Aequationes Math. 70 (2005) 225–239
0001-9054/05/030225-15
DOI 10.1007/s00010-005-2799-1

Aequationes Mathematicae

On the reconstruction index of permutation groups: general bounds

Philip Maynard and Johannes Siemons

Summary. We obtain a general bound for the reconstruction index of a permutation group. As a consequence bounds for the index of primitive and linear permutation groups can be obtained. In addition we give expressions for the reconstruction index of imprimitive wreath products in terms of the index of the constituent factors.

Mathematics Subject Classification (2000). 05C60, 05C65; 20B05.

Keywords. Reconstruction index, permutation actions.

1. Introduction

The reconstruction index belongs to the less well-known invariants of permutation groups. For its definition see the end of this section, more background can be found in our paper [7]. The relationship to other permutational properties is not very well understood, and in some way we are still at the stage of 'collecting specimens'. Other than for the groups considered in [7] the index is not known for any general class of permutation groups. In addition, only few computational results are available as computations beyond degree 30 or so are not feasible.

This paper therefore concentrates on upper and lower bounds for the reconstruction index. A useful general result is Theorem 2.6 which is a consequence of the Nash-Williams Lemma (see [10]). In [7] this was used to determine the index precisely for all semi-regular group actions. Here we use Theorem 2.6 to obtain an upper bound for the reconstruction index for a permutation group in which the pointwise stabilizer of suitably many k-element subsets is trivial, for a fixed value of k. Such groups may be finite or infinite. They include for instance Frobenius groups (when $k = 2$) or subgroups of linear groups (when k typically is the dimension of the underlying space). These results are contained in Section 3. One of our results implies for instance that the reconstruction index ρ of the full linear groups in dimension d satisfies $d \leq \rho \leq d(1 + \log_2 d)$ for large d. It is remarkable that

We acknowledge support from the Leverhulme Foundation for a project on the Reconstruction Index of Permutation Groups.

such relatively strong upper bounds for the reconstruction index can indeed be obtained by no more than the systematic application of Nash-Williams' idea. The theorem can also be used to bound the index for primitive permutations groups, particularly if the classification of finite simple groups is applied.

In the second part we are interested in imprimitive actions. In general the reconstruction index lies between 2 and about half of the degree. The imprimitive wreath products are remarkable by the fact that they are among the actions which realize both extremes. Theorem 5.1 gives a construction of permutation actions which attain the upper bound. The other results in Section 5 provide bounds for the index for the imprimitive wreath product action in terms of the indices of the constituents.

Notation. This paper is a continuation of [7] but should be self-contained. The following is a resumé of the main definitions and our notation.

Let (G, Ω) be an action. For $\omega \in \Omega$ the image under $g \in G$ is denoted $g(\omega)$ or $\omega^g \in \Omega$. If $\Delta \subseteq \Omega$ then $\Delta^g := \{\delta^g : \delta \in \Delta\}$ and $\Delta^G := \{\Delta^g : g \in G\}$. The stabilizer in G of ω is G_ω; if $\Delta \subseteq \Omega$ then $G_{\{\Delta\}}$ is the setwise stabilizer and G_Δ is the pointwise stabilizer of Δ. The symmetric and alternating groups on n letters, or on the set Ω, are denoted as Sym_n, Sym_Ω, Alt_n and Alt_Ω respectively. We write Ω_n to say that Ω is a set of n elements.

Let (G, Ω) be an action and let Δ, Δ' be two finite subsets of Ω. Then Δ, Δ' are *isomorphic*, denoted $\Delta \approx \Delta'$, if $\Delta' = \Delta^g$ for some $g \in G$. We say that Δ and Δ' are *hypomorphic*, denoted $\Delta \sim \Delta'$, if there exists a bijection $h : \Delta \to \Delta'$ for which $\Delta \setminus \{\delta\} \approx \Delta' \setminus \{h(\delta)\}$ for all $\delta \in \Delta$. Further, Δ is *reconstructible* if any set hypomorphic to Δ is isomorphic to Δ. The *reconstruction index* $\rho(G, \Omega)$ is the least integer r so that every set of r or more elements is reconstructible. If no such integer exists we put $\rho(G, \Omega) = \infty$. These definitions do of course depend on G: it will be clear throughout from the context what this group is in each case.

2. Bounds for the reconstruction index

In this section we shall derive general bounds for the reconstruction index of a permutation group. Our starting point is the Nash-Williams Lemma (see [10], [1]).

Lemma 2.1. *Let G act on a set Ω of arbitrary cardinality. Suppose that $\Delta \subset \Omega$ is not reconstructible and that for some $S \subseteq \Delta$ the setwise stabilizer G_S is finite. Then for every set K with $S \subseteq K \subseteq \Delta$ and $|K| \equiv |\Delta| \pmod 2$ there is some $g \in G$ with $\Delta \cap \Delta^g = K$.*

Analysing this result carefully gives the following inequalities:

Lemma 2.2. *Let (G, Ω) be a permutation group with Ω arbitrary. Suppose that $\Delta \subseteq \Omega$ is not reconstructible and let $S \subseteq \Delta$. If $n_G(S, \Delta) := |\{S^g : g \in G \text{ and } S^g \subseteq \Delta\}|$ then*

$$2^{|\Delta|-|S|-1} \cdot |G_{\{\Delta\}}| \leq n_G(S, \Delta) \cdot |G_{\{S\}}| = n_G(S, \Delta) \cdot |G^S| \cdot |G_S|$$

where $G^S := G_{\{S\}}/G_S$ is the group induced on S. In particular,

$$2^{|\Delta|-|S|-1} \cdot |G_{\{\Delta\}}| \leq \binom{|\Delta|}{|S|} \cdot |S|! \cdot |G_S|.$$

Proof. If $G_{\{S\}}$ is infinite then the inequalities hold. So suppose that $G_{\{S\}}$ is finite and let $S \subseteq X \subseteq \Delta$ be such that $\Delta \setminus X$ is of even size. By Lemma 2.1 there exists some $g \in G$ such that $\Delta \cap \Delta^g = X$. But then each $g' \in G_{\{\Delta\}}g$ has the same property. (In principle there could be more than one such coset.) There are $2^{|\Delta|-|S|-1}$ choices for X and therefore we have a set M of at least $2^{|\Delta|-|S|-1} \cdot |G_{\{\Delta\}}|$ distinct elements g for which $\Delta \cap \Delta^g$ contains S. For each such g then $S^h \subseteq \Delta$, with $h = g^{-1}$. The set M^* of elements h with $S^h \subseteq \Delta$ is a union of cosets of the shape $G_{\{S\}}h$, one for each distinct G-image of S contained in Δ. Thus $|M^*| = n_G(\Delta, S) \cdot |G_{\{S\}}|$. The result follows as $|M| \leq |M^*|$. □

Definition 2.3. For the positive integer s let $\beta(s)$ be the least integer $b > s$ for which $2^{b-s-1} > \binom{b}{s} \cdot s!$.

We list the first few values of this function: $\beta(1) = 5$, $\beta(2) = 10$, $\beta(3) = 16$, $\beta(4) = 23$, etc. More generally we have:

Lemma 2.4. (i) *For all s we have $2s < \beta(s) < \beta(s+1)$.*
(ii) *If $b \geq \beta(s)$, then $2^{b-s-1} > \binom{b}{s} \cdot s!$.*
(iii) *For all $s > 3$ we have $\beta(s) \leq 2s(1 + \log_2 s)$.*

Proof. (i) If $2^{b-s-1} > \binom{b}{s}s!$ but $2^{b-1-s-1} \leq \binom{b-1}{s}s!$ then $2\binom{b-1}{s} > \binom{b}{s}$ and hence $b > 2s$. The second inequality follows similarly. (ii) This follows by induction: Suppose that $2^{b-s-1} > \binom{b}{s}s!$ but $2^{b+1-s-1} \leq \binom{b+1}{s}s!$. Then $\binom{b+1}{s} > 2\binom{b}{s}$ and so $2s > b+1$ which contradicts (i). The statement (iii) can be checked for $4 \leq s \leq 8$. So let $s \geq 9$ and let $b = 2s(1+\log_2 s)$. It is sufficient to show that $b-s-1 > s \log_2 b$ (since $\binom{b}{s}s! < b^s$.) Now, $b - s - 1 = 2s \log_2 s + s - 1 = s \log_2 s^2 + s - 1 > s \log_2 b$ since for $s \geq 9$ we have $b < s^2$. □

Proposition 2.5. *Asymptotically $\beta(s) \sim s(1 + \log_2 s)$ as $s \to \infty$.*

Proof. First we show that for every $\epsilon > 0$ there is an s_ϵ for which $\beta(s) \leq (1 + \epsilon) \cdot s \cdot (1+\log_2 s)$ for all $s > s_\epsilon$. For this let $b = (1+\epsilon)s(1+\log_2 s)$. As in Lemma 2.4 (iii) it is sufficient to show that $b-s-1 > s \log_2 b$. Now, $b-s-1 = (1+\epsilon)s \log_2 s + \epsilon s - 1 = s \log_2 s^{1+\epsilon} + \epsilon s - 1$. For all large enough s we have $s^{1+\epsilon} > (1 + \epsilon)s(1 + \log_2 s) = b$ and hence $b - s - 1 > s \log_2 b$, as required.

Next we show that for every $\frac{1}{2} > \epsilon > 0$ there is an s_ϵ such that $(1-\epsilon)\cdot s\cdot(1+\log_2 s) < \beta(s)$ whenever $s > s_\epsilon$. For this put $b = (1-\epsilon)\cdot s\cdot(1+\log_2 s)$ for $s > 2$. We have to show that $2^{b-s-1} \le \binom{b}{s} s!$ for all sufficiently large s. As $(b-s+1)^s < \binom{b}{s} s!$ it is sufficient to show that $2^{b-s-1} < (b-s+1)^s = 2^{s\log_2(b-s+1)}$, or that $b-s-1 = s\log_2 s^{1-\epsilon} - \epsilon s - 1 < s\log_2(b-s+1)$ for all $s > s_\epsilon$. For the latter it is sufficient that $\log_2 s^{1-\epsilon} < \log_2[(1-\epsilon)s(1+\log_2 s)-s] = \log_2[(1-\epsilon)s\log_2 s - \epsilon s]$, or that $s^{1-\epsilon} < (1-\epsilon)s\log_2 s - \epsilon s$. Simplifying further we obtain $s^{-\epsilon} < (1-\epsilon)\log_2 s - \epsilon$ which holds whenever $s^{-\epsilon} < (1-2\epsilon)\log_2 s$. This latter inequality holds for all sufficiently large s. □

We are now able to formulate a simple general criterion for the reconstructibility of sets:

Theorem 2.6. *Let (G, Ω) be a permutation group with Ω of arbitrary cardinality. Let $\Delta \subseteq \Omega$ and suppose that there is some $S \subseteq \Delta$ with $\beta(|S|) \le |\Delta|$ such that $|G_S| < \infty$ and $|G_S| \le |G_{\{\Delta\}}|$. Then Δ is reconstructible.*

Proof. By definition and Lemma 2.4 (ii) we have $2^{|\Delta|-|S|-1} > \binom{|\Delta|}{|S|}\cdot|S|!$. Hence $2^{|\Delta|-|S|-1}|G_{\{\Delta\}}| > \binom{|\Delta|}{|S|}\cdot|S|!\cdot|G_{\{S\}}|$ so that Δ is reconstructible by Lemma 2.2. □

Note. It would be extremely useful to dispose of the condition $|G_S| < \infty$ in the theorem. So far we have made no progress on this question, nor do we have any idea about what else the condition could be substituted by.

For an arbitrary action (G, Ω) a subset $B \subseteq \Omega$ is a *base* if its pointwise stabilizer is trivial, $G_B = 1$. Hence

Corollary 2.7. *Let (G, Ω) be a permutation group with Ω of arbitrary cardinality and let B be a base. Then any Ω-subset containing B and of cardinality $\ge \beta(|B|)$ is reconstructible.*

Remarks. 1. The action (G, Ω) is *semi-regular* if $G_\alpha = 1$ for all $\alpha \in \Omega$, that is, if and only if every point of Ω is a base. For such an action by the corollary therefore all sets of size $\ge 5 = \beta(1)$ are reconstructible. The possibilities for the reconstruction index are therefore $\rho(G, \Omega) = 3$, 4 or 5. Each of these occur and a complete classification for each case is given in [7].

2. If (G, Ω) is such that the stabilizer $G_{\alpha,\beta} = 1$ for all $\alpha \ne \beta \in \Omega$ then all two-element subsets are bases. (This case includes for instance all Frobenius groups.) As $\beta(2) = 10$ any set of size at least 10 is reconstructible. However, this time this bound is rather crude, and by direct computation it can be shown that in fact also all sets of size $6 \le |\Delta| \le 9$ are reconstructible, for finite or infinite Ω. Hence the reconstruction index for all such groups is $\rho(G, \Omega) \le 6$.

This is the work of Helen Treacher [11] which is based on computational methods of working with *partial permutations*. Here a classification for each of the possible values $\rho(G, \Omega) = 3, \ldots, 6$ appears rather complicated. The values for the reconstruction index in the following few cases point towards the difficulties one will face in such a classification. For instance, we have computed the following: $\rho(\mathrm{AGL}(1,7)) = 4$, $\rho(\mathrm{AGL}(1,8)) = 5$, $\rho(\mathrm{AGL}(1,9)) = 5$, $\rho(\mathrm{AGL}(1,11)) = 6$, $\rho(\mathrm{AGL}(1,13)) = 4$, $\rho(\mathrm{AGL}(1,16)) = 6$, $\rho(\mathrm{AGL}(1,17)) = 5$, $\rho(\mathrm{AGL}(1,19)) = 5$. For $\mathrm{A\Gamma L}(1,16)$ we have $\rho(\mathrm{A\Gamma L}(1,16)) = 7$, showing that the bound $\rho \leq 6$ really holds only for Frobenius groups.

3. Linear groups

Here we shall apply the bounds from the preceding section to finite-dimensional linear groups and their natural actions. This is straightforward whenever one can satisfy the two conditions in Theorem 2.6. However, there are two situations where some interesting cases need to be considered. In the first part we consider linear groups over finite fields where more general results can be proved; in the second part we deal with the full linear groups over infinite fields.

3.1. Finite fields

Let $d > 0$ be an integer, F an arbitrary field and let $\mathrm{AGL}(d, F)$ be the affine general linear group acting on the vectors of the space F^d. By an *affine permutation group on* F^d we shall mean any subgroup $G \subseteq \mathrm{AGL}(d, F)$ acting on the vectors of F^d.

Theorem 3.1. *Let (G, F^d) with $G \subseteq \mathrm{AGL}(d, F)$ be an affine permutation group on F^d where F is finite. If Δ is contained in the coset $x_0 + V$, where V is a subspace of dimension e, and if $\beta(e+1) \leq |\Delta|$ then Δ is reconstructible. In particular, $\rho(G, F^d) \leq \beta(d+1)$.*

Proof. The vectors $x_0, x_1, \ldots, x_d$ are an *affine frame* for F^d if $x_1 - x_0, \ldots, x_d - x_0$ is a basis of F^d. It is well-known that a frame is a base for $\mathrm{AGL}(d, F)$. Therefore, if $\Delta \subseteq F^d$ has cardinality at least $\beta(d+1)$ and if Δ contains a frame then the result follows from Corollary 2.7.

If Δ does not contain a frame let $\Delta = \{x_0, x_1, \ldots, x_e, x_{e+1}, \ldots, x_{k-1}\} \subseteq x_0 + V$ where the subspace $V = \langle x_1 - x_0, \ldots, x_e - x_0 \rangle \subset F^d$ is of least possible dimension $e < d$. Set $S := \{x_0, x_1, \ldots, x_e\}$. It is clear that $G_{(S)} \subseteq G_{\{\Delta\}}$ and $|G_{(S)}| < \infty$. It follows from Theorem 2.6 that Δ is reconstructible if $|\Delta| \geq \beta(|S|) = \beta(e+1)$. The last part follows since by Lemma 2.4(i) we have that $\beta(e+1) \leq \beta(d+1)$ for $e \leq d$. □

If $G \subseteq \mathrm{GL}(n, F)$ is regarded as a permutation group on the set of non-zero

vectors of F^n we will say that $(G,\, F^n \setminus \{0\})$ is a *linear permutation group.* (This group is imprimitive if $|F| > 2$, with blocks formed by the sets $\{\, \lambda x \;:\; 0 \neq \lambda \in F \,\}$.) Working with bases instead of frames the arguments in the proof above can be modified in an obvious way to give the following:

Theorem 3.2. *Let $(G,\, F^d \setminus \{0\})$ with $G \subseteq \mathrm{GL}(d, F)$ be a linear permutation group where F is finite. If Δ is contained in a subspace of dimension $e \leq d$ and if $\beta(e) \leq |\Delta|$ then Δ is reconstructible. In particular, $\rho(G,\, F^d \setminus \{0\}) \leq \beta(d)$.*

Finally we come to the projective linear groups. If $G \subseteq \mathrm{PGL}(d, F)$ is regarded as a permutation group on the points P of projective space, where P are the set of all one-dimensional subspaces of F^d, then we shall say that $(G,\, P)$ is a *projective linear permutation group.* Here we have the following:

Theorem 3.3. *Let $(G,\, P)$ with $G \subseteq \mathrm{PGL}(d, F)$ be a projective linear group where $d \geq 2$ and F is finite. If Δ is contained in a subspace V of dimension $e \leq d$ and if $\beta(e+1) \leq |\Delta|$ then Δ is reconstructible. In particular, $\rho(G,\, P) \leq \beta(d+1)$.*

Proof. The subspaces $\langle x_1\rangle, \langle x_2\rangle, \ldots, \langle x_{d+1}\rangle$ with $x_i \in F^d$ form a *projective frame* for F^d if $x_1, \ldots, x_d$ are a basis of F^d and if $x_{d+1} = \sum_{1 \leq i \leq d} \lambda_i x_i$ with $\lambda_i \neq 0$ for all $1 \leq i \leq d$. (Of course, any reordering of this set still yields a frame.) As is well-known, a projective frame is a base for $\mathrm{PGL}(d, F)$. Therefore, if $\Delta \subseteq P$ has cardinality at least $\beta(d+1)$ and if Δ contains a frame then Δ is reconstructible by Corollary 2.7. The case when Δ does not contain a projective frame for F^d can be treated just as in the proof of Theorem 3.1. □

In all cases above we have assumed that G is a linear group, rather than a semi-linear group. Thus what can be said if $G \subseteq \mathrm{A\Gamma L}(d, F)$, $\Gamma\mathrm{L}(d, F)$ or $\mathrm{P\Gamma L}(d, F)$? Clearly, if F has degree n over its prime field F_p then $\Gamma\mathrm{L}(d,\, F) \subseteq \mathrm{GL}(dn,\, F_p)$ and so we may apply the Theorems 3.1 and 3.2 to this situation in some cases. We note therefore

Corollary 3.4. *Let $F = GF(p^n)$ where p is a prime and let $G \subseteq \mathrm{A\Gamma L}(d, F)$, or $\Gamma\mathrm{L}(d, F)$, in its natural action. Then $\rho(G,\, \Omega) \leq \beta(nd+1)$ or $\beta(nd)$ respectively.*

Remarks. 1. There are cases where $\rho(\mathrm{GL}(n, F),\, F^n\setminus\{0\}) < \rho(\Gamma\mathrm{L}(n, F),\, F^n\setminus\{0\})$ and so it matters whether G is a subgroup of $\mathrm{GL}(n, F)$ or of $\Gamma\mathrm{L}(n, F)$. However, the bounds of the corollary are probably not best possible for semi-linear groups which are not linear.

2. Some examples for the index of small linear groups include $\rho(\mathrm{PGL}(2, 9)) = 5$ and $\rho(\mathrm{P\Gamma L}(2, 9)) = 6$, $\rho(\mathrm{PSL}(2, 16)) = 7$ and $\rho(\mathrm{P\Gamma}L(2, 16)) = 5$, $\rho(\mathrm{PSL}(2, 13)) = 4$ and $\rho(\mathrm{PGL}(2, 13)) = 5$, $\rho(\mathrm{PSL}(2, 17)) = 6$ and $\rho(\mathrm{PGL}(2, 17)) = 7$. Again, it appears that an exact classification may be rather difficult.

3.2. Infinite fields

When G is an infinite linear group then the requirement that G_S is finite, needed in all proofs above, may not hold. Nevertheless we can prove the following

Theorem 3.5. *Let F be an arbitrary field and let $d \geq 1$. Then $\rho(\mathrm{AGL}(d,F), F^d) \leq \beta(d+1)$.*

Proof. Let $G := \mathrm{AGL}(d,F)$. As before, if Δ contains an affine frame for F^d then we may take S to be the points of this frame so that $G_S = 1$ and so the result follows from Theorem 2.6. In particular, the theorem holds when $d = 1$ and for induction we will assume that it holds for all $e < d$.

For any subset $X \subseteq F^d$ let $V \subseteq F^d$ be the subspace of least dimension such that X is contained in the coset $x + V$ for some $x \in X$. We let then $\dim X := \dim V$ be the *dimension* of X. It remains to rule out the existence of two sets Δ, Δ' of cardinality $k \geq \beta(d+1)$ which are hypomorphic but not isomorphic to each other and which do not contain frames for F^d. Thus $e := \dim \Delta < d$ and $e' := \dim \Delta' < d$.

So let $\Delta = \{x_0, x_1, \ldots, x_e, x_{e+1}, \ldots, x_{k-1}\} \subseteq x_0 + V$ where $x_1 - x_0, \ldots, x_e - x_0$ is a basis of V and let $\Delta' = \{x'_0, x'_1, \ldots, x'_{e'}, x'_{e'+1}, \ldots, x'_k\} \subseteq x'_0 + V'$ where $x'_1 - x'_0, \ldots, x'_{e'} - x'_0$ is a basis of V'. As Δ is hypomorphic to Δ' there is an $h \in G$ such that $h(\Delta \setminus \{x_{e+1}\}) \subseteq \Delta'$. We conclude that $e \leq e'$, and similarly $e' \leq e$. Thus $e = e'$. By taking suitable G-images of Δ and Δ' we may assume that Δ, $\Delta' \subseteq V$ and so these are sets which are hypomorphic but not isomorphic with $e = \dim \Delta = \dim \Delta' = \dim V$ of cardinality $k \geq \beta(d+1) \geq \beta(e+1)$.

Let $G_{\{V\}}$ and G_V be the setwise and pointwise stabilizers of V respectively. Then $G^V := G_{\{V\}}/G_V$ is an affine linear group on V and by induction Δ and Δ' are reconstructible with respect to this action. To complete the proof we are therefore required to prove that the maps which afford the hypomorphism between the two sets belong to $G_{\{V\}}$.

For this let $I(\Delta) := \{x \in \Delta : \dim(\Delta \setminus \{x\}) < e\}$. We claim that $I(\Delta) = \emptyset$. For suppose that $\Gamma = \Delta \setminus \{x\}$ has dimension $e-1$. Then there is a set $\Gamma' = \Delta' \setminus \{x'\}$ and an element $g \in G$ such that $g(\Gamma) = \Gamma'$. It follows that $\dim \Gamma' = e - 1$ and if U with dimension $e-1$ is the space such that $\Gamma' \subseteq y + U$ for some $y \in \Gamma'$, then $g(x)$ and x' are not on $y + U$. But the pointwise stabilizer in G of $y + U$ is transitive on $F^d \setminus (y+U)$ which means that Δ and Δ' are in the same G-orbit. This is a contradiction.

Therefore, if $x \in \Delta$ then the coset of least dimension containing $\Delta \setminus \{x\}$ is V, and if $g \in G$ is such that $g(\Delta \setminus \{x\}) \subseteq \Delta' \subseteq V$ then $g(V) \subseteq V$. This implies that each of the maps which afford the hypomorphism between Δ and Δ' belong to $G_{\{V\}}$, and this completes the proof. □

As in the case of finite fields, working with bases instead of frames, the arguments in the proof above give us the following:

Theorem 3.6. *Let F be an arbitrary field and let $d \geq 1$. Then $\rho(\mathrm{GL}(d, F),\ F^d \setminus \{0\}) \leq \beta(d)$.*

Similarly we may find the reconstruction index for the projective general linear groups:

Theorem 3.7. *Let F be a arbitrary field and let $d \geq 2$. Then $\rho(\mathrm{PGL}(d, F),\ P) \leq \beta(d+1)$.*

Proof. Set $G := (\mathrm{PGL}(d, F),\ P)$. If $X \subseteq P$ we let $\dim X$ be the dimension of the subspace $\langle X \rangle \subseteq F^d$. If $\Delta \subseteq P$ has cardinality $\geq \beta(d+1)$ and if $\dim \Delta = d$ then Δ is reconstructible by the same argument as in the proof of Theorem 3.3. In particular, the theorem holds when $d = 2$ and by induction we shall assume that it does hold for all $e < d$.

So now let Δ and Δ' be hypomorphic but not isomorphic subsets of P of cardinality $\geq \beta(d+1)$ and dimensions $e = \dim \Delta$ and $e' = \dim \Delta'$. As before we show that $e = e'$, and as in the proof of Theorem 3.5 we can show that $e = \dim \Delta \setminus \{\delta\} = \dim \Delta' \setminus \{\delta'\}$ for any $\delta \in \Delta$ and $\delta' \in \Delta'$.

We may assume that both Δ and Δ' are contained in a subspace V of dimension e. As in the proof of Theorem 3.5 we see that the elements $g \in G$ which afford the hypomorphism between Δ and Δ' are contained in the setwise stabilizer $G_{\{V\}}$. Hence by induction Δ and Δ' are isomorphic in G^V and hence in G, a contradiction. □

Remark. It is not clear whether the same bounds apply for arbitrary subgroups of $\mathrm{AGL}(d, F)$, $\mathrm{GL}(d, F)$ and $\mathrm{PGL}(d, F)$. We have no examples where the index is known for such groups and it is difficult even to conjecture how this question should be answered.

3.3. Asymptotic bounds

We conclude with some comments on the asymptotic behaviour of the reconstruction index of the general linear groups when F is an arbitrary field and d is large. If $G = \mathrm{AGL}(d, F)$ acts on $V = F^d$, let $v_1, v_2, \ldots, v_d$ be a basis of V and put $v = \sum_{1 \leq i \leq d-1} v_i$. Then $\{v_1, v_2, \ldots, v_d\}$ is hypomorphic but not isomorphic to $\{v_1, v_2, \ldots, v_{d-1}, v\}$. Thus $d+1 \leq \rho(\mathrm{AGL}(d, p), V)$. The same construction works for the natural actions of $\mathrm{GL}(d, p)$ and $\mathrm{PGL}(d, p)$.

Theorem 3.8. *Let F be an arbitrary field and let d be sufficiently large. Then*

(i) $d \leq \rho(\mathrm{AGL}(d-1, F),\ F^d) \leq d \cdot (1 + \log_2 d)$.

(ii) $d+1 \leq \rho(\mathrm{GL}(d, F),\ F^d \setminus \{0\}) \leq d \cdot (1 + \log_2 d)$.

(iii) $d \leq \rho(\mathrm{PGL}(d-1, F),\ P) \leq d \cdot (1 + \log_2 d)$.

Proof. The upper bounds follow from Theorems 3.5, 3.6 and 3.7 and from Proposition 2.5. □

Remark. We conjecture that it should be possible to replace also the upper bound by d, hence that the reconstruction index is asymptotically the same as the dimension. However, no arguments to prove this appear to be available at this moment.

4. Bounds for finite groups

In this section we shall derive some further bounds from Lemma 2.2 for the reconstruction index of a finite group. So let now (G, Ω) be a finite permutation group of degree n. Let $\Delta \subseteq \Omega$ be a set of cardinality k, and for $S \subseteq \Delta$ we put $n_G(S, \Delta) = |\{S^g : g \in G,\ S^g \subseteq \Delta\}|$, as in Lemma 2.2. Similarly put $\overline{n}_G(S, \Delta) := |\{\Delta^h : h \in G,\ S \subseteq \Delta^h\}|$.

If $X := \{g \in G : S^g \subseteq \Delta\}$ then $n_G(S, \Delta) \cdot |G_{\{S\}}| = |X| = \overline{n}_G(S, \Delta) \cdot |G_{\{\Delta\}}|$. Thus $\overline{n}_G(S, \Delta) = |\Delta^G|$ if $S = \emptyset$. By a simple counting argument the following is immediate: If G is transitive then $\overline{n}_G(S, \Delta) = \frac{k}{n} \cdot |\Delta^G|$ for any set S of size 1; if G is 2-homogeneous then $\overline{n}_G(S, \Delta) = \frac{k(k-1)}{n(n-1)} \cdot |\Delta^G|$ for any 2-element set S. Hence the first part of Lemma 2.2 gives:

Lemma 4.1. *Let (G, Ω) be a finite permutation group of degree $|\Omega| = n$. Suppose that the set $\Delta \subseteq \Omega$ of cardinality k is not reconstructible. Then*

(i) $2^{k-1} \leq |G : G_{\{\Delta\}}|$*; furthermore*

(ii) $2^{k-2} \cdot \frac{n}{k} \leq |G : G_{\{\Delta\}}|$ *if G is transitive, and*

(iii) $2^{k-3} \cdot \frac{n(n-1)}{k(k-1)} \leq |G : G_{\{\Delta\}}|$ *if G is doubly homogeneous on Ω.*

In particular, putting $|G_\Delta| \geq 1$ in Lemma 4.1 (i) we have a well-known general bound for the reconstruction index, see [3] or [8]:

Theorem 4.2. *If (G, Ω) is a finite permutation group then $\rho(G, \Omega) \leq 2 + \log_2 |G|$.*

The following bound due to Mnukhin and Livshiz is the analogue of Lovász's bound (see [6]) on edge-reconstructibility of graphs with sufficiently many edges:

Theorem 4.3 (Livshiz [5], Mnukhin [8])**.** *If (G, Ω) is a finite permutation group with $|\Omega| = n < \infty$ let $\Delta \subset \Omega$ with $\frac{n}{2} < |\Delta|$. Then Δ is reconstructible. In particular, $\rho(G, \Omega) \leq \frac{n}{2} + 1$.*

Proof. Assume that there are $\Delta, \Delta' \subset \Omega$ with $\Delta' \sim \Delta \not\cong \Delta'$. By Lemma 2.1 it follows that if $|\Delta|$ is even then there is some $g \in G$ with $\Delta \cap \Delta^g = \emptyset$. It also follows, see the proof in [1], that if $|\Delta|$ is odd then there is some $h \in G$ with

$\Delta \cap \Delta'^g = \emptyset$. In either case we have $2|\Delta| \leq n$. □

For primitive groups, more specifically, good bounds on the order of the group are available, and these may be applied to the situation here. The next theorem uses Cameron's bound in [2, 4] derived from the classification of the finite simple groups.

Theorem 4.4 (CFSG)**.** *There exists a constant c such that the following is true: If (G, Ω) is a finite permutation group of degree n with an overgroup $\overline{G} \supseteq G$ such that $\overline{G} \neq \mathrm{Alt}_\Omega$ is primitive on Ω, then one of the following is true:*

(i) $\mathrm{Alt}_m^{\,\ell} \subseteq \overline{G} \subseteq \mathrm{Sym}_m \wr \mathrm{Sym}_\ell$ *where* $\mathrm{Sym}_m \wr \mathrm{Sym}_\ell$ *is in the product action,* $n = m^\ell$ *and where* Sym_m *acts on the k-subsets of an m-set. Here* $\rho(G, \Omega) \leq 2 + c^* \cdot n^{1/k\ell} \cdot \log_2 n$ *where c^* depends on k and ℓ only.*

(ii) $\rho(G, \Omega) \leq 2 + c \cdot (\log_2 n)^2$.

Proof. This is immediate from Theorem 4.2 and the estimates for the order of $\overline{G}$ given in Theorem 4.13 in [4]. □

Remarks. 1. Groups of type (i) include symmetric groups acting on k-sets. These are important for reconstruction problems, in particular for the edge-reconstruction of graphs. Müller's result (see [9]) on the edge reconstructibility of graphs with sufficiently many edges is of this kind. His theorem is a direct application of Theorem 4.2 to the action (G, Ω) when G is a symmetric group (on the vertex set V of the graphs to be reconstructed) and where Ω is the set of all pairs from V.

2. If the socle of $\overline{G}$ is solvable then (G, Ω) is an affine linear group of degree $n = p^d$ and here $\overline{G}$ belongs to type (ii). Therefore we have the bound $\rho(\overline{G}, \Omega) \leq 2(d+1) \cdot (1 + \log_2 (d+1))$, by Theorem 3.1 and Lemma 2.4. For large n this bound is better than the one under (ii) in the theorem.

5. Imprimitive actions

In this section we will turn to imprimitive groups as a source of actions with *large* reconstruction index. Thus in particular we shall be looking at the imprimitive action of wreath products.

Let (G, Ω) and (H, Γ) be permutation groups on the disjoint sets Ω and Γ. Then the wreath product $G \wr H$ is the semi-direct product of the base group $G^\Gamma := G \times G \times \ldots \times G$, the cartesian product of $|\Gamma|$ copies of G, by H. Conjugation by $h \in H$ is permutation of the co-ordinates. This group acts imprimitively on $\Omega \times \Gamma$ as follows: If $\Gamma = \{\gamma_1, \ldots, \gamma_l\}$ then $x \in G \wr H$ is of the form

$$x = (g_1, \ldots, g_l) \cdot h; \quad h \in H,\ g_i \in G;\ i = 1, \ldots, l$$

and we put

$$x : (\omega, \gamma_i) \mapsto (\omega, \gamma_i)^x = (\omega^{g_i}, \gamma_i^h).$$

Intuitively, $G \wr H$ acts on an $|\Omega| \times |\Gamma|$ rectangular grid, permuting the $|\Omega|$ cells within a row under the action of G and interchanging (bodily) the $|\Gamma|$ rows under the action of H. By a *row* we mean any set of the kind $\Omega \times \{\gamma\}$ for some $\gamma \in \Gamma$.

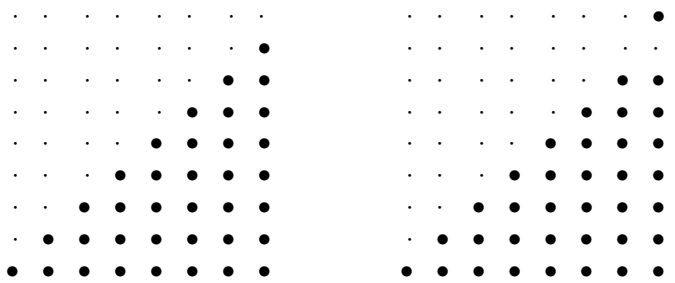
5.1. Examples of actions with maximal reconstruction index

As the Theorem 4.3 shows, the reconstruction index of a group of degree n always satisfies $\rho \leq \frac{n}{2} + 1$. That there are actions which meet this bound can be seen from the following:

Theorem 5.1. *For all $n \geq 2$ we have*

$$\rho(\mathrm{Sym}_n \wr \mathrm{Alt}_{n+1},\, \Omega_n \times \Omega_{n+1}) = \frac{1}{2} \cdot n(n+1) + 1.$$

Proof. By Theorem 4.3 it is sufficient to exhibit two sets of size $\frac{1}{2} \cdot n(n+1)$ which are hypomorphic but not isomorphic to each other. So let Δ_1 and Δ_2 be as represented below, where in general we have n columns and $n+1$ rows.



Δ_1 Δ_2

Then Δ_1 and Δ_2 are not isomorphic for it would take an odd permutation of the rows to map Δ_1 to Δ_2. However, it is easy to verify that $\Delta_1 \sim \Delta_2$. □

Groups with such large reconstruction index necessarily are imprimitive because of the bounds in Section 4. Previously the only actions known to attain the bound of Theorem 4.3 were intransitive examples due to Livshiz. So Theorem 5.1 shows that there are large transitive groups with maximal reconstruction index.

5.2. Bounds for the imprimitive action of wreath products

Our aim is to develop the theory for general wreath products a little further. For this let (J, X) be an action and let $R = \{R_1, \ldots, R_s\}$ be a complete set of

representatives for the J-orbits on 2^X. We define the function $\mu : R \times R \to \mathbb{N}$ by

$$\mu(R_i, R_j) = |\{T \in R_i^J : T \subseteq R_j\}|$$

which sometimes is called the *(lower) orbit inclusion multiplicity* of the orbit R_i^J in the orbit R_j^J. Clearly $\mu(R_i, R_j) = \mu(R_i', R_j')$ for any $R_i' \in R_i^J$ and $R_j' \in R_j^J$, and so μ does not depend on the choice of representatives.

Lemma 5.2. *Let (G, Ω) and (H, Γ) be actions and let $R = \{R_1, R_2, \ldots, R_s\}$ be a complete set of representatives for the G-orbits on 2^Ω. For $\Delta, \Delta' \subseteq \Omega \times \Gamma$ with $|\Delta| = |\Delta'| \geq \max\{3, \rho(G, \Omega)\}$ let n_i and n_i' be the number of rows of Δ and Δ', respectively, containing a member from R_i^G. If $\Delta \sim \Delta'$ in the imprimitive action of $G \wr H$ on $\Omega \times \Gamma$ then $n_i = n_i'$ for all $i = 1, 2, \ldots, s$.*

Proof. Let $\Delta, \Delta' \subseteq \Omega \times \Gamma$ be hypomorphic with respect to $G \wr H$ with $|\Delta| = d$. Firstly, we may assume that neither Δ nor Δ' are contained in just one row. For, assume that Δ is contained in just one row. If Δ' is also contained in just one row then, since $d \geq \rho(G, \Omega)$, we must have $\Delta' \approx \Delta$ and so $n_i' = n_i$ for $i = 1, \ldots, s$. IfΔ' is not contained in a single row we can show, as $d \geq 3$, that some point-deleted subset of Δ' is also not contained in a single row. Since every point-deleted subset of Δ is contained in just one row this contradicts $\Delta \sim \Delta'$.

Fix some i and let N_i be the total number of rows of $\Delta \setminus \{\delta\}$ containing a member from R_i^G as δ varies over Δ. Let $I \subseteq \{1, \ldots, s\}$ be determined by the following requirements: (i) $|R_k| = |R_j|$ for each k, $j \in I$; (ii) $n_k \neq 0$ for each $k \in I$, and (iii) if $k \in I$ and $j \in \{1, \ldots, s\} \setminus I$ then $|R_k| > |R_j|$.

We can determine I and hence n_i for $i \in I$ from the one-point deleted subsets of Δ, as follows. Let t be the maximum number of points in any row occurring among the one-point deleted subsets of Δ. If some member from R_i^G occurs in a row of some point-deleted subset of Δ then $|R_i| = t$ if and only if $i \in I$. For $i \in I$ let l_i be the maximum number of rows containing a G-image of R_i in any point-deleted subset of Δ. If all point-deleted subsets have the same number of rows containing G-images of R_i then $n_i = l_i + 1$, otherwise $n_i = l_i$.

We have the following equation connecting the numbers N_i and n_i. First we define I_i to be the subset of $\{1, \ldots, s\}$ with the property that for each $j \in I_i$ we have $|R_j| = i$. Then for $i \in \{1, \ldots, s\}$ we have

$$\begin{aligned} N_i = n_i \left(d - n_i|R_i| - \sum_{j \in I_{|R_i|+1}} \mu(R_i, R_j) n_j \right) \\ + (n_i + 1) \sum_{j \in I_{|R_i|+1}} \mu(R_i, R_j) n_j + (n_i - 1) n_i |R_i|. \end{aligned}$$

That is,

$$N_i = n_i(d - |R_i|) + \sum_{j \in I_{|R_i|+1}} \mu(R_i, R_j) n_j$$

and so we have

$$n_i = \frac{N_i - \sum_{j \in I_{|R_i|+1}} \mu(R_i, R_j) n_j}{d - |R_i|}$$

for any $i \in \{1, \ldots, s\}$ for which $|R_i| \leq t$. (Note that $d > t \geq |R_i|$ since we assume that Δ is not contained in a single row). Now since we know n_i for $i \in I$ we may determine n_i for $i \in I_{t-1}$. Continuing in this way we determine all n_i for $i \in I_{t-2}, I_{t-3}, \ldots, I_2, I_1$. □

Lemma 5.3. *Let (G, Ω) and (H, Γ) be actions. Let $\Delta \subseteq \Omega \times \Gamma$ be non-reconstructible with respect to the imprimitive action of $G \wr H$ and suppose that $|\Delta| \geq \max\{3, \rho_G\}$. Further, let $R = \{R_1, \ldots, R_s\}$ be a complete set of representatives for the G-orbits on 2^Ω. If R_i is in some row of Δ, up to isomorphism, and if $\mu(R_j, R_i) \neq 0$ then R_j is also in some row of Δ, up to isomorphism.*

Proof. Let R_i and R_j be as in the lemma. It is sufficient to prove the lemma with the added assumption that $|R_j| = |R_i| - 1$. By Lemma 2.6 we can reconstruct the number n_k of rows of Δ containing copies isomorphic to R_k for any $k = 1, 2, \ldots, s$. For a contradiction thus assume $n_i \neq 0$ but $n_j = 0$ for some j with $\mu(R_j, R_i) \neq 0$ and $|R_j| = |R_i| - 1$. Then some point-deleted subset of Δ contains in some row a copy isomorphic to R_j. Choose one which has a minimal number of copies isomorphic to R_i, say $\Delta \setminus \{\delta\}$, for some $\delta \in \Delta$. It is now an easy matter to see that Δ is uniquely reconstructible from $\Delta \setminus \{\delta\}$ by replacing the row containing the copy of R_j by a copy of R_i. This contradicts the fact that Δ is not reconstructible. □

Lemma 5.4. *Let (G, Ω) and (H, Γ) be actions. If $\Delta \subseteq \Omega \times \Gamma$ has cardinality $\geq \max\{3, \rho_G\}$ and if $\Delta \cap \Omega \times \{\gamma\} \neq \emptyset$ for all $\gamma \in \Gamma$ then Δ is reconstructible with respect to the imprimitive action of $G \wr H$.*

Proof. Suppose that such a Δ is not reconstructible. Now Lemma 5.3 implies that some row of Δ consists of just one point, say $\alpha \in \Omega \times \{\gamma\}$. Consider $\Delta \setminus \{\alpha\}$. Then there exists $\beta \in \Omega \times \Gamma$ with $\Delta' \setminus \{\beta\} \approx \Delta \setminus \{\alpha\}$. Then for some $\alpha' \in (\Omega \times \Gamma)$ we have $\Delta \approx \Delta^* \cup \alpha$ and $\Delta' \approx \Delta^* \cup \alpha'$ where $\Delta^* = \Delta \setminus \{\alpha\}$. Then Lemma 5.2 shows that α and α' are in the same row. In fact, by Lemma 5.2 we have that $\alpha \approx_G \alpha'$ from which it follows that $\Delta \approx \Delta'$, a contradiction. □

We can now state and prove the main general theorem about imprimitive wreath product actions:

Theorem 5.5. *Let (G, Ω) and (H, Γ) be finite actions with $2 \leq |\Omega|, |\Gamma|$ and reconstruction indices $\rho_G := \rho(G, \Omega)$ and $\rho_H := \rho(H, \Gamma)$. If $n := |\Omega|$ then*

$$\max\{2, \rho_G, \rho_H\} \leq \rho(G \wr H, \Omega \times \Gamma) \leq \max\left\{3, \rho_G, \frac{1}{2}n(n-1) + 1\right\}$$

for $G \wr H$ in its imprimitive action on $\Omega \times \Gamma$.

These bounds are sharp. For the lower bound consider for instance $G = 1 = H$ on arbitrary Ω, Γ. Then $\rho(G \wr H, \Omega \times \Gamma) = 2 = \rho(H, \Gamma) = \rho(G, \Omega)$. For the upper bound recall Theorem 5.1.

Proof. The lower bound is clear. Let Δ, $\Delta' \subseteq \Omega \times \Gamma$ be hypomorphic but not isomorphic with respect to $G \wr H$ and suppose that their size is at least $\max\{3, \rho_G, \frac{1}{2}n(n-1)+1\}$. By Lemma 5.4 we know that if $|\Delta \cap (\Omega \times \gamma)| \neq 0$ for all $\gamma \in \Gamma$ then Δ is reconstructible.

Let therefore $l := \max\{|\Delta \cap (\Omega \times \gamma)| \, \gamma \in \Gamma\}$. Then by Lemma 5.3 there are rows of Δ containing t points for any $t \in \{l-1, l-2, \ldots, 2, 1\}$. Also there is at least one "empty" row. In particular $l < n$. It follows that $|\Delta| \leq \frac{1}{2}l(l+1) + (n-l-1)l$.

Clearly, for any integers n and l we have $\frac{1}{2}n(n-1) = \frac{1}{2}l(l+1) + (n-l-1)l + \frac{1}{2}(n-l)(n-l-1)$ and since $n > l$ it follows that $\frac{1}{2}(n-l)(n-l-1) \geq 0$. In particular, $|\Delta| \leq \frac{1}{2}n(n-1)$, a contradiction. □

Corollary 5.6. *Let (G, Ω) be an action with finite Ω and reconstruction index $\rho_G := \rho(G, \Omega)$. Let $n \geq 3$ be an integer with $\rho_G \geq \frac{1}{2}n(n-1)+1$. Then*

$$\rho(G \wr H, \Omega \times \Gamma) = \rho(G, \Omega)$$

for any action (H, Γ) with $|\Gamma| \leq n$.

Proof. By assumption we have $\rho(G, \Omega) \geq \frac{1}{2}n(n-1)+1$ and thus also $\rho(G, \Omega) \geq 3$. The inequalities of Theorem 5.5 imply $\rho(G, \Omega) \leq \rho(G \wr H, \Omega \times \Gamma) \leq \rho(G, \Omega)$. □

As another application of Lemma 5.2 we calculate reconstruction index of the imprimitive action of wreath products where the second factor is the symmetric group.

Theorem 5.7. *Let (G, Ω) be an action with $2 \leq |\Omega|$ and reconstruction index $\rho_G := \rho(G, \Omega)$. If Γ is a set of at least two elements then $G \wr \mathrm{Sym}_\Gamma$ has reconstruction index $\rho(G \wr \mathrm{Sym}_\Gamma, \Omega \times \Gamma) = \max\{3, \rho_G\}$ in its imprimitive action on $\Omega \times \Gamma$.*

Proof. Let $\Delta_1, \Delta_2 \subseteq \Omega \times \Gamma$ with $\Delta_1 \sim \Delta_2$ be given. If $|\Delta_1| = |\Delta_2| \geq \max\{3, \rho_G\}$ then by Lemma 5.2 the number of copies of a particular G-orbit on 2^Ω, up to isomorphism, appearing in the rows of both Δ_1 and Δ_2 are the same and so clearly $\Delta_1 \approx \Delta_2$. Hence $\rho(G \wr \mathrm{Sym}_\Gamma, \Omega \times \Gamma) \leq \max\{3, \rho_G\}$.

Evidently, $\rho(G \wr \mathrm{Sym}_\Gamma, \Omega \times \Gamma) \geq \rho_G$. We now show that there are non-reconstructible sets of size 2. Take $a, a' \in \Omega$, $b, b' \in \Gamma$ and let $\Delta := \{(a,b), (a',b)\}$, $\Delta' := \{(a,b), (a',b')\}$. Then $\Delta \sim \Delta'$ but $\Delta \not\approx \Delta'$. Thus $\rho(G \wr \mathrm{Sym}_\Omega, \Omega \times \Gamma) \geq \max\{3, \rho_G\}$. □

References

[1] N. Alon, Y. Caro, I. Krasikov and Y. Roditty, *Combinatorial reconstruction problems*, J. Combin. Theory Ser. B *47* (1989), 153–161.

[2] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. *13* (1981), 1–22.

[3] P. J. Cameron, *Some open problems on permutation groups*, in: Liebeck, M. W. and Saxl, J. (eds.), *Groups, Combinatorics and Geometry*, 340–350, London Mathematical Society Lecture Note Series *165*, Cambridge University Press, Cambridge, 1990.

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

[5] E. M. Livshiz, *On the reconstruction of configurations from their maximum fragments*, Manuscript, Tbilisi, 1983.

[6] L. Lovász, *A note on the line reconstruction problem*, J. Combin. Theory Ser. B *13* (1972), 309–310.

[7] P. M. Maynard and I. J. Siemons, *On the reconstruction index of permutation groups: regular groups*, Aequationes Math. *64* (2002), 218–231.

[8] V. B. Mnukhin, *The k-orbit reconstruction and the orbit algebra*, Acta Appl. Math. *29* (1992), 83–117.

[9] V. Müller, *The edge reconstruction conjecture is true for graphs with more than $n \log_2 n$ edges*, J. Combin. Theory Ser. B *22* (1977), 281–283.

[10] C. Nash-Williams, *The reconstruction problem*, in: L. W. Beineke and R. J. Wilson (eds.), *Selected Topics in Graph Theory*, 205–236, Academic Press, New York, 1978.

[11] H. Treacher, *The reconstruction index of permutation groups whose two-point stabilizer is the identity*, Manuscript, UEA Norwich, 2004.

Ph. Maynard and J. Siemons
School of Mathematics
University of East Anglia
Norwich, NR4 7TJ
United Kingdom

Manuscript received: September 29, 2003 and, in final form, February 1, 2005.