JOURNAL OF COMBINATORIAL THEORY, Series A **74**, 249–286 (1996)
ARTICLE NO. 0050

Arities of Permutation Groups: Wreath Products and k-Sets

GREGORY L. CHERLIN*

Mathematics Department, Rutgers University, New Brunswick, New Jersey 08403

GARY A. MARTIN†

Mathematics Department, University of Massachusetts Dartmouth, North Dartmouth, Massachusetts 02747

AND

DANIEL H. SARACINO‡

Mathematics Department, Colgate University, Hamilton, New York 13346

Communicated by William M. Kantor

Received April 17, 1995

We introduce an invariant of finite permutation groups called the arity which is well known to model theorists but has not been examined from an algebraic point of view. There are few cases in which this invariant is known explicitly. We analyze the behavior of this invariant in power representations of wreath products. We compute it exactly for the action of the symmetric group on n letters on the set of k-sets from an n-element set, and we estimate it rather closely for symmetric powers of these actions. In the case $k = 1$ we formulate an explicit combinatorial conjecture which would pin down the values exactly in all cases. © 1996 Academic Press, Inc.

INTRODUCTION

This paper is devoted to the study of a certain invariant attached to a finite permutation group (G, X), which we call the "arity" of the permutation

* Supported in part by NSF Grant DMS89-03006 and the year in Field Arithmetic of the Institute for Advanced Studies, Hebrew University, Jerusalem, 1991/2. E-mail: cherlin@math.rutgers.edu.

† E-mail: g1martin@umassd.edu.

‡ E-mail: saracino@center.colgate.edu.

0097-3165/96 $18.00

group. An action of a group G on a set X induces actions of G on each power X^n. The arity of G on X may be defined very roughly as the least r such that the set of orbits of G on X^r determines the set of orbits of G on X^n in a straightforward manner. More precisely, what we require of r is that for each n, any two n-tuples $\mathbf{a}$, $\mathbf{b}$ from X should lie in the same G-orbit if they have the following property: every r-tuple from $\mathbf{a}$ lies in the same orbit as the corresponding r-tuple from $\mathbf{b}$.

A word of warning is in order here: although many permutation groups arise naturally as automorphism groups of graphs, they are rarely of arity 2. On the other hand the *regular* representation of any group has arity 2. Another point worth noting is that the arity of the full symmetric group on $n > 1$ symbols is 2, while for the alternating group it is $n - 1$, so that while such groups may be nearly indistinguishible from some points of view, for us they lie at opposite ends of the spectrum.

Although the arity has played a leading rôle in some very general model theoretic work on finite structures, notably [10], [5], and [9], surprisingly little is known about it in concrete cases, even for very familiar primitive permutation representations. The most striking, though ill-posed, question in this context is whether one can say anything at all about a large, primitive permutation group, given only a bound on the arity. There is some general machinery for at least attempting to reduce such questions to the study of almost simple groups, associated in the first place with O'Nan/Scott and subsequently with Aschbacher [1], and vigorously exploited in [8] in a rather more promising context of a similar type. One (early) step in such a reduction would be to reduce the case of a wreath product of a group G by another group H, acting on a power, to the analysis of the actions of G and H separately. (All necessary definitions will be given in §1.)

Our goal initially was to produce concrete information about the arities of certain primitive permutation representations of symmetric groups, but it soon became clear that a systematic investigation of arities of wreath products would be a necessary ingredient of any such project. Consequently we deal almost exclusively with the analysis of wreath products here. At the same time, for the general theory of wreath products it turns out to be quite useful to know the arities of some specific representations of symmetric groups (k-set actions: see §3).

In order to say something intelligible about the arity of a power representation of a wreath product $(G \wr H, X^Y)$, we have found that it is necessary to consider the *induced action* of H on $\mathscr{P}(Y)$, the power set of Y. It turns out that the arity of the power set representation $(H, \mathscr{P}(Y))$ plays a key role in the computation of the arity of a general wreath product, and this has no clearcut relationship to the arity of (H, Y). Our most general result is as follows.

THEOREM I. *Let $\mathscr{F} = \{(G \wr H, X^Y)\}$ be a family of permutation representations of wreath products. Then there will be a uniform bound on the arities of the permutation representations in $\mathscr{F}$ if and only if the following two conditions are satisfied*:

(1) *The arity of the componentwise actions (G, X) are uniformly bounded*;

(2) *There is a uniform bound on the arities of the power set representations $(H, \mathscr{P}(Y))$ associated with the representations (H, Y) which occur as factors.*

Here we assume tacitly that $|X| > 1$ as there is little point in taking a wreath product otherwise.

In view of this result it would be worthwhile to undertake a systematic study of power set representations. Because of the applications we had in view we have tended to focus on the case in which H is the full symmetric group operating on Y. In this case we have a completely explicit result:

THEOREM II. *Let $H = \mathrm{Sym}(d)$ operating naturally on a d-element set Y. Then the arity of H on $\mathscr{P}(Y)$ is $[1 + \log_2 d]$.*

COROLLARY. *Let $\mathscr{F} = \{(G \wr \mathrm{Sym}(d), X^d)\}$ be a family of permutation representations of wreath products with all X of cardinality greater than* 1. *Then there will be a uniform bound on the arities of the permutation representations in $\mathscr{F}$ if and only if the following two conditions are satisfied*:

(1) *The arity of the componentwise actions (G, X) are uniformly bounded*;

(2) *There is a uniform bound on d.*

This may be illustrated by the following two cases, which make use of further concrete information given below.

Case 1. Let I be an index set consisting of triples (n, k, d) of integers with $2k \leqslant n$, and let $\mathscr{F}_I$ be the set of actions of $\mathrm{Sym}(n) \wr \mathrm{Sym}(d)$ on the set of d-tuples of k-sets taken from an n-element set, as (n, k, d) range over I. Then the arities of these actions are uniformly bounded if and only if k and d are bounded uniformly for triples in I. If K and D are bounds for k and d, then the arities of the representations in $\mathscr{F}_I$ are bounded by:

$$[2 + \log_2 K][1 + \log_2 D].$$

Case 2. Let I be an index set consisting of pairs (κ, d) with d a natural number and κ a finite multiset of natural numbers; write $|\kappa| = \sum_{i \in \kappa} i$, summing with multiplicities. Let $\mathscr{F}_I$ be the set of actions of $\mathrm{Sym}(|\kappa|) \wr \mathrm{Sym}(d)$ on the set $\mathscr{E}_\kappa^d$ of all d-tuples of partitions of a $|\kappa|$-element set of type κ.

Then the arities of all these actions are uniformly bounded if and only if d is uniformly bounded and for some uniform bound K we have:

(i) κ contains at most K elements greater than 1;

(ii) If m is the multiplicity of 1 in κ then: $\inf(m, \sup\kappa) \leqslant K$; κ contains at most one element greater than K; and if $\max(m, \sup\kappa) > K$ then the multiplicity of any element of κ other than 1 is one.

Theorem I follows immediately from the following rather loose estimates. We use the notation $\mathrm{Ar}(G, X)$ for the arity of G on X. We sometimes write $\mathrm{Ar}(X)$ or even $\mathrm{Ar}\, X$ when the group and its action on X have been described recently in the text.

THEOREM III. *Let (G, X) be a permutation representation of arity r_0, with $|X| > 1$, and let (H, Y) be a permutation representation with H nontrivial. Let $r^* = \mathrm{Ar}(H, \mathscr{P}(Y))$. Then*

$$\max(r_0, r^*) \leqslant \mathrm{Ar}(G \wr H, X^Y) \leqslant r_0 \cdot r^*.$$

Both of these estimates give the correct value in certain cases. It will be seen from the proof that the upper value will be achieved when (G, X) has enough "room" in it.

If one is only concerned with the qualitative information produced by an assumed bound on the arity, then Theorem III or even Theorem I is entirely adequate. As we have said, our own point of view has been somewhat different. We are hoping to use these results in the study of concrete representations of the kind considered in case 2, and in such cases it is reasonable to ask for exact values or at least very sharp asymptotic estimates as the parameters involved tend to infinity in various ways. By a direct argument used also in the proof of Theorem II we have exact information for the representation of $\mathrm{Sym}(n)$ on k-sets, less exact but still quite sharp asymptotic information on the families $\mathrm{Sym}(n) \wr \mathrm{Sym}(d)$ acting on d-tuples of k-sets, and very weak information on the actions on partitions (equivalence relations).

We will write $[{n \atop k}]$ for the set of unordered k-element subsets of a fixed set of n elements; but we generally write n^d for $[{n \atop 1}]^d$. Our results on the natural action of $(\mathrm{Sym}\, n \wr \mathrm{Sym}\, d)$ on $[{n \atop k}]^d$ include the following:

THEOREM IV A. $\mathrm{Ar}(2^d) = 2 + 2 \cdot [\log_4 d]$. *In other words, this is the largest even integer below* $2 + [\log_2 d]$.

THEOREM IV B. $\mathrm{Ar}[{n \atop k}]^d \leqslant [2 + \log_2 k][1 + \log_2 d]$ *with equality if* $n \geqslant 2k[1 + \log_2 d]$.

THEOREM IV C. *Let* $r = [n/2k]$. *If* $r \leqslant [1 + \log_2 d]$ *then* $\mathrm{Ar}[{n \atop k}]^d \geqslant r[2 + \log_2 k]$.

This result will be proved in a slightly sharper form below, which allows a further contribution from the remainder of n after division by $[1 + \log_2 d]$.

In concrete cases these results leave a significant gap for $n < 2k [1 + \log_2 d]$. We specialize further, to $k = 1$, so that we consider wreath products of the form $(n^d, \mathrm{Sym}(n) \wr \mathrm{Sym}(d))$ where one would certainly look for very concrete results. In this case the results are asymptotically very sharp, if one adds the following estimate:

THEOREM IV D. $\mathrm{Ar}(n^d, \mathrm{Sym}(n) \wr \mathrm{Sym}(d)) \leqslant [\log_2 d] + n$.

For $k = 1$ the estimate in IV B is $\mathrm{Ar}(n^d) \leqslant 2[1 + \log_2 d]$, with equality for $n \geqslant 2[1 + \log_2 d]$. Within the interesting range $n < 2[1 + \log_2 d]$, the estimate in Theorem IV D is superior half the time (for $n < 2 + \log_2 d$).

EXAMPLES. We consider as examples the wreath product actions on 4^7 and 4^8. According to Theorem IV B we have the upper bounds of 6 and 8 on their respective arities. With $k = 1$ the bound in IV C is no better, and sometimes worse, than the bound in Theorem IV A, which applies as a lower bound for $n \geqslant 2$: so the arities are at least 4 in both cases. The upper bounds in Theorem IV D are 6 and 7, so in this case Theorem IV D is better than Theorem IV B, though for $n = 5$ the situation would be reversed. So we have

$$4 \leqslant \mathrm{Ar}(4^7) \leqslant 6; \qquad 4 \leqslant \mathrm{Ar}(4^8) \leqslant 7.$$

The correct values are 5 and 6 respectively.

Individual values of these arities can be computed exactly for suitably small values of the parameters using linear algebra. A direct-search computation of the arity by looking at the orbit structure on n-tuples involves a blow-up in computation time which could be exponential and in any case is not polynomially bounded in the degree of the representation. In practice this is satisfactory in most cases up to degree 50, a number which is however considerably less than, say, 4^8. However if one has an *a priori* bound R on the arity then the problem of computing the arity of a wreath product n^d can be reduced to the study of the lattice of integer solutions to a $R \cdot p(R-1) \times p(R)$ homogeneous linear system where $p(R)$ is the number of partitions of an R-element set. (So for $R = 6$ this is a 312×205 system.) The precise problem is the identification of the vectors of minimum l^1

norm in this integer lattice. We will explain this in §5. This technique, it should be emphasized, works in any wreath product $(G \wr \mathrm{Sym}(d), X^d)$ though the linear systems will be distinctly larger, for a fixed set X, when the group G is not the full symmetric group. If G is the identity group the corresponding linear system would be of size $R \cdot |X|^{R-1} \times |X|^R$. On the other hand in this particular case our results yield the exact value explicitly: $[1+\log_2 d]$.

At present the linear algebra technique is the only one we know of for getting exact values for $\mathrm{Ar}(n^d)$ in concrete cases with $3 \leqslant n < 2[1+\log_2 d]$. However it delivers not just numerical information, but optimal examples in specific cases, and a study of these examples leads to conjectures regarding the arity of n^d which is discussed in §7. If these conjectures are correct then it would be rather awkward to write down a formula for the arity of n^d, but it would be trivial to compute it. At present the conjectured formula is known to give a lower bound for the arity, and Theorem IV D implies a fairly close upper bound. We do not have a more general conjecture for the case of $[{n \atop k}]^d$ with $k > 1$ and it would be interesting to explore constructions analogous to those used in §6 in this more general context.

One special case of all of this was noticed long ago. The wreath products $(\mathrm{Sym}(n) \wr \mathrm{Sym}(2), n^2)$ may be thought of as graphs: the vertices are ordered pairs of indices in the range $(1, ..., n)$, with an edge between pairs that agree in at least one coordinate. This is also called the "line graph" of the complete bipartite graph $K_{n,n}$. The classification of all finite homogeneous graphs [11], [6] is quite simple: apart from $m \cdot K_n =$ the disjoint sum of some complete graphs, and its complementary graph, there is only the pentagon (5-cycle) and the line graph of $K_{3,3}$, that is (3^2) in our notation. What happens in fact is that the arity of (n^2) is 4 for for $n > 3$ and hence these structures cannot be thought of as homogeneous binary structures.

We conclude this introduction with a bit more discussion of the model theoretic background alluded to above. If one bounds both the *arity* r of a permutation group as well as the *number of orbits* on r-tuples, one gets a very highly developed theory presented in [10], [5], [9] and developed further in [8], applicable also to a class of infinite permutation groups, and which does not require primitivity or even transitivity, though it depends on a detailed analysis of the primitive case, based on the classification of the finite simple groups. The permutation-theoretic condition we have given is expressed in model-theoretic terms as: "homogeneity with respect to a finite relational language". The main result of Lachlan's theory resists summary, but it may be expressed very loosely as saying that large finite structures which are homogeneous for a finite relational language can be classified into finitely many types in a manner which is quite satisfactory from a theoretical point of view. Since as we have noted every regular representation of a finite group has arity 2, no such statement would be valid just under the assumption of a bound on the arity. It is less clear what the effect of such a bound will be in the primitive case.

Accordingly we would like to know what can be said about a "typical" finite primitive permutation group if the arity r is bounded, but no restriction is placed on the number of orbits of G on r-tuples. Given the detailed knowledge already available for a broad variety of families of permutation representations, and the theoretical underpinnings provided by O'Nan/Scott and Aschbacher, this seems like a reasonable enterprise.

Though this is not the place to enter into the details, it seems worth noting that these questions also make sense for infinite structures. The setting would then be that one has a structure $\mathscr{X}$ and a finite permutation group (H, Y), and one forms the generalized product $\mathscr{X}^Y$ which can be described syntactically in a Feferman-Vaught style language: for each formula ϕ in m variables in the language of $\mathscr{X}$, there is a "truth value" map $\langle \phi \rangle$: $(X^Y)^m \to \mathscr{P}(Y)$ taking a sequence of elements $\mathbf{a}^1, ..., \mathbf{a}^m \in X^Y$ to the set of y for which $\phi(a_y^1, ..., a_y^m)$ holds, and then for every orbit $\mathscr{O}$ in $\mathscr{P}(Y)$ under the induced action of H, there is a predicate in the language of $\mathscr{X}^Y$ interpreted as: "$\langle \phi \rangle(\mathbf{a}^1, ..., \mathbf{a}^m) \in \mathscr{O}$". The question then becomes: assuming $\mathscr{X}$ admits quantifier elimination in a language with r_0-place relations, what is the minimum r for which $\mathscr{X}^Y$ admits quantifier elimination in a language with r-place relations? Here we consider only the finite case, which can be treated by methods that are more widely understood.

We thank Ron Solomon for information about heights of subgroup lattices.

1. Preliminaries

We will define the arity of a permutation group precisely (in two nearly identical variants) and give its most basic properties. We include a discussion of an upper bound that can be used in concrete cases to make a direct computation of the arity practical on a computer, by bounding the length of a search, when the size of the set on which the group acts is not too large.

We consider a group G acting on a finite set X. We do not insist that the action be transitive, or even faithful, though there is no harm in imposing the latter condition. Occasionally, in statements of the form "G equals some given group" it is tacitly assumed that G has been replaced by its image in Sym X.

An orbit of the action of G on X^n is called an *n-type*. We write tp($\mathbf{a}$) for the G-orbit of the n-tuple $\mathbf{a}$. For $I \subseteq \{1, ..., n\}$ we have the projection π_I: $X^n \to X^I$ which induces a map from X^n/G to X^I/G; if we take an order-preserving bijection of I with $\{1, ..., r\}$ we may view this as a map from

n-types to r-types, which is again denoted π_I. The *r-type* of an n-tuple $\mathbf{a}$, for $r \leqslant n$, will be the function which associates to each $I \subseteq \{1, ..., n\}$ of cardinality r the type $\pi_I \operatorname{tp}(\mathbf{a}) = \operatorname{tp}(\pi_I \mathbf{a})$. We will say that r-types *determine* n-types if any two n-tuples with the same r-type have the same n-type. The *arity* of (G, X) is the least r such that r-types determine n-types for all $n \geqslant r$; it is clear that this is at most $|X|$.

There is a slightly different definition which is equally natural, and occasionally gives a different value. Let $X^{(n)}$ denote the set of n-tuples with no repeated entry (so this is empty for large n). Repeat all the definitions using $X^{(n)}$ in place of X^n. Call the resulting notion of arity the "weak arity". (This amounts model theoretically to treating equality as a logical notion rather than as part of the structure imposed on X.) For the symmetric group the arity is 2 and the weak arity is 0. This is virtually the only discrepancy between these notions:

PROPOSITION 1. *If (G, X) is a finite permutation group of arity r and weak arity r' then*:

(1) $r = \max(r', 2)$ *unless* $G = (1)$, *in which case* $r = 1$ *unless* $|X| = 1$ (*and* $r = 0$);

(2) $r = r'$ *unless* $G = \prod \operatorname{Sym}(X_i)$ *with* (X_i) *a partition of* X. *In this case* $r' = 1$ *unless* G *is* $\operatorname{Sym}(X)$, *in which case* $r' = 0$.

Proof. One divides into two cases: either $r' \geqslant 2$ and then easily $r = r'$, or else $r' < 2$ and then G has the form stated in (2). ∎

We will use the notation $\operatorname{Ar}(G, X)$ for the arity, and $\operatorname{Ar}'(G, X)$ for the weak arity. By a common abuse of notation in contexts where one or the other of G or X is understood we may use notations like $\operatorname{Ar}(G)$ or $\operatorname{Ar}(X)$ (more often the latter).

One should observe that the notion of the arity of a permutation group is in some sense complementary to the notion of the degree of transitivity of the group. In particular notice that if the arity of (G, X) is r and the action is r-transitive, then G is the full symmetric group.

FACT. $\operatorname{Ar}(G, X)$ *is the greatest r for which $(r-1)$-types do not determine r-types.*

EXAMPLE. This does not mean that the arity is the least r for which r-types *do* determine $(r+1)$-types, though this is frequently the case. As an example, in the action of $\operatorname{Sym}(4) \wr \operatorname{Sym}(2)$ on $X = \Omega^2$, where Ω has order 4 and $\operatorname{Sym}(4)$ acts as $\operatorname{Sym}(\Omega)$ on Ω, one may check that 2-types determine 3-types, but the arity is 4.

Note also that $(\mathrm{Alt}\, X, X)$ has arity $|X|-1$. This is a rather extreme example. With few exceptions we expect the arity in general to be less than $\sqrt{|X|}$ for reasons indicated below.

Notation. If $A \subseteq X$, Let G_A denote the pointwise stabilizer of the set A in G, and let $X_A = X - A$. Then G_A acts on X_A.

In several cases the upper bound in the next result turns out to be tight.

PROPOSITION 2. *Let (G, X) be a permutation group and let $k < |X|$ be positive. Then*

$$\max(\mathrm{Ar}(G_A, X_A) : A \subseteq X, |A| = k) \leqslant \mathrm{Ar}(G, X)$$
$$\leqslant \max(\mathrm{Ar}'(G_A, X_A) : A \subseteq X, |A| = k) + k$$

with one exception: the case $k = 1$, $G = \mathrm{Sym}\, X$.

Proof. Let $r = \mathrm{Ar}(G, X)$ and let $A \subseteq X$. We claim first that $\mathrm{Ar}(G_A, X_A) \leqslant r$, or in other words that for $n \geqslant r$, r-types determine n-types in (G_A, X_A).

Fix n-tuples $\mathbf{a}, \mathbf{b} \in X_A$ with the same r-type in (G_A, X_A). We claim then that $\mathbf{a}$ and $\mathbf{b}$ have the same type in (G_A, X_A). Extend $\mathbf{a}$, $\mathbf{b}$ to $(n+k)$-tuples $\mathbf{a}'$, $\mathbf{b}'$ by adding the elements of A in some definite order. Observe then that $\mathbf{a}'$, $\mathbf{b}'$ have the same r-type in (G, X). It then follows that $\mathbf{a}'$ and $\mathbf{b}'$ are in the same orbit under G, which means precisely that $\mathbf{a}$ and $\mathbf{b}$ lie in the same G_A orbit, as claimed.

Now suppose that $\mathrm{Ar}'(G_A, X_A) \leqslant r$ for all A of order k contained in X. We claim then that $\mathrm{Ar}(G, X) \leqslant r + k$, that is that $(r+k)$-types determine n-types in (G, X) for all $n \geqslant r + k$.

Let $\mathbf{a}$, $\mathbf{b}$ be n-tuples in X with the same $(r+k)$-types. It is possible that $r + k < 2$, but this means that we are in the exceptional case mentioned. So we may take $r + k \geqslant 2$, and consequently we may suppose that in $\mathbf{a}$, $\mathbf{b}$ there are no repeated entries. Now write $\mathbf{a} = \mathbf{a}'\mathbf{a}''$, $\mathbf{b} = \mathbf{b}'\mathbf{b}''$, with $\mathbf{a}'$, $\mathbf{b}'$ of length k and $\mathbf{a}''$, $\mathbf{b}''$ of length $n - k$. Then $\mathbf{a}'$ and $\mathbf{b}'$ have the same type in (G, X) and hence after applying an element of G we may suppose $\mathbf{a}' = \mathbf{b}'$. Let A be the set consisting of the elements of the sequence $\mathbf{a}'$. In (G_A, X_A) the sequences $\mathbf{a}''$ and $\mathbf{b}''$ have the same r-type, hence have the same type. This means that in (G, X) the sequences $\mathbf{a}$ and $\mathbf{b}$ have the same type, as claimed. ▮

We specialize this result to the k-transitive case:

COROLLARY 3. *Let (G, X) be a k-transitive permutation group, and let $A \subseteq X$ have order k. Then*

$$\mathrm{Ar}(G_A, X_A) \leqslant \mathrm{Ar}(G, X) \leqslant \mathrm{Ar}'(G_A, X_A) + k$$

unless $k = 1$ and $G = \mathrm{Sym}(X)$.

PROPOSITION 4. *Let (G, X) be a permutation group and let Y be a G-invariant subset of X, or more generally an equivalence class of a G-invariant equivalence relation. Then*

$$\mathrm{Ar}(G, Y) \leqslant \mathrm{Ar}(G, X).$$

(If one prefer to work with faithful actions, replace (G, Y) by the induced action (G^Y, Y).)

Proof. The action of G on Y^n is part of the action of G on X^n for all n. ∎

We will say that (G, X) is the *complete sum* of the permutation groups (G^Y, Y) where Y varies over the orbits of G on X (or any other partition of X into G-invariant sets) if G induces $\prod_Y G^Y$ on X.

FACT. *The arity of a complete sum of permutation groups is the maximum arity of the constituents.*

Proof. Let r be this maximum arity. We know $r \leqslant \mathrm{Ar}(G, X)$ and the reverse inequality is also evident. ∎

By contrast with the preceding proposition, quotients are notoriously badly behaved in this context. Every transitive permutation group is a quotient of a regular representation, and these have arity 2.

We now introduce another invariant which gives a weak bound on the arity. This is of no direct relevance to the work in the present paper, though as we will explain it is quite relevant to computational issues and may perhaps illustrate the behavior of the arity in a useful way.

DEFINITION. The *height* $h(G, X)$ of a permutation group is the least number h such that every set $A \subseteq X$ contains a set B of order at most h with $G_A = G_B$.

For example, a transitive permutation group is regular if and only if it is of height 1.

LEMMA 5. *Let (G, X) be a permutation group of height h. Then:*

(1) *h is the smallest number such that every subset A of X of order $h+1$ contains a subset B of order h with $G_A = G_B$;*

(2) If $G \leqslant \mathrm{GL}(n, \mathbb{F}_q)$ *and X is a vector space of dimension n over $\mathbb{F}_q$ on which G acts naturally, then $h \leqslant n$.*

(3) $\mathrm{Ar}(G, X) \leqslant h+1$.

Proof. (1) The main point is that if $A \subseteq B$ and $G_A = G_{A_0}$ for some proper subset A_0 of A, then setting $B_0 = A_0 \cup (B - A)$, we have $G_B = G_{B_0}$ with B_0 a proper subset of B.

(2) This is clear.

(3) Let $r = h + 1$, and let $\mathbf{a}$, $\mathbf{b}$ be two n-tuples in X with the same r-type. Let $\mathbf{a}'$ be a subsequence of $\mathbf{a}$ of length at most h such that $G_{\mathbf{a}'} = G_{\mathbf{a}}$ and let $\mathbf{b}'$ be the corresponding portion of $\mathbf{b}$, that is: $\mathbf{a}' = \pi_I \mathbf{a}$ and $\mathbf{b}' = \pi_I \mathbf{b}$ for some I of order h. As $\mathbf{a}$ and $\mathbf{b}$ have the same h-type we may apply an element of G and suppose that $\mathbf{a}' = \mathbf{b}'$. We claim that then $\mathbf{a} = \mathbf{b}$. Suppose that $i \leqslant n$ and set $J = I \cup \{i\}$. Then $\pi_J \mathbf{a}$ and $\pi_J \mathbf{b}$ have the same type, as $|J| \leqslant h + 1$, so there is some $g \in G$ carrying $\pi_J \mathbf{a}$ to $\pi_J \mathbf{b}$. In particular g fixes $\mathbf{a}'$ pointwise and hence fixes a_i as well, so $b_i = a_i$. Thus $\mathbf{a} = \mathbf{b}$. ∎

COROLLARY 6. *If G is sharply t-transitive on X and $G \neq \operatorname{Sym} X$ then* $\operatorname{Ar}(G, X) = t + 1$.

Proof. By assumption the stabilizer of any t points is trivial, so $h \leqslant t$ and hence $\operatorname{Ar}(G, X) \leqslant t + 1$.

On the other hand if $\operatorname{Ar}(G, X) \leqslant t$ and G is t-transitive then G is n-transitive for all n, and $G = \operatorname{Sym} X$. ∎

This is one source of examples with relatively large arity. If we take the projective line over a quite small field (say, of order 13) we violate the inequality $\operatorname{Ar}(G, X) \leqslant \sqrt{|X|}$ which we mentioned at the outset. We expect that the primitive groups violating this inequality can be classified along the lines suggested below. (On the other hand we do not think this inequality is very sharp in practice.)

We will say a few words about the significance of the invariant h for computation of the arity. The arity is the least r such that r-types determine h-types, where h is the height. As the number of r-types tends to grow rapidly, perhaps even exponentially, with r, this is a useful cutoff point for a computation of the arity by brute force, and in fact is the main reason that brute force succeeds on small examples. Actually this remark can be refined in a useful way. Call a set A *independent* if its stabilizer is not the stabilizer of proper subset, and call a type *nondegenerate* if its entries form an independent set. In computing the arity it is enough to work with nondegenerate types (unless this results in arity 1, in which case the original arity may have been 2), so not only does this bound the sizes of the types in a useful way, it also prunes the search tree in a way that has significant impact on the computation time in practice. Of course in the cases of interest in the present paper there are much better computational approaches, as well as better *a priori* upper bounds on the arity. On the other hand, we think it might be interesting to get an overview of the arities of *all* primitive representations of a few small nearly simple groups, and for this brute force computation might well be the most appropriate approach. We have computed arities of almost all primitive permutation groups of degree at most 50 using these ideas.

We may also note a few formal properties of the height.

LEMMA 7. *Let* (G, X) *be a permutation group.*

(1) *If* $(Y_i: i < o)$ *are the orbits of* G *on* X *then* $h(G, X) \leqslant \sum h(G^{Y_i}, Y_i)$.

(2) *If* G *is transitive on* X *and imprimitive, and* E *is a nontrivial* G*-invariant equivalence relation on* X *with* c *classes, then for any* E*-class* C *in* X *we have*

$$h(G, X) \leqslant c \cdot h]G^C, C).$$

(3) $h(G, X) < |X| - 2$ *unless* G *contains eigher* $\mathrm{Alt}(X)$ *or* $\mathrm{Sym}(X_1) \times \mathrm{Sym}(X_2)$ *with* X_1, X_2 *a partition of* X.

Proof. (1) and (2) are instances of a single principle: if we have a G-invariant equivalence relation we can estimate the height of G by summing the heights of (G^C, C) over each E-class C. This follows at once from the definitions.

For (3) we begin by proving:

$$h(G, X) < |X| - 1 \qquad \text{unless} \quad G = \mathrm{Sym}\, X. \tag{$*$}$$

Let $n = |X|$. It is clear in any case that $h(G, X) \leqslant n - 1$. If $h(G, X) = n - 1$ this means we have a set A of cardinality $n - 1$ such that for each element $a \in A$, $G_{A - \{a\}} > G_A$; in other words every transposition which involves the unique element $b \notin A$ belongs to G, and thus $G = \mathrm{Sym}\, X$.

Now suppose that $h(G, X) = n - 2$. Then there is a set A of order $n - 2$ such that for every element $a \in A$, the pointwise stabilizer of $A - \{a\}$ in G is nontrivial, and therefore contains a transposition or a 3-cycle. If G is primitive on X then a theorem of C. Jordan (cf. [7, p. 171]) states that G contains $\mathrm{Alt}\, X$. Assume therefore that G is imprimitive on X and let E be a nontrivial G-invariant equivalence relation on X. For each E-class C, $h(G^C, C) \leqslant |C| - 1$ and hence by (1) and (2) it follows that E has exactly two equivalence classes X_1, X_2 on X. It is clear as well that the set A contains all but one point in each of X_1 and X_2. Hence as in the proof of $(*)$ G contains enough transpositions to generate $\mathrm{Sym}(X_1) \times \mathrm{Sym}(X_2)$. ∎

No doubt one could get much sharper results in this vein by restricting to primitive groups. For example one might try to show that in this case $h(G, X) \leqslant \sqrt{|X|}$ apart from some sporadic examples, such as some small multiply transitive groups. However in most cases this will give a poor estimate for the arity.

COROLLARY 8. *Let* (G, X) *be a permutation group with* $G \neq \mathrm{Alt}\, X$ *and with* $|X| \geqslant 4$. *Then* $\mathrm{Ar}(G, X) \leqslant |X| - 2$.

Proof. This follows from the bound on h in part (3) of the previous result unless G is one of the exceptions mentioned there. So the only case that needs to be considered is that in which G has a nontrivial invariant equivalence relation with two classes X_1, X_2 and G contains $\mathrm{Sym}\, X_1 \times \mathrm{Sym}\, X_2$. There are two cases: either $G = \mathrm{Sym}\, X_1 \times \mathrm{Sym}\, X_2$ or G is a wreath product $\mathrm{Sym}(X_1) \wr \mathrm{Sym}(2)$ (here $|X|_1 = |X|_2 = |X|/2$). In both cases (G, X) has arity 2, by inspection. ∎

2. WREATH PRODUCTS ACTING ON POWERS

If (G, X) and (H, Y) are two permutation groups there is a natural action of the wreath product $G \wr H = G^Y \rtimes H$ acting on X^Y. Here G^Y acts on the points of X^Y coordinatewise, and H permutes the coordinates.

THEOREM 1. *Let* (G, X) *be a permutation representation of arity* r_0, *with* $|X| > 1$, *and let* (H, Y) *be a permutation group of degree d. Let* $r^* = \mathrm{Ar}(H, \mathscr{P}(Y))$. *Then*

$$r_0 \leqslant \mathrm{Ar}(G \wr H, X^Y) \leqslant r_0 \cdot r^*.$$

Proof. The lower bound $r_0 \leqslant \mathrm{Ar}(G \wr H, X^Y)$ is immediate. Any two r_0-tuples $\mathbf{a}$, $\mathbf{b}$ in X with the same $(r_0 - 1)$-type and distinct r_0-types will extend to similar r_0-tuples $\hat{\mathbf{a}}$, $\hat{\mathbf{b}}$ in X^Y, by taking the remaining entries equal to a fixed constant $c \in X$. The extended r_0-tuples certainly have the same $(r_0 - 1)$-type in X^Y, and it is easily seen that their r_0-types remain distinct.

We now consider two n-tuples $\mathbf{a}, \mathbf{b}$ in X^Y with the same $(r_0 \cdot r^*)$-type under $G \wr H$, and we claim that they have the same type. Each element of $\mathbf{a}$ or $\mathbf{b}$ will be thought of as a row vector with entries in X, indexed by Y. Let $d = |Y|$ (the "dimension"). The n-tuples $\mathbf{a}$ and $\mathbf{b}$ may be thought of as $n \times d$ matrices (a_{ij}), (b_{ij}) with entries in X. The main point will be to look closely at the columns, which are indexed by elements of Y. The column in $\mathbf{a}$ or $\mathbf{b}$ indexed by y will be denoted $\mathbf{a}_y$ or $\mathbf{b}_y$ respectively. Each such column is an n-tuple in X and as such its type is determined by its r_0-type in X.

We now associate with $\mathbf{a}$ and $\mathbf{b}$ a number of subsets of Y. For each subset I of $\{1, ..., n\}$ with $|I| = r_0$, and for each r_0-type p, let $A_{I,p}$ be the set of $y \in Y$ such that $\pi_I \,\mathrm{tp}\, \mathbf{a}_y = p$, and let $B_{I,p}$ be associated in a similar way with $\mathbf{b}$. As we have assumed that $\mathbf{a}$ and $\mathbf{b}$ have the same $(r_0 \cdot r^*)$-type in

$(G \wr H, X^Y)$, it follows that the sequences of sets $(A_{I,p})$ and $(B_{I,p})$ have the same r^*-type in $(H, \mathscr{P}(Y))$. This is the critical observation.

Accordingly, after applying an element of H we may suppose that $A_{I,p} = B_{I,p}$ for all I, p, or in other words that for each $y \in Y$, the columns $\mathbf{a}_y$ and $\mathbf{b}_y$ have the same r_0-type in (G, X). Accordingly these columns have the same type in (G, X) and some element g_y carries $\mathbf{a}_y$ to $\mathbf{b}_y$. The element $(g_y: y \in Y)$ then carries $\mathbf{a}$ to $\mathbf{b}$. ▌

This result contains most of Theorem III, from which the main purely qualitative result Theorem I follows. We now finish the proof of Theorem III.

THEOREM III. *Let (G, X) be a permutation representation of arity r, with (as always) $|X| > 1$, and let (H, Y) be a permutation representation. Let $r_0 = \mathrm{Ar}(G, X)$ and $r^* = \mathrm{Ar}(H, \mathscr{P}(Y))$. Then*

$$\max(r_0, r^*) \leqslant \mathrm{Ar}(G \wr H, X^Y) \leqslant r_0 \cdot r^*.$$

Proof. It remains to get the bound $r^* \leqslant \mathrm{Ar}(G \wr H, X^Y)$. Consider the set Δ of "constant elements" in X^Y. The pointwise stabilizer of Δ in $G \wr H$ is just H. Let c, c' be two elements of X, and let $P = \{c, c'\}^Y$. Then P is an H-invariant subset of X^Y and (H, P) may be naturally identified with $(H, \mathscr{P}(Y))$. Thus we have:

$$\mathrm{Ar}(H, \mathscr{P}(Y)) = \mathrm{Ar}(H, P) \leqslant \mathrm{Ar}(H, X^Y) \leqslant \mathrm{Ar}(G, X^Y)$$

where we have used Propositions 1.2 and 1.4. ▌

Now we look for an improved lower bound. Within a family of naturally occurring permutation groups it frequently occurs that the larger ones contain many independent copies of the smaller ones in a natural way. Accordingly we make the following definitions.

DEFINITION. Let (G, X) be a permutation group.

(1) The subset $X_0 \subseteq X$ is said to be *smoothly embedded* in X if any two r-tuples $\mathbf{a}, \mathbf{b}$ in X_0 which lie in the same orbit under the action of G, are also in the same orbit under the action of the induced group G^{X_0}.

(2) A collection of disjoint sets $X_i \subseteq X$ is said to be (*jointly*) *smoothly embedded* in X if each X_i is smoothly embedded in X and $G^{\bigcup X_i}$ contains $\prod G^{X_i}$.

For example, in the representation of $\mathrm{Sym}(n)$ on the set of k-sets $[{n \atop k}]$, if n_i are numbers with $\sum n_i \leqslant n$ then in various natural ways the collection $([{n_i \atop k}])$ is smoothly embedded in $[{n \atop k}]$.

THEOREM 2. *Let (G, X) and (H, Y) be permutation groups. Let r^* be chosen so that in $(H, \mathscr{P}(Y))$ there are two r^*-tuples with the same (r^*-1)-types and distinct types; so $r^* \leqslant \mathrm{Ar}(H, \mathscr{P}(Y))$, although in general not every value of r^* below the arity will do. Suppose that (X_i) is a collection of r^* disjoint subsets of X, which is smoothly embedded in X. Then*

$$\mathrm{Ar}(G \wr H, X^Y) \geqslant \sum_i \mathrm{Ar}(G^{X_i}, X_i).$$

Proof. Let $r_i = \mathrm{Ar}(G^{X_i}, X_i)$, and within X_i fix r_i-tuples $\mathbf{a}^i, \mathbf{b}^i$ with distinct types, but with the same (r_i-1)-types. As X_i is smoothly embedded in X, these types may be taken either with respect to the action of G on X, or with respect to the action of G^{X_i} on X_i. In what follows it is better to think of them under the action of G. Take two r^*-sequences $(I_i : i < r^*)$, $(I'_i : i < r^*)$ of subsets of Y with distinct types but with the same (r^*-1) type.

For $y \in Y$ we define a sequence $\mathbf{c}_y$ of length $r = \sum r_i$, with entries in X, by concatenating r^* sequences $\mathbf{c}_{iy}$ of length r_i chosen as follows: $\mathbf{c}_{iy} = \mathbf{a}^i$ if $y \in I_i$ and $\mathbf{c}_{iy} = \mathbf{b}^i$ otherwise. Substituting I'_i for I_i we define $\mathbf{c}'_y$ similarly.

We consider the matrix C whose columns are the sequences $\mathbf{c}_y$ for $y \in Y$. The rows of this matrix are elements of X^Y and hence the whole matrix may be viewed as an r-tuple $\hat{\mathbf{c}}$ of elements of X^Y. Similarly the sequences $\mathbf{c}'_y$ make up a matrix C' whose rows form an r-tuple $\hat{\mathbf{c}}'$ of elements of X^Y. It remains to be checked that:

$$\hat{\mathbf{c}} \text{ and } \hat{\mathbf{c}}' \text{ realize distinct } r\text{-types;} \tag{1}$$

$$\hat{\mathbf{c}} \text{ and } \hat{\mathbf{c}}' \text{ realize the same } (r-1)\text{-type.} \tag{2}$$

We now check (1). Suppose that $g \in G \wr H$ carries C to C'. In particular g induces an element $h \in H$. Consider any i, y with $1 \leqslant i \leqslant r^*$ and $y \in Y$, and suppose $y \in I_i$. Then the i-th block in $\mathbf{c}_y$ is $\mathbf{a}^i$, and hence the i-th block in $\mathbf{c}'_{y^h}$ has the type of $\mathbf{a}^i$. However this block is either $\mathbf{a}^i$ or $\mathbf{b}^i$, and hence it is $\mathbf{a}^i$, and $y^h \in I'_i$. It follows that h carries each I_i onto I'_i, which contradicts the choice of these sets.

We turn to (2). Consider the effect of dropping one of the rows of the matrix C, and the corresponding row of C', getting matrices D, D'. This row will lie in the i_0-th block for some $i_0 \leqslant r^*$. Fix an element $h \in H$ which carries I_i to I'_i for all $i \neq i_0$. We claim

$$\text{Corresponding columns of } D^h \text{ and } D' \text{ have the same type in } X; \tag{3}$$

it then follows that some element of $G^{|Y|}$ carries D^h to D'.

It remains to check the claim (3). Accordingly fix a column index $y \in Y$. Let $y^* = y^{h^{-1}}$, and consider the y^*-th column $\mathbf{d}_{y^*}$ of D and the y-th column

$\mathbf{d}'_y$ of D'. Then $\mathbf{d}_{y^*}$ is the y-th column of D^h, and we claim that $\mathbf{d}_{y^*}$ and $\mathbf{d}'_y$ realize the same type. For $i \neq i_0$, we have $y^* \in I_i$ iff $y \in I'_i$, and hence the i-th block of $\mathbf{d}_{y^*}$ and of $\mathbf{d}'_y$ realize the same type. For $i = i_0$ since one entry is omitted, the i-th block of $\mathbf{d}_{y^*}$ and of $\mathbf{d}'_y$ again realize the same type. As these blocks belong to a collection of jointly smoothly embedded subsets of X, G operates independently on these blocks, and the two columns realize the same type. This completes the proof of (3) and hence (2). ∎

COROLLARY 3. *Let (G, X) and (H, Y) be fixed with $G = \mathrm{Sym}(n)$ acting on $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]$ where n, k are chosen so that $n \geqslant 2k\,\mathrm{Ar}(H, \mathscr{P}(Y))$. Then*

$$\mathrm{Ar}(G \wr H, X^Y) \geqslant \mathrm{Arg}\left(G, \begin{bmatrix} 2k \\ k \end{bmatrix}\right) \cdot \mathrm{Ar}(H, \mathscr{P}(Y)).$$

Actually we will compute the arity of $(\mathrm{Sym}(n), \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right])$ and see that it is independent of n for $n \geqslant 2k$ and hence we can put this in the more striking form

$$\mathrm{Ar}(G \wr H, X^Y) = \mathrm{Ar}(G, X) \cdot \mathrm{Ar}(H, \mathscr{P}(Y)).$$

More generally, when (G, X) contains a large enough smoothly embedded collection of sets (X_i) such that $\mathrm{Ar}(G, X) = \mathrm{Ar}(G^{X_i}, X_i)$ for all i, then the upper bound given in Theorem 1 is in fact the arity of the power action of the wreath product. This condition is more likely to be met with in "combinatorial" contexts than in linear actions where a dimension parameter would be expected to contribute to the arity in a way that cardinalities do not. In any case, this condition on (G, X) is the "roominess" condition referred to in the introduction.

We give one more rather specialized lower bound which may not look very strong but actually is quite sharp (and which can be iterated in some situations).

PROPOSITION 4. *Let (G, X) contain a smoothly embedded pair of subsets X_0, X_1, with $\mathrm{Ar}(G^{X_1}, X_1) \geqslant 2$ (in other words, G^{X_1} does not reduce to the identity). Let Y be a set of even order $2d$ and let H be a permutation group on Y containing $\mathrm{Sym}(d) \wr \mathrm{Sym}(2)$ acting naturally with respect to some decomposition of Y into two sets Y_1, Y_2 of size d. (We are thinking primarily of the case in which $H = \mathrm{Sym}(2d)$, but this generalization costs nothing.) Then*

$$\mathrm{Ar}(G \wr H, X^Y) \geqslant \mathrm{Ar}(G \wr \mathrm{Sym}(d), X_0^d) + 2.$$

Proof. Let $r = \mathrm{Ar}(G \wr \mathrm{Sym}(d), X_0^d)$ and fix r-tuples $\mathbf{a}$, $\mathbf{b}$ in X_0^d with distinct types but with the same $(r-1)$-type. We may think of $\mathbf{a}$ and $\mathbf{b}$ as $r \times d$

matrices with entries in X. It then makes sense to think of them as forming a new matrix **ab** when placed side by side, whose rows may be construed as elements of X^Y. Let $\mathbf{c} = \mathbf{ab}$ in this sense, that is view $\mathbf{c}$ as an r-tuple of elements of X^Y.

Now extend $\mathbf{c}$ as follows. Pick distinct elements e, e' of X_1 lying in the same G-orbit and let $\hat{e}$ be the constant element of X^Y with value e. Finally, let $\hat{e}_i \in X^Y$ be defined for $i = 1, 2$ as the sequence with value e' on Y_i and e on $Y - Y_i$. Let $\mathbf{d}^i = \mathbf{c}, \hat{e}, \hat{e}_i$, an $(r+2)$-tuple in X^Y for $i = 1, 2$. These two $(r+2)$-tuples have distinct types by construction; to carry one to the other it would be necessary to interchange Y_1 and Y_2, which would force the columns of **a** and **b** to realize the same types though not necessarily in the same order. As by assumption $\mathrm{Sym}(d)$ acts on Y_1 and Y_2, it would follow that **a** and **b** realize the same types, a contradiction.

To conclude it will therefore suffice to check that $\mathbf{d}^1$ and $\mathbf{d}^2$ will realize the same type after a single row is omitted from both sequences. There are two possibilities to consider: the row omitted is one of the first r, or one of the last two, and in either case the claim is clear. ▮

3. Power Set Actions and k-Sets

In the previous section we saw that the arity of a wreath product $(G \wr H, X^Y)$ is controlled, to a large extent, by the arity of the induced power set action $(H, \mathscr{P}(Y))$. We would prefer to express this in terms of the arity of (H, Y), but this is not possible. For example, when H is the full symmetric group it has arity 2 in its natural action but we will see that the arity goes to infinity logarithmically in the size of Y in the power action. On the other hand any action of a cyclic group of prime order has height 1 and hence (by Lemma 1.5) has arity $\leqslant 2$. Varying the prime and taking, say, the regular representation gives a series of primitive group actions of unbounded degree for which the arity of the induced action on the power set is bounded. It is of course true that the power set action has arity at least that of the original action, since the original action occurs as one of the orbits in the induced action.

There are two extreme cases which deserve special attention. If $H = (1)$ then the power X^Y is the ordinary power which is normally used in algebra and model theory. As the arity of H will be 1 in its action on any set with more than one element, here Theorem III tells us that $\mathrm{Ar}(G \wr H, X^Y) = \mathrm{Ar}(G, X)$. At the other extreme take $H = \mathrm{Sym}(Y)$; then $(G \wr H, X^Y)$ may be called the "symmetric power" of (G, X) by Y. We will give an explicit computation of $\mathrm{Ar}(\mathrm{Sym}(Y), \mathscr{P}(Y))$ in a form which also gives the arities of the individual orbits $(\mathrm{Sym}(Y), [\begin{smallmatrix} Y \\ k \end{smallmatrix}])$; this gives an interesting family of primitive representations for which the arity is known exactly. The results of the previous section will then give rather decent estimates (asymptotically excellent) on the arities of symmetric powers of k-set actions; here our precise numerical information will be used twice, once in the factors and once on the power set of Y. These latter results will be given in the following section. The present section will conclude with some comments on the general case of the power set representation, an area in which it would be useful to have more incisive results of some generality.

In the present section we adopt the following notation. If K is a subset of $\{1, ..., n\}$, we will write $[{n \atop K}]$ for $\dot{\bigcup}_{k \in K} [{n \atop k}]$. As we are interested in the action of Sym(n) on $[{n \atop K}]$, we may always restrict ourselves to values with $2k \leqslant n$, since for any $k \in K$ we may replace k by $n-k$, replacing each set by its complement, and obtain an equivalent permutation group. One might object that it is possible that both k and $n-k$ already belong to K; in this case we may omit one of these indices, and the arity of the resulting permutation group will not be affected, though since some points are omitted this representation will not be "equivalent" to the original one according to the usual definitions. To see that the arity is not affected by the removal of "duplicate" points, recall that only nondegenerate types in the sense of §1 need be considered, so that when two elements of X have the same stabilizer in G they may be identified. For similar reasons the case $k=0$ may be excluded without loss of generality. As we have indicated, we are interested in just two cases: K is a singleton, and we compute the arity of (Sym(n), $[{n \atop k}]$); or K consists of all k (with $k \leqslant n$ or $1 \leqslant k \leqslant n/2$, as one prefers) in which case we get the arity of (Sym(n), $\mathscr{P}(n)$). In particular when we examine symmetric powers $[{n \atop k}]^d$ we will be interested in both cases.

Example. We get a lower bound on the arity from a specific example. Let n and k be fixed with $2k \leqslant n$ and let $r = 1 + [\log_2 k]$. Let Ω be a set of size n, let $A \subseteq \Omega$ have order 2^r, and let $A' \subseteq \Omega - A$ have order $k - 2^{r-1}$. Identify A with the set of strings in $\{0, 1\}^r$. For $1 \leqslant i \leqslant r$ let A_i be the set of strings in A whose i-th coordinate is 1, and let A_{e} and A_{o} be the sets of strings in A with an even or odd number of nonzero entries, respectively. Let $B_i = A_i \cup A'$, $B_{\mathrm{e}} = A_e \cup A'$, $B_{\mathrm{o}} = A_{\mathrm{o}} \cup A'$.

Let $\mathbf{a} = (B_1, ..., B_r, B_{\mathrm{e}})$ and $\mathbf{b} = (B_1, ..., B_r, B_{\mathrm{o}})$. We claim that $\mathbf{a}$ and $\mathbf{b}$ have the same r-type and distinct $(r+1)$-types.

Let σ_i be the element of Sym(Ω) which takes a string in A to the same string with its i-th bit altered, and which is the identity off A. Then σ_i carries B_j to itself for $j \neq i$ and switches B_{e} and B_{o}. From this it follows that $\mathbf{a}$ and $\mathbf{b}$ have the same r-type in (Sym Ω, $[{\Omega \atop k}]$). On the other hand, any element of Sym Ω which carries B_i to itself for every $i \leqslant r$ must fix A pointwise, and hence cannot switch B_{e} and B_{o}. Thus $\mathbf{a}$ and $\mathbf{b}$ have distinct types in (Sym Ω, $[{\Omega \atop k}]$).

PROPOSITION 1. *Let K be a set of indices with $1 \leqslant k \leqslant n/2$. Then the arity of* $(\mathrm{Sym}(n), [{n \atop K}])$ *is at least* $2 + [\log_2 \sup K]$.

In fact:

THEOREM 2. *Let K be a set of indices k with $1 \leqslant k \leqslant n/2$. Then the arity of* $(\mathrm{Sym}(n), [{n \atop K}])$ *is* $2 + [\log_2 \sup K]$. *In particular*:

(1) $\mathrm{Ar}(\mathrm{Sym}(n), [{n \atop k}]) = 2 + [\log_2 k]$ *for* $1 \leqslant k \leqslant n/2$;

(2) $\mathrm{Ar}(\mathrm{Sym}(n), \mathscr{P}(n)) = 1 + [\log_2 n]$; *here $\mathscr{P}(n)$ is the set of all subsets of* $\{1, ..., n\}$.

Proof. We know $\mathrm{Ar}(\mathrm{Sym}(n), [{n \atop K}]) \geqslant 2 + [\log_2 \sup K]$ and we will prove the reverse inequality.

Given two r-tuples $\mathbf{a}$, $\mathbf{b}$ in $[{n \atop K}]$, let A and B be the boolean algebras they generate, and let B_r be the free boolean algebra on r generators $c_1, ..., c_r$. Let $f\colon B_r \to A$ and $g\colon B_r \to B$ be the homomorphisms induced by $f(c_i) = a_i$ and $g(c_i) = b_i$, respectively. Then $\mathbf{a}$ and $\mathbf{b}$ realize the same type if and only if for each atom $\alpha \in B_r$, $f(\alpha)$ and $g(\alpha)$ have the same cardinality. This is because a permutation of $\{1, ..., n\}$ that carries $\mathbf{a}$ to $\mathbf{b}$ is a disjoint union over the atoms $\alpha \in B_r$ of bijections from $f(\alpha)$ onto $g(\alpha)$.

It may also be useful to have a more explicit notation for the atoms of B_r. For $c \in B_r$ let c^1 be c and c^{-1} be the complement of c. There is a bijection α between $\{\pm 1\}^r$ and the atoms of B_r given by $\alpha(\varepsilon) = \bigcap_i c_i^{\varepsilon_i}$ for $\varepsilon \in \{\pm 1\}^r$.

Now let $k = \sup K$. We claim that for $r > 1 + [\log_2 k]$, r-types determine $(r+1)$-types. With r fixed, we consider the graph Γ_r whose vertices are the atoms of B_{r+1}, with edges between atoms whose codes in $\{\pm 1\}^{r+1}$ differ in one place. We label such an edge with the union of the atoms associated to its vertices. Observe that if $\varepsilon, \varepsilon' \in \{\pm 1\}^{r+1}$ differ in the i-th position then the label on the corresponding edge may be interpreted as an atom in the algebra generated by the c_j with $j \neq i$.

Now consider two $(r+1)$-tuples $\mathbf{a}$, $\mathbf{b}$ with the same r-type, where $r > 1 + [\log_2 k]$. Let A, B be the boolean algebras generated by the entries in $\mathbf{a}$ and in $\mathbf{b}$ respectively. Let Γ_r^A be the labelled graph in which every vertex and edge of Γ_r is labelled by the cardinality of the corresponding element of A, and define Γ_r^B analogously. Our claim is that $\mathbf{a}$ and $\mathbf{b}$ have the same type, or in other words that the vertex labels in Γ_r^A and Γ_r^B coincide.

As $\mathbf{a}$ and $\mathbf{b}$ have the same r-type, the edge labels coincide in Γ_r^A and in Γ_r^B respectively. Furthermore the graph Γ_r is connected, and if two vertices are joined by an edge then the sum of their labels is the label of that edge. Accordingly, to prove that the vertex labels in Γ_r^A and in Γ_r^B coincide, it suffices to find one vertex at which these labels coincide.

Consider the 2^{r-1} edges of Γ_r that correspond to atoms in the algebra generated by $c_1, ..., c_r$, for which $\varepsilon_1 = 1$. The images of these atoms under f are 2^{r-1} disjoint subsets of a_1, which has at most k elements. Since $2^{r-1} > k$, at least one of these sets is empty, and hence one of these edges is labelled 0 in Γ_r^A and hence also in Γ_r^B. It follows that both vertices adjacent to this edge are labelled 0 in Γ_r^A and in Γ_r^B, and this completes the argument. ▮

We conclude this section with some further general observations about arities of power set actions.

One source of power set actions of bounded arity comes by considering the *height* of the representation as defined in §1. A case in which the height is certainly bounded, independently of the particular permutation group under consideration, is that in which H varies over the set of groups whose subgroup lattice has height less than some specified bound. (It is quite easy to prove that the height of a permutation group is at most the height of the subgroup lattice of the abstract group.) This is equivalent to the condition that the order of H has a bounded number of prime factors (with multiplicities).

LEMMA 3. *Let $\mathscr{A}$ be a collection of finite groups. Then the following are equivalent*:

(1) *The subgroup lattices of the groups in $\mathscr{A}$ have bounded height*;

(2) *There is a bound on the number of prime divisors* (*with multiplicities*) *of the orders of groups in $\mathscr{A}$*.

Proof. The height of the subgroup lattice of G is bounded by the number of prime divisors of the order of G. For the converse, given a bound h on the height of the subgroup lattice of G, we have a bound on the length of a composition series and the height of the subgroup lattice in each factor. So the problem reduces to the case in which the groups in $\mathscr{A}$ are simple and nonabelian.

For solvable groups H the height of the subgroup lattice equals the number of prime factors of the order of H, with multiplicities. In particular this applies to sylow subgroups of groups $G \in \mathscr{A}$. Accordingly it is enough to bound the number of distinct primes dividing $|G|$.

As there are only finitely many sporadic groups they may be ignored, and the alternating group presents no difficulty. So we consider groups $G = G(n, q)$ of Lie type, possibly twisted. A bound on the rank n may be obtained by considering the Weyl group. Accordingly we may suppose that the Lie type and the rank are fixed, and only the base field $\mathbb{F}_q$ varies.

For $G \in \mathscr{A}$, any element of prime order p with $p \nmid q$ is semisimple, and lies in a maximal torus. The number of conjugacy classes of maximal tori is the same as the number of conjugacy classes in the Weyl group [2, § E]. As each torus is abelian, the number of primes dividing the order of each torus is bounded by h. So we have a bound on the total number of distinct primes dividing $|G|$. ∎

One may expect that "generically", chains of maximal length in subgroup lattices of groups of Lie type will pass through Borel subgroups; this would produce much tighter estimates above. Cf. [12] and the references cited therein.

These examples show that one can form very "wide" wreath products of permutation groups without appreciably increasing the arity. For example, if one forms the family of wreath product actions of (G, X) by (H, Y), where the (G, X) ranges over a family of representations and (H, Y) ranges over a family of representations of unbounded degree for which $\mathrm{Ar}(H, \mathscr{P}(Y))$ is bounded, then $\mathrm{Ar}(G \wr H, X^Y)$ is at most a bounded multiple of $\mathrm{Ar}(G, X)$.

When looking for other possibilities for families of representations whose induced power set actions have bounded arity, it is natural to consider the power set action induced by the action of $\mathrm{Sym}(n)$ on $[{n \atop k}]$ with k fixed. However, this succumbs to a fairly general constraint for n large: the presence of too many "indiscernibles", defined as follows.

DEFINITION. A set $I \subseteq X$ is *indiscernible* in the representation (G, X) if $G^I = \mathrm{Sym}(I)$.

For a general result on the existence of indiscernibles in primitive groups see [5]. When one has a set of d indiscernibles then the power set representation induces $(\mathrm{Sym}(d), \mathscr{P}(d))$ on the corresponding subset, and the arity of this is unbounded.

For natural linear representations of classical groups arity tends to go up with the dimension. The rule of thumb which says that the "n" in $\mathrm{Sym}(n)$ can be identified with, e.g., the "n" in $\mathrm{GL}(n, q)$, goes rather badly awry here.

4. THE ACTION OF $\mathrm{Sym}(n)$ ON $[{n \atop k}]^d$

The remainder of this paper is devoted to the study of the arity of power representations of wreath products of symmetric groups on $[{n \atop k}]^d$. In particular $(H, Y) = (\mathrm{Sym}(d), \{1, ..., d\})$ throughout. Most of the results of previous sections bear on this case. Specializing the main facts proved above to this particular case, we will obtain:

THEOREM IV B. *$\mathrm{Ar}[{n \atop k}]^d \leqslant [2 + \log_2 k][1 + \log_2 d]$ with equality if $n \geqslant 2k[1 + \log_2 d]$.*

We will also illustrate the use of our previous results in a case not settled by Theorem IV B. The main gap in our knowledge concerns the behavior of $\mathrm{Ar}([{n \atop k}]^d)$ for n, k fixed and d variable, especially for $k>1$. For $k=1$ we will give more precise information in §6 together with some very precise conjectures.

We begin by restating Theorem III.

PROPOSITION 1.

$$\max([2+\log_2 k], [1+\log_2 d]) \leqslant \mathrm{Ar}\left(\begin{bmatrix} n \\ k \end{bmatrix}^d\right) \leqslant [2+\log_2 k] \cdot [1+\log_2 d].$$

The lower bound in Theorem 2.2 is easily computed explicitly but is somewhat harder to write as a formula. The statement becomes:

PROPOSITION 2. *Let (n_i) be a collection of at most $[1+\log_2 d]$ numbers whose sum is at most n. Then*

$$\mathrm{Ar}\left(\begin{bmatrix} n \\ k \end{bmatrix}^d\right) \geqslant \sum \mathrm{Ar}\left(\begin{bmatrix} n_i \\ k \end{bmatrix}\right).$$

Here we did not apply the formula for $\mathrm{Ar}([{n_i \atop k}])$ because, as we will see, there may be good reasons for taking $n_i<2k$. However to a first approximation the essential information is obtained by taking $n_i=2k$, in which case we may say:

COROLLARY 3. *Let $r=[\inf(1+\log_2 d, n/2k)]$. Then $\mathrm{Ar}([{n \atop k}]^d) \geqslant r[2+\log_2 k]$.*

In particular:

COROLLARY 4. *For $n \geqslant 2k[1+\log_2 d]$, $\mathrm{Ar}([{n \atop k}]^d) = [2+\log_2 k][1+\log_2 d]$.*

Proposition 1 and Corollary 4 yield Theorem IV B.

There is a clearcut way to exploit Proposition 2 more thoroughly. There are two sorts of numerical improvements that can be made relative to the statement in Corollary 3, entirely within the framework provided by Proposition 2. Firstly, since the arity of $[{n \atop k}]$ is $[2+\log_2 k]$ we may as well take $n_i=k+2^{[\log_2 k]}$, rather than $2k$, and secondly, we can make some use of the remainder after division by this number.

EXAMPLE. We illustrate all this with a detailed example. Consider $[{52 \atop 7}]^{16}$. The upper bound given by Proposition 1 is $\mathrm{Ar}([{52 \atop 7}]^{16}) \leqslant 4 \cdot 5 = 20$. We will examine several lower bounds given by Proposition 2, of which the best will be $18 \leqslant \mathrm{Ar}({52 \atop 7}]^{16})$. This is impressively close to the upper bound, but only because 52 is close to 55, where the upper bound becomes exact; this is because we can strengthen Corollary 4—it is enough to have $n \geqslant (k+2^{[\log_2 k]})[1+\log_2 d]$, using the stronger form of Corollary 3.

In applying Proposition 2, since $1+\log_2 d = 5$ we may obtain a lower bound from at most five numbers adding up to at most 52. The estimate given in Corollary 3 is $3 \cdot 4 = 12$, based on $n_1 = n_2 = n_3 = 14$. However as noted we can also use $n_1 = n_2 = n_3 = n_4 = 11$, even though $11 < 2 \cdot k$, to get four (instead of three) blocks with arity 4; this yields a lower bound of $4 \cdot 4 = 16$. Furthermore we can go a step further with $n_5 = 8$ and get an additional $\mathrm{Ar}([\begin{smallmatrix} 8 \\ 7 \end{smallmatrix}]) = 2$; so our lower bound becomes 18.

Our feeling, which is supported by the limited numerical evidence available, is that the natural lower bounds are close to the truth. Our detailed study of the case $k=1$ in §6 will show that the situation is quite complicated. We propose:

Problem. With n, k fixed determine

$$\lim_{d \to \infty} \mathrm{Ar}\left(\begin{bmatrix} n \\ k \end{bmatrix}^d\right) \Big/ (1+\log_2 d).$$

We conjecture that this limit is 1. In the case $k=1$ we conjecture also that $\mathrm{Ar}([\begin{smallmatrix} n \\ k \end{smallmatrix}]^d) - (1+\log_2 d) \sim n/2$ as $n,\ d \to \infty$, within the range $2 \leqslant n \leqslant 2[1+\log_2 d]$.

In the next section we will compute the arity of 2^d explicitly and show that it is near to the theoretical lower bound, but always even (hence frequently slightly bigger). The technique used to analyze 2^d involves linear algebra and will be used to get strong lower bounds in other cases.

Before we enter into this, however, we will discuss the "propagation" of lower bounds on arity. Our first remark is quite evident, but obviously important in this context.

LEMMA 5. *If $n_1 \leqslant n_2$, and $d_1 \leqslant d_2$ then* $\mathrm{Ar}([\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]^{d_1}) \leqslant \mathrm{Ar}([\begin{smallmatrix} n_2 \\ k \end{smallmatrix}]^{d_2})$.

Proof. Take a pair of r-tuples $\mathbf{a}$ and $\mathbf{b}$ in $[\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]^{d_1}$ realizing the same $(r-1)$-type and distinct types. Extend them first to r-tuples $\mathbf{a}'$ and $\mathbf{b}'$ in $[\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]^{d_2}$ by adjoining the same $d_2 - d_1$ elements of $[\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]$ to each of the given elements of $[\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]^{d_1}$. Then take a natural embedding of $[\begin{smallmatrix} n_1 \\ k \end{smallmatrix}]^{d_2}$ into $[\begin{smallmatrix} n_2 \\ k \end{smallmatrix}]^{d_2}$. The key to seeing that $\mathbf{a}'$ and $\mathbf{b}'$ realize distinct types is that an r-type in a wreath product is determined by specifying, for each r-type in the base structure, in how many coordinates that type is realized. ∎

Our second result in this vein has considerably more content. It is Proposition 2.4 applied to the case at hand.

PROPOSITION 6. $\mathrm{Ar}(\genfrac{}{}{0pt}{}{n+k+1}{k}]^{2d}) \geqslant \mathrm{Ar}([\genfrac{}{}{0pt}{}{n}{k}]^d)+2$.

The lower bounds we considered earlier would normally behave in the same fashion: $\log_2(2d) = 1 + \log_2 d$, and hence we can take one more term n_i in the application of Proposition 2. Viewing $n+k+1$ as n plus $(k+1)$, with $(k+1)$ as the additional term, this means we are adding 2 to our previous estimate. In such a case, if our estimate for $\mathrm{Ar}([\genfrac{}{}{0pt}{}{n}{k}]^d)$ was too low then the estimate for $\mathrm{Ar}([\genfrac{}{}{0pt}{}{n+k+1}{k}])^{2d})$ is off by at least the same amount.

Let us now examine what becomes of all of this when we specialize further by setting $k=1$. In this case we are just considering $(\mathrm{Sym}(n) \wr \mathrm{Sym}(d), n^d)$ which we tend to refer to simply as n^d. In this case we arrive at:

PROPOSITION 7. (1) $[1+\log_2 d] \leqslant \mathrm{Ar}(n^d) \leqslant 2 \cdot [1+\log_2 d]$;

(2) $\mathrm{Ar}(n^d) = 2[1+\log_2 d]$ *for* $n \geqslant 2[1+\log_2 d]$;

(3) $\mathrm{Ar}(n^d) \geqslant 2[n/2]$ *for* $n \leqslant 2[1+\log_2 d]$;

(4) $\mathrm{Ar}((n+2)^{2d}) \geqslant \mathrm{Ar}(n^d)+2$.

In (1) we are supposed to write $\max(2, [1+\log_2 d])$ for the lower bound (we have assumed $n>1$, more generally $n \geqslant 2k$), which only matters for $d=1$. The above relations and the trivial Lemma 5 exhaust the results proved up to this point for $k=1$. Notice that an application of (4), starting with $\mathrm{Ar}(2^1)=2$, yields the less trivial relation $\mathrm{Ar}(4^2) \geqslant 4$, which is the ancient observation that although 3^2 can be thought of as a homogeneous graph, 4^2 cannot.

Let us trace through this example in more detail, from the point of view of the proof of (4). We take 00 and 01 as pairs in 2 (i.e., 2^1) with the same 1-type and distinct 2-types. We form the matrix

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

whose columns are the given pairs. We then extend this matrix by the two rows 22 and either 23 or 32 which look much like the first two pairs, but in the context of the proof of Proposition 2.4 play quite a different role. We assemble these ingredients into the two arrays

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \\ 3 & 2 \end{pmatrix}.$$

The rows here represent distinct 4-types in 4^2 with the same 3-types. This is the standard example, and in fact the only example available in this context: in the graph picture, drawn as a grid, we have two disjoint edges, parallel in the first case and not parallel in the second.

We will use this example in the next section to illustrate the application of linear algebra to these problems. Using this technique we will determine the arity of 2^d exactly. However the information recorded so far leaves the matter open, for d fixed, with n in the range $2 \leqslant n \leqslant 2[1+\log_2 d]$, while offering two competing lower bounds, one a function of d alone, the other a function of n alone. For $n \leqslant [1+\log_2 d]$ the former is the better bound, and for $n > [1+\log_2 d]$ the latter gives the best information. At $n = [1+\log_2 d]$ the bounds agree if this number is even.

5. The Arity of 2^d

We will compute the arity of 2^d for all d by reducing the problem to a simple problem in linear algebra. In the following section we will use the same technique to get lower bounds on the arity of n^d in general. We conjecture that the lower bounds obtained are in fact the exact values. This method could work for $k > 1$ as well, but the systems involved become large quite rapidly, and it is more promising to look directly for a combinatorial generalization of the case $k = 1$.

To illustrate the method, we recall the example given at the end of the previous section, which demonstrates that $\mathrm{Ar}\, 4^2 \geqslant 4$. This was

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \\ 2 & 2 \\ 3 & 2 \end{pmatrix}.$$

The point of this example, as we know, is that there is no element of Sym-(4) $\wr$ Sym(2) which takes one matrix to the other, but if any row is omitted from both matrices then such an element exists. This means that the unordered pair of 4-types realized by the columns of the first matrix is different from the unordered pair of 4-types realized by the columns of the second matrix, but that the restrictions of these pairs by omitting the i-th entry systematically, for any fixed i, agree. This can be said more simply if we consider how the type of a column may be described. The only information in a column is the pattern of equalities occurring. That is, each column imposes an equivalence relation on the index set $\{1, 2, 3, 4\}$: two indices are equivalent if the corresponding entries in the column are equal. With this definition we have the following key relationship:

> Two columns have the same type if and only if they induce the same equivalence relation on $\{1, 2, 3, 4\}$.

In the case at hand, the first matrix has columns $[0, 0, 2, 2]$ and $[0, 1, 2, 3]$ corresponding to the equivalence relations:

$$(1, 2)(3, 4) \qquad \text{and} \qquad (1)(2)(3)(4).$$

The second matrix has columns $[0, 0, 2, 3]$ and $[0, 1, 2, 2]$ corresponding to the relations

$$(1, 2)(3)(4) \qquad \text{and} \qquad (1)(2)(3, 4).$$

Here we have four distinct equivalence relations, which we will call E_1, E_2, E'_1, and E'_2 respectively; so the types involved are certainly distinct. Now let us consider what happens if we omit, say, the second row in both matrices. The effect is to drop out the index 2 from the domain of the equivalence relations. In this case E_1 and E'_2 restrict to $(1)(3, 4)$ while E_2 and E'_1 restrict to $(1)(3)(4)$. So we see that this is a very efficient notation for checking examples. However it is much more than that.

We will now describe the method somewhat more generally for n, d arbitrary, but still taking $k=1$. The problem is best viewed as one of determining, for a fixed r, the pairs n, d for which $(r-1)$-types determine r-types in n^d, and more specifically: for fixed r, to give a list of all minimal pairs (n, d) for which $(r-1)$-types do *not* determine r-types in n^d. For example for $r=4$ this list is: $(2, 4)$; $(4, 2)$; $(3, 3)$.

To any r-tuple $\mathbf{a}$ in n^d we associate the following invariant. Let $I=\{1, ..., r\}$. Thinking of $\mathbf{a}$ as usual as an $r \times d$ matrix (a_{ij}) with entries in $\Omega=\{1, ..., n\}$, then as suggested above we will associate to the j-th column the equivalence relation E_j on I defined by

$$E_j(i_1, i_2) \text{ iff } a_{i_1, j} = a_{i_2, j},$$

and we will attach to $\mathbf{a}$ the multiset (set with multiplicities) $\mathscr{E}(\mathbf{a}) := \langle E_1, ..., E_d \rangle$. This invariant characterizes the type of $\mathbf{a}$. Furthermore the $(r-1)$-type of $\mathbf{a}$ is characterized by the ordered sequence of invariants $\mathscr{E}_i = \mathscr{E} \upharpoonright (I - \{i\})$, where the restriction of a multiset of equivalence relations is defined as the multiset consisting of the restrictions of the given relations. In this notation

d is the number of equivalence *relations*;

n is a bound on the number of *classes* of each relation.

So at this stage our problem is:

Problem. For what values of n, d, r are there two distinct multisets $\mathscr{E}$, $\mathscr{E}'$ of total multiplicity d whose elements are equivalence relations on a set

I of cardinality r, where each relation has at most n classes, such that the restrictions $\mathscr{E}_i$, $\mathscr{E}'_i$ of $\mathscr{E}$, $\mathscr{E}'$ to $I-\{i\}$ coincide for all $i \in I$?

We will now reformulate this problem as one of determining the shortest nonzero vector in the l^1-norm in an appropriate integer lattice.

With r fixed, we consider the collection $\mathbf{E}_r$ of equivalence relations E on the set $\{1, ..., r\}$. Any r-type in n^d will correspond exactly to a multiset of such equivalence relations, with d the cardinality of the multiset and with n a bound on the number of classes occurring in any of the relations. Let V_r be the rational vector space with basis $\mathbf{E}_r$. Its dimension, the number of relations in $\mathbf{E}_r$, is called the rth *Bell number* and is denoted B_r. The l^1-norm of a vector is the sum of the absolute values of its coefficients with respect to the distinguished basis. Each multiset $\mathscr{E}$ of relations in $\mathbf{E}_r$ is determined by its characteristic function, the vector in V_r whose Eth coordinate is the multiplicity of E in $\mathscr{E}$. To an ordered pair of multisets we associate the difference of their characteristic vectors. We are only interested in pairs of disjoint multisets; such pairs may be recovered unambiguously from their associated vectors. Furthermore when two disjoint multisets have the same cardinality d, this is half the l^1-norm of the associated vector.

The condition on equality of restrictions of the two multisets is a linear condition on the associated vectors. Thus these vectors form an integer lattice L_r in V_r and the restriction to equivalence relations with at most n classes defines a sublattice $L_{r,n}$. Our problem is to find the length of the shortest nonzero vector in each of these lattices, with respect to the l^1-norm. We found it useful to gather some data by machine computation in these lattices for $r \leqslant 7$. This is discussed in some detail in [4], and we will just say a few words about it here.

The dimension of L_r was computed in [4]. It is an alternating sum of Bell numbers $\sum_{i=0}^{r-1} (-1)^i B_{r-1-i}$. This is also the number of equivalence relations on r elements having no singleton equivalence class, and it is possible to write down a sparse basis for L_r with coefficients of moderate size, parametrized naturally by the set of all such equivalence relations. Since this basis can be defined combinatorially, it is invariant under the natural action of $\mathrm{Sym}(r)$. We emphasize these points because the dimensions involved are rather large and these properties are therefore computationally significant; for example when $r=7$ we are computing in a lattice of rank 162 inside a space of dimension 877, and we have been led to make computations out to a radius of $d=45$ in some cases (making use of a simple heuristic in such cases to speed up the search for examples). More details will be found in [4]. The rôle played by such computations in suggesting general patterns will be indicated in the following section.

TABLE I

A Basis for L_4

$$
\begin{array}{l}
[\ \ 1\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ -1\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ ] \\
[\ \ 1\ \ 0\ \ -1\ \ 0\ \ 0\ \ 0\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ ] \\
[\ \ 1\ \ 0\ \ 0\ \ -1\ \ 0\ \ -1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ ] \\
[\ \ -3\ \ 1\ \ 1\ \ 1\ \ -1\ \ 1\ \ 1\ \ -1\ \ 1\ \ -1\ \ -1\ \ 0\ \ 0\ \ 0\ \ 1\ \ ].
\end{array}
$$

Example. We illustrate the foregoing with a concrete example, the case $r=4$. We begin by choosing an ordering for the basis $\mathbf{E}_4$ of V_4, exhibited here (reading across the rows):

$$
\begin{array}{lllll}
(1)(2)(3)(4), & (1)(2)(3,4), & (1)(3)(2,4), & (1)(4)(2,3), & (1)(2,3,4), \\
(2)(3)(1,4), & (2)(4)(1,3), & (2)(1,3,4), & (3)(4)(1,2), & (3)(1,2,4), \\
(4)(1,2,3), & (1,2)(3,4), & (1,3)(2,4), & (1,4)(2,3), & (1,2,3,4).
\end{array}
$$

The restriction conditions lead to a system of $20=4\cdot 5$ equations in 15 unknowns, but the rank of the system is 11 and there is a four-dimensional integer lattice L_4 of solutions. The particular basis we get is exhibited in Table I as row vectors of coefficients with respect to the ordering of $\mathbf{E}_4$ given above.

Each of the first three vectors encodes an example $(\mathscr{E}_1, \mathscr{E}_2)$, with $\mathscr{E}_i$ a pair of equivalence relations on the set $\{1, 2, 3, 4\}$, illustrating $\mathrm{Ar}(4^2)\geqslant 4$. (Here, $\mathscr{E}_1$ consists of equivalence relations for which the corresponding coefficients are positive, and $\mathscr{E}_2$ consists of equivalence relations for which the corresponding coefficients are negative.

Therefore $\mathscr{E}_1=\langle (1)(2)(3)(4),\ (1,2)(3,4)\rangle$ and $\mathscr{E}_2=\langle (1)(2)(3,4), (1,2)(3)(4)\rangle$.

The difference of the first two vectors encodes an example showing that $\mathrm{Ar}(3^3)\geqslant 4$, and the sum of all four vectors encodes an example showing that $\mathrm{Ar}(2^4)\geqslant 4$.

For the remainder of this section we deal with one simple case in which the situation can be analyzed completely: $n=2$. In this case things are sufficiently transparent that one could dispense with the linear algebra entirely.

We will use the notation $v=(v_E\colon E\in \mathbf{E}_r)$ for vectors in V_r. With r fixed, the linear condition saying that the restrictions are equal is the system of equations:

$$v_E + v_{E'} = 0 \qquad (S_r^2)$$

where E, E' vary over equivalence relations with at most two classes with a common restriction; in other words E can be converted into E' by moving an element from one class to the other. Here it is convenient to think of the degenerate relation E with only one class as having a second, empty, class to which an element can be transferred. By performing r such transfers one converts a given E back into itself by interchanging its two classes, so from the given equations one gets $v_E = (-1)^r v_E$. We conclude:

PROPOSITION 1. *In 2^d, $(r-1)$-types determine r-types for any odd r.*

On the other hand for r even it makes sense to speak of the *parity* $\operatorname{sgn} E \in \{\pm 1\}$ of an equivalence relation with (at most) two classes, as the parity of either class, and our system S_r^2 then says that for some constant m:

$$v_E = \operatorname{sgn} E \cdot m.$$

The minimum nonzero solution has $m = \pm 1$, $d = (1/4)\, 2^r = 2^{r-2}$, so we find:

PROPOSITION 2. *For r even, $(r-1)$-types determine r-types in 2^d if and only if $d < 2^{r-2}$.*

So we may conclude:

THEOREM IV A. $\operatorname{Ar}(2^d) = 2(1 + [\log_4 d])$.

The lattice $L_{r,2}$ is 1-dimensional for r even, and 0-dimensional for r odd. Parity considerations and congruences modulo 4 play a key rôle in the conjectures of the next section.

A combinatorial argument gives a somewhat different interpretation of the result. If one fixes one point of 2^d the resulting permutation group is equivalent to $(\operatorname{Sym} d, \mathscr{P}(d))$ with arity $1 + [\log_2 d]$. Hence it follows by Proposition 1.2 that $1 + [\log_2 d] \leqslant \operatorname{Ar} 2^d \leqslant 2 + [\log_2 d]$. For a fixed value of $[\log_2 d]$ our method of computing the arity actually shows that there is essentially a unique pair of $(1 + [\log_2 d])$-types available to prove the lower bound. Hence there is a unique candidate in 2^d available to demonstrate $\operatorname{Ar}(2^d) > 1 + [\log_2 d]$ and one finds that when $[\log_2 d]$ is even this candidate works, while for $[\log_2 d]$ odd it fails. Our other approach, via linear algebra, has been more useful to date.

6. THE ARITY OF n^d

In dealing with $r = \operatorname{Ar}(n^d)$ it is easier to analyze the behavior of d as a function of r and n. This remark is implicit in the discussion of the previous section. There is more than one way to set this up, and we prefer the following definition.

DEFINITION. For $2 \leqslant n \leqslant r$ let $\delta(r, n)$ be the least d (or ∞) such that there is a pair $\mathscr{E}$, $\mathscr{E}'$ of disjoint multisets, each consisting of d equivalence relations on a set of r elements, such that:

(1) n is the maximum number of equivalence classes occurring in the relations of $\mathscr{E} \cup \mathscr{E}'$;

(2) The restrictions of $\mathscr{E}$ and $\mathscr{E}'$ to any $r-1$ elements coincide.

For the purposes of computations of arity, it makes no difference whether we take n as an upper bound on the number of equivalence classes involved, or in the stricter sense of (1). We prefer our definition in part because it brings out more clearly the difference between n even and n odd (see the conjectures below).

Computation of δ for all relevant r, n is nearly equivalent to the computation of the arity of n^d for all n, d, though in fact δ is a slightly more precise invariant. One recovers $\mathrm{Ar}(n^d)$ as the least r such that $\delta(r', n') > d$ for $r < r' \leqslant 2[1 + \log_2 d]$ and $n' \leqslant n$. In particular upper bounds on δ give lower bounds on r. In what follows we generally deal with δ directly, as the results are considerably more transparent in this form. The analysis of the case $n = 2$ in the previous section may be expressed as follows:

PROPOSITION 1.

$$\delta(r, 2) = \begin{cases} 2^{r-2} & r \textit{ even} \\ \infty & r \textit{ odd.} \end{cases}$$

In this section we will prove a number of upper bounds on δ, and hence implicitly we have corresponding lower bounds on $\mathrm{Ar}(n^d)$. In most cases we believe these lower bounds are sharp (except where they overlap).

To prove an upper bound for δ one exhibits a suitable example. Obviously the business of getting matching lower bounds should be considerably more subtle.

Since most of the results of this section are conjectured to be sharp, we express them as conjectured formulas for δ, and prove the corresponding inequalities.

Conjecture A. $\delta(r+2, n+2) = 2 \cdot \delta(r, n)$.

Here we have to make an exception for r odd, $n = 2$. One might anticipate other sporadic exceptions for small values of r and n but our machine computations suggest there are no other exceptions. (The only value that seems to have a sporadic character is $\delta(3, 3)$ and the values arising by shifting it using Conjecture A.) The corresponding inequality $\delta(r+2, n+2) \leqslant 2 \cdot \delta(r, n)$ is straightforward. Starting from a pair of multisets $\mathscr{E}$, $\mathscr{E}'$ of equivalence relations on r elements serving to demonstrate $\delta(r, n) \leqslant d$ one extends them to multisets $\hat{\mathscr{E}}$, $\hat{\mathscr{E}}'$ of equivalence relations on $r+2$ elements by adjoining two new elements a and b and letting $\hat{\mathscr{E}}$ consist of the relations of $\mathscr{E}$ extended by singleton classes $[a]$ and $[b]$ together with the relations of $\mathscr{E}'$ extended by a single class $[a, b]$, while $\hat{\mathscr{E}}'$ is defined dually. The same argument yields $\delta(r_1+r_2, n_1+n_2) \leqslant 2\delta(r_1, n_1)\, \delta(r_2, n_2)$, which in general is a weaker estimate.

The effect of Conjecture A would be to reduce the computation of δ to certain values for $n \leqslant 4$, specifically:

Conjecture A′. (1) $\delta(r, n) = 2^{(n-2)/2}\delta(r-n+2, 2)$ for r, n even.

(2) $\delta(r, n) = 2^{(n-3)/2}\delta(r-n+3, 3)$ for n odd.

(3) $\delta(r, n) = 2^{(n-4)/2}\delta(r-n+4, 4)$ for r odd, n even.

In particular formula (1) would combine with Proposition 1 to give $\delta(r, n) = 2^{r-(n/2)-1}$ for r, n even. The formulas corresponding to other values of r and n are similar, hence this upper bound on δ is conjecturally the main factor in determining the arity of n^d, Qualitatively, the result is simply that the arity of n^d should be approximately $(\log_2 d) + n/2 + 1$ within the range $n \leqslant 2[1 + \log_2 d]$. A better approximation formula is: $r = 2[\log_4 d + n/4 + 1/2]$. This matches our conjecture within the given range exactly, when d is a power of 2.

The final conjectures corresponding to formulas (2) and (3) of Conjecture A′ are a bit more elaborate. In Conjecture B we will consider only the values of $\delta(r, 3)$, and of $\delta(r, 4)$ with r odd. One can of course combine parts (2) and (3) of Conjecture A′ with Conjecture B.

Conjecture B.

$$(1)\quad \delta(r, 3) = \begin{cases} 3(2^{r-3}-1) & \text{for} \quad r \geqslant 5 \text{ odd} \\ 2^{r-1} - 2^{r-4} - 3 & \text{for} \quad r \geqslant 6 \text{ even}, r \neq 8 \\ 3 & \text{for} \quad r = 4 \\ 108 & \text{for} \quad r = 8 \end{cases}$$

$$(2)\quad \delta(r, 4) = 2^{r-2} - 1 \qquad \text{for} \quad r \geqslant s \text{ odd}$$

The value $\delta(3, 3) = 3$ seems exceptional. Our formula for $\delta(r, 3)$, $r \geqslant 5$ odd, fails badly for $r = 3$, and the real value is higher. There is another family of examples showing that $\delta(r, 3) \leqslant \frac{1}{2}(6^{r/2-1})$ for $r \equiv 0 \bmod 4$ which gives better bounds than $2^{r-1} - 2^{r-4} - 3$ when $r = 4$ and $r = 8$. We present this family generally below, rather than just the two sporadic examples.

Saracino, in a recent manuscript that is too long for inclusion here, proved that $\delta(r, 3) \geqslant 3(2^{r-3} - 1)$ for $r \geqslant 5$ odd. The argument involves careful counting and a division into three cases. We will now describe the various examples which establish the upper bounds on δ given in Conjecture B. We omit the examples for the two sporadic bounds discussed above.

Example. $\delta(r, 3) \leqslant 3(2^{r-3} - 1)$ for $r \geqslant 5$ odd.

We fix a set X with r elements and we fix two of the elements, say a and a'. We consider equivalence relations on X with two or three classes in which a and a' lie in distinct classes. To such a relation we associate the pair (m, m') consisting of the cardinalities of the classes containing a and a' respectively. We let $\mathscr{E}$ consist of the equivalence relations E with a and a' in distinct classes, such that either E has two classes and $m \leqslant r-3$ is even, or else E has three classes, and satisfies: $m = 1$ and m' is even, or $m' = 1$ and $m \geqslant 3$ is odd. We define $\mathscr{E}'$ dually. For $r \geqslant 5$ odd these two collections are disjoint and nonempty. Furthermore they have the same restrictions to any $r-1$ elements, again because r is odd. The number of relations in $\mathscr{E} \cup \mathscr{E}'$ with two classes is $2^{r-2} - 2$ and the number with three classes is $2 \cdot (2^{r-2} - 2)$. Thus each of the two collections has $3(2^{r-3} - 1)$ members.

Example. $\delta(r, 4) \leqslant 2^{r-2} - 1$ for r odd.

We take a set X consisting of a distinguished element $*$ and two sets A, A' of even cardinality $r_1 r_2$ with $r_1 + r_2 = r - 1$. Any partition of A or A' into two sets has a well-defined parity, the parity of either class. Let $\mathscr{E}_1$ be the set of partitions of X into at most four pieces arising from partitions of A and A' into at most two classes each, with $*$ adjoined to one of the nonempty classes. Let $\mathscr{E}_2$ be the set of partitions of X into exactly four pieces in which $*$ represents a singleton class, and either A or A' constitutes a single class. We will divide $\mathscr{E}_1 \cup \mathscr{E}_2$ into two sets satisfying our conditions.

In $\mathscr{E}$ we place those elements of $\mathscr{E}_1$ arising from partitions of A and A' of equal parity, with $*$ put in a class with a subset of A, together with the elements of $\mathscr{E}_1$ arising from partitions of A and A' of unequal parity, with $*$ put in a class with a subset of A'. The remaining elements of $\mathscr{E}_1$ are put in $\mathscr{E}'$. We also put into $\mathscr{E}$ the elements of $\mathscr{E}_2$ which involve a nontrivial partition of A of odd parity or a nontrivial partition of A' of even parity, with the remainder going into $\mathscr{E}'$. One checks the condition on restrictions (and eventually one sees the need for the elements of $\mathscr{E}_2$ as a result). The cardinality of $\mathscr{E}_1 \cup \mathscr{E}_2$ is $2^{r_1 + r_2} - 2 = 2^{r-1} - 2$ and the stated formula follows.

EXAMPLE. $\delta(r, 3) \leqslant 2^{r-1} - 2^{r-4} - 3$ for r even, $r \geqslant 4$.

We take a set X of r elements partitioned into a three-element set I and its complement J. We consider partitions of X into three (possibly empty) classes A, B, C, in which $A \cap I \neq \varnothing$ and either $A = I$ or $A \cap J \neq \varnothing$, $B = I - A$, and $C = J - A$. We take $\mathscr{E}$ to be those partitions for which $|A|$ is even, and $\mathscr{E}'$ to be those for which $|A|$ is odd. It is straightforward to check that $|\mathscr{E}| = |\mathscr{E}'| = 2^{r-1} - 2^{r-4} - 3$.

In checking the restriction condition, we distinguish the cases where the omitted element x is in I from those where it is in J. In each case, we define a map σ from $\mathscr{E} \cup \mathscr{E}'$ into itself which it is easy to check is a bijection between $\mathscr{E}$ and $\mathscr{E}'$. Given a partition E into classes A, B, C, the partition $\sigma(E)$ into classes A', B', C' is completely determined by specifying A'. In the former case, we take

$$A' = \begin{cases} A \cup \{x\} & \text{if} \quad x \in B \\ A - \{x\} & \text{if} \quad x \in A \text{ and either } |B| = 1 \text{ or both } B = \varnothing \text{ and } A \neq I \\ C \cup \{x\} & \text{if} \quad x \in A \text{ and either } A = I \text{ or both } |B| = 2 \text{ and } C \neq \varnothing \\ B \cup \{x\} & \text{if} \quad x \in A,\ |B| = 2, \text{ and } C = \varnothing. \end{cases}$$

In the latter case, we take

$$A' = \begin{cases} A - \{x\} & \text{if} \quad x \in A \text{ and either } |A \cap J| \geqslant 2 \text{ or } A = I \cup \{x\} \\ B \cup \{x\} & \text{if} \quad A - I = \{x\} \\ A \cup \{x\} & \text{if} \quad x \in C. \end{cases}$$

We are grateful to James Schmerl for providing this example in a private communication.

EXAMPLE. $\delta(r, 3) \leqslant \frac{1}{2}(6^{r/2-1})$ for $r \equiv 0 \bmod 4$.

We take a set X of cardinality r divided into $r/2$ disjoint pairs. We consider the partitions of X into at most three classes such that no distinguished pair belongs to any class. The number of such partitions is $6^{r/2-1}$ since after fixing one pair we can distinguish the three classes of the partition (one of which may be empty) and each of the remaining pairs can then be distributed among the classes in six ways. For $r/2$ even it remains to be seen that these partitions can be divided into two classes which agree when restricted to any subset omitting one element.

Call the class of partitions under consideration $\mathscr{E}_r$. For each element $x \in X$ there is an involution without fixed point ι_x acting naturally on $\mathscr{E}_r$ as follows: for each $E \in \mathscr{E}_r$ there is a unique element $E' \in \mathscr{E}_r$ agreeing with E modulo x but distinct from E. It is easy to see that if $x, y \in X$ are paired then these involutions generate a copy of Sym(3) and that all of them together generate the product of $r/2$ copies of Sym(3) acting transitively on $\mathscr{E}_r$. We note that the third involution in each copy of Sym(3) acts by interchanging the locations of x and its mate. Let $G = \langle \iota_x : x \in X \rangle$ be the resulting group. There is a natural map $G \to \mathbb{Z}_2$, the composite $G \simeq \mathrm{Sym}(3)^{r/2} \to \mathbb{Z}_2^{r/2} \to \mathbb{Z}_2$ where the last map is the parity map on bit strings; an element of G will be called even or odd depending on its image under this map. All that needs to be checked now is that the stabilizer of a point consists of even elements of G, so that $\mathscr{E}_r$ inherits a notion of parity. More exactly, we may say that two elements of $\mathscr{E}_r$ have the same parity if some even $g \in G$ takes one element to the other. The involutions ι_x interchange the two parity classes in $\mathscr{E}_r$.

In computing the stabilizer of an element of $\mathscr{E}_r$ one may work with any element one prefers; a partition into two classes is a convenient choice. In any case one finds that the stabilizer is a certain diagonal copy of Sym(3), and as $r/2$ is even it consists entirely of even elements of G.

This completes the verification of our upper bounds for δ. As we have indicated, these conjectures are based on what seem to be the natural generalizations of the examples found computationally. While it would not be surprising to discover that another infinite series of examples requires a revision of the conjectures, we do think it very likely that a conjecture of at least the same general character will prove correct.

Table II shows what the arities of n^d would look like if all conjectures in this section were correct.

The following result shows that from one point of view these estimates are reasonably sharp:

Fact. $\delta(r, n) \geqslant 2^{r-n}$.

We sketch the argument. One shows that in an example $\mathscr{E}$, $\mathscr{E}'$ witnessing that $\delta(r, n) \leqslant d$, one has at least one relation E with at most $n-1$ classes. After picking representatives $a_1, ..., a_k$ for all the classes, with $k \leqslant n-1$, one sees that for any subset A of the remaining $r-k$ elements, there is at least one relation occurring in $\mathscr{E} \cup \mathscr{E}'$ for which exactly the elements of A are displaced, relative to their original positions (in E) with respect to the class representatives. This yields the bound $2d = |\mathscr{E} \cup \mathscr{E}'| \geqslant 2^{r-k} \geqslant 2^{r-n+1}$, as claimed.

We may phrase this also as follows:

THEOREM IV D. $\mathrm{Ar}(n^d) \leqslant [\log_2 d] + n$.

TABLE II

Conjectured Arities of n^d

n \ d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
2	2	2	2	4	4	4	4	4	4	4	4	4	4	4	4	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
3		2	4	4	4	4	4	4	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
4		4	4	4	4	4	5	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	8	8	8	8	8
5				4	4	6	6	6	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7	7	7	7	7	8	8	8	8	8
6				6	6	6	6	6	6	6	6	6	6	7	7	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
7								6	6	6	6	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	9
8								8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	9	9	9	9	10	10	10	10	10
9																8	8	8	8	8	8	8	8	10	10	10	10	10	10	10	10	10	10	10	10	10
10																10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
11																																10	10	10	10	10
12																																12	12	12	12	12

This is also interesting for the small, fixed values of n we have been considering, and shows that at least to a first approximation, our constructions are reasonably efficient.

7. Remarks on Equivalence Relations

The following example was given as Case 2 in the introduction. Let I be an index set consisting of pairs (κ, d) with d a natural number and κ a finite multiset of natural numbers; write $|\kappa| = \sum_{i \in \kappa} i$, summing with multiplicities. Let $\mathscr{F}_I$ be the set of actions of $\mathrm{Sym}(|\kappa|) \wr \mathrm{Sym}(d)$ on the set $\mathscr{E}_\kappa$ of all partitions of a $|\kappa|$-element set of type κ. Then the arities of all these actions are uniformly bounded if and only if:

(1) d is bounded

(2) For some uniform bound K:

(2.1) κ contains at most K elements greater than 1;

(2.2) If m is the multiplicity of 1 in κ then: $\inf(m, \sup \kappa) \leqslant K$; κ contains at most one element greater than K; and if $\max(m, \sup\kappa) > K$ then the multiplicity of any element of κ other than 1 is one.

Here we exclude the case in which κ contains only the element 1 (repeatedly) as in this case $\mathscr{E}_\kappa$ contains a single element. Accordingly, it is clear that to bound the arity of $(\mathrm{Sym}(|\kappa|) \wr \mathrm{Sym}(d), \mathscr{E}_\kappa^d)$ we must bound d and bound $\mathrm{Ar}(\mathrm{Sym}(|\kappa|), \mathscr{E}_\kappa)$. We must show the latter condition is equivalent to (2) above. For brevity we will write r_κ for $\mathrm{Ar}(\mathrm{Sym}(|\kappa|), \mathscr{E}_\kappa)$. We will also write r'_κ for the arity of the representation obtained by fixing one point in $\mathscr{E}_\kappa$. Then r_κ and r'_κ differ by at most 1.

Suppose first that we have a bound on r_κ. In this case we use the following five relations, which will be checked at the end:

$$\text{For } \kappa' \subseteq \kappa,\ r_\kappa \geqslant r_{\kappa'}. \tag{2}$$

$$\begin{aligned}&\text{If } \kappa = \{k, l\} \text{ with } k \neq l, \text{ or } \kappa = \{1^k, l\},\\ &\text{then } r_k = \mathrm{Ar}\left(\begin{bmatrix} k+l \\ k \end{bmatrix}\right) = 2 + [\log_2 \inf(k, l)].\end{aligned} \tag{4}$$

$$\text{If } \kappa = \{k, k\} \text{ and } k' = \left[\frac{k-1}{2}\right] \text{ then } r_\kappa \geqslant r_{\{k', k-k'\}}, \text{ (and then (4) applies).} \tag{5}$$

$$\text{If } \kappa = \{k, k, l\} \text{ or } \{1^l, k, k\} \text{ with } k > 1 \text{ then } r_\kappa \geqslant \left[\frac{l+2k}{2(k-1)}\right]. \tag{6}$$

$$\begin{aligned}&\text{If } k > 1 \text{ and } \kappa = \{k, ..., k\} \text{ with multiplicity } 2l,\\ &\text{then } r_\kappa \geqslant \mathrm{Ar}(\mathscr{P}(l)) = 1 + [\log_2 l].\end{aligned} \tag{7}$$

Now using $(3-5)$ and a bound on r_κ we may find K_0 so that κ contains at most one element greater than K_0, of multiplicity one, and so that either $\sup \kappa \leqslant K_0$ or the multiplicity of 1 in κ is at most K_0. Using (3) and (7) we bound the number of elements of κ below K_0 and greater than one. Using (6) we may find $K \geqslant K_0$ so that if $\max(m, \sup \kappa) > K$ (where m is the multiplicity of 1 in κ) then the elements of κ in the interval $[2, K_0]$ are distinct. All of this together yields (2) for this value of K.

Now suppose that we have K and κ satisfying (2). We have to obtain a bound on r_κ. If $\max(m, \sup \kappa) \leqslant K$ this is immediate, as $|\kappa|$ is also bounded in this case. So assume $\max(m, \sup \kappa) > K$ and hence all elements of κ greater than 1 occur exactly once. Let κ' be the set of elements of κ greater than 1, together with the multiplicity of 1 in κ (at most one element occurs twice in κ'). Put the following ordering on κ': first the elements of κ above 1 occur, in increasing order, and the multiplicity of 1 is placed at the end. Let $\mathscr{E}'_\kappa$ be the set of ordered partitions of type κ', where the set in the i-th place has size given by the i-th entry of κ'. The actions of $\mathrm{Sym}(|\kappa|)$ on $\mathscr{E}_\kappa$ and on $\mathscr{E}'_\kappa$ are equivalent; let $E \in \mathscr{E}_\kappa$ correspond to the partition in which the classes of E which are not singletons occur first, in order of increasing size, and the set of all elements lying in singleton classes is placed at the end. On the other hand, if s is the length of a sequence in $\mathscr{E}'_\kappa$ (namely, the cardinality of the multiset κ') then $\mathscr{E}'_\kappa$ is just the set of realizations of a certain s-type in $[{}^{|k|}_{k'}]$ (in the notation of §3). It follows easily that $\mathrm{Ar}(\mathscr{E}'_\kappa) \leqslant \mathrm{Ar}([{}^{|k|}_{k'}])$, which is bounded.

Finally we should check points $(3-7)$ used above.

$$\text{For } \kappa' \subseteq \kappa, \; r_\kappa \geqslant r_{\kappa'}. \tag{3}$$

Let $X = \{1, ..., |\kappa|'\}$ and fix a relation E' on the complement of X of type $\kappa - \kappa'$. Let Ω be the set of extensions of E' by a relation of type κ' on X. We identify $\mathrm{Sym}(X)$ with the pointwise stabilizer in $\mathrm{Sym}(|\kappa|)$ of the complement of X. Then $\mathrm{Sym}(X)$ acts on Ω and this action is equivalent to the action of $\mathrm{Sym}(X)$ on $\mathscr{E}_{\kappa'}$. On the other hand, for any r, two r-sequences in Ω are in the same orbit under the full symmetric group $\mathrm{Sym}(|\kappa|)$ if and only if they lie in the same orbit under $\mathrm{Sym}(X)$. This gives the desired inequality.

Points (4) and (5) may be checked easily by the reader.

$$\text{If } \kappa = \{k, k, l\} \text{ or } \{1^l, k, k\} \text{ with } k > 1 \text{ then } r_\kappa \geqslant \left[\frac{l + 2k}{2(k-1)} \right]. \tag{6}$$

This is essentially an old observation of Lachlan (he took l infinite and noted that the arity is then infinite). Let an *n-band* be a sequence of relations E_i of type κ indexed by $i \in \mathbb{Z}/n\mathbb{Z}$ such that the classes of size k in two of these relations E_i and E_j intersect if and only if $i = j \pm 1$, and such that for all i each class of E_i of size k meets exactly one class of E_{i+1} of size k, and meets it in exactly one point. (For $n = 3$ we must add: no point belongs to a class of size k in all three equivalence relations.) In an n-band the classes of size k will have exactly $2(k-1)n$ elements. There are two orbits of n-bands under the action of the symmetric groups: Möbius n-bands such that the sequence of intersecting classes of size k forms a loop of length $2n$, and ordinary n-bands for which there are two loops of length n. It is not difficult to construct representatives of these two orbits provided that $2(k-1)n \leqslant l + 2k$, which happens for $n = [l + 2k/2(k-1)]$. These n-bands demonstrate that the arity is at least n.

$$\begin{aligned} &\text{If } k > 1 \text{ and } \kappa = \{k, ..., k\} \text{ with multiplicity } 2l, \\ &\text{then } r_\kappa \geqslant \mathrm{Ar}(\mathscr{P}(l)) = 1 + [\log_2 l]. \end{aligned} \tag{7}$$

We partition $\{1, ..., |\kappa|\}$ into l disjoint sets X_i of cardinality $2k$ and we take two equivalence relations E_1, E_2 which partition each of the sets X_i into two sets of size k, so that the relations induced by E_1 and E_2 on each X_i are distinct. We then consider the set Ω of relations which agree with either E_1 or E_2 on each of the sets X_i. Ω is invariant under the stabilizer of E_1, E_2 and this action is equivalent to $(\mathrm{Sym}(l), \mathscr{P}(l))$.

Note added in proof. Saracino has recently confirmed Conjecture B, part (1).

References

1. M. Aschbacher and Leonard Scott, Maximal Subgroups of Finite Groups, *J. Algebra* **92**, 1985, 44–80.
2. A. Borel, R. Carter, C. W. Curtis, N. Iwahori, T. A. Springer, and R. Steinberg, "Seminar on Algebraic Groups and Related Finite Groups, Part E," Lecture Notes Math., Vol. 131, Springer-Verlag, New York, 1970.
3. G. Cherlin, L. Harrington, and A. H. Lachlan, $\aleph_0$-Categorical, $\aleph_0$-stable structures, *Ann. Pure Appl. Logic* **28** (1985), 103–135.
4. G. Cherlin and G. Martin, An integer lattice arising in the model theory of wreath products, *in* "Logical Methods: In Honor of Anil Nerode's Sixtieth Birthday" (John N. Crossley, Ed.), Progress in Computer Science and Applied Logic, Vol. 12, Birkhäuser, Cambridge, MA, 1993.
5. G. Cherlin and A. H. Lachlan, Finitely homogeneous relational structures, *Trans. Amer. Math. Soc.* **296** (1986), 815–850.
6. A. Gardiner, Homogeneity conditions in graphs, *J. Combin. Theory Ser. B* **24** (1978), 301–310.
7. B. Huppert, "Endliche Gruppen I," Grundlehren der math. Wiss. in Einzeldarst., Vol. 134, Springer-Verlag, Berlin, 1967.
8. W. Kantor, M. Liebeck, and D. Macpherson, $\aleph_0$-Categorical structures smoothly approximated by finite substructures, *Proc. London Math. Soc.* **59** (1989), 439–463.
9. J. Knight and A. H. Lachlan, "Shrinking, Stretching, and Codes for Homogeneous Structures; Classification Theory, Chicago, 1985" (John Baldwin, Ed.), Lecture Notes in Math., Vol. 1292, Springer-Verlag, New York, 1987.
10. A. H. Lachlan, On countable stable structures which are homogeneous for finite relational language, *Israel J. Math* **49** (1984), 69–153.
11. J. Sheehan, Smoothly embeddable subgraphs, *J. London Math. Soc.* **9** (1974), 212–218.
12. R. Solomon and A. Turull, Chains of subgroups in groups of Lie type, III, *J. London Math. Soc.* **44** (1991), 437–441.