JOURNAL OF COMBINATORIAL THEORY, Series A **65**, 322–329 (1994)

Note

Small Blocking Sets of Hermitian Designs*

DAVID A. DRAKE AND CYRUS KITTO

University of Florida, Gainesville, Florida 32611

Communicated by Jonathan I. Hall

Received October 11, 1991

A Hermitian design $H(q)$ consists of the points and Hermitian unitals of $PG(2, q^2)$. A committee of $H(q)$ is a blocking set of $H(q)$ of minimum cardinality $b(H(q))$. It is proved that the committees of $H(3)$ are the lines of $PG(2, 9)$ and, for all odd q, that $2q+2 \leqslant b(H(q)) < (1+7 \ln q)(q^2+1)\, q^{-1}$. © 1994 Academic Press, Inc.

INTRODUCTION

A $t-(v, k, \lambda)$ *design* is a set of v *points* and a collection of distinguished subsets of size k called *blocks*, such that every subset of t points lies in precisely λ blocks. A *hitting set* of a design I is a set of points of I which contains at least one point of every block of I. A hitting set which contains no block is called a *blocking set* of I. We write $h(I)$ and $b(I)$, respectively, to denote the minimum cardinalities of hitting sets and blocking sets of I. Blocking sets of cardinality $b(I)$ are called *committees* of I.

A (*Hermitian*) *unital* H of the projective plane $\Pi = PG(2, q^2)$, q odd, is the set of all points with homogeneous coordinates (x, y, z) which satisfy $(xyz)\, A(x^q y^q z^q)^t = 0$ where A is a fixed non-singular Hermitian matrix. Every unital H is a blocking set of Π: each line of Π is *tangent* (meeting H in one point) or a *secant* that meets H in $q+1$ points. Thus, Π induces on H the structure of a *unitary design*; i.e., the structure of a $2-(q^3+1, q+1, 1)$ design.

Throughout the paper, we write Π or $\Pi(q)$ to denote $PG(2, q^2)$ where q is odd. We write $H(q)$ to denote the incidence structure which consists of the points of Π as points and the unitals of Π as blocks. The plane Π admits the doubly transitive automorphism group $G = PGL(3, q^2)$. Since G preserves unitals, $H(q)$ is a $2-(v, k, \lambda)$ design. Since the unitary subgroup of G has order $(q^3+1)\, q^3(q^2-1)$, it is routine to verify that the parameters

* The first author acknowledges the support of the National Science Foundation. Both authors have been supported in part by NSA/MSP Grant MDA90-H-1012.

0097-3165/94 $6.00

are $v = q^4 + q^2 + 1$, $k = q^3 + 1$, and $\lambda = q^4(q^2 - 1)$. We call $H(q)$ the *Hermitian design* of Π. One of the goals of this paper is to prove

THEOREM 1. *For odd* q, $2q + 2 \leqslant b(H(q)) < (1 + 7 \ln q)(q^2 + 1)\, q^{-1}$.

Two designs defined on the same point set are called *mutually blocking* or *mutually committing*, respectively, if every block of each design is a blocking set or a committee of the other design. Thus, Π and $H(q)$ are mutually blocking designs. A widely known theorem of Bruen [2, 3] asserts that the committees of Π are the Baer subplanes of Π, i.e., the subplanes of order q. Let $B(\Pi)$ denote the design defined on the point set of Π by using the Baer subplanes of Π as blocks. Jungnickel [8] has proved that the committees of $B(\Pi)$ are the lines of Π, so Π and $B(\Pi)$ are mutually committing designs. If I is a design with a doubly transitive automorphism group, then the committees of I form a design $C(I)$ on the point set of I, which we call the *committee design* of I. Thus, the Bruen and Jungnickel results can be formulated as $C(\Pi) = B(\Pi)$ and $C^2(\Pi) = \Pi$.

In the case $q = 3$, we can improve Theorem 1 to $b(H(q)) = 10$. In fact, we obtain the following characterization of $PG(2, 9)$.

THEOREM 2. $PG(2, 9)$ *is the committee design of* $H(3)$.

It follows that $C^3(H(3)) = C(H(3))$, so the sequence $\{C^i(H(3))\}$ has period 2. Our final result is obtained by sharpening some of the arguments that produce the upper bound in Theorem 1.

Remark 3. *For* $q \geqslant 23$, $b(H(q)) \leqslant q^2$; *so* $C(H(q)) \neq PG(2, q^2)$.

1. THE LOWER BOUND

In section 1, we obtain the lower bound of Theorem 1 and prove Theorem 2. We represent the points and lines of Π by homogeneous triples of elements of $F = GF(q^2)$. We write K to denote the subfield of F of order q and $H[c, e]$ to denote the unital of Π which is represented by the matrix

$$A = \begin{pmatrix} 0 & 0 & c \\ 0 & 1 & e \\ c^q & e^q & e^{q+1} \end{pmatrix}.$$

LEMMA 4. *The lines* $(0, 0, 1)^t = h$ *and* $(1, 0, 0)^t = g$ *are tangent to* $H[c, e]$ *at the respective points* $(1, 0, 0) = P$ *and* $(0, -e^q, 1)$.

Proof. The tangents to the unital of a matrix A are the lines $(u, v, w)^t$ which satisfy $(u^q, v^q, w^q)\, A^{-1}(u, u, w)^t = 0$: see [6, pp. 47, 48]. The conclusions follow by computation.

For b in K and non-zero a in F, we write $L[a, b]$ to denote $\{x \in F \mid (ax)^q + ax + b = 0\}$; we define $f\colon F \times F \to K$ by $f(e, s) = (e + s^q)^{q+1}$.

LEMMA 5. *For $r \neq 0$, the point $(r, s, 1)$ of Π is in $H[c, e]$ if and only if c is in $L := L[r, f(e, s)]$; L contains 0 if and only if $e = -s^q$.*

Proof. The point $(r, s, 1)$ is in $H[c, e]$ if and only if $0 = (cr)^q + cr + e^{q+1} + (es)^q + es + s^{q+1} = (cr)^q + cr + (e + s^q)^{q+1}$.

LEMMA 6. *Let Σ_1 denote the collection of distinct sets $L[a, 0]$ with $0 \neq a \in F$. Then Σ_1 is a spread of F regarded as a vector space over K. The affine plane Σ determined by Σ_1 is Desarguesian.*

Proof. Since $y \to y^q$ is a linear transformation of F over K, each $L[a, 0]$ is a subspace of F. The set $L[a, 0]$ contains the nonzero vector $r = a^{-1}\sigma^{(q+1)/2}$, where σ is a primitive root of F. Thus, the dimension of $L[a, 0]$ is 1. If $0 \neq c \in F$, then c is in $L[rc^{-1}, 0]$, so the sets $L[a, 0]$ cover F. Since distinct one-dimensional subspaces intersect trivially, Σ_1 is a spread. The Desarguesian plane of order q can be represented as the collection of cosets of the unique spread Σ_1 of F over K, so Σ must be Desarguesian.

LEMMA 7. *Every $L[a, b]$ with $0 \neq a \in F$ and $b \in K$ is a coset of $L[a, 0]$ and, hence, a line of Σ. Lines $L[a, b]$ and $L[c, d]$ are parallel if and only if ac^{-1} is in K; in particular, $L[a, 0] = L[c, 0]$ if and only if ac^{-1} is in K.*

Proof. Since the linear mapping $x \to (ax)^q + ax$ from F to K is surjective, there is an e in K with $(ae)^q + ae = -b$. Then $e + L[a, 0] \subseteq L[a, b]$. Equality of these sets is a consequence of the fact that $|L[a, b]| \leqslant q$.

Since $L[a, b]$ is parallel to $L[a, 0]$ for all a and b, $L[a, b] \parallel L[c, d]$ if and only if $L[a, 0] \parallel L[c, 0]$ if and only if $L[a, 0] = L[c, 0]$. It remains only to prove that the preceding equality is equivalent to the condition $ac^{-1} \in K$. Let $0 \neq x \in L[a, 0]$. Then $ac^{-1}x \in L[c, 0]$. Thus, $L[a, 0] = L[c, 0]$ if and only if $ac^{-1}x \in L[a, 0]$ if and only if $ac^{-1} \in K$.

LEMMA 8 (Jamison [7, Theorem 1′, p. 257], or see Brouwer and Schrijver [1]). *Let F be a vector space of dimension n over a finite field K with q elements. Then any covering of the nonzero elements of F with hyperplanes not containing zero must consist of at least $n(q-1)$ hyperplanes.*

LEMMA 9. *Let B be a blocking set of $H(q)$. Let g, h, l, be a non-concurrent triple of lines of Π with $|B \cap l| = 0$. Then $|B \backslash (g \cup h)| \geqslant 2q - 2$.*

Proof. Coordinatize Π with homogeneous triples so that $l \cap h = P = (1, 0, 0)$, $g \cap h = Q = (0, 1, 0)$, and $l \cap g = T = (0, 0, 1)$. Then $B \backslash (g \cup h)$ consists of points $R_j = (r_j, s_j, 1)$, $1 \leqslant j \leqslant i$, where all r_j and all s_j are nonzero. By Lemma 4, every unital $H[c, 0]$ is tangent to h at P and to g at T. Since P and T are in l, they are not in B, so each $H[c, 0]$ must contain some R_j. By Lemma 5, each nonzero c in F lies in $L_j := L[r_j, f(0, s_j)]$ for some $j \leqslant i$, and no L_j contains the point 0. Lemma 8 yields the conclusion $i \geqslant 2q - 2$.

PROPOSITION 10. $b(H(q)) \geqslant 2q + 2$.

Proof. Assume, by way of contradiction, the existence of a blocking set B of $H(\Pi)$ of cardinality $2q + 1$ or less. Choose distinct lines g, h of Π to maximize $|B \cap (g \cup h)|$. Since $2q + 1 < q^2$, there is a point P in $h \backslash (B \cup g)$, and P is incident with a line l with $l \neq h$ and $|l \cap B| = 0$. By Lemma 9, $|B| \geqslant 2q - 2 \geqslant 4$, so $|B \cap (g \cup h)| \geqslant 4$. A second application of Lemma 9 completes the proof.

Proposition 10 supplies the lower bound of Theorem 1. We next proceed, in a series of steps, to prove Theorem 2, that the committees of $H(3)$ are the lines of $PG(2, 9)$. For the next four steps, we assume that $q = 3$; i.e., that $\Pi = \Pi(3) = PG(2, 9)$.

Step 1. Let B be a blocking set of $H(3)$. Let g and h be distinct lines of Π meeting in a point Q and satisfying $|(g \cup h) \cap (B \backslash \{Q\})| \leqslant 8$, $|B \backslash h| \leqslant 8$. Then $|B \backslash (g \cup h)| \geqslant 5$.

Proof. Assume, by way of contradiction, that $|B \backslash (g \cup h)| \leqslant 4$. Since $|h \cap (B \backslash \{Q\})| \leqslant 8$, there is a point P' in $h \backslash (B \cup \{Q\})$; since $|B \backslash h| \leqslant 8$, there is a line l' which satisfies $|l' \cap (B \cup \{Q\})| = 0$. Then Lemma 9 yields the conclusion that $B \backslash (g \cup h)$ is a set of 4 points, which we denote by R_1, R_2, R_3, R_4. There is a line l through R_4 such that $l \cap h =: P$ and $l \cap g =: T$ are not in B. Coordinatize Π so that $P = (1, 0, 0)$, $Q = (0, 1, 0)$, $T = (0, 0, 1)$. For $1 \leqslant j \leqslant 4$, denote the coordinates of R_j by $(r_j, s_j, 1)$; then $s_4 = 0$, but no r_j is zero.

Define $L_i^e := L[r_i, f(e, s_i)]$, $J_e := L_1^e \cup \cdots \cup L_4^e$. From the assumption $|B \backslash h| \leqslant 8$, one concludes that $|B \cap (g \backslash \{Q\})| \leqslant 4$. Thus, Lemma 4 guarantees the existence of at least five values of e such that $H[c, e]$ is disjoint from $g \cap B$ and $h \cap B$ for all c. Fix one of these e's which also satisfies $e \neq -s_i^q$ for $1 \leqslant i \leqslant 4$. For every nonzero c, the unital $H[c, e]$ contains a point R_i. By Lemma 5, J_e is the set of eight nonzero points of the affine plane Σ. Then the four lines L_i^e are distinct, and two of the four are parallel, but no three are mutually parallel.

A similar argument shows that J_0 contains all nine points c of Σ. Lines L_i^e and L_j^e are parallel if and only if L_i^0 and L_j^0 are parallel. Then the nine points of Σ are covered by a set of four of fewer lines, two of which are parallel to each other but not parallel to the other two. This impossibility completes the proof of Step 1.

Step 2. Let B be a blocking set of $H(3)$ with $|B| \leqslant 10$ so that B is neither a line nor an oval of Π. Then there is a line h of Π with $|B \cap h| = 3$, and no three points of $B \backslash h$ are collinear.

Proof. Let h be a line which maximizes $|B \cap h|$. Then $3 \leqslant |B \cap h| \leqslant 9$. Step 1 gives $|B \backslash h| \geqslant 5$. Then there is a line $g' \neq h$ so that $|(B \backslash h) \cap g'| \geqslant 2$. Lemma 9 implies that $|(g' \cup h) \cap B| \leqslant 6$, so a second application of Step 1 gives $|B \backslash h| \geqslant 7$. Then $|B \cap h| = 3$, and $|B \backslash h| = 7$. A third application of Step 1 gives $|(B \backslash h) \cap g| \leqslant 2$ for every line $g \neq h$.

Step 3. Let B be a blocking set of $H(3)$ with $|B| \leqslant 10$. Then B is either a line or an oval of Π.

Proof. Assume, by way of contradiction, that B is neither a line nor an oval. Then, by Step 2, the 7 points of $B \backslash h$ must be joined to each other by 21 distinct lines, 3 of which must meet in some point Q of h. Denote the points of $B \backslash h$ by $R_1, ..., R_7$ so that the lines R_2R_3, R_4R_5, and $R_6R_7 := g$ are incident with Q. For some i with $2 \leqslant i \leqslant 5$, the line R_1R_i intersects h and R_6R_7 in points P and T, respectively, which are not points of B. Without loss of generality, take $i = 2$. Let R_0 denote $R_1R_2 \cap R_4R_5$. Coordinatize Π so that $P = (1, 0, 0)$, $Q = (0, 1, 0)$, and $T = (0, 0, 1)$. Denote the coordinates of R_i by $(r_i, s_i, 1)$, $0 \leqslant i \leqslant 7$.

For e in F, let L_i^e denote $L[r_i, f(e, s_i)]$; and let J_e denote $L_1^e \cup \cdots \cup L_5^e$. If e is any one of the seven values with $-e^3 \neq s_6, s_7$, Lemma 4 guarantees that the unitals $H[c, e]$ are tangent to g and h at points which do not belong to B. Every such $H[c, e]$ must contain a point R_i for some i with $1 \leqslant i \leqslant 5$. By Lemma 5, J_e must contain all eight nonzero points of Σ for $e \neq -s_6^3, -s_7^3$.

Since $r_2 = r_3$ and $r_4 = r_5$, Lemma 7 gives $L_2^e \parallel L_3^e$ and $L_4^e \parallel L_5^e$. Clearly, the condition that lines L_i^e and L_j^e be parallel is independent of the choice of e.

We claim that $L_2^e \nparallel L_4^e$. Suppose otherwise. Choose e with $e \neq -s_i^3$ for all $i \leqslant 7$. By Lemma 5, neither L_1^e nor any of the four parallel lines L_i^e, $i \leqslant 5$, contains the point 0. Thus, the four constitute at most two distinct lines of a parallel class; and the five lines cannot cover all eight nonzero points of Σ, a contradiction.

As $-0^3 \neq s_6, s_7$, the set J_0 must contain all nonzero points of Σ and, in particular, the two nonzero points in L_0^0. Since L_4^0 and L_5^0 are parallel to L_0^0 and do not contain the point 0, they are disjoint from L_0^0. L_2^0 meets L_0^0 only in the point 0, and L_3^0 contains only one of the two nonzero points of L_0^0. Then L_1^0 must contain the other. Since L_1^0 also contains the point 0, $L_1^0 = L_0^0$, so $L_1^0 \| L_4^0$. Then $L_1^e \| L_4^e$ for all e.

To summarize, L_1^e, L_4^e, and L_5^e are in one common parallel class while L_2^e and L_3^e are in a different common class.

Let G be the set of all e such that L_1^e, L_4^e, and L_5^e are not distinct. Let H be the set of all e such that either $L_2^e = L_3^e$ or $L_2^e \cup L_3^e$ contains the point 0. We prove that $|G| \geqslant 7$ and $|H| \geqslant 5$. It follows that $|G \cap H| \geqslant 3$. Then there is an e in $G \cap H$ with $e \neq -s_6^3, -s_7^3$; for this e, one has the contradiction that some non-zero c in Σ is not in J_e, a contradiction which completes the proof of Step 3.

If $e \neq -s_i^3$ for $i = 1, 4, 5$; none of L_1, L_4, L_5 contains 0, so e is in G. Thus, it suffices to prove that G contains $-s_i^3$ for some i in $\{1, 4, 5\}$. Suppose that $0 = -s_1^3$ is not in G. Then $L_4^0 \neq L_5^0$. Since $r_4 = r_5$, $f(0, s_4) \neq f(0, s_5)$; so $s_4^4 \neq s_5^4$. We may take $s_4^4 = 1 = -s_5^4$. Then $f(-s_5^3, s_4) = (-s_5^3 + s_4^3)^4 = f(-s_4^3, s_5) =: \alpha \neq 0$. If $\alpha = 1$, we take $e = -s_5^3$ and obtain $f(e, s_1) = f(e, 0) = -1 = -f(e, s_4)$. Since $r_1 \neq r_4$ while $r_1 r_4^{-1}$ is in K, one concludes that $r_1 = -r_4$. Thus, $L_1^e = L_4^e$, and $e = -s_5^3$ is in G. The other possibility is that $\alpha = -1$, in which case a similar argument proves that $-s_4^3$ is in G. In all cases, $|G| \geqslant 7$.

The lines L_2^e and L_3^e are equal if and only if $e^4 = (e + s_3^3)^4$ if and only if $e = xs_3^3$ where $x^4 = (x+1)^4$. The solutions are the roots of $g(x) = x^3 + x + 1 = (x-1)(x^2 + x - 1)$ which splits in F. Since the derivative $g'(x) = 1$, the roots are distinct; and $L_2^e = L_3^e$ for three values of e. Since 0 is in $L_2^e \backslash L_3^e$ for $e = 0$ and 0 is in $L_3^e \backslash L_2^e$ for $e = -s_3^3$, $|H| \geqslant 5$.

Step 4. No oval is a blocking set of $H(3)$.

Proof. By a well known theorem of Segré, every oval is a conic. Since all conics are projectively equivalent, it suffices to prove that some conic of Π is disjoint from some unital of Π. Let B be the conic consisting of the solutions to $X^2 + Y^2 - \sigma Z^2 = 0$ where σ is a primitive root of $F = GF(9)$. Let U be the unital of the identity matrix. Suppose that $P = (x, y, z)$ is in $B \cap U$. Then $x^2 + y^2 - \sigma z^2 = 0$ and $x^4 + y^4 + z^4 = 0$. If $z = 0$, neither x nor y is 0, so one may take $y = 1$. Then $x^2 = -1 = x^4$. By the contradiction, $z \neq 0$; and we may take $z = 1$. Then $x^2 + y^2 = \sigma$ and $x^4 + y^4 = 2$. Squaring the first equation and subtracting the result from the second yields $x^2y^2 = = 2 + 2\sigma^2 = \sigma^4(1 + \sigma^2)$. Then $1 + \sigma^2$ is a square, i.e., an even power of σ. The contradiction follows easily.

Proof of Theorem 2. Apply Steps 3 and 4.

Remark 11 (Kitto [9]). No oval is a blocking set of $H(q)$ for any odd q.

2. The Upper Bound

A *fractional hitting set* of an incidence structure I is a function f from the points of I to the non-negative reals with the property that $f(L) := \Sigma f(P) \geqslant 1$ for each block L, where the sum is taken over all points P incident with L. Write $|f|$ for $\sum f(P)$ where the sum is taken over all P in I. The *fractional hitting number* $h^*(I)$ is the minimum $|f|$ as f ranges over all fractional hitting sets of I.

Lemma 12 (Lovász and Stein; see, e.g., [4, Corollary 6.29]). *Let I be a finite incidence structure, and r be the largest number of blocks incident with a point of I. Then*

$$h(I) < (1 + \ln r)\, h^*(I).$$

We now present a proof of the upper bound of Theorem 1 which was communicated to us by Aart Blokhuis and Tamás Szőnyi.

For $H(q)$, every point lies in r blocks, where $r = (v-1)\,\lambda/(k-1) = q^7 - q^3$. The constant function $f(P) = 1/k = 1/(q^3+1)$ is a fractional hitting set of $H(q)$, and $|f| = v/k = (q^4+q^2+1)(q^3+1)^{-1}$. By Lemma 12, $h(H(q)) \leqslant (1+\ln(q^7-q^3))(q^4+q^2+1)(q^3+1)^{-1} < (1+7\ln q)(q^2+1)\,q^{-1}$. For $q \geqslant 5$, this upper bound for $h(H(q))$ is less than q^3+1; when $q=3$, the smallest hitting sets are the lines of Π. In both cases, the smallest hitting sets of $H(q)$ are blocking sets. Then $b(H(q)) = h(H(q))$, and the proof of Theorem 1 is complete.

The upper bound is less than q^2+1 for $q \geqslant 23$, which establishes Remark 3.

Acknowledgments

The authors thank Aart Blokhuis and Tamás Szőnyi for a number of helpful discussions and, in particular, for supplying the proof of the upper bound.

References

1. A. E. Brouwer and A. Schrijver, The blocking number of an affine space, *J. Combin. Theory, Ser. A* **24** (1978), 251–253.
2. A. A. Bruen, Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970), 342–344.
3. A. A. Bruen, Blocking sets in finite projective planes, *SIAM J. Appl. Math.* **21** (1971), 380–392.
4. Z. Füredi, Matchings and covers in hypergraphs, *Graphs Combin.* **4** (1988), 115–206.

5. J. W. P. HIRSCHFELD, "Projective Geometries over Finite Fields," Oxford Mathematical Monographs, Clarendon, Oxford, 1979.
6. D. R. HUGHES AND F. C. PIPER, "Projective Planes," Graduate Texts in Mathematics, Vol. 6, Springer, New York/Heidelberg/ Berlin, 1973.
7. R. E. JAMISON, Covering finite fields with cosets of subspaces, *J. Combin. Theory, Ser. A* **22** (1977), 253–266.
8. D. JUNGNICKEL, Some self-blocking block designs, *Discrete Math.* **77** (1989), 123–135.
9. C. L. KITTO, "Some Problems in Blocking Sets," Ph.D. dissertation, University of Florida, 1992.