sequence* $\{r_d\}_{d=2}^{\infty}$ *is strictly increasing.*

Proof. We now show how to construct a set $X \subset \mathcal{B}_{d+1}$ from R_d such that X does not contain a trade and $|X| = r_d + 1$. R_d is structurally isomorphic to a collection of blocks X', say, in $\mathcal{B}_{d+1}$ that contain a common element e say (see [7], page 65). Let $B \in \mathcal{B}_{d+1} \setminus X'$ and $e \notin B$. We claim that $X = B \cup X'$ is one possible construction. Certainly X' does not contain a trade as it is structurally isomorphic to R_d which does not contain a trade. Thus any trade $T \subseteq X$ must contain block B in which case the element e occurs in all blocks of T except B contradicting Lemma 3.6. Thus X

does not contain a trade. Now $r_{d+1} \geq |X| > r_d$ and the sequence $\{r_d\}_{d=2}^{\infty}$ is strictly increasing. □

Theorem 3.10 *The size s_5 of a smallest defining set of D_5 satisfies $52 \leq s_5 \leq 55$.*

Proof. By Theorem 3.9, $r_5 \geq r_4 + 1 = 8$. By inequality (1),

$$\binom{r_5}{2} \leq 63$$

which implies that $r_5 \leq 11$. These results together with the fact that $s_5 = 63 - r_5$ yields the inequality $52 \leq s_5 \leq 55$. □

Acknowledgements I would like to thank an anonymous referee for improving the clarity of this paper and Professor Anne Penfold Street for providing financial assistance which enabled me to present these results at the Twenty-Second Australasian Conference on Combinatorial Mathematics and Combinatorial Computing held at the University of Technology, Sydney in July 1996.

References

[1] Elizabeth J. Billington and D.G. Hoffman, *Trades and Graphs*, submitted for publication.

[2] Rebecca A. H. Gower, *Minimal defining sets in a family of Steiner triple systems*, Australasian Journal of Combinatorics **8** (1993), 55-73.

[3] Brenton D. Gray, *The maximum number of trades of volume four in a symmetric design*, Utilitas Mathematica (to appear).

[4] Ken Gray, *On the minimum number of blocks defining a design*, Bulletin of the Australian Mathematical Society **41** (1990), 97-112.

[5] Ken Gray, *Defining sets of single-transposition-free designs*, Utilitas Mathematica **38** (1990), 97-103.

[6] Ken Gray and Anne Penfold Street, *Smallest defining sets of the* $2-(15,7,3)$ *design associated with* $PG(3,2)$*: a theoretical approach*, Bulletin of the Institute of Combinatorics and its Applications **11** (1994), 77-83.

[7] J. W. P. Hirschfeld, *"Projective geometries over finite fields"*, Oxford University Press, Oxford, 1979.

[8] H.L. Hwang, *On the structure of* (v,k,t) *trades*, Journal of Statistical Planning and Inference **13** (1986), 179-191.

[9] Anthony T. Moran, *Block designs and their defining sets*, Phd Thesis, The University of Queensland, 1997.

[10] Jennifer Seberry, *On small defining sets for some* $SBIBD(4t-1, 2t-1, t-1)$, Bulletin of the Institute of Combinatorics and its Applications **4** (1992), 58-62; *corrigendum* **6** (1992), 62.

[11] Anne Penfold Street and Deborah J. Street, *"Combinatorics of Experimental Design"*, Clarendon Press, Oxford 1987.

(Received 22/4/96; revised 5/11/96)