PETER J. CAMERON AND FRANCESCO MAZZOCCA*

BIJECTIONS WHICH PRESERVE BLOCKING SETS

ABSTRACT. We consider the following question: Given a family $\mathscr{A}$ of sets for which $\mathscr{A}$-blocking sets exist, is it true that any bijection of the set of points which preserves the family of $\mathscr{A}$-blocking sets must preserve $\mathscr{A}$? Using a variety of techniques, we show that the answer is 'yes' in many cases, for example, when $\mathscr{A}$ is the family of subspaces of fixed dimension in a projective space, lines in an affine plane, or blocks of a symmetric design, but that it is 'no' for lines of an arbitrary linear space.

1. INTRODUCTION

Let $\mathscr{A}$ be a family of subsets of the finite set X. A subset S of X *hits* $\mathscr{A}$ if $S \cap A \neq \emptyset$ for all $A \in \mathscr{A}$; it *blocks* $\mathscr{A}$ if, in addition, S contains no member of $\mathscr{A}$; that is, S and $X \setminus S$ both hit $\mathscr{A}$. We let $H(\mathscr{A})$, $B(\mathscr{A})$ denote the collections of all sets which hit $\mathscr{A}$, resp. block $\mathscr{A}$. For any family $\mathscr{A}$, let $\mathscr{A}_{\min}$ denote the set of all elements of $\mathscr{A}$ which are minimal with respect to inclusion, and let $h(\mathscr{A}) = H(\mathscr{A})_{\min}$, $b(\mathscr{A}) = B(\mathscr{A})_{\min}$. Finally, Aut $(\mathscr{A})$ denotes the group

$$\{g \in \mathrm{Sym}(X) \mid g(A) \in \mathscr{A} \text{ for all } A \in \mathscr{A}\}$$

of bijections (permutations) of X, where $\mathrm{Sym}(X)$ is the symmetric group on X.

We consider the following general problem, raised by Mazzocca [6]: *For which families* $\mathscr{A}$ *is it true that* $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$?

We note that, for any family $\mathscr{A}$, we have $H(\mathscr{A}) = H(\mathscr{A}_{\min})$ and $B(\mathscr{A}) = B(\mathscr{A}_{\min})$; moreover, $\mathrm{Aut}(\mathscr{A}_{\min}) \geqslant \mathrm{Aut}(\mathscr{A})$. So our problem may have a negative answer if $\mathscr{A} \neq \mathscr{A}_{\min}$, and we consider only the case when $\mathscr{A} = \mathscr{A}_{\min}$, which holds if and only if $\mathscr{A}$ is a clutter. (A *clutter*, otherwise known as a *Sperner family* or *antichain*, is a family $\mathscr{A}$ of subsets of X with the property that, for all $A_1, A_2 \in \mathscr{A}$, $A_1 \not\subset A_2$.)

We have the following inclusion.

LEMMA 1.1. $\mathrm{Aut}(H(\mathscr{A})) = \mathrm{Aut}(h(\mathscr{A})) \leqslant \mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(b(\mathscr{A}))$.

Proof. To show the equalities, we must show that each family determines the other. We have $h(\mathscr{A}) = H(\mathscr{A})_{\min}$ and

$$H(\mathscr{A}) = \{A \subseteq X \mid \exists A_1 \in h(\mathscr{A}) \text{ with } A_1 \subseteq A\};$$

also $b(\mathscr{A}) = B(\mathscr{A})_{\min}$ and

$$B(\mathscr{A}) = \{A \in X \mid \exists A_1, A_2 \in b(\mathscr{A}) \text{ with } A_1 \subseteq A, A_2 \cap A = \emptyset\}.$$

* Work supported by National Research Project on 'Strutture geometriche, combinatoria loro applicazioni' of M.P.I. and by G.N.S.A.G.A. of C.N.R.

Geometriae Dedicata **21** (1986) 219–229.

GEOM 402

Also, we may substitute $h(\mathscr{A})$ for $b(\mathscr{A})$ in the last equality to show that $\mathrm{Aut}(h(\mathscr{A})) \leqslant \mathrm{Aut}(b(\mathscr{A}))$.

In Section 2, we apply a result of Edmonds and Fulkerson to show that $\mathrm{Aut}(H(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$ for any clutter $\mathscr{A}$, and to obtain some sufficient conditions for $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$. We pursue these ideas further in Section 3 to show that, in the case where $\mathscr{A}$ is the set of lines in a projective or affine plane, then elements of $\mathscr{A}$ are the sets of smallest cardinality in $h(b(\mathscr{A}))$, so that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$. In section 4, we establish the same conclusion on the assumption that $\mathrm{Aut}(\mathscr{A})$ is a maximal subgroup of $\mathrm{Sym}(X)$ or $\mathrm{Alt}(X)$ and $B(\mathscr{A}) \neq \emptyset$; this includes projective spaces, and affine spaces over prime fields, whose dimension is not too large. For affine spaces over arbitrary fields, we construct in Section 5 some line-blocking sets which permit the same conclusion to be drawn. The final section describes a family of linear spaces $\mathscr{A}$ for which $\mathrm{Aut}(B(\mathscr{A})) \neq \mathrm{Aut}(\mathscr{A})$.

2. Blocking sets and hitting sets

Edmonds and Fulkerson [3] established the following result. For completeness, we include the proof.

PROPOSITION 2.1 *For any clutter $\mathscr{A}$, the following hold:*

(i) *$h(\mathscr{A})$ is a clutter;*
(ii) *$h(h(\mathscr{A})) = \mathscr{A}$;*
(iii) *For any $A \in \mathscr{A}$ and any $a \in A$, there exists $B \in h(\mathscr{A})$ with $A \cap B = \{a\}$.*

Proof. (i) is clear; we turn next to (iii). Given $a \in A \in \mathscr{A}$, let $B' \in h(\mathscr{A}')$, where $\mathscr{A}'$ is the family

$$\{A' \setminus A \mid A' \in \mathscr{A},\ a \notin A'\};$$

then $B = \{a\} \cup B'$ is the required set.

Now, for any $A \in \mathscr{A}$, clearly $A \in H(h(\mathscr{A}))$; by (iii), for any $a \in A$, $A \setminus \{a\} \notin H(h(\mathscr{A}))$, so $A \in H(h(\mathscr{A}))_{\min} = h(h(\mathscr{A}))$. Suppose that $S \in h(h(\mathscr{A}))$ but $S \notin \mathscr{A}$. Then S contains no member of $\mathscr{A}$; so the complement of S is in $H(\mathscr{A})$, and so there is a set in $h(\mathscr{A})$ disjoint from S, contrary to assumption. So $h(h(\mathscr{A})) = \mathscr{A}$, as required.

COROLLARY 2.2. $\mathrm{Aut}(H(\mathscr{A})) = \mathrm{Aut}(h(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$ *for any clutter $\mathscr{A}$.*

Thus the analogue of our question for hitting sets is trivial. Also, from the corollary, we can deduce a sufficient condition:

PROPOSITION 2.3. *Let $\mathscr{A}$ be a clutter in which no two sets meet in precisely one point. Then $b(\mathscr{A}) = h(\mathscr{A})$, and so* $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$.

Proof. Clearly $b(\mathscr{A}) = h(\mathscr{A}) \cap B(\mathscr{A}) \subseteq h(\mathscr{A})$. Assume that $S \in h(\mathscr{A})$ but $S \notin b(\mathscr{A})$. Then S contains a member A of $\mathscr{A}$. For any $a \in A$, there is a set $A' \in \mathscr{A}$ with $A' \cap S = \{a\}$ (since, if not, then $S \setminus \{a\} \in H(\mathscr{A})$, contradicting the minimality of S). Then $A \cap A' = \{a\}$, contrary to assumption.

This result shows that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$ for many families $\mathscr{A}$; for example, the family of h-spaces in projective or affine n-space over $\mathrm{GF}(q)$ with $h > \frac{1}{2}n$; symmetric designs other than projective planes (or, more generally, semisymmetric designs other than semiplanes), etc.

3. Projective and affine planes

In contrast to Proposition to Proposition 2.1, it is not generally true that either $b(b(\mathscr{A})) = \mathscr{A}$ or $h(b(\mathscr{A})) = \mathscr{A}$. However, we might study these families in the hope of recognizing $\mathscr{A}$ from them. We have the following general result:

PROPOSITION 3.1. (i) *Let $\mathscr{A}$ be any clutter. If $S \in h(b(\mathscr{A}))$ then either $S \in \mathscr{A}$ or there exists $A \in \mathscr{A}$ with $A \cap S = \emptyset$. Hence $h(b(\mathscr{A})) \subseteq \mathscr{A} \cup b(b(\mathscr{A}))$.*

(ii) *Let $\mathscr{A}$ be any clutter with the property that, for all $A \in \mathscr{A}$ and all $a \in A$, there exists $B \in B(\mathscr{A})$ with $A \cap B = \{a\}$. Then $\mathscr{A} \subseteq h(b(\mathscr{A}))$. Hence $h(b(\mathscr{A})) = \mathscr{A} \cup b(b(\mathscr{A}))$.*

Proof. (i) Suppose that $S \in h(b(\mathscr{A}))$ and there is no set $A \in \mathscr{A}$ with $S \cap A = \emptyset$. Then S hits $\mathscr{A}$, and so S hits every member of $h(\mathscr{A})$ which contains a member of $\mathscr{A}$; that is, every element of $h(\mathscr{A}) \setminus b(\mathscr{A})$. But also S hits $b(\mathscr{A})$ by assumption; so S hits $h(\mathscr{A})$. Clearly $S \in H(h(\mathscr{A}))_{\min} = h(h(\mathscr{A}))$; so $S \in \mathscr{A}$, by Proposition 2.1. Thus, if $S \in h(b(\mathscr{A}))$ and $S \notin \mathscr{A}$, then S contains no $\mathscr{A}$-blocking set, and $S \in b(b(\mathscr{A}))$.

(ii) Clearly $\mathscr{A} \subseteq H(b(\mathscr{A}))$ with this assumption. As in Proposition 2.3, the hypothesis ensures that $\mathscr{A} \subseteq H(b(\mathscr{A}))_{\min} = h(b(\mathscr{A}))$. The final equality follows from this inclusion, (i), and the obvious $b(b(\mathscr{A})) \subseteq h(b(\mathscr{A}))$.

PROPOSITION 3.2. *Let $\mathscr{A}$ be the set of lines of a projective plane of order $n > 2$, or of an affine plane of order $n > 3$. Then $\mathscr{A}$ is the set of elements of $h(b(\mathscr{A}))$ of least cardinality; so* $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$.

Proof. The argument is similar for projective and affine planes. First, let $\mathscr{A}$ be a projective plane of order $n > 2$. Let L and M be lines; choose $x \in L \setminus M$, $y \in M \setminus L$, and $z \in N \setminus \{x, y\}$, where N is the line xy. Then $(L \setminus \{x\}) \cup (M \setminus \{z\}$ hits every line, and contains at most three points of any line except L or M; so it is a blocking set (clearly minimal). Since any line can play the role of N in this construction, the hypotheses of Proposition 3.1(ii) are satisfied, and $\mathscr{A} \subseteq h(b(\mathscr{A}))$.

Now take $S \in h(b(\mathscr{A}))$, $S \notin \mathscr{A}$. By Proposition 3.1(i), there is a line L of $\mathscr{A}$ disjoint from S.

CASE 1: There is a line $M \neq L$ with $|S \cap M| \leqslant 1$. Let y be a point of M such that $S \cap M \subseteq \{y\}$. For any $z \notin L \cup M$, let x be the intersection of L with $N = yz$. Then, as above, $(L \setminus \{x\}) \cup (M \setminus \{y\}) \cup \{z\}$ is in $b(\mathscr{A})$; since S contains no point of $L \setminus \{x\}$ or $M \setminus \{y\}$, we must have $z \in S$. Thus $|S| \geqslant n(n-1)$.

CASE 2: S contains at least two points of each line $M \neq L$. Choosing a point $x \notin L \cup S$, each of the $n+1$ lines through x contains at least two points of S, and so $|S| \geqslant 2(n+1)$.

In either case the result follows.

Now let $\mathscr{A}$ be an affine plane of order $n > 3$. We construct a blocking set as follows. Let L and M be parallel lines; choose $x \in L$, $y \in M$, and let N be the line xy. Then $B = L \cup M \cup N \setminus \{x, y\}$ is a blocking set. For any line T parallel to L but different from L and M, $|T \cap B| = 1$. Since T may be any line of the plane the hypotheses of Proposition 3.1 hold.

Again, take $S \in h(b(\mathscr{A}))$ with $S \notin \mathscr{A}$, and let L be a line disjoint from S.

CASE 1: There is a line M parallel to L with $|M \cap S| \leqslant 1$. Take $y \in M$ with $M \cap S \subseteq \{y\}$. Using the blocking set previously constructed, we see that each of the n lines through y other than M contains another point of S. So $|S| \geqslant n$. If $y \in S$, then $|S| \geqslant n+1$; so suppose that $M \cap S = \emptyset$. Now S is not a line parallel to M, so there exist two points of S lying on a line N which meets M. Repeating the argument with $y = M \cap N$, we see that $|S| \geqslant n+1$ in this case also.

CASE 2: S contains at least two points of each line parallel to L. Then $|S| \geqslant 2(n-1)$.

REMARK 1. The conditions on n are necessary; none of the three excluded planes has any blocking sets.

REMARK 2. Our first proof of the final assertion of Proposition 3.2 (obtained by F.M.) used a different argument. it was shown, by a fairly lengthy case analysis, that projective planes of order $n > 2$ and affine planes of order $n > 3$ share the following property:

(α) *Any set S of points, whose cardinality is equal to that of a line but which is not a line, is contained in a blocking set.*

Clearly any family $\mathscr{A}$ of sets of constant cardinality k which satisfies (α) has the further property that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$, since $\mathscr{A}$ is characterized as the family of k-sets contained in no member of $B(\mathscr{A})$.

PROBLEM. For which n and q does the family of lines in PG(n, q) (or AG(n, q)) have property (α)?

REMARK 3. Let $\mathscr{A}$ be a projective plane of order $n > 2$. Then, for any two lines $L, M \in \mathscr{A}$, the complement of $L \cup M$ is in $h(b(\mathscr{A}))$. (No blocking set is contained in $L \cup M$; but, for any $z \notin L \cup M$, the blocking set used in Proposition 3.2 is contained in $L \cup M\{z\}$.) This set falls under Case 1, and has cardinality $n(n-1)$. For $n = 3$, every element of $h(b(\mathscr{A})) \setminus \mathscr{A}$ has this form. In general, however, there are others: for example, if $n = 4$, the complement of $O \cup L$ is such a set, where O is a 6-arc and L an exterior line. This set falls under Case 2, and has cardinality $10 = 2(n+1)$. The lower bound for the cardinality of sets in $h(b(\mathscr{A})) \setminus \mathscr{A}$ can be improved to approximately $n^{3/2}$ by a more careful argument.

4. Projective and Affine Spaces

For $n > h > 0$ and q a prime power, we let $\mathrm{PG}_h(n,q)$ and $\mathrm{AG}_h(n,q)$ denote the families of h-spaces in $\mathrm{PG}(n,q)$ and $\mathrm{AG}(n,q)$ respectively. In this section, we show that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$ holds if $\mathscr{A} = \mathrm{PG}_h(n,q)$ or if $\mathscr{A} = \mathrm{AG}_h(n,q)$ and q is prime, provided that $B(\mathscr{A}) \neq \emptyset$. Our tools are theorems of Kantor and McDonough and of Mortimer asserting the maximality of $\mathrm{Aut}(\mathscr{A})$ in the symmetric or alternating group: if $\mathrm{Aut}(B(\mathscr{A}))$ were larger, it would be symmetric or alternating. So first we determine those clutters $\mathscr{A}$ for which $B(\mathscr{A}) \neq \emptyset$ and $\mathrm{Aut}(B(\mathscr{A}))$ is symmetric or alternating.

Note that Ramsey's theorem for finite projective and affine spaces implies that, given h and q, blocking sets for $\mathrm{PG}_h(n,q)$ or $\mathrm{AG}_h(n,q)$ exist for only finitely many values of n (Mazzocca and Tallini [7]).

We let $\binom{X}{k}$ denote the family of all k-element subsets of the set X.

PROPOSITION 4.1. *Let $\mathscr{A}$ be a clutter on X, with $|X| = n$.*

(i) *The following are equivalent:*

(a) *for some $k \leqslant n$, $\binom{X}{k} \subseteq B(\mathscr{A})$.*

(b) *for all $A \in \mathscr{A}$, $|A| \geqslant \frac{1}{2}n + 1$.*

(ii) *The following are equivalent:*

(a) *$B(\mathscr{A}) \neq \emptyset$ and, for every $k \leqslant n$, either $\binom{X}{k} \subseteq B(\mathscr{A})$ or $\binom{X}{k} \cap B(\mathscr{A}) = \emptyset$;*

(b) *for some* $l \geqslant \frac{1}{2}n + 1, \mathscr{A} = \binom{X}{l}$.

Proof. (i) If (b) holds, then $\binom{X}{k} \subseteq B(\mathscr{A})$ for the unique k satisfying $\frac{1}{2}n \leqslant k < \frac{1}{2}n + 1$. Conversely, suppose that (a) holds. Then, for any $A \in \mathscr{A}$, we have $|A| \geqslant k + 1$ (otherwise A is contained in a k-set) and $|A| \geqslant n - k + 1$ (otherwise A is disjoint from a k-set). So $2|A| \geqslant n + 2$.

(ii) Clearly (b) implies (a). Suppose that (a) holds. By (i), every set $A \in \mathscr{A}$ has $|A| \geqslant \frac{1}{2}n + 1$. Hence an element $B \in h(\mathscr{A})$ satisfies $|B| < \frac{1}{2}n + 1$, and so B cannot contain an element of $\mathscr{A}$; that is, $b(\mathscr{A}) = h(\mathscr{A})$. Moreover, $b(\mathscr{A})$ is the set of elements of minimal cardinality in $B(\mathscr{A})$, that is, $b(\mathscr{A}) = \binom{X}{k}$ for some k. Then $\mathscr{A} = h(h(\mathscr{A})) = \binom{X}{l}$, where $l = n - k + 1$.

COROLLARY 4.2. *If* $\mathscr{A}$ *is a clutter on* X *such that* $B(\mathscr{A}) \neq \emptyset$ *and* $\mathrm{Aut}(\mathscr{A})$ *is a maximal proper subgroup of* $\mathrm{Sym}(X)$ *or* $\mathrm{Alt}(X)$, *then* $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$.

Proof. If not, then $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Sym}(X)$ or $\mathrm{Alt}(X)$; but then $\mathrm{Aut}(\mathscr{A}) = \mathrm{Sym}(X)$, since condition (a) of Proposition 4.1(ii) holds.

PROPOSITION 4.3. *Suppose that* $n > h > 0$ *and* q *is a prime power; let* $\mathscr{A} = \mathrm{PG}_h(n, q)$. *If* $B(\mathscr{A}) \neq \emptyset$, *then* $\mathit{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$.

Proof. We have $\mathrm{Aut}(\mathscr{A}) = \mathrm{P\Gamma}L(n + 1, q)$; the maximality of this group in the symmetric or alternating group was shown by Kantor and McDonough [5].

REMARK. Unlike our earlier results, this proof is non-constructive; it gives no indication of how to reconstruct $\mathscr{A}$ from $B(\mathscr{A})$. It is possible that, when n is close to the Ramsey number (beyond which blocking sets fail to exist), the procedure for reconstructing $\mathscr{A}$ from $B(\mathscr{A})$ becomes arbitrarily complicated.

Mortimer [8] showed that the only groups of permutations properly containing the affine group $\mathrm{A\Gamma L}(n, q)$, other than the symmetric and alternating groups, are affine groups $\mathrm{A\Gamma L}(nk, r)$, where k and r satisfy $r^k = q$, $k > 1$, under the natural identification of the point sets of $\mathrm{AG}(n, q)$ and $\mathrm{AG}(nk, r)$ given by restricting scalars. Suppose that $\mathscr{A} = \mathrm{AG}_h(n, q)$ and that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{A\Gamma L}(nk, r)$. Then every h-blocking set in $\mathrm{AG}(n, q)$ must block all images of an h-flat under $\mathrm{A\Gamma L}(nk, r)$; that is, all hk-flats in $\mathrm{AG}(nk, r)$. Hence, we have the following result:

PROPOSITION 4.4. *Suppose that* n, q, h *are given. Assume that* h*-blocking* *sets in* AG(n,q) *exist and that, whenever* $q = r^k$ *with* $k > 1$, *there exists an h-blocking set in* AG(n,q) *which is not an hk-blocking set in* AG(nk,r) (*with the natural identification*). *Then, if* $\mathscr{A} = \mathrm{AG}_h(n,q)$, *we have* $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$. *In particular, this holds if q is prime* (*and* $B(\mathscr{A}) \neq \emptyset$).

In the next section, we construct some examples of line-blocking sets for which the hypothesis of Proposition 4.4 holds.

5. Some line-blocking sets in affine spaces

LEMMA. 5.1. *Suppose that* $x \geqslant 1$ *and that S is a subset of* AG(m,q) *with the property that, for any line L,* $|L \cap S| \geqslant 2x$ *and* $|L \setminus S| \geqslant 2x$. *Then there is a subset S′ of* AG$(m+1,q)$ *with the property that, for any line L,* $|L \cap S'| \geqslant x$ *and* $|L \setminus S'| \geqslant x$.

Proof. Let C be a subset of GF(q) with $|C| = x$. Now set $S' = \{(\mathbf{x},t) \mid \mathbf{x} \in S, t \in \mathrm{GF}(q) \setminus C, \text{ or } \mathbf{x} \in \mathrm{AG}(m,q) \setminus S, t \in C\}$. Let L be any line of AG$(m+1,q)$. There are three cases:

(i) The $(m+1)st$ coordinate of points on L is constant. Then L is contained in a hyperplane $H = \{(\mathbf{x},c) \mid \mathbf{x} \in \mathrm{AG}(m,q)\}$ and $H \cap S' = S$ or $H \setminus S$ according as $c \notin C$ or $c \in C$. Thus $|L \cap S'| \geqslant 2x$ and $|L \setminus S'| \geqslant 2x$.

(ii) The first m coordinates of points on L are constant. Then, clearly, either $|L \cap S'| = |C|$ or $|L \setminus S'| = |C|$, according as the point represented by the first m coordinates of L is not or is in S.

(iii) Neither of the above. Then $L = \{(\mathbf{x}(t),t) | t \in \mathrm{GF}(q)\}$ where $\mathbf{x}$ is a function from GF(q) to AG(m,q) which is the parametric form of a line L^0. Let

$$D = \{t \in \mathrm{GF}(q) \mid \mathbf{x}(t) \in S\},$$

so that $2x \leqslant |D| \leqslant q - 2x$. Then

$$\{t \in \mathrm{GF}(q) \mid (\mathbf{x}(t),t) \in S'\} = C \triangle D,$$

and $x \leqslant |C \triangle D| \leqslant q - x$, as required.

(The case $x = 1$ of this result has been proved by Tallini [9, XXI].)

COROLLARY 5.2. *Suppose that there is a subset S of* AG(m,q) *with the property that, for any line L,* $|L \cap S| \geqslant 2^d$ *and* $|L \setminus S| \geqslant 2^d$. *Then there is a line-blocking set in* AG$(m+d,q)$.

EXAMPLE 1. If $q \geqslant 2^n$, then there is a line-blocking set in AG(n,q). (We apply the corollary with $d = n-1$, $m = 1$; any set of 2^{n-1} points in AG$(1,q)$

satisfies the hypothesis.) Note that, for $n = 2$, this example is the symmetric difference of two parallel lines and a line from a different parallel class, which we used in our earlier discussion of affine planes.

EXAMPLE 2. Choose a random subset S of $AG(n, q)$, by including points independently with probability $\frac{1}{2}$. The probability that a given line L is contained in or disjoint from S is $1/2^{q-1}$; so the expected number of such lines is $q^{n-1}(q^n - 1)/(q-1)2^{q-1}$. If $2^{q-1} > q^{n-1}(q^n - 1)/(q-1)$, then the expected number is less than one, and so, for some choice of S, no line is contained in or disjoint from S; that is, S is a line-blocking set.

This example is better than the preceding one for $n \geqslant 6$; it requires q to be greater than a function of n which grows a little faster than $n \log n$. However, a further improvement can be made by combining the methods.

EXAMPLE 3. Given d, choose a random subset S of $AG(n-d, q)$ as above. The probability that a line L satisfies $|L \cap S| < 2^d$ or $|L \setminus S| < 2^d$ is $(2^{q-1}/\sum_{i=0}^{2d-1}\binom{q}{i})^{-1}$. Thus if

$$2^{q-1} \Bigg/ \sum_{i=0}^{2d-1} \binom{q}{i} > q^{n-d-1}(q^{n-d} - 1)/(q-1),$$

then there is a choice of S for which no such line exists, and hence (by Corollary 5.2) a line-blocking set in $AG(n, q)$.

Table I lists the least integer values of q satisfying the various inequalities for different values of n. In general, Example 3 with $d = 2$ gives the best bound.

TABLE I

	n							
	3	4	5	6	7	8	9	10
Ex. 1	8	16	32	64	128	256	512	1024
Ex. 2	18	31	45	61	76	93	110	127
Ex. 3, $d = 1$	12	25	38	53	69	85	101	119
Ex. 3, $d = 2$	8	21	35	49	65	81	98	115
Ex. 3, $d = 3$	—	16	34	51	68	85	102	120
Ex. 3, $d = 4$	—	—	32	59	79	99	118	138

EXAMPLE 4. By random search, we found subsets of affine planes which give (using Corollary 5.2) line-blocking sets in the following affine spaces: $AG(3, 7)$, $AG(4, 13)$, $AG(5, 31)$, $AG(5, 29)$, $AG(6, 47)$. For example, the

following subset of AG(2, 7) meets every line in at least two and at most five points: (0, 0), (0, 4), (1, 3), (1, 4), (2, 0), (2, 3), (3, 0), (3, 2), (3, 3), (3, 4), (3, 6), (4, 1), (4, 3), (4, 4), (4, 5), (4, 6), (5, 0), (5, 2), (5, 3), (5, 5), (5, 6), (6, 0), (6, 1).

EXAMPLE 5. PG(2, 25) contains a family of 21 pairwise disjoint Baer subplanes (the orbit of one under a Singer cycle). (See, for example, Hirschfeld [4, p. 92].) Let S^0 be the union of 9 of these subplanes. Then S^0 meets every line in 9 or 14 points. Removing a line at infinity, we find a subset S of AG(2, 25) meeting every line in at least 8 and at most 14 points, and so (using Corollary 5.2) a line-blocking set in AG(5, 25).

It is known that no line-blocking set exists in AG$(3, q)$ for $q \leqslant 4$. (For $q \leqslant 3$, there is no blocking set in AG$(2, q)$. For $q = 4$, the result has been proved by Brown [2] and by Tallini [9]. Thus, in three-dimensional affine space, only for $q = 5$ is the existence of line-blocking sets in doubt.

We saw in Section 4 that, if q is prime, the existence of a line-blocking set in AG(n, q) guarantees that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$, where $\mathscr{A}$ is the set of lines; but, in general, more is required: whenever $q = r^k$, $k > 1$, we need a line-blocking set in AG(n, q) which is not a k-blocking set in AG(nk, r). We note first that Example 1 with $n = 2$ has this property. For the set is

$$S = \{(x, y) \mid x = 0 \text{ or } x = 1 \text{ or } y = 0\} \setminus \{(0, 0), (1, 0)\}.$$

Restricting scalars, we represent AG$(2, q)$ as $V \oplus V$, where V is a k-dimensional space over GF(r). Choose proper subspaces U_1, U_2 of V with $\dim U_1 + \dim U_2 = \dim V$ and $1 \in U_1$; then select $a_1 \notin U_1$ and $a_2 \notin U_2$. The set

$$W = \{(x_1 + a_1, x_2 + a_2) \mid x_1 \in U_1, x_2 \in U_2\}$$

is an affine k-flat over GF(r) which is disjoint from S.

Now observe that, in any example constructed using Corollary 5.2 with $d \geqslant 2$ (and so, in particular, in Example 3 with $d \geqslant 2$, and in Example 1 with $n \geqslant 2$), there exist planes π (obtained by holding all but the last two coordinates constant) for which $\pi \cap S$ is the blocking set of Example 1 with $n = 2$. So all these examples satisfy the condition of Proposition 4.4 as well.

In particular, if $\mathscr{A}$ is the set of lines in AG$(3, q)$, we have shown that $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$ for all prime powers q except $q \leqslant 4$ (where $B(\mathscr{A}) = \emptyset$) and possibly $q = 5$ (where the question is equivalent to the existence of blocking sets).

REMARK. The argument of Example 2 shows that line-blocking sets in PG(n, q) exist whenever $2^q > (q^{n+1} - 1)(q^n - 1)/(q - 1)(q^2 - 1)$. Note also that the union of line-blocking sets in AG(n, q) and PG$(n - 1, q)$ (the hyperplane at infinity) is a line-blocking set in $PG(n, q)$. Furthermore, if line-blocking sets exist, then $\mathrm{Aut}(B(\mathscr{A})) = \mathrm{Aut}(\mathscr{A})$, where $\mathscr{A}$ is the set of lines (Proposition 4.3). Similarly, the argument yields h-blocking sets with $h > 1$.

For further results and information on blocking sets, we refer the reader to [1], [9] and [10].

6. Linear spaces

The simplest clutter $\mathscr{A}$ for which $B(\mathscr{A}) \neq \emptyset$ and $\mathrm{Aut}(B(\mathscr{A})) \neq \mathrm{Aut}(\mathscr{A})$ is the family

$$\mathscr{A} = \{\{1,2\}, \{2,3\}, \{3,4\}\};$$

we have $B(\mathrm{A}) = \{\{1,3\}, \{2,4\}\}$, so $|\mathrm{Aut}(\mathrm{A})| = 2$, $|\mathrm{Aut}(B(\mathrm{A}))| = 8$. We construct linear spaces by encoding this example. (A *linear space* is a family $\mathscr{A}$ of subsets of X, called *lines*, such that any line contains at least two points, while any two points lie in a unique line.)

PROPOSITION 6.1. *There are infinitely many linear spaces $\mathscr{A}$ for which $B(\mathscr{A}) \neq \emptyset$ and $\mathrm{Aut}(B(\mathscr{A})) \neq \mathrm{Aut}(\mathscr{A})$.*

Proof. Take a linear space $(x, \mathscr{A})$ containing a blocking set B with the following properties:

(i) any line contains at least six points altogether, and at least four points outside B;

(ii) there is a point $x_2 \in B$ lying on at least two tangents L_1, L_2 to B, and a point $x_4 \in B$ lying on a tangent L_3 which intersects L_2 (at a point x_3, say).

(A line L is a *tangent* to B if $|L \cap B| = 1$.)

For example, take $(X, \mathscr{A})$ to be $PG(2, q^2)$, $q > 2$, and let B be a Baer subplane.

Let x_1 be any point of L_1 other than x_2. Now let

$$x' = (x \setminus (L_1 \cup L_2 \cup \mathrm{L}_3)) \cup \{x_1, x_2, x_3, x_4\},$$

and $\mathscr{A}'$ the linear space induced on x' by $\mathscr{A}$; that is,

$$\mathscr{A}' = \{L \cap X' \mid L \in \mathscr{A}, |L \cap X'| \geqslant 2\}.$$

Now we have:

(i) The only lines of $\mathscr{A}'$ which have just two points are $\{x_1, x_2\}$, $\{x_2, x_3\}$ and $\{x_3, x_4\}$; for any line L other than L_1, L_2 or L_3 contains at most three points of $L_1 \cup L_2 \cup L_3$.

(ii) B is a blocking set for $\mathscr{A}'$; for clearly B meets each line of $\mathscr{A}'$ but, as in (i), any line of $\mathscr{A}'$ contains a point outside B.

(iii) For any blocking set B', either

$$B' \cap \{x_1, \ldots, x_4\} = \{x_1, x_3\}, \quad \text{or}$$
$$B' \cap \{x_1, \ldots, x_4\} = \{x_2, x_4\}.$$

Define a bijection f of X' by

$$f(x_1) = x_3,$$
$$f(x_3) = x_1,$$
$$f(x) = x \quad \text{for all} \quad x \neq x_1, x_3$$

By (iii), $f \in \mathrm{Aut}(B(\mathscr{A}))$. But $f \in \mathrm{Aut}(\mathscr{A})$, since the image of the two-point line $\{x_3, x_4\}$ is not a line.

References

1. Berardi, L., Beutelspacher A., and Eugeni, F., 'On the $(s, t; h)$ – Blocking Sets in Finite Projective and Affine Spaces', *Atti Sem. Mat. Fis. Univ. Modena* **32** (1983), 130–157.
2. Brown, T. C., 'Monochromatic Affine Lines in Finite Vector Spaces', *J. Com. Theory (A)*, **39** (1985), 35–41.
3. Edmonds, J. and Fulkerson, D. R., 'Bottleneck Extrema', *J. Comb. Theory* **8** (1970), 299–306.
4. Hirschfeld, J. W. P., *Projective Geometries over Finite Fields*, Oxford Univ. Press, Oxford, 1979.
5. Kantor, W. M. and McDonough, T. P., 'On the Maximality of $P\Gamma L(d, q)$, $d > 2$', *J. London Math. Soc.* (2) **8** (1974), 426.
6. Mazzocca, F., 'Some Results on Blocking-Sets', Announcements at conferences *Combinatorics '84*, Bari, 1984, and *Finite Geometries*, Oberwolfach, 1985.
7. Mazzocca, F. and Tallini, G., 'On the Nonexistence of Blocking Sets in $PG(n, q)$ and $AG(n, q)$' (to appear, in *Simon Stevin*).
8. Mortimer, B., 'Permutation Groups Containing Affine Groups of the Same Degree', *J. London Math. Soc.* **15** (1977), 445–455.
9. Tallini, G., 'k-Insiemi e blocking-sets in $PG(r, q)$ e in $AG(r, q)$', Quaderno n. 1, *Sem. Geom. Comb., Ist. Mat. Appl.*, Univ. L'Aquila, 1982.
10. Tallini, G., 'Blocking-Sets nei sistemi di Steiner e d-blocking sets in $PG(r, q)$ ed $AG(r, q)$', Quaderno n. 3, *Sem. Geom. Comb., Ist. Mat. Appl.*, Univ. L'Aquila, 1983.

Author's addresses:

Peter J. Cameron,
Department of Mathematics
Merton College,
Oxford OX1 4JD,
England

Francesco Mazzocca,
Dipartimento di Matematica e Applicazioni,
Universita di Napoli,
Via Mezzocannone n. 8,
80134 Napoli,
Italy

(Received, July 26, 1985)