Groups of Generalised Projectivities in Projective Planes of Odd Order

D. G. Glynn* and G.F. Steinke**

Department of Mathematics
University of Canterbury
Christchurch, New Zealand

Abstract. The generalised projectivities (GP's) associated with projective planes of odd order are investigated. These are non-singular linear mappings over $GF(2)$ defined from the binary codes of these planes. One case that is investigated in detail corresponds to the group of an affine plane – every point corresponds to a GP. It is shown how many collineations that fix the line at infinity point-wise can be constructed as a product of these GP's.

1. The Self-dual Code

Since our groups of generalised projectivities will be constructed from mappings associated with the main self-dual code of a finite projective plane of odd order, let us recall some of the properties of this code; see [**2**] for further details. First, we have some notation. Let π be a finite projective plane of *odd order* q. Let P and L be the sets of points and lines respectively of π. Thus $|P| = |L| = q^2 + q + 1$. If S is any set define S^β to be 0 if $|S|$ is even, or 1 if $|S|$ is odd. Also, if $g \in P$ or L let $\hat{g}$ be the set of $q+1$ elements of $P \cup L$ that are incident with g. Note that often we identify $g \in P \cup L$ with the set $\{g\}$. (This is not unusual in geometry.)

Next, if $S \subseteq P$, and dually $T \subseteq L$, let

$$\delta S := \{g \in L \mid (\hat{g} \cap S)^\beta + S^\beta = 1\} \quad (= |S|L + \sum_{x \in S} \hat{x}), \text{ and}$$

$$\partial T := \{p \in P \mid (\hat{p} \cap T)^\beta + T^\beta = 1\} \quad (= |T|P + \sum_{y \in T} \hat{y}),$$

where the set of all points and lines is made into a vector space over $GF(2)$, the subsets being vectors and symmetric difference being addition; the above sums in brackets are taken in this vector space. We say that δS is the *coboundary* of S, and that ∂T is the *boundary* of T. One can easily check that δ and ∂ are inverses of one-another.

The self-dual code $\mathcal{C}_B$ is made up of subsets, called *words*, of $P \cup L$, so that

$$\mathcal{C}_B := \{S \cup \delta S \mid S \subseteq P\} = \{T \cup \partial T \mid T \subseteq L\}.$$

*This research was supported by a grant from the University of Canterbury.
**This research was supported by a Feodor Lynen Fellowship.

As shown in [2], $\mathcal{C}_B$ contains a doubly-even subcode $\mathcal{C}_A$ of index 2, so that

$$\mathcal{C}_A := \{S \cup \delta S \mid S \subseteq P, S^\beta = 0\} = \{T \cup \partial T \mid T \subseteq L, T^\beta = 0\}.$$

The weight (or size) of every word of $\mathcal{C}_A$ is then divisible by 4. Also, every word of the coset $\mathcal{C}_B \setminus \mathcal{C}_A$ has weight congruent to 2 modulo 4, and is the complement in $P + L$ of a word in $\mathcal{C}_A$. Note that the sum $X + Y$ of any two subsets of $P \cup L$ is the same as the symmetric difference of the two subsets. Also, $\bar{X}$ is defined to be the complement of X in P if $X \subseteq P$, or the complement in L, if $X \subseteq L$. Often we write these complements as $P + X$ or $L + X$ respectively. Here are some properties that we shall need for our later theory.

LEMMA 1.1.

(1) $\partial = \delta^{-1}$;
(2) $\delta(u + v) = \delta u + \delta v$, $\forall\, u, v \subseteq P$;
(3) $\partial(g + h) = \partial g + \partial h$, $\forall\, g, h \subseteq L$;
(4) $|r| \equiv |\delta r| \pmod 2$, $\forall r \subseteq P$;
(5) $|u| \equiv |\partial u| \pmod 2$, $\forall u \subseteq L$;
(6) $\delta x = L + \hat{x}$, $\partial \hat{x} = P + x = \overline{x}$, $\forall x \in P$;
(7) $\partial y = P + \hat{y}$, $\delta \hat{y} = L + y = \overline{y}$, $\forall y \in L$;
(8) $\delta P = L$, $\partial L = P$;
(9) $(X + Y) \cap Z = (X \cap Z) + (Y \cap Z)$, $\forall\, X, Y, Z \subseteq P + L$.

PROOF: We leave these as exercises; see [2] for some ideas.

2. The Generalised Projectivities of the Plane

Here we investigate a generalisation of the projectivities first intensively studied last century by von Staudt.

DEFINITION 2.1. *Let $S \subseteq P$ and $T \subseteq L$.*

(1) *The generalised projectivity $\delta(S,T)$ is the mapping $2^S \longrightarrow 2^T$ taking $u \mapsto \delta u \cap T$, $\forall\, u \subseteq S$.*
(2) *The generalised projectivity $\partial(T,S)$ is the mapping $2^T \longrightarrow 2^S$ taking $v \mapsto \partial v \cap S$, $\forall\, v \subseteq T$.*

Note that with this notation $\delta = \delta(P,L)$ and $\partial = \partial(L,P)$, so that generalised projectivities are the restrictions of the boundary and coboundary operators to subsets of the plane. Next, we see that these restrictions are also linear mappings of the codes corresponding to the subsets of the various sets of points and lines.

LEMMA 2.2.

$$(u_1 + u_2)^{\delta(S,T)} = u_1^{\delta(S,T)} + u_2^{\delta(S,T)}, \ \forall\, u_1, u_2 \subseteq P.$$

Similarly,

$$(v_1 + v_2)^{\partial(T,S)} = v_1^{\partial(T,S)} + v_2^{\partial(T,S)}, \ \forall\, v_1, v_2 \subseteq L.$$

PROOF: From Lemma 1.1 there holds

$$(u_1 + u_2)^{\delta(S,T)} = \delta(u_1 + u_2) \cap T = (\delta u_1 + \delta u_2) \cap T = (\delta u_1 \cap T) + (\delta u_2 \cap T).$$

The second formula has a similar proof.

Note that $\delta(S,T)$ can be represented as a *matrix transformation* from the vector space $V(S)$ of dimension $|S|$ over $GF(2)$ consisting of all subsets of S to the vector space $V(T)$ of dimension $|T|$ consisting of all subsets of T. With bases of $V(S)$ and $V(T)$ being the points of S and the lines of T respectively, the matrix of $\delta(S,T)$ is the complement of the submatrix of the incidence matrix of π that is induced by S and T. (Here, *complement* means the mapping of $(0,1)$-matrices induced by $0 \leftrightarrow 1$.) Dually, the matrix of $\partial(T,S)$ with respect to the same bases is the transpose of the matrix of $\delta(S,T)$. These facts follow from Lemma 1.1 (6-7).

DEFINITION 2.3. *A generalised projectivity is said to be non-singular if the mapping is a bijection.*

Such a non-singular generalised projectivity corresponds to a non-singular square submatrix of C, the complement of the incidence matrix of π, and so we always have that $|S| = |T|$ for a non-singular $\delta(S,T)$ or $\partial(T,S)$.

The matroid $\mathcal{M} := \mathcal{M}(\pi)$ corresponding to the code $\mathcal{C}_B$ of π is defined to be the combinatorial geometry which has $P \cup L$ as set of points, and where $\emptyset \neq X \subseteq P \cup L$ is linearly dependent in $\mathcal{M}$ if and only if it contains a word of $\mathcal{C}_B$. This matroid is self-dual and can be coordinatised by the columns of the matrix formed by the union of an identity matrix side-by-side with C. For more details see [**3**].

LEMMA 2.4. *Let $S \subseteq P$ and $T \subseteq L$. The following are all equivalent.*

(1) *$\delta(S,T)$ is non-singular;*
(2) *$\partial(T,S)$ is non-singular;*
(3) *$\delta(\bar{S},\bar{T})$ is non-singular;*
(4) *$\partial(\bar{T},\bar{S})$ is non-singular;*
(5) *$S + \bar{T}$ is a basis of the matroid $\mathcal{M}$;*
(6) *$\bar{S} + T$ is a basis of the matroid $\mathcal{M}$.*

PROOF: These follow from the fact that the code $\mathcal{C}_B$ is self-dual, or equivalently, that the matrix C is orthogonal modulo two, or that $\mathcal{M}$ is self-dual.

DEFINITION 2.5. *Let U be a set of subsets of points of π, and let V be a set of subsets of lines such that the sizes of all these subsets are the same integer n. The generalised projectivity group, $GP(U,V)$, corresponding to U and V is the group of non-singular linear transformations ($\cong$ to a subgroup of $GL(n,2)$) generated by the non-singular generalised projectivities in*

$$\{\delta(u,v) \mid u \in U,\ v \in V\} \cup \{\partial(v,u) \mid u \in U,\ v \in V\}.$$

We only consider products of mappings that make sense. That is, we only allow products of consecutive mappings of the type $\delta(a,b)\partial(b,c)$, or $\partial(b,c)\delta(c,d)$. Next, *the subsets $U \cup V$ should be "connected", which means that given any two members of $U \cup V$, there will be an element of the generalised projectivity group taking one member to the other. Also, we consider products that always start with a certain subset $w \in U \cup V$ and end with w, so that we obtain a group of non-singular linear transformations of the vector space corresponding to the subsets of w. Clearly, it does not matter which subset w we fix, as the same abstract group is always obtained.*

DEFINITION 2.6. *The **dimension** of a generalised projectivity group is the integer n, which is the size of the subsets of points and lines, from which the group is constructed.*

The following result can be proved from elementary properties of the incidence matrix. It is not used any further, and so we state it without proof.

THEOREM 2.7. *Some formulae involving δ and ∂.*

(1) $\delta(S,T)\partial(T,\bar{S}) = \delta(S,\bar{T})\partial(\bar{T},\bar{S}), \forall\, S \subseteq P,\ T \subseteq L$

(2) $\delta(S,T)\partial(T,S) + \delta(S,\bar{T})\partial(\bar{T},S) = id$, *where we consider these as linear mappings, and id is the identity map from S to S.*

3. The Von Staudt Group

Here we show how the classical group of projectivities of the given plane (of order q) is a special case of generalised projectivities of dimension $q+1$. Probably the most up-to-date reference for the theory of von Staudt groups is the Proceedings of the Conference at Bad Windsheim in July 1980 [**9**].

THE VON STAUDT PROJECTIVITY GROUP. *The von Staudt group of the projective plane, $ST(\pi)$, is generated by all the abstract projectivities $\alpha(A,b)$, taking $\hat{A} \to \hat{b}$, such that $x \mapsto x.b$, $\forall x \in \hat{A}$; and the inverse mappings $\beta(b,A)$, taking $\hat{b} \to \hat{A}$, such that $R \mapsto R \cap A$, $\forall R \in \hat{b}$; where A is a line not incident with a point b. The mappings are multiplied in a manner analogous to the groups of generalised projectivities, (with alternating sequences of α's and β's ending up with the same point or line), so that a permutation group on $q+1$ elements is obtained.*

The most famous result about these groups is that $ST(\pi)$ is always 3-transitive on the $q+1$ elements, and it is sharply 3-transitive if and only if the plane is Pappian (coordinatised by a field); see [**9**].

We leave it as an exercise to show that $ST(\pi)$ is abstractly isomorphic to the group of generalised projectivities of $\pi = (P,L)$ given by

$$W := GP(\{\hat{G} \mid G \in L\}, \{\hat{p} \mid p \in P\}).$$

In fact, if $G \in L$, a point of $\hat{G}$ will always be mapped by an element of W to a point of $\hat{G}$, and the permutation group induced by W will be the same as the classical von Staudt permutation group of the plane. However, in general the group $GP(U,V)$ does not induce a permutation group on the points (or lines) of a subset (of size n) of U or V, but is a certain subgroup of $GL(n,2)$.

Note that the mappings $\partial(\hat{G},\hat{p})$ and $\delta(\hat{p},\hat{G})$ are non-singular if and only if $p \notin \hat{G}$. One way to see this is to calculate the determinant of the corresponding submatrix of C, the complement of the incidence matrix of π. With an appropriate coordinate system, when $p \in \hat{G}$ the matrix has a row of zero's, but in the other case the matrix is equal to $J - I$, where J is the matrix of all one's and I is the identity matrix. (Naturally, both are $q+1 \times q+1$.) Then

$$\det(J-I) = q \cdot (-1)^q \equiv 1 \pmod 2.$$

4. Some Generalised Projectivity Groups of Small Dimension

Sets of size one give subgroups of $GL(1,2)$, and thus are trivial, and so the smallest non-trivial dimension is two. In this case we always obtain subgroups of $GL(2,2) \cong S_3$, (the symmetric group on three letters).

EXAMPLE 4.1. *Sets of size two*

Let x and y be two distinct points in π and let A, B, C be three lines such that $x \in A$, $y \in C$, $x \notin B$ or C, and $y \notin A$ or B. Now consider the generalised projectivity groups

$$G_1 := GP(\{\{x,y\}\},\{\{A,B\}\})$$

and

$$G_2 := GP(\{\{x,y\}\},\{\{A,C\}\}).$$

Up to isomorphism these are the only possibilities to obtain non-singular mappings on sets of two points. The first group G_1 is generated by the linear extension of the mapping

$$x \mapsto \{x,y\},\ \ y \mapsto x;$$

thus G_1 is cyclic of order three. For the second group G_2 one finds that $G_2 = 1$. Combining both groups one sees that it is essential to require that the collection $U \cup V$, in Definition 2.6, is connected. Let x_1, x_2, y_1, y_2 be four distinct points and let $U = \{\{x_1,y_1\},\{x_2,y_2\}\}$; also choose four distinct lines A_1, B, A_2, C such that A_i contains precisely the point x_i, C contains precisely the point y_2, and B contains none of the four points. Put $V = \{\{A_1,B\},\{A_2,C\}\}$; then the only way to compose generalised projectivities is with respect to $\{x_1,y_1\},\{A_1,B\}$ and $\{x_2,y_2\},\{A_2,C\}$. Thus the disconnected "generalised projectivity group" $GP(U,V)$ is trivial with respect to $\{x_2,y_2\}$ and is cyclic of order three with respect to $\{x_1,y_1\}$.

Using an additional point z, the lines $x \cdot y, x \cdot z, y \cdot z$, and 3 further distinct lines (one line through each of the three points x,y,z) it is easy to construct the linear extension of the mapping $x \mapsto y$, $y \mapsto x$. Thus, if P_2 and L_2 denotes the set of all subsets of size 2 of P and L respectively, then $G = GP(P_2, L_2) \cong GL(2,2)$.

EXAMPLE 4.2. *Sets of size three*

Let a,b,c,d,e be 5 distinct points such that a,d,e and b,c,e are collinear; further let $A = a \cdot e$, $B = b \cdot d$, $C = c \cdot e$, and $D = a \cdot b$. We consider the generalised projectivities

$$\delta_1 = \delta(\{a,c,e\},\{A,C,D\}),$$

$$\begin{aligned}
\delta_2 &= \delta(\{a,c,e\},\{A,B,D\}),\\
\delta_3 &= \delta(\{b,d,e\},\{A,B,D\}),\\
\partial_1 &= \partial(\{A,C,D\},\{a,c,e\}),\\
\partial_2 &= \partial(\{A,C,D\},\{b,d,e\}),\\
\partial_3 &= \partial(\{A,B,D\},\{a,c,e\}).
\end{aligned}$$

It is easy to check that

$$\alpha_1 = \delta_1\partial_1, \quad \alpha_2 = \delta_2\partial_3, \quad \alpha_3 = \delta_1\partial_2\delta_3\partial_3,$$

have orders 3, 7, and 4 respectively. Thus these three generalised projectivities generate a subgroup H of $GL(3,2)$ whose order is divisible by $84 = 3 \cdot 7 \cdot 4$. Since $GL(3,2)$ is a simple group of order 168 and a subgroup of index two is always normal, the subgroup H must be the full group. In particular, if P_3 and L_3 denotes the set of all subsets of size 3 of P and L respectively, then the generalised projectivity group $GP(P_3, L_3)$ is isomorphic to $GL(3,2)$.

The above examples show that generalised projectivity groups based on small element sets do not allow us to distinguish between different projective planes. The same conclusion also follows for certain groups of generalised projectivities based on large element sets; see §5 and §6. However, as the classical von Staudt group shows, there are cases where different planes yield non-isomorphic generalised projectivity groups.

EXAMPLE 4.3. *The affine plane of order three (sets of size nine)*

Let $\pi_3 := PG(2,3) = (P,L)$ be the projective plane of order $q = 3$. If $l \in L$ is a fixed line of π, then note that $\partial l = P + \hat{l}$, and if $x \in \partial l$, then $\delta x = L + \hat{x}$; these are both sets of size $q^2 = 9$. Also, note that $l + L = \delta\hat{l}$; see Lemma 1.1. Then $\pi_3' := PG(2,3) = (\partial l, l + L)$ is the affine plane of order three obtained from π by deleting l.

We define the generalised projectivity group (of dimension $q^2 = 9$)

$$G_l := GP(\{\partial l\}, \{\delta x \mid x \in \partial l\}),$$

which is generated by all mappings

$$\alpha_x := \delta(\partial l, \delta x)\partial(\delta x, \partial l),$$

where x ranges over all points of π_3' ... thus $x \in \partial l$. Note that these mappings are non-singular because the mappings for the complementary sets are of "von Staudt" type. In particular, refer to Lemma 2.4 and the calculation at the end of §3.

It is only for the case of $q = 3$, that α_x maps points to points – this does not hold for planes of order greater than three. To see this, one calculates that $x^{\alpha_x} = x$, $\forall x \in \pi'$; and if $y \neq x$, $y \in \pi'$, $m := x.y$, then $y^{\alpha_x} = \hat{m} + x + y + (\hat{m} \cap \hat{l})$. Thus in the case of $q = 3$, y^{α_x} is the third affine point, distinct from x and y, on the line m joining x and y. From this it readily follows that α_x is a collineation of the affine plane π_3' and that α_x comes from a central collineation of π_3 having axis l and centre x. Thus G_l is the group of all axial collineations of π_3 with fixed axis l. From this description of the group G_l one easily sees that G_l is generated by any three of the mappings α_x, where the corresponding points are not collinear.

It is well known that this group is non-abelian of order 18. It has a normal abelian subgroup isomorphic to $Z_3 \times Z_3$, which is the group of translations with axis l. In the next section we shall see that similar groups appear when general affine planes of odd order are considered.

5. Generalised Projectivities in the Affine Plane

In his section we investigate the interesting case of generalised projectivities of dimension q^2 based on an affine plane of odd order q. We covered the exceptional case of $q = 3$ in Example 4.3. As this is a special situation we always assume in this section that $q > 3$.

PROBLEM 5.1. *Let l_∞ be a fixed line of π. Classify the group*

$$G := GP(\{\partial l_\infty\}, \{\delta p \mid p \in \partial l_\infty\}).$$

Note that passing over to complements $GP(\{\hat{l}_\infty\}, \{\hat{p} \mid p \in \partial l_\infty\})$ we obtain the trivial group on $\hat{l}_\infty$ (as a subgroup of the von Staudt group).

From now on we shall investigate the group of generalised projectivities proposed by the above problem. We shall see that any line of the affine plane gives rise to a representation of the symmetric group S_{q+1}, and that every translation of the plane – any collineation fixing every point on l_∞ and fixing all or no points not on l_∞ – is represented as an element of the group of each of its fixed affine lines.

First, let us consider a general representation of the symmetric group. It will be useful, not only in the present section but also in the next. The representation of S_{n+1} contains the usual permutation representation of S_n as a subgroup.

THEOREM 5.2. *Let n be an odd integer ($n \geq 5$) and put $N = \{1, 2, \ldots, n\}$. The symmetric group S_{n+1} is the group of all permutations of $N \cup \{\infty\}$ and has size $(n+1)!$. The subgroup S^∞ fixing ∞ is isomorphic to S_n. The group $GL(n,2)$ acts in the usual way on the set of all subsets of N with addition in the vector space corresponding to symmetric difference of subsets of N. Consider the mapping $\sigma: S_{n+1} \to GL(n,2)$ such that $\alpha \mapsto \alpha^\sigma$, where*

a) $\alpha \in S^\infty \Rightarrow j^{\alpha^\sigma} = j^\alpha, \forall j \in N$; and

b) $$\alpha \notin S^\infty \Rightarrow \begin{cases} (\infty^{\alpha^{-1}})^{\alpha^\sigma} = \infty^\alpha, \\ j^{\alpha^\sigma} = N + \infty^\alpha + j^\alpha, \quad \forall j \in N \setminus \{\infty^{\alpha^{-1}}\} \end{cases}.$$

Then σ is a 1-1 homomorphism from $S_{n+1} \to GL(n,2)$. Thus σ induces a faithful representation of S_{n+1} in $GL(n,2)$.

PROOF: If $\alpha \in S^\infty$, $N^{\alpha^\sigma} = (\sum_{j\in N} j)^{\alpha^\sigma} = \sum_{j\in N} j^{\alpha^\sigma} = \sum_{j\in N} j^\alpha = \sum_{j\in N} j = N$. Otherwise, $N^{\alpha^\sigma} = (\sum_{j\in N} j)^{\alpha^\sigma} = \sum_{j\in N} j^{\alpha^\sigma} = \sum_{j\in N\setminus\{\infty^{\alpha^{-1}}\}} j^{\alpha^\sigma} + (\infty^{\alpha^{-1}})^{\alpha^\sigma} =$

$\sum_{j\in N\setminus\{\infty^{\alpha^{-1}}\}}(N+\infty^\alpha+j^\alpha)+\infty^\alpha=(n-1)N+(n-1)\infty^\alpha+(N+\infty^\alpha)+\infty^\alpha=$ $nN+(n+1)\infty^\alpha=N$, (as n is odd). Thus $N^{\alpha^\sigma}=N$, $\forall\ \alpha\in S_{n+1}$.

To show that σ is a homomorphism we consider the various cases as follows.

(1) $\alpha\in S^\infty,\ \beta\in S^\infty\Rightarrow\alpha\beta\in S^\infty\Rightarrow(\alpha\beta)^\sigma=\alpha^\sigma\beta^\sigma$.

(2) $\alpha\notin S^\infty,\ \beta\in S^\infty$
$\Rightarrow(\infty^{(\alpha\beta)^{-1}})^{\alpha^\sigma\beta^\sigma}=(\infty^{\alpha^{-1}})^{\alpha^\sigma\beta^\sigma}=(\infty^\alpha)^{\beta^\sigma}=\infty^{\alpha\beta}$;
and for $j\in N\setminus\{\infty^{\alpha^{-1}}\}$, $j^{\alpha^\sigma\beta^\sigma}=(N+\infty^\alpha+j^\alpha)^{\beta^\sigma}=N+\infty^{\alpha\beta}+j^{\alpha\beta}$.

(3) $\alpha\in S^\infty,\ \beta\notin S^\infty$
$\Rightarrow(\infty^{(\alpha\beta)^{-1}})^{\alpha^\sigma\beta^\sigma}=(\infty^{\beta^{-1}\alpha^{-1}\alpha})^{\beta^\sigma}=(\infty^{\beta^{-1}})^{\beta^\sigma}=\infty^\beta=\infty^{\alpha\beta}$;
and for $j\in N\setminus\{\infty^{(\alpha\beta)^{-1}}\}$, $j^{\alpha^\sigma\beta^\sigma}=(j^\alpha)^{\beta^\sigma}=N+\infty^\beta+j^{\alpha\beta}$.

(4) $\alpha\notin S^\infty,\ \beta\notin S^\infty,\ \alpha\beta\notin S^\infty$
$\Rightarrow(\infty^{\alpha^{-1}})^{\alpha^\sigma\beta^\sigma}=(\infty^\alpha)^{\beta^\sigma}=N+\infty^{\alpha\beta}+\infty^\beta$; also,
$(\infty^{(\alpha\beta)^{-1}})^{\alpha^\sigma\beta^\sigma}=(N+\infty^{(\alpha\beta)^{-1}\alpha}+\infty^\alpha)^{\beta^\sigma}=N+\infty^\beta+(N+\infty^{\alpha\beta}+\infty^\beta)=$ $\infty^{\alpha\beta}$;
and for $j\in N\setminus\{\infty^{\alpha^{-1}},\ \infty^{(\alpha\beta)^{-1}}\}$,
$j^{\alpha^\sigma\beta^\sigma}=(N+\infty^\alpha+j^\alpha)^{\beta^\sigma}=N+(N+\infty^{\alpha\beta}+\infty^\beta)+(N+\infty^\beta+j^{\alpha\beta})$
$=N+\infty^{\alpha\beta}+j^{\alpha\beta}$.

(5) $\alpha\notin S^\infty,\ \beta\notin S^\infty,\ \alpha\beta\in S^\infty$. Thus $\infty^\alpha=\infty^{\beta^{-1}}$.
$\Rightarrow(\infty^{\alpha^{-1}})^{\alpha^\sigma\beta^\sigma}=(\infty^\alpha)^{\beta^\sigma}=(\infty^{\beta^{-1}})^{\beta^\sigma}=\infty^\beta=(\infty^{\alpha^{-1}})^{\alpha\beta}$; also,
for $j\in N\setminus\{\infty^{\alpha^{-1}},\infty^{(\alpha\beta)^{-1}}\}$,
$j^{\alpha^\sigma\beta^\sigma}=(N+\infty^\alpha+j^\alpha)^{\beta^\sigma}=N+\infty^\beta+(N+\infty^\beta+j^{\alpha\beta})=j^{\alpha\beta}$; and
$(\infty^{(\alpha\beta)^{-1}})^{\alpha^\sigma\beta^\sigma}=(N+\infty^{(\alpha\beta)^{-1}\alpha}+\infty^\alpha)^{\beta^\sigma}=N+\infty^\beta+(N+\infty^{\alpha\beta}+\infty^\beta)=$ $\infty^{\alpha\beta}=\infty$.

Finally, it is easy to check that the kernel of σ is the identity, or equivalently that the action of α^σ is non-trivial for $\alpha\neq 1$. (Here we need that $n>3$.)

Now we consider the representation σ of S_{n+1} in $GL(n,2)$ above, and determine some of its properties. With each element i of N we identify a variable x_i in order to consider the set of all non-empty subsets of N as the set of points $(x_1,\ldots,x_n)$ of a projective space $PG(n-1,2)$ with fixed coordinate system. If the representation fixes a quadric of $PG(n-1,2)$ it must be of the type

$$\mathcal{Q}_{k,\lambda}:\quad k\sum_i x_i^2+\lambda\sum_{i<j}x_ix_j=0,\quad k,\ \lambda\in\ \{0,1\},(k,\lambda)\neq(0,0).$$

This is because the representation contains S_n as a subgroup which permutes the x_i's in all possible ways. The Arf invariant (see [**6**]) shows that $\mathcal{Q}_{k,\lambda}$ is non-singular if and only if $\det(A)\equiv 2\pmod 4$ where $A=(2k-\lambda)I+\lambda J$
$\Rightarrow\det(A)=(2k-\lambda)^{n-1}(2k+(n-1)\lambda)$. Thus $\mathcal{Q}_{k,\lambda}$ is non-singular $\Longleftrightarrow$

a) $(k,\lambda)=(0,1)$ and $n\equiv 3\pmod 4$; or

b) $(k,\lambda)=(1,1)$ and $n\equiv 1\pmod 4$.

Next we see that every element of $(S_{n+1})^\sigma$ either takes a subset of N of size s to a set of size s, $n-s-1$ or $n-s+1$. In fact, if $U \subseteq N$, $|U| = s$, then

$$U^{\alpha^\sigma} = \begin{cases} U^\alpha & \text{if } \sigma \in S^\infty; \\ \sum_{j\in U}(N + \infty^\alpha + j^\alpha) = U^\alpha + |U|(N+\infty^\alpha) & \text{if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \notin U; \\ \infty^\alpha + (|U|-1)(N+\infty^\alpha) + (U+\infty^{\alpha^{-1}})^\alpha & \text{if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \in U. \end{cases}$$

Hence,

$$U^{\alpha^\sigma} = \begin{cases} U^\alpha & \text{(size } s\text{), if } \sigma \in S^\infty; \\ U^\alpha + \infty + \infty^\alpha & \text{(size } s\text{), if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \in U \text{ and } s \text{ is odd;} \\ U^\alpha & \text{(size } s\text{), if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \notin U \text{ and } s \text{ is even;} \\ U^\alpha + \infty^\alpha + N & \text{(size } n-s-1\text{), if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \notin U \text{ and } s \text{ is odd;} \\ U^\alpha + \infty + N & \text{(size } n-s+1\text{), if } \sigma \notin S^\infty,\ \infty^{\alpha^{-1}} \in U \text{ and } s \text{ is even.} \end{cases}$$

We can calculate whether or not every member of the representation fixes one of the above quadrics from this information. Thus, a mapping fixes the quadric $\mathcal{Q}_{0,1}$
$\iff$ a set of size s is taken to a set of size t, where $\binom{s}{2} \equiv \binom{t}{2} \pmod 2$
$\iff (s-t)(s+t-1) \equiv 0 \pmod 4$
$\iff s \equiv t \pmod 4$, or $s+t \equiv 1 \pmod 4$.
But mappings of our representation conserve the parity of subsets, (preserving "oddness" and "evenness"), and so the condition $s+t \equiv 1 \pmod 4$ is never satisfied. Hence the condition becomes $s \equiv t \pmod 4$. Thus if s is odd, we must have that $n-1-s \equiv s \pmod 4 \iff n \equiv 3 \pmod 4$. Also, if s is even, $n+1-s \equiv s \pmod 4 \iff n \equiv 3 \pmod 4$ must be satisfied.

Now consider $\mathcal{Q}_{1,1}$. In this case the condition is
$\binom{s+1}{2} \equiv \binom{t+1}{2} \pmod 2$
$\iff (s-t)(s+t+1) \equiv 0 \pmod 4$
$\iff s \equiv t \pmod 4$, or $s+t \equiv 3 \pmod 4$.
As before, $s+t \equiv 3 \pmod 4$ is never satisfied, and so we must have $s \equiv t \pmod 4$. By the same argument as before we learn that $n \equiv 3 \pmod 4$ — but in this case $\mathcal{Q}_{1,1}$ is singular. We can summarize these results in the following.

THEOREM 5.3. *If $n \equiv 3 \pmod 4$ the representation σ of S_{n+1} in $GL(n,2)$ is orthogonal. That is, it leaves invariant a non-singular quadric of $PG(n-1,2)$ and is contained in $PGO(n,2)$. (For odd n, $PGO(n,2) \cong PGSp(n-1,2)$, and is a simple group for $n \geq 7$.) If $n \equiv 1 \pmod 4$, the representation is not orthogonal.*

Since $PGO(5,2) \cong S_6$, (see [5] appendix III), at first sight the image of S_6 under σ for $n=5$ could be the full orthogonal group. However, since $5 \equiv 1 \pmod 4$, our representation does not fix any non-singular quadric of $PG(4,2)$.

Perhaps more important is that the representation σ always fixes the point corresponding to N and also the subspace of all even subsets of N - a hyperplane of $PG(n-1,2)$. Hence is it clear that a faithful representation σ' of S_{n+1} is induced by σ on the $PG(n-2,2)$ that is the set of all non-empty even subsets of N.

Now consider the mapping $\gamma\colon S_{n+1} \to GL(n,2)$ such that $\alpha \mapsto \alpha^\gamma$, where

a) $\alpha \in S^\infty \Rightarrow j^{\alpha^\gamma} = j^\alpha, \forall\, j \in N$; and

b) $\alpha \notin S^\infty \Rightarrow \begin{cases} (\infty^{\alpha^{-1}})^{\alpha^\gamma} = \infty^\alpha, \\ j^{\alpha^\gamma} = \infty^\alpha + j^\alpha, \qquad \forall\, j \in N \setminus \{\infty^{\alpha^{-1}}\} \end{cases}.$

If we use the basis $i+\infty$, $(i \in N)$, on the subspace h of all even subsets of $N \cup \{\infty\}$, this representation can be seen to be the same as the permutation representation of degree $n+1$ of S_{n+1}, restricted to the hyperplane h, (which passes in this case through a fixed point). The fixed point is $N + \infty$, and so there is an even smaller representation γ' of degree $n-1$ obtained by projecting γ from this point. It is easily seen that γ' is the same representation as σ'. From the D-matrices given in [**11**, $2-6$, $2-8$, $2-10$ of the appendix], there is considerable evidence that for $n \geq 7$, σ' is *the unique irreducible representation of S_{n+1} of degree $n-1$* , and $n-1$ is minimal, in that the only smaller representations are the two linear ones – the trivial representation and the one taking even permutations to 1 and odd permutations to -1. When $n = 5$ there are two inequivalent 2-modular representations of S_6 of degree 4. Note that D-matrices tell how the ordinary representations (over the complex numbers or the rationals) split into irreducible modular representations. The uniqueness of the above representations was in fact shown by Ascher Wagner in [**12**]. See [**11**] for further information about modular representations of the symmetric group.

Now we return the Problem 5.1 and consider mappings based on the vector space of dimension q^2 of the set of points of the affine plane π' with points $x \in \partial l_\infty$. The group G is generated by the following q^2 mappings corresponding to each point x of π' ... in a slight abuse of notation we often identify π' with the set of points ∂l_∞ and with the vector space corresponding to the subsets of this set.

$$x : \pi' \to \pi', \text{ where } p \mapsto p^{\delta(\pi',\delta x)\partial(\delta x,\pi')}, \ \forall\, p \in \pi'.$$

For the remainder of this section let us consider lines to be subsets of the affine plane π'. That is, we neglect the points on l_∞. Also, if a and b are distinct points of π, $a.b$ denotes the line joining a and b, considered as a point-set.

LEMMA 5.4. *Let x be a point of π'. Then, for all points $p \in \pi'$,*

$$p^x = \begin{cases} p.x + p + x, & \text{if } p \neq x; \\ p, & \text{if } p = x. \end{cases}$$

Thus $x^2 = 1$, where 1 represents the identity linear mapping.

PROOF: $x^{\delta(\pi',\delta x)} = \delta x$ is the set of all lines of π not passing through x, so that $x^x = \partial\delta x \cap \pi' = x \cap \pi' = x$. For $p \neq x$, $p^{\delta(\pi',\delta x)}$ is the set of all lines not passing through p or x. ∂ of this set of $q^2 - q$ lines is the set of $q-1$ points of π on the line $p.x$ not equal to p or x. When we intersect this set with π', the resulting set is $p.x + p + x$, where we neglect the point on l_∞. Next, we can check that if T is a subset of a line M passing through $x \in \pi'$, there holds

$$T^x = \begin{cases} M + x + T, & \text{where } |T \setminus \{x\}| \text{ is odd}, \\ T, & \text{where } |T \setminus \{x\}| \text{ is even}. \end{cases}$$

(Already we can see that there is a relationship with the representation σ; c.f. Lemma 5.6.) Now $x^{x^2} = x^x = x$. Also, if $p \neq x$ and $M = p.x$, then $p^x = M + x + p$ is a set of odd size, and so $p^{x^2} = (M + x + p)^x = M + x + (M + x + p) = p$. Hence x is an involution on every subset of points on M. Since the actions on the $q+1$ lines through x are independent of one-another we see that x is an involution on the whole affine plane π'.

LEMMA 5.5. *In the vector space of all subsets of points of π', G has $q+1$ invariant subspaces V_i of dimension q corresponding to the points $a_0, \ldots, a_q$ on l_∞.*

PROOF: The subspace V_i is generated by the q lines of π' passing through a_i – in $\hat{a}_i + l_\infty$. Here we consider a line as a set of points. The action of G on V_i with the basis of q lines is given by

$$\hat{d}^x = \begin{cases} \hat{d}, & \text{if } x \in \hat{d}; \\ \pi' + \hat{d} + x.a_i, & \text{if } x \notin \hat{d}, \end{cases}$$

for any line d of π' through a_i and point $x \in \pi'$. For brevity, we write d^x although x is defined only on sets of points; with this notation, which we always use henceforth, the above equation becomes

$$d^x = \begin{cases} d, & \text{if } x \in \hat{d}; \\ (\hat{a}_i + l_\infty) + d + x.a_i, & \text{if } x \notin \hat{d}, \end{cases}$$

— in this notation $l^x = \sum_{i=1}^m l_i$ for lines $l, l_1, \ldots, l_m$ means that $\hat{l}^x = \sum_{i=1}^m \hat{l}_i$. Thus the action of G on V_i is seen to be the same as that of S_{q+1} in Theorem 5.2. Now every point p of π' can be obtained as $\pi' + \sum_{d \in \hat{p}} d$. Thus the action of G on the lines of π' determines the action on the points (and vice-versa). In particular we see that in terms of the subspaces V_i and the action on the lines, G may be thought of as a subgroup of the direct product

$$\overbrace{S_{q+1} \times \cdots \times S_{q+1}}^{q+1 \text{ times}}$$

From now on let $G(S)$ denote the subgroup of G generated by the subset of involutions $S \subseteq \pi'$. For example, $G = G(\pi')$, where $\pi' = \partial l_\infty$. An interesting problem, which we only solve for some cases, is to calculate $G(S)$ for any given subset.

THEOREM 5.6. *Suppose $q \geq 5$. Let M be any line of π' – distinct from l_∞. Then $G(M) \cong S_{q+1}$, where the correspondence is induced by $i \in M \leftrightarrow (i\ \infty) \in S_{q+1}$.*

PROOF: Suppose M passes through the point a_0 on l_∞. The subgroup $G(M)$ of G acting on the subspace induced by $\hat{M}$ is S_{q+1} and it is faithful, by Theorem 5.2.

Although it is not strictly necessary for the proof, we can also check that the action on the q subspaces $V_1, \ldots, V_q$ (see above) is essentially the same (with respect to the bases of lines through $a_1, \ldots, a_q$). Hence $G(M)$ is a faithful representation of S_{q+1} in the direct product of the q S_{q+1}'s. On the subspace V_0, however, the action is different. The group induced is the cyclic group Z_2 of order 2. Products of an even number of points of M (in the alternating group A_{q+1}) fix every line through a_0, while products of an odd size take a line d to $\pi' + d + M$. Thus there is a homomorphism from $G(M)$ to Z_2 induced on V_0. In any case we see that $G(M)$ corresponds to a subgroup isomorphic to S_{q+1} in the direct product of $q+1$ S_{q+1}'s above.

Let us consider the line M of π'. We have seen that the q points of $M \in \pi'$ give a representation $G(M)$ of G, isomorphic to S_{q+1}, which splits into two distinct components, the points of M and the points of $\pi' + M$. Let $K_M = \pi' + M$, so that $|K_M| = q^2 - q$. We shall investigate some properties of the representation $G(M)$ on K_M and M.

LEMMA 5.7. *Let κ be the linear mapping $\pi' \to \pi'$ which fixes all points on M and takes a point a of K_M to $K_M + a$. For distinct points x and y of M the following hold, (when we consider points of M to be linear mappings acting on K_M and M).*

(1) $xyx + xy + yx + x + y = \kappa$;
(2) $xyx = yxy$, and $(xy)^3 = 1$;
(3) $\kappa x = x\kappa = x + \kappa + 1$.

PROOF: Consider part (1). Let $a \in K_M$, and let $R = a.x$, $S = a.y$, $u = R \cap \hat{l}_\infty$, $v = S \cap \hat{l}_\infty$, $T = x.v$, $U = u.y$, and $a' = T \cap U$. Also let γ be the set of points of K_M not on R, S, T, or U. Then one can easily check that
$a^1 = a;\ a^x = R + a + x;\ a^y = S + a + y;$
$a^{xy} = \gamma + T + a' + x;\ a^{yx} = \gamma + U + a' + y;\ a^{xyx} = \gamma + a'.$
Summing these equations shows that
$a^{xyx+xy+yx+x+y+1} = a + a' + \gamma + R + S + T + U = K_M = a^{\kappa+1}$, which gives us the answer for the points of K_M. Now if $a \in M$, we have to look at several cases. The first is $a = x$. Then
$x^1 = x;\ x^x = x;\ x^y = M + x + y;\ x^{xy} = M + x + y;\ x^{yx} = y;\ x^{xyx} = y.$
Summing these gives $x^{xyx+xy+yx+x+y+1} = 0$. Similarly $y^{xyx+xy+yx+x+y+1} = 0$.
Finally, if $a \in (M + x + y)$, we have that
$a^1 = a;\ a^x = M + a + x;\ a^y = M + a + y;\ a^{xy} = M + a + x;$
$a^{yx} = M + a + y;\ a^{xyx} = a.$
Summing gives $a^{xyx+xy+yx+x+y+1} = 0$. Hence the equation is satisfied in all cases. Part (2) is proved from part (1) simply by noting that (1) is also valid when we permute x and y. Finally, $(xy)^3 = xyxyxy = (xyx)(xyx) = 1$, as $x^2 = y^2 = 1$, from Lemma 5.4. We leave part (3) as an easy exercise – the hint is to multiply (1) by x, and then simplify.

An alternative approach to part (2) is to use the correspondence of Theorem 5.6. Then $(\infty\ x)(\infty\ y)(\infty\ x) = (x\ y) = (\infty\ y)(\infty\ x)(\infty\ y)$, and $[(\infty\ x)(\infty\ y)]^3 = (\infty\ x\ y)^3 = 1$.

LEMMA 5.8. *For three distinct points x, y, z on M, the following equation is* *satisfied.*

$$(x+1)y(z+1) = xyz + xy + yz + y = 0.$$

PROOF: Consider $a^{x+1} = a^x + a$, where $a \notin M$. This is clearly the line $a.x$ minus the point x ($\in \pi'$). Then it is just a matter of checking that if N is any line not through y, z, or $M \cap l_\infty$, then for points not on M, there holds $N^{yz} = N^y$. (We leave this to the reader.) And so, for the points not on M at least, we have that $(x+1)yz = (x+1)y \implies (x+1)y(z+1) = 0$. It is also easy to see that the formula holds on M.

LEMMA 5.9. *$\langle xyx \mid x \neq y \in M\rangle$ is a group on M that is permutation isomorphic to S_q.*

PROOF: From Theorems 5.2 and 5.6, this is the subgroup S^∞ that fixes ∞, since $(\infty i)(\infty j)(\infty i) = (ij)$, and it is the usual permutation representation of S_q on M.

DEFINITION 5.10. *Let $T(M)$, where M is a line of π', be the set of linear transformations*

$$\{xy \mid x \neq y \in M\} \cup \{x \mid x \in M\} \cup \{1\}.$$

Using Lemmas 5.7 and 5.8, we can reduce any product of points on M to a sum of members of $T(M) \cup \{\kappa\}$. This proves

THEOREM 5.11. *Every product $x_1 \ldots x_n$ of points on M can be reduced to a sum of the transformations in $T(M) \cup \{\kappa\}$.*

Note that the sum of linear transformations above will be unique if it can be proved that $T(M) \cup \{\kappa\}$ is a linearly independent set of transformations of the vector space π'. We leave this question to the reader.

Now let $X = \{x_1, \ldots, x_n\}$ be any set of n points of π'. Let X_i be $X \setminus \{x_i\}$. Then we can define $n+1$ subgroups of $G(X)$ as follows:

$$T_i = \langle X_i\rangle,\ \forall\, 1 \leq i \leq n; \quad T_\infty = \langle x_i x_j x_i \mid i \neq j \in X\rangle.$$

Let (*) denote the condition that x_k and $x_i x_j x_i$ commute for all triples of distinct points x_i, x_j, and $x_k \in X$. If H is any subgroup of G define $H^g := g^{-1}Hg$, for any element g of G. H^g is called a *conjugate subgroup* of H, which is isomorphic to H.

LEMMA 5.12. *Suppose that condition (*) holds. Then*

(1) ${T_\infty}^{x_i} = T_i$, *if* $1 \leq i \leq n$;
(2) $T_i^{x_i} = T_\infty$, *if* $1 \leq i \leq n$;
(3) $T_i^{x_j} = T_i$, *if* $i \neq j$.

Thus T_i and T_∞ are conjugate subgroups of G, ($\forall\, 1 \leq i \leq n$).

PROOF:

(1) ${T_\infty}^{x_i}$ is the subgroup generated by elements of the form $x_i x_k x_j x_k x_i$, where i, j, and k are all distinct, and also by elements of the form $x_i x_i x_j x_i x_i$, where $i \neq j$, and $x_i x_k x_i x_k x_i$, where $i \neq k$. From (*) the terms of the first kind simplify to $x_k x_j x_k$, which are in T_i. Terms of the second kind simplify to x_j

– also in T_i. And terms of the third kind simplify to $x_k \in T_i$. (Remember that $x_i{}^2 = 1 = (x_i x_k)^3$.) Thus $T_\infty{}^{x_i} \subseteq T_i$. Also $T_i \subseteq T_\infty{}^{x_i}$, because the generators for T_i are found in terms of the second or third kind above. Thus $T_\infty{}^{x_i} = T_i$.

(2) This follows from (1) as $x_i{}^2 = 1$.

(3) If $i \neq j$, $T_i{}^{x_j} = \langle x_j x_k x_j \mid k \neq i \in X \rangle \subseteq T_i$. Thus $T_i = T_i{}^{x_j{}^2} \subseteq T_i{}^{x_j} \subseteq T_i$, which implies part (3).

PROPOSITION 5.13. *The group $G(M) \cong S_{q+1}$ acts by conjugation on the $q+1$ subgroups T_i and T_∞ constructed from any line M of π', and this action is equivalent to the natural action of S_{q+1} as a permutation group.*

PROOF: From the correspondence of Theorem 5.6 it is clear that (*) holds with respect to triples of points on M; using Lemma 5.12 we only have to show that the subgroups are indeed distinct. This is obvious from the correspondence.

There are still some further things to be said about the group G of the affine plane but we shall have to consider non-collinear points before the differences between various affine planes emerge.

DEFINITION 5.14. *For any subset of points $N \subseteq \hat{l}_\infty$ let G_N denote the subgroup of G that fixes every line of π' through a point of N. Also, let G^N denote the "projection" of G onto N. That is, we consider G to act on the lines of π' through N, disregarding the other lines of π'. G^N is the image of the "projection" homomorphism $\gamma_N : G \to G^N$. This mapping has kernel G_N, which is therefore a normal subgroup of G.*

We saw in Lemma 5.5 that the action of the group G on the lines can be considered as a subgroup of the direct product of $q+1$ copies of S_{q+1}. This can be improved to the following. A_{q+1} denotes the alternating group, which is the subgroup of S_{q+1} of all even permutations. We assume that $q \geq 5$, so that A_{q+1} is simple.

THEOREM 5.15. *The action of G on the lines of π' is as a subgroup of the group*

$$\overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q+1 \text{ times}} \cup \overbrace{(S_{q+1} \setminus A_{q+1}) \times \cdots \times (S_{q+1} \setminus A_{q+1})}^{q+1 \text{ times}}.$$

PROOF: The product of an even number of points of π' is in the A_{q+1} of the subspace of each point on l_∞, while the product of an odd number of points is in the complementary coset of these subgroups.

Note that the order of the above group is $[(q+1)!]^{q+1}/2^q$.

THEOREM 5.16. *Let $q \geq 5$, let l be a line of π' distinct from l_∞, let x be a point not on these two lines, and let $L_x := \hat{l} + x$. Then the group $G(L_x) \leq G$ which is generated by x and the points on l, is equal to the group*

$$A_3 \times \overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q \text{ times}} \cup (S_3 \setminus A_3) \times \overbrace{(S_{q+1} \setminus A_{q+1}) \times \cdots \times (S_{q+1} \setminus A_{q+1})}^{q \text{ times}}.$$

PROOF: Let $a_0 \in l_\infty$ be the infinite point of l and let $a_1 \in l_\infty \setminus \{a_0\}$. We label the remaining points on l_∞ with $a_2, \ldots, a_q$. As in the construction in Lemma 5.5 let V_i be the subspace generated by the q lines of π' passing through a_i. The action, $G^{\{a_i\}}$, of G on V_i with the basis of q lines is the same as that of S_{q+1} in Theorem 5.2. We define the affine points on l as $x_i := \hat{l} \cap x.a_i$ for $i = 1, \ldots, q$. With the correspondence of Theorem 5.2 a point x_j becomes the transposition $(\infty\ j)$ in V_i and similarly x becomes the transposition $(\infty\ 1)$ in V_1. We construct a generalised projectivity that induces a 3-cycle in V_1 and the identity in all other V_i's.

As a first step consider the product $\beta_{i,j} := (xx_ix_j)^2$ for $i \neq j$, and $i, j > 1$. In V_1 this mapping corresponds to the involutory permutation

$$(\infty\ 1)(\infty\ i)(\infty\ j)(\infty\ 1)(\infty\ i)(\infty\ j) = (\infty\ i)(1\ j).$$

Furthermore, since points on a line through a_k induce the same transposition in V_k and because points in $\beta_{i,j}$ appear in pairs, it easily follows that $\beta_{i,j}$ induces the identity in V_0, V_i, and V_j.

Next let $i_1, i_2, i_3 > 1$ be distinct. We define γ_{i_1,i_2,i_3} to be the commutator of β_{i_1,i_2} and β_{i_1,i_3}, i.e. $\gamma_{i_1,i_2,i_3} = \beta_{i_1,i_2}\beta_{i_1,i_3}\beta_{i_1,i_2}{}^{-1}\beta_{i_1,i_3}{}^{-1}$. Since β_{i_1,i_2} and β_{i_1,i_3} induce the identity in V_0, V_{i_1}, V_{i_2} and V_0, V_{i_1}, V_{i_3} respectively, γ_{i_1,i_2,i_3} induces the identity in V_0, V_{i_1}, V_{i_2}, and V_{i_3}. In V_1 we obtain the following permutation:

$$(\infty\ i_1)(1\ i_2)(\infty\ i_1)(1\ i_3)(\infty\ i_1)(1\ i_2)(\infty\ i_1)(1\ i_3) = (1\ i_3\ i_2).$$

We continue in the same way. Let $i_1, i_2, i_3, i_4 > 1$ be distinct and define γ_{i_1,i_2,i_3,i_4} to be the commutator of γ_{i_1,i_2,i_3} and β_{i_1,i_4}. Then γ_{i_1,i_2,i_3,i_4} induces the identity in V_0, V_{i_1}, V_{i_2}, V_{i_3}, and V_{i_4}, thus raising the number of those subspaces by 1. In V_1 we obtain again a 3-cycle:

$$(1\ i_3\ i_2)(\infty\ i_1)(1\ i_4)(1\ i_2\ i_3)(\infty\ i_1)(1\ i_4) = (1\ i_4\ i_2).$$

By induction one finds that the successive commutator $\gamma_{i_1,\ldots,i_{q-1}}$, where $\gamma_{i_1,\ldots,i_{k+1}} := \gamma_{i_1,\ldots,i_k}\beta_{i_1,i_{k+1}}\gamma_{i_1,\ldots,i_k}{}^{-1}\beta_{i_1,i_{k+1}}{}^{-1}$, for $k = 3, \ldots, q-2$, acts trivially on all subspaces V_i except for V_1; on the latter subspace the commutator induces the 3-cycle $(1\ i_{q-1}\ i_2)$. Varying the order of the indices $i_1, \ldots, i_{q-1}$ we obtain all 3-cycles $(1\ i\ j)$ where $i, j > 1$. Conjugation with x_j, i.e. $(\infty\ j)$, produces

$$(\infty\ j)(1\ i\ j)(\infty\ j) = (1\ i\ \infty)$$

Hence we can construct any 3-cycle $(1\ i\ j)$ where $i, j \in \{2, \ldots, q, \infty\}$. They generate a group isomorphic to A_{q+1}. This shows that

$$H_1 = 1 \times A_{q+1} \times \overbrace{1 \times \cdots \times 1}^{q-1 \text{ times}} \leq \overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q+1 \text{ times}}$$

is contained in $G(L_x)$.

Since a_1 was arbitrary on $l_\infty \setminus \{a_0\}$ we can do the same construction for any subspace V_j, $j \neq 0$. This shows that

$$1 \times \overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q \text{ times}}$$

is contained in $G(L_x)$. Since all points x_i represent the same transposition in V_0, the group $G(L_x)$ obviously induces the symmetric group S_3 in V_0. As the product xx_1 induces a 3-cycle in V_0 and a member of A_{q+1} in all other V_i's we find that

$$H = A_3 \times \overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q \text{ times}}$$

is a subgroup of $G(L_x)$.

Finally, a point induces a transposition in each V_i, and thus cannot be contained in H. Therefore $G(L_x)$ must be the full group

$$A_3 \times \overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q \text{ times}} \cup (S_3 \setminus A_3) \times \overbrace{(S_{q+1} \setminus A_{q+1}) \times \cdots \times (S_{q+1} \setminus A_{q+1})}^{q \text{ times}}.$$

THEOREM 5.17. *The group of the generalised projectivities G proposed by Problem 5.1 is equal to the full group*

$$\overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q+1 \text{ times}} \cup \overbrace{(S_{q+1} \setminus A_{q+1}) \times \cdots \times (S_{q+1} \setminus A_{q+1})}^{q+1 \text{ times}}$$

of Theorem 5.15 above. Furthermore, the points on two lines intersecting in an affine point form a minimal generating set for G.

PROOF: We keep the notation as in the proof of the preceding Theorem. Let l' be a second line not passing through the point a_0. Taking a suitable product of points on l' the full alternating group A_{q+1} is induced in V_0. Thus we have

$$\overbrace{A_{q+1} \times \cdots \times A_{q+1}}^{q+1 \text{ times}}$$

as a subgroup of G. Again, a point induces a transposition in each V_i, and thus cannot be contained in this group. Thus G is the full group.

Let s be the point of intersection of l and l' and assume that l' passes through a_1. If we delete s, then the remaining points of l and l' generate a group that induces S_q in any V_i, $i = 2, \ldots, q$, since the line $a_i.s$ is always fixed in V_i. If we delete a point $y \neq s$ on l or a point $y' \neq s$ on l', then similarly the remaining points generate a group that induces S_q in V_1 or V_0 respectively, since $a_1.y$ or $a_0.y'$ is always fixed. Thus the points on l and l' form a minimal generating set for G.

REMARK 5.18.

(1) Obviously, the $q-1$ points different from s on the second line l' can be replaced by any $q-1$ points such that each line through a_0, and distinct from l and l_∞, contains one of the points. Generalising the construction of Theorems 5.16 and 5.17 one is led to conjecture that any blocking set of points of the affine plane π' forms a generating set for G, and that the minimal generating sets correspond to the minimal sets of points "hit" by every line of the affine plane. These conjectures are supported by many examples run using the symbolic algebra package MAPLE.

(2) Given $S \subseteq P$ and $T \subseteq L$ we can extend the generalised projectivities $\delta(S,T)$ and $\partial(T,S)$ in a natural way by

$$A \mapsto (A \cap S)^{\delta(S,T)} + (A \cap \bar{S})^{\delta(\overline{S},\overline{T})},$$

for $A \subseteq P$; and

$$B \mapsto (B \cap T)^{\partial(T,S)} + (B \cap \overline{T})^{\partial(\overline{T},\overline{S})},$$

for $B \subseteq L$ respectively. In particular, given an anti-flag (p,l) we can extend the generalised projectivities $\delta(\partial l, \delta p)$ and $\partial(\delta p, \partial l)$. If we work with these extensions we obtain the group G of Problem 5.1 acting on the whole projective plane π and each member of G extends to the identity on l_∞. In general, however, we obtain a larger group. If we look at the full generalised projectivity group of the affine plane $G' := GP(\{\partial l \mid l \in L\}, \{\delta p \mid p \in P\})$, then the extension shows that the von Staudt group $GP(\{\hat{l} \mid l \in L\}, \{\hat{p} \mid p \in P\})$ must be involved in the group G' and thus it must be possible to distinguish projective planes by their groups G'.

Next we are led to a consideration of the interaction of the automorphisms (or collineations) of the affine plane and the group of generalised projectivities G. The important automorphisms that we consider are

a) *Translations*: fixing each point on l_∞ and fixing all or no points of π'. The non-identity translations τ have a unique centre $c(\tau)$ on l_∞ such that all lines through $c(\tau)$ are fixed by τ.

b) *Homologies*: fixing each point on l_∞ and fixing all points or exactly one point of π'. The non-identity homologies ξ have a unique centre $c(\xi)$ not on l_∞ such that all lines through $c(\xi)$ are fixed by ξ.

First note that one of the axial collineations above can be represented as an element of G if and only if there is a product of points of π', which gives an element of G that permutes the points of π', and permutes the lines of π' in the same way as the collineation. (Since every element of G is linear, it is easy to see that such a mapping permuting points and lines must be an axial collineation.) By Remark 5.18(2) these are the only collineations of π' that can be represented as an element of G.

THEOREM 5.19. *Every translation of π' is represented as an element of G.*

PROOF: If the translation is the identity mapping then this is trivial. Now suppose that we are given a non-identity translation τ. Let M be any line of π' passing through the centre $c(\tau)$ of τ. Now τ has n' point-orbits of size $n = q/n'$ on M. (Otherwise, some power of τ would be a non-identity translation with a fixed point in π'; also, since q is odd, both n and n' are odd and n is the order of τ.) Let the i'th orbit of τ on M be

$$\{m_i,\ m_i^{\tau},\ \ldots,\ m_i^{\tau^{n-1}}\},\ \forall\, 1 \le i \le n'.$$

Consider the following product of points in $G(M)$:

$$\prod(\tau, M) := \prod_{i=1}^{n'} \prod_{j=0}^{n} m_i^{\tau^j}.$$

First we see that this product contains $n'(n+1)$ points, which is even, and so the product with respect to $c(\tau)$ is the identity. Thus $\prod(\tau, M)$ fixes all lines through $c(\tau)$. Also, each subproduct $\prod_{j=0}^{n} m_i^{\tau^j}$ of points on each orbit emulates the action of τ on that orbit; c.f. Lemma 5.9. (Note that $m_i^{\tau^n} = m_i$; hence $\prod_{j=0}^{n} m_i^{\tau^j} = \prod_{j=1}^{n-1} m_i m_i^{\tau^j} m_i^{-1}$. The subproduct fixes ∞ in the S_{q+1} of M. Also, these subproducts commute with one-another. And it doesn't matter where one starts in the subproduct, as long as one finishes with the same element as one starts.) Since the subproducts fix ∞ in $G(M)$ we see that the same is true for the action on the lines through each point on l_∞. Hence $\prod(\tau, M)$ permutes each set of lines through every point at infinity. Thus this product of points in G has exactly the same action on the points and lines as the translation τ.

Note that in the above proof the line M can be chosen as any of the q lines through the centre of the translation τ. Hence we see that $G(M)$ and $G(N)$ intersect at least in the group of translations that have centre $M \cap N$, if M and N are any pair of lines passing through the same point of l_∞. Also, for every non-identity translation of π' we obtain relations in the group G such that a point of $M \cup N$ above is given by a product of the remaining points of $M \cup N$.

Using a similar method we obtain

THEOREM 5.20. *Every homology of π' that has an odd number of orbits on each (affine) line through the centre is represented as an element of G.*

PROOF: If the homology is the identity mapping then this is trivial (the identity has q orbits (= points) on each (affine) line). Now suppose that we are given a non-identity homology ρ with centre $c(\rho)$. Let $M_1, \ldots, M_{q+1}$ be the lines through $c(\rho)$ and let $a_k := \hat{M}_k \cap \hat{l}_\infty$. On each of these lines ρ has n' orbits of size $n = (q-1)/n'$ and one orbit of size one (the fixed point $c(\rho)$). Thus n' must be even by assumption. Let the i'th orbit of ρ on M_k be

$$\{m_{ik},\ m_{ik}^{\rho},\ \ldots,\ m_{ik}^{\rho^{n-1}}\},\quad \forall\, 1 \le i \le n', 1 \le k \le q+1.$$

Consider the following product of points in G:

$$\rho' = \prod_{k=1}^{q+1} \prod_{i=1}^{n'} \prod_{j=0}^{n} m_{ik}^{\rho^j}.$$

As in the proof of the preceding theorem each subproduct $\prod_{j=0}^{n} m_{ik}^{\rho^j}$ of points on each orbit emulates the action of ρ on that orbit. Also, these subproducts for fixed k commute with one-another. Since $n'(n+1) = q - 1 + n'$ is even, the product

$$\rho_k = \prod_{i=1}^{n'} \prod_{j=0}^{n} m_{ik}^{\rho^j}$$

fixes each line through the infinite point a_k and it emulates the action of ρ on the set of lines through a_l, distinct from a_k. Now the whole product $\rho' = \prod_{k=1}^{q+1} \rho_k$ acts on the set of lines through a_l, since $\rho_l^q = \rho_l$ because $\rho_l^{q-1} = \rho^{q-1} = 1$. This shows that ρ' acts on the set of lines as ρ does.

Note that the condition of the theorem is satisfied for all homologies of odd order. Also, the relation $nn' = q - 1$ shows that the number of orbits $n' + 1$ on a central line is odd if the order n of the homology ρ is not divisible by the highest power of 2 contained in $q - 1$. In particular no homology of order $q - 1$ can be obtained in this way.

By dualisation and by extension to the whole plane one obtains the following.

COROLLARY 5.21. *Every elation of the projective plane π and every homology that has an even number of orbits on each (projective) line through the centre is represented as an element of the group $GP(\{\partial l \mid l \in L\}, \{\delta p \mid p \in P\})$, where the base set is a suitably chosen affine plane.*

6. Generalised Projectivities of Dimension $q^2 + q$

In this section we investigate the case of generalised projectivities with element size q^2+q. These are the maximal proper subsets of points (or lines) of the projective plane π. A GP of this dimension is generated by the complements of antiflags. We shall fix a point p and consider the group generated by complements of antiflags containing p. We proceed as in §5, but it turns out that things are simpler.

PROBLEM 6.1. *Let p_∞ be a fixed point of π. Classify the group*

$$G = GP(\{\overline{p}_\infty\}, \{\overline{l} \mid l \in \delta p_\infty\}).$$

From now on we shall investigate the group of generalised projectivities proposed by the above problem. We shall see that this gives rise to a representation of the symmetric group S_{q^2+1}. We base the group on the vector space generated by the point set $\overline{p}_\infty$. Since $\overline{p}_\infty$ is the only set of points appearing in its definition, the group of generalised projectivities G is obviously generated by all mappings of the form

$$\delta(\overline{p}_\infty, \overline{l})\partial(\overline{l}, \overline{p}_\infty),$$

where l is any line not passing through p_∞. For brevity, we denote this mapping by $x \mapsto x^l$.

LEMMA 6.2. *Let l be a line not passing through p_∞. Then for all points $x \in \overline{p}_\infty$*

$$x^l = \begin{cases} \partial l + p_\infty + x, & \text{if } x \in \partial l; \\ x, & \text{if } x \in \hat{l}. \end{cases}$$

PROOF: Suppose $x \in \partial l + p_\infty$. Then $\delta x \cap \overline{l} = \delta x + l$. Now

$$\partial(\delta x + l) \cap \overline{p}_\infty = x + \partial l \cap \overline{p}_\infty = \partial l + p_\infty + x,$$

which is the value of x^l. Further, if $x \in \hat{l}$, then $\delta x \cap \overline{l} = \delta x$, and

$$\partial(\delta x) \cap \overline{p}_\infty = x \cap \overline{p}_\infty = x.$$

Thus we have the value of x^l in this case.

Note that $\partial l + p_\infty = \hat{l} + \overline{p}_\infty$. Here are some of the conventions that we use for the remainder of this section. As in the proof of Lemma 5.5 we set $m^l := \sum_{d \in D} d$ for some set of lines D, if $\hat{m}^l = \sum_{d \in D} \hat{d}$. However, it is to be noted that there is a single relation that holds between sums of lines; since there are $q+1$ lines through each point, when we consider lines to be subsets there holds $\sum_{y \in L} \hat{y} = 0$ — we can write this as $L = 0$. Thus a subset of lines is equivalent to its complement in L and we can consider line-sets to be modulo L. This will cause no problem when we consider the action of G on the subsets of $\overline{p}_\infty$. We restrict all sets to $\overline{p}_\infty$ ... for example $\hat{m}$, where $m \in \hat{p}_\infty$, actually is the set of q points $\hat{m} + p_\infty$.

As an aside ... for $x \in \overline{p}_\infty$ there holds

$$\partial(x + p_\infty) = \hat{x} + \hat{p}_\infty = x,$$

when we take in account the convention that lines are subsets of $\overline{p}_\infty$. Since the mapping corresponding to l conserves the parity of sets of points we could define

$$m^l := \sum_{x \in \hat{m}^l} (\hat{x} + \hat{p}_\infty) = |\hat{m}|\hat{p}_\infty + \sum_{x \in \hat{m}^l} \hat{x}.$$

By linear extension this defines a mapping on the vector space of all subsets of L.

LEMMA 6.3. *Let l be a line not passing through p_∞. Then*

$$m^l = \begin{cases} \delta p_\infty + m + l, & \text{if } m \in \delta p_\infty, m \neq l; \\ m, & \text{if } m \in \hat{p}_\infty, \text{ or } m = l, \end{cases}$$

for every line m. Thus $l^2 = 1$, where 1 represents the identity linear mapping.

PROOF: By Lemma 6.2 we have $\hat{l}^{\,l} = \sum_{x \in \hat{l}} x^l = \sum_{x \in \hat{l}} x = \hat{l}$, and if $m \in \hat{p}_\infty$

$$\hat{m}^l = \sum_{x \in \hat{m}} x^l = \hat{l} \cap \hat{m} + p_\infty + \sum_{x \in \hat{m}, x \in \partial l, x \neq p_\infty} (\partial l + p_\infty + x) = \hat{m}.$$

Thus $m^l = m$, $\forall\, m \in \hat{p}_\infty + l$. If $m \in \delta p_\infty + l$, then we find that

$$\hat{m}^l = \sum_{x \in \hat{m}} x^l = \hat{l} \cap \hat{m} + \sum_{x \in \hat{m}, x \in \partial l} (\partial l + p_\infty + x) = \partial l + p_\infty + \hat{m} = \overline{p}_\infty + \hat{l} + \hat{m}.$$

Since this calculation is in terms of points we must convert to a sum of lines. It is only necessary to note that the sum of lines (converted to a point-set)

$$\delta p_\infty + m + l = L + \hat{p}_\infty + m + l = \hat{p}_\infty + m + l.$$

But then the set of points on $\hat{p}_\infty$ is $\overline{p}_\infty = P + p_\infty$. These calculations also prove the stated form of m^l in every case.

The formulae in Lemma 6.2 yield $x^{l^2} = x$, if $x \in \hat{l}$; also $\hat{l}^{\,l} = \hat{l}$ and $\overline{p}_\infty{}^l = \overline{p}_\infty$. Thus $x^{l^2} = (\overline{p}_\infty + \hat{l} + x)^l = \overline{p}_\infty + \hat{l} + \overline{p}_\infty + \hat{l} + x = x$, $\forall\, x \in \partial l + p_\infty$. This shows that $l^2 = 1$ as a group on the points. Similarly we can use the formulae for the action of l on lines, and because $(\hat{p}_\infty)^l = \hat{p}_\infty$ and also $L^l = L (= 0)$, we obtain

$$m^{l^2} = (\delta p_\infty + m + l)^l = \delta p_\infty + (\delta p_\infty + m + l) + l = m, \ \forall m \in \delta p_\infty + l;$$

obviously, $m^{l^2} = m$, if $m \in \hat{p}_\infty$, or $m = l$. Hence $l^2 = 1$ as a group on the lines.

THEOREM 6.4. *The group of generalised projectivities G of Problem 6.1 is isomorphic to S_{q^2+1}.*

PROOF: Consider the vector space of dimension $q^2 + q$ which is the set of all subsets of $\overline{p}_\infty$. Then L corresponds to a set of $q^2 + q + 1$ non-zero vectors satisfying one non-trivial linear equation: the sum of all lines is zero. Thus L is a "circuit" of the corresponding matroid — every proper subset of lines is linearly independent. Let V and W be the subspaces generated by δp_∞ and $\hat{p}_\infty$ respectively. These subspaces have dimension q^2 and $q + 1$ respectively, and they intersect in the 1-dimensional subspace generated by $\overline{p}_\infty$, which is the set of points covered by both δp_∞ and $\hat{p}_\infty$. Each vector of W and also the space V is fixed by the group G; see Lemma 6.3. Thus the group G is linearly (and faithfully) represented on V. We compare the action of the generators $l \in \delta p_\infty$ on V with that given in Theorem 5.2. To do so, we adopt the notation of Theorem 5.2; let $\delta p_\infty = \{l_1, \ldots, l_{q^2}\}$ and $N = \{1, \ldots, q^2\}$. Then, according to Lemma 6.3, a generator l_i is given by

$$j^{l_i} = \begin{cases} j, & \text{if } j = i; \\ N + j + i, & \text{if } j \neq i. \end{cases}$$

Hence l_i has the same matrix representation as the transposition $\alpha_i = (\infty\ i) \in S_{q^2+1}$. As G is generated by the l_i's and S_{q^2+1} is generated by the α_i's, both groups must be isomorphic.

We leave the reader with the following observation. The representation G of S_{q^2+1}, acting on the set of all subsets of lines of δp_∞, has a subgroup (fixing ∞) which is the standard group of all permutations of these lines. Also, G fixes every line of $\hat{p}_\infty$. Thus one can prove

THEOREM 6.5. *Every central collineation with centre p_∞ can be represented as an element of the group of generalised projectivities G of Problem 6.1.*

7. Conclusion

We have shown how non-trivial groups of generalised projectivities arise from any projective plane of odd order. It would be possible to define even more general groups by considering groups generated by the inverse mappings. Indeed, the consideration of collections of mappings that might be singular could be interesting. Generalised projectivity groups can also be defined in projective planes of infinite order (especially with finite subsets of points and lines) or in planes of even order.

Another extension of these ideas would be to consider representations modular p, where p is a divisor of $q-1$, (q the order of the plane). The crucial definitions of coboundary and boundary (mod p) would be then:

$$\delta S := |S|L - \sum_{x\in S} \hat{x} \pmod p, \text{ and } \partial T := |T|P - \sum_{y\in T} \hat{y} \pmod p, \ (S \subseteq P, T \subseteq L).$$

Many of the results in this paper would still hold. However, we leave such discussions to later papers.

There are two main applications of this theory that the authors have in mind. Firstly, one could find interesting representations of finite groups by considering appropriate finite projective planes. And secondly, one could use the well-developed theory of finite groups to enhance that of finite projective planes. All one needs to do is find appropriate groups of generalised projectivities.

REFERENCES

1. T. Brylawski and D. Kelly, "Matroids and Combinatorial Geometries," Carolina Lecture Series, Department of Mathematics, Uni. of North Carolina at Chapel Hill, 1980.
2. D.G. Glynn, *The construction of self-dual binary codes from projective planes of odd order*, Proc. 16th Australasian Conf. on Comb. Math. and Comb. Computing, Australasian J. Combinatorics (to appear).
3. ————, *The matroid properties of the self-dual binary code of a projective plane of odd order*, (preprint).
4. J.W.P. Hirschfeld, "Projective Geometries over Finite Fields," Oxford Uni. Press, Oxford, 1979.
5. ————, "Finite Projective Spaces of Three Dimensions," Clarendon Press, Oxford, 1985.
6. ————, *Quadrics over Finite Fields*, Academic Press, London - New York, Symposia Math. **XXVIII** (1986), 53–87.
7. D.R. Hughes and F.C. Piper, "Projective Planes," Springer, New York, Heidelberg, Berlin, 1973.
8. F.J. MacWilliams and N.J.A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, New York, Oxford, 1977.
9. P. Plaumann and K. Strambach, "Geometry - von Staudt's Point of View," NATO Advanced Study Institute Series C, Reidel, Dordrecht, Boston, London, 1981.
10. V. Pless, "Introduction to the Theory of Error-Correcting Codes," Wiley, New York, 1982.

11. G. de B. Robinson, “Representation Theory of the Symmetric Group,” Edinburgh University Press, Edinburgh, 1961.

12. A. Wagner, *The faithful linear representation of least degree of S_n and A_n over a field of characteristic 2*, Math. Z. **151** (1976), 127–137.

13. ——————, *The faithful linear representations of least degree of S_n and A_n over a field of odd characteristic*, Math. Z. **154** (1977), 103–114.

1980 *Mathematics subject classifications*: 51E15, 51E20, 05B25, 94B05, 11T71