Can. J. Math., Vol. XXXI, No. 1, 1979, pp. 211–224

INDICATOR SETS IN AN AFFINE SPACE OF ANY DIMENSION

F. A. SHERK

1. Introduction. It is well known that a translation plane can be represented in a vector space over a field F, where F is a subfield of the kernel of a quasifield which coordinatizes the plane [**1**; **2**; **4**, p.220; **10**]. If Π is a finite translation plane of order q^r ($q = p^n$, p any prime), then Π may be represented in $V_{2r}(q)$, the vector space of dimension $2r$ over $GF(q)$, as follows:

(i) The *points* of Π are the vectors in $V = V_{2r}(q)$.

(ii) The *lines* of Π are

(a) A set $\mathscr{S}$ of $q^r + 1$ mutually disjoint r-dimensional subspaces of V.

(b) All translates of $\mathscr{S}$ in V.

(iii) Incidence is inclusion.

$\mathscr{S}$ is called a *congruence* or a *spread*. In terms of the projective $(2r - 1)$-space $\Sigma = PG(2r-1, q)$, whose points, lines, ..., i-flats are $1, 2, \ldots, (i+1)$-dimensional subspaces respectively of V, $\mathscr{S}$ is a set of mutually skew $(2r-1)$-flats. Thus $\mathscr{S}$ may be interpreted either as a set of $q^r + 1$ mutually disjoint r-dimensional subspaces in V or as a set of $q^r + 1$ mutually disjoint $(r - 1)$-flats in Σ.

Any given spread $\mathscr{S}$ completely determines some translation plane Π, and therefore translation planes can be studied through spreads. The approach of this paper is to represent $\mathscr{S}$ in V (or in Σ) by a set $\mathscr{I}$ of q^r points in $AG(r, q^r)$, the affine space of dimension r over $GF(q^r)$. $\mathscr{I}$ is called an *indicator set*, and it must satisfy a certain characteristic property, to be described presently. We then study the spread $\mathscr{S}$, and therefore the translation plane Π, by observing the properties of the indicator set $\mathscr{I}$.

This approach has been used effectively in the case $r = 2$ by Bruen [**3**] and by Sherk and Pabst [**13**]. The generalization for $r > 2$ which we develop here was suggested to me by T. G. Ostrom, who also commented that it would be particularly useful if this approach were to throw light on cases in which r is odd. Consequently, in what follows, we concentrate on the cases in which $q = p$, a prime, and $r = 3$. Where it is convenient to do so, however, we deal in greater generality.

After necessary preliminary definitions, we develop, in Theorem 1, a necessary and sufficient condition for two indicator sets to define isomorphic translation planes. This is then easily adapted to yield a description of symmetries which an indicator set may possess (Theorem 2). Such symmetries are impor-

Received October 8, 1977 and in revised form February 21, 1978.

tant for their close relationship to the collineations of the corresponding translation plane.

Section 6 is devoted to a study of permutations in the indicator r-space. We find the necessary and sufficient condition for a permutation to be a collineation (Theorem 3).

Section 7 uses the foregoing work to give explicit information on the Desarguesian plane and the André planes. This includes the nature of a representative indicator set, and some indication of the extent of the class of André planes. Section 8 deals with semifield planes of order p^3, and exhibits an example of a semifield plane indicator set in the case $p = 3$. This example is shown in section 9 to have an interesting connection with Hering's plane of order 27.

Throughout the paper some more or less standard notation will be used without comment. The greatest common divisor of two integers a and b will be denoted by (a, b). We shall denote the cardinality of a finite set S by $|S|$, and occasionally also use the same symbol, "$|\ |$", to denote a determinant. The symbol $\langle A, B, C \ldots \rangle$ will denote the group generated by $A, B, C, \ldots$. Finally, if H is a subgroup of a group G, then $N(H)$ will denote the normalizer of H in G.

The author is grateful to the referee for many helpful comments.

2. The indicator r-space. Consider the vector space $V = V_{2r}(q)$ $(q = p^n)$. As already noted, the points of a translation plane Π, the kernel of whose coordinatizing quasifield contains $F = \mathrm{GF}(q)$, can be identified with the vectors in V. After fixing a suitable basis in V, we can denote these vectors in matrix form by the order pairs $(X\ Y)$, where X and Y are $1 \times r$ matrices over F. The set $\{(0\ Y)\}$, where 0 is the zero matrix and Y ranges over all $1 \times r$ matrices over F, is an r-dimensional subspace of V, as is the set $\{(X\ XM)\}$, where M is any given $r \times r$ matrix over F [**10**, p.5, 51]. We denote the former r-space by the matrix equation $X = 0$, and the latter by $Y = XM$.

It is obvious from inspection that $Y = XM$ is disjoint from $X = 0$. Conversely,

LEMMA 1. *Every r-dimensional subspace in V that is disjoint from $X = 0$ can be expressed in the form $Y = XM$ for one and only one choice of M.*

Proof. Any r-space in V is the solution set $(X\ Y)$ of a set of r simultaneous linear equations

$$(2.1)\quad \sum_{i=1}^{r} (\alpha_{ij}x_i + \beta_{ij}y_i) = 0 \quad (j = 1, 2, \ldots, r)$$

in the $2r$ variables $(x_1, \ldots, x_r, y_1, \ldots, y_r) = (X\ Y)$. As a matrix equation, (2.1) is

$$(2.2)\quad XP + YQ = 0,$$

where P and Q are $r \times r$ matrices over F. Now if Q is singular, then there is a matrix $Y_1 \neq 0$ such that $Y_1 Q = 0$. Since $0P + Y_1 Q = 0$, the r-space defined by (2.2) contains the vector $(0\ Y_1) \neq (0\ 0)$, and therefore has non-trivial intersection with $X = 0$. Hence if an r-space l is disjoint from $X = 0$, and if (2.2) is the equation of l, then Q is non-singular. Thus we have $0 = 0Q^{-1} = (XP + YQ)Q^{-1} = XPQ^{-1} + Y$, and so l is given by the equation $Y = XM$, where $M = -PQ^{-1}$. It is obvious that two r-spaces represented by $Y = XM_1$ and $Y = XM_2$ respectively are identical if and only if $M_1 = M_2$.

Lemma 1 establishes a 1-1 correspondence between the set $\mathscr{L}$ of r-spaces in V disjoint from $X = 0$ and the set $\mathscr{M}$ of $r \times r$ matrices over $\mathrm{GF}(q)$.

Next let us consider the affine space $\mathscr{A} = \mathrm{AG}(r, q^r)$ of dimension r over $\mathrm{GF}(q^r)$, which can be described as follows: Let $f(x) = x^r - \rho_{r-1}x^{r-1} - \rho_{r-2}x^{r-2} - \ldots - \rho_0$ be an irreducible polynomial over $\mathrm{GF}(q)$, and let t be a primitive root of $f(x)$ in $\mathrm{GF}(q^r)$ (regarded as an extension field of $\mathrm{GF}(q)$). Then each element of $\mathrm{GF}(q^r)$ is uniquely denoted by the polynomial $\alpha_0 + \alpha_1 t + \ldots + \alpha_{r-1}t^{r-1}$, where $\alpha_0, \ldots, \alpha_{r-1} \in \mathrm{GF}(q)$ and $t^r = \rho_0 + \rho_1 t + \ldots + \rho_{r-1}t^{r-1}$.

Notation. Elements of $\mathrm{GF}(q)$ and of $\mathrm{GF}(q^r)$ will be denoted by small Greek letters: $\alpha, \beta, \gamma, \ldots$, and small Latin letters: $a, b, c, \ldots$, respectively.

Any point of $\mathscr{A}$ is identified by the coordinates

$$(\lambda_{11} + \lambda_{21}t + \ldots + \lambda_{r1}t^{r-1}, \ \ldots, \lambda_{1r} + \lambda_{2r}t + \ldots + \lambda_{rr}r^{r-1}),$$

which, expressed as a $1 \times r$ matrix, is the product JM, where $J = (1\ t\ t^2 \ldots t^{r-1})$ and

$$M = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1r} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2r} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \lambda_{r1} & \lambda_{r2} & \cdots & \lambda_{rr} \end{pmatrix}.$$

M of course is an $r \times r$ matrix over $\mathrm{GF}(q)$, and uniquely determines the point in $\mathscr{A}$. Thus we have a 1-1 correspondence between the set $\mathscr{M}$ of $r \times r$ matrices over $\mathrm{GF}(q)$ and the points of $\mathscr{A}$. Recalling the above correspondence between $\mathscr{L}$ and $\mathscr{M}$, we establish a 1-1 correspondence between the points of $\mathscr{A}$ and the r-spaces of $\mathscr{L}$ in V. Thus each point of $\mathscr{A}$ represents, or *indicates* an r-space in $\mathscr{L}$.

Definition. The affine r-space $\mathscr{A} = \mathrm{AG}(r, q^r)$ is called the *indicator r-space* of $\mathscr{L}$, the set of r-dimensional subspaces $Y = XM$ of V.

It is both convenient and suggestive of our use of indicator r-spaces to denote a point JM of $\mathscr{A}$ simply by the matrix M. Thus for example the point J itself is denoted by the $r \times r$ identity matrix I. There is a rough analogy between this convention and the well-known practice of denoting the points of the Argand plane by complex numbers.

We now proceed to establish the fundamental relationship between the r-spaces of $\mathscr{L}$ and the points of $\mathscr{A}$:

LEMMA 2. *Two r-spaces $Y = XM_1$ and $Y = XM_2$ in $\mathscr{L}$ are disjoint if and only if $M_1 - M_2$ is non-singular.*

Proof. Suppose that $Y = XM_1$ and $Y = XM_2$ have a common vector $(X'\ Y')$ where $X' \neq 0$. Then $X'M_1 = X'M_2$, so that $X'(M_1 - M_2) = 0$; thus $M_1 - M_2$ is singular. The argument is reversible.

Definitions. Any n elements $a_1, a_2, \ldots, a_n$ of $\mathrm{GF}(q^r)$ are *linearly dependent* over $\mathrm{GF}(q)$ if there exist n elements $\lambda_1, \lambda_2, \ldots, \lambda_n$ of $\mathrm{GF}(q)$, not all zero, such that $\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n = 0$. The elements are *linearly independent* over $\mathrm{GF}(q)$ if they are not linearly dependent.

Any line in the indicator r-space $\mathscr{A}$ is determined by two distinct points on it. If a line l contains the distinct points $A = (a_1, a_2, \ldots, a_r)$ and $B = (b_1, b_2, \ldots, b_r)$, then any point on l, except B, is given by the coordinates $(a_1 + k(b_1 - a_1), a_2 + k(b_2 - a_2), \ldots, a_r + k(b_r - a_r))$ for some $k \in \mathrm{GF}\ (q^r)$. Using the term of classical geometry, we call the ordered set of elements $\{b_1 - a_1, b_2 - a_2, \ldots, b_r - a_r\}$ the set of *direction numbers* of l. Up to homogeneity, the direct numbers of l are the same for any choice of A and B on l.

LEMMA 3. *Two r-spaces $Y = XM_1$ and $Y = XM_2$ in $\mathscr{L}$ are disjoint if and only if the direction numbers of the line joining the points M_1 and M_2 in $\mathscr{A}$ are linearly independent over* $\mathrm{GF}(q)$.

Proof. By Lemma 2, $Y = XM_1$ and $Y = XM_2$ are disjoint if and only if the matrix $M_1 - M_2$ is non-singular. The line in $\mathscr{A}$ which joins the points M_1 and M_2 has direction numbers $\{JC_1, \ldots, JC_r\}$, where $J = (1\ t\ t^2\ \ldots\ t^{r-1})$, as before, and $C_1, \ldots, C_r$ are the column matrices of $M_1 - M_2$. $M_1 - M_2$ is non-singular if and only if its column matrices (considered as vectors over $\mathrm{GF}(q)$) are linearly independent. This establishes Lemma 3.

Definition. Two points M_1 and M_2 in $\mathscr{A}$ are *compatible* if the corresponding r-spaces $Y = XM_1$ and $Y = XM_2$ in $\mathscr{L}$ are disjoint. Otherwise M_1 and M_2 are *incompatible.*

Thus by Lemma 3, M_1 and M_2 are compatible if and only if the direction numbers of the line M_1M_2 are linearly independent over $\mathrm{GF}(q)$.

3. Spread sets and indicator sets. Let $\mathscr{S}$ be a spread in V. By suitable choice of basis in V, we may assume that one of the $q^r + 1$ components of $\mathscr{S}$ is the r-dimensional subspace $X = 0$. The other components are then

r-subspaces $\{Y = XM_i\}$ $(i = 0, 1, \ldots, q^r - 1)$ in $\mathscr{L}$, and are mutually disjoint. The set of matrices

(3.1) $S = \{M_0, M_1, \ldots, M_{q^r-1}\}$

is called a *spread set* [**2**, **4**; p. 220], and has the property that $M_i - M_j$ $(i, j = 0, 1, \ldots, q^r - 1; i \neq j)$ is non-singular. The set S may also be viewed as a set

(3.2) $\mathscr{I} = \{M_0, M_1, \ldots, M_{q^r-1}\}$

of q^r points in the indicator r-space $\mathscr{A}$. We call $\mathscr{I}$ the *indicator set* of the spread $\mathscr{S}$. By Lemma 3, $\mathscr{I}$ has the characteristic property that the line joining any two points M_i and M_j has direction numbers which are linearly independent over $\mathrm{GF}(q)$.

An indicator set consists of q^r points, representing all but one of the $q_r + 1$ components of the spread in V. The component not represented is the subspace $X = 0$. From the point of view of determining a plane from a given indicator set, this blemish presents no difficulties. However, it does complicate the isomorphism problem (see Section 4), and can be removed by the following process: Add to the indicator r-space $\mathscr{A}$ a single ideal point, denoted by the symbol ∞, in the same manner in which an ideal point is added to a Euclidean r-space to form an inversive r-space. ∞ has the property that it lies on every line of $\mathscr{A}$. Let $\mathscr{A}^*$ denote $\mathscr{A} \cup \{\infty\}$.

Definition. An *augmented indicator set* $\mathscr{I}^*$ in $\mathscr{A}^*$ is the union of an indicator set $\mathscr{I}$ in $\mathscr{A}$, and the point ∞.

Now $|\mathscr{I}^*| = q^r + 1$ and there is a 1-1 correspondence between the points of $\mathscr{I}^*$ and the components of the spread $\mathscr{S}$ indicated by $\mathscr{I}$.

4. Isomorphism and equivalence of indicator sets. In the remainder of this paper, we shall let $q = p$ (p a prime) so that $F = \mathrm{GF}(q) = \mathrm{GF}(p)$ is a prime field. This restriction, without which some of the arguments following would need qualification, does not cut out any translation planes from consideration. It only eliminates some indicator set representations of some planes, forcing a higher value of r.

We noted in the proof of Lemma 1 that any r-dimensional subspace in V is the set of vectors $(X\ Y)$ for which $XP + YQ = 0$, with given fixed $r \times r$ matrices P and Q. It is easy to show that $\mathrm{GL}(2r, p)$, the group of all non-singular linear transformations in V, is transitive on the set of all r-dimensional subspaces, and this is why we lose no generality in always choosing a spread $\mathscr{S}$ that has the r-space $X = 0$ as one of its components. The linear transformations may be represented by non-singular matrices in the block form

$$\begin{pmatrix} A & C \\ B & D \end{pmatrix},$$

where A, B, C, and D are $r \times r$ matrices, and where

$$\begin{vmatrix} A & C \\ B & D \end{vmatrix} \neq 0.$$

A linear transformation

$$\Gamma = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

may correspond to a permuation of points in $\mathscr{A}^* = \mathscr{A} \cup \{\infty\}$. Clearly this will be true if and only if Γ fixes the subset $\mathscr{L}^* = \mathscr{L} \cup \{X = 0\}$ of r-spaces in V. But Γ may also carry a subset of $\mathscr{L}^*$ (a spread, for example) onto another subset of $\mathscr{L}^*$ without actually fixing $\mathscr{L}^*$. In this case, a set of points in $\mathscr{A}^*$ is carried onto another set of points in $\mathscr{A}^*$ by some mapping induced by Γ in $\mathscr{A}^*$ which does not necessarily include images for all the points of $\mathscr{A}^*$. For convenience, we call this mapping a *partial permutation* of $\mathscr{A}$.

Now let $\mathscr{S}_1$ and $\mathscr{S}_2$ be any two spreads in V, both containing the component $X = 0$. Let Π_1 and Π_2 be the translation planes defined by $\mathscr{S}_1$ and $\mathscr{S}_2$. Now it can be shown that Π_1 and Π_2 are isomorphic if and only if there is a non-singular linear transformation Γ in V taking $\mathscr{S}_1$ onto $\mathscr{S}_2$ [**7**, p.82; **8**, p.486]. If $\mathscr{I}_1^*$ and $\mathscr{I}_2^*$ are the corresponding augmented indicator sets in $\mathscr{A}^*$, then Π_1 and Π_2 are isomorphic if and only if there is a partial permutation in $\mathscr{A}^*$ taking $\mathscr{I}_1^*$ onto $\mathscr{I}_2^*$.

Definition. Two indicator sets $\mathscr{I}_1$ and $\mathscr{I}_2$ are *equivalent* if the corresponding planes Π_1 and Π_2 are isomorphic.

To be more specific, let $\mathscr{I}_1^*$ and $\mathscr{I}_2^*$ be the sets of points $\{\infty \cup M_i\}$ and $\{\infty \cup N_i\}$ $(i = 0, 1, \ldots, p^r - 1)$ respectively in $\mathscr{A}^*$. These correspond to the spreads $\mathscr{S}_1 = \{(0\ Y) \cup (X\ XM_i)\}$ and $\mathscr{S}_2 = \{(0\ Y) \cup (X\ XN_i)\}$ of $\mathscr{L}^*$ in V respectively. $\mathscr{I}_1$ and $\mathscr{I}_2$ are equivalent if and only if there is a linear transformation

$$\Gamma = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$$

of V taking $\mathscr{S}_1$ onto $\mathscr{S}_2$. Therefore

$$(0 \quad Y)\begin{pmatrix} A & C \\ B & D \end{pmatrix} = (YB \quad YD) \in \mathscr{S}_2.$$

Hence $(YB\ YD) = (0\ Y)$, or else $(YB\ YD) = (X\ XN_i)$ for some value of i. It follows that either $B = 0$ or else B is non-singular (since if $B \neq 0$ then YB cannot be 0 for any value of $Y \neq 0$). In the latter case, $(YB\ YD) = (YB \quad YBB^{-1}D) = (X\ XB^{-1}D) = (X\ XN_i)$, so that $B^{-1}D = N_i$ for some i. More generally,

$$\begin{aligned}(X \quad XM_i)\begin{pmatrix} A & C \\ B & D \end{pmatrix} &= (XA + XM_iB \quad XC + XM_iD) \\ &= (X(A + M_iB) \quad X(C + M_iD)) \in \mathscr{S}_2.\end{aligned}$$

Since this must therefore be either ∞ or N_j for some value of j, we have

THEOREM 1. *$\mathscr{I}_1 = \{M_i\}$ and $\mathscr{I}_2 = \{N_i\}$ $(i = 0, 1, \ldots, p_r - 1)$ are equivalent indicator sets if and only if there exist $r \times r$ matrices A, B, C, and D over $GF(p)$ with the following properties:*

$$(a) \begin{vmatrix} A & C \\ B & D \end{vmatrix} \neq 0.$$

(b) *Either*

(i) *$B = 0$, A is non-singular, and for each $i \exists j \in \{0, 1, \ldots, p^r - 1\}$ such that $A^{-1}(C + M_iD) = N_j$ or*

(ii) *B is non-singular, and there is one value of $j \in \{0, 1, \ldots, p_r - 1\}$ such that $B^{-1}D = N_j$. Also, there is one value of i such that $A + M_iB = 0$. For each of the other i, $A + M_iB$ is non-singular and $\exists$ j such that $(A + M_iB)^{-1}(C + M_iD) = N_j$.*

Notation. We shall denote a partial permutation of $\mathscr{A}^*$ in the form $M \rightarrow (A + MB)^{-1}(C + MD)$, where M denotes any point of $\mathscr{A}^*$.

Note that $\infty \rightarrow \infty$ or $B^{-1}D$, depending on whether or not $B = 0$. Also, if $B \neq 0$, then $-AB^{-1} \rightarrow \infty$. In all other cases, the image of M is obtained by the indicated matrix operations.

It is interesting to note that the partial permutations of $\mathscr{A}^*$ considered here are reminiscent in their form of the classical linear fractional transformations.

Another necessary and sufficient condition for equivalence (of spread sets) is given by Maduram [**8**, p.487].

5. Collineations and Symmetries. Theorem 1 provides a criterion for determining when two indicator sets $\mathscr{I}_1$ and $\mathscr{I}_2$ are equivalent. In the case that $\mathscr{I}_2 = \mathscr{I}_1$, any partial permutation Γ taking $\mathscr{I}_1^*$ to $\mathscr{I}_2^*$ permutes the points of $\mathscr{I}_1^*$ and is a *symmetry* of $\mathscr{I}_1^*$. In the corresponding translation plane Π_1, Γ induces a collineation which fixes the point $(0\,0)$, i.e. it lies in the *translation complement* of the full collineation group of Π_1 [**11**, p.197]. Conversely, since a collineation belonging to the translation complement of Π_1 is given by a non-singular linear transformation in V which fixes the spread $\mathscr{S}_1$ [**1**, p.178; **10**, p.52], it induces a symmetry of $\mathscr{I}_1^*$. It follows that *the symmetry group of $\mathscr{I}_1^*$ is a homomorphic image of the translation complement of* Π_1. The kernel of the homomorphism is the group denoted by the matrices

$$\begin{pmatrix} \lambda I & 0 \\ 0 & \lambda I \end{pmatrix} \quad (\lambda \in \mathrm{GF}(p)).$$

From Theorem 1, we now have

THEOREM 2. *Let $\mathscr{I} = \{M_i\}$ $(i = 0, 1, \ldots, p^r - 1)$ be an indicator set. The symmetries of $\mathscr{I}^*$ are the partial permutations $M \rightarrow (A + MB)^{-1}(C + MD)$,* *where*

$$(a) \quad \begin{vmatrix} A & C \\ B & D \end{vmatrix} \neq 0.$$

(b) *Either*

(i) $B = 0$, *A is non-singular, and for each* $i \,\exists\, j \in \{0, 1, \ldots, p_r - 1\}$ *such that* $A^{-1}(C + M_i D) = M_j$ *or*

(ii) *B is non-singular and there is one value of* $j \in \{0, 1, \ldots, p^r - 1\}$ *such that* $B^{-1}D = M_j$. *Also there is one value of i such that* $A + M_i B = 0$. *For each of the other values of i,* $A + M_i B$ *is non-singular and* $\exists\, j$ *such that* $(A + M_i B)^{-1} (C + M_i D) = M_j$.

6. Some special permutations of $\mathscr{A}^*$. As we noted in Section 4, a partial permutation of $\mathscr{A}^*$ is not necessarily a permutation of all the points of $\mathscr{A}^*$. It is easy to show, in fact, that a partial permutation $M \to (A + MB)^{-1} (C + MD)$ is a permutation of $\mathscr{A}^*$ if and only if $B = 0$. In this case, ∞ is fixed and we have a permutation Γ: $M \to A^{-1}C + A^{-1}MD$ of the points of $\mathscr{A}$. (Note that for Γ to be a permutation, D must be non-singular). It is instructive to determine the circumstances under which Γ is then a collineation of $\mathscr{A}$, and the nature of that collineation.

In the series of lemmas which follow, we make constant use of the fact that $\mathscr{A}$ can be thought of as a vector space of dimension r over $\mathrm{GF}(p^r)$. The points of $\mathscr{A}$, which we are denoting by the $r \times r$ matrices $\{M\}$ over $\mathrm{GF}(p)$, are the vectors in this vector space, and vector addition can be identified with matrix addition. To avoid confusion, we shall use the symbol $\bar{M}$ to represent the vector corresponding to the point M. (We continue to let M denote both the matrix M and the point of $\mathscr{A}$ determined by M.) Thus for example the symbol $a\bar{M}$ denotes the vector $\bar{M}$ multiplied by the scalar $a \in \mathrm{GF}(p^r)$, but the symbol aM has no meaning unless $a \in \mathrm{GF}(p)$.

The semi-linear transformations are collineations in $\mathscr{A}$ fixing 0. Any other collineation of $\mathscr{A}$ is the product of a semi-linear transformation and a translation [**4**, p.32].

LEMMA 4. *Γ: $M \to A^{-1}C + A^{-1}MD$ is a translation of $\mathscr{A}$ if and only if $A = D = I$. All translations of $\mathscr{A}$ are present as permutations of $\mathscr{A}$.*

Proof. If $A = D = I$, then Γ is $M \to C + M$. In the vector space interpretation of $\mathscr{A}$, Γ is $\bar{M} \to \bar{C} + \bar{M}$, which is a translation in $\mathscr{A}$. Conversely, any translation in $\mathscr{A}$ is given in the form $\bar{M} \to \bar{C} + \bar{M}$.

In virtue of Lemma 4 and Theorem 1 we can conclude that any indicator set is equivalent to some indicator set containing 0. Thus no generality is lost in restricting our consideration of indicator sets to those which contain 0, and this we now consistently do.

We proceed to examine the question of when a permutation of $\mathscr{A}$ fixing 0 is a semi-linear transformation. Such a permutation has the form $M \to A^{-1}MD$.

https://doi.org/10.4153/CJM-1979-022-6 Published online by Cambridge University Press

Certainly $\bar{M} \to \bar{M}D$ is a linear transformation, since $\bar{M} = \bar{I}M$. So $M \to MD$ is a collineation of $\mathscr{A}$ for any (non-singular) matrix D.

Next, let W be the point such that $\bar{W} = e\bar{I}$, where e is a primitive root of $\mathrm{GF}(p^r)$. Then $e^i\bar{I} = \bar{W}^i$, and W has period $p^r - 1$.

LEMMA 5. *The points on the line* $0M$ *are* 0 *and* W^iM $(i = 0, 1, \ldots, p^r - 2)$.

Proof. The points are the vectors $\bar{0}$ and $e^i\bar{M} = e^i\bar{I}M = \bar{W}^iM = \overline{W^iM}$.

One semilinear transformation of $\mathscr{A}$ is the mapping τ: $(x_1, x_2, \ldots, x_r) \to (x_1^p, x_2^p, \ldots, x_r^p)$. Let T be the point with coordinates $(1, t^p, t^{2p}, \ldots, t^{rp})$. Under τ, $\bar{M} \to \bar{T}M$; therefore the permutation $M \to TM$ is a collineation of $\mathscr{A}$.

LEMMA 6. $TWT^{-1} = W^p$.

Proof. Under the mapping τ, $\bar{W} = e\bar{I} \to e^p\bar{T} = \overline{W^pT}$. Therefore $TW = W^pT$.

Lemma 6 has three corollaries:

COROLLARY 1. *The collineation* $M \to MW$ *fixes the line* $0T^i$ $(i = 0, 1, \ldots)$.

Proof. $TW = W^pT$ implies $T^iW = W^{p^i}T$, i.e. $\overline{T^i}W = \overline{W^{p^i}T^i}$. The result follows from Lemma 5.

COROLLARY 2. *T has period r, and* $\bar{I}, \bar{T}, \overline{T^2}, \ldots, \overline{T^{r-1}}$ *are linearly independent.*

Proof. T has period r since the semi-linear transformation τ clearly has period r. If $\bar{I}, \bar{T}, \ldots, \overline{T^{r-1}}$ are not linearly independent, then some vector $\overline{T^i}$ $(0 \leqq i < r)$ can be uniquely expressed as a linear combination

$$a_1\overline{T^{j_1}} + a_2\overline{T^{j_2}} + \ldots + a_n\overline{T^{j_n}} \quad (n < r; 0 \leqq j_1, \ldots, j_n < r),$$

where $i \neq j_1, \ldots, j_n$, $\overline{T^{j_1}}, \ldots, \overline{T^{j_n}}$ are linearly independent, and no $a_1, a_2, \ldots a_n$ is 0. Now by Corollary 1,

$$\overline{T^i}W = \overline{W^{p^i}T^i} = e^{p^i}\overline{T^j}.$$

Thus

$$e^{p^i}\overline{T^i} = (a_1\overline{T^{j_1}} + \ldots + a_n\overline{T^{j_n}})W = a_1\overline{W^{p^{j_1}}T^{j_1}} + \ldots + a_n\overline{W^{p^{j_n}}T^{j_n}}$$
$$= a_1e^{p^{j_1}}\overline{T^{j_1}} + \ldots + a_ne^{p^{j_n}}\overline{T^{j_n}}.$$

Since the expression for $\overline{T^i}$ as a linear combination of $T^{j_1}, \ldots, \overline{T^{j_n}}$ is unique,

$$e^{p^i} = e^{p^{j_1}} = \ldots = e^{p^{j_n}}.$$

But this is a contradiction since $i \neq j_1, j_2, \ldots, j_n$, and $0 \leqq i, j_1, \ldots, j_n < r$.

COROLLARY 3. $\langle W, T\rangle = N(\langle W\rangle)$ *in* $\mathrm{GL}(r, p)$.

Proof. By Lemma 6, T normalizes $\langle W\rangle$. If $A \in N(\langle W\rangle)$, then $AW = W^iA$, i.e. W fixes the line $0A$. But the eigenvectors of the linear transfor-

https://doi.org/10.4153/CJM-1979-022-6 Published online by Cambridge University Press

mation $\bar{M} \rightarrow \bar{M}W$ are the linearly independent vectors $\bar{I}, \bar{T}, \ldots, \overline{T^{r-1}}$, so that line $0A$ = line $0T^b$ ($b = 0, 1, \ldots, r-1$). Thus $A = W^aT^b$ for some a, b.

THEOREM 3. *The permutation* $\Gamma: M \rightarrow A^{-1}C + A^{-1}MD$ *is a collineation of* $\mathscr{A}$ *if and only if* $A \in \langle W, T \rangle$.

Proof. Γ is the product of the permutation Γ_1: $M \rightarrow A^{-1}MD$ and the translation $M \rightarrow A^{-1}C + M$, so that Γ is a collineation if and only if Γ_1 is a collineation. But since $M \rightarrow MD^{-1}A$ is a collineation, Γ_1 is a collineation if and only if Γ_2: $M \rightarrow A^{-1}MA$ is a collineation.

If Γ_2 is a collineation, then Γ_2 fixes the line $0I$ since it fixes I. Therefore $A^{-1}WA = W^i$ for some i, and so $A \in N(\langle W \rangle) = \langle W, T \rangle$. On the other hand, we have already noted that $M \rightarrow TM$ is a collineation, and it is easy to show that $M \rightarrow WM$ is the collineation (dilatation) $\bar{M} \rightarrow e\bar{M}$. It follows then that $M \rightarrow W^aT^bMD$ is a collineation, and the proof of Theorem 3 is complete.

7. Desarquesian and André planes of order p^r. In this section we exhibit indicator sets for Desarguesian and André planes of order p^r. In view of the large number of partial permutations $M \rightarrow (A + MB)^{-1}(C + MD)$ relating equivalent indicator sets, the choice of indicator set for any plane is very great. The choice of a representative indicator set is therefore somewhat arbitrary; we choose the representatives that are the simplest to grasp and/or which display their symmetries to best advantage.

The most obvious indicator set is the set of all points on a line whose direction numbers are linearly independent. By Theorem 1 and the theory developed in the last section, it is easy to show that all such indicator sets are equivalent, so we choose the points of the line $0I$ as a convenient representative. This indicator set is

$$\mathscr{I}_D = \{0 \cup W^i\} \quad (i = 0, 1, \ldots, p^r-2).$$

The matrices $\{0 \cup W^i\}$ clearly form a ring, and therefore the translation plane defined by $\mathscr{I}_D$ is the Desarguesian plane [**4**, p.220].

Let G be the group of symmetries of $\mathscr{I}_D$. By Theorem 2 and the lemmas of Section 6, the usual well-known facts about G are easily derived. For example, G is transitive on $\mathscr{I}_D$ since $\infty \rightarrow 0$ under $M \rightarrow M^{-1}$ and $\infty \rightarrow W^i$ under $M \rightarrow M^{-1}(I + MW^i)$ (that the above are symmetries of $\mathscr{I}_D$ is instantly verified). But G is doubly transitive on $\mathscr{I}_D$, since $M \rightarrow W^i + M$ fixes ∞ and carries 0 into W^i. Finally, G is triply transitive on $\mathscr{I}_D$ since $M \rightarrow MW^i$ fixes ∞ and 0, and carries I into W^i. The analysis can even be carried one step further to note that there is a symmetry of $\mathscr{I}_D$, different from the identity, which fixes ∞, 0, and I, namely $M \rightarrow TMT^{-1}$. Under this symmetry, $W \rightarrow W^p$ (Lemma 6); the symmetry induces a non-projective collineation of the Desarguesian plane defined by $\mathscr{I}_D$.

A generalized André plane is usually described in terms of its coordinatizing quasifield Q [**5**, **9**, **10**] (for a characterization in terms of collineations, see [**9**]).

The elements of Q are identified with the elements of the field $K = \mathrm{GF}(p^r)$, addition in Q is addition in K, but multiplication is defined by $x \cdot m = x^{p^\lambda}m$, where λ is an integer dependent upon m. The spread for the plane is obtained from the spread for the Desarguesian plane by replacement of the components $\{y = xm\}$ by the components $\{y = x^{p^\lambda}m\}$. In terms of indicator sets, this amounts to a series of replacements of sets of points $\{W^{a_j}\}$ $(j = 1, 2, \ldots, n)$ by points $\{W^{a_j}T^b\}$ [**10**, p.27].

For example, the indicator sets of the André planes are obtained from $\mathscr{I}_D = \{O \cup W^i\}$ $(i = 0, 1, \ldots, p^r - 2)$ by replacement of some of the sets $\{\mathscr{U}_k\} = \{\{W^{k+(p-1)i}\}\}$ $(i = 1, 2, \ldots, (p^r-1)/(p-1);\ k = 0, 1, \ldots, p-2)$ by the sets $\{\mathscr{U}_kT^{b_k}\}$ $(b_k = 1, 2, \ldots, r-1)$. The lines $OT^a\backslash O$ $(a = 0, 1, \ldots, r-1)$ are each partitioned into $p - 1$ disjoint sets of points $\mathscr{U}_0T^a, \mathscr{U}_1T^a, \ldots, \mathscr{U}_{p-2}T^a$, and it is not difficult to show that each point of $\mathscr{U}_kT^a$ is compatible with each point of $\mathscr{U}_jT^b$ whenever $j \neq k$. Thus the indicator set of any André plane may be taken to be sets of points:

$\mathscr{U}_0T^{a_1}, \mathscr{U}_1T^{a_2}, \ldots, \mathscr{U}_{p-2}T^{a_{p-1}}$, lying on lines
$OT^{a_1}, OT^{a_2}, \ldots, OT^{a_{p-1}}$, together with the point O.

By means of indicator sets, much detailed knowledge on André planes can be won. We illustrate by considering the case in which $p = r = 3$.

THEOREM 4. *Aside from the Desarguesian plane, there is only one André plane of order* 27.

We shall call this plane the *proper* André plane of order 27, to distinguish it from the Desarguesian plane.

Proof. Any indicator set of the Desarguesian plane of order 27 is equivalent to the set $\mathscr{I}_D = \{0 \cup \mathscr{U}_0 \cup \mathscr{U}_1\}$, where, as before, $\mathscr{U}_k = \{W^{k+2i}\}$ $(i = 0, 1, \ldots, 12)$ for $k = 0, 1$. Now $\mathscr{U}_k$ can be replaced by $\mathscr{U}_kT$ or $\mathscr{U}_kT^2$ to yield the indicator set $\mathscr{I}'$ of an André plane. Applying the collineation $M \to MT$ or $M \to MT^2$ and invoking Theorem 1, we have that $\mathscr{I}'$ is equivalent to an indicator set containing 0 and $\mathscr{U}_0$. So aside from $\mathscr{I}_D$, we have at most two non-equivalent indicator sets, $\mathscr{I}_1 = \{0 \cup \mathscr{U}_0 \cup \mathscr{U}_1T\}$ and $\mathscr{I}_2 = \{0 \cup \mathscr{U}_0 \cup \mathscr{U}_1T^2\}$. But the collineation $M \to WMT$ takes $\mathscr{I}_2$ into $\mathscr{I}_1$, so $\mathscr{I}_1$ and $\mathscr{I}_2$ are equivalent.

Theorem 3 is the first of a whole class of counts of André planes of given order. Similar reasoning yields for example that there are, aside from the Desarguesian plane, eight non-isomorphic André planes of order 125.

Collineation groups of generalized André planes (and therefore symmetry groups of the corresponding indicator sets) have been determined by Foulser [**5**].

8. Semifield planes. As we have already observed, the spread set of a semifield plane is closed under addition [**4**, p. 220]. Interpreting this property

https://doi.org/10.4153/CJM-1979-022-6 Published online by Cambridge University Press

in the indicator r-space $\mathscr{A}$, we easily see that the indicator set $\mathscr{I}_s$ of a semifield plane of order p^r in $\mathscr{A}$ is the orbit of points under a translation group of order p^r.

With the help of Theorem 1, equivalence classes of indicator sets of semifield planes can be set up. When $r = 3$ it can be shown that any such indicator set is equivalent to one which contains the p^2 points $(\lambda + \mu t, \lambda t + \mu t^2, \lambda t^2 + \mu t^3)$ $(\lambda, \mu \in GF(p))$ on the line $0I$. Such a "canonical form" is useful in determining the number of non-equivalent semifield plane indicator sets; I used it to show that there are only two semifield planes of order 27, including the Desarguesian plane.

Let us call the non-Desarguesian semifield plane of order 27 the *proper* semifield plane of that order. Of the many equivalent indicator sets defining this plane, one with considerable symmetry by collineations of $\mathscr{A}$ is the following: Let

$$t^3 = t - 1, \quad U = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}, \quad P_0 = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Let $P_1 = U^3 P_0 U$, $P_2 = U^6 P_0 U^2$. The indicator set, which we denote by $\mathscr{I}_S$, consists of the points $\lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2$ $(\lambda_i \in GF(3))$. It is a matter of straightforward verification to show that the points of $\mathscr{I}_S$ are mutually compatible, so that $\mathscr{I}_S$ is indeed an indicator set. $\mathscr{I}_S$ does not however indicate a Desarguesian plane, since the equivalent spread set $\{\lambda_0 I + \lambda_1 P_1 P_0^{-1} + \lambda_2 P_2 P_0^{-1}\}$ is not closed under multiplication [**4**, p.220]. Now (again by direct verification) the permutation Γ: $M \to U^3 M U$ is a symmetry of $\mathscr{I}_S$. Thus

$$(8.1) \quad \mathscr{I}_S = \{0 \cup U^{3i} P_0 U^i \cup U^{3i}(-P_0) U^i\} \ (i = 0, 1, \ldots, 12).$$

Since U fixes the line $0I$, $U \in \langle W \rangle$ and therefore Γ is a collineation of $\mathscr{A}$ (Theorem 3).

9. Hering's plane of order 27. Hering's plane [**6**] can be described in terms of the matrices

$$s = \begin{pmatrix} E & O \\ O & A \end{pmatrix} \quad \text{and} \quad r = \begin{pmatrix} B & B \\ C & D \end{pmatrix},$$

where

$$E = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A = \begin{pmatrix} -1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & -1 \end{pmatrix},$$

$$C = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & -1 & -1 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix},$$

over $GF(3)$. The spread consists of the components $X = 0$, $Y = 0$, and images of these under the linear transformations r and s. In particular $\{Y = 0\} \xrightarrow{r} \{Y = X\}$ and $\{X = 0\} \xrightarrow{r} \{Y = XC^{-1}D\}$, where

$$C^{-1}D = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix} = K, \text{ say.}$$

Applying s to $\{Y = X\}$ and $\{Y = XK\}$, we obtain the spread set

(9.1) $\{0 \cup E^{-i}A^i \cup E^{-i}KA^i\}$ $(i = 0, 1, \ldots, 12)$.

If we now apply the permutation $M \to R^{-1}MS$, where

$$R = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & -1 & -1 \end{pmatrix},$$

we obtain the equivalent indicator set

(9.2) $\mathscr{I}_H = \{0 \cup U^{3i}P_0U^i \cup U^{3i}QU^i\}$,

where

$$U = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix} \text{ and } P_0 = R^{-1}S = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

the same as in the semifield plane of Section 8. Also,

$$Q = R^{-1}KS = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & -1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Comparing (9.2) with (8.1), we see that $\mathscr{I}_H \cap \mathscr{I}_S = \{0 \cup U^{3i}P_0U^i\}$, and the remaining set of 13 points $\{U^{3i}QU^i\}$ in $\mathscr{I}_H$ is a replacement for the set $\{U^{3i}(-P_0)U^i\}$ in $\mathscr{I}_S$. Thus we have

THEOREM 5. *The Hering plane of order* 27 *can be derived from the proper semifield plane of order* 27 *by replacement of a net of degree* 13.

Theorem 5 is an interesting analog to the manner in which the proper André plane of order 27 is derived from the Desarguesian plane of order 27 by replacement (cf. Section 7 and [**10**, pp.8, 54]).

10. The plane of Rao and Rao. This plane, which is of order 27 and flag transitive [**12**], is also given by displaying the spread set. We reproduce it here since it is a good illustration of the use of partial permutations in generating indicator sets.

Using the language of Theorem 1 and the notation of [**12**], consider the partial permutation Γ: $M \rightarrow (MQ)^{-1}(P + MR)$, where

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & 1 \\ -1 & -1 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & -1 \\ -1 & 0 & -1 \end{pmatrix}$$

over GF(3). Under Γ, $\infty \rightarrow Q^{-1}R = M_2$, $M_i \rightarrow Q^{-1}M_i^{-1}P + M_2 = M_{i+1}$ $(i = 2, 3, \ldots, 26)$ and $M_{27} \rightarrow 0 \rightarrow \infty$. The set $\mathscr{I}_R = \{0, M_2, M_3, \ldots, M_{27}\}$ is an indicator set of the Rao-Rao plane.

References

1. J. André, *Über nicht-Desarquessche Ebenen mit transitiver. Translationsgruppe*, Math. Zeit *60* (1954), 156–186.

2. R. H. Bruck and R. C. Bose, *The construction of translation planes from projective spaces*, J. Algebra *1* (1964), 85–102.

3. A. Bruen, *Spreads and a conjecture of Bruck and Bose*, J. Algebra *23* (1972), 519–537.

4. P. Dembowski, *Finite geometries* (Springer-Verlag, Berlin, 1968).

5. D. A. Foulser, *Collineation groups of generalized André planes*, Can. J. Math. *21* (1969), 358–369.

6. C. Hering, *Eine nicht-desarquessche zweifach transitive affine Ebene der Ordnung 27*, Abh. Math. Sem. Hamb. *34* (1969), 203–208.

7. H. Lunelburg, *Die Suzukigruppen und ihre Geometrien* (Springer-Verlag, Berlin, 1965).

8. D. M. Maduram, *Matrix representation of translation planes*, Geometriae Dedicata *4* (1975), 485–492.

9. T. G. Ostrom, *A characterization of generalized André planes*, Math. Zeit. *110* (1969), 1–9.

10. ——— *Finite translation planes* (Springer-Verlag, Berlin, 1970).

11. ——— *Classification of finite translation planes*, Proceedings of the international conference on projective planes held at Washington State University, April 25–28, 1973 (Washington State University Press, 1973).

12. M. L. N. Rao and K. K. Rao, *A new flag transitive affine plane of order* 27, Proc. of the Amer. Math. Soc. *59* (1976), 337–345.

13. F. A. Sherk and G. Pabst, *Indicator sets, reguli, and new a class of spreads*, Can. J. Math. *29* (1977), 132–154.

University of Toronto,
Toronto, Ontario