Highly transitive imprimitivities

Marston Conder *
Department of Mathematics, University of Auckland,
Private Bag 92019, Auckland, New Zealand
m.conder@auckland.ac.nz

Vaughan Jones †
Mathematics Department, University of California Berkeley,
Berkeley, CA 94720, U.S.A.
vfr@math.berkeley.edu

November 8, 2005

Abstract

Some new observations are made about imprimitive permutation groups associated with subfactors of von Neuman algebras. Of particular interest are examples of a group G containing two maximal subgroups H and K such that $G \neq HK$, and such that the action of G on the space of cosets of $H \cap K$ has small rank (few suborbits). The rank 6 case turns out to correspond to the action of the collineation group on flags of a Desarguesian projective plane, and a special case of interest for rank 7 corresponds to the action of a 4-transitive group on ordered pairs of distinct points. Some other new (and unexpected) fundamental properties of groups are described along the way.

1 Introduction

Organising groups by the transitivity of their actions is as old as group theory itself. The idea that highly transitive group actions are scarce is basic to the discovery and classification of finite simple groups.

Subfactors began as an infinite dimensional non-commutative extension of Galois theory. A subgroup H of a finite group G gives rise to a subfactor by choosing an (outer)

*Research supported in part by the N.Z. Centres of Research Excellence Fund (grant UOA 201)
†Research supported in part by NSF Grant DMS93–22675, the N.Z. Centres of Research Excellence Fund (grant UOA 201), and the Swiss National Science Foundation

aciton of G on a II_1 factor R and letting $N \subseteq M$ be the pair of fixed point algebras $R^G \subseteq R^H$. These are the simplest and best understood subfactors.

To a subfactor of finite index is associated a 'standard invariant' or planar algebra, which is primarily a sequence P_n (for $n \geq 0$) of finite-dimensional vector spaces (obtained by decomposing tensor powers $\otimes_N^n M$ as a bimodule). The planar algebra for $R^G \subseteq R^H$ is well understood. The vector space P_n is naturally the space of functions on X^n (where X is the coset space $(G : H)$, which we will denote by G/H), invariant under the action of G. Thus $\dim P_n$ is the number of orbits of G on X^n.

Before proceeding further, we should point out that (a) for the simplest II_1 factor R, an outer action of a finite group is *unique* up to conjugacy [13], and that (b) Izumi has shown in [11] that if the action of G on X is *primitive*, that is, if H is maximal in G, then one can reconstruct both G and H from the subfactor $R^G \subseteq R^H$.

Clearly the number of orbits for the action of the symmetric group S_X on X^n is a lower bound for $\dim P_n$, and to say an action is k-transitive is just to say that $\dim P_k$ is equal to that lower bound. For $|X| > n$ this number of orbits is equal to the number of partitions of a set of size n, called the nth *Bell number*, also equal to the coefficient of $x^n/n!$ in the exponential generating function $E(E(x)) + 1$, where $E(x) = e^x - 1$ (see [1] or [8]).

For a subfactor not necessarily of the form $R^G \subseteq R^H$, planar partitions still make sense, and the universal lower bound on $\dim P_n$ is the Catalan number $\frac{1}{n+1}\binom{2n}{n}$, for all but small values of n. Accordingly, subfactors can be "more transitive" than group actions. This observation led the second author to the notion of *supertransitivity*, and the beginnings of the study of subfactors from this point of view in [14] and [15].

The planar algebra encodes all the algebraically accessible data for a subfactor $N \subseteq M$. The most obvious piece of extra structure that can arise for a subfactor is the existence of an intermediate subfactor $N \subset T \subset M$. In [3] it is shown that in the presence of such a T, planar partitions can be enriched, and the necessary loss of supertransitivity is reflected in a lower bound of $\frac{1}{2n+1}\binom{3n}{n}$ for $\dim P_n$, for all but small n. An intermediate subfactor for $R^G \subset R^H$ is necessarily of the form R^K for some subgroup K with $H < K < G$. This leads to the following (somewhat vague) group-theoretic question:

Question 1.1 *What are the most transitive* imprimitive *actions of finite groups?*

In a sense, the most highly transitive imprimitive permutation groups of given composite degree d are the wreath products $S_a \operatorname{wr} S_b$ where $ab = d$, with $1 < b \leq a < d$. Each such group G is a semi-direct product of the direct product of b copies of the symmetric group S_a (acting independently on b copies of a set of size a, called the *blocks*) by a single copy of the symmetric group S_b which permutes the b blocks. We may take the stabilizer of a point as the subgroup H, and the setwise stabilizer of the block containing that point as the intermediate subgroup K.

These are rank 3 permutation groups (see [6] or [7] for example), having three orbits on $X \times X$: one the diagonal, one containing ordered pairs of distinct points from the same block, and the other containing ordered pairs of points from different blocks. Moreover,

every imprimitive permutation group of degree $d = ab$ having b blocks of imprimitivity (each of size a), is a subgroup of $S_a \operatorname{wr} S_b$, and so these examples give the highest amount of transitivity.

A generic lower bound on the number of orbits on X^n is the coefficient of $x^n/n!$ in the exponential generating function $E(E(E(x))) + 1$, with $E(x) = e^x - 1$ as before.

The next natural step in considering subfactor structure from this point of view is to investigate more complicated intermediate subfactor lattices, following earlier work by Watatani [18] and Watatani and Sano [17].

The simplest situation beyond a chain of intermediate subfactors is that of a 'quadrilateral' $(M; S, T; N)$ where S, T and N are subfactors of M such that $N \subset S \cap T$. In this case we might as well always suppose that $S \cap T = N$ and that S and T generate M, for otherwise transitivity is decreased. Further, we may suppose that $ST = M$ and that S and T 'commute', in the sense that the orthogonal projections e_S and e_T (onto S and T) commute. Planar partitions can now be further enriched to give a generic lower bound of $\left[\frac{1}{n+1}\binom{2n}{n}\right]^2$ for $\dim P_n$.

In the group-theoretic context, this case involves intermediate subgroups K_1 and K_2 of G such that $K_1 \cap K_2 = H$ is core-free in G and also

$$K_1 K_2 = G, \tag{1}$$

which leads naturally to the following:

Question 1.2 *What are the most transitive imprimitive group actions with two intermediate subgroups as in condition (1)?*

It is not difficult to see that in this case the group G must have at least four orbits on $X \times X$: one the diagonal, one containing ordered pairs of distinct points from the same orbit of K_1 but different orbits of K_2, another like this but with the roles of K_1 and K_2 reversed, and another containing ordered pairs of points from different orbits of both K_1 and K_2. Hence the rank of G on the coset space $X = G/H$ is at least 4.

One family of examples is as follows: For any integer $k > 1$, let G be the direct product $S_k \times C_2$, of order $2k!$, and in this group take K_1 and K_2 as the natural subgroups $S_{k-1} \times C_2$ (of index k in G) and S_k (of index 2 in G), so that $H = K_1 \cap K_2 = S_{k-1}$. The rank of the action of G on the coset space $X = G/H$ is 4, with orbits on $X \times X$ of lengths $2k, 2k, 2k(k-1)$ and $2k(k-1)$.

Similarly, the factor C_2 can be replaced by S_l for any $l > 1$, and the rank of the resulting action is still 4. In fact it may not be difficult to prove that these are essentially the only examples of rank 4 (or at least the largest possible examples for given indices $|G : K_i|$ and $|K_i : H|$), but in any case, because they are direct products, the resulting subfactors are simply tensor products of the subfactors corresponding to the coset spaces G/K_1 and G/K_2, and are therefore not particularly interesting.

The next case in the subfactor situation is to disallow the possibility that $ST = M$, thereby *decreasing* transitivity.

One important point we have not mentioned so far is that for the action of G on G/H to be as transitive as possible, we want the 'elementary' actions of G on G/K_1 and G/K_2 and the actions of K_1 and K_2 on K_1/H and K_2/H to be highly transitive. For subfactors generally, we make the assumption (called "no extra structure") that the lower bounds for supertransitivity of the elementary inclusions are attained. Thinking about this concept led to the surprising result in [10] that there are in fact only two possibilities for $N \subset M$ if there is no extra structure: one where N is the fixed point algebra under an outer action of S_3, and the other where the index $[M : N]$ is $6 + 4\sqrt{2}$. For groups we are led to this:

Question 1.3 *Among the imprimitive group actions with two intermediate subgroups K_1 and K_2 such that $K_1 \cap K_2 = H$ is core-free in G, and*

$$K_1K_2 \neq K_2K_1, \tag{2}$$

which are the most transitive?

Here we have some very interesting answers. First, as will be shown later, we can use an elementary but not well known observation (with an elegant proof due to David Goldschmidt) that gives $G \neq K_1K_2 \cup K_2K_1$ in this case, and it then follows that there must be at least 6 orbits of G on $X \times X$. Moreover, for the case where this bound is attained, we find the following:

Theorem 1.4 *Let K_1 and K_2 be maximal subgroups of the finite group G such that $K_1K_2 \neq K_2K_1$, and the action of G on the coset space $X = G/H$ (where $H = K_1 \cap K_2$) is faithful and has rank 6. Then up to isomorphism either*

(a) *$G = S_3$, $|K_1| = |K_2| = 2$ and $|H| = 1$, or*

(b) *$|G : K_1| = |G : K_2| = q^2+q+1$ and $|K_1 : H| = |K_2 : H| = q+1$ for some prime-power q, and there is a 1-to-1 correspondence between points of X and the flags (incident point-line pairs) of a Desarguesian projective plane Π of order q, under which cosets of K_1 correspond to points of Π and cosets of K_2 correspond to lines of Π, respectively, and G corresponds to a flag-transitive collineation group of Π.*

In a sense, this theorem provides an analogy to doubly-transitive permutation groups. For transitive groups of degree > 1, the minimum rank is 2, attained only when the group is 2-transitive. For groups satisfying the condition given by (2), the minimum rank is 6, attained only by flag-transitive collineation groups of Desarguesian finite projective planes. The corresponding analogue for primitive group actions of rank 3 would be a full classification of examples satisfying (2) with 7 orbits on $X \times X$ (where $X = G/H$). We do not have that, but we do have a complete list in a non-trivial special case:

Theorem 1.5 *Let K_1 and K_2 be maximal subgroups of the finite group G such that $K_1K_2 \neq K_2K_1$, and $|G : K_1| \geq |G : K_2|$, and such that the action of G on the coset space $X = G/H$ (where $H = K_1 \cap K_2$) is faithful and has rank 7, with two orbits on $X \times X$ of length $|X|$. Then*

(a) *$|X| = |G : H| = s(s+1)$ for some integer s, and*

(b) *$|G : K_2| = s+1$, and $|G : K_1| = s+1$ or $s(s+1)/2$, and*

(c) *the action of G on G/K_2 is 4-transitive, and the action of G on X is equivalent to its action on ordered pairs of distinct points of G/K_2, while the action of G on G/K_1 is either equivalent to that on G/K_2 or equivalent to the action of G on unordered pairs of distinct points of G/K_2, and*

(d) *G is isomorphic to the alternating group A_{s+1} or the symmetric group S_{s+1}, or to one of the Mathieu groups M_{11}, M_{12}, M_{23} or M_{24}.*

Conversely, if G is one of the Mathieu groups M_{11}, M_{12}, M_{23} or M_{24}, or the alternating group A_k (for $k \geq 5$) or the symmetric group S_k (for $k \geq 4$), then the action of G on ordered pairs of distinct points (in its natural action) gives rise to subgroups K_1 and K_2 satisfying the above conditions.

We arrived at these theorems following observations made about examples investigated with the help of the MAGMA system [5].

2 Preliminaries

Before proving Theorems 1.4 and 1.5, we prove two preliminary facts that are fundamental to the study of imprimitive group actions of the types discussed in the Introduction, and introduce some additional notation.

Proposition 2.1 *If K and L are maximal subgroups of the finite group G for which $KL \neq G$, and the actions of G on the coset spaces G/K and G/L are both 2-transitive, then $|G : K| = |G : L|$.*

Note that $H = K \cap L$ does not appear in the statement of this result, and so there is no need for $K \cap L$ to have any particular properties.

The proposition can be proved in several ways. One way is to use Schur's lemma from group representation theory (see [9] or [12] for example).

Let V be the vector space of functions from G to a field $\mathbb{C}$ of zero characteristic. Let ρ denote right translation on V, and define $p = \sum_{x \in K} \rho(x)$ and $q = \sum_{y \in L} \rho(y)$. Then qp takes right K-invariant functions to right L-invariant functions, and commutes with the left action of G. But since $KL \neq LK$, the composite qp is non-zero on the orthogonal

complement of constant functions, and so by 2-transitivity and Schur's lemma, qp is an isomorphism. Hence the dimensions of the spaces of functions from G/K and G/L to $\mathbb{C}$ are the same.

Another proof (pointed out to us independently by Peter Cameron and Geoff Robinson) goes as follows: Let $\{\chi_i : 1 \leq i \leq m\}$ be the irreducible characters of G over $\mathbb{C}$, with χ_1 trivial, and let χ_K and χ_L be the permutation characters for the actions of G on the coset spaces G/K and G/L. Then by 2-transitivity, $\chi_K = \chi_1 + \chi_i$ and $\chi_L = \chi_1 + \chi_j$ for some $i, j > 1$, with inner product $(\chi_K, \chi_L) = 1 + (\chi_i, \chi_j) = 1$ unless $i = j$. On the other hand,

$$(\chi_K, \chi_L) = \frac{1}{|G|} \sum_{g \in G} \chi_K(g)\overline{\chi_L(g)} = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}_{G/K}(g)\mathrm{Fix}_{G/L}(g) = \frac{1}{|G|} \sum_{g \in G} \mathrm{Fix}_{G/K \times G/L}(g),$$

which by Burnside's lemma is the number of orbits of G on $G/K \times G/L$. As $G \neq KL$, this number of orbits is at least two, so $(\chi_K, \chi_L) > 1$, and hence $i = j$, so $\chi_K = \chi_L$ and therefore $|G : K| = |G : L|$ (and in fact K and L are conjugate subgroups in G).

Finally, we have a third proof, offered to us by Primož Potočnik, using the theory of block designs (see [2]): The coset spaces G/K and G/L can be taken as the point-set and block-set of a block design, with incidence given by non-empty intersection

$$Kx \sim Ly \quad \text{if and only if} \quad Kx \cap Ly \neq \emptyset.$$

By 2-transitivity of G on G/K, any two points lie in the same number of blocks, so this is a 2-design, and since $G \neq KL$, the design is incomplete. Now by Fisher's inequality (provable by considering the ranks of the incidence matrix M and the product MM^T) there are at least as many blocks as points, so $|G : K| \leq |G : L|$. But the same argument applies to the dual design, and so $|G : L| \leq |G : K|$; hence equality.

Proposition 2.2 *If K and L are subgroups of the finite group G such that $KL \cup LK$ is a subgroup of G, then also KL is a subgroup of G.*

Proof (a simplification of an unpublished one by David Goldschmidt). Let $M = LK \cup KL$, and define $J = \{g \in M : KLg = KL\}$. Then J is a subgroup of M, with $L \subseteq J \subseteq KL$, and $M = KJ \cup JK$, and $KJ = KLJ = KL$. Now assume $JK \neq M$, and let g be any element of $M \setminus JK$. Then $Lg \cap JK = \emptyset$ (for otherwise g would be an element of $LJK = JK$), but $M = KJ \cup JK$, and so $Lg \subseteq KJ$. It follows that $KLg \subseteq KJ = KL$, so by definition of J (and finiteness of G), we find $g \in J$ and hence $g \in JK$, contrary to the hypothesis on g. Thus $JK = M$, so JK is a subgroup of G, giving $KL = KJ = JK$, which in turn implies that KL is a subgroup of G (and $KL = LK$). □

Now suppose that G is a transitive but imprimitive permutation group on a set X of size d, and that $H = G_x$, the stabilizer in G of some point $x \in X$. Also suppose that the stabilizer H is contained in two different maximal subgroups K and L of G, such that $KL \neq LK$ (or equivalently, such that KL is not a subgroup of G), and that $K \cap L = H$.

Observe that the condition $KL \neq LK$ implies that $G \neq KL$, and the fact that H is the stabilizer of a point in X implies that H is core-free in G.

Let $k = |G : K|$ and $l = |G : L|$, the numbers of (right) cosets of K and L respectively in G, and similarly, let $r = |K : H|$ and $s = |L : H|$. Then G has a system of imprimitivity with k blocks $B_1, B_2, \ldots, B_k$, each of size r, such that B_1 is the orbit of x under the subgroup K (and the remaining $k-1$ blocks B_i are the images of B_1 under elements of G), and another system with l blocks $C_1, C_2, \ldots, C_l$, each of size s, such that C_1 is the orbit of x under the subgroup LK (and so on).

Lemma 2.3 *Under the above conditions, the following hold:*

(a) $d = kr = ls$,

(b) $rs < d < kl$,

(c) $k > s$ *and* $l > r$,

(d) *If* $r \leq s$ *then* $k \geq l$,

(e) $B_1 \cap C_1 = \{x\}$, *and*

(f) $|B_i \cap C_j| = 0$ *or* 1 *for* $1 \leq i \leq k$ *and* $1 \leq j \leq l$.

Proof. First note that $d = |G|/|H| = (|G|/|K|)(|K|/|H|) = kr$ and similarly $d = (|G|/|L|)(|L|/|H|) = ls$. Also $|G| > |KL| = |K||L|/|K \cap L| = |K||L|/|H|$, which gives both $d = |G|/|H| > (|K|/|H|)(|L|/|H|) = rs$ and $kl = (|G|/|K|)(|G|/|L|) > |G|/|H| = d$. The other properties involving k, l, r and s now follow easily. Next, the assumption that $K \cap L = H = G_x$ implies that $B_1 \cap C_1 = x^K \cap x^L = x^H = \{x\}$. Furthermore, if $y \in B_i \cap C_j$, then choosing $g \in G$ such that $x^g = y$ gives $B_i = B_1^g$ and $C_j = C_1^g$, and it follows that $B_i \cap C_j = B_1^g \cap C_1^g = (B_1 \cap C_1)^g = \{x\}^g = \{y\}$, and thus $|B_i \cap C_j| \leq 1$ for all i and j. $\square$

Without loss of generality we may assume that $r \leq s$. Let us now label the points of some of the blocks for K and L as follows:

$$
\begin{array}{ll}
B_1 = \{x, y_2, y_3, \ldots, y_r\} & C_1 = \{x, z_2, z_3, z_4, \ldots, z_s\} \\
B_2 = \{z_2, u_{22}, u_{23} \ldots, u_{2r}\} & C_2 = \{y_2, v_{22}, v_{23}, v_{24}, \ldots, v_{2s}\} \\
B_3 = \{z_3, u_{32}, u_{33} \ldots, u_{3r}\} & C_3 = \{y_3, v_{32}, v_{33}, v_{34}, \ldots, v_{3s}\} \\
\ldots \quad \ldots & \ldots \quad \ldots \\
\ldots \quad \ldots & C_r = \{y_r, v_{r2}, v_{r3}, v_{r4}, \ldots, v_{rs}\} \\
B_s = \{z_s, u_{s2}, u_{s3} \ldots, u_{sr}\} & \ldots \quad \ldots \\
\ldots \quad \ldots &
\end{array}
$$

We can think of the blocks B_i as cosets of K in G, and the blocks C_j as cosets for L in G, respectively. Note that x and the points $y_2, y_3, \ldots, y_r$ of block B_1 lie in r different

L-blocks C_j, while x and the points $z_2, z_3, \ldots, z_s$ of block C_1 lie in s different K-blocks B_i, by the last part of Lemma 2.3. These observations help give us a partial classification of the sub-orbits of the given group action, as follows.

Lemma 2.4 *Each of the following sets is a union of orbits of $H = G_x$ on X:*

$X_1 = \{x\}$,
$X_2 = B_1 \setminus X_1 = \{y_2, y_3, \ldots, y_r\}$,
$X_3 = C_1 \setminus X_1 = \{z_2, z_3, \ldots, z_s\}$,
$X_4 = (B_2 \cup B_3 \cup \cdots \cup B_s) \setminus X_3 = \{u_{ji} : 2 \le i \le r,\ 2 \le j \le s\}$,
$X_5 = (C_2 \cup C_3 \cup \cdots \cup C_r) \setminus X_2 = \{v_{ij} : 2 \le i \le r,\ 2 \le j \le s\}$,
$X_6 = X \setminus (X_1 \cup X_2 \cup X_3 \cup X_4 \cup X_5)$.

Proof. The first is obvious; the second and third follow from the fact that $B_1^g = B_1$ and $C_1^g = C_1$ for all $g \in G_x$; the fourth and fifth follow from the fact that G_x must preserve the union of blocks B_i containing a point of X_3 and the union of blocks C_j containing a point of X_2; and the last now follows easily. □

This immediately gives us a lower bound on the number of sub-orbits:

Lemma 2.5 *The sets X_4 and X_5 are distinct, so the union $X_4 \cup X_5$ contains at least two orbits of $H = G_x$, and hence the number of orbits of G_x on X is at least five.*

Proof. Assume that $X_4 = X_5$. Then $\bigcup_{1 \le i \le s} B_i = \bigcup_{1 \le j \le r} C_j$. Call this common union U. Next, the subgroup K preserves the block B_1 and therefore preserves the set $\{C_1, C_2, \ldots, C_r\}$ of all blocks C_j containing a point of B_1, and similarly the subgroup L preserves the set $\{B_1, B_2, \ldots, B_s\}$ of all blocks B_i containing a point of C_1, and hence the common union U is preserved by both K and L. This, however, implies that U is preserved by $\langle K, L \rangle = G$ (the latter following since K and L are distinct maximal subgroups of G), and so $U = X$, and therefore $d = |X| = |U| = rs$, contradicting part (b) of Lemma 2.3. □

But further, we have the following, as a consequence of Proposition 2.2:

Lemma 2.6 *The set X_6 is non-empty, and hence the number of orbits of $H = G_x$ on X must be at least six.*

Proof. First, observe that since $\{x\}^L = C_1 = \{x, z_2, z_3, z_4, \ldots, z_s\}$, every element L takes the block B_1 to one of $B_1, B_2, \ldots, B_s$, and therefore $\{x\}^{KL} = B_1^L = \bigcup_{1 \le i \le s} B_i$. Similarly $\{x\}^{LK} = C_1^K = \bigcup_{1 \le j \le r} C_j$, and it follows that $\{x\}^{KL \cup LK} = \bigcup_{1 \le i \le s} B_i \cup \bigcup_{1 \le j \le r} C_j = \bigcup_{1 \le t \le 5} X_t$. Proposition 2.2 gives $G \ne KL \cup LK$, however, and so $X = \{x\}^G \ne \{x\}^{KL \cup LK} = \bigcup_{1 \le t \le 5} X_t$. Thus X_6 is non-empty, and the rest is easy. □

3 The rank 6 case

We now prove Theorem 1.4, using the notation and preliminary results of the previous Section.

Suppose G_x has exactly six orbits on X. By what we have seen above, these must be X_1, X_2, X_3, X_6 and two other orbits whose union is $X_4 \cup X_5$. Moreover, since $|X_4| = |X_5|$ $(= (r-1)(s-1))$ but $X_4 \neq X_5$, we see that each of $X_4 \backslash X_5$ and $X_5 \backslash X_4$ is non-empty, while $X_4 \cap X_5 = \emptyset$ (for otherwise $X_4 \cup X_5$ would contain three different orbits of G_x), and hence the six orbits of G_x have to be X_1, X_2, X_3, X_4, X_5 and X_6. Note here also that $X_5 \cup X_6$ must be the union of all the blocks B_i containing a point of X_5, and similarly $X_4 \cup X_6$ must be the union of all the blocks C_j containing a point of X_4.

Furthermore, the subgroup K acts transitively on the block $B_1 = \{x, y_2, y_3, \ldots, y_r\}$, and therefore contains elements that take points of $X_3 = C_1 \backslash X_1 = \{z_2, z_3, \ldots, z_s\}$ to points of $X_5 = \{v_{ij} : 2 \leq i \leq r,\ 2 \leq j \leq s\}$, and as these elements take the blocks $B_2, B_3, \ldots, B_s$ to blocks B_i for $s < i \leq k$, it follows that the orbits of K are $X_1 \cup X_2$, $X_3 \cup X_5$ and $X_4 \cup X_6$. Similarly, the orbits of L on X are $X_1 \cup X_3$, $X_2 \cup X_4$ and $X_5 \cup X_6$.

In particular, if g is any element of K that takes one of the blocks $B_2, B_3, \ldots, B_s$ to some block B_i for $s < i \leq k$, then B_i contains exactly one point of X_5 (the image under g of a point of X_3) and $r-1$ points of X_6 (the images under g of $r-1$ points of X_4). From this it follows that the $(r-1)(s-1)$ points of X_5 all lie in different blocks B_i, and therefore $|X_6| = |X_5|(r-1) = (r-1)(s-1)(r-1)$, and the number of blocks B_i is $k = s + |X_5| = s + (r-1)(s-1)$. But similarly, the $(r-1)(s-1)$ points of X_4 must all lie in different blocks C_j, so that $|X_6| = |X_4|(s-1) = (r-1)(s-1)(s-1)$, and the number of blocks C_j is $l = r + |X_4| = r + (r-1)(s-1)$. Comparison of the expressions for $|X_6|$ now gives $r = s$, and also $k = l = s + (s-1)(s-1) = s^2 - s + 1$.

Now consider the blocks B_i as 'points' and the blocks C_j as 'lines' of an incidence structure in which the point-line incidence relation is non-empty intersection (that is, so that B and C are incident if and only if $B \cap C$ is non-empty). Then what we have is a set of k points and a set of k lines, such that every point is incident with s lines and every line is incident with s points. We claim also that every two points are together incident with a unique line, and that every two lines are together incident with a unique point.

To prove these claims, we can argue as follows. First, the point B_1 is incident with the s lines $C_1, C_2, \ldots, C_s$, while each point B_i for $2 \leq i \leq s$ is incident with C_1 and $s-1$ of the lines $C_{s+1}, C_{s+2}, \ldots, C_l$, and each point B_i for $i > s$ is incident with just one of the lines $C_2, C_3, \ldots, C_s$ and $s-1$ of the lines $C_{s+1}, C_{s+2}, \ldots, C_l$. Thus B_1 and any given B_i for $2 \leq i \leq s$ are together incident with only the line C_1, and B_1 and any given B_i for $i > s$ are together incident with only one of the lines $C_2, C_3, \ldots, C_s$, and therefore the first claim holds when one of the points is B_1. But the group G acts transitively on the set $\{B_1, B_2, \ldots, B_k\}$ of blocks for K, and as the definition of incidence is independent of the choice of x, it follows that the first claim holds for every point B_i. The second claim holds by exactly the same argument, with points and lines interchanged.

It follows (by a standard definition) that this incidence structure is a finite projective plane, of order $q = s - 1$, with $k = q^2 + q + 1$.

If $s = 2$, then $q = 1$ and this plane is just a triangle, and so we have case (a) of our theorem. From here on we will suppose that $s > 2$.

Now the group G acts on this plane Π as a group of incidence-preserving automorphisms (or *collineations*); indeed G acts primitively on both the set of q^2+q+1 points (the blocks B_i for the maximal subgroup K) and the set of $q^2 + q + 1$ lines (the blocks C_j for the maximal subgroup L), and transitively but imprimitively on the set of incident point-line pairs (*flags*), which correspond to the original elements of X.

By a theorem of Kantor on flag-transitive projective planes [16], it follows that either Π is Desarguesian (with q a prime-power, and with G involving $\mathrm{PSL}(3, q)$), or otherwise G is a Frobenius group, q^2+q+1 is prime, and $|G|$ divides $(q^2+q+1)(q+1)$ or $(q^2+q+1)q$. In our case, the second of these is impossible, because it would imply that K and L have order $q + 1$ or q, yet we know that K acts 2-transitively on B_1 (since G_x is transitive on $X_2 = B_1 \setminus \{x\}$) and so $|K|$ is divisible by $s(s-1) = (q+1)q$. Hence, by Kantor's theorem, our incidence structure is a Desarguesian projective plane, of prime-power order q, and with $\mathrm{PSL}(3, q)$ involved in its collineation group.

This completes the proof.

4 The rank 7 case

A similar approach can be taken to prove Theorem 1.5. Again using the notation of Section 2, suppose that G_x has exactly seven orbits on X, two of which have size 1. By our previous observations, each of the sets X_1, X_2, X_3, X_4, X_5 and X_6 must be a non-empty union of orbits of G_x, with $|X_4| = |X_5| = (r-1)(s-1)$ but $X_4 \neq X_5$, and $X_4 \cup X_5$ must be the union of at least two such orbits. Hence there are just two possibilities to consider:

4.1 Suppose $X_4 \cap X_5 \neq \emptyset$.

In this case the seven orbits of G_x on X must be $X_1, X_2, X_3, X_4 \setminus X_5, X_4 \cap X_5, X_5 \setminus X_4$ and X_6, and one of these apart from X_1 has size 1.

At this stage we make the observation that each of $|X_4 \setminus X_5|$, $|X_4 \cap X_5|$ and $|X_5 \setminus X_4|$ must be divisible by both $r-1$ and $s-1$. For suppose the block C_i containing the point y_i (of X_2) contains also the points $p_1, p_2, \ldots, p_t$ of $X_4 \cap X_5$, and y_j is any other point of X_2. Then there exists an element $g \in G_x$ taking y_i to y_j, and as this element must take C_i to C_j it follows that g takes the t points $p_1, p_2, \ldots, p_t$ (of $X_4 \cap X_5$) lying in C_i to t points of $X_4 \cap X_5$ lying in C_j. Hence all of the $r-1$ blocks $C_2, C_3, \ldots, C_r$ (containing a point of X_2) contain the same numbers of points of $X_4 \cap X_5$, and so $|X_4 \cap X_5|$ is divisible by $r-1$. The analogous argument for the blocks $B_2, B_3, \ldots, B_s$ containing points of X_3 shows that $|X_4 \cap X_5|$ is divisible by $s-1$, and since $|X_4| = |X_5| = (r-1)(s-1)$, it follows that also both $|X_4 \setminus X_5|$ and $|X_5 \setminus X_4|$ are divisible by $r-1$ and $s-1$ as well.

Now if $|X_2| = 1$, then $r = 2$, but then the above observation gives $|X_4 \cap X_5| = s - 1 = |X_4|$, and so $X_4 = X_5$, a contradiction. Thus $s \geq r > 2$. In particular, this rules out the possibilities that $|X_3| = 1$ or $|X_4 \setminus X_5| = 1$ or $|X_4 \cap X_5| = 1$ and $|X_5 \setminus X_4| = 1$, and so we conclude that $|X_6| = 1$.

By definition of X_6, it follows that the number of blocks B_i for K is $k = s + 1$ and the number of blocks C_j for L is $l = r + 1$. In particular, $d = kr = r(s+1) = rs + r$ while also $d = ls = (r+1)s = rs + s$, and therefore $r = s$ and $k = l = s + 1$ and $d = s(s+1)$.

Now consider the action of G on the set $\mathcal{L} = \{C_1, C_2, \ldots, C_l\}$ of blocks for L. First the subgroup K permutes transitively the s blocks $C_1, C_2, \ldots, C_s$ containing a point of B_1, so fixes $C_l = C_{s+1}$ (setwise), and therefore G is 2-transitive on $\mathcal{L}$. Furthermore, the subgroup G_x fixes each of C_1 and C_{s+1} (setwise) and permutes transitively the $s - 1$ blocks $C_2, C_3, \ldots, C_s$ containing a point of X_2, so G is 3-transitive on $\mathcal{L}$.

Next, clearly the subgroup $G_x = K \cap L$ is the stabilizer of the ordered pair (C_1, C_{s+1}) in this action of G on $\mathcal{L}$, and it follows that the original action of G on X is equivalent to its action on ordered pairs of distinct members of $\mathcal{L}$. Letting $\alpha = C_1$ and $\omega = C_{s+1}$, we now see that K and L are the stabilizers in G of ω and α respectively, and that the seven orbits of G_x on X must be equivalent to the following:

$$
\begin{aligned}
O_1 &= \{(\alpha, \omega)\}, \\
O_2 &= \{(\lambda, \omega) : \lambda \in \mathcal{L} \setminus \{\alpha, \omega\}\}, \\
O_3 &= \{(\alpha, \lambda) : \lambda \in \mathcal{L} \setminus \{\alpha, \omega\}\}, \\
O_4 &= \{(\omega, \lambda) : \lambda \in \mathcal{L} \setminus \{\alpha, \omega\}\}, \\
O_5 &= \{(\lambda, \alpha) : \lambda \in \mathcal{L} \setminus \{\alpha, \omega\}\}, \\
O_6 &= \{(\lambda, \mu) : \lambda, \mu \in \mathcal{L} \setminus \{\alpha, \omega\}, \lambda \neq \mu\}, \text{ and} \\
O_7 &= \{(\omega, \alpha)\}.
\end{aligned}
$$

(In fact $O_1, O_2, O_3, O_4, O_5, O_6$ and O_7 are equivalent to $X_1, X_2, X_3, X_4 \setminus X_5$, $X_5 \setminus X_4$, $X_4 \cap X_5$ and X_6 respectively; and the orbits of K are $O_1 \cup O_2$ ($\approx X_1 \cup X_2$), $O_3 \cup O_5 \cup O_6$ ($\approx X_3 \cup X_5$) and $O_4 \cup O_7$ ($\approx (X_4 \setminus X_5) \cup X_6$), while the orbits of L are $O_1 \cup O_3$ ($\approx X_1 \cup X_3$), $O_2 \cup O_4 \cup O_6$ ($\approx X_2 \cup X_4$) and $O_5 \cup O_7$ ($\approx (X_5 \setminus X_4) \cup X_6$).)

In particular, as $G_x = K \cap L = G_{\alpha\omega}$ has to be transitive on the set O_6, it follows that G is 4-transitive on $\mathcal{L}$. By the classification of 2-transitive finite groups, all finite 4-transitive permutation groups are known; see [6] or [7]. Accordingly, the action of G on $\mathcal{L}$ is equivalent to the natural action of either one of the Mathieu groups M_{11}, M_{12}, M_{23} or M_{24}, or the alternating group A_k (for $k \geq 5$) or the symmetric group S_k (for $k \geq 4$). As each of these groups is 'almost simple', the permutation group induced by the action of G on ordered pairs of members of $\mathcal{L}$ is isomorphic to the permutation group induced by the action of G on $\mathcal{L}$, and therefore G itself is isomorphic to one of them, as required.

4.2 Suppose $X_4 \cap X_5 = \emptyset$.

In this case one of X_2, X_3, X_4, X_5 and X_6 is a union of two orbits of G_x, while the four others and $X_1 = \{x\}$ are all single orbits of G_x.

Now if X_2 is the union of two orbits of G_x, say U and V, then also X_5 will split into two orbits of G_x (one consisting of points of X_5 from blocks C_j containing a point of U and the other consisting of points of X_5 from blocks C_j containing a point of V), so X_2 must be a single orbit. Similarly, X_3 is a single orbit.

Next, just as in the proof of Theorem 1.4, we can show that $X_1 \cup X_2$ and $X_3 \cup X_5$ are orbits of K, and that $X_1 \cup X_3$ and $X_2 \cup X_4$ are orbits of L. (Note: the possibility that X_4 or X_5 is a union of two orbits of G_x does not affect the argument, since X_2 and X_3 are orbits of $K \cap L = G_x$, and only one of X_4, X_5 and X_6 is not.) Moreover, again we find that the $(r-1)(s-1)$ points of X_5 all lie in different blocks B_i (for $s < i \leq k$), and that the $(r-1)(s-1)$ points of X_4 must all lie in different blocks C_j (for $r < j \leq l$).

Now if X_6 were a single orbit, then it would have to consist of all the points in the blocks $B_{s+1}, B_{s+2}, \ldots, B_k$ other than those already lying in X_5, and at the same time consist of all points in the blocks $C_{r+1}, C_{r+2}, \ldots, C_l$ other than those already lying in X_4, and in particular, we would have $|X_6| = |X_5|(r-1)$ and $|X_6| = |X_4|(s-1)$ in this case. But if p and q are any points of X_6 lying in different blocks B_i and B_j, and g is any element of G_x taking p to q, then g takes B_i to B_j and therefore takes the unique point of X_5 in B_i to the unique point of X_5 lying in B_j, and it follows that X_5 forms a single orbit of G_x. The analogous argument for the blocks $C_{r+1}, C_{r+2}, \ldots, C_l$ shows that X_4 is a single orbit of G_x. It follows that G_x has only six orbits, a contradiction. Thus X_6 is the union of two orbits of G_x, while X_4 and X_5 are single orbits of G_x.

Next, let U be the union of all blocks B_i that contain a point of X_5, and let V be the union of all blocks C_j containing a point of X_4. Then $|U| = |X_5|r = r(r-1)(s-1)$ while $|V| = |X_4|s = s(r-1)(s-1)$. Also U and V are preserved by G_x and hence each of $U \setminus X_5$ and $V \setminus X_4$ is a union of orbits of G_x contained in X_6. It follows that each of $(U \setminus X_5) \setminus (V \setminus X_4)$ and $(V \setminus X_4) \setminus (U \setminus X_5)$ and $(U \setminus X_5) \cap (V \setminus X_4)$ is a union of orbits of G_x, but at most two of these can be non-empty.

If $r = s$ then $|U| = |V| = s(s-1)^2$ so $|U \setminus X_5| = |V \setminus X_4| = s(s-1)^2 - (s-1)^2 = (s-1)^3$. Now if $U \setminus X_5 \neq V \setminus X_4$, then $(U \setminus X_5) \cap (V \setminus X_4)$ must be empty, and hence the seven orbits of G_x are X_1, X_2, X_3, X_4, X_5, $U \setminus X_5$ and $V \setminus X_4$, of sizes 1, $s-1$, $s-1$, $(s-1)^2$, $(s-1)^2$, $(s-1)^3$ and $(s-1)^3$ respectively, but this makes it impossible for just two of the orbits of G_x to have size 1. Thus $U \setminus X_5 = V \setminus X_4 = T$, say. Again none of the orbits X_2, X_3, X_4 and X_5 can have size 1 (for otherwise $r = s = 1$ and then all of them have size 1), so either T is an orbit of G_x and $|X_6| = |T| + 1$, or $T = X_6$ is a union of two orbits of G_x, one of which has size 1. In the former case, summing the orbit sizes gives $d = |X| = 1 + (s-1) + (s-1) + (s-1)^2 + (s-1)^2 + (s-1)^3 + 1 \equiv 1 \bmod s$, but since $d = ls$, this gives a contradiction; in the latter case, the block B_i containing both a point of X_5 and the orbit of G_x of size 1 must be fixed by G_x, and hence the point of X_5 forms another single orbit for G_x of size 1, another contradiction.

Thus $r < s$. Clearly this gives $|U| < |V|$ and so $|U \setminus X_5| < |V \setminus X_4|$. It follows that $U \setminus X_5$ must be an orbit of G_x, and the seventh orbit of G_x must be $X_6 \setminus (U \setminus X_5)$, which could be either $V \setminus X_4$ or $(V \setminus X_4) \setminus (U \setminus X_5)$. The sizes of the seven orbits of G_x are therefore 1,

$r-1$, $s-1$, $(r-1)(s-1)$, $(r-1)(s-1)$, $(r-1)^2(s-1)$ and either $(r-1)(s-1)^2$ or $(r-1)(s-1)(s-r)$. Since $(r-1)(s-1) > s-1 > r-1$, the smallest of these sizes are 1 and $r-1$, and so the second orbit of G_x of size 1 must be X_2, and thus $r = 2$.

In particular, we now know that the orbits of G_x have sizes $1, 1, s-1, s-1, s-1, s-1$ and either $(s-1)^2$ or $(s-1)(s-2)$. Note that the sum of first five of these is $3s-1$, so $|X_6| = d-(3s-1) = d-3s+1$. Since $d = ls$, however, $|X_6| = d-3s+1 \equiv 1$ modulo s, so $|X_6|$ cannot be the sum of $|U \setminus X_5| = s-1$ and $|V \setminus X_4| = (s-1)^2$, and it follows that $X_6 = V \setminus X_4$, and the seventh orbit of G_x has to be $(V \setminus X_4) \setminus (U \setminus X_5)$, of size $(s-1)(s-2)$. Thus $d = |X_6| + 3s - 1 = (s-1)^2 + 3s - 1 = s^2 + s = s(s+1)$.

Also $k = d/r = s(s+1)/2$, while $l = d/s = s+1$.

Now consider the action of G on the set $\mathcal{L} = \{C_1, C_2, \ldots, C_l\}$ of blocks for L. Just as in case 4.1, we see that G is 3-transitive on $\mathcal{L}$, and that the action of G on X is equivalent to its action on ordered pairs of distinct members of $\mathcal{L}$. In this case, however, if $(\alpha, \omega) = (C_1, C_l) = (C_1, C_{s+1})$ then K is the stabilizer in G of $\{\alpha, \omega\}$ (while L is still the stabilizer of α), and the orbits of G_x on X are still equivalent to the sets $O_1, O_2, \ldots, O_7$ defined in case 4.1. (Also $O_1, O_2, O_3, O_4, O_5, O_6$ and O_7 are equivalent to X_1, $U \setminus X_5$, X_3, X_5, X_4, $(V \setminus X_4) \setminus (U \setminus X_5)$ and X_2 respectively; and the orbits of K are $O_1 \cup O_7$ ($\approx X_1 \cup X_2$), $O_3 \cup O_4$ ($\approx X_3 \cup X_5$), $O_2 \cup O_5$ ($\approx X_4 \cup (U \setminus X_5)$) and O_6 ($\approx (V \setminus X_4) \setminus (U \setminus X_5)$), while the orbits of L are $O_1 \cup O_3$ ($\approx X_1 \cup X_3$), $O_5 \cup O_7$ ($\approx X_2 \cup X_4$) and $O_2 \cup O_4 \cup O_6$ ($\approx X_5 \cup V$).) Again $G_x = G_{\alpha\omega}$ has to be transitive on the set O_6, and so G is 4-transitive on $\mathcal{L}$, and the rest follows.

References

[1] C. Berge, *Principes de Combinatoire*, Dunod, Paris, 1968.

[2] N. Biggs and A.T. White, *Permutation groups and combinatorial structures*, Math. Soc. Lect. Note Series, vol. 33 (Cambridge Univ. Press, Cambridge), 1979.

[3] D. Bisch and V. Jones, Algebras associated to intermediate subfactors, *Invent. Math.* 128 (1997) 89–158.

[4] D. Bisch and V. Jones, Singly generated planar algebras of small dimension, *Duke Math. J.* 101 (2000), 41–75.

[5] W. Bosma, J. Cannon and C. Playoust: The MAGMA Algebra System I: The User Language, *J. Symbolic Comput.* 24 (1997), 235–265.

[6] P.J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts, 45, Cambridge University Press (Cambridge), 1999.

[7] J.D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[8] M. Gilpin, Three identities between Stirling numbers and the stabilizing character sequence, *Proc. Amer. Math. Soc.* 60 (1976), 360–364.

[9] D. Gorenstein, *Finite Groups*, 2nd ed., Chelsea Publishing Co., New York, 1980.

[10] P. Grossman and V.F.R. Jones, Intermediate subfactors with no extra structure, *preprint.*

[11] M. Izumi, Characterization of isomorphic group-subgroup subfactors, *Int. Math. Res. Not.* 34 (2002), 1791–1803.

[12] G. James and M. Liebeck, *Representations and Characters of Groups*, 2nd ed., Cambridge University Press, New York, 2001.

[13] V.F.R. Jones, Actions of finite groups on the hyperfinite type II_1 factor, *Mem. Amer. Math. Soc.* 28 (1980), no. 237, v+70 pp.

[14] V.F.R. Jones, The annular structure of subfactors, In: *Essays on Geometry and Related Topics* (ed. E. Ghys, P. de la Harpe, V.F.R. Jones, V. Sergiescu, T. Tsuboi), *L'Enseignement Mathematique* 38 (2001), 401–463.

[15] V.F.R. Jones, Quadratic tangles in planar algebras, *preprint.*

[16] W.M. Kantor, Primitive permutation groups of odd degree, and an application to finite projective planes, *J. Algebra* 106 (1987), 15–45.

[17] T. Sano and Y. Watatani, Angles between two subfactors, *J. Operator Theory* 32 (1994), 209–241.

[18] Y. Watatani, Lattices of intermediate subfactors, *J. Funct. Anal.* 140 (1996), 312–334.