Finite geometry after Aschbacher's Theorem: PGL(n, q) from a Kleinian viewpoint

Peter J. Cameron

Abstract

Studying the geometry of a group G leads us to questions about its maximal subgroups and primitive permutation representations (the G-invariant relations and similar structures, the base size, recognition problems, and so on). Taking the point of view that finite projective geometry is the geometry of the groups PGL(n, q), Aschbacher's theorem gives us eight natural families of geometric objects, with greater or smaller degrees of familiarity. This paper presents some speculations on how the subject could develop from this point of view.

1 Introduction

The worldwide fellowship of finite geometers has some features in common with the Pythagorean brotherhood (as described by Jean Doyen at the conference). I hope that I don't suffer the fate of Hippasos for revealing the secret that, in the last decade or so, a number of initiates have questioned the direction of future research in the subject. If Pythagoras will not inspire me, I can invoke the help of two mathematicians of more recent times, whose names are in my title.

The central object of finite geometry is the projective space PG$(n-1, q)$. Now, projective geometry has many different meanings. A topologist's real projective plane is the simplest closed non-orientable 2-manifold, obtained from the unit square by identifying each pair of opposite sides in opposite senses. A computer scientist uses it for the practical business of putting graphics on a screen.

Even to a finite geometer, there are several aspects. It can be regarded as a lattice, whose elements are the subspaces, ordered by inclusion. It is a building, whose chambers are the maximal flags of subspaces, two chambers i-adjacent if they agree in all dimensions except i. It may be a geometry in Buekenhout's sense, whose varieties are all the subspaces, and incidence is symmetrised inclusion. Probably, we are more used to thinking of it as a finite set of points, equipped with various distinguished subsets called 'subspaces'. The translations between one viewpoint and another are not difficult; but choice of viewpoint influences how we think about the projective geometry, and how we choose to generalise it.

For example, the chamber system approach fits most naturally into the scheme of buildings, BN-pairs, algebraic groups, and so on. On the other hand, from the point of view of complexity, note that $\mathrm{PG}(n-1,q)$ has roughly q^n points, $q^{n^2/4}$ subspaces of all dimensions, and $q^{n^2/2}$ maximal flags.

The theme of Felix Klein's *Erlanger Programm* is that geometry comes from groups. If we are given the group of a geometry, then interesting geometrical configurations are those stabilised by interesting subgroups of the group.

In this article, I want to draw attention to some implications of this viewpoint for the geometry $\mathrm{PG}(n-1,q)$. We know that the full collineation group of the geometry is $\mathrm{P\Gamma L}(n,q)$; for most purposes, we can work in the subgroup $\mathrm{PGL}(n,q)$, or even in the covering matrix group $\mathrm{GL}(n,q)$. The subgroups of these groups are now much better understood, and I want to look at the implications of this understanding for a Kleinian view of the geometry. Very little here is original, but I hope to show that this point of view leads to many interesting questions.

The main topics of geometry can be regarded as *axiomatisation* (or *recognition*), and the study of *configurations* or subsets. There is no sharp dividing line between the two, and many questions blend from one to the other.

For further information on permutation groups, see Wielandt [35] or Cameron [6]; for classical groups, Artin [1] or Dieudonné [11], or Kleidman and Liebeck [20] for their maximal subgroups; and for the finite simple groups, Gorenstein [14] or the $\mathbb{ATLAS}$ [9], or Carter [8] for the Lie-theoretic viewpoint.

2 Aschbacher's Theorem

Since the Classification of Finite Simple Groups was announced in 1980 (see Gorenstein [14]), one of the main areas of interest in finite group theory has been listing the maximal subgroups of almost simple groups. There are several sources for this interest. Some are considered later in this paper. One of the principal ones is the study of primitive permutation groups, along the lines suggested by the O'Nan–Scott Theorem [30]. This shows that the classification of primitive permutation groups can be 'reduced' (modulo various 'extension' problems) to two types: those groups which have an elementary abelian regular normal subgroup V (an n-dimensional vector space over $\mathrm{GF}(p)$, where p is prime), in which the stabiliser of the origin is a primitive irreducible linear subgroup of $\mathrm{GL}(n,p)$; and those groups which are almost simple, in which the point stabiliser is a maximal subgroup. This meant that it was necessary to study maximal subgroups of almost simple groups, and primitive irreducible linear groups.

Both of these problems point towards Aschbacher's Theorem [2]. Since the Classification, we know that 'most' simple groups are classical groups, of which $\mathrm{PSL}(n,q)$ is the prototype. Also, the first step towards finding all linear groups is to find the maximal ones.

The O'Nan–Scott Theorem was originally not about primitive permutation groups, but about maximal subgroups of symmetric and alternating groups. If such a subgroup is intransitive or imprimitive, then it is the full stabiliser of a subset or a partition, and these are easily described; so it is necessary only to examine the primitive maximal subgroups. Aschbacher's Theorem does a similar job for classical groups, though I will concentrate on the general linear groups.

The O'Nan–Scott Theorem states that a maximal subgroup of S_n or A_n either belongs to one of five easily described classes of 'large' subgroups (stabilisers of subsets or partitions, wreath products of symmetric groups in the product action, diagonal groups, and affine groups), or else is almost simple. Aschbacher's Theorem has a similar form. Though it applies to all types of classical groups, I will consider only the case of the (projective) linear groups. First, we describe the classes of 'large' subgroups of $G = \mathrm{PGL}(n,q)$ which occur. Let V be the underlying n-dimensional vector space over $\mathrm{GF}(q)$.

$\mathcal{C}_1$: Stabilisers of subspaces of V.

$\mathcal{C}_2$: Stabilisers of direct sum decompositions of V into subspaces of the same dimension.

$\mathcal{C}_3$: Stabilisers of extension fields of $\mathrm{GF}(q)$ of prime degree.

$\mathcal{C}_4$: Stabilisers of tensor product decompositions $V = V_1 \otimes V_2$.

$\mathcal{C}_5$: Linear groups over subfields of prime index.

$\mathcal{C}_6$: Normalisers of r-groups of symplectic type, where r is a prime different from p.

$\mathcal{C}_7$: Stabilisers of tensor product decompositions $V = \bigotimes_{i=1}^t V_i$, where the V_i all have the same dimension.

$\mathcal{C}_8$: Classical groups.

Theorem 2.1 (Aschbacher's Theorem) *Let H be a subgroup of* $\mathrm{PGL}(n,q)$*, not containing* $\mathrm{PSL}(n,q)$*. Then either* *(a) H is contained in a member of one of the classes $\mathcal{C}_1$–$\mathcal{C}_8$; or*

(b) H is almost simple and is induced by an absolutely irreducible subgroup modulo scalars.

At first glance, this appears a very powerful result. On closer inspection, the theorem suggest at least the strategy of the proof. For example, if G is reducible, it fixes a subspace; if it is irreducible but not absolutely irreducible, then by Schur's Lemma it fixes an extension field; if it has a non-trivial normal subgroup, then Clifford's Theorem indicates how to decompose the space.

It next appears that the weakness of the theorem is that all the difficulties are swept into the ragbag case (b). Even such natural examples as $G = \mathrm{GL}(m,q)/\{\pm 1\}$, embedded in $\mathrm{GL}(n,q)$ (for $n = \binom{m}{2}$) by the action of $\mathrm{GL}(m,q)$ on the exterior square of its natural module, falls under case (b) for $n > 4$. (For $n = 4$, G preserves the Klein quadric, and is in $\mathcal{C}_8$.) The gain is that, from the Classification of Finite Simple Groups [14], we can list the candidates for G; all we have to do is to determine their absolutely irreducible representations over $\mathrm{GF}(q)$. There remains the question of the maximality of the various subgroups; this is dealt with by Kleidman and Liebeck [20].

The classification of finite simple groups allows very strong general assertions to be made about the groups in case (b). For example, Liebeck [24] showed:

Theorem 2.2 *Let H fall under case (b) in Aschbacher's Theorem. Then either H is S_m or A_m, with $m = n+1$ or $m = n+2$, or H has order at most q^{3n}.*

In this theorem, the symmetric or alternating group acts on the set of words with coordinate sum zero, or (if the characteristic of the field divides m) the quotient of this space modulo constant words. For even moderate values of n, the bound q^{3n} is very small compared to the order of $\mathrm{PGL}(n,q)$ (approximately cq^{n^2-1}).

The knowledge of maximal subgroups of the general linear group given by Aschbacher's Theorem is important in other areas besides geometry. One of these is the computational investigation of matrix groups. The number of bits of information in a 100×100 matrix over $\mathrm{GF}(2)$ is approximately the same as for a permutation on 1146 points (this is just the assertion that $\mathrm{GL}(100,2)$ has approximately the same order as S_{1146}). Permutation groups of this degree are now routinely handled by computer, and we might expect that groups of 100×100 matrices would be as easy. But the smallest permutation representation of $\mathrm{GL}(100,2)$ has degree $2^{100} - 1 \approx 1.268 \times 10^{30}$, far too large for any foreseeable computer. So another method must be found.

One basic question is to decide whether a given set of $n \times n$ matrices over $\mathrm{GF}(q)$ generates at least $\mathrm{SL}(n,q)$. This will be the case if and only if there is no maximal subgroup which contains all the given matrices. To test this, the first step is to decide, for each of the Aschbacher classes, whether the matrices preserve a structure in that class. A classic result of this type is Parker's 'meat-axe' algorithm [28], which decides whether or not such a group is reducible (that is, fixes a subspace, and hence lies in a subgroup in the class $\mathcal{C}_1$). Holt, Leedham-Green, O'Brien and Rees [18], [23] are currently developing similar tests for the other classes. There remains the possibility that the group comes under alternative (b) in Aschbacher's Theorem. Since such groups are 'small', we might hope to handle them directly.

3 $\mathrm{PGL}(n,q)$ from a Kleinian viewpoint

Suppose we take the view that finite projective geometry is the geometry of the group $\mathrm{PGL}(n,q)$. What should we study? It is a truism that geometry is what geometers do; so I shall be descriptive rather than prescriptive, and suggest some properties which have been studied in various cases and may be interesting more generally.

Geometric objects will be elements of sets affording permutation representations of the group. Of course, any permutation representation is the disjoint union of transitive ones, so we should consider these first. The transitive representations (up to permutation isomorphism) correspond to conjugacy classes of subgroups of the group. However, there are still far too many of these, so we must select 'interesting' ones. Natural criteria for these include primitivity, small degree, and small permutation rank (or high degree of transitivity, if possible).

If the action of G on X is imprimitive, let Y be a system of imprimitivity. Then (as geometric objects) a member of X can be regarded as a member of Y (the block containing it) together with some additional structure or information (to specify it in the block). To keep individual objects as simple as possible, we first discard this structure. Now the primitivity of G on Y is equivalent to the maximality of the corresponding subgroup (the stabiliser of a point in Y).

For a simple example, consider the symmetric group S_n, acting on the set of ordered pairs (i,j) with $1 \le i,j \le n$ and $i \ne j$. The stabiliser of (i,j) is contained in the stabiliser of the unordered pair $\{i,j\}$; and (i,j) is obtained just by 'ordering' $\{i,j\}$ in one of the two possible ways.

The other desiderata are more for convenience. We choose actions of small degree (corresponding to large maximal subgroups) in order not to have too many objects to look at; and actions of small rank in order that the number of different relationships in which two objects may stand is not too large. (The minimal G-invariant binary relations are the G-orbits on Ω^2, and their number is the rank of G.)

Of course, these conditions are not identical, but tend to push in the same direction. The transitive representation of smallest degree of a simple group is primitive; small degree and small rank often go together (but not always: the Higman–Sims simple group acts with rank 3 on 100 points, but 2-transitively on 176 points).

Given a collection of interesting transitive representations of G, we look for the binary (or higher-order) relations in each set preserved by G, and whether there are structures with geometric significance. For example, an invariant binary relation may be the collinearity graph of a partial linear space with lines of size greater than 2. If so, then several more questions arise: Is this partial linear space embeddable in a projective space (as a set of points together with all lines contained in this set)? Is it of some familiar type, such as a generalised polygon or a net? We can also ask whether one of the G-invariant graphs is distance-transitive. In more combinatorial terms, properties such as diameter, girth, connectivity, and expansion properties of these graphs can be examined.

Also, we may consider how many objects are required as a 'basis' for the space, so that their pointwise stabiliser in G is trivial. In principle at least, any element of the space is uniquely specified by its G-invariant relations to the basis elements. Of course, the simplest case is a vector space V, where a base for $\mathrm{GL}(V)$ is a basis for V in the usual sense, and any vector is uniquely a linear combination of basis vectors. For another example, consider the projective line over $\mathrm{GF}(q)$. The cross-ratio provides not only a description of the orbits of $\mathrm{PGL}(2,q)$ on 4-tuples, but also an indexing of the points relative to the base $(\infty, 0, 1)$.

We further consider the binary 'incidence' relations between elements of sets affording different representations of G. We can ask whether the resulting incidence structure belongs to one of the many special classes which have been studied (designs of various kinds, partial geometries, and so on).

If we take several permutation representations and study the binary relations, we obtain Buekenhout geometries of various kinds. It would also be possible to consider relations of higher arity, though I don't have any interesting examples.

The 'classical' example of the interplay between several types of maximal subgroups is the construction of the Witt designs and the binary Golay code from $\mathrm{PGL}(3,4)$ (see Lüneburg [26]). The points of the 5-$(24,8,1)$ large Witt design are the points of the projective plane together with three extra points (which are the cosets of $\mathrm{PSL}(3,4)$ in $\mathrm{PGL}(3,4)$). The blocks are the lines, hyperovals, Baer subplanes, and symmetric differences of two lines. Unitals give dodecads in the Golay code and hence carry the 5-$(12, 6, 1)$ small Witt design.

A further problem concerns axiomatisation. Given one or several sets, and some relations or other structures on these sets, how do we recognise that we are looking at a geometry for a specified group?

For $\mathrm{PGL}(n, q)$, we take the interesting permutation representations to be those corresponding to subgroups in the Aschbacher classes. Most of our desirable properties will hold, and the structures should behave relatively uniformly for different n and q.

Needless to say, the same kind of analysis can be applied to all the classical groups (for which Aschbacher's Theorem holds), and also to the exceptional groups of Lie type, for which similar theorems have been proved. What about the symmetric and alternating groups? As noted earlier, the analogue of Aschbacher's theorem for these groups is the O'Nan–Scott theorem, which gives five classes of large maximal subgroups. The geometry of the first two of these (the maximal intransitive or imprimitive groups) is, from a different viewpoint, the combinatorics of subsets and partitions of a finite set, which has an extensive literature. Perhaps the other three classes (product actions of wreath products, diagonal groups, and affine groups) could be given a similar treatment.

The remainder of this paper, apart from the last section, consists of examples of the geometry of some of the Aschbacher classes taken from the literature.

4 Reducible groups

Classical projective geometry is more-or-less the geometry of the maximal reducible subgroups of $\mathrm{PGL}(n, q)$, since these are the stabilisers of subspaces of the projective space (points, lines, planes, ..., hyperplanes).

With finitely many exceptions, the faithful permutation representation of smallest degree is that on the points (or hyperplanes) of the projective space. This result goes back to the roots of the subject: one of Galois' discoveries [13] is that, among the groups $\mathrm{PSL}(2, p)$ for p prime, the smallest-degree representation is the one on the $p + 1$ points except when $p = 2, 3, 5, 7, 11$. (In each of these cases, there is a representation of degree p, though it is not faithful for $p < 5$.) The smallest degrees of permutation representations of all classical groups were determined by Cooperstein [10].

More generally, Kantor [19] showed that a maximal subgroup of $G = \mathrm{PGL}(n, q)$ with order greater than roughly the square root of $|G|$ is necessarily reducible. These results of Cooperstein and Kantor can be seen as precursors of Liebeck's theorem, asserting that subgroups of $\mathrm{PGL}(n, q)$ are either 'known' or small.

The subspace stabilisers play a very important role in the point of view which regards $\mathrm{PSL}(n,q)$ as a group of Lie type: they are the maximal parabolic subgroups. A subgroup is parabolic if it contains the *Borel subgroup* B of G (the normaliser of a Sylow p-subgroup, where p is the characteristic of $\mathrm{GF}(q)$). A Borel subgroup is the stabiliser of a maximal flag (set of mutually incident subspaces), and the parabolic subgroups containing it are precisely the stabilisers of sub-flags. There are two different but related points of view here. Diagram geometry takes the basic objects or 'varieties' to be all the subspaces (corresponding to the maximal parabolic subgroups), with two subspaces incident if one contains the other, that is, if their intersection is parabolic. The theory of buildings takes the basic objects as the chambers or maximal flags (corresponding to the Borel subgroup), and imposes on the set of chambers a number of partitions, one for each subset of the set of types. The finest non-trivial partitions correspond to the minimal parabolic subgroups. See Carter [8], or the chapters by Scharlau and Cohen in the *Handbook of Incidence Geometry* [3].

A general fact about parabolic representations of the groups of Lie type is that the behaviour of the G-invariant binary relations is independent of the field order. If a group G acts transitively on a set Ω, the orbits of G on Ω^2 (the minimal G-invariant binary relations) are in one-to-one correspondence with the double cosets HxH, where H is the stabiliser of a point. If G is a group of Lie type (more generally, a group with a BN-pair), these double cosets correspond to the double cosets in the corresponding parabolic representation of the Weyl group. Moreover, this correspondence preserves the decomposition into orbits of the composition of two such minimal relations. Also, the same holds for relations between two parabolic representations, using double cosets HxK, where H and K are the two parabolic subgroups.

These facts are easily seen directly in the case $G = \mathrm{PGL}(n,q)$, where the Weyl group is the symmetric group S_n. Corresponding to the representation of G on k-spaces is the representation of S_n on k-sets. The minimal binary relations for G have the form $\{(U_1,U_2) : \dim(U_1 \cap U_2) = i\}$, for $0 \le i \le k$; correspondingly, in the symmetric group we have relations $\{(X_1,X_2) : |X_1 \cap X_2| = i\}$. And so on.

Of course, we cannot expect anything so simple to occur in the other Aschbacher classes. If the subgroup H of G has order smaller than the square root of G (as do almost all the irreducible subgroups of $\mathrm{PGL}(n,q)$), then in the representation on the cosets of H, the rank (the number of H-orbits) is at least $|G|/|H|^2$; typically this will be an increasing function of q.

The group $\mathrm{PGL}(n,q)$ is 2-transitive on the set of points. If $n > 2$, its smallest orbit on triples is the ternary relation of *collinearity*; a *line* consists of two points together with all points collinear with them, and a *subspace* is a set of points containing the line through any two of its points. These subspaces are of course just those corresponding to the other subgroups in $\mathcal{C}_1$. If, instead, we take the family of k-subspaces, for $0 < k < n-2$, then the group is not 2-transitive, and it preserves a partial linear space, whose maximal singular subspaces give us the $(k-1)$-subspaces and the $(k+1)$-subspaces. So we can work up and down through the collection of subspaces.

Axiomatisation in the case of points and lines is classical; for other dimensions, see Sprague [31] and Tallini [32]. Also, the geometry of k-spaces can be embedded in $\bigwedge^k V$, the k-spaces $U = \langle v_1, \ldots, v_k \rangle$ being represented by the 1-space $\langle v_1 \wedge \cdots \wedge v_k \rangle$: the lines of the partial linear space are precisely the lines of the embedding projective space which are contained within the set of such points (any other line of the projective space meets the set in at most two points).

Alternatively, if we take two of these permutation representations (corresponding to subspaces of different dimension), then the smallest non-empty G-invariant relation between then is the usual incidence relation.

If $n = 2$, these methods give us no non-trivial geometry, since there is only one class of maximal reducible subgroups, and G is 3-transitive on the points of the projective line. The G-invariant quaternary relations are specified by prescribing values of the cross-ratio of the four points.

As far as I know, the size of a minimal base in each of these permutation representations has not been completely determined. For the action on points, everything is known: the smallest base has size n if $q = 2$, or $n+1$ otherwise. For, if we take n points spanned by the vectors of a basis, their stabiliser consists of diagonal matrices. This is trivial for $q = 2$, since the only non-zero scalar is 1. For larger fields, we must also fix a point in general position.

At the other extreme, if $n = 2m$ is even, then there is a base of size 5 for the action on m-spaces, consisting of the row spaces of the $m \times 2m$ matrices (in block form) $(O\ I)$, $(I\ O)$, $(I\ I)$, $(I\ A)$, and $(I\ B)$, where O and I are the zero and identity matrices, and A and B generate an absolutely irreducible subgroup of $\mathrm{GL}(m, q)$. Now fixing the first and second spaces forces a matrix to be block-diagonal, with $m \times m$ blocks X and Y (say); fixing the third space forces $X = Y$; and fixing the fourth and fifth forces X to commute with A and B, and hence to be a scalar (so trivial in $\mathrm{PGL}(n, q)$).

In fact, we can say more:

Theorem 4.1 *(a) For fixed n and $q \to \infty$, almost all $(n+1)$-tuples of points are bases for* $\mathrm{PGL}(n, q)$.

(b) For fixed m and $q \to \infty$, almost all 5-tuples of m-spaces are bases for $\mathrm{PGL}(2m, q)$.

Problem. Complete these results for subspaces of other dimensions.

5 Direct sums and tensor products

The stabiliser of a direct sum decomposition of the vector space V into subspaces $V_1, \ldots, V_t$ (all of the same dimension) permutes these subspaces among themselves. It is irreducible but, by definition, imprimitive.

There is an interesting connection with permutation groups. One case in the O'Nan–Scott theorem consists of primitive groups G which have an abelian regular normal subgroup V, which is necessarily an elementary abelian p-group for some prime p. We can identify the set of points with V so that V acts on itself by translation. The stabiliser of the zero vector is then a linear group $H = G_0$. Any H-invariant subspace would be a block of imprimitivity for G; so the primitivity of G translates into irreducibility of H. Furthermore, if H is an imprimitive linear group (that is, if it preserves a direct sum decomposition of V), then G is contained in a wreath product with the product action, another case in the O'Nan–Scott theorem. (This means that G preserves a 'product structure' or 'Hamming graph'.) So it is often permissible to deal with this possibility in a different part of the analysis, and to assume that H is primitive.

Let G be the stabiliser of a direct sum decomposition. Then G has a normal subgroup which fixes all the subspaces in the decomposition; the factor group is a subgroup of the symmetric group S_t (permuting the subspaces). Of course, the subspaces $V_1, \ldots, V_t$ are independent (they span their direct sum).

In the case where $\dim(V_i) = 1$, the group G is important from the Lie-theoretic viewpoint: it is the normaliser of a maximal split torus T (induced by the group of diagonal matrices), and the quotient is the *Weyl group* of $\mathrm{PGL}(n, q)$, which is the symmetric group S_n in this case; see Carter [8].

In general, in the projective space $\mathrm{PG}(mt - 1, q)$ (where $\dim(V_i) = m$), G fixes a set S of points which is the union of t independent subspaces $\mathrm{PG}(m - 1, q)$. Some information about the relations between these objects, of the type described by Eisfeld for subfield geometries (see Section 7), could probably be established.

The problem of recognising when a matrix group is *imprimitive* (that is, preserves a direct sum decomposition of this type) has been solved by Holt *et al.* [18].

Questions about the rank, suborbits, or minimum base size for the permutation representations of this kind seem to be open.

Tensor products are inherently more complicated than direct sums. The direct sum $U \oplus W$ has subspaces naturally isomorphic to U and W, and can be recognised by the familiar internal characterisation of direct sums. In terms of the projective space this reads: any point outside the union of the two subspaces lies on a unique line meeting both of them. However, $V = U \otimes W$ does not contain copies of U and W invariant under the corresponding group.

One approach to the geometry, which has been exploited by Leedham-Green and O'Brien [22], [23] for matrix group algorithms, works as follows. Let $k = \dim(U)$, $l = \dim(W)$ (so that $\dim(V) = kl$). Now consider the subspaces $U \otimes X$, as X ranges over all subspaces of W. As partially ordered set, this family of subspaces is isomorphic to the subspace lattice of the projective geometry $\mathrm{PG}(l-1, q)$ corresponding to W. Its atoms are $(k-1)$-subspaces of $\mathrm{PG}(kl-1, q)$. Leedham-Green and O'Brien show how, given generators of a group preserving such a tensor product, this lattice can be efficiently computed.

The smallest example of this case is given by the ruled (hyperbolic) quadric in $\mathrm{PG}(3, q)$. The 4-dimensional vector space is expressed as $U \otimes W$, where $\dim(U) = \dim(W) = 2$; the points on the quadric are those spanned by the rank 1 tensors $u \otimes w$, for $u \in U$ and $w \in W$.

The other tensor case, that where $V = \bigotimes_{i=1}^{t} V_i$, is even more recondite. The group G fixing such a decomposition has a normal subgroup N preserving the tensor factors, the quotient group being S_t. Geometrically, N preserves t sublattices of the projective space, each isomorphic to the projective space based on V_i.

6 Classical groups

These are the subgroups of G which preserve non-degenerate alternating or Hermitian forms or non-singular quadratic forms (the *symplectic, unitary* and *orthogonal* groups). Because we are considering only maximal subgroups, some cases do not need to be considered. In characteristic 2, an orthogonal group of odd degree fixes a point, namely the radical of the form, while an orthogonal group of even degree fixes the symplectic form obtained by polarisation and so is contained in the symplectic group.

This example illustrates the earlier remark about imprimitive permutation representations:

- if n is odd, an orthogonal geometry is specified by giving a point (the radical) together with a symplectic geometry on the quotient space;
- if n is even, an orthogonal geometry is specified by saying which of the totally isotropic subspaces for the symplectic geometry are totally singular.

The geometry of the classical groups is well-known, see for example the

Handbook of Incidence Geometry [3]. The usual description takes the varieties of the incidence geometry to be the subspaces which are totally isotropic or totally singular with respect to the form. There are familiar axiomatisations of these *polar spaces* (Tits, Buekenhout and Shult). No more need be said here.

The membership test for classical groups is reasonably straightforward. Suppose that the group G generated by a set of $n \times n$ matrices over $\mathrm{GF}(q)$ is irreducible. Then G is contained in the general symplectic group if and only if it fixes a 1-dimensional subspace in the space of alternating bilinear forms. (If there is a fixed 1-space of forms, the common radical of its members is fixed by G, and so is zero, since G is irreducible.) This space is the dual of $V \wedge V$, where $V = \mathrm{GF}(q)^n$, so the appropriate representation may be constructed and decomposed with standard computational tools. To test membership in orthogonal or unitary groups, we test similarly the spaces of symmetric bilinear or Hermitian forms.

The type of question which arises from our point of view is the following. Given two symplectic forms (say) on a vector space, what is the relationship between them? For example, what are the possible structures of the geometry of subspaces which are totally singular for both forms? The question on base size reads: What is the smallest set of symplectic forms with the property that the only linear maps preserving all of them (up to scalar factors) are scalar transformations?

The last question was investigated by Tracey Maund [27] in her (unpublished) thesis. She considered one particular relationship between two forms. Let $n = 2m$, and take a 2-dimensional vector space over $\mathrm{GF}(q^m)$. On restriction of scalars, this becomes an n-dimensional vector space over $\mathrm{GF}(q)$. Now all symplectic forms on $V(2, q^m)$ are equivalent under scalar multiplication. Take two such forms b and λb, where λ generates $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$. Let Tr denote the trace map from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$. Then $B_1 = \mathrm{Tr}(b)$ and $B_2 = \mathrm{Tr}(\lambda b)$ are symplectic forms on $V(2m, q)$. The subgroup of $\mathrm{GL}(2m, q)$ fixing both these forms up to scalar factors is $\Gamma\mathrm{L}(2, q^m)$ (the extension of $\mathrm{GL}(2, q^m)$ by the group of automorphisms of $\mathrm{GF}(q^m)$ over $\mathrm{GF}(q)$). The maximal subspaces which are totally isotropic for both B_1 and B_2 form a Desarguesian spread in $V(2m, q)$. If n is large enough, it is possible to find a third symplectic form such that only scalars fix the three forms, so that there is a base of size 3 for this representation of $\mathrm{PGL}(n, q)$.

Problem. Do almost all triples constitute bases (say, as $q \to \infty$ and fixed n)?

The geometry of symplectic forms can be embedded in a projective space over $\mathrm{GF}(q)$, as follows. An alternating bilinear form on $V = \mathrm{GF}(q)^{2m}$ can be regarded as a linear map from $V \wedge V$ to $\mathrm{GF}(q)$. We dualise, and consider the vector space $V \wedge V$. Now the duals of non-degenerate forms are the elements of rank m, where the rank of an element of $V \wedge V$ is the smallest number of vectors of the form $v_1 \wedge v_2$ of which it is the sum. Since we are allowed to multiply forms by scalar factors, the geometry associated with this representation consists of all points of the projective space spanned by vectors of rank m in $V \wedge V$. This vector space also represents the 2-spaces of V, as the points spanned by vectors of rank 1.

One well-known instance is the case $m = 2$, where these two sets between them make up the whole projective space $\mathrm{PG}(5, q)$. The points corresponding to rank 1 vectors comprise the Klein quadric, and those corresponding to symplectic forms to the points outside the quadric.

Another case which has been studied is the case $q = 2$, in connection with coding theory. Here, sets of alternating forms of maximum cardinality subject to the condition that the difference between any two is non-degenerate give rise to *Kerdock codes*. Moreover, the quadratic forms on $V(2m, 2)$ form a vector space which has the space of alternating bilinear forms as a homomorphic image. Much of the geometry and combinatorics of quadratic forms can be seen in this space; see Cameron and Seidel [7].

(The maximum cardinality of such a set on a $2m$-dimensional vector space is 2^{2m-1}. The Kerdock code consists of all the quadratic forms which polarise to bilinear forms in X. It is necessarily non-linear: indeed, a subspace of alternating forms all of whose non-zero members are non-degenerate has dimension at most m, as can easily be seen by applying the Chevalley–Warning theorem to the Pfaffian function on the space of skew-symmetric matrices representing the forms.)

Similar questions can be posed for the other types of classical groups, but have not received much attention yet from geometers. Gow [15] considered the permutation representation on non-degenerate Hermitian forms from a character-theoretic point of view, and showed that it is multiplicity-free.

7 Subfields and superfields

If $q = r^t$, the subgroup $\mathrm{PGL}(n, r)$ of $\mathrm{PGL}(n, q)$ acts on a projective geometry $\mathrm{PG}(n-1, r)$ 'embedded' in $\mathrm{PG}(n-1, q)$. Its subspaces are those spanned by vectors whose coordinates lie in the subfield $\mathrm{GF}(r)$ of $\mathrm{GF}(q)$. In the case $q = r^2$, this is a *Baer subgeometry.* In general, a line of the large geometry belongs to the subgeometry if two of its points do; so any line meets the subgeometry in $0, 1$ or $r + 1$ points. The Baer case in the plane is characterised by the fact that the case 0 does not occur; that is, every line meets the subgeometry (which thus forms a minimal line-blocking set).

How are two such subgeometries related? Some relations have been studied. For example, if n and t are coprime (in particular, if n is odd and

$q = r^2$), a Singer cycle C for $\mathrm{PG}(n-1,q)$(a cyclic subgroup of $\mathrm{PGL}(n,q)$ acting transitively on the points) contains a subgroup which is a Singer cycle for $\mathrm{PG}(n-1,r)$; the images of this subgeometry partition the points of $\mathrm{PG}(n-1,q)$.

Ueberberg [33], [34] showed that, if two Baer subplanes Π_1 ands Π_2 of $\mathrm{PG}(2,r^2)$ are disjoint, then there is a unique Singer cycle for which the corresponding partition contains Π_1 and Π_2. So the geometry of Baer subplanes has the structure of a partial linear space with $r^2 - r + 1$ points per line. For $r = 2$, Ueberberg showed that conjugates of the Frobenius automorphism can be used to describe 'planes' in this geometry, each plane being a 3×3 grid. This rank 3 Buekenhout geometry, with diagram $C_2.c$, is a subgeometry of Ronan's geometry with the more general diagram $C_2.L$, consisting of the octads, trios and sextets related to the Golay code [29], [5]. Hence, Ueberberg's partial linear space is embeddable in the projective space $\mathrm{PG}(10,2)$, corresponding to the (extended) Golay code modulo the all-1 vector.

Note that a Singer cycle belongs to the Aschbacher class $\mathcal{C}_3$ (superfield stabiliser). This is an example of a relationship between subfield and superfield geometries.

The relationships between these subfield geometries have been considered more generally by Jörg Eisfeld [12]. Let $q = r^t$, and let P be a $\mathrm{PG}(n-1,r)$ subgeometry of $\mathrm{PG}(n-1,q)$. For any point p, we define its 'distance' $d(p,P)$ from P to be the (geometric) dimension of the smallest subspace of P (that is, spanned by points of P) containing p. Then $0 \le d(p,P) \le t-1$; and if $d(p,P) = t-1$, the subspace in question is unique. Eisfeld constructed a 'large' set $\mathcal{M}$ of $\mathrm{PG}(n-1,q)$ subgeometries of $\mathrm{PG}(n-1,q)$ with the property that, for $P, P' \in \mathcal{M}$, the distance $d(p,P)$ is the same for all $p \in P'$. In particular, if t and n are coprime, the subgeometries of $\mathcal{M}$ partition the points of $\mathrm{PG}(n-1,q)$, and we obtain the Singer cycle partitions as before. At the other extreme, if $t = n$, there is a subset of $q-1$ subgeometries which are pairwise at maximum distance $t-1$.

Also, in the Baer case ($t = 2$), Gow [15] showed that the permutation character is multiplicity-free.

If $n = kl$, then $\mathrm{GF}(q^l)^k$ is identified with $\mathrm{GF}(q)^n$ by restricting scalars, and so $\mathrm{GL}(k,q^l)$ is a subgroup of $\mathrm{GL}(n,q)$. Moreover, the Galois automorphisms of $\mathrm{GF}(q^l)$ over $\mathrm{GF}(q)$ are also $\mathrm{GF}(q)$-linear and normalise $\mathrm{GL}(k,q^l)$. The points, lines, ... of $\mathrm{PG}(k-1,q^l)$ become l-spaces, $2l$-spaces, ... of the geometry over $\mathrm{GF}(q)$. In particular, the points give rise to a Desarguesian spread of l-spaces in $\mathrm{GF}(q)^n$.

8 Symplectic-type r-groups

I have little to say about this class of subgroups. But I would like to draw attention to a different but related context in which they arose recently, a surprising development in coding theory.

The Lee metric on $\mathbb{Z}_4$, defined by

$$d(x, y) = \min\{x - y, y - x\}$$

(where the arithmetic is mod 4) is isometric to the Hamming metric on $\mathbb{Z}_2^2$. Hence there is an isometry, the *Gray map*, from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$. Hammons *et al.* [17] showed that some famous non-linear binary codes are the images of $\mathbb{Z}_4$-linear codes under the (non-linear) Gray map. These include the Kerdock codes discussed briefly in the last section, and also a modified version of the Preparata codes. Subsequently, Calderbank *et al.* [4] showed that the Gray map is closely connected with the real and complex geometry associated with extraspecial 2-groups. It may be that there are interesting finite analogues of this real and complex geometry.

9 Appendix: Very small base groups

Recall that, if G is a permutation group acting on a set Ω, a *base* for G is a sequence of points whose pointwise stabiliser is the identity. Apart from their role in geometry, bases are very important in computational permutation group theory, and the question of the minimal base size for a group has been considered by many authors. Often, efficient algorithms must treat groups differently according as they have 'large' or 'small' bases.

If G has a base of size c, then its images under distinct group elements are distinct, and so $|G| \leq n^c$, where n is the degree of G. There is a feeling that primitive groups of polynomially bounded order should have bases of bounded size. This has been proved only in special cases, most of which exclude groups like $\mathrm{PGL}(n, q)$. The only general result I know, dealing with very small groups, is the following unpublished result of Cameron and Kantor.

Let $l(n)$ be a monotonic increasing function on the natural numbers satisfying $l(n!) = n$ for all n.

Theorem 9.1 *Let G be a primitive group of degree n, and suppose that the order of the point stabiliser in G is smaller than $\sqrt{l(n)}$. Then G has a base of size 2.*

The proof depends on the following result of some independent interest.

Theorem 9.2 *Let G be a primitive group of degree n. Then any element $g \in G$ which is not semiregular lies in a conjugacy class of size at least $l(n)$.*

Remark. The hypothesis excluding semiregular elements is necessary. For example, in the dihedral group of order $2p$ (where p is prime), elements of order p lie in conjugacy classes of size 2. Also, the result is not far from best possible, as can be seen by taking G to be the symmetric group S_m acting on the cosets of a very small maximal subgroup (so that n is nearly $m!$), and g to be a transposition in S_m (lying in a class of size $m(m-1)/2$).

Proof Let $|g^G| = m < l(n)$. Then $\bigcap_{h\in g^G} C_G(h) = N$ is a normal subgroup of G of index at most $m!$, hence less than n. So $N \neq 1$, and N is transitive. But N centralises g, so g is semiregular. □

Proof of Theorem 9.1. Choose $\alpha \in \Omega$, and let $H = G_\alpha$. Count pairs (β, g) with $g \in G$, $g \neq 1$, $\beta g = \beta$. We have

$$\begin{aligned} n(|H|-1) &= \sum_{g\in(H^\sharp)^G} \mathrm{fix}(g) \\ &= \sum_i \mathrm{fix}(g_i)|g_i^G| \\ &= \sum_{h\in H^\sharp} \mathrm{fix}(h)|h^G|/|h^G \cap H| \\ &\geq \left(\sum_{h\in H^\sharp} \mathrm{fix}(h)\right)\left(\min_{h\in H^\sharp} |h^G|/(|H|-1)\right). \end{aligned}$$

(Here $H^\sharp = H \setminus \{1\}$, and the sum in the second line is over a set of conjugacy class representatives of elements with fixed points.) So the number of choices of β for which (α, β) is *not* a base is at most

$$\sum_{h\in H^\sharp} \mathrm{fix}(h) \leq n(|H|-1)^2/l(n) < n.$$

□

The proof in fact shows that, in a family of primitive groups with $|G_\alpha| = o(\sqrt{l(n)})$, asymptotically almost all pairs of points are bases.

In the case where $G = \mathrm{PGL}(n,q)$, rather than apply Theorem 9.1 directly, we use the fact that the smallest non-trivial conjugacy class has size roughly q^{2n}, together with the results of Hall, Liebeck and Seitz [16] on generation, and Landazuri and Seitz [21] on minimal degree. The conclusion is that, if $|H|$ is smaller than roughly q^n, there is a base of size 2. This deals with some of the smaller Aschbacher classes, depending on the relative sizes of n and q. Unfortunately, it doesn't deal with Aschbacher's case (b), since the bound is smaller than Liebeck's q^{3n}. It would be interesting to improve the technique to remove this defect.

References

[1] E. Artin, *Geometric Algebra*, Interscience, New York, 1957.

[2] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[3] F. Buekenhout (ed.), *Handbook of Incidence Geometry*, Elsevier, 1995.

[4] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets, in preparation.

[5] P. J. Cameron, *Projective and Polar Spaces*, *QMW Maths Notes* **13**, Queen Mary and Westfield College, London, 1991.

[6] P. J. Cameron, Permutation groups, in *Handbook of Combinatorics* (ed. R. L. Graham, M. Grötschel and L. Lovász), Elsevier, 1995, pp. 611–645.

[7] P. J. Cameron and J. J. Seidel, Quadratic forms over GF(2), *Proc. Kon. Nederl. Akad. Wetensch.* (A) **76** (1973), 1–8.

[8] R. W. Carter, *Simple Groups of Lie Type*, Wiley, New York, 1972.

[9] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An* $\mathbb{ATLAS}$ *of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[10] B. N. Cooperstein, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.

[11] J. Dieudonné, *La Géometrie des Groupes Classiques*, Springer, Berlin, 1963.

[12] J. Eisfeld, Some big sets of mutually disjoint subgeometries of $\mathrm{PG}(d, q^t)$, preprint.

[13] É. Galois, Oeuvres mathématique: lettre à M. Auguste Chevalier, *J. Math. Pures Appl. (Liouville)* (1846), 400–415.

[14] D. Gorenstein, *Finite Simple Groups: An Introduction to their Classification*, Plenum Press, New York, 1982.

[15] R. Gow, Two multiplicity-free permutation representations of the general linear group $\mathrm{GL}(n, q^2)$, *Math. Z.* **188** (1984), 45–54.

[16] J. I. Hall, M. W. Liebeck and G. M. Seitz, Generators for finite simple groups, with applications to linear groups, *Quart. J. Math. Oxford* (2) **43** (1992), 441–458.

[17] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory,* to appear.

[18] D. F. Holt, C. R. Leedham-Green, E. A. O'Brien and S. E. Rees, Primitivity testing for matrix groups, *J. Algebra*, to appear.

[19] W. M. Kantor, Permutation representations of the finite classical groups of small degree or rank, *J. Algebra* **60** (1979), 158–168.

[20] P. B. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups, London Math. Soc. Lecture Notes* **129**, Cambridge Univ. Press, Cambridge, 1990.

[21] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418–443.

[22] C. R. Leedham-Green and E. A. O'Brien, Tensor products are projective geometries, *J. Algebra*, to appear.

[23] C. R. Leedham-Green and E. A. O'Brien, Recognising tensor products of matrix groups, preprint.

[24] M. W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* (3) **50** (1985), 426–446.

[25] M. W. Liebeck, C. E. Praeger and J. Saxl, On the O'Nan–Scott reduction theorem for finite primitive permutation groups, *J. Austral. Math. Soc.* **44** (1988), 389–396.

[26] H. Lüneburg, *Transitive Erweiterungen endlicher Permutationsgruppen, Lecture Notes in Math.* **84**, Springer, Berlin, 1969.

[27] T. Maund, D. Phil. thesis, Oxford, 1987.

[28] R. A. Parker and R. A. Wilson, The computer construction of matrix representations of finite groups over finite fields, *J. Symbolic Computation* **9** (1990), 583–590.

[29] M. A. Ronan, Locally truncated buildings and M_{24}, *Math. Z.* **180** (1982), 489–501.

[30] L. L. Scott, Representations in characteristic p, *Proc. Symp. Pure Math.* **37** (1980), 319–331.

[31] A. P. Sprague, Pasch's axiom and projective spaces, *Discrete Math.* **33** (1981), 79–87.

[32] G. Tallini, On a characterization of the Grassman manifold representing the lines in a projective space, pp. 354–358 in *Finite Geometries and Designs* (ed. P. J. Cameron, J. W. P. Hirschfeld and D. R. Hughes), *London Math. Soc. Lecture Notes* **49**, Cambridge University Press, Cambridge, 1981.

[33] J. Ueberberg, Projective spaces and dihedral groups, to appear.

[34] J. Ueberberg, A class of partial linear spaces related to $\mathrm{PGL}(3, q^2)$, *Europ. J. Combinatorics*, to appear.

[35] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.

Peter J. Cameron, School of Mathematical Sciences, Queen Mary and Westfield College, Mile End Road, London E1 4NS, U.K.
e-mail p.j.cameron@qmw.ac.uk