# **Tactical Decompositions of Steiner Systems and Orbits of Projective Groups**

KELDON DRUDGE

Queen Mary and Westfield College, School of Mathematical Science, London EI 4NS, UK

Received March 24, 1999; Revised August 16, 1999

**Abstract.** Block's lemma states that the numbers *m* of point-classes and *n* of block-classes in a tactical decomposition of a 2- $(v, k, \lambda)$  design with *b* blocks satisfy  $m \le n \le m + b - v$ . We present a strengthening of the upper bound for the case of Steiner systems (2-designs with  $\lambda = 1$ ), together with results concerning the structure of the block-classes in both extreme cases. Applying the results to the Steiner systems of points and lines of projective space PG(N, q), we obtain a complete classification of the groups inducing decompositions satisfying the upper bound; answering the analog of a question raised by Cameron and Liebler (P.J. Cameron and R.A. Liebler, *Lin. Alg. Appl.* **46** (1982), 91–102) (and still open).

Keywords: tactical decompositions, partial spread, tightset, Steiner systems, projective group

#### 1. Introduction

The notion of tactical decomposition of an incidence geometry is the natural combinatorial generalisation of the notion of an automorphism group, in that any automorphism group of an incidence geometry induces a tactical decomposition of it. In general, however, many more tactical decompositions than collineation groups exist for a given incidence geometry. In this paper we consider the question of which tactical decompositions of arbitrary Steiner systems (2-designs with  $\lambda = 1$ ) exist. We obtain a significant strengthening of Block's lemma for this case, along with a characterisation of the cases achieving equality. Applying this result to the case of finite projective spaces, we give a characterisation of the groups which occur in the extremal case, answering the natural analog of a question raised by Cameron and Liebler in [2].

#### 2. Tactical decompositions of Steiner systems

Let  $\mathcal{D} = (\mathcal{V}, \mathcal{B})$  be a 2- $(v, k, \lambda)$  design with *r* blocks on each point and *b* blocks. A *tactical decomposition* of  $\mathcal{D}$  consists of partitions  $\mathbb{V} = \{\mathcal{V}_1, \ldots, \mathcal{V}_m\}$  of  $\mathcal{V}$  and  $\mathbb{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_n\}$  of  $\mathcal{B}$  with the property that for each *i*, *j*,  $1 \le i \le m$ ,  $1 \le j \le n$ , the incidence structure with point-set  $\mathcal{V}_i$  and blocks, the intersections of blocks of  $\mathcal{B}_j$  with  $\mathcal{V}_i$  is a tactical configuration (that is, each point of  $\mathcal{V}_i$  is on the same number of blocks of  $\mathcal{B}_j$ , and each block of  $\mathcal{B}_j$  contains

Research supported by an N.S.E.R.C. of Canada post-doctoral fellowship.

the same number of points of  $\mathcal{V}_i$ ). As was mentioned in the introduction, any automorphism group G of  $\mathcal{D}$  induces such a decomposition, with partitions the various orbits of G on  $\mathcal{V}$ and  $\beta$ . A natural question to ask concerning tactical decompositions is, for what values of *m* and *n* can they occur? An answer is supplied by *Block's lemma* (see [3]), which states that  $m \leq n \leq m + b - v$  (the trivial decomposition of  $\mathcal{D}$ , with just one point- and one line-class, shows  $b \ge v$ , and thus Block's lemma is a generalisation of Fisher's inequality). Moreover, the result is sharp in the sense that there exist decompositions satisfying both the upper and lower bounds: the aforementioned trivial decomposition gives an example for the lower bound, and the decomposition with all point- and line-classes singletons, gives an example satisfying the upper bound. Furthermore, other decompositions with m = n(symmetric tactical decompositions) of arbitrary designs exist, for example the punctured decomposition with point classes  $\{V\}$  and  $\mathcal{V}\setminus\{V\}$  and block classes (V) and  $\mathcal{B}\setminus\{(V)\}$  for  $V \in \mathcal{V}$  (here and elsewhere, (V) denotes the set of blocks containing  $V \in \mathcal{V}$ ). However, there appear to be no other 'obvious' examples of decompositions satisfying the upper bound, and thus the question of sharpening this bound arises. (The question of classifying the decompositions satisfying the lower bound is very difficult even in specific cases—see [2].) We do this here in the case of Steiner systems, that is 2-designs with  $\lambda = 1$ . Since all decompositions of symmetric designs are symmetric, we may assume that  $\mathcal{D}$  is not symmetric, that is, that b > v.

To any tactical decomposition  $(\mathbb{V}, \mathbb{B})$  of  $(\mathcal{V}, \mathcal{B})$ , there exist two associated  $m \times n$  integral matrices,  $A = (a_{ij})$  and  $B = (b_{ij})$ , where  $a_{ij} = |\mathcal{V}_i \cap l|$  for  $l \in \mathcal{B}_j$  and  $b_{ij} = |(\mathcal{V}) \cap \mathcal{B}_j|$  for  $\mathcal{V} \in \mathcal{V}_i$ . Since  $\mathcal{D}$  is a design, these matrices both have rank m (see [3]). Thus the  $n \times n$  product  $H = B^t A$  also has rank m. Put  $H = (h_{cd})$ .

**Lemma 2.1** The entries of *H* have the following interpretation:  $h_{cd}$  is the number of triples (m, V, l) where  $m \in \mathcal{B}_c$  and  $V \in m \cap l$  for a specific  $l \in \mathcal{B}_d$ .

We omit the proof of this lemma, since it is a similar (but simpler) argument to the one which proves Lemma 2.3 below.

**Lemma 2.2** We have  $trace(H) \ge nk$ , with equality if and only if each element of  $\mathbb{B}$  is a set of pairwise skew blocks.

**Proof:** We simply note that if c = d, exactly k triples (l, V, l) occur, one for each  $V \in l$ , and therefore the previous lemma implies that  $h_{cc} \ge k$ , with equality if and only if each block of  $\mathcal{B}_c \setminus \{l\}$  is skew to l. Since the decomposition is tactical, this is independent of choice of  $l \in \mathcal{B}_c$ , and since this holds for each  $c, 1 \le c \le n$ , the result follows.  $\Box$ 

We also note that, since  $\mathcal{D}$  is a Steiner system,  $h_{cd}$  is just the number of blocks of  $\mathcal{B}_c$ which intersect a given block of  $\mathcal{B}_d$  when  $c \neq d$ . This implies that for all  $c, d, |\mathcal{B}_d|h_{cd}$ is the number of intersections of lines of  $\mathcal{B}_c$  with lines of  $\mathcal{B}_d$  (if c = d, each line of  $\mathcal{B}_c$  is interpreted as intersecting itself k times); therefore we have

$$\sum_{i=1}^{n} |\mathcal{B}_i| h_{ci} = |\mathcal{B}_c| kr,$$

so *kr* is an eigenvalue of *H* with eigenvector  $(|\mathcal{B}_1|, \ldots, |\mathcal{B}_n|)^t$ . To find the other eigenvalues of *H*, we make use of the following lemma.

**Lemma 2.3** The matrix H satisfies  $H^2 = (r-1)H + kM$ , where  $M = (m_{cd})$  has  $m_{cd} = |\mathcal{B}_c|$ .

**Proof:** Lemma 2.1 above, together with a simple count, shows that  $h_{ci}h_{id}$  is the number of quintuples (n, W, m, V, l) where  $W \in n \cap m$ ,  $V \in m \cap l$ , for arbitrary  $n \in \mathcal{B}_c$ ,  $m \in \mathcal{B}_i$  and a fixed  $l \in \mathcal{B}_d$ . Therefore the (c, d)-entry of  $H^2$  is the number of such quintuples where now m is an arbitrary block of  $\mathcal{D}$ . Since  $\mathcal{D}$  is a Steiner system, the number of such quintuples can be counted, as follows. For any  $n \in \mathcal{B}_c$  which is skew to l, there are exactly  $k^2$  choices for m, each giving rise to exactly one quintuple. Therefore there are  $(|\mathcal{B}_c| - h_{cd})k^2$  quintuples with n skew to l if  $c \neq d$ , and  $(|\mathcal{B}_c| - 1 - (h_{cc} - k))k^2$  such if c = d. Each  $n \neq l$  which intersects l (necessarily in exactly one point) is included in exactly  $(k-1)^2$  quintuples with  $W \neq n \cap l \neq V, r-2$  quintuples with  $W = V = n \cap l$  but  $n \neq m \neq l$ , and 2k quintuples with n = m or l = m, for a total of  $k^2 + r - 1$ . Thus we have  $(k^2 + r - 1)h_{cd}$  quintuples with  $n \neq l$  intersecting l when  $c \neq d$ , and  $(k^2 + r - 1)(h_{cd} - k)$  when c = d. Finally, if c = d there is the possibility n = l, which contributes  $(r - 1)k + k^2$  quintuples. Adding the possibilities shows that in both cases, the (c, d)-entry of  $H^2$  is  $|\mathcal{B}_c|k^2 + (r - 1)h_{cd}$ , which gives the result.

Lemma 2.2 shows that a special role is played by sets of pairwise disjoint blocks. When  $\mathcal{D}$  is the design of points and lines of PG(3, q), such sets are called partial spreads. Accordingly, we define a *partial spread* of  $\mathcal{D}$  to be a set of pairwise disjoint blocks. A partial spread whose blocks partition the point-set of  $\mathcal{D}$  will be called a *spread*. One more definition will be convenient: a set S of blocks will be called *tight* if the number of blocks of S which intersect a given block  $B \in \mathcal{B}$  depends only on whether or not  $B \in S$ . The name 'tight sets' was first applied to certain subsets of generalized quadrangles by S. Payne in [8]; such sets are directly analogous to the 'Cameron-Liebler line classes' introduced in [2] (see [4]); the above definition is the natural generalisation of this result to Steiner systems, as Theorem 2.2 below shows. Before proving Theorem 2.2 we must obtain a few facts concerning tight sets in arbitrary Steiner systems.

**Theorem 2.1** Suppose that  $\mathcal{D} = (\mathcal{V}, \mathcal{B})$  is a 2-(v, k, 1) design with b blocks and r blocks on each point. If  $S_1 \subset \mathcal{B}$  is a set of s blocks of  $\mathcal{D}$ , the average number  $\delta$  of blocks of  $S_1 \setminus \{B\}$  which intersect a given block  $B \in S_1$  satisfies

$$\delta \le r - k - 1 + \frac{sk}{r}.$$

Equality is achieved if and only if  $S_1$  is a tight set.

**Proof:** If A is a block-block adjacency matrix of  $\mathcal{D}$  (with zeroes on the main diagonal), counting shows that A satisfies  $A^2 = A(r-2k-1) + k(r-k-1)I + k^2J$ , where J is the all-one matrix. Thus the eigenvalues of A are (r-1)k with multiplicity one, r-k-1 and

-k. Set  $S_2 = \mathcal{B} \setminus S_1$ . The partition  $\{S_1, S_2\}$  of  $\mathcal{B}$  induces a partition of A into four matrices  $A_{11}, A_{12}, A_{21}, A_{22}$ ; if  $\delta_{ij}$  is the average row sum of  $A_{ij}$  then  $\delta_{ij}$  is the average number of blocks of  $S_i$  which intersect a given block of  $S_j$ . Furthermore, we have  $\delta_{i2} = (r-1)k - \delta_{i1}$  for i = 1, 2, and

$$\delta_{21} = \frac{s}{b-s}((r-1)k - \delta_{11}).$$

These facts imply that the eigenvalues of the matrix  $(\delta_{ij})$  are  $\delta_{11} - \delta_{21}$  and (r - 1)k. Now Haemer's generalisation of the Higman-Sims technique (see [6]) implies that the eigenvalues of the matrix  $(\delta_{ij})$  interlace the eigenvalues of A; since  $\delta_{11} - \delta_{21} \le (r - 1)k$ , we must have  $\delta_{11} - \delta_{21} \le r - k - 1$ . The bound on  $\delta = \delta_{11}$  follows by manipulating the above equation (using the fact that vr = bk). Furthermore, equality holds in Haemer's theorem exactly when each  $A_{ij}$  has constant row sums; this is clearly equivalent to  $S_1$  being tight.

**Corollary 2.1** A set *S* of blocks is tight if and only if for each  $B \in \mathcal{B}$  there are exactly  $(r - k - 1)\chi_S(B) + sk/r$  blocks of *S* distinct from *B* which intersect *B*, where  $\chi_S$  is the characteristic function of *S*. A tight set has x(r/gcd(r, k)) elements for some integer *x*.

**Theorem 2.2** The numbers m and n of point- and block-classes of an arbitrary tactical decomposition of the Steiner system D with parameters v, k, r, b satisfies

$$m \le n \le r + \frac{(m-1)(r-1)}{k}.$$

The lower bound is satisfied if and only if all block classes are tight sets, and the upper bound is satisfied if and only if all block classes are partial spreads.

**Proof:** The previous lemma shows that *H* and *M* commute, so their eigenspaces coincide. Now *M*, having rank one, has just one non-zero eigenvalue, *b*, with eigenvector  $(|\mathcal{B}_1|, \ldots, |\mathcal{B}_n|)^t$ . As noted above, the eigenvalue of *H* for this vector is *rk*. All other eigenspaces of *H* must be in the kernel of *M*, and thus their eigenvalues  $\rho$  must satisfy  $\rho = 0$  or  $\rho = r - 1$ , by the same lemma. Since *H* has rank *m*, exactly m - 1 eigenvalues of *H* must be r - 1, while n - m are zero, so the trace of *H* is exactly rk + (m - 1)(r - 1). But the interpretation of *H* given by Lemma 2.1 implies that this trace is at least *kn*, with equality if and only if all block-classes are partial spreads.

Now if m = n, the matrix H is non-singular, and in fact H - (r - 1)I is identically zero on the kernel of M, which is the set of vectors whose entries sum to zero. This implies that all entries in a given row of H - (r - 1)I are the same, so the number of blocks of each  $\mathcal{B}_i$  which intersect a given block B depends only on whether or not  $B \in \mathcal{B}_i$ . Thus m = n implies that all block classes are tight. Conversely, if all block-classes are tight, the entries of H are given by Corollary 2.1 (but note that the diagonal entries are in fact r - 1 + sk/r, since the matrix H counts self-intersection of blocks), and it is clear in this case that H - (r - 1)I is identically zero on the kernel of M, so H has no zero eigenvalues, hence is non-singular, so m = n. Note that the decomposition with all points and lines forming singleton classes (m = v, n = b) satisfies the upper bound, and that if m < v, the upper bound is lower than the  $n \le m + b - v$  of Block's lemma. As *m* decreases, the difference between the two bounds grows.

In fact, the above proof gives a bit more information concerning the possible number of tight sets and partial spreads which can occur in arbitrary tactical decompositions, as follows.

**Corollary 2.2** Suppose that a tactical decomposition of  $\mathcal{D}$  has c block classes which are tight sets and which together contain d blocks. Then we have

$$n \leq r + \frac{(m-d-1)(r-1)}{k} - \frac{c}{r} + d.$$

**Corollary 2.3** Suppose that a tactical decomposition of D has c block classes which are partial spreads, and which together contain d blocks. Then we have

$$n \ge \frac{k}{r-1}\left(r-c+\frac{d}{r}\right) - \frac{v}{r-1} + m + c - 1.$$

#### 3. Projective spaces

In this section we consider the special case where  $\mathcal{D}$  is the set of points and lines of the N-dimensional projective space PG(N, q). Since PG(2, q) is a symmetric design, all of its decompositions satisfy m = n, and therefore we assume that  $N \ge 3$ . In [2], the problem of determining all collineation groups of PG(N, q) with the same number of point- and line-orbits was considered. This problem was eventually solved by Penttila [9] for  $N \ge 5$ , but is still open for N = 3, 4. The above work suggests an analogous problem, namely the determination of the subgroups of  $P\Gamma L(N + 1, q)$  which induce tactical decompositions satisfying the upper bound in Theorem 2.2. The Steiner system  $\mathcal{D}$  of points and lines of PG(N, q) has  $v = q^N + \cdots + 1, k = q + 1, b = (q^N + \cdots + 1)(q^{N-1} + \cdots + 1)/(q+1)$  and  $r = q^{N-1} + \cdots + 1$ . Thus the maximum number of line-classes for a tactical decomposition with m point-classes is

$$n = \frac{(q^N + \dots + 1 + mq(q^{N-2} + \dots + 1))}{q+1},$$
(1)

by Theorem 2.2. We now prove that non-trivial groups inducing such decompositions exist if and only if N is odd, and determine the examples which occur in this case.

**Lemma 3.1** Suppose that the collineation group G of PG(N, q) induces a tactical decomposition satisfying Eq. (1). Then G acts regularly on each of its point-orbits.

**Proof:** If some  $g \in G$  fixes the point P, then g must also fix all lines on P, since by Theorem 2.2, the line-orbits of G must all be partial spreads. Therefore g is a central

collineation (see [3]), but a central collineation of PG(N, q) also has an axis—that is, a hyperplane *H* such that *g* fixes every point of *H*. But every line of PG(N, q) intersects *H* in at least one point, so by the above reasoning every line of PG(N, q) is fixed by *g*. Thus *g* is the identity.

This implies that the size of G divides the number  $v = q^N + \cdots + m + 1$  of points of PG(N, q). Put |G| = a (so  $a = (q^N + \cdots + 1)/m$ ).

#### **Lemma 3.2** Each non-identity element of G must fix exactly one line-spread of PG(N, q).

**Proof:** Applying the orbit counting lemma (see [1]) and Eq. (1) to the action of G on the lines of PG(N, q) yields

$$\frac{(q^N + \dots + 1 + mq(q^{N-2} + \dots + 1))}{q+1} = \frac{1}{a} \sum_{g \in G} |\operatorname{fix}(g)|.$$

Of course, the identity element fixes all *b* lines of PG(N, q); taking this into account and manipulating the above equation shows that the average number of lines fixed by a given non-identity element  $g \in G$  is exactly  $(q^N + \cdots + 1)/(q + 1)$ . Now any set *S* of pairwise skew lines of PG(N, q) has cardinality at most  $(q^N + \cdots + 1)/(q + 1)$ , with equality if and only if *S* is a spread. But the intersection of two fixed lines is a fixed point, so the fact that *G* acts regularly on its point-orbits implies that no two lines fixed by *g* can meet. Therefore no non-identity element of *G* may fix more than  $(q^N + \cdots + 1)/(q + 1)$  lines, so each must fix exactly this number, that is, each non-identity element of *G* fixes exactly one spread.

Now line-spreads of PG(N, q) exist if and only if N is odd [3], so G can be non-trivial only if N = 2R + 1 is odd. From now on, we assume that  $\mathcal{D}$  is the design of points and lines of  $PG(2R + 1, q), R \ge 1$ . Note that the set of spreads fixed by non-identity elements of G is also acted on by G—if g fixes S then hS is fixed by  $gh^{-1}$ . Now this action has the property that each non-identity element of G fixes exactly one spread; therefore by the orbit counting lemma (or otherwise) we conclude that all elements of G fix the same spread. Now an easy geometric argument shows that a non-trivial collineation of PG(2R + 1, q)which fixes a line spread cannot fix any points. Thus any such group must have size dividing q + 1.

Examples are constructed as follows. D.G. Glynn in [5] observed that the line orbits of the Singer group of PG(3, q) are of two types: one regular spread, and q sets of lines covering each point (q + 1) times. The regular spread is fixed by the unique subgroup of G of order q + 1. In fact, this analysis goes through for arbitrary odd dimension, and thus there exist line spreads of PG(2R + 1, q) fixed by a cyclic group of size q + 1, and hence for every a dividing q + 1 there exists a group of size a inducing a decomposition of D satisfying the upper bound 1 and having  $a(q^{2R} + q^{2R-2} + \cdots + 1)$  point classes.

Now in PG(3, q) any line spread which is fixed by a non-trivial collineation is regular (the kernel of the corresponding translation plane of order  $q^2$  has size at least 2(q-1); since this

number is a power of q it must be  $q^2$ , so the plane is desarguesian—see [7]). Furthermore, if S is a line spread of PG(2R + 1, q) which is fixed by a non-trivial collineation group G, then S has the property that any three-dimensional subspace of PG(2R + 1, q) contains 0, 1, or  $q^2 + 1$  lines of S: any two lines of S span a unique three-dimensional subspace Xwhich is fixed by all elements of G, and if a line of S intersects X in one point, this point is fixed by any element of G, so G is trivial. Now restricting to any of these three-dimensional subspaces X shows that the spread contained in X must be regular, and therefore that G is cyclic of order dividing q + 1 in the general case. If X is a subspace of PG(2R + 1, q), we will say that X is a subspace of S if the set of lines of S contained in X form a spread of X.

**Theorem 3.1** Let S be a line spread of PG(2R + 1, q) which is fixed by a non-trivial collineation group G. Then the geometry whose points are the lines of S and whose i dimensional subspaces (i < R) are the 2i + 1 dimensional subspaces of S, is isomorphic to  $PG(R, q^2)$ , and G is contained in a cyclic group of size q + 1 which fixes all lines of S.

**Proof:** We show first that the set S of lines, together with the set of (2R - 1)-dimensional subspaces of S forms a design isomorphic to the design of points and lines of  $PG(R, q^2)$ . The comments preceeding the theorem show that any pair of elements of  $\mathcal{V}$  are contained in exactly one three-space of S. Let X be such a three-space. If  $l \in S$  is not contained in X, l is disjoint from X, so  $X \vee l$  is a five-dimensional space Y, and all elements of G fix Y, so (as the non-identity elements of G act fixed-point freely) Y is a subspace of S. Now counting shows that any two lines of S are contained in the same number of five dimensional subspaces of S, and continuing inductively we see that any two lines of S are contained in the same number of 2i + 1 dimensional subspaces of S, for all i < R - 1. This shows that S and the set of (2R-1)-dimensional subspaces of S is a design  $\mathcal{E}$ . The lines of this design are clearly the three-dimensional subspaces of S, and since in PG(2R + 1, q) any 2R - 1dimensional subspace meets any three-dimensional subspace in at least a line, every line of  $\mathcal{E}$  meets every block of  $\mathcal{E}$ . Thus, by 2.1.22 of Dembowski [3, p. 67],  $\mathcal{E}$  is the design of points and hyperplanes of a projective geometry, which must be  $PG(R, q^2)$  (this is clear from the number of points on each block when R > 3; when R = 2 the plane is desarguesian since it occurs as the point-residue of the following embedding of  $AG(3, q^2)$  in AG(6, q). Now when PG(2R+1, q) is regarded as the hyperplane H at infinity of an AG(2R+2, q), the points of the affine geometry together with the planes whose intersections with H are lines of S forms an  $AG(R + 1, q^2)$ ; the group of  $q^2 - 1$  dilatations of this geometry induces a cyclic group of q + 1 collineations fixing all lines of S; clearly G is contained in this group. 

As far as the groups inducing tactical decompositions satisfying the upper bound in Theorem 2.2, we have:

**Theorem 3.2** Let G be a subgroup of  $P\Gamma L(N + 1, q)$  which induces a tactical decomposition of PG(N, q) satisfying Eq. (1). If N is even, G is the trivial group. If N is odd, G is contained in a cyclic group of order q + 1 which fixes all lines of a line spread of PG(N, q).

## Acknowledgment

The author wishes to thank Prof. Peter Cameron for illuminating discussions on this material.

## References

- 1. P.J. Cameron, Permutation Groups, Cambridge University Press, Cambridge, 1999.
- 2. P.J. Cameron and R.A. Liebler, "Tactical decompositions and orbits of projective groups," *Lin. Alg. Appl.* **46** (1982), 91–102.
- 3. P. Dembowski, Finite Geometries, Springer-Verlag, Berlin-Heidelberg, 1968.
- 4. K. Drudge, "Extremal sets in projective and polar spaces," Ph.D. Thesis, University of Western Ontario, 1998.
- D.G. Glynn, "On a set of lines of PG(3, q) corresponding to a maximal cap contained in the Klein quadric of PG(5, q)," Geom. Ded. 26 (1988), 273–280.
- 6. W.H. Haemers, *Eigenvalue Techniques in Design Theory and Graph Theory*, Mathematisch Centrum, Amsterdam, 1980. Mathematical Centre Tracts #121.
- 7. H. Lüneburg, Translation Planes, Springer-Verlag, Berlin-Heidelberg, 1980.
- 8. S.E. Payne, "Tight pointsets in finite generalized quadrangles I," *Congressus Numerantium* **60** (1987), 243–260; II, *Congressus Numerantium* **77** (1990), 31–41.
- 9. T. Penttila, "Collineations and configurations in projective spaces," Ph.D. Thesis, Oxford University, 1985.

# 130