PRIMITIVE SUBGROUPS OF WREATH PRODUCTS IN PRODUCT ACTION

L. G. KOVÁCS

[Received 5 October 1987—Revised 5 May 1988]

1. *Introduction*

This paper is concerned with *finite* primitive permutation groups G which are subgroups of wreath products W in product action *and are such that the socles of G and W are the same.* The aim is to explore how the study of such groups may be reduced to the study of smaller groups.

The O'Nan–Scott Theorem (see Liebeck, Praeger, Saxl [**12**] for the most recent and detailed treatment) sorts finite primitive permutation groups into several types, the groups in any one type admitting a common discussion. One of the types (III(b) in [**12**]) consists of groups G which are contained in, and contain the socle of, a suitable wreath product W in product action. It is easy to see that in this case the socles of G and W actually coincide. Thus the aim here amounts to pursuing the discussion of primitive groups of this type beyond the conclusions reached, say, in [**12**]. It has not proved possible to make direct use of those conclusions here. Instead, it seems necessary to repeat, elaborate, extend, and recombine arguments from various proofs of the O'Nan–Scott Theorem. No attempt will be made here to trace the origins of the ideas so used.

For a sketch of the main results, some terminology is needed. By a wreath product $A \operatorname{Wr} S_n$ we mean the usual semidirect product W of the symmetric group S_n and the n-fold direct power A^n of the (abstract) group A. The projection of W onto S_n corresponding to this semidirect decomposition will be denoted by π. Consider π a permutation representation of W and take a point stabilizer W_o: this has an obvious direct factorization

$$W_o = S_{n-1}A^n = A \times S_{n-1}A^{n-1} = A \times (A \operatorname{Wr} S_{n-1});$$

let π_o denote the corresponding projection of W_o onto the first direct factor A. A subgroup B of W will be called *large* if $B\pi$ is transitive (as a subgroup of S_n) and $(B \cap W_o)\pi_o = A$. Note that once $B\pi$ is transitive the validity of $(B \cap W_o)\pi_o = A$ is independent of the point o whose stabilizers in S_n and W were taken as S_{n-1} and W_o, respectively. Also, all conjugates of large subgroups are large. If A is a group of permutations, say, on a set Ω, then W has an obvious faithful permutation representation on the cartesian power Ω^n: this is called the product action of W, and we refer to its image as W *in product action.* (James and Kerber [**5**] call this permutation group W the exponentiation of A by S_n.)

The paper is centred on the following construction. The input consists of a primitive group G with socle M, say, and of a large subgroup B in a wreath product $(G/M) \operatorname{Wr} S_n$ with $n > 1$. The output is a permutation group we denote

---

A.M.S. (1980) subject classification: 20B15.

by $G \uparrow B$; more precisely, a subgroup $G \uparrow B$ of the wreath product $G \operatorname{Wr} S_n$ in product action. Namely, $G \uparrow B$ is the complete inverse image of B under the natural homomorphism of $G \operatorname{Wr} S_n$ onto $(G/M) \operatorname{Wr} S_n$. We call $G \uparrow B$ the *blow-up of G by B,* and n the *blow-up index.*

It will be shown (in the next section) that the socle of $G \operatorname{Wr} S_n$ is the socle of $G \uparrow B$ whenever $G \uparrow B$ is primitive. Conversely, if G is any primitive subgroup of a wreath product $W = A \operatorname{Wr} S_n$ in product action, then $G\pi$ must be transitive and $(G \cap W_o)\pi_o$ must be a primitive subgroup, G_0 say, in A. Further, if this G contains the socle of W, then the socle of G_0 is the socle of A and G is (conjugate in W to) a blow-up of G_0. Thus the problem posed in the opening paragraph amounts to the study of primitive blow-ups.

When G has prime order, each blow-up of G has proper non-trivial centre and is therefore imprimitive. The opposite extreme is characterized by the following theorem.

THEOREM 1. *All blow-ups of a primitive group G are primitive if and only if the socle of G is not regular. In that case, the socles of the blow-ups of G are also non-regular.*

If a primitive G is a blow-up of G_1 and G_1 is a blow-up of G_0 then G is also (permutationally isomorphic to) a blow-up of G_0: so a group can be a blow-up in many different ways. When the socle of G is non-regular, this matter can be kept under control.

THEOREM 2. *If a primitive group G with non-regular socle is a blow-up at all, then in particular it is a blow-up $G_0 \uparrow B$ of a unique G_0 which is not itself a blow-up. The socle M_0 of G_0 is also non-regular; the blow-up index n and the relevant large subgroup B of $(G_0/M_0) \operatorname{Wr} S_n$ are determined by G.*

This theorem is something of an over-simplification. The first sentence of this theorem will be re-phrased and amplified in terms of the *blow-up decomposition* concept and proved as Theorem 2^+ in § 4. General facts concerning that concept will be dealt with in § 3, the first half of the second sentence of Theorem 2 finding justification in the second paragraph of the proof of Theorem (3.3). The second half of the second sentence will be elaborated and proved as Theorem 2^{++} in § 5.

In a sense, these results reduce the study of primitive groups with non-regular socle to the case of groups which are not blow-ups. In view of the previous discussion (or see (2.4) below), a group of the latter kind cannot lie in a wreath product W in product action so as to contain the socle of W: that is, it cannot be of Type III(b) in the sense of Liebeck, Praeger, Saxl **[12]**. Thus the O'Nan–Scott Theorem implies that *the primitive groups with non-regular socle which are not blow-ups are precisely the following: the primitive groups with non-abelian simple socle; those subgroups of the holomorphs of non-abelian simple groups which contain all right translations and all left translations; and the primitive groups in which the socle is minimal normal and a maximal normal subgroup of the socle is regular.* The groups of the last kind are sometimes called *primitive groups of simple diagonal type:* see **[9]**.

For primitive groups with regular socle, the results on blow-ups are far less conclusive. A primitive group G with abelian socle is, of course, a subgroup of an affine group $\mathrm{AGL}(k, p)$ over a finite prime field; the socle M of G is the (regular) group of all translations, while a point stabilizer H is an irreducible subgroup of $\mathrm{GL}(k, p)$. If B is a large subgroup of $W = H \mathrm{Wr}\, S_n$, set $C = B \cap W_o$ and regard M as a C-module with action given by π_o: the blow-up $G \uparrow B$ is then the semidirect product of B and of the B-module induced from this C-module M, the semidirect factor B being one of the point-stabilizers in $G \uparrow B$. Since a linear representation induced from an irreducible representation need not be irreducible, the blow-up $G \uparrow B$ need not be primitive. In general, no canonical choice seems possible among the subgroups minimal with respect to a given irreducible linear representation being induced from them. Thus Theorems 1 and 2 correspond to fundamental issues of linear representation theory which are not capable of so simple a resolution.

A primitive group with non-abelian regular socle is a twisted wreath product (with the socle as base group and a point stabilizer as top group). It has proved more profitable to investigate such groups in terms other than blow-ups: see Lafuente [**11**], Kovács [**10**], and Förster and Kovács [**4**].

2. *Blow-up constructions*

A point of terminology may need clarification. Each direct power A^n will be thought of as the group of all functions $\{1, \ldots, n\} \to A$. Among these, the constant functions form *the* 'diagonal' subgroup, which will be denoted $\operatorname{diag} A^n$.

The aim of this section is to prove the claims made in the Introduction up to, and including, Theorem 1. Throughout, G is a primitive group with socle M and B is a large subgroup of $(G/M)\mathrm{Wr}\, S_n$, with $n > 1$; moreover, H is a point stabilizer in G, and W is $G \mathrm{Wr}\, S_n$ in product action so $S_n H^n$ is a point stabilizer in W.

If M is abelian then it is its own centralizer $\mathbb{C}_G(M)$, while if M is non-abelian then $\mathbb{C}_G(M) = 1$, so in either case $\mathbb{C}_G(M) \leqslant M$. As $\mathbb{C}_W(M^n) \leqslant G^n$, it follows that $\mathbb{C}_W(M^n) \leqslant M^n$. Thus each minimal normal subgroup of $G \uparrow B$ or of W must lie in M^n:

$$\operatorname{soc}(G \uparrow B) \leqslant M^n \quad \text{and} \quad \operatorname{soc} W \leqslant M^n.$$

If M is non-abelian, then the normal subgroup M^n is a direct product of non-abelian simple groups and is therefore contained in $\operatorname{soc}(G \uparrow B)$ and in $\operatorname{soc} W$. If M is abelian but the order $|G|$ of G is not prime, then M is minimal normal in G and the mutual commutator subgroup $[M, G]$ is M. In this case the minimal normal subgroups of G^n are just the obvious direct factors (the 'coordinate subgroups') of M^n; as these are transitively permuted by S_n, now M^n is minimal normal in W. This has established most of the following.

(2.1) *We always have* $\operatorname{soc} W \leqslant M^n \leqslant G \uparrow B$, *with* $\operatorname{soc} W = M^n$ *except perhaps when* $|G|$ *is prime. If* M *is non-abelian or if* $G \uparrow B$ *is primitive, then* $\operatorname{soc}(G \uparrow B) = M^n = \operatorname{soc} W$.

The outstanding part of this is the case of abelian M and primitive $G \uparrow B$. Then $\operatorname{soc}(G \uparrow B) = M^n$ because M^n is a non-trivial abelian normal subgroup in the

primitive group $G \uparrow M$, and $M^n = \operatorname{soc} W$ because (as we noted in the Introduction) $|G|$ cannot be a prime. This completes the proof of (2.1).

We shall need a general fact which does not depend on G being a permutation group, let alone on G being primitive.

(2.2) *If $X \leqslant W$ and $X\pi$ is transitive, then there is an element w in $G^n \cap \ker \pi_o$ such that the conjugate X^w of X lies in $(X \cap W_o)\pi_o \operatorname{Wr} S_n$.*

Proof. The transitivity of $X\pi$ means precisely that $|X : (X \cap W_o)| = n$, so the Embedding Theorem (see the last section of [**3**] for a recent treatment) provides certain embeddings of X into $(X \cap W_o) \operatorname{Wr} S_n$. Compose one of these first with the inclusion of this wreath product in $W_o \operatorname{Wr} S_n$ and then with the natural homomorphism $\pi_o \operatorname{Wr} S_n$: $W_o \operatorname{Wr} S_n \to W$ defined from π_o. Use the Uniqueness Theorem from [**6**] to verify that this composite, whose image lies in the subgroup $(X \cap W_o)\pi_o \operatorname{Wr} S_n$ of W, is the inclusion $X \hookrightarrow W$ followed by an inner automorphism of W induced by some element of $G^n \cap \ker \pi_o$. This proves (2.2).

We shall use repeatedly the following simple fact (see Proposition 3.2 and the last sentence of § 3 of Cameron [**1**], or Lemma 2.1 of Praeger, Saxl, and Yokoyama [**13**]).

(2.3) *The wreath product in product action of two permutation groups is primitive if and only if the second group is transitive while the first group is primitive and not of prime order.*

Let X be any primitive subgroup of W; then the larger subgroup $G \operatorname{Wr} X\pi$ is also primitive, so $X\pi$ must be transitive. Set $X_0 = (X \cap W_o)\pi_o$: by (2.2), $X_0 \operatorname{Wr} S_n$ contains some conjugate of X and is therefore primitive; consequently X_0 is a primitive subgroup, not of prime order, in G. As G has a primitive subgroup X_0 which is not of prime order, $\operatorname{soc} W = M^n$ by (2.1): in particular, $\operatorname{soc} W$ is either abelian or a direct product of non-abelian simple groups. Suppose also that $X \geqslant \operatorname{soc} W$. Being a normal subgroup with the given structure in the primitive group X, $\operatorname{soc} W$ must lie in $\operatorname{soc} X$; on the other hand,

$$\mathbb{C}_X(\operatorname{soc} W) \leqslant \mathbb{C}_W(\operatorname{soc} W) \leqslant \operatorname{soc} W$$

implies that $\operatorname{soc} W$ must contain each minimal normal subgroup of X: thus $\operatorname{soc} X = \operatorname{soc} W = M^n$. It follows that $M \leqslant X_0$. Imitate the argument above: if the socle (there $\operatorname{soc} W$, here $\operatorname{soc} G$) lies in a primitive subgroup (there X, here X_0), then it is the socle of that subgroup, so $M = \operatorname{soc} X_0$. Finally, by (2.2) there is a w in $G^n \cap \ker \pi_o$ such that $X^w \leqslant X_0 \operatorname{Wr} S_n$. As w normalizes M^n, we have $M^n \trianglelefteq X^w$. Set

$$B = X^w/M^n \leqslant (X_0 \operatorname{Wr} S_n)/M^n = (X_0/M) \operatorname{Wr} S_n;$$

then B is a large subgroup of the last wreath product, and $X^w = X_0 \uparrow B$. We have proved the following.

(2.4) *If X is a primitive subgroup of W containing* $\operatorname{soc} W$, *then X is conjugate in W to a blow-up of a primitive subgroup X_0 of G such that* $\operatorname{soc} X_0 = M$.

It remains to prove Theorem 1. To this end, suppose first that M is regular; choose $n = 2$ and $B = S_2 \times \operatorname{diag}(G/M)^2$, and form $G \uparrow B$. Now $(G \uparrow B) \cap S_2H^2$ is a point stabilizer in $G \uparrow B$. The regularity of M means that G is the semidirect product of H and M; hence W is the semidirect product of S_2H^2 and M^2, while $G \uparrow B$ is the semidirect product of $(G \uparrow B) \cap S_2H^2$ and M^2. Since $S_2 \operatorname{diag} H^2$ is obviously a subgroup of $(G \uparrow B) \cap S_2H^2$ and

$$|S_2 \operatorname{diag} H^2| = 2\,|H| = 2\,|G/M| = |B| = |(G \uparrow B)/M^2| = |(G \uparrow B) \cap S_2H^2|,$$

we have that $S_2 \operatorname{diag} H^2$ is the point stabilizer $(G \uparrow B) \cap S_2H^2$ in $G \uparrow B$, and then $S_2 \operatorname{diag} H^2 < S_2 \operatorname{diag} G^2 < G \uparrow B$ show that the blow-up $G \uparrow B$ is not primitive.

The starting points for the second half of the proof are two general properties of blow-ups. First, *each blow-up is transitive;* because M, being a non-trivial normal subgroup of the primitive G, is transitive on Ω and so M^n is transitive on Ω^n. The second we establish as a separate item.

(2.5) *For the point stabilizer $(G \uparrow B) \cap S_nH^n$ of $G \uparrow B$,*

$$[(G \uparrow B) \cap S_nH^n \cap W_o]\pi_o = H.$$

Proof. The only point to prove is that each element h of H has a pre-image in this point stabilizer. As $G \uparrow B$ is large (because B is), there certainly is an x in $(G \uparrow B) \cap W_o$ with $x\pi_o = h$. Since M^n is transitive, one can write x as yz with $y \in (G \uparrow B) \cap S_nH^n$ and $z \in M^n$. Further, this z factorizes according to the direct decomposition

$$W_o = G \times S_{n-1}G^{n-1} \geq M^n = M \times M^{n-1};$$

say, as $z = uv$, with $u \in M \times 1$ and $v \in 1 \times M^{n-1}$. Then

$$h = x\pi_o = (yuv)\pi_o = (y\pi_o)(u\pi_o),$$

so $u\pi_o = (y\pi_o)^{-1}h \in H \cap M$ shows that

$$u \in (H \cap M) \times 1 \leq (H \cap M)^n \leq (G \uparrow B) \cap (H \operatorname{Wr} S_n);$$

thus $yu \in (G \uparrow B) \cap S_nH^n \cap W_o$ and $(yu)\pi_o = h$, as required.

To proceed with the proof of Theorem 1, suppose M is not regular: $H \cap M > 1$. Then M is non-abelian, so (2.1) shows that $\operatorname{soc}(G \uparrow B) = M^n$, and hence $S_nH^n \cap M^n = (H \cap M)^n > 1$ shows that $\operatorname{soc}(G \uparrow B)$ is certainly not regular. Moreover, now M is the normal closure of $H \cap M$ in G. (For, as H is maximal in G, so $H \cap M$ is maximal among the subgroups of M normalized by H; thus the only alternative is that $H \cap M$ is normal in G. Every non-trivial normal subgroup of a primitive group is transitive, but $H \cap M$ fixes a point, so this alternative is not available.) This will be used in establishing the outstanding part of Theorem 1, namely, that in this case $G \uparrow B$ is primitive. We shall do this by proving that a subgroup K of $G \uparrow B$ which properly contains the point stabilizer $(G \uparrow B) \cap S_nH^n$ must be equal to $G \uparrow B$.

The first point to show is that $(K \cap W_o)\pi_o = G$. Since (2.5) holds and H is a maximal subgroup of G, the alternative is $(K \cap W)\pi_o = H$. By (2.2), there is then a w in W such that $K \leq (S_nH^n)^w$. As $W = (S_nH^n)M^n$, one can write $w = uv^{-1}$ with

$u \in S_nH^n$ and $v \in M^n$, and obtain that $G \uparrow B \geqslant K^v \leqslant (S_nH^n)^u = S_nH^n$, whence $K^v \leqslant (G \uparrow B) \cap S_nH^n < K$ follows, which is impossible.

Now consider the subgroup $K \cap W_o$ of the direct product $W_o = G \times S_{n-1}G^{n-1}$. As $(K \cap W_o)\pi_0 = G$, we have

$$W_o = (K \cap W_o)(1 \times S_{n-1}G^{n-1});$$

since $K \cap (M \times 1)$ is normalized by $K \cap W_o$ and centralized by $1 \times S_{n-1}G^{n-1}$, it is normal in W_o and hence also in $G \times 1$. On the other hand,

$$K \cap (M \times 1) \geqslant (G \uparrow B) \cap S_nH^n \cap (M \times 1) = (H \cap M) \times 1,$$

and, as we have seen, the normal closure of $H \cap M$ in G is M: so $K \geqslant M \times 1$. Now $KM^n \geqslant [(G \uparrow B) \cap S_nH^n]M^n = G \uparrow B$, so $K\pi = (G \uparrow B)\pi$; thus K permutes transitively the coordinate subgroups of M^n: as it contains $M \times 1$, which is one of them, it contains them all, so $K \geqslant M^n$ and $K = KM^n = G \uparrow B$ follows, as required. This completes the proof of Theorem 1.

3. *Blow-up decompositions: the concept*

In analogy with external and internal direct products, the blow-up construction is matched by an appropriate decomposition concept: we need to set conventions for this. These will take advantage of the assumption that the socle is not regular; otherwise they could not be kept quite so simple. The whole of this section will be devoted to establishing the relevant general facts.

It is convenient to take the view that a direct decomposition amounts to the (unordered) set of the subgroups which play the role of direct factors. We shall say that a *blow-up decomposition* of a primitive group G with non-regular socle M and point stabilizer H is a direct decomposition (with more than one factor) of M such that

(3.1) *first, the direct factors form a (single, complete) conjugacy class of subgroups in G, and*
second, $H \cap M$ is the product of its intersections with these direct factors.

(Clearly, whether a given direct decomposition of M satisfies these conditions does not depend on which point stabilizer was named H). In one direction, (3.1) is immediately justified: by construction, the socle of each blow-up is a direct power, so it comes with a distinguished direct decomposition which obviously satisfies (3.1).

In the other direction one would like to show that, *given a direct decomposition of M satisfying* (3.1), *there is a distinguished permutational isomorphism from G to a certain blow-up taking the given decomposition of M to that which the socle of the blow-up has by construction.* Unfortunately this long sentence is not long enough to match the complexity of the situation. Indeed, even the analogous statement for direct products involves choosing an order on the set of direct factors first. Here one has to start by picking out one of the direct factors but need not order the rest: on this preference depends the wreath product in product action in which the blow-up lives, but the dependence is only within permutational isomorphism. Then one has to choose a transversal for the normalizer of the preferred direct factor: on this depends the actual copy of the blow-up and

the permutational isomorphism from G to the blow-up, but only up to composition with inner automorphisms of the wreath product.

We now proceed to make this explicit. Let G be a primitive group acting on a set Ω, with socle M and point stabilizer H, and such that $H \cap M > 1$. Consider a conjugacy class $\{R_1, \ldots, R_n\}$ of non-normal subgroups of G such that $M = R_1 \times \ldots \times R_n$ and $H \cap M = (H \cap R_1) \times \ldots \times (H \cap R_n)$. Set $P = R_2 \times \ldots \times R_n$ and $Q = \mathbb{N}_G(P)$; denote by Z the normal core of $(H \cap Q)P$ in Q. The first point to establish is that $Z \cap M = P$. To this end, note that $P \leqslant Z \leqslant (H \cap Q)P$ yields $Z = (H \cap Z)P$ whence

$$P \leqslant Z \cap M = [(H \cap Z) \cap (Z \cap M)]P \leqslant (H \cap M)P = (H \cap R_1) \times P,$$

and therefore $Z \cap M = [(H \cap R_1) \cap (Z \cap M)] \times P = (H \cap Z \cap R_1) \times P$. On the other hand, $P \leqslant Z \cap M \leqslant M = R_1 \times P$ gives that $Z \cap M = (Z \cap R_1) \times P$. Comparing this with the conclusion of the previous sentence, we see that $Z \cap R_1 \leqslant H$. Since $Z \cap R_1$ is normal in M (because Z is normal in Q which contains M), the product of the H-conjugates of $Z \cap R_1$ is normal both in H and in M; but H is corefree in G, so we must have $Z \cap R_1 = 1$. Thus indeed $Z \cap M = (Z \cap R_1) \times P = P$. Now it is straightforward to verify that the sublattice generated in the subgroup lattice of G by H, M, P, Q, and Z, is as pictured on the left of Fig. 1.

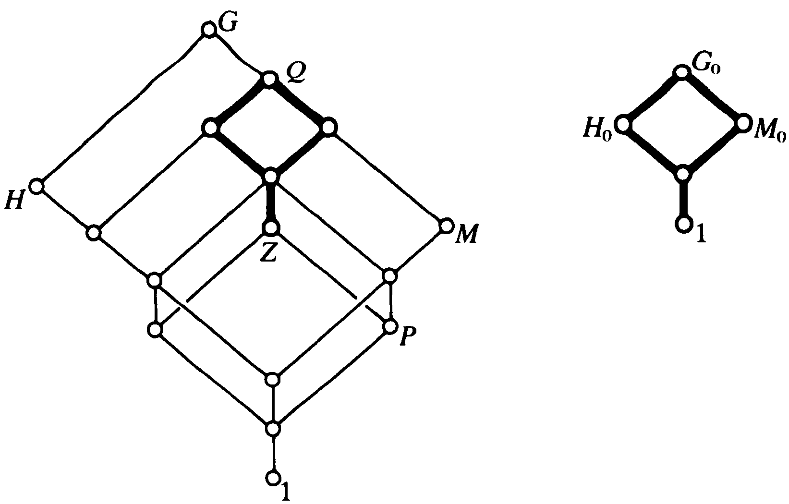

FIG. 1

As we shall see later,

$$Z = \mathbb{C}_Q(M/P). \tag{3.2}$$

Let G_0 be the group of permutations induced by Q on the set Ω/P of the P-orbits in Ω, and ζ the obvious homomorphism of Q onto G_0. Note that G_0 is transitive (on Ω/P, because $Q \geqslant M$ and M is transitive on Ω). Further, $(H \cap Q)P$ is a point stabilizer in Q with respect to the transitive permutation representation ζ of Q on Ω/P, so $\ker \zeta = Z$ and $(H \cap Q)\zeta$ is a point stabilizer H_0 in G_0. Let $M_0 = \operatorname{soc} G_0$. Choose a transversal for Q in G and use the Embedding Theorem to obtain an embedding φ of G (as an abstract group) in $Q \operatorname{Wr} S_n$ (also viewed as an abstract group); note that φ is unique up to composition with inner automorphisms of $Q \operatorname{Wr} S_n$ (see [**8**]), and that $G\varphi$ is large as a subgroup of this wreath

product. Compose φ first with the homomorphism $\bar{\zeta}$: $Q \operatorname{Wr} S_n \twoheadrightarrow G_0 \operatorname{Wr} S_n$ obtained from ζ and then with the obvious homomorphism $G_0 \operatorname{Wr} S_n \twoheadrightarrow (G_0/M_0) \operatorname{Wr} S_n$: the image B of this composite is then large in the last wreath product. Consider $G_0 \operatorname{Wr} S_n$ a permutation group with respect to its product action; then $G\varphi\bar{\zeta}$ also becomes a permutation group on $(\Omega/P)^n$.

(3.3) THEOREM. *There is a bijection β: $\Omega \to (\Omega/P)^n$ such that 'conjugation' by β acts on G as $\varphi\bar{\zeta}$ and so gives a permutational isomorphism of G onto $G\varphi\bar{\zeta}$. Moreover, G_0 is primitive, $G\varphi\bar{\zeta} = G_0 \uparrow B$, and the $R_j\varphi\bar{\zeta}$ are the 'coordinate subgroups' of the socle of $G_0 \uparrow B$.*

Defer the proof of the first sentence for the moment. By definition, the complete inverse image of B in $G_0 \operatorname{Wr} S_n$ is $(G\varphi\bar{\zeta})M_0^n$. By the first sentence of the theorem, $G\varphi\bar{\zeta}$ is primitive; therefore so is $G_0 \operatorname{Wr} S_n$, and hence G_0 itself is primitive because of (2.3). We can now say that $(G\varphi\bar{\zeta})M_0^n = G_0 \uparrow B$. Moreover, the primitivity of G_0 yields that either M_0 is minimal normal or the (two) non-trivial normal subgroups of G_0 properly contained in M_0 are regular. Now use the assumption that M is not regular: then $M\zeta$ is a direct product of non-abelian simple groups and is a normal subgroup of G_0, so $M\zeta \leq M_0$; on the other hand, $M\zeta$ is not regular (because $(H \cap M)\zeta \cong H \cap R_1 \neq 1$), so by the previous sentence we must have $M\zeta = M_0$. It follows that $M\varphi\bar{\zeta} = M_0^n$, whence $G\varphi\bar{\zeta} = (G\varphi\bar{\zeta})M_0^n = G_0 \uparrow B$. It is routine to verify that $\varphi\bar{\zeta}$ maps the R_j to the obvious direct factors, the 'coordinate subgroups', of M_0^n.

We have seen here that the socle M_0 of G_0 is not regular; this justifies the first part of the second sentence of Theorem 2. It also implies that M_0 has trivial centralizer (in G_0) and so $\mathbb{C}_Q(M/P) = Z$, which proves (3.2).

In preparation for the deferred proof of the first sentence of (3.3), we establish that $|\Omega| = |\Omega/P|^n$. To this end, note that

$$|\Omega| = |G : H| = |HM : H| = |M : (H \cap M)| = \prod_{j=1}^{n} |R_j : (H \cap R_j)|.$$

As the R_j are normal in M and $G = HM$, they are already H-conjugate: hence $|R_j : (H \cap R_j)|$ is independent of j, and $|\Omega| = |R_1 : (H \cap R_1)|^n$. On the other hand,

$$|P : (H \cap P)| = \prod_{j=2}^{n} |R_j : (H \cap R_j)| = |R_1 : (H \cap R_1)|^{n-1}.$$

The other point stabilizers in G are M-conjugates of H and M normalizes P: hence $|P : (H \cap P)|$ is the common length of the P-orbits on Ω. It follows that $|\Omega/P| = |R_1 : (H \cap R_1)|$, and hence also that $|\Omega| = |\Omega/P|^n$. Note in particular that P cannot be transitive on Ω.

For the explicit definition of φ, see the third paragraph of the last section of [3]. That definition makes use of a transversal of Q in G. In forming $Q \operatorname{Wr} S_n$, we used there the set of the right cosets of Q in G as the n-element set on which S_n acts and which indexes the coordinate subgroups (so the base group consists of the functions from the set of cosets to Q). Similarly one may think of $(\Omega/P)^n$ as the set of all functions from this set of cosets to the orbit set Ω/P. Define β by requiring that the image under β of an element ω of Ω be the function whose value at any coset is the P-orbit containing the image of ω under the inverse of the relevant coset representative. Since P is not transitive on Ω, the image of β is

not a singleton. It is straightforward to verify that β intertwines the action of G on Ω and the action of G via $\varphi\bar{\xi}$ on $(\Omega/P)^n$. Given this, the complete inverse images under β of the single elements of $(\Omega/P)^n$ form a system of imprimitivity for the primitive action of G on Ω. To avoid a contradiction, the system must be degenerate: as the image of β is not a singleton, the system has more than one block, so the only option is that each block is a singleton. This proves that β is one-to-one. We have seen that $|\Omega| = |\Omega/P|^n$, so β must then be bijective. This completes the proof of Theorem (3.3), and with it the justification of the definition of blow-up decomposition.

We close this section with an 'abstract' variant of (3.3). In this, φ is as before. Let ψ denote the obvious homomorphism of $Q \operatorname{Wr} S_n$ onto $(Q/Z) \operatorname{Wr} S_n$, and χ the obvious map of $(Q/Z) \operatorname{Wr} S_n$ onto $(Q/ZM) \operatorname{Wr} S_n$.

(3.4) THEOREM. *The socle of Q/Z is ZM/Z, and $(H \cap Q)P/Z$ is a corefree maximal subgroup of Q/Z which meets the socle ZM/Z non-trivially. The group $G\varphi\psi\chi$ is a large subgroup in $(Q/ZM) \operatorname{Wr} S_n$, and its complete inverse image under χ is $G\varphi\psi$. Moreover, $\varphi\psi$ is one-to-one, and $H\varphi\psi$ is conjugate in $G\varphi\psi$ to $G\varphi\psi \cap S_n[(H \cap Q)P/Z]^n$.*

This is obtained from (3.3) by identifying G_0 with Q/Z in the natural way (so $\bar{\xi}$ becomes ψ) and by including some extra detail from the preamble and the proof of (3.3).

4. *Blow-up decompositions: the overview*

At last we are ready to state the variant of the first sentence of Theorem 2 which we actually prove.

THEOREM 2^+. *Let G be a primitive group with non-regular socle M; let H be a point stabilizer in G and K a maximal normal subgroup of M. The set of all blow-up decompositions of G is bijective with the set of all proper subgroups of G containing $M\mathbb{N}_H(H \cap K)$. Namely, number the direct factors $R_1, \ldots, R_n$ of a blow-up decomposition of G so that $K \geqslant R_2 \times \ldots \times R_n$ and map this decomposition to $M\mathbb{N}_H(H \cap (R_2 \times \ldots \times R_n))$: the map so defined is such a bijection.*

REMARK. It should be clear what is meant by one decomposition being a refinement of another; with respect to that partial order on the first set, and partial order by inclusion on the second set, *the bijection described is an order-isomorphism.* In particular, if G has any blow-up decompositions at all, then among them there is a unique finest: namely that corresponding to $M\mathbb{N}_H(H \cap K)$. For the easiest example, let G be $A \operatorname{Wr} B$ in product action, with A a primitive non-abelian simple group and B a regular group (so that abstractly G is just a standard wreath product). Then $M\mathbb{N}_H(H \cap K)$ is the base group, so the poset of the blow-up decompositions of G is bijective with the poset of the proper subgroups C of B: form the product of the C-conjugates of the first coordinate subgroup; the G-conjugates of the subgroup so obtained are the direct factors in the blow-up decomposition corresponding to C.

The critical step in the proof will be the following.

(4.1) LEMMA. *Let P denote the intersection of those maximal normal subgroups $K_1, \ldots, K_k$ of M for which $H \cap K_i = H \cap K$; let $P_1, \ldots, P_l$ be the distinct conjugates of P in G; and set $R_j = \bigcap \{P_{j'} \mid j' \neq j\}$. If $l > 1$, then $\{R_1, \ldots, R_l\}$ is a blow-up decomposition of G. If M is minimal normal and $k > 1$, then K is transitive.*

We defer the proof of this for the time being, and start by showing how Theorem 2^+ can be deduced from it.

Suppose (4.1) is true, and $l > 1$. We may as well number the K_i so that $K_1 = K$, and the P_j so that $P_1 = P$: then $K_1 \geqslant P_1 = R_2 \times \ldots \times R_l$ and

$$H \cap K_1 = H \cap P_1 = (H \cap R_2) \times \ldots \times (H \cap R_l).$$

Let $\{A_1, \ldots, A_n\}$ be another blow-up decomposition of G. Each maximal normal subgroup of M, so in particular each of the K_i, contains all but one of the A_m; number the A_m so that $K_1 \geqslant A_2 \times \ldots \times A_n$: then

$$H \cap K_1 = H \cap M \cap K_1 = (H \cap A_1 \cap K_1) \times (H \cap A_2) \times \ldots \times (H \cap A_n).$$

Here $H \cap A_1 \cap K_1 < H \cap A_1$: else $H \cap P_1 = H \cap K_1 = H \cap M \trianglelefteq H$; on the other hand, $HM = G$ implies that the P_j are all H-conjugate, so

$$H \cap M = \bigcap (H \cap M)^h = \bigcap (H \cap P_1)^h = \bigcap (H \cap P_j) = 1,$$

contrary to the assumed non-regularity of M. Now $H \cap K_i = H \cap K$ implies that $H \cap A_1 \cap K_i < H \cap A_1$ but $H \cap A_m \cap K_i = H \cap A_m$ (whenever $i = 1, \ldots, k$ and $m = 2, \ldots, n$): thus for each K_i it is A_1 (and not one of the other A_m) which does not lie in K_i. It follows that $P_1 = \bigcap K_i \geqslant A_2 \times \ldots \times A_n$. Since R_1 centralizes P_1, it lies in the centralizer (in M) of $A_2 \times \ldots \times A_n$: this centralizer is A_1, so $R_1 \leqslant A_1$. Each R_j is a conjugate R_j^g of R_1 and so lies in some A_m (namely in A_1^g). Partition the set Σ of the R_j by putting R_j and $R_{j'}$ into the same part whenever they lie in the same A_m. This partition is obviously a system of imprimitivity for the (conjugation) action of G on Σ. Conversely, given any system of imprimitivity for this action of G on Σ, for each block form the product of the members of the block: the set of these product is easily seen to be a blow-up decomposition of G. The set of all systems of imprimitivity is of course bijective with the set of all the proper subgroups which properly contain a point stabilizer. Here a point stabilizer is $\mathbb{N}_G(R_1)$ which is also $\mathbb{N}_G(P)$. By Dedekind's Law $\mathbb{N}_G(P) = M\mathbb{N}_H(P)$. Obviously

$$\mathbb{N}_H(P) \leqslant \mathbb{N}_H(H \cap P) = \mathbb{N}_H(H \cap K);$$

conversely, if an element of H normalizes $H \cap K$, then by conjugation it permutes the subgroups $K_1, \ldots, K_k$ among themselves and so normalizes their intersection P: thus $\mathbb{N}_H(P) = \mathbb{N}_H(H \cap K)$. This proves Theorem 2^+ whenever $l > 1$.

When $P \trianglelefteq G$, one has to show that G has no blow-up decomposition. If $\{A_1, \ldots, A_n\}$ were a blow-up decomposition, $P_1 \geqslant A_2 \times \ldots \times A_n$ would follow as above, contrary to the conjugacy of A_1 and A_2.

The rest of this section will be devoted to the proof of Lemma (4.1).

Consider the easiest case first: suppose M is not minimal normal in G. Then G has precisely two minimal normal subgroups, M_1 and M_2 say, and H complements

both: $HM_1 = HM_2 = G$ and $H \cap M_1 = H \cap M_2 = 1$. Consequently, $(H \cap M)M_1 = (H \cap M)M_2 = M$ and $H \cap M \cong M_1 \cong M_2$, the latter being H-isomorphisms. Each maximal normal subgroup of M contains M_1 or M_2; say, $K_1 = K \geqslant M_1$: then $K_1 = (H \cap K)M_1$. Similarly each K_i with $H \cap K_i = H \cap K$ is of the form $(H \cap K)M_j$ for $j = 1$ or 2, so $K_2 = (H \cap K)M_2$ is the only possibility beyond K_1. The K_2 so defined is indeed normal in M, being normalized both by $H \cap M$ and by M_2: thus $k = 2$ and $P_1 = P = K_1 \cap K_2$. In particular, P does not contain either M_1 or M_2, so $\bigcap P_j = 1$: thus $M = R_1 \times \ldots \times R_l$. In any case, the R_j obviously form a conjugacy class of subgroups in G, so all we need to prove is that

$$H \cap M = (H \cap R_1) \times \ldots \times (H \cap R_l).$$

Note that $K_1 = M_1 \times (K_1 \cap M_2)$ and $K_2 = (K_2 \cap M_1) \times M_2$, so

$$P = (K_2 \cap M_1) \times (K_1 \cap M_2) = (P \cap M_1) \times (P \cap M_2).$$

Further, $H \cap P = H \cap K = H \cap K_i$, and so

$$H \cap P \leqslant P \leqslant K_i = (H \cap K)M_i = (H \cap P)M_i$$

gives that $P = (H \cap P)(P \cap M_i)$. Thus we have H-isomorphisms

$$H \cap P \cong P/(P \cap M_1) \cong P \cap M_2,$$
$$H \cap P \cong P/(P \cap M_2) \cong P \cap M_1.$$

Consequently, the centralizer $\mathbb{C}_H(H \cap P)$ acts trivially on all of P, whence

$$\mathbb{C}_{H \cap M}(H \cap P) \leqslant \mathbb{C}_M(P) = \mathbb{C}_M(P_1) = R_1$$

and therefore $\mathbb{C}_{H \cap M}(H \cap P) = H \cap R_1$ follow. On the other hand, $H \cap M$, being isomorphic to M_1, is a direct product of non-abelian simple groups; therefore $H \cap P$, like any normal subgroup of $H \cap M$, is a direct factor in $H \cap M$, with $\mathbb{C}_{H \cap M}(H \cap P)$ the direct complement: so

$$H \cap M = (H \cap P_1) \times (H \cap R_1).$$

Similarly $H \cap M = (H \cap P_j) \times (H \cap R_j)$ for all j, and hence

$$H \cap M = \bigcap [(H \cap P_j) \times (H \cap R_j)] = (H \cap R_1) \times \ldots \times (H \cap R_l).$$

This completes the proof of (4.1) for the case of M not being minimal normal.

Before moving on, the reader may wish to identify, for the present blow-up decomposition of such a G, the corresponding G_0 given by Theorem (3.3). To aid this, Fig. 2 shows on the left the sublattice generated in the subgroup lattice of G by H, M_1, M_2, K, Q, and Z. Note that, in this case, M_0 is the product of the simple minimal normal subgroups $M_1\zeta$ and $M_2\zeta$, so G_0 may be thought of as a subgroup of the holomorph of a non-abelian simple group (containing both groups of translations). Of course, G itself may be similarly thought of as a subgroup of the holomorph of M_2, containing both groups of translations.

The remaining task is to prove Lemma (4.1) under the additional assumption that M is minimal normal in G. In this case M is the direct product of the G-conjugates of the non-abelian simple group $\mathbb{C}_M(K)$. Each maximal normal subgroup of M is the product of all but one of these simple direct factors of M, so it is precisely the centralizer in M of that missing direct factor. It follows that the maximal normal subgroups of M are all conjugate in G. As $HM = G$, the maximal normal subgroups of M are therefore the H-conjugates of K; in

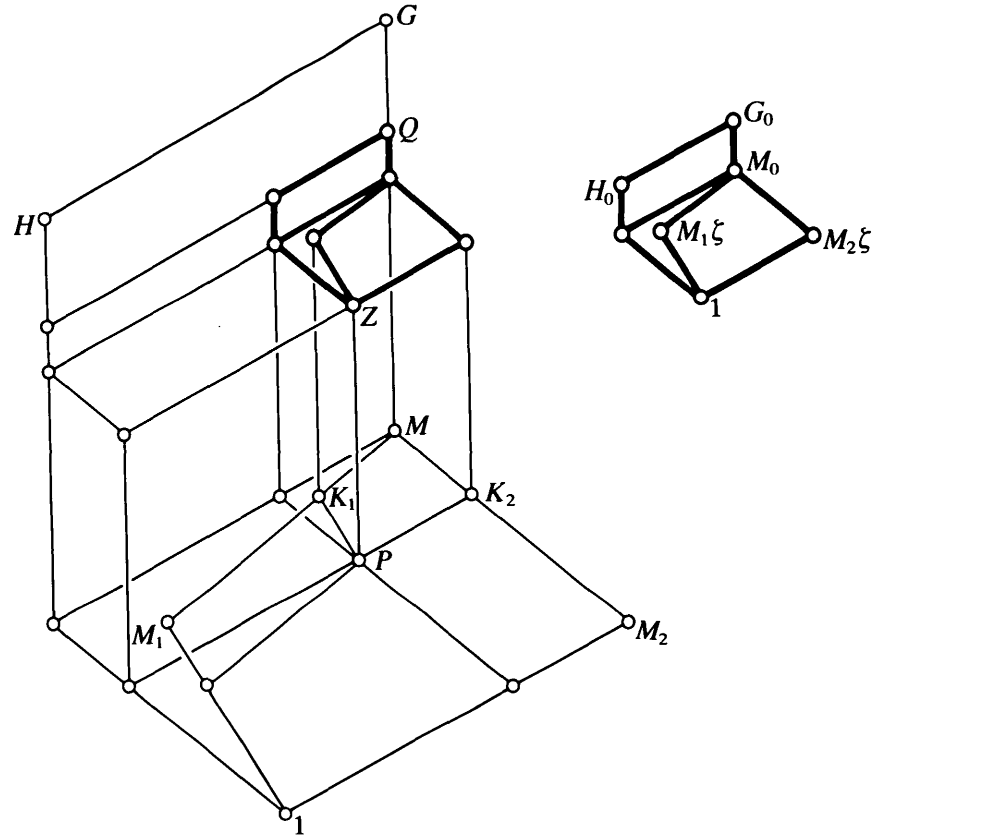

FIG. 2

particular, there are precisely $|H:\mathbb{N}_H(K)|$ of them. Moreover, $K_1, \ldots, K_k$, are then just the $\mathbb{N}_H(H \cap K)$-conjugates of K, and $k = |\mathbb{N}_H(H \cap K):\mathbb{N}_H(K)|$. Similarly, we may say that K is the direct product of the (distinct) conjugates of $\mathbb{C}_M(K)$ under the elements of H outside $\mathbb{N}_H(K)$; and, a little more generally, each conjugate of K is the direct product of the conjugates of $\mathbb{C}_M(K)$ under the elements of H outside some particular coset of H modulo $\mathbb{N}_H(K)$. Here the cosets relevant to forming $K_1, \ldots, K_k$ are those which lie in $\mathbb{N}_H(H \cap K)$; so one may conclude that P is the direct product of the conjugates of $\mathbb{C}_M(K)$ under the elements of H outside $\mathbb{N}_H(H \cap K)$. Further, each conjugate of P is then the direct product of the conjugates of $\mathbb{C}_M(K)$ under the elements of H outside some coset of H modulo $\mathbb{N}_H(H \cap K)$. In particular, $\mathbb{N}_H(P) = \mathbb{N}_H(H \cap K)$ and $l = |H:\mathbb{N}_H(H \cap K)|$. Moreover, the intersection of all but one of the conjugates of P is the direct product of the conjugates of $\mathbb{C}_M(K)$ under one particular coset of H modulo $\mathbb{N}_H(H \cap K)$. This proves that $\{R_1, \ldots, R_l\}$ is a direct decomposition of M. The only role of the assumption $l > 1$ is to ensure that this decomposition has more than one factor. Note for repeated use that K has precisely kl conjugates and $|M| = |M/K|^{kl}$.

The first statement of Lemma (4.1) will be proved by showing that this direct decomposition of M satisfies the conditions in (3.1). The first of these conditions holds obviously, as $HM = G$ and M normalizes the R_j while conjugation action by H permutes them transitively (just as translation action permutes the cosets of H

modulo $\mathbb{N}_H(H \cap K)$). The second condition requires that $H \cap M = \prod (H \cap R_j)$. This is equivalent to $H \cap M = \bigcap [(H \cap M)P_j]$. As H is maximal in G, so $H \cap M$ is maximal among the H-admissible subgroups of M: thus the only alternative is that the right-hand side of the last equation is M. We shall rule out this alternative by showing that it leads to a contradiction.

Suppose then that $\bigcap [(H \cap M)P_j] = M$: equivalently, that $(H \cap M)P = M$. Then also $(H \cap M)K = M$, so

$$|M| = |(H \cap M) : (H \cap P)|\,|P| = |(H \cap M) : (H \cap K)|\,|K|;$$

as $H \cap P = H \cap K$, this implies that $|P| = |K|$, $P = K$, $k = 1$. The $H \cap P_j$ are l pairwise distinct normal subgroups of $H \cap M$ with all quotients $(H \cap M)/(H \cap P_j)$ isomorphic. Now these quotients are isomorphic to the non-abelian simple group M/K, because

$$(H \cap M)/(H \cap P) \cong (H \cap M)P/P = M/P = M/K.$$

It follows that $|H \cap M| \geqslant |M/K|^l = |M/K|^{kl} = |M|$: but then $H \geqslant M$, and we have the desired contradiction. This completes the proof of the first statement of (4.1).

Finally, suppose that K is intransitive: that is, $HK \neq G \neq KH$. The second statement of (4.1) will be proved by showing that, under this assumption, $k = 1$. As $HM = G$, the assumption is equivalent to $(H \cap M)K \neq M$. Let K_i range through the kl distinct conjugates of K; then $\bigcap [(H \cap M)K_i]$ is an H-admissible proper subgroup of M containing $H \cap M$, so $\bigcap [(H \cap M)K_i] = H \cap M$. Choose a right transversal $\{h_1, \ldots, h_{kl}\}$ for $\mathbb{N}_H(K)$ in H so that $K_i = h_i^{-1}Kh_i$ for $i = 1, \ldots, kl$. To each element x of M consider the function $\bar{x}$: $\{1, \ldots, kl\} \to M/K$ whose value at i is the coset $h_ixh_i^{-1}K$. It is straightforward to see that $x \mapsto \bar{x}$ is an isomorphism of M onto the direct power $(M/K)^{kl}$ and that it maps $H \cap M$ into $[(H \cap M)K/K]^{kl}$. In fact it maps $H \cap M$ onto $[(H \cap M)K/K]^{kl}$, because the image of the latter under the inverse of this isomorphism is $\bigcap [(H \cap M)K_i]$ and we have already seen that this intersection is $H \cap M$. The conclusion we want to retain is that $|H \cap M| = |(H \cap M)K/K|^{kl}$. Of course

$$(H \cap M)K/K \cong (H \cap M)/(H \cap K) = (H \cap M)/(H \cap P) \cong H \cap R_1;$$

for we have already established that $H \cap M = \prod (H \cap R_j)$, and so the conclusion is equivalent to $|H \cap M| = |H \cap R_1|^{kl}$. On the other hand, the $H \cap R_j$ are all conjugate, so $|H \cap R_j|$ is independent of j and therefore $|H \cap M| = |H \cap R_1|^l$. As $|H \cap M| \neq 1$, the last two equations imply that $k = 1$. This completes the proof of (4.1).

The reader may now wish to identify the G_0 given by Theorem (3.3) for the blow-up decomposition given by this case (the case of $l > 1$ and minimal normal M) of (4.1). To aid this, Fig. 3 shows on the left the sublattice generated in the subgroup lattice of G by H, K, M, $\mathbb{N}_G(K)$, P, Q, and Z when $k > 1$ and $l > 1$. On the right of Fig. 3 we have set $K_0 = K\zeta$. Note that in this case M_0 is not simple, K_0 is a maximal normal subgroup of M_0, and K_0 is regular (because it complements the point stabilizer H_0): thus G_0 is of simple diagonal type. One may say that G itself is now of *compound diagonal type.*

When $k = 1$ but $l > 1$ we have $K = P$ and $\mathbb{N}_G(K) = Q$, so the relevant lattice is just that shown in Fig. 1. In that case M_0 is simple, so G_0 is almost simple.

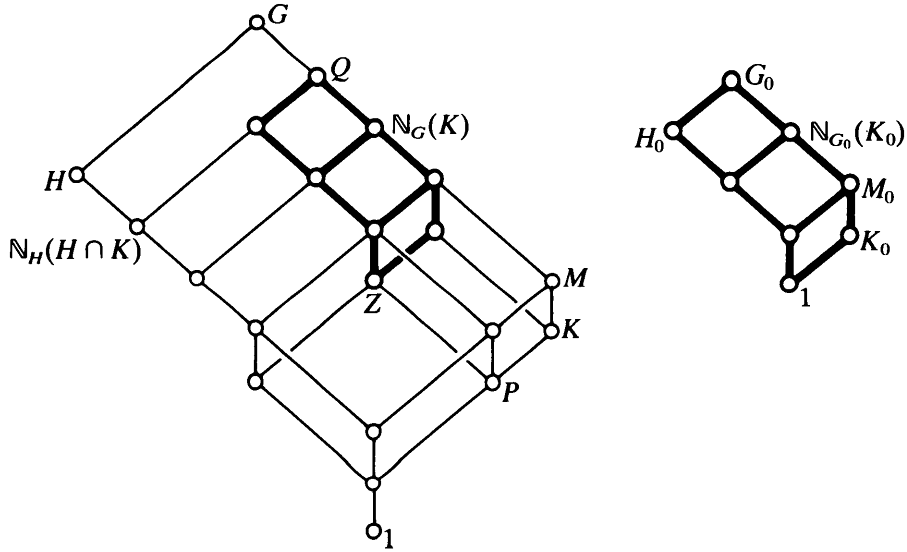

FIG. 3

5. *Isomorphism of blow-ups*

The interpretation and proof of the uniqueness claims of Theorem 2 are still outstanding. These can be dealt with as follows.

THEOREM 2^{++}. *Let G be a primitive group that is not a blow-up, M the socle of G, and B a large subgroup in a $(G/M)\,\mathrm{Wr}\, S_n$ with $n > 1$, and suppose that M is not regular. Choose G_1, M_1, B_1, n_1 similarly. The blow-ups $G \uparrow B$ and $G_1 \uparrow B_1$ are permutationally isomorphic if and only if $n = n_1$ and there is a permutational isomorphism of G onto G_1 such that the corresponding isomorphism of $(G/M)\,\mathrm{Wr}\, S_n$ onto $(G_1/M_1)\,\mathrm{Wr}\, S_n$ maps B to a conjugate of B_1.*

As always, a permutational isomorphism of two permutation groups is an isomorphism induced by a bijection of the sets on which the groups act. It will be convenient to make no reference to the permuted sets in this section, but to rely instead on the fact that an abstract isomorphism of two transitive groups is permutational if and only if it matches the conjugacy class of the point stabilizers in one group to the conjugacy class of the point stabilizers in the other. The 'if' part of Theorem 2^{++} is obvious. The proof of the 'only if' part will occupy the rest of this section, after we clear up one point.

REMARK. Theorem 2^{++} does not mean that if B and B_1 are non-conjugate large subgroups in $(G/M)\,\mathrm{Wr}\, S_n$ then $G \uparrow B$ and $G \uparrow B_1$ cannot be permutationally isomorphic: for G could still have a permutational automorphism such that the corresponding automorphism of $(G/M)\,\mathrm{Wr}\, S_n$ maps B to (a conjugate of) B_1. The following example shows that this can actually happen. Let T be a non-abelian simple group and $G/(\mathrm{Inn}\, T)$ a normal subgroup of $\mathrm{Out}\, T$: then the socle M of G is $\mathrm{Inn}\, T$. Further, let X/M be a normal subgroup of G/M which is not normal in $\mathrm{Out}\, T$, and Y a maximal subgroup of $\mathrm{Aut}\, T$ such that $GY = \mathrm{Aut}\, T$ and $G \cap Y$ is maximal in G. According to the Atlas [2] one could, for instance, take $T = O_8^+(3)$ so $\mathrm{Out}\, T \cong S_4$ and then take G/M of order 4, X/M of order 2, and Y of index

36400. Then X has an (Aut T)-conjugate X_1 which is not conjugate to X in G. Consider Aut T a permutation group with respect to its natural action on the set of its cosets modulo Y. Then G is a primitive subgroup of Aut T and G has a permutational automorphism which maps X to X_1. Define D as the set $(X/M)^n \operatorname{diag}(G/M)^n$ of all functions

$$f = \{1, \ldots, n\} \to G/M$$

such that $f(i) \equiv f(j) \bmod X/M$ for all i, j, and D_1 as $(X_1/M)^n \operatorname{diag}(G/M)^n$; put $B = S_n D$ and $B_1 = S_n D_1$. Then B and B_1 are non-conjugate large subgroups of $(G/M) \operatorname{Wr} S_n$, yet $G \uparrow B$ and $G \uparrow B_1$ are permutationally isomorphic.

We are now ready to proceed with the proof of the 'only if' part of Theorem 2^{++}. The first steps amount to some further analysis of $G \uparrow B$. Let H be a point stabilizer in G, and K a maximal normal subgroup of M. By assumption, $H \cap M > 1$. Since G is not a blow-up, it follows easily from (4.1) that $H \cap K = 1$. Write $W = G \operatorname{Wr} S_n$, let S_{n-1} be a point stabilizer in S_n,

$$W_o = S_{n-1}G^n = G \times S_{n-1}G^{n-1} > M^n = M \times M^{n-1} \tag{5.1}$$

the corresponding direct decompositions, and π_o: $W_o \to G$ the projection of W_o onto its first direct factor. Now $M^n < G \uparrow B \leqslant W$ by definition, and $\operatorname{soc}(G \uparrow B) = \operatorname{soc} W = M^n$ by (2.1). Of course, $K \times M^{n-1}$ is a maximal normal subgroup of M^n. Further, $(G \uparrow B) \cap S_n H^n$ is a point stabilizer in $G \uparrow B$; its intersection with $K \times M^{n-1}$ is $(H \cap M)^{n-1}$: the same as its intersection with M^{n-1}. Therefore, by Theorem 2^+, the blow-up decomposition which $G \uparrow B$ has by construction (and in which M^{n-1} plays the role of $R_2 \times \ldots \times R_n$) is the unique finest blow-up decomposition of $G \uparrow B$.

The point stabilizer $(G \uparrow B) \cap S_n H^n$ will need a name: call it simply $H\Uparrow$. Write P for the last direct factor M^{n-1} in (5.1); put

$$Q = (G \uparrow B) \cap W_o = (G \uparrow B) \cap S_{n-1}G^n,$$
$$Z = (G \uparrow B) \cap \ker \pi_o = (G \uparrow B) \cap S_{n-1}G^{n-1},$$

and let ζ: $Q \to G$ be the relevant restriction of π_o. Then $\ker \zeta = Z$ and, as B is large, $Q\zeta = G$; write ζ^*: $Q/Z \to G$ for the corresponding isomorphism. Note that $Q = \mathbb{N}_{G \uparrow B}(P)$ and $Z = \mathbb{C}_Q(M^n/P) \geqslant P$, while $(H\Uparrow \cap Q)\zeta = H$ by (2.5).

Similar claims hold for G_1, M_1, B_1, n_1 and the $H_1\Uparrow$, P_1, Q_1, Z_1, ζ_1, ζ_1^* defined by analogy. Suppose that $G \uparrow B$ and $G_1 \uparrow B_1$ are permutationally isomorphic. A permutational isomorphism of two primitive groups (with non-regular socles) must match their unique finest blow-up decompositions: thus we must have $n = n_1$ and indeed can choose a permutational isomorphism γ: $(G \uparrow B) \to (G_1 \uparrow B_1)$ so that $P\gamma = P_1$. Of course then $Q\gamma = Q_1$ and $Z\gamma = Z_1$ follow, but without further argument we can only say that $(H\Uparrow)\gamma$ is conjugate in $G_1 \uparrow B_1$ to $H_1\Uparrow$. Let γ^* denote the isomorphism $Q/Z \to Q_1/Z_1$ induced by γ; the inverse of ζ^* followed by $\gamma^* \zeta_1^*$ is then an isomorphism, call it δ, of G onto G_1.

By Theorem 3.01 of [7], the conjugacy of $(H\Uparrow)\gamma$ to $H_1\Uparrow$ in $G_1 \uparrow B_1$ implies that $[(H\Uparrow)\gamma \cap Q_1]P_1$ is conjugate to $(H_1\Uparrow \cap Q_1)P_1$ in Q_1; consequently, $[(H\Uparrow)\gamma \cap Q_1]Z_1$ is conjugate to $(H_1\Uparrow \cap Q_1)Z_1$ in Q_1. Of course $[(H\Uparrow)\gamma \cap Q_1]Z_1 = [(H\Uparrow \cap Q)Z]\gamma$, so we may conclude that $[(H\Uparrow \cap Q)Z/Z]\gamma^*$ is conjugate to $(H_1\Uparrow \cap Q_1)Z_1/Z_1$ in Q_1/Z_1. As $[(H\Uparrow \cap Q)Z/Z]\zeta^* = H$ and $[(H_1\Uparrow \cap Q_1)Z_1/Z_1]\zeta_1^* = H_1$, this means that $H\delta$ is conjugate to H_1 in G_1. Thus δ is a permutational isomorphism.

We now identify G with G_1 along δ: then H and H_1 become conjugate subgroups of G. Moreover, B and B_1 become subgroups of the same wreath product $(G/M) \operatorname{Wr} S_n$; a wreath product we shall think of as W/M^n. Thus $G \uparrow B$ and $G \uparrow B_1$ are subgroups of W, both containing M^n, with $(G \uparrow B)/M^n = B$ and $(G \uparrow B_1)/M^n = B_1$. We shall prove the 'only if' part of Theorem 2^{++} by showing that, after these identifications, $G \uparrow B$ and $G \uparrow B_1$ are conjugate in W.

To this end we shall use the Uniqueness Theorem of [6] (or its paraphrase in [8]) for comparing the inclusion, say ψ, of $G \uparrow B$ in W with the composite $\gamma\psi_1$ where ψ_1 is the inclusion of $G \uparrow B_1$. First use the projection π: $W \to S_n$. From $Q\gamma = Q_1$ we see that Q is the stabilizer, in $G \uparrow B$, of the point whose stabilizer in S_n we took as S_{n-1}, with respect to both permutation representations $\psi\pi$ and $\gamma\psi_1\pi$. Since B and B_1 are large, both permutation representations are transitive. It follows that the two permutation representations are equivalent: indeed, that there is a t in S_{n-1} such that $\psi\pi(\operatorname{inn} t) = \gamma\psi_1\pi$ where $\operatorname{inn} t$ denotes the inner automorphism of S_n induced by t. Since $S_n \leqslant W$, this t also induces an inner automorphism of W; in terms of that, we have $\psi(\operatorname{inn} t)\pi = \gamma\psi_1\pi$. Consider an arbitrary element x in Q. As $t \in \ker \pi_o$,

$$x\psi(\operatorname{inn} t)\pi_o = x\psi\pi_o = x\zeta = (xZ)\zeta^*;$$

on the other hand,

$$x\gamma\psi_1\pi_o = x\gamma\zeta_1 = [(x\gamma)Z_1]\zeta_1^* = (xZ)\gamma^*\zeta_1^*.$$

By the definition of δ we have $\zeta^*\delta = \gamma^*\zeta_1^*$; but we have identified G with G_1 along δ, so the last two displayed lines show that $x\psi(\operatorname{inn} t)\pi_o = x\gamma\psi_1\pi_o$ for all x in Q. The Uniqueness Theorem now gives that there is an element f in G^{n-1} such that $\psi(\operatorname{inn} t)(\operatorname{inn} f) = \gamma\psi_1$. Consequently $G \uparrow B_1$ is the conjugate of $G \uparrow B$ by the element tf of W. This completes the proof of Theorem 2^{++}.

Acknowledgement

The author is indebted to Professor Cheryl E. Praeger and Dr Jan Saxl for many stimulating discussions on this subject.

References

1. P. J. CAMERON, 'Finite permutation groups and finite simple groups', *Bull. London. Math. Soc.* 13 (1981) 1–22.
2. J. H. CONWAY, R. T. CURTIS, S. P. NORTON, R. A. PARKER, and R. A. WILSON, *Atlas of finite groups* (Clarendon Press, Oxford, 1985).
3. J. COSSEY, O. H. KEGEL, and L. G. KOVÁCS, 'Maximal Frattini extensions', *Arch. Math.* 35 (1980) 210–217.
4. P. FÖRSTER and L. G. KOVÁCS, 'On primitive groups with a single nonabelian regular normal subgroup', preprint, Australian National University, 1989.
5. G. JAMES and A. KERBER, *The representation theory of the symmetric group* (Addison-Wesley, Reading, 1981).
6. L. G. KOVÁCS, 'Two results on wreath products', *Arch. Math.* 45 (1985) 111–115.
7. L. G. KOVÁCS, 'Maximal subgroups in composite finite groups', *J. Algebra* 99 (1985) 114–131.
8. L. G. KOVÁCS, 'Some theorems on wreath products', *Publ. Math. Debrecen* 35 (1988) 155–160.
9. L. G. KOVÁCS, 'Primitive permutation groups of simple diagonal type', *Israel J. Math.* 63 (1988) 119–127.

10. L. G. KOVÁCS, 'Twisted wreath products as primitive permutation groups', preprint, Australian National University, 1989.

11. J. LAFUENTE, 'Grupos primitivos con subgrupos maximales penqueños', *Publ. Sec. Mat. Univ. Auton. Barcelona* 29 (1985) 154–161.

12. M. W. LIEBECK, C. E. PRAEGER, and J. SAXL, 'On the O'Nan–Scott Theorem for finite primitive permutation groups', *J. Austral. Math. Soc. Ser. A* 44 (1988) 389–396.

13. C. E. PRAEGER, J. SAXL, and K. YOKOYAMA, 'Distance transitive graphs and finite simple groups', *Proc. London Math. Soc.* (3) 55 (1987) 1–21.

Department of Mathematics
Australian National University
GPO Box 4
Canberra
ACT 2601
Australia

A direct proof of Lemma 2.2 in

Proc. London Math. Soc. (3) 58 (1989), 306–322

I write permutations on the left and homomorphisms on the right; accordingly, I compose them differently. Where convenient, I also use function notation.

Let G be any finite group, n any integer greater than 1, G^n the set of all functions $\phi\colon \{1,\dots,n\} \to G,\ i \mapsto \phi(i)$, and let the symmetric group S_n (on $\{1,\dots,n\}$) act on G^n by $\phi^\alpha(i) = \phi(\alpha i)$. Think of the wreath product $W = G \operatorname{Wr} S_n$ as the semidirect product $S_n \ltimes G^n$ formed with respect to this action. Write the elements of W as ordered pairs (α, ϕ). The map $\pi\colon W \to S_n,\ (\alpha,\phi) \mapsto \alpha$ may be thought of as a permutation representation of W on $\{1,\dots,n\}$. Let W_1 denote the stabilizer in W of the symbol 1 with respect to this permutation representation: then $W_1 = \{\,(\alpha,\phi) \in W \mid \alpha 1 = 1\,\}$, and $\pi_1\colon W_1 \to G,\ (\alpha,\phi) \mapsto \phi(1)$ is a homomorphism.

In these terms, Lemma 2.2 stated that *if $X \le W$ and $X\pi$ is transitive, then there is an element w in $G^n \cap \ker \pi_1$ such that the conjugate X^w of X lies in $(X \cap W_1)\pi_1 \operatorname{Wr} S_n$.* To be quite pedantic, this means that there is an function η in G^n such that $\eta(1) = 1$ and the conclusion holds for $w = (1, \eta)$. In that conclusion, $(X \cap W_1)\pi_1 \operatorname{Wr} S_n$ is the set of the elements (α,ϕ) of W such that all values of ϕ lie in the subgroup $(X \cap W_1)\pi_1$ of G. [In the paper, the symmetric group S_n acted on a set Ω and o stood for an arbitrarily chosen element of that Ω; with the present choice of Ω, it seems natural to choose o as 1.]

For a direct proof of this lemma, one may exhibit such an η as follows.

Choose representatives (α_i, ϕ_i) for the left cosets of X modulo $X \cap W_1$, indexing them so that $\alpha_i i = 1$ (this is where we use the assumption that $X\pi$ is transitive), and ensuring that the trivial coset is represented by the trivial element. Define η by setting

$$\eta(i) = (\phi_i(i))^{-1} \qquad \text{for } i = 1,\dots,n:$$

we shall see that this works. The easy point certainly does: since we chose the trivial element to represent the trivial coset, we do have $\eta(1) = 1$.

Calculate that $(\alpha,\phi)^{(1,\eta)} = (\alpha, (\eta^\alpha)^{-1}\phi\eta)$, so what we expect of η is that every value of $(\eta^\alpha)^{-1}\phi\eta$ should lie in $(X \cap W_1)\pi_1$. Explicitly, to each (α,ϕ) in X and i in $\{1,\dots,n\}$, there should exist a (β_i,ψ_i) in X such that $\beta_i 1 = 1$ and $(\eta(\alpha i))^{-1}\phi(i)\eta(i) = \psi_i(1)$. Direct calculation will show that this does hold if we choose

$$(\beta_i,\psi_i) = (\alpha_{\alpha i}, \phi_{\alpha i})(\alpha,\phi)(\alpha_i,\phi_i)^{-1}.$$

The choice is legitimate, because this is a product of three elements of X, so it does lie in X. It yields $\beta_i = \alpha_{\alpha i}\alpha\alpha_i^{-1}$, which does map the symbol 1 to itself as required (remember that permutations are written on the left and composed accordingly: since α_i maps i to 1, its inverse maps 1 to i, then α maps i to αi, and in turn $\alpha_{\alpha i}$ maps that back to 1). Thus $(\beta_i,\psi_i) \in X \cap W_1$. It remains to calculate that $\psi_i = \phi_{\alpha i}^{\alpha\alpha_i^{-1}} \phi^{\alpha_i^{-1}} (\phi_i^{\alpha_i^{-1}})^{-1}$ and evaluate at 1:

$$\psi_i(1) = \phi_{\alpha i}(\alpha\alpha_i^{-1}1)\phi(\alpha_i^{-1}1)(\phi_i(\alpha_i^{-1}1))^{-1} = \phi_{\alpha i}(\alpha i)\phi(i)(\phi_i(i))^{-1}$$

while $((\eta^\alpha)^{-1}\phi\eta)(i) = (\eta(\alpha i))^{-1}\phi(i)\eta(i) = \phi_{\alpha i}(\alpha i)\phi(i)(\phi_i(i))^{-1}$ by the definition we have chosen for η. Since the two right hand sides are equal, the proof is complete.

October 1997 LGK