Groups generated by derangements

R. A. Bailey*, Peter J. Cameron*,
Michael Giudici† and Gordon F. Royle†

Abstract

We examine the subgroup $D(G)$ of a transitive permutation group G which is generated by the derangements in G. Our main results bound the index of this subgroup: we conjecture that, if G has degree n and is not a Frobenius group, then $|G : D(G)| \leqslant \sqrt{n} - 1$; we prove this except when G is a primitive affine group. For affine groups, we translate our conjecture into an equivalent form regarding $|H : R(H)|$, where H is a linear group on a finite vector space and $R(H)$ is the subgroup of H generated by elements having eigenvalue 1.

If G is a Frobenius group, then $D(G)$ is the Frobenius kernel, and so $G/D(G)$ is isomorphic to a Frobenius complement. We give some examples where $D(G) \neq G$, and examine the group-theoretic structure of $G/D(G)$; in particular, we construct groups G in which $G/D(G)$ is not a Frobenius complement.

Keywords: permutation group, derangement, Frobenius group, linear group

MSC: 20B05

1 Introduction

Jordan proved in 1872 that a finite transitive permutation group G of degree $n > 1$ must contain a derangement (an element with no fixed points). The

*School of Mathematics and Statistics, University of St Andrews, St Andrews, Fife KY16 9SS, UK

†Centre for the Mathematics of Symmetry and Computation, University of Western Australia, Crawley, WA 6009, Australia

existence of such elements is important in various contexts in number theory and elsewhere [8, 17, 18]. It is known that there must be many derangements (at least $|G|/n$, see [5]), and that at least one has prime power order [8]. We are interested here in the subgroup $D(G)$ of G generated by the derangements in G.

In most cases, $D(G) = G$. For example, of the 3302368 transitive groups of degree from 2 to 47 inclusive as classified in [12] and available in MAGMA [2], only 893 have $D(G) \neq G$ (of which 103 are Frobenius groups); and, of the 24558 primitive groups of degree from 2 to 4095 inclusive as classified in [7] and available in MAGMA, only 9155 have $D(G) \neq G$ (of which 7872 are Frobenius groups).

The subgroup $D(G)$ was first considered by H. Zantema [18], who proved the first two parts of the following theorem. We include the proof since we extend the ideas to prove the rest of the theorem. Here and throughout the paper, if G is a permutation group on Ω, then G_α denotes the stabiliser of the point α of Ω.

Theorem 1.1. *Let G be a transitive permutation group on the finite set Ω, and $N = D(G)$ the (normal) subgroup generated by the derangements in G. Then the following hold.*

(a) *N is transitive.*

(b) *N contains every element of G whose number of fixed points is different from 1.*

(c) *If r_G and r_N denote the permutation ranks of G and N, then*

$$r_N - 1 = (r_G - 1)|G : N|.$$

(d) *The N-orbits on ordered pairs of distinct elements are permuted semiregularly by G/N; equivalently, for $\alpha \in \Omega$, the N_α-orbits different from $\{\alpha\}$ are permuted semiregularly by G_α/N_α.*

Any Frobenius group G gives an example with $D(G) \neq G$; for in this case $D(G)$ is the Frobenius kernel, and its index is the order of a point stabiliser. (This corresponds to the case in Theorem 1.1 where $N_\alpha = \{1\}$.) So, in a sharply 2-transitive group of degree n, we have $|G : D(G)| = n - 1$. On the other hand, by part (d) of the theorem, the index cannot be larger than $n - 1$ (and indeed divides $n - 1$), where $n = |\Omega|$. Equality implies that

$r_G = 2$ (so that G is 2-transitive), and $r_N = n$ (so that N is regular, and G is a Frobenius group). Since the degree of a 2-transitive Frobenius group is a prime power, we have shown:

Corollary 1.2. *If G is a transitive permutation group of degree $n > 1$, then $|G : D(G)|$ divides $n-1$; equality is possible if and only if n is a prime power.*

We also obtain the following corollary.

Corollary 1.3. *Let G be a transitive permutation group on the finite set Ω, and suppose that $D(G) \neq G$. Let G_α be the stabiliser of $\alpha \in \Omega$, acting on the remaining points. Then at least half the elements of G_α are derangements, and $G_\alpha = D(G_\alpha)$.*

It follows, for example, that if G is a Zassenhaus group (a 2-transitive group in which the point stabiliser is a Frobenius group) then $D(G) = G$.

Our main interest is in proving better bounds in the case when G is not a Frobenius group. We prove the following two theorems:

Theorem 1.4. *If G is a transitive imprimitive permutation group of degree n, then $|G : D(G)| \leqslant \sqrt{n} - 1$. Equality is possible if n is an even power of a prime.*

Theorem 1.5. *If G is a primitive permutation group of degree n which is not of affine type, then $|G : D(G)| \leqslant \sqrt{n} - 1$.*

We conjecture that the same bound is true for all primitive groups which are not Frobenius groups:

Conjecture 1.1. If G is a primitive permutation group of degree n which is not a Frobenius group, then $|G : D(G)| \leqslant \sqrt{n} - 1$; moreover, this bound is attained only if G is an affine group.

For the first part of this conjecture, it suffices to consider affine groups, and we explain in Section 3 the partial results we have obtained on this. The second part follows from the first together with our results on non-affine primitive groups, where we obtain substantially better bounds in all cases. For example, groups of twisted wreath product type satisfy $D(G) = G$, and almost simple groups with $D(G) \neq G$ can be completely classified. See Section 5 below.

Another question we pose is the following:

Question 1.2. Which groups can arise as $G/D(G)$ for some transitive permutation group G?

We have no example of a group H which cannot be isomorphic to $G/D(G)$ for any transitive finite permutation group G, but the evidence is far too thin to support the conjecture that all groups arise.

If G is a Frobenius group, then $D(G)$ is the Frobenius kernel, and so $G/D(G)$ is isomorphic to the Frobenius complement. The structure of Frobenius complements was determined by Zassenhaus; either such a group is metacyclic, or it has a normal subgroup of index at most two which is isomorphic to the direct product of $\mathrm{SL}(2,3)$ or $\mathrm{SL}(2,5)$ and a metacyclic group. See Passman [16] for an account of this.

There are transitive groups with $G/D(G)$ not isomorphic to a Frobenius complement, though they are rather rare. The smallest degree of a primitive group with this property is 625; there are primitive groups of this degree for which $G/D(G)$ is isomorphic to the Klein group V_4 or the symmetric group S_3. In the final section of the paper, we construct a number of further examples of this phenomenon.

2 Proofs of the basic results

We begin with the proof of Theorem 1.1. As noted, parts (a) and (b) are due to H. Zantema [18], and are repeated here since we will push the arguments a little further to prove the rest of the theorem.

Proof. Let π be the permutation character. Since G is transitive, the Orbit-Counting Lemma gives

$$\sum_{g\in G}(\pi(g)-1)=0.$$

Now similarly

$$\sum_{g\in N}(\pi(g)-1)=(k-1)|N|,$$

where k is the number of N-orbits. So

$$\sum_{g\in G\setminus N}(\pi(g)-1)=-(k-1)|N|.$$

But every term in the sum on the left is non-negative, since all the elements with $\pi(g)-1<0$ lie in N. We conclude that both sides are zero. The

right-hand side shows that $k = 1$, and the left-hand side contains no terms with $\pi(g) > 1$, so all such elements lie in N. This proves (a) and (b).

For (c), note that

$$\begin{aligned} |G|(r_G - 1) &= \sum_{g \in G} (\pi(g)^2 - 1), \\ |N|(r_N - 1) &= \sum_{g \in N} (\pi(g)^2 - 1). \end{aligned}$$

Since every element of $G \setminus N$ has $\pi(g) = 1$, the two displayed expressions are equal, which proves (c).

Finally, (d) follows from (c) since the $r_N - 1$ orbits of N on ordered pairs of distinct elements fall into $r_G - 1$ orbits under the action of G/N. □

We mention another derivation of (b) from (a), since we will need this later. This depends on the following (well-known) generalisation of the Orbit-Counting Lemma. For completeness, we give the proof.

Lemma 2.1. *Let G be finite transitive permutation group on Ω, and t an arbitrary permutation on Ω. Then the average number of fixed points of elements in the coset tG is 1.*

Proof. We follow the usual proof of the Orbit-Counting Lemma. If G is transitive on Ω, with $|\Omega| = n$, count pairs (α, g) for which $\alpha \in \Omega$, $g \in G$, and $\alpha tg = \alpha$. For each of the n choices of α, there are $|G|/n$ elements $g \in G$ mapping αt to α; so there are $|G|$ such pairs. Counting the other way, we sum the numbers of fixed points of elements in the coset tG. □

Now suppose that $g \in G \setminus D(G)$. By (a) and Lemma 2.1, the average number of fixed points of elements of $gD(G)$ is 1, but none of these elements is a derangement; so all have exactly one fixed point.

Proof of Corollary 1.3 Since $D(G)$ is transitive, $|G_\alpha : G_\alpha \cap D(G)| = |G : D(G)| > 1$. But all the elements of G_α not in $D(G)$ are derangements (they fix only α); so there are at least $|G_\alpha|/2$ derangements in G_α, and they generate G_α (since any group is generated by the complement of any proper subgroup). □

Proof of Theorem 1.4 Let $N = D(G)$, and $H = G/N$. By Corollary 1.2 we have that $|H|$ divides $n-1$. Moreover, as N is transitive we have $|H| = |G : N| = |G_\alpha : N_\alpha|$. Furthermore, by Theorem 1.1(d), G_α/N_α permutes the N_α-orbits different from $\{\alpha\}$ semiregularly.

Suppose that G is imprimitive, with ℓ blocks of size k, where $k\ell = n$. Then G_α permutes among themselves the N_α-orbits in the block containing α; so $|H|$ divides $k-1$. Then also $|H|$ divides $n-k = k(\ell-1)$, and since $|H|$ is coprime to k, we see that $|H|$ divides $\ell-1$. But $\min\{k,\ell\} \leqslant \sqrt{n}$, and so the result follows.

Equality can be attained if n is a prime power (and a square). Let V be a 2-dimensional vector space over the finite field F. Then the semi-direct product of the additive group of V and the multiplicative group of F is a Frobenius group of order $|F|^2(|F|-1)$. □

3 Affine groups

In this section we consider affine groups.

3.1 Preliminaries and a conjecture

Let V be a d-dimensional vector space over the field of order q. Let T be the translation group of V, and H a linear group on V (a subgroup of $\mathrm{GL}(d,q)$). Then the semidirect product $G = T \rtimes H$ is a transitive permutation group on V; it is primitive if and only if the linear group H is irreducible.

Given a linear group H, we let $R(H)$ be the subgroup of H generated by elements which have an eigenvalue 1 in their action on V.

Proposition 3.1. *With the above notation, $D(G)$ is the semidirect product $T \rtimes R(H)$. In particular, $G/D(G) \cong H/R(H)$, and so $|G : D(G)| = |H : R(H)|$.*

Proof. Clearly $T \leqslant D(G)$. By Lemma 2.1, the average number of fixed points of elements in a coset hT (for $h \in H$) is 1; so there are two possibilities:

- some element of hT is a derangement, in which case $hT \subseteq D(G)$ and $h \in D(G)$;
- every element of hT has exactly one fixed point; then h fixes the zero vector and no other, so no eigenvalue of h is equal to 1.

So $hT \subseteq D(G)$ if and only if $h \in R(H)$, and the result follows. □

Thus, using Theorems 1.1 and 1.4 and Corollary 1.2, we can formulate a result and a conjecture which if true would settle our main conjecture for primitive groups.

Proposition 3.2. *If H is any subgroup of $\mathrm{GL}(d,q)$, then $|H : R(H)| \leqslant q^d - 1$, and $H/R(H)$ permutes the $R(H)$-orbits semiregularly. If H is reducible, then $|H : R(H)| \leqslant q^{d/2} - 1$.*

Conjecture 3.1. If H is an irreducible subgroup of $\mathrm{GL}(d,q)$, then either H acts semiregularly on the non-zero vectors of V, or $|H : R(H)| \leqslant q^{d/2} - 1$.

3.2 An example

In this subsection, we give an example to show that the bound $|G : D(G)| \leqslant \sqrt{n} - 1$, if true, is best possible for primitive groups which are not Frobenius groups, by giving an example meeting the bound.

Let q be a prime power, and G the group

$$\{x \mapsto ax^i + c \mid a, c \in F, a \neq 0, i \in \{1, q\}\}$$

of permutations of the field F of order q^2. Then G is a 2-transitive (and hence primitive) group of degree q^2, which is not a Frobenius group since the map $x \mapsto x^q$ fixes 0 and 1.

Let $A = \{a \in F \mid a^{q+1} = 1\}$, and let H be the subgroup of G consisting of the transformations of the above form with $a \in A$. Notice that A is the set of $(q-1)^{st}$ powers of non-zero elements of F.

Clearly, the group $T = \{x \mapsto x + c : c \in F\}$ of translations is contained in $D(G)$. Now consider the map $x \mapsto ax^q$. The point x is fixed if and only if $x = 0$ or $x^{-(q-1)} = a$. Let $a \in A$. Then the equation $x^{-(q-1)} = a$ has $q - 1$ solutions, and so by Theorem 1.1(b) the map $x \mapsto ax^q$ belongs to $D(G)$. Composing this with the element $x \mapsto x^q$ (which is in $D(G)$) we see that the map $x \mapsto ax$ also lies in $D(G)$. Thus $H \leqslant D(G)$.

We now consider the transformations not in H. We separately consider transformations of the form $x \mapsto ax + c$ and $x \mapsto ax^q + c$, where in both cases $a \notin A$. In the former case, it is easy to see that $x \mapsto ax + c$ has a unique fixed point, namely $x = c/(1 - a)$, for all $a \neq 1$, and in particular for all $a \notin A$. In the latter case, as there are no non-zero solutions to the

equation $x = ax^q$, the transformation $x \mapsto x - ax^q$ has trivial kernel and therefore is surjective. In particular, there is a unique value of x such that $x - ax^q = c$ and thus a unique fixed point for the transformation $x \mapsto ax^q + c$. Hence every transformation outside H has a unique fixed point, and so H contains all derangements. Thus $H \geqslant D(G)$. As we have already seen that $H \leqslant D(G)$, equality holds. It is then clear that $G/D(G)$ has order $q - 1$.

4 Examples

In this section, we describe a few examples of non-affine groups G with $D(G) \neq G$. Further affine examples appear in the final section.

There is no useful product construction. For suppose that G_1 and G_2 are transitive on Ω_1 and Ω_2, and consider $G_1 \times G_2$ acting on $\Omega_1 \times \Omega_2$. Then an element $(g_1, g_2) \in G_1 \times G_2$ is a derangement if and only if either g_1 or g_2 is a derangement. So $D(G_1 \times G_2)$ contains both $D(G_1) \times G_2$ and $G_1 \times D(G_2)$, and hence it is equal to $G_1 \times G_2$.

4.1 General remarks

Before giving some more examples we note a couple of useful lemmas.

Lemma 4.1. *Let G be a primitive permutation group with socle N. Then $N \leqslant D(G)$.*

Proof. If N is the unique minimal normal subgroup of G then clearly $N \leqslant D(G)$, as $D(G) \neq 1$ by Jordan's result. If N is not the unique minimal normal subgroup of G, then by a well-known "folklore" result (see [4, Theorem 4.4]), $N = M_1 \times M_2$, where M_1 and M_2 are regular. Hence we also have $N \leqslant D(G)$ in this case as well. □

Lemma 4.2. *Let $G = N \rtimes \langle \sigma \rangle$ be a permutation group on the finite set Ω such that σ has order a power of the prime p, with p coprime to $|N|$. If $C_G(\sigma) \leqslant G_\alpha$ for $\alpha \in \Omega$, then $D(G) \leqslant N$.*

Proof. Let $g \in G \backslash N$. If g has order a power of p then Sylow's Theorem implies that g is conjugate to an element of $\langle \sigma \rangle$ and hence fixes a point of Ω. Suppose that g does not have order a power of p. Then $|g| = mp^i$ for some $i > 0$ and with $\gcd(m, p) = 1$. Thus there exist $a, b \in \mathbb{Z}$ such that $am + bp^i = 1$ and so $g = (g^{p^i})^b (g^m)^a$. Now we have written g as the

product of two commuting elements, one of which (namely $(g^m)^a$) has order a nontrivial power of p. Thus g is conjugate to an element of the form $x\sigma^i$ for some $x \in C_G(\sigma)$. Hence g is conjugate to an element of $C_G(\sigma)$ and so fixes a point. Thus all derangements in G lie in N. □

4.2 The examples

Almost simple groups

(a) Let $G = \mathrm{P\Gamma L}(2, 2^p) = N \rtimes \langle\sigma\rangle$, where $N = \mathrm{PGL}(2, 2^p)$ for p an odd prime, and σ a field automorphism of order p, acting on the set Δ of right cosets of a subgroup $H = C_{2^p+1} \rtimes C_{2p} \geqslant C_G(\sigma)$ of index $2^{p-1}(2^p - 1)$. When $p = 3$, a MAGMA calculation shows that $D(G) = \mathrm{PGL}(2, 2^p)$. For $p \geqslant 5$ we have that p is coprime to $|\mathrm{PGL}(2, 2^p)|$ and so Lemma 4.2 implies that $D(G) = \mathrm{PGL}(2, 2^p)$. Thus for all primes p we have $|G : D(G)| = p$.

(b) Let $G = \mathrm{PSL}(d, p^f) \rtimes \langle\varphi\rangle$ where f is a power of a prime r which does not divide $|\mathrm{PSL}(d, p^f)|$, and φ is a field automorphism of $\mathrm{PSL}(d, p^f)$ of order f. Let $H = \mathrm{PSL}(d, p) \times \langle\varphi\rangle$ and let G act on the set of right cosets of H. Then by Lemma 4.2 we have that $D(G) = \mathrm{PSL}(d, p^f)$. (The fact that all derangements in G lie in $\mathrm{PSL}(d, p^f)$ was previously observed in [11].)

Product action Let N be $\mathrm{PGL}(2, 2^p)$ in the action on Δ defined in part (a) above, with $p \geqslant 5$. Let $G = N^p \rtimes \langle g\rangle$ act on $\Omega = \Delta^p$, where $g = (\sigma, 1, \ldots, 1)(1, 2, \ldots, p)$. Then g has order p^2 and we can choose $\alpha \in \Omega$ such that $G_\alpha = H^p \rtimes \langle g\rangle$. Moreover, $C_G(g) = \{(h, \ldots, h) \mid h \in C_N(\sigma)\} \rtimes \langle g\rangle \leqslant G_\alpha$. Thus Lemma 4.2 implies that $D(G) = N^p$ and so $|G : D(G)| = p^2$.

Diagonal action Let T be a non-abelian simple group, and p be a prime coprime to $|T|$. Let $G = T^p \rtimes \langle\sigma\rangle$ where σ has order p and permutes the p simple direct factors of T^p. Then $C_G(\sigma) = \{(t, \ldots, t) \mid t \in T\} \times \langle\sigma\rangle$. In its action on the cosets of $C_G(\sigma)$, G is a primitive group of diagonal type on a set of size $|T|^{p-1}$. Any element of T^p that is trivial in all but exactly one of the coordinates is a derangement and so $T^p \leqslant D(G)$ and then Lemma 4.2 implies that $D(G) = T^p$.

5 Primitive groups

We now consider the various types of primitive groups, and prove Theorem 1.5 in all cases. By the O'Nan-Scott Theorem, a primitive group that does not preserve a product structure on Ω is either almost simple, affine or diagonal type. See for example [4].

5.1 Diagonal type

We note the following famous result, see [9, Theorem 1.48].

Lemma 5.1. *Let T be a non-abelian finite simple group and let $\tau \in \mathrm{Aut}(T)$. Then there exists $t \in T\backslash\{1\}$ such that $t^\tau = t$.*

We also need the following lemma.

Lemma 5.2. *Let G be a transitive permutation group on Ω with a regular non-abelian minimal normal subgroup. Then $G = D(G)$.*

Proof. Let N be a non-abelian regular minimal normal subgroup of G. Then $N \cong T^k$ for some non-abelian simple group T, and $N \leqslant D(G)$. Note that, for $\alpha \in \Omega$, we have $G = N \rtimes G_\alpha$. Moreover, we can identify Ω with N such that, for $\alpha = 1_N$, each nontrivial element of G_α acts as a nontrivial automorphism of N. Let $g \in G_\alpha$ and write $g = (\tau_1, \ldots, \tau_k)\sigma$ where each $\tau_i \in \mathrm{Aut}(T)$ and $\sigma \in S_k$. Suppose that $(i_1, i_2, \ldots, i_r)$ is a cycle of σ. By Lemma 5.1, there exists $t \in T\backslash\{1\}$ such that $\tau_{i_1}\tau_{i_2}\ldots\tau_{i_k}$ fixes t. Let $t_{i_1} = t$ and for each $j \in \{2, \ldots, r\}$ let $t_{i_j} = t^{\tau_{i_1}\cdots\tau_{i_{j-1}}}$. Doing this for each cycle of σ we construct a nontrivial element $\beta = (t_1, \ldots, t_k) \in N$ such that $\beta^g = \beta$. Hence g has at least two fixed points and so by Theorem 1.1(b) we have that $g \in D(G)$. Since $G = N \rtimes G_\alpha$ it follows that $G = D(G)$. □

We are now able to obtain a bound for $|G : D(G)|$ when G is primitive of diagonal type.

Lemma 5.3. *Let G be primitive of diagonal type and $G \neq D(G)$. Then the socle of G is $N = T^p$ for some non-abelian finite simple group T and some odd prime p not dividing $|T|$, and G induces a cyclic group of prime order on the set of p simple direct factors of N. Moreover, $|G : D(G)| = p$.*

Proof. Let $N = T^k$ be the socle of G and let $\alpha \in \Omega$. We may assume that $N_\alpha = \{(t, t, \ldots, t) \mid t \in T\}$ and by Lemma 4.1 we have $N \leqslant D(G)$. Since N is transitive we have $G = NG_\alpha$. Thus it remains to determine which elements of G_α lie in $D(G)$.

Let $\pi\colon G \to S_k$ be the permutation representation of G on the set of k simple direct factors of N. By Lemma 5.2 we only need to consider the case where $\pi(G)$ is transitive and primitive. Since $G = NG_\alpha$ we have that $\pi(G) = \pi(G_\alpha)$. Now $G_\alpha \leqslant \mathrm{Aut}(T) \times S_k$. Identifying Ω with the set of cosets of N_α in N we see that for $\tau \in \mathrm{Aut}(T)$ we have $(N_\alpha(t_1, \ldots, t_k))^\tau = N_\alpha(t_1^\tau, \ldots, t_k^\tau)$, while for $\sigma \in S_k$ we have $(N_\alpha(t_1, \ldots, t_k))^\sigma = N_\alpha(t_{1^{\sigma^{-1}}}, \ldots, t_{k^{\sigma^{-1}}})$.

Let X be the preimage in G_α of the stabiliser in S_k of the first entry and let $g = \tau\sigma \in X$ with $\tau \in \mathrm{Aut}(T)$ and $\sigma \in S_k$. By Lemma 5.1, there exists $t \in T\backslash\{1\}$ such that $t^\tau = t$. Then g fixes both the coset N_α and the coset $N_\alpha(t, 1, \ldots, 1)$. It follows from Theorem 1.1(b) that $X \leqslant D(G)$. Since $\pi(G)$ is a primitive subgroup of S_k, X is a maximal subgroup of G_α. Suppose first that $\pi(X) \neq 1$. Then there exists $h \in G_\alpha\backslash X$ such that h fixes the second simple direct factor of N. Then h fixes the two distinct cosets N_α and $N_\alpha(1, t, 1, \ldots, 1)$, where $t \in T$ is fixed by τ. This again implies that $h \in D(G)$ and since $G_\alpha = \langle X, h\rangle$ it follows that $G_\alpha \leqslant D(G)$. Thus $G = D(G)$. Hence if $G \neq D(G)$ then we must have that $\pi(X) = 1$, that is, $\pi(G)$ is a regular primitive subgroup of S_k. Thus k is a prime, $\pi(G) = C_k$, $D(G) = NX$ and $|G : D(G)| = |G : NX| = k$.

It remains to show that k is coprime to $|T|$. Suppose to the contrary that k divides $|T|$. Choose $g \in G \setminus NX$. Without loss of generality, $g = \tau(1, 2, \ldots, k)$. Since τ and $(1, \ldots, k)$ commute, we can choose g so that τ has order a power of k (raising g to a power coprime to k if necessary). Now we can find $s \in T$ with order k and fixed by τ, as follows: let P be a Sylow k-subgroup of $T\langle\tau\rangle$ containing τ, and choose s to be an element of order k in $Z(P) \cap T$.

Consider the coset $N_\alpha(s, s^2, \ldots, s^{k-1}, 1)$. We have

$$\begin{aligned}(N_\alpha(s, s^2, \ldots, s^{k-1}, 1))^g &= N_\alpha(1, s^\tau, (s^\tau)^2, \ldots, (s^\tau)^{k-1})\\ &= N_\alpha(1, s, s^2, \ldots, s^{k-1})\\ &= N_\alpha(s, s^2, \ldots, s^{k-1}, 1).\end{aligned}$$

Thus g fixes two elements of Ω and so by Theorem 1.1(b) it follows that $g \in D(G)$. Since $G = \langle NX, g\rangle$, it follows that $G = D(G)$, a contradiction. Hence k is coprime to $|T|$.

By the Odd Order Theorem, k is odd. □

5.2 Product action

Now we discuss the product action case. By [14, (2.2)], we may assume that G is contained in $H \wr K$, where H is the group induced on one coordinate by its stabiliser in G, and K the permutation group induced on the coordinates; thus $n = m^k$, where m and k are the degrees of H and K respectively.

Proposition 5.4. *With the above hypotheses,*

$$|G : D(G)| \leqslant k|H : D(H)|.$$

Proof. Let G_1 be the subgroup of G fixing a coordinate. Then $|G : G_1| = k$, and there is an epimorphism $\phi\colon G_1 \to H$. Let $G_2 = D(H)\phi^{-1}$, so that $|G_1 : G_2| = |H : D(H)|$. So we are done if we can show that $G_2 \leqslant D(G)$.

But a generator of G_2 has no fixed points on the first coordinate of the product space, so has no fixed points on the whole space. (If a tuple is fixed then all its coordinates must be fixed.) The result follows. □

We note that the product action examples given in Section 4.2 show that this bound is sharp.

Corollary 5.5. *If the primitive group G is contained in a wreath product action as above, and G is not a Frobenius group, then $|G : D(G)| \leqslant \sqrt{n} - 1$.*

Proof. We have $|H : D(H)| \mid m - 1$. Note that primitivity requires $m > 2$. If $k, m \geqslant 3$, then $k(m-1) \leqslant m^{k/2} - 1$ except for the cases $k = 3$, $3 \leqslant m \leq 7$. These cases can be tested by computer, and give no counterexamples.

Suppose that $k = 2$, so that $G \leqslant H \wr C_2$. If $|H : D(H)| < m - 1$, then $|H : D(H)| \leqslant (m-1)/2$, and so $|G : D(G)| \leqslant m - 1$ by Proposition 5.4, as required. So we may assume that $|H : D(H)| = m - 1$, so that H is sharply 2-transitive. Thus, $H = P \rtimes Q$, where P is the Frobenius kernel and Q the complement.

The intersection K of G with the base group of the wreath product is a subdirect product of two copies of H, containing $P \times P$ and invariant under an interchange of the factors. This is an extension of R^2 by C, where $R \geqslant P$ has order rm, say, and C is a quotient of Q of order $(m-1)/r$. So

$|K| = m^2(m-1)r$. Now $R^2 \leqslant D(G)$, since each element of one factor can be combined with a derangement in the other to give a derangement in G. So $|G| = 2m^2(m-1)r$ and $|D(G)| \geq (rm)^2$, giving $|G : D(G)| \leqslant 2(m-1)/r$. So we are done unless $r = 1$, in which case $R = P$.

In this case, if $D(G) = P^2$, then it is regular, and so G is a Frobenius group; if not, then $|D(G)| \geqslant 2m^2$, and so $|G : D(G)| \leqslant m-1$, as required. □

5.3 Almost simple type

We now prove Theorem 1.5 for almost simple primitive groups.

Lemma 5.6. *Let G be an almost simple primitive permutation group of degree n. Then $|G : D(G)| \leqslant \sqrt{n} - 1$.*

Proof. If G is almost simple with socle T then, by Lemma 4.1, $T \leqslant D(G) \leqslant G \leqslant \mathrm{Aut}(T)$, so $|G : D(G)|$ is bounded by the order of the outer automorphism group of T. On the other hand, n is at least the degree n_0 of the smallest faithful permutation representation of T. The outer automorphism group of a sporadic simple group has order at most 2, while from [6] we see that $n_0 \geqslant 11$. Similarly, the outer automorphism group of A_n has order 2 unless $n = 6$, while $n_0 = n$. The values for n_0 when T is a group of Lie type are given in [10, Table 4] and the values for $|\mathrm{Out}(T)|$ are given in [13, Tables 5.1A and 5.1B]. We find that the only simple groups T for which $|\mathrm{Out}(T)| > \sqrt{n_0} - 1$ are:

- $T = A_n$ $(n = 5, 7, 8)$, $|\mathrm{Out}(T)| = 2$, $n_0 = n$;
- $T = A_6$, $|\mathrm{Out}(T)| = 4$, $n_0 = 6$;
- $T = \mathrm{PSL}(3, 2)$, $|\mathrm{Out}(T)| = 2$, $n_0 = 7$;
- $T = \mathrm{PSL}(3, 4)$, $|\mathrm{Out}(T)| = 12$, $n_0 = 21$;
- $T = \mathrm{PSL}(2, 2^f)$ $(f = 3, 4, 5)$, $|\mathrm{Out}(T)| = f$, $n_0 = 2^f + 1$.

Thus if G is a counterexample, either $n < 36$ or $T = \mathrm{PSL}(3, 4)$ and $n < 169$. A Magma calculation shows that no such counterexamples exist. □

In this case we can say much more. The memoir by Guralnick, Müller and Saxl [11] defines a pair of permutation groups (X, Y) to be *exceptional* if $Y \lhd X$ and X fixes no non-trivial Y-orbit on ordered pairs. They determine all exceptional pairs where X is almost simple and X/Y is cyclic. This

applies to our situation, since if $D(G) \neq G$ then Theorem 1.1(d) implies that $(G, D(G))$ is exceptional. Hence if $D(G) < H \leqslant G$ with $H/D(G)$ cyclic and G almost simple then $D(G)$ must occur in their list.

Theorem 5.7. *[11, Theorem 1.5] Let G be a primitive almost simple group of degree n and with socle T such that $D(G) \neq G$. Then one of the following holds:*

(a) *T is a group of Lie type and T_α is the centraliser in T of a field automorphism of odd prime order r. Moreover, r is not the characteristic of T, unless $T = \mathrm{PSL}(2, q)$;*

(b) *$T = \mathrm{PSL}(2, 2^f)$ and $T_\alpha = D_{2(2^f+1)}$ with $f \geqslant 3$ odd;*

(c) *$T = \mathrm{PSL}(2, p^f)$ and $T_\alpha = D_{p^f-1}$ with p odd and f even;*

(d) *$T = \mathrm{PSL}(2, 3^f)$ and $T_\alpha = D_{3^f+1}$, with $f \geqslant 3$ odd;*

(e) *$T = Sz(2^f)$ and T_α is the normaliser of a Sylow 5-subgroup of T;*

(f) *$T = \mathrm{PSU}(3, 2^a)$ with $a > 1$ odd and T_α is the stabiliser in T of a decomposition of the 3-dimensional space into the direct sum of three orthogonal nonsingular 1-spaces.*

We currently do not know any examples here where $G/D(G)$ is not cyclic.

6 Affine primitive groups

As we noted earlier, we have not been able to prove the bound $|G : D(G)| \leqslant \sqrt{n} - 1$ for affine primitive groups which are not Frobenius. We outline here what we have been able to prove.

Recall that it suffices to show that, if $H \leqslant \mathrm{GL}(d, p)$ for prime p and H is irreducible but not semiregular, then $|H : R(H)| \leq p^{d/2} - 1$. We work in greater generality, with a view towards Conjecture 3.1.

So let $H \leq \mathrm{GL}(d, q)$ be an irreducible linear group. We distinguish three cases:

Case 1: $R(H) = 1$.

Case 2: $R(H) > 1$ and $R(H)$ is reducible.

Case 3: $R(H)$ is irreducible.

Lemma 6.1. *Case 1 occurs if and only if H is semiregular on the set of non-zero elements.*

Proof. If $R(H) = 1$, then an element of $H \setminus \{1\}$ cannot have eigenvalue 1, and so such an element fixes no non-zero vector. The converse is clear. □

Lemma 6.2. *If Case 2 occurs, then H preserves a direct sum or tensor product decomposition of V.*

Proof. Let W be a minimal non-zero $R(H)$-invariant subspace. Let $\mathcal{S} = \{Wg : g \in H\}$. Then every subspace in $\mathcal{S}$ is $R(H)$-invariant. By minimality, any two members of $\mathcal{S}$ intersect in $\{0\}$. Also, the subspace $\langle\mathcal{S}\rangle$ is H-invariant. Since H is irreducible, $\langle\mathcal{S}\rangle = V$. Note that Proposition 3.2 implies that $H/R(H)$ permutes $\mathcal{S}$ regularly. Let $\dim(W) = e$.

Case 2A: $V = \bigoplus\{U : U \in \mathcal{S}\}$. Then $|\mathcal{S}| = d/e$ and H preserves this direct sum decomposition.

Case 2B: $|\mathcal{S}| > d/e$.

We claim there is a subset of $\mathcal{S}$ whose direct sum is V. For choose a subset of $\mathcal{S}$, say $\mathcal{S}_0$, maximal subject to generating its direct sum, and suppose $U \in \mathcal{S} \setminus \mathcal{S}_0$. Let X be the direct sum of the spaces in $\mathcal{S}_0$. Then X is also $R(H)$-invariant, and so is its intersection with U. If $X \cap U = \{0\}$, then $\mathcal{S}_0 \cup \{U\}$ also generates its direct sum, contrary to assumption. So $U \subseteq X$. But if this holds for all $U \in \mathcal{S} \setminus \mathcal{S}_0$, then $X = V$.

Suppose that $V = W_1 \oplus \cdots \oplus W_k$, where $W_i \in \mathcal{S}$. We have $k = d/e$. If W' is another subspace in $\mathcal{S}$, then each non-zero vector in W' has non-zero projections onto at least two W_i. Since $R(H)$ fixes all these spaces, we have $R(H)$-invariant isomorphisms between them.

Now define a relation on $\mathcal{S}$ by the rule that $U_1 \sim U_2$ if the actions of $R(H)$ on U_1 and U_2 are isomorphic. The result of the preceding paragraph shows that this relation is not the relation of equality, and it is clearly an equivalence relation. The span of an equivalence class is a $R(H)$-invariant subspace, which contains no members of any other equivalence class. So, arguing as before, V is a direct sum of these subspaces.

If there is more than one equivalence class, then H preserves this direct sum decomposition.

If there is just one equivalence class, then $V \cong W \otimes U$ for some space U; and $R(H)$ acts on the first factor of the tensor product. □

Finally, suppose that Case 3 occurs, so $R(H)$ is an irreducible linear group. In this case, the obvious approach is to apply Aschbacher's Theorem [1] to H. We have dealt with some of the cases, but have not completed the analysis. We make one simple observation.

Lemma 6.3. *Conjecture 3.1 holds if H is a subfield subgroup or an imprimitive linear group.*

Proof. In the subfield case, suppose that $H \leqslant \mathrm{GL}(d, q_0) \leqslant \mathrm{GL}(d, q)$, where $q = q_0^e$ with $e > 1$. Observing that the eigenvalues of an element of H are the same whether we regard H as acting on $\mathrm{GF}(q)^d$ or $\mathrm{GF}(q_0)^d$, we see that $|H : R(H)| \leqslant q_0^d - 1 = q^{d/e} - 1$ (the inequality coming from Proposition 3.2), and the result follows since $e \geqslant 2$.

In the imprimitive case, the semidirect product $T \rtimes H$ is contained in a wreath product with product action, and the result follows from Corollary 5.5 (whose proof did not assume that G is not affine). □

7 On the quotient $G/D(G)$

In this section we consider the group-theoretic structure of the quotient $G/D(G)$.

We have seen that any Frobenius complement can occur as this quotient. It turns out that in general the class of groups that can appear is wider, as the following examples testify.

Example 7.1. (a) Let $X, Y \leqslant \mathrm{GL}(2, 5)$ such that $X \cong D_{12}$ and $Y \cong Q_8$. Then $R(X) = D_{12}$, as it is generated by its non-central involutions. Moreover, any element of X that is not an involution does not have any eigenvalues in $\mathrm{GF}(5)$. Furthermore, $R(Y) = \langle -I_2 \rangle$ and all eigenvalues of elements of Y lie in $\mathrm{GF}(5)$.

Let $H = X \circ Y \leqslant \mathrm{GL}(2, 5) \circ \mathrm{GL}(2, 5)$ acting on the tensor product of two $\mathrm{GF}(5)$-spaces of dimension 2. (Here $\circ$ denotes central product.) Then all elements of H with 1 as an eigenvalue lie in X and so $H/R(H) = Y/R(Y) \cong C_2^2$. The primitive group G with $G/D(G) \cong C_2^2$ arising from Proposition 3.1 is the number 41 of degree 625 in the Magma database.

(b) Let X and Y be subgroups of $\mathrm{GL}(2,23)$ with $X \cong D_{44}$ and $Y \cong \mathrm{SL}(2,3)$. Both X and Y are irreducible. Then $R(X) = X$ as it is generated by involutions. Moreover, all eigenvalues of elements of X lie in $\mathrm{GF}(23)$. The group Y acts semiregularly on the set of 1-dimensional subspaces of $\mathrm{GF}(23)^2$ and so $-I_2$ is the only element of Y with eigenvalues in $\mathrm{GF}(23)$. Now, $\mathrm{GL}(4,23)$ contains $\mathrm{GL}(2,23) \circ \mathrm{GL}(2,23)$ acting on the tensor product of two $\mathrm{GF}(23)$-spaces of dimension 2. Considering X as a subgroup of the first copy of $\mathrm{GL}(2,23)$ and Y as a subgroup of the second copy of $\mathrm{GL}(2,23)$, put $H = X \circ Y \leq \mathrm{GL}(2,23) \circ \mathrm{GL}(2,23)$. Then put $G = T \rtimes H$ where T is the translation subgroup of $\mathrm{GL}(4,23)$. Then $H/R(H) = Y/R(Y) \cong A_4$ and so by Proposition 3.1 G is a primitive permutation group of degree 23^4 with $G/D(G) \cong A_4$.

(c) Here take $X, Y \leqslant \mathrm{GL}(2,59)$ with $X \cong D_{116}$ and $Y \cong \mathrm{SL}(2,5)$. The group Y acts semiregularly on the set of 1-dimensional subspaces of $\mathrm{GF}(59)^2$ and so taking $H = X \circ Y \leqslant \mathrm{GL}(2,59) \circ \mathrm{GL}(2,59)$ acting on the tensor product of two $\mathrm{GF}(59)$-spaces of dimension 2 the same argument as above yields a primitive group with G with $G/D(G) \cong A_5$.

We now give an infinite family of non-Frobenius examples.

Lemma 7.1. *Let p be a prime and $f \geqslant 1$ such that $q = p^f \equiv -1 \pmod 4$. Then there is a primitive group G such that $G/D(G) \cong D_{q+1}$.*

Proof. Let X be the subgroup of $\mathrm{GL}(2,q)$ generated by $\begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ (for $u \neq 0$) and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Then $X \cong D_{2(q-1)}$. Since $q \equiv -1 \pmod 4$, the group X does not have an element of order 4. Moreover, X is generated by its non-central involutions and these all have 1 as an eigenvalue. Furthermore, all eigenvalues of the elements of X lie in $\mathrm{GF}(q)$.

Let $x, y \in \mathrm{GF}(q^2)$ with x having order $q+1$ and y having order $2(q+1)$. Consider x and y as elements of $\mathrm{GL}(2,q)$. Let σ be the field automorphism of $\mathrm{GF}(q^2)$ that raises each element to its q^{th} power and consider σ as an element of $\mathrm{GL}(2,q)$. Then $(y\sigma)^2 = y^{q+1} = -I_2 = x^{(q+1)/2}$. Thus $y\sigma$ is an element of order 4. Let $Y = \langle x, y\sigma \rangle \leqslant \mathrm{GL}(2,q)$. All elements in $\langle x \rangle$ other than those in $\langle -I_2 \rangle$ have no elements in $\mathrm{GF}(q)$ as an eigenvalue. All elements of Y outside $\langle x \rangle$ have order 4 and the condition on q implies that they also have no eigenvalues in $\mathrm{GF}(q)$. Moreover, $x^{y\sigma} = x^q = x^{-1}$ and so $Y/\langle -I_2 \rangle \cong D_{q+1}$.

Now take $H = X \circ Y \leqslant \mathrm{GL}(2,q) \circ \mathrm{GL}(2,q)$ acting on the tensor product of two $\mathrm{GF}(q)$-spaces of dimension 2. For each $g \in X$ and $h \in Y$, the eigenvalues of the element arising from (g,h) are of the form $\lambda\mu$ where λ is an eigenvalue of g and μ is an eigenvalue of h. Since the elements of $Y \setminus \langle -I_2 \rangle$ do not have elements of $\mathrm{GF}(q)$ as eigenvalues, the elements of H with 1 as an eigenvalue lie in X and so $H/R(H) = Y/Z(Y) \cong D_{q+1}$. Moreover, as X and Y are both irreducible subgroups of $\mathrm{GL}(2,q)$ we have that H is an irreducible subgroup of $\mathrm{GL}(4,q)$. Thus by Proposition 3.1, there exists a primitive group G such that $G/D(G) \cong D_{q+1}$. □

Under extra hypotheses, we can restrict the structure of the quotient. For example:

Proposition 7.2. *Suppose that the transitive group G has a regular normal subgroup N, and that G splits over $D(G)$, say $G = D(G) \rtimes H$. Then N is nilpotent and H is isomorphic to a Frobenius complement.*

Proof. Non-identity elements of H have unique fixed points. It follows that H fixes a point α and is semiregular on $\Omega \setminus \{\alpha\}$. (If not, then H acts faithfully as a regular or Frobenius group on each orbit, and with at least one Frobenius orbit. But then elements of the Frobenius kernel K can be recognised – K is the Fitting subgroup of H – and so they have no fixed points at all, a contradiction.)

Thus H normalises N and acts semiregularly on $N \setminus \{1\}$, so that NH is a Frobenius group with kernel N and complement H. Then N is nilpotent by Thompson's theorem. □

We note that for the examples in Example 7.1 and Lemma 7.1, G does not split over $D(G)$.

On the other hand, every Frobenius complement can occur in a non-Frobenius group:

Proposition 7.3. *Let H be a Frobenius complement. Then there is a transitive, non-Frobenius group G such that $G/D(G) \cong H$.*

Proof. Suppose that NH is a Frobenius group on a set Δ with kernel N and complement H. Without loss of generality we may suppose that N is abelian. (For by Thompson's theorem, N is nilpotent; thus $Z(N) \neq \{1\}$, and H acts faithfully and fixed-point-freely on $Z(N)$, so $Z(N)H$ is a Frobenius group.) For convenience we write N additively below.

Choose a prime q which does not divide $|H|$. Let $G = N^q \rtimes (H \times C_q)$ act on Δ^q in product action, where H acts in the same way on each factor and C_q permutes the factors. We have $N^q \leqslant D(G)$. Moreover, elements of C_q fix the diagonal elements of N^q, so by Theorem 1.1(b) $C_q \leqslant D(G)$. We show that elements outside $N^q \rtimes C_q$ have just one fixed point; it follows that $D(G) = N^q \rtimes C_q$, and so $G/D(G) \cong H$ as required. Since N^q is a regular normal subgroup, we can identify Ω with N^q.

Take an element $g = h(a_1, \ldots, a_q)\sigma^i$, where $C_q = \langle\sigma\rangle$, $a_1, \ldots, a_q \in N$, and $h \neq 1$, and suppose that g fixes $(x_1, \ldots, x_q)$, with $x_1, \ldots, x_q \in \Delta$.

Case 1: $i = 0$. Then

$$(x_1, \ldots, x_q)g = (x_1^h + a_1, x_2^h + a_2, \ldots, x_q^h + a_q).$$

So, if g fixes $(x_1, \ldots, x_q)$, we have $x_j^h + a_j = x_j$ for all $j = 1, \ldots, q$. Since $N^q \rtimes H$ is a Frobenius group and $h \neq 1$, there is a unique such element.

Case 2: $i \neq 0$. Without loss of generality, $i = 1$. Then

$$(x_1, \ldots, x_q)g = (x_q^h + a_q, x_1^h + a_1, \ldots, x_{q-1}^h + a_{q-1}).$$

So, if g fixes $(x_1, \ldots, x_q)$, then

$$x_1^h + a_1 = x_2, x_2^h + a_2 = a_3, \ldots, x_q^h + a_q = x_1.$$

Telescoping these formulae gives $x_1^{h^q} + b_1 = x_1$, where

$$b = a_1^{h^{q-1}} + \cdots + a_q.$$

Now q is coprime to $|H|$, so $h^q \neq 1$; the same argument as in Case 1 shows that the value of x_1 is uniquely determined. A similar argument shows that $x_2, \ldots, x_q$ are unique.

The proof is complete. □

Remark 7.2. In all examples constructed in this section, the group $G/D(G)$, if not itself a Frobenius complement, is a quotient of one. So we tentatively propose the following problem:

Question 7.3. Is it true that, for any finite transitive permutation group G, the group $G/D(G)$ is a quotient of a Frobenius complement?

8 One more problem

The derangements in a finite transitive permutation group G form a non-empty union of conjugacy classes; so, if G is simple, they generate G. In a recent preprint, Larsen, Shalev and Tiep [15] proved the following theorem:

Theorem 8.1. *Let G be a finite simple transitive permutation group. If $|G|$ is sufficiently large, then any element of G can be written as the product of two derangements.*

More generally, we could pose the following problem:

Question 8.1. Is it possible to classify the finite transitive permutation groups G for which some element of $D(G)$ cannot be written as the product of two derangements?

We note that, in a Frobenius group G, every non-identity element of $D(G)$ is a derangement.

Acknowledgment This work was begun when the first two authors were visiting The University of Western Australia in 2016; they acknowledge with thanks support from UWA. The research of the last two authors is supported by the Australian Research Council Discovery Project DP200101951.

The first three authors would like to thank the Isaac Newton Institute for Mathematical Sciences, Cambridge, for support and hospitality during the programme *Groups, representations and applications: new perspectives*, where part of the research for this paper was done. This work was supported by EPSRC grant no EP/R014604/1. In addition, the second author was supported by a Simons Fellowship.

Declaration of interest: None

References

[1] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469–514.

[2] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system I: The user language, J. Symbolic Comput. 24 (1997) 235–265.

[3] J. N. Bray, D. F. Holt and C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*. London Math. Soc. Lecture Note Ser., **407**, Cambridge University Press, Cambridge, 2013.

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

[5] P. J. Cameron and A. M. Cohen, On the number of fixed-point-free elements in a permutation group, *Discrete Math.* **106/107** (1992), 135–138.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *An ATLAS of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[7] H. J. Coutts, M. Quick and C. M. Roney-Dougal, The primitive permutation groups of degree less than 4096. *Comm. Algebra* **39** (2011), 3526–3546.

[8] B. Fein, W. M. Kantor and M. Schacher, Relative Brauer groups, II, *J. Reine Angew. Math.* **328** (1981), 39–57.

[9] D. Gorenstein, *Finite simple groups. An introduction to their classification*, University Series in Mathematics. Plenum Publishing Corp., New York, 1982.

[10] S. Guest, J. Morris, C. E. Praeger and P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[11] R. M. Guralnick, P. Müller and J. Saxl, The rational function analogue of a question of Schur and exceptionality of permutation representations, *Memoirs Amer. Math. Soc.* **162**, no. 773 (2003), 1–79.

[12] D. Holt and G. Royle, A census of small transitive groups and vertex-transitive graphs, *J. Symbolic Comput.* **101** (2020), 51–60. doi:10.1016/j.jsc.2019.06.006.

[13] P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*. London Math. Soc. Lecture Note Ser., **129**, Cambridge Univeristy Press, Cambridge, 1990.

[14] L. G. Kovács, Primitive subgroups of wreath products in product action, *Proc. London Math. Soc.* (3) **58** (1989), 306–322.

[15] M. Larsen, A. Shalev and P. H. Tiep, Products of normal subsets and derangements, `https://arxiv.org/abs/2003.12882`

[16] D. S. Passman, *Permutation Groups*, Dover Publications, 2012 (reprint of 1968 edition)

[17] J.-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

[18] H. Zantema, Integer valued polynomials over a number field, *Manuscripta Math.* **40** (1982), 155–203.