Imprimitive permutations in primitive groups

J. Araújo, J.P. Araújo, P.J. Cameron, T. Dobson, A. Hulpke, P. Lopes

PII: S0021-8693(17)30257-0
DOI: http://dx.doi.org/10.1016/j.jalgebra.2017.03.043
Reference: YJABR 16204

To appear in: *Journal of Algebra*

Received date: 19 December 2016

IMPRIMITIVE PERMUTATIONS IN PRIMITIVE GROUPS

J. ARAÚJO, J. P. ARAÚJO, P. J. CAMERON, T. DOBSON, A. HULPKE, AND P. LOPES

Abstract. The goal of this paper is to study primitive groups that are contained in the union of maximal (in the symmetric group) imprimitive groups. The study of types of permutations that appear inside primitive groups goes back to the origins of the theory of permutation groups. However, this is another instance of a situation common in mathematics in which a very natural problem turns out to be extremely difficult. Fortunately, the enormous progresses of the last few decades seem to allow a new momentum on the attack to this problem. In this paper we prove that there are infinite families of primitive groups contained in the union of imprimitive groups and propose a new hierarchy for primitive groups based on that fact. In addition we introduce some algorithms to handle permutations, provide the corresponding GAP implementation, solve some open problems, and propose a large list of open problems.

Keywords: Primitive groups; imprimitive groups; GAP; permutation type.

1. Introduction

In many practical situations we know that a primitive group contains a given permutation and we want to know which group it can be; in some other practical situations we know the group and would like to know if it contains a permutation of some given type. For example, a group $G \leq S_n$ is said to be *non-synchronizing* if it is contained in the automorphism group of a non-trivial primitive graph with complete core, that is, with clique number equal to chromatic number (see for example, [1, 2, 3, 5, 6, 9, 31]). When trying to check if some group is synchronizing, typically, we have only partial information about the graph but enough to say that it has an automorphism of some type, and the goal would be to have in hand a classification of the primitive groups containing permutations of that type. As an illustration of this, the key ingredient in some of the results in [2] was the observation that the primitive graph under study has a 2-cycle automorphism and hence the automorphism group of the graph is the symmetric group. For many more examples of the importance of knowing the groups that contain permutations of a given type, please see Praeger's slides [32].

This type of investigation is certainly very natural since it appears on the eve of group theory, with Jordan, Burnside, Marggraff, but the difficulty of the problem is well illustrated by the very slow progress throughout the twentieth century. Given the new tools available (chiefly the classification of finite simple groups), the topic seems to have new momentum (see, for example, [17, 21, 22, 25, 26, 29]).

Let S_n denote the symmetric group on n points; a permutation $g \in S_n$ is said to be *imprimitive* if there exists an imprimitive subgroup of S_n that contains g. An imprimitive group is said to be *minimally imprimitive* if it contains no transitive proper subgroup [20]. An imprimitive group $G \leq S_n$ is said to be *maximally imprimitive* if for all $g \in S_n \setminus G$, the group $\langle g, G\rangle$ is primitive. The next result, whose proof is straightforward, provides some alternative characterizations of imprimitive permutations.

Theorem 1.1. *Let n be a natural number and let $g \in S_n$. Then the following are equivalent:*

(1) *there exists an imprimitive group $H \leq S_n$ such that $g \in H$;*
(2) *there exists a maximally imprimitive group $H \leq S_n$ such that $g \in H$;*
(3) *there exists an imprimitive group $H \leq S_n$ such that $\langle g, H \rangle$ is imprimitive;*
(4) *there exists a minimally imprimitive group $H \leq S_n$ such that $\langle g, H \rangle$ is imprimitive;*
(5) *there exists a permutation $h \in S_n$ such that h and g are conjugate (under S_n) and $h \in H$, for some imprimitive group $H \leq S_n$.*

We use the idea of imprimitive permutations to propose a new hierarchy for primitive groups. Roughly speaking this hierarchy measures the size of sets of imprimitive permutations contained in a given primitive group.

In Section 2 we introduce some definitions, basic results and GAP algorithms. In Section 3 we prove that there are infinite families of primitive groups entirely composed of imprimitive permutations. In Section 4 we introduce the hierarchy and prove some results about it. In Section 5 we solve some of the problems posed in [26]. The paper ends with a list of open problems.

2. Preliminaries

Let S_n denote the symmetric group on n points. A permutation $g \in S_n$ is said to be *primitive* if it fails to be imprimitive. It follows that a permutation $g \in S_n$ is primitive if and only if any transitive group $G \leq S_n$ containing g is primitive; the permutation g is said to be *strongly primitive* if the only transitive groups containing g are the symmetric and alternating groups.

Asymptotically, almost all permutations are strongly primitive. This follows from the theorem of Łuczak and Pyber [28] (the asymptotics are given in [12, 14]):

Theorem 2.1. *The proportion of strongly primitive permutations in S_n tends to 1 as $n \to \infty$.*

In this connection, note that in [12] a good upper bound is given for the number of permutations which are primitive but not strongly primitive. Indeed, according to [10], for almost all n (a set of density 1), the only primitive groups of degree n are symmetric and alternating groups, and so there is no difference between primitive and strongly primitive permutations.

The next theorem provides a more technical, but much more practical, characterization of imprimitive permutations. We start with some definitions.

Definition 2.2. *Let k and m be positive integers, and $(m_1, \ldots, m_l)$ a partition of m. Then the partition $(km_1, \ldots, km_l)$ of km is said to be an* ic-partition *(for "imprimitive cycle") of type (k, m).*

Note that an ic-partition of type (k, m) is also an ic-partition of type $(k/d, md)$ for any divisor d of k. For example, the partition $(30, 24, 12)$ of 66 is an ic-partition of type $(2, 33)$ since $(30, 24, 12) = (2 \times 15, 2 \times 12, 2 \times 6)$ and $15 + 12 + 6 = 33$; it is also an ic-partition of type $(6, 11)$ since $(30, 24, 12) = (6 \times 5, 6 \times 4, 6 \times 2)$ and $5 + 4 + 2 = 11$.

Definition 2.3. *For a partition P with r parts, a* clustering *of P is a partition of the set of parts of P into parts (called* clusters*) $P_1, \ldots, P_r$ (each of which is a partition).*

For example, $((2,2),(2,1,1),(1,1))$ is a clustering of $(2,2,2,1,1,1,1)$. The clusters are partitions of 4, 4 and 2 respectively.

Definition 2.4. *An* i-partition *(for "imprimitive") of type (k,m) is a partition of km which has a clustering into clusters which are ic-partitions of $k_i m$ of type (k_i, m) for $i = 1, \ldots, r$, where $(k_1, \ldots, k_r)$ is a partition of k.*

Example. The partition $(1,5,10,10,10,10,10,10)$ is an i-partition of type $(11,6)$. This is shown by the clustering $((1,5),(10,10,10,10,10,10))$. For the partition $(1,5) = (1 \times 1, 1 \times 5)$ is an ic-partition of type $(1,6)$, and $(10,\ldots,10) = (10 \times 1, \ldots, 10 \times 1)$ is an ic-partition of type $(10,6)$.

Theorem 2.5. *The permutation g is contained in an imprimitive permutation group with k blocks of size m if and only if the cycle partition of g on $\{1,\ldots,km\}$ (with $k,m > 1$) is an i-partition of type (k,m).*

Proof. First we observe that the cycle partition of g is an ic-partition of type (k,m) if and only if g is contained in an imprimitive group as in the theorem and induces a cyclic permutation on the set of blocks. For if g permutes the blocks cyclically, then we return to the same block after k steps, so every cycle has length divisible by k; and conversely, if every cycle has length divisible by k, we obtain the block system by assigning the points in each cycle to the k blocks in cyclic order.

Now for an arbitrary permutation, if its cycle type is an i-partition, then we can construct a block system on the union of the cycles in each ic-partition, and this block system is preserved by g. The converse is clear. □

As a simple illustration, we show:

Theorem 2.6. *Let Ω be a set of size n and let $P = (p_1, \ldots, p_l)$ be a partition of n, in which the parts have a common divisor larger than 1. Then any permutation of cycle-type P is imprimitive.*

For if the greatest common divisor is m, and $mk = n$, then take the partition $(p_1/m, \ldots, p_l/m)$ of k, and for each i take the ic-partition of p_i with a single part, to verify that P is an i-partition.

The following variant of Theorem 2.5 turns out to be useful for testing.

Lemma 2.7. *If a partition P of n points is an i-partition of type $(n/m, m)$, then there exists a clustering $P_1, \ldots, P_r$ of P with $l_i = \sum_{p \in P_i} p$ and $g = \gcd(\ell_1, \ldots, \ell_r)$ such that m is a divisor of g and P_i is an ic-partition of type $(k_i = l_i/g, g)$. Conversely, if such a clustering exists, then P is an i-partition of type $(n/m, m)$.*

In particular, P is the cycle shape of an imprimitive permutation if and only if such a clustering exists for which $1 < g < n$.

Proof. Note that $n = \sum l_i$ is a multiple of g, and hence any divisor of g is a divisor of n.

Suppose that $P_1, \ldots, P_r$ is a clustering that identifies P as an i-partition with P_i an ic-partition of type (k_i, m). Then m divides every l_i and thus divides g. Furthermore, P_i is also an ic-partition of type $(k_i m/g, g)$, as $k_i m/g$ divides k_i. The converse statement is the definition of an i-partition.

The last statement follows immediately from Theorem 2.5. □

A final result concerns using a pair of permutations to guarantee primitivity. We follow the terminology of Definition 2.4.

Definition 2.8. *The i-type of a partition is the set of pairs (k, m), where $k, m > 1$, for which the partition has an i-partition of type (k, m). The i-type of a permutation is the i-type of its cycle partition.*

A permutation is primitive if and only if its i-type is empty. Now suppose that a transitive group G contains two imprimitive permutations g_1 and g_2 whose i-types are disjoint. Then necessarily G is primitive.

For example, $G = 2^4.3^2 : 4$, the 8th primitive group of degree 16 in GAP, contains an element g_1 with cycle structure $[8, 8]$, and an element g_2 with cycle structure $[3, 3, 3, 3, 3, 1]$. Then g_1 is of *i*-types $(2, 8)$ and $(8, 2)$, while g_2 is of *i*-type $(4, 4)$ only.

2.1. **An algorithm to identify primitive permutations.** By Theorem 2.5, the test to check if a given permutation is primitive can be based purely on its cycle structure; it needs to be an *i*-partition. In particular it is sufficient to test conjugacy class representatives if testing whether a group contains a primitive permutation.

We therefore describe an algorithm that tests whether a given partition P of a composite number n, consisting of l parts, is an i-partition. We will write $P = (p_1, \ldots, p_l)$ as a collection of parts, assuming without loss of generality that $p_i \geq p_{i+1}$. By Lemma 2.7 we need to consider all clusterings of P.

The starting point for this is a process for enumerating partitions of a set (the set being the parts of P). Following [23, Section 7.2.1.5], partitions of a set of cardinality l correspond to restricted growth strings $(a_i)_{i=1}^{l}$ of length l (the i-th entry of the string gives the part number in which the i-th set element is placed), that is, $a_{j+1} \leq 1 + \max(a_1, \ldots, a_j)$.

Since the partition P might have parts of equal size, this parameterization of set partitions will produce partitionings that are equal, i.e. if the partition is $P = (A, a, B, b)$ (with upper/lower case to distinguish equal entries: $A = a$, $B = b$) then $(A, B)(a, b)$ and $(A, b), (a, B)$ are, nominally different, equal partitionings. That is, if I is a set of indices (because P is ordered it will be in fact an interval) such that p_i is constant for $i \in I$, and π is a permutation with support I, the sequences (a_i) and (a_{i^π}) result in equivalent partitionings.

We incorporate this equivalency in the construction process by requiring that if P is constant on the interval I, the sequence (a_i) is non-decreasing on I. In the construction algorithm for the restricted growth strings, Algorithm H of [23, Section 7.2.1.5], this condition can only be violated if $a_j \leftarrow 0$ in step H6. We modify this step by setting $k \leftarrow j$ at the start of this step and replacing, as long as $p_j = p_k$, the assignment $a_j \leftarrow 0$ with $a_j \leftarrow a_k$.

Each string then defines a clustering $P_1, \ldots, P_r$ of P. By 2.7 we calculate $g = \gcd(l_i)_{i=1}^r$ with $l_i = \sum_{p \in P_i} p$. If $1 < g < n$ test whether for each i all parts of P_i are of length a multiple of l_i/g. If so, P is an i-partition.

The cost of this algorithm grows rapidly with the number of parts of the partition P. Such partitions tend to have many parts of small size. To speed up handling in these cases, we begin by testing whether for any proper divisor m of n we can cluster the parts of P into subsets of cardinality m each (in this case each cluster is an ic-partitions of type $(1, m)$ and thus P will be an i-partition). We do so with a greedy algorithm that increases each partial cluster by adding the largest remaining part that does not push the cluster content over m. This test is very quick and succeeds for example if there are many parts of size 1. Only if the greedy algorithm fails we start the full search for clusterings.

We have implemented this test in GAP [15]; the code is available at `http://www.math.colostate.edu/~hulpke/examples/primitivepermutation.g`.

3. Primitive groups without primitive permutations

The aim of this section is to provide examples of primitive groups fully composed by imprimitive permutations. We start with three infinite families.

First construction: Covering with imprimitive subgroups. This construction provides a very flexible way of producing primitive groups without primitive permutations. Let H and K be finite permutation groups and consider the wreath product $G = H \wr K$ in the product action. By [11, Lemma 2.7.A.] this is primitive if and only if

(1) H is primitive and not cyclic of prime order;
(2) K is transitive.

The goal now is to produce a primitive group which is a union of imprimitive subgroups. We can do this from the wreath product construction if K is a transitive group which is the union of intransitive subgroups (this simply means that K contains no cyclic transitive subgroup – so there are many examples, e.g. non-cyclic groups acting regularly). Take, for example, $H = S_3$, and $K = (C_2)^m$ acting regularly. Then G is primitive of degree 3^{2^m} and the minimum number of generators for G is at least m since if we take fewer than m elements of G, then the subgroup they generate projects onto a proper (and hence intransitive) subgroup of K, and so is imprimitive; thus we require at least m elements to generate a primitive subgroup.

Second construction: Some affine groups. As some primitive affine groups can also be written as a product action, namely primitive subgroups of $G \wr S_k$ where $G \leq \mathrm{AGL}(1, p)$ is transitive but not cyclic, we focus on such groups. In light of the previous construction, we mainly focus on $G \wr C_k$ with the product action where C_k is the cyclic group of order k. We begin by fixing some notation and a general result which characterizes imprimitive elements of $\mathrm{AGL}(k, p)$.

Of course, $\mathrm{AGL}(k, p)$ contains a normal regular elementary abelian subgroup, which we call E, and $\mathrm{AGL}(k, p) = \mathrm{GL}(k, p) \cdot E$. The following result characterizes imprimitive elements of $\mathrm{AGL}(k, p)$.

Lemma 3.1. *Let $g \in \mathrm{AGL}(k,p)$ with $g = Ae$, where $A \in \mathrm{GL}(k,p)$ and $e \in E$. The element g is imprimitive if and only if the characteristic polynomial of A is reducible.*

Proof. Since the group E acts regularly, the E-invariant partitions are the coset partitions corresponding to the subgroups of E (this well-known result is a special case of [35, Theorem 7.5]). So, if A has an invariant subspace, then A (and hence also $g = Ae$) preserves the partition into cosets of this subspace.

Now A has an invariant subspace (subgroup of E) if and only if its characteristic polynomial is reducible. (One way round is clear: if A has an invariant subspace then it is represented by a matrix of the form $\begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$. Conversely, suppose that the characteristic polynomial $\phi(x)$ of A factorises as $f(x)g(x)$. If $f(A) = 0$, then the A-submodule spanned by a vector v has dimension at most the degree of f. Similarly if $g(A) = 0$. Otherwise, $Ef(A)$ is annihilated by $g(A)$ and so it is a proper submodule of E.) □

Now let $S \in \mathrm{GL}(k,p)$ be the permutation matrix which shifts the coordinates of $\mathbb{F}_p^k$ one to the left (so that S is a cyclic group of order k acting regularly on the coordinates of $\mathbb{F}_p^k$), and $D \in \mathrm{GL}(k,p)$ be a diagonal matrix. Let d_i be the entry in D in row i and column i, and $d = \prod_{i=1}^k d_i$. Straightforward computations will show that DS has characteristic polynomial $x^k - d$. Also, any element of $\mathrm{GL}(k,p)$ contained in $\mathrm{AGL}(1,p) \wr C_k$ will either fix a subspace of dimension dividing k (if it projects onto an element of order smaller than k in C_k) or have the form DS, with D and S as above (this is easiest to see computing in $\mathrm{AGL}(1,p) \wr C_k$). We give our first example of a subgroup of $\mathrm{AGL}(k,p) \cap (\mathrm{AGL}(1,p) \wr C_k)$ that is imprimitive. We denote the dihedral group of order $2p$ by D_p.

Lemma 3.2. *Let p be prime and $G = D_p \wr C_4 \leq \mathrm{AGL}(4,p)$. Then every element of G is imprimitive.*

Proof. By definition and comments above, if $g \in G$ is contained in $\mathrm{GL}(4,p)$ then either g preserves a subspace of dimension 1 or 2, or it has characteristic polynomial $x^4 \pm 1$, both of which are reducible. (Since $p^2 - 1$ is divisible by 8, the roots of this polynomial lie in $\mathbb{F}_{p^2}$.) The result follows by Lemma 3.1. □

Theorem 3.3. *Let k be an integer and p be prime, $R = \{s \in \mathbb{F}_p^* : s = t^k \text{ for some } t \in \mathbb{F}_p^*\}$, $G \leq \mathrm{AGL}(1,p) \wr C_k \leq \mathrm{AGL}(k,p)$ be transitive, and $g \in G$. Write $g = D_g S^{a_g}$ where $D_g \in \mathrm{GL}(k,p)$ is diagonal and a_g is an integer. Suppose that, whenever $g \in G \cap \mathrm{GL}(k,p)$ cyclically permutes the coordinates of $\mathbb{F}^k$ as a k-cycle then $\det(D_g) \in R$. Then every element of G is imprimitive.*

Proof. Suppose that whenever $g \in G \cap \mathrm{GL}(k,p)$ cyclically permutes the coordinates of $\mathbb{F}^k$ as a k-cycle then $\det(D) \in R$. By comments above, the characteristic polynomial of g is $x^k - d$ where $d = \det(D)$ which is reducible as d is a k-th root. The result follows by Lemma 3.1. □

Applying the covering argument from the previous construction and observing that any two regular cyclic subgroups of S_k are conjugate in S_k, we have the following result.

Corollary 3.4. *Let p be prime, k a positive integer, $R = \{s \in \mathbb{F}_p^* : s = t^k \text{ for some } t \in \mathbb{F}_p^*\}$, and $G = \langle x \mapsto rx+b : r \in R, b \in \mathbb{Z}_p \rangle \leq \mathrm{AGL}(1,p)$. Then every element of $G \wr S_k$ with the product action is imprimitive.*

Note that in the previous result if $\gcd(k, p-1) = 1$, then $G = \mathrm{AGL}(1, p)$.

Corollary 3.5. *Let $p \geq 5$, and $H \leq \mathrm{AGL}(1, p)$ consist of all elements of the form $x \mapsto ax + b$, where a is a quadratic residue modulo p. Then $H \wr S_2$ is primitive but contains no primitive elements and contains a normal imprimitive subgroup of index 2.*

Proof. We first apply Corollary 3.4 with $k = 2$, in which case R is the set of quadratic residues modulo p. As $p \geq 5$, $R \neq \{1\}$ and so $H = \langle x \mapsto rx+b : r \in R, b \in \mathbb{Z}_p\rangle \ncong \mathbb{Z}_p$. Then every element of $H \wr S_2$ is imprimitive by Corollary 3.4 and this group is primitive of degree p^2 by [11, Lemma 2.7.A.]. Finally, $H \times H \lhd H \wr S_2$ is a normal imprimitive subgroup of index 2. □

The next result will allow us to verify the unsurprising fact that there are primitive permutation groups that are product actions which have primitive elements.

Theorem 3.6. *Let $k = 2$ or 3, p be prime, and $R = \{s \in \mathbb{F}_p^* : s = t^k \text{ for some } t \in \mathbb{F}_p^*\}$, $G \leq \mathrm{AGL}(1, p) \wr C_k$, and $g \in G$. Write $g = D_g S^{a_g}$ where $D_g \in \mathrm{GL}(k, p)$ is diagonal and a_g is an integer. Then every element of G is imprimitive if and only if whenever $g \in G \cap \mathrm{GL}(k, p)$ cyclically permutes the coordinates of $\mathbb{F}^k$ as a k-cycle then $\det(D_g) \in R$.*

Proof. In view of Theorem 3.3, we need only to prove the converse. Suppose that every element of G is imprimitive. We will show that that if $\det(D_g) = d \notin R$ then g is primitive by Theorem 2.5. So suppose that $d \notin R$. It is clear that g fixes the 0 vector. If g fixes any other vector $\mathbf{v}$, then $\mathbf{v}$ is an eigenvector of g with eigenvalue 1. As the characteristic polynomial of g is $x^q - d$ and $d \notin R$, this implies that $d = 1 \in R$. Straightforward computations will show that $g^k = dI_n$. Now, if $s \in \mathbb{Z}_p^*$ but there is no $t \in \mathbb{Z}_p^*$ with $t^k = s$, then $k|(p-1)$ and the highest power k^a of k dividing $p-1$ also divides the order of s. We conclude that any orbit of g that is not the singleton orbit $\{(0, 0)\}$ has order a multiple k^{a+1} as g^k has order a multiple of k^a. Now, if g is imprimitive and preserves the invariant partition $\mathcal{B}$, then g fixes the block $B \in \mathcal{B}$ that contains $(0, 0)$, so $B - \{(0, 0)\}$ is a union of orbits of g. Suppose that $|B| = p$. Then $p-1$ is a sum of multiples of k^{a+1}, and so the highest power of k dividing $p-1$ is k^{a+1}, a contradiction. Suppose that $|B| = p^2$ (and so $k = 3$). Then $p^2 - 1$ is a multiple of k^{a+1} and as the highest power of k that divides $p-1$ is k^a, we conclude that k divides $p+1$. However, $\gcd(p-1, p+1) = 2 \neq k$, a contradiction which establishes the result. □

Corollary 3.7. *Let $p \geq 3$ be prime. The group $\mathrm{AGL}(1, p) \wr C_2$ is a primitive group that is a product action and contains primitive elements. Similarly, if $3|(p-1)$, then $\mathrm{AGL}(1, p) \wr C_3$ is a primitive group that is a product action and contains primitive elements.*

Proof. If $p \geq 3$ then there are elements in $\mathbb{F}_p^*$ which are not quadratic residues, and let a be such an element. Choose a diagonal matrix D such that D has determinant a. The element $g = DS \in (\mathrm{AGL}(1, p) \wr C_2) \cap \mathrm{GL}(2, p)$, and the result follows from Theorem 3.6. The second statement follows similarly as the arithmetic condition that $3|(p-1)$ ensures there are elements in $\mathbb{F}_p^*$ that are not cubes. □

Third construction: From a problem of Wielandt. Another infinite class of examples comes from the following observation. We say that the *spectrum* of a subgroup of S_n is the set of cycle types of elements it contains.

Theorem 3.8. *Two faithful actions of a group G with the same permutation character have the same spectrum. Hence if the group G has two faithful transitive actions, one primitive and one imprimitive, with the same permutation character, then every element in the primitive action of G is an imprimitive permutation.*

Proof. If g has c_i cycles of length i, then for any divisor d of the order of g, the number of fixed points of g^d is $\sum_{f|d} c_f$; then Möbius inversion shows that the numbers c_i are determined by the character values on powers of g. So the first statement is true; and the second follows immediately. □

Such groups are not easy to find: Wielandt asked in 1979 whether they could exist. An infinite family based on the exceptional groups of type E_8 was found by Guralnick and Saxl [18], while a sporadic example in the group J_4 was found by Breuer [8].

It is worth pointing out that this construction gives examples of primitive groups where all the permutations have a common i-type, namely the block size and number of blocks of its imprimitive companion.

Fourth construction: Some groups of diagonal type.

Theorem 3.9. *Let T be a nonabelian simple group. Then no element of the primitive group T^2 with the diagonal action is primitive.*

Proof. That T^2 with the diagonal action is primitive follows from [11, Theorem 4.5a (i)]. Also, T^2 contains T as a regular subgroup, and we lose no generality by assuming that $T_L \leq T^2$, where T_L is the left regular representation of T. In T^2, T_L is centralized by subgroup isomorphic to T, and the centralizer in S_T is T_R by [11, Lemma 4.2A]. So we may assume without loss of generality that $T \times T = T_L \times T_R$. Now, both T_L and T_R are regular, and being so are imprimitive by [11, Theorem 1.5A] as they are simple and nonabelian and so have proper nontrivial subgroups. Hence any element of T^2 of the form $(t, 1)$ or $(1, t)$ with $t \in T$ is imprimitive. Consider an element of the form (t, s), where $t, s \in T$ and neither is the identity. Let $H = \langle (r, 1), (t, s) : r \in T \rangle$, and let $\pi_i : T^2 \to T$ be projection in the coordinate i, $i = 1, 2$. Of course, $\pi_1(H) = T$, while $\pi_2(H) = \langle s \rangle < T$. Additionally, $H = T_L \times \langle s \rangle$, and is transitive as T_L is transitive. However, $\langle (1, s) \rangle \triangleleft H$ is not transitive, and so its orbits form a complete block system of H. Thus H is imprimitive and so (r, s) is imprimitive. Thus every element of T^2 is imprimitive as required. □

Miscellaneous examples. We know finitely many further examples of such groups. Some come from the computer search with the GAP implementation of the algorithm above. We investigated the primitive groups of degree up to 120.

n	#	G	n	#	G	n	#	G	n	#	G

15	2	A_6	64	2	$2^6:D_{14}$	81	40	$3^4:2^{2+2+2}$	100	10	$A_{10}^2.2^2$
	3	S_6		6	$2^6:3^2:3$		42	$3^4:D_{16}:4$		11	$A_{10}^2.4$
16	4	$(A_4 \times A_4):2$		7	$2^6:7:6$		43	$3^4:(SA_{16}:2):2$		12	$S_{10} \wr S_2$
	7	$2^4.S_3 \times S_3$		9	$2^6:3^2:S_3$		49	$3^4:2^3:A_4$		13	$A_6 \wr S_2$
	8	$2^4.3^2:4$		10	$2^6:3^2:S_3$		50	$3^4:(Q_8:2):S_3$		14	$A_6^2.2^2$
	10	$(S_4 \times S_4):2$		16	$2^6:(7 \times D_{14})$		51	$3^4:Q_8.S_3:2$		15	$A_6^2.2^2$
25	4	$5^2:Q(8)$		17	$2^6:3^2:D_{12}$		52	$3^4:(2 \times Q_8):6$		16	$A_6^2.4$
	5	$5^2:D(2 \cdot 4)$		18	$2^6:(3^2:3):4$		53	$3^4:Q_8.S_3:2$		17	$A_6^2.2^2$
	11	$5^2:D(2 \cdot 4):2$		25	$2^6:(3^2:3):Q_8$		54	$3^4:(SA_{16}:2):3$		18	$A_6^2.4$
27	1	$3^3.A_4$		26	$2^6:(3^2:3):8$		55	$3^4:(Q_8:3):2^2$		19	$A_6^2.2^2$
	3	$3^3(A_4 \times 2)$		27	$2^6:(3^2:3):D_8$		56	$3^4:Q_8.S_3:2$		20	$A_6^2.D_8$
	4	$3^3.2.A_4$		28	$2^6:7:7:6$		57	$3^4:(Q_8:3):4$		21	$A_6^2.2^3$
	5	$3^3.S_4$		29	$2^6:7^2:S_3$		58	$3^4:(\mathrm{GL}_1(3) \wr D_4)$		22	$A_6^2.D_8$
	8	$3^3(S_4 \times 2)$		33	$2^6:(3^2:3):SD_{16}$		59	$3^4:Q_{16}:D_8$		23	$A_6^2.D_8$
28	1	$\mathrm{PGL}_2(7)$		38	$2^6:7^2:(3 \times S_3)$		60	$3^4:(4 \times 8):4$		24	$A_6^2.D_8$
	4	$\mathrm{PSU}_3(3)$		42	$2^6:(\mathrm{GL}_3(2) \wr 2)$		61	$3^4:2^{2+3+1+1}$		25	$A_6^2.D_8$
	5	$\mathrm{P\Gamma U}(3,3)$		47	$2^6:3.S_6$		63	$3^4:2^{2+3+1+1}$		26	$A_6^2.(2 \times 4)$
	9	$\mathrm{PSL}_2(27)$		48	$2^6:3.A_6$		64	$3^4:2^{3+4}:4$		27	$A_6^2.D_8$
	10	$\mathrm{PGL}_2(27)$		58	$2^6:S_8$		66	$3^4:2^{2+3+1+1}$		28	$A_6^2.(2 \times 4)$
35	1	A_8		59	$2^6:A_8$		72	$3^4:(\mathrm{GL}_1(3) \wr A_4)$		29	$A_6^2.(2 \times 4)$
	2	S_8		60	$2^6:S_7$		73	$3^4:Q_8:S_4$		30	$A_6^2.2^2:4$
	3	A_7		61	$2^6:A_7$		74	$3^4:2^3:S_4$		31	$A_6^2.(2 \times D_8)$
	4	S_7		62	$2^6:\Sigma U(3,3)$		75	$3^4:(2 \times Q_8):A_4$		32	$A_6^2.2^2:4$
36	3	M_{10}		63	$2^6:SU_3(3)$		76	$3^4:2^{3+2}:S_3$		33	$A_6^2.(2 \times D_8)$
	4	$\mathrm{PGL}_2(9)$		64	$2^6:\mathrm{PGL}_2(7)$		77	$3^4:(Q_8.S_3:2):2$		34	$A_6^2.(2 \times D_8)$
	5	$\mathrm{P\Gamma L}(2,9)$		65	$A_8 \wr S_2$		78	$3^4:(SA_{16}:2):6$		35	$A_6^2.2^2:4$
	8	$\mathrm{PSp}_4(3)$		66	$A_8^2.2^2$		79	$3^4:(SA_{16}:2):6$		36	$\mathrm{P\Gamma L}(2,9) \wr S_2$
	9	$\mathrm{PSp}_4(3):2$		69	$\mathrm{PSL}_2(7) \wr S_2$		80	$3^4:Q_8.S_3:4$	102	1	$\mathrm{PSL}_2(17)$
	13	$(A_6 \times A_6):2$		70	$\mathrm{PSL}_2(7)^2.2^2$		81	$3^4:Q_8.S_3:2^2$	105	1	$\mathrm{PSL}_3(4).2$
	14	$(A_6 \times A_6):2^2$		71	$\mathrm{PSL}_2(7)^2.4$		82	$3^4:2^{2+3+1+2}$		2	$\mathrm{PSL}_3(4).2$
	15	$(A_6 \times A_6):4$		72	$\mathrm{PGL}_2(7) \wr S_2$		83	$3^4:(\mathrm{GL}_1(3) \wr D_4):2$		3	$\mathrm{PSL}_3(4).2^2$
	16	$(S_6 \times S_6):2$	65	1	$\mathrm{PSL}_2(5^2)$		85	$3^4:8^2:4$		4	$\mathrm{PSL}_3(4).S_3$
	17	$(A_5 \times A_5):2$		2	$\mathrm{P\Sigma L}(2,5^2)$		88	$3^4:\mathrm{SL}_2(3):A_4$		5	$\mathrm{PSL}_3(4).6$
	18	$(A_5 \times A_5).4$		3	$\mathrm{PSU}_3(4)$		91	$3^4:(\mathrm{GL}_1(3) \wr S_4)$		6	$\mathrm{PSL}_3(4).D_{12}$
	19	$((A_5 \times A_5):2)2$	66	1	$\mathrm{PGL}_2(11)$		92	$3^4:Q_8^2:6$		7	S_8
	20	$(S_5 \times S_5):2$		2	M_{11}		93	$3^4:Q_8^2:S_3$	112	1	$\mathrm{PSU}_4(3)$
40	1	$\mathrm{PSp}_4(3)$		3	M_{12}		94	$3^4:\mathrm{GL}_2(3):D_8$		2	$\mathrm{PSU}_4(3).2$
	2	$\mathrm{PSp}_4(3):2$	77	1	M_{22}		96	$3^4:\mathrm{SL}_2(3):S_4$		3	$\mathrm{PSU}_4(3).2$
	3	$\mathrm{PSp}_4(3)$		2	$M_{22}.2$		97	$3^4:(2^3:A_4):S_3$		4	$\mathrm{PSU}_4(3).2$
	4	$\mathrm{PSp}_4(3):2$	81	4	$3^4:D_{16}$		98	$3^4:\mathrm{GL}_2(3):(3 \times S_3)$		5	$\mathrm{PSU}_4(3).2^2$
45	1	$\mathrm{PGL}_2(9)$		5	$3^4:SA_{16}$		100	$3^4:Q_8^2:D_{12}$		6	$\mathrm{PSU}_4(3).4$
	2	M_{10}		6	$3^4:Q_8:2$		101	$3^4:(\mathrm{SL}_2(3) \wr 2)$		7	$\mathrm{PSU}_4(3).2^2$
	3	$\mathrm{P\Gamma L}(2,9)$		8	$3^4:SD_{16}$		102	$3^4:\mathrm{GL}_2(3):S_4$		8	$\mathrm{PSU}_4(3).D_8$
	4	$\mathrm{PSp}_4(3)$		13	$3^4:SA_{16}:2$		103	$3^4:(2^3:A_4):S_3$	117	1	$\mathrm{PSL}_3(3).2$
	5	$\mathrm{PSp}_4(3):2$		14	$3^4:2^2:4:2$		104	$3^4:(2^3:2^2):(3^2:4)$	120	1	S_7
	6	A_{10}		15	$3^4:SA_{16}:2$		106	$3^4:Q_8^2:S_3^2$		2	A_9
	7	S_{10}		16	$3^4:2^3:2^2$		107	$3^4:(2^3:2^2):3^2:D_8$		6	$\mathrm{PSL}_3(4)$
49	2	$7^2:S_3$		17	$3^4:D_{16}:2$	84	1	A_9		7	$\mathrm{PSL}_3(4).2$
	7	$7^2:D(2 \cdot 6)$		18	$3^4:2^{2+2+1}$		2	S_9		8	$\mathrm{PSL}_3(4).2$

	12	$7^2{:}3 \times D(2 \cdot 3)$		19	$3^4{:}Q_{16}{:}2$	85	1	$\mathrm{PSp}_4(4)$		9	$\mathrm{PSL}_3(4).2$
	21	$7^2{:}3 \times D(2 \cdot 6)$		20	$3^4{:}2^{2+1+2}$		2	$\mathrm{PSp}_4(4).2$		10	$\mathrm{PSL}_3(4).2^2$
52	1	$\mathrm{PSL}_3(3).2$		21	$3^4{:}D_{16}{:}2$	91	1	$\mathrm{PSL}_2(13)$		11	S_8
60	1	A_5^2		22	$3^4{:}(2 \times Q_8){:}2$		2	$\mathrm{PGL}_2(13)$		14	$\mathrm{PSp}_6(2)$
	2	$A_5^2.2$		23	$3^4{:}SA_{16}{:}2$		3	$\mathrm{PSL}_2(13)$		16	$O^+(8,2)$
	3	$A_5 \wr S_2$		30	$3^4{:}Q_8.S_3$		4	$\mathrm{PGL}_2(13)$		17	$\mathrm{PSO}^+(8,2)$
	4	$A_5 \wr S_2$		31	$3^4{:}(Q_8{:}3){:}2$	100	1	J_2		18	A_{10}
	5	$A_5^2.2^2$		32	$3^4{:}(\mathrm{GL}_1(3) \wr 4)$		2	$J_2.2$		19	S_{10}
63	1	$\mathrm{PSU}_3(3)$		33	$3^4{:}4^2{:}4$		5	$A_5 \wr S_2$		20	A_{16}
	2	$\mathrm{PSU}_3(3).2$		34	$3^4{:}Q_8{:}D_8$		6	$A_5^2.2^2$		21	S_{16}
	3	$\mathrm{PSU}_3(3)$		35	$3^4{:}2^3{:}D_8$		7	$A_5^2.4$			
	4	$\mathrm{PSU}_3(3).2$		37	$3^4{:}2^{2+3+1}$		8	$S_5 \wr S_2$			
	5	$\mathrm{PSp}_6(2)$		39	$3^4{:}D_{16}{:}4$		9	$A_{10} \wr S_2$			

These groups belong to the following classes (in GAP's version of the O'Nan-Scott Theorem):

"1": Affine.

"2": Almost simple.

"3a": Diagonal, Socle consists of two normal subgroups.

"3b": Diagonal, Socle is minimal normal.

"4c": Product action with the first factor primitive of type 2.

The next table contains the synchronizing groups without primitive permutations.

Degree	Groups				
28	$\mathrm{PSU}(3,3)$	$\mathrm{P\Gamma U}(3,3)$	$\mathrm{PSL}(2,27)$	$\mathrm{PGL}(2,27)$	
36	$\mathrm{PSp}(4,3)$	$\mathrm{PSp}(4,3):2$			
40	$\mathrm{PSp}(4,3)$	$\mathrm{PSp}(4,3):2$	$\mathrm{PSp}(4,3)$	$\mathrm{PSp}(4,3):2$	
63	$\mathrm{PSU}(3,3)$	$\mathrm{PSU}(3,3).2$	$\mathrm{PSp}(6,2)$		
64	$2^6:(3^2:3):Q_8$	$2^6:(3^2:3):8$	$2^6:(3^2:3):\mathrm{SD}_{16}$	$2^6:\Sigma\mathrm{U}(3,3)$	$2^6:\mathrm{SU}(3,3)$
65	$\mathrm{PSL}(2,5^2)$	$\mathrm{P\Sigma L}(2,5^2)$	$\mathrm{PSU}(3,4)$		

They are very few; this means that up to degree 100, the overwhelming majority of primitive groups without primitive permutations are non-synchronizing.

The next observation may provide some more sporadic examples of primitive groups without primitive permutations. Let G be a primitive group with an imprimitive normal subgroup N of index 2. Then all elements of N are imprimitive, and it is only necessary to check half the elements of G. For example, let $G = \mathrm{PGL}(2,11)$, with degree 66. The elements of G not in the imprimitive normal subgroup have cycle types $(6,12,12,12,12,12)$, $(1,5,10,10,10,10,10,10)$, and two types corresponding to cubes of the first and fifth powers of the second. Theorem 2.5 shows that all these permutations are imprimitive.

4. An infinite hierarchy for primitive groups

The previous results suggest the following hierarchy for primitive groups based on the cycle-type of permutations they contain.

A set of permutations $S \leq S_n$ is said to be *imprimitive* if there exists an imprimitive group $H \leq S_n$ such that $S \subseteq H$; otherwise S is said to be *primitive*. If S is imprimitive, then the intersection of the i-types of its elements is non-empty; but the converse is false.

Let k and n be two natural numbers. The class $\mathbf{EP}_{k,n}$ is composed by all degree n primitive groups G in which there exist some k-subsets which are primitive. For example, A_6 (degree 15) does not contain primitive permutations, but contains several primitive 2-sets and hence this group belongs to $\mathbf{EP}_{2,15}$.

A set $S \subseteq G \leq S_n$ is said to be independent if

$$(\forall g \in S)\ g \notin \langle S \setminus \{g\} \rangle.$$

The class $\mathbf{AP}_{k,n}$ is composed by all degree n primitive groups G in which all independent k-subsets are primitive. For example, it is obvious that every transitive group of prime degree p belongs to $\mathbf{AP}_{1,p}$.

The class $\mathbf{NP}_{k,n}$ contains all degree n primitive groups G in which there are no primitive k-subsets. For example, A_6 (degree 15) belongs to $\mathbf{NP}_{1,15}$. Also, the groups $S_3 \wr 2^m$ belong to $\mathbf{NP}_{m,3^{2^m}}$. So our hierarchy is infinite.

The following observations are obvious:

- if G belongs to $\mathbf{AP}_{k,n}$, then it also belongs to $\mathbf{AP}_{m,n}$, for all $m \geq k$;
- if G belongs to $\mathbf{NP}_{k,n}$, then it also belongs to $\mathbf{NP}_{m,n}$, for all $m \leq k$;
- if G belongs to $\mathbf{EP}_{k,n}$, then it belongs to $\mathbf{EP}_{m,n}$, for all $m \geq k$.

A group G belongs to the class $\mathbf{NAP}_{k,n}$ if the group belongs to $\mathbf{AP}_{k,n}$ and to $\mathbf{NP}_{k-1,n}$. Similarly, a group belongs to $\mathbf{NEP}_{k,n}$ if the group belongs to $\mathbf{EP}_{k,n}$ and to $\mathbf{NP}_{k-1,n}$.

4.1. Testing for $\mathbf{EP}_{k,n}$ and $\mathbf{AP}_{k,n}$.

To test membership of a group G in $\mathbf{EP}_{k,n}$ or $\mathbf{AP}_{k,n}$ for given natural numbers k and n, we need to iterate through the k-subsets of G. Clearly it is sufficient to do so up to conjugacy in $N = N_{S_n}(G)$.

An algorithm that will run through sequences of group elements up to conjugacy is given in [19, Section V.5] in the context of searching for homomorphisms. Its input consists of N-conjugacy classes of elements of G.

While enumerating sequences clearly enumerates sets, there is a substantial amount of duplication. By demanding that the conjugacy class for the $i+1$-th sequence element is not smaller (in some arbitrary ordering of conjugacy classes) than the class for the i-th element, it is possible to eliminate a substantial amount of duplication of the same set by different sequences. We found this to be a reasonable tradeoff of runtime efficiency and implementation cost.

We consider first the case of $\mathbf{EP}_{k,n}$, that is we test whether a primitive set exists: For every sequence A we test whether $\langle A \rangle$ is a primitive subgroup of S_n (in which case the property is true), or whether $\langle A \rangle$ is transitive (in which case A can be discarded). We collect a pool of those A which generate intransitive subgroups.

We reduce this pool by eliminating sequences if the groups generated by them are N-conjugate.

Next we test for a failure of A to be primitive within G: We determine the maximal transitive but imprimitive subgroups of G and (if they are not too large) calculate the subgroups thereof. If $\langle A\rangle A$ is conjugate to any of these subgroups it cannot be primitive.

It turns out that for all examples we considered so far this strategy was successful in either eliminating all A's or finding one A that actually generated a primitive group. It is possible however that neither case holds, that is an A that generates an intransitive group cannot be eliminated.

In this case we test whether A is contained in a maximal imprimitive subgroup $H \leq S_n$. These groups are wreath products of symmetric groups, parameterized by partitions of n into blocks of equal size, and thus can be constructed easily.

For efficiency, we note that we need to consider H only up to conjugacy by $M = N_{S_n}(\langle A\rangle)$. This is achieved by selecting H up to conjugacy (note that H is maximal in S_n and thus self-normalizing) and let r run through a set of representatives of the double cosets $M \setminus S_n/H$. For each r we test whether $A^r \subset H$.

The test for $\mathbf{AP}_{k,n}$ proceeds similar, but with different stopping criteria: We iterate over sequences A. If $\langle A\rangle$ is primitive, or A is not independent we discard A. If $\langle A\rangle$ is transitive and imprimitive the group is not in $\mathbf{AP}_{k,n}$. We collect those A for which $\langle A\rangle$ is intransitive.

As soon as a single independent imprimitive sequence is found the search terminates (as the group is not in $\mathbf{AP}_{k,n}$).

Otherwise we proceed as for $\mathbf{EP}_{k,n}$ and reduce sequences up to subgroup conjugacy and test that indeed all remaining sequences are primitive.

4.2. **Building groups belonging to $\mathbf{NEP}_{k,n}$ and $\mathbf{NAP}_{k,n}$.** According to GAP, up to degree 63, every primitive group in $\mathbf{NP}_{1,n}$ belongs to $\mathbf{NEP}_{2,n}$.

4.3. **A partial order and an equivalence relation on primitive groups.** Recall that, for a permutation group, $G \leq S_n$, the set of cycle-types of elements of G is said to be the *spectrum* of G. The relation *equality of spectrum* is obviously an equivalence relation on the subgroups of S_n, with conjugacy implying equality of spectrum. These equivalence classes can be ordered by inclusion of spectra, yielding a lattice that is an image of the lattice of classes of groups under inclusion.

We note that the spectrum cannot determine primitivity. The solutions to Wielandt's problem in Section 3 demonstrate this. Also, primitive group 4 in degree 25 – $5^2{:}Q(8)$ – has three maximal subgroups of index 2 which all are imprimitive and all have the same spectrum as the whole group.

The table below shows that affine groups with degrees that are perfect square predominate for small degrees, but the examples answering Wielandt's question show that there are others:

Degree	Groups with the same spectrum
9	$\{3^2{:}Q_8, 3^2{:}4\}$
16	$\{2^4.S_3 \times S_3, (A_4 \times A_4){:}2\}$
25	$\{5^2{:}D(2*4){:}2, 5^2{:}D(2*4)\}, \{5^2{:}((Q_8{:}3)'2), 5^2{:}4 \times D(2*3)\}$ $\{5^2{:}(Q_8{:}3), 5^2{:}Q_{12}\}$
49	$\{7^2{:}3 \times Q_{12}, 7^2{:}3 \times (Q_8{:}3)\}, \{7^2{:}3 \times Q_8, 7^2{:}12\},$ $\{7^2{:}(3 \times Q_{16}), 7^2{:}24\}, \{7^2{:}Q_{12}, 7^2{:}Q_8{:}3\}, \{7^2{:}Q_8, 7^2{:}4\}, \{7^2{:}Q_{16}, 7^2{:}8\}$
64	$\{2^6{:}(3^2{:}3){:}4, 2^6{:}(3^2{:}3){:}Q_8\}, \{2^6{:}(3 \wr A_3){:}2, 2^6{:}(3 \wr A_3){:}2\}$
81	$\{3^4{:}D_{16}, 3^4{:}SA_{16}, 3^4{:}SA_{16}{:}2, 3^4{:}D_{16}{:}2, 3^4{:}2^{2+2+1}, 3^4{:}Q_{16}{:}2, 3^4{:}2^{2+1+2}, 3^4{:}D_{16}{:}2, 3^4{:}SA_{16}{:}2,$ $3^4{:}2^{2+2+2}, 3^4{:}D_{16}{:}4\}, \{3^4{:}Q_8{:}2, 3^4{:}2^3{:}2^2, 3^4{:}(2 \times Q_8){:}2\},$ $\{3^4{:}SA_{16}{:}2, 3^4{:}Q_8{:}D_8, 3^4{:}2^{2+3+1}, 3^4{:}D_{16}{:}4, 3^4{:}(SA_{16}{:}2){:}2, 3^4{:}Q_{16}{:}D_8, 3^4{:}2^{2+3+1+1}, 3^4{:}2^{2+3+1+1}\},$ $\{3^4{:}(Q_8{:}3){:}2, 3^4{:}(Q_8{:}3){:}2^2\}, \{3^4{:}8.D_8, 3^4{:}8.D_8{:}2\}, \{3^4{:}D_{16}{:}4, 3^4{:}16{:}4\},$ $\{3^4{:}(8 \times D_{10}), 3^4{:}5{:}2^{2+1+2}\}, \{3^4{:}(Q_8{:}2){:}S_3, 3^4{:}Q_8.S_3{:}2, 3^4{:}Q_8.S_3{:}2, 3^4{:}Q_8.S_3{:}2^2\},$ $\{3^4{:}(SA_{16}{:}2){:}3, 3^4{:}(SA_{16}{:}2){:}6\}, \{3^4{:}(Q_8{:}3){:}4, 3^4{:}2^{3+2}{:}S_3\}, \{3^4{:}2^{2+3+1+1}, 3^4{:}2^{2+3+1+2}\},$ $\{3^4{:}(Q_8.S_3{:}2){:}2, 3^4{:}Q_8^2{:}6\}, \{3^4{:}4.A_6, 3^4{:}4.S_5\}, \{3^4{:}4.A_6, 3^4{:}4.S_5\}$

There is at least one easy way to guarantee two primitive groups of the same degree that are not isomorphic have the same spectrum.

Lemma 4.1. *Let K be a primitive group of degree m acting on Ω that is not a regular cyclic group of prime degree, and G and H nonisomorphic transitive subgroups of S_n with the same spectrum. Then $K \wr G$ and $K \wr H$ with the product action are nonisomorphic primitive groups with the same spectrum.*

Proof. That $K \wr G$ and $K \wr H$ are primitive follows from [11, Lemma 2.7.A.] as K is not cyclic of prime degree. Also, $K \wr G$ and $K \wr H$ are not isomorphic as G and H are not isomorphic [30, Theorem 10.3]. Clearly $K \wr G$ and $K \wr H$ are contained in $K \wr S_n$. It is also clear that as $K^n \leq (K \wr G) \cap (K \wr H)$, if $g \in K \wr G$ has cycle structure different from every element of $K \wr H$, it must be the case that g nontrivially permutes the coordinates of Ω^n. For $g \in K \wr S_n$, we denote the action of g on the coordinates of Ω^n by $\bar{g}$. Now, as G and H have the same spectrum, there exists $\bar{h} \in H$ with the same cycle structure as $\bar{g}$. Then $\bar{h}$ and $\bar{g}$ are conjugate in S_n, and so there exists $\delta \in K \wr S_n$ such that $\overline{\delta^{-1} g \delta} = \bar{h}$. But then $\delta^{-1} g \delta \in K \wr H$ and there is no element of $K \wr G$ of cycle structure different from that of g. Thus $K \wr G$ and $K \wr H$ have the same spectrum. □

Theorem 4.2. *There exist primitive groups G and H of the same degree n, with the same spectrum, and G is in $\mathbf{NEP}_{k,n}$ but H is not.*

Proof. Let $K \leq S_n$ be primitive but not cyclic of prime order generated by two elements (for example, a non-cyclic subgroup of $\mathrm{AGL}(1, q)$ for some prime q). There exists a nonabelian group G_1 of order p^5 for $p \geq 5$ a prime such that every element of G_1 has order p and G_1 is generated by two elements [7]. Let $H_1 = \mathbb{Z}_p^5$. Then the spectra of G_1 and H_1 are the same, and so by Lemma 4.1 $G = K \wr G_1$ and $H = K \wr H_1$ have the same spectrum and are not isomorphic. As H_1 is generated by five elements, we have that at least five elements are needed to generate H. So $H \in \mathbf{NEP}_{4,n}$. Let g_1 and g_2 generate

G_1 and g_3 and g_4 be elements of K^{p^5} that generate K in the first coordinate and are the identity in all others. Then $G = \langle g_1, g_2, g_3, g_4\rangle$ so that $G \notin \mathbf{NEP}_{4,n}$. □

There are infinite families of nonisomorphic primitive groups with the same spectrum.

Lemma 4.3. *Let $p \equiv 3 \pmod 4$. Then $p^2 : Q_8$ and $p^2 : 4$ are nonisomorphic primitive groups of degree p^2 with the same spectrum.*

Proof. First recall that $\mathrm{SL}(2, p)$ has order $(p^2-1)p$. As $p \equiv 3 \pmod 4$, a Sylow 2-subgroup of $\mathrm{SL}(2, p)$ has order 8. By [16, Theorem 8.3 (ii)] a Sylow 2-subgroup of $\mathrm{SL}(2, p)$ is generalized quaternion, and a Sylow 2-subgroup of $\mathrm{SL}(2, p)$ is Q_8. Let I be the 2×2 identity matrix. Then $-I \in \mathrm{SL}(2, p)$ and so is contained in a Sylow 2-subgroup Q of $\mathrm{SL}(2, p)$. As $Q \cong Q_8$ has a unique subgroup of order 2, namely $\langle -I\rangle$ whose only fixed point in its action on $\mathbb{F}_{p^2}$ is $(0, 0)$, we see that each element of order 4 in Q is a product of disjoint 4-cycles with one fixed point. Let $g \in Q$ be a 4-cycle, and $P = \{(i, j) \mapsto (i+a, j+b) : a, b \in \mathbb{Z}_p\}$ so that $P \lhd \mathrm{ASL}(2, p)$. Then $P \lhd \langle P, g\rangle = p^2 : 4$ is solvable, and by [13, Theorem 4 (4)] and Burnside's Theorem [11, Theorem 3.5B] a maximal solvable imprimitive subgroup of S_{p^2} with Sylow p-subgroup $\mathbb{Z}_p^2$ is $\mathrm{AGL}(1, p) \times \mathrm{AGL}(1, p)$. Again as $p \equiv 3 \pmod 4$ the group $\mathrm{AGL}(1, p) \times \mathrm{AGL}(1, p)$ has Sylow 2-subgroup $\mathbb{Z}_2^2$, and so $p^2 : 4$ is primitive. Then each primitive subgroup of $\mathrm{ASL}(2, p)$ of the form $p^2 : 4$ is a subgroup of index 2 in some subgroup of $\mathrm{ASL}(2, p)$ of the form $p^2 : Q_8$. Given that each element of order 4 in $p^2 : Q_8$ is a product of 4-cycles and one fixed point, it is easy to see that $p^2 : 4$ has the same spectrum as $p^2 : Q_8$. □

5. On the problems in [26]

Lopes [26] introduces two families of primitive permutations, proves results about them and asks a number of questions. In this section we recall the concepts, extend his results and answer some of the questions.

Definition 5.1. *Let n be a natural number and consider a partition $P = (p_1, p_2, \ldots, p_l)$ of n, for $l > 1$. If the p_i can be rearranged into subsets so that the sum of the elements of each subset is equal to a constant m, that divides n, then P is said to be an m-*partition*.*

If the largest part, say p_l, is divisible by m, and the remaining parts $p_1, \ldots, p_{l-1}$ can be rearranged in sets whose sum is equal to m, then we say that P is a special m-partition*. (Note that a special m-partition is not generally an m-partition!)*

These concepts can be illustrated by examples that we borrow from [26]. Consider $P = (2, 3, 5)$; this is an m-partition as the parts can be arranged into two sets $\{\{2, 3\}, \{5\}\}$, with the sum of the elements in each set being equal to 5. An example of a special m-partition, is $P = (2, 3, 10)$. The largest part (10) has 5 among its divisors, and the remaining parts can be rearranged in a set $\{2, 3\}$ whose sum is 5. Another example is $P = (1, 2, 5, 7, 17, 19, 23, 111)$. The largest part (111) has 37 among its divisors, and the other parts can be rearranged in sets adding up to that number: $\{\{2, 5, 7, 23\}, \{1, 17, 19\}\}$.

We state (and use Theorem 2.5 to prove) the main results of [26].

Theorem 5.2 ([26]). *Let Ω be a set of size n and let $P = (p_1, \ldots, p_l)$ be a partition of n, in which the p_i are pairwise distinct. Let S_n be the symmetric group on Ω. Then*

(1) *if $l = 2$ and p_1, p_2 are co-prime, then any permutation $g \in S_n$ of type P is primitive; if in addition $p_1, p_2 > 1$, then g is strongly primitive;*
(2) *if $l \geq 3$, the p_i are pairwise co-prime, and P is neither an m-partition nor a special m-partition, then any permutation in S_n of cycle-type P is strongly primitive.*

Proof. It is clear that a 2-part partition has non-empty i-type if and only if the two parts are not co-prime, giving half of (1). Let G be a primitive group containing a permutation of type $P = (p_1, p_2)$, with $p_1, p_2 > 1$. Since they are co-primes, it follows that G contains a p_1-cycle and a p_2-cycle. If one of them is a 2-cycle, then G is the symmetric group [2]. Otherwise, G contains a cycle of length smaller than $n - 2$, which by [21] implies that G contains the alternating group. The proof of (1) is complete.

Regarding (2), observe that as above a primitive group containing a permutation with such a cycle-type must contain a cycle of length at most $n - 2$, thus containing the alternating group. It remains to prove that a transitive group containing a permutation with such a cycle-type is primitive. Suppose that a partition with its parts pairwise co-prime is an i-partition of type (m, k). Let $(k_1, k_2, \ldots)$ be the corresponding partition of k. Then there are parts of size divisible by k_i summing to mk_i for each i. The pairwise co-prime condition shows that, for each i, either $k_i = 1$ (so there are some parts summing to m), or there is a single part of size mk_i. The second alternative can hold at most once (else there are two parts with a common factor m); if it holds once, then we have a special m-partition, otherwise an m-partition. This gives (2) and also shows how the two types of partitions emerge naturally. □

The next result extends to full classifications the partial results in [26]. To do this we only need to use [21].

Theorem 5.3 ([21, 26]). *Let Ω be a set of size n and let $P \in \{(1, n-1), (n)\}$ be a partition of n, in which the parts are pairwise distinct. Now we have the following:*

(1) *if $P = (1, n-1)$, then any permutation of this cycle-type is primitive, and a proper primitive group G contains a permutation of such type if and only if one of the following holds:*
  (a) $\mathrm{AGL}(d, q) \leq G \leq \mathrm{A\Gamma L}(d, q)$, *with $n = q^d$ and $d \geq 1$, for some prime power q;*
  (b) $G = \mathrm{PSL}(2, p)$ *or* $\mathrm{PGL}(2, p)$ *with $n = p + 1$ for some prime $p \geq 5$;*
  (c) $G = \mathrm{M}_{11}, \mathrm{M}_{12}$ *or* M_{24} *with $n = 12, 12$ or 24 respectively;*
(2) *if $P = (n)$, then*
  (a) *if n is prime, then every permutation in S_n is primitive, and the proper primitive groups containing a permutation of cycle-type P are the following:*
    (i) $C_p \leq G \leq \mathrm{AGL}(1, p)$, *with $n = p$ prime;*
    (ii) $\mathrm{PGL}(d, q) \leq G \leq \mathrm{P\Gamma L}(d, q)$ *with $n = (q^d - 1)/(q - 1)$ and $d \geq 2$ for some prime power q, and n prime;*
    (iii) $G = \mathrm{PSL}(2, 11), \mathrm{M}_{11}$ *or* M_{23} *with $n = 11, 11$ or 23 respectively;*

(b) *if n is not prime, then every n-cycle is an imprimitive permutation as the cyclic group it generates is imprimitive.*

In the end of his paper, Lopes [26] asks the following questions whose answers easily follow from our results:

(1) Is it always possible to identify the primitive permutations of a primitive group?
(2) Are there primitive permutations of cycle-type a relatively prime [special] m-partition?
(3) Are there primitive permutations whose cycle-types have parts with multiplicity greater than one, but the different parts are still mutually prime?

Regarding the last question, the partitions $P = (1, 1, n-2)$, for $n > 2$, satisfy the property and about them we have the following result.

Theorem 5.4. *A permutation of type $(1, 1, n-2)$ is primitive if and only if n is odd. In addition a degree n primitive group G contains a permutation of type $(1, 1, n-2)$ if and only if $\mathrm{PGL}(2, q) \leq G \leq \mathrm{P\Gamma L}(2, q)$, with $n = q + 1$ for some prime power q.*

Proof. The first part of the theorem is a simple consequence of Theorem 2.5. The second part of the result follows from [21]. □

Theorem 2.5 and Subsection 2.1 answer the first question above.

Finally, to solve question (2), suppose we have a m-partition of n, and suppose we can organize the parts in sets that sum up to k each. Then k must divide n (as the total sum is n) and a permutation of this cycle-type is found in the k-fold direct power of $S_{n/k}$. But this group lies in the imprimitive wreath product $S_{n/k} \wr S_k$. So the permutation cannot be primitive.

Alternatively, it can be shown that both m-partitions and special m-partitions are i-partitions, and therefore imprimitive. Let p be an m-partition with cycle-type $(a_1, a_2, \cdots, a_n)$. Now partition this partition into parts where the sum of the elements is m. All those parts are ic-partitions of type $(1, m)$, and therefore this new partition is a clustering. For special m-partitions, the argument is similar, except that we have a cluster where the larger part is alone.

As an example, consider the partitions given after the definition of m-partition. We have the partitions $P_1 = (2, 3, 5)$ and $P_2 = (2, 3, 10)$. For P_1, we have the clustering $\{(2, 3), (5)\}$, where the clusters are both $(1, 5)$ ic-partitions. For P_2, we have the clustering $\{(2, 3), (10)\}$, where the clusters are, respectively, a $(1, 5)$ ic-partition and a $(2, 5)$ ic-partition.

6. Problems

Problem 6.1. *Does Theorem 3.6 hold for all integers $q \geq 2$?*

Problem 6.2. *Are there primitive groups $G, H \leq S_n$ with the same spectrum, but such that G belongs to $\mathbf{NAP}_{k,n}$, but H does not?*

Problem 6.3. *Is there a natural transversal for the spectrum equivalence classes for the degree n primitive groups?*

Problem 6.4. *For every natural k is there a natural n such that $\mathbf{NEP}_{k,n}$ [$\mathbf{NAP}_{k,n}$] is non-empty?*

We observed that A_6 acting on pairs is a primitive group containing only imprimitive permutations; and also observed that since A_6 is 2-generated, there exists a primitive group containing no primitive permutation, but containing primitive pairs of imprimitive permutations. Therefore, the following theorem might be of some use to attack the previous problem.

Theorem 6.5. ([27]) *Let $G \leq S_n$ be a primitive permutation group. Then the smallest number of elements needed to generate G is at most*

$$\frac{C \log n}{\sqrt{\log \log n}},$$

where C is a universal constant.

Let $G \leq S_n$ and denote by $d(G)$ the smallest number of elements of G needed to generate this group. Let $m(n)$ be the maximum of the set $\{d(G) \mid G \leq S_n \text{ is primitive}\}$. To handle the previous question we certainly will need a very good lower bound for $m(n)$. So we propose the following problem.

Problem 6.6. *Let n be a natural number. Find good lower bounds for $m(n)$.*

Theorem 6.5 does not solve the problem (since when n is an odd prime then $m(n) = 2$), but it shows that the upper bound cannot be improved in general. See also [24, 34].

It is worth observing that by [4], every 2-homogeneous group G has $d(G) = 2$.

Problem 6.7. *Is it true that $\mathbf{NP}_{1,n}$ intersects every type of primitive groups in GAP's version of the O'Nan-Scott theorem?*

Answer similar questions for $\mathbf{NAP}_{k,n}$ and in $\mathbf{NEP}_{k,n}$.

Problem 6.8. *Classify the primitive groups in $\mathbf{NAP}_{k,n}$ and in $\mathbf{NEP}_{k,n}$.*

Problem 6.9. *Can the examples included in the tables of subsection 3 and subsection 4.3 be extended to infinite families?*

We saw above, for small values of n, that the class of $\mathbf{NP}_{1,n}$ is to a large extent contained in the class of non-synchronizing groups. Therefore the next question looks natural.

Problem 6.10. *Are there natural numbers n and m such that for every $k > m$ every group in $\mathbf{NAP}_{k,n}$ [$\mathbf{NEP}_{k,n}$] is non-synchronizing?*

The classification of synchronizing groups is still to be done. Here we propose an (hopefully) easier problem.

Problem 6.11. *Classify the synchronzing groups in which every element is an imprimitive permutation.*

7. Acknowledgments

The first author acknowledges that this work was developed within FCT projects CAUL (PEst-OE/MAT/UI0143/2014) and CEMAT-CIÊNCIAS (UID/Multi/04621/2013).

The second author acknowledges that this work was developed within Fundação Caluste Gulbenkian "Novos Talentos em Matemática 2015" grant.

The work of the fifth author was supported by Simons Foundation Collaboration Grant 244502.

References

[1] J. Araújo, W. Bentz, P. J. Cameron, G. Royle and A. Schaefer, Primitive groups and synchronization, *Proc. London Math. Soc.* (2016); doi: 10.1112/plms/pdw040

[2] J. Araújo and P. J. Cameron, Primitive groups synchronize non-uniform maps of extreme ranks, *Journal of Combinatorial Theory, Series B*, **106** (2014), 98–114.

[3] J. Araújo and P. J. Cameron, Two generalizations of homogeneity in groups with applications to regular semigroups, *Trans. Amer. Math. Soc.*, in press (published on-line 1 July 2015).

[4] J. Araújo and P. J. Cameron. Orbits of primitive k-homogenous groups on $(n-k)$-partitions with applications to semigroups. http://arxiv.org/abs/1512.05608

[5] J. Araújo, P. J. Cameron and B. Steinberg. Between primitive and 2-transitive: Synchronization and its friends *to appear.*

[6] F. Arnold and B. Steinberg, Synchronizing groups and automata, *Theoretical Computer Science* **359** (2006), 101–110.

[7] Bender, H. A., A determination of the groups of order p^5, *Ann. of Math. (2)*, **29** (1927/28), 61–72.

[8] Thomas Breuer, Subgroups of J_4 inducing the same permutation character, *Commun. Algebra* **23** (1995), 3173–3176.

[9] P. J. Cameron and P. A. Kazanidis, Cores of symmetric graphs, *J. Austral. Math. Soc.* **85** (2008), 145–154.

[10] Peter J. Cameron, Peter M. Neumann and D. N. Teague, On the degrees of primitive permutation groups, *Math. Z.* **180** (1982), 141–149.

[11] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[12] Persi Diaconis, Jason Fulman, and Robert Guralnick, On fixed points of permutations, *J. Algebraic Combin.* **28** (2008), 189–218.

[13] Edward Dobson and Dave Witte, Transitive permutation groups of prime-squared degree, *J. Algebraic Combin.* **16** (2002), 43–69.

[14] Sean Eberhard, Kevin Ford and Ben Green, Permutations fixing a k-set, https://arxiv.org/pdf/1507.04465.pdf

[15] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.2*; x2016. (www.gap-system.org)

[16] Daniel Gorenstein, *Finite groups* Harper & Row, New York, 1968.

[17] S. Guest, J. Morris, C. E. Praeger and P. Spiga, Finite primitive permutation groups containing a permutation having at most four cycles. Journal of Algebra, **454** (2016), 233–251.

[18] Robert Guralnick and Jan Saxl, Primitive permutation characters *Groups, Combinatorics and Geometry* (Durham, 1990), 364–367, London Math. Soc. Lecture Note Ser., **165**, Cambridge Univ. Press, Cambridge, 1992.

[19] A. Hulpke. Konstruktion Transitiver Permutationsgruppen. Thesis, RWTH Aachen, (1996)

[20] A. Hulpke. Constructing transitive permutation groups. J. Symbolic Comput. 39 (2005), no. 1, 1–30.

[21] G. Jones. Primitive permutation groups containing a cycle. Bull. Australian Math. Soc. 89 (2014), no. 1, 159–165.

[22] C.S.H. King. Generation of finite simple groups by an involution and an element of prime order. http://arxiv.org/pdf/1603.04717v1.pdf

[23] D.E. Knuth. The Art of Computer Programming, Volume 4A: Combinatorial Algorithms Part 1, Addison-Wesley, 2011.

[24] L.G. Kovács and M. F. Newman, Generating transitive permutation groups. Quart. J. Math. Oxford (2) **39** (1988), 361–372.

[25] M.W. Liebeck and J. Saxl. Primitive permutation groups containing an element of large prime order J. Lond. Math. Soc., **31** (1985), 237–249.

[26] P. Lopes. Permutations which make transitive groups primitive. Cent. Eur. J. Math. **7** (2009), no. 4, 650–659.

[27] A. Lucchini, F. Menegazzo and M. Morigi, Assymptotic results for primitive permutation groups and irreducible linear groups, *J. Algebra* **223** (2000), 154–170.

[28] T. Łuczak, and L. Pyber, On random generation of the symmetric group, *Comb. Probab. Comput.* **2** (1993), 505–512.

[29] P. Müller. Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials. Ann. Sc. Norm. Super. Pisa Cl. Sci., **12** (2013), 369–438.

[30] Peter M. Neumann, On the structure of standard wreath products of groups. Math. Z., **84**, (1964) 343–373.

[31] Peter M. Neumann, Primitive permutation groups and their section-regular partitions, *Michigan Math. J.* **58** (2009), 309–322.

[32] C. E. Praeger. Permutations and polynomial factorisation. `http://istanbulgroup2013.dogus.edu.tr/invited/C.Praeger.pdf`

[33] Gareth Tracey, Minimal generation of transitive permutation groups, `http://arxiv.org/pdf/1504.07506.pdf`

[34] Gareth Tracey, Generating minimally transitive permutation groups. `http://arxiv.org/pdf/1506.04256.pdf`

[35] Helmut Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964. MR MR0183775 (32 #1252)

Universidade Aberta and CEMAT-Ciências Faculdade de Ciências, Universidade de Lisboa, 1749-016, Lisboa, Portugal
E-mail address: `jjaraujo@fc.ul.pt`

Instituto Superior Técnico, Universidade de Lisboa, 1749-016, Lisboa, Portugal
E-mail address: `joao.p.araujo@tecnico.ulisboa.pt`

Mathematical Institute, University of St Andrews, St Andrews, Fife KY16 9SS, Scotland
E-mail address: `pjc20@st-andrews.ac.uk`

Department of Mathematics and Statistics, Mississippi State University, PO Drawer MA Mississippi State, MS 39762 USA, and IAM, University of Primorska, Koper 6000, Slovenia
E-mail address: `dobson@math.msstate.edu`

Department of Mathematics, Colorado State University, 1874 Campus Delivery, Fort Collins, CO 80523-1874, USA
E-mail address: `hulpke@math.colostate.edu`

Department of Mathematics and CAMGSD, Instituto Superior Técnico, Universidade de Lisboa, 1049-001, Lisboa, Portugal
E-mail address: `pelopes@math.tecnico.ulisboa.pt`