Invariable generation of permutation and linear groups

Tracey, Gareth

Invariable generation of permutation and linear groups

Gareth Tracey*

*Department of Mathematical Sciences, University of Bath,
Bath BA2 7AY, United Kingdom*

January 30, 2017

Abstract

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $\{x_1^{g_1}, x_2^{g_2}, \ldots, x_d^{g_d}\}$ generates G for every d-tuple $(g_1, g_2 \ldots, g_d) \in G^d$. We prove that a finite completely reducible linear group of dimension n can be invariably generated by $\lfloor \frac{3n}{2} \rfloor$ elements. We also prove tighter bounds when the field in question has order 2 or 3. Finally, we prove that a transitive [respectively primitive] permutation group of degree $n \geq 2$ [resp. $n \geq 3$] can be invariably generated by $O\left(\frac{n}{\sqrt{\log n}}\right)$ [resp. $O\left(\frac{\log n}{\sqrt{\log \log n}}\right)$] elements.

1 Introduction

There is a continually growing body of literature which broadly concerns the various generation properties in finite groups. This has involved the analysis of many "generation type" group theoretic invariants, such as the minimal size $d(G)$ of a generating set for the group G. In this paper, we study a related invariant: the minimal size of an *invariable* generating set.

Definition 1.1. Let G be a group.

(a) We say that a subset $\{x_1, x_2, \ldots, x_d\}$ of G *invariably generates* G if $\{x_1^{g_1}, x_2^{g_2}, \ldots, x_d^{g_d}\}$ generates G for every d-tuple $(g_1, g_2 \ldots, g_d) \in G^d$.

(b) Suppose that G is finite. Define $d_I(G)$ to be the smallest size of an invariable generating set for G.

1.1 Warnings

There are a couple of warnings that should be pointed out here. Firstly, there exist infinite groups G in which $\bigcup_{g \in G} H^g = G$ for some proper subgroup H of G. In this case G does not even have an invariable generating set, so $d_I(G)$ is certainly not well-defined. Thus, the

---

*Electronic address: `G.M.Tracey@bath.ac.uk`

requirement that G is finite in Definition 1.1 Part (b) really is necessary (of course one could also weaken this to "finitely invariably generated").

Secondly, one may be tempted to study an even stronger generation property, by requiring that $\langle\{x_1^{g_1}, x_2^{g_2}, \ldots, x_d^{g_d}\}\rangle = G$ for every d-tuple $(g_1, g_2 \ldots, g_d) \in \operatorname{Aut}(G)^d$. However, an arbitrary finite group G may not even contain such a generating set. For example, when G is elementary abelian of order p^a, for some prime p, then $\operatorname{Aut}(G) \cong GL_a(p)$ acts transitively on the non-identity elements of G.

1.2   History, motivation and main results

The notion of invariable generation was first discussed by B.L. van der Waerden in 1934 [35]. Motivated by the problem of computing Galois groups, van der Waerden asked about probabilistic invariable generation in the case $G = \operatorname{Sym}(n)$. For more information about this direction see also [9].

Suppose that a subset $X := \{x_1, \ldots, x_d\}$ of the finite group G fails to invariable generate G. Then X is contained in the union $\bigcup_{g \in G} M^g$ of conjugates of a maximal subgroup M of G. In other words, no element of X acts fixed point freely in the action of G on the set of (right) cosets of M in G. Thus, the study of invariable generation is closely related to the theory of derangements in transitive permutation groups. This direction has seen a lot of recent attention, particularly in the case when the group in question is a non-abelian simple group: see [30], [16], [17], [18], [19], [31], and [10].

A more general analysis of invariable generation in finite groups was undertaken by Kantor, Lubotzky and Shalev in [22]. This is, as far as we know, where the notation $d_I(G)$ first appeared. Among many interesting results, they showed that while it is clear that $d_I(G) \geq d(G)$, we have $d_I(G) = d(G)$ when G is nilpotent [22, Proposition 2.4], but that $d_I(G) - d(G)$ can be arbitrarily large in general [22, Propostion 2.5]. In fact, this is even true if we restrict to the case when G is soluble (see [8, Corollary 10]). Thus, if one fixes a class of finite groups $\mathcal{C}$, it is an interesting (and open) problem to determine if bounds on $d(G)$ carry over to comparable bounds on $d_I(G)$. For instance, it has been proven independently in [13] and [22] that $d_I(G) = d(G) = 2$ when G is a nonabelian finite simple group.

In this paper, we investigate the "naturally occurring finite groups", namely the permutation and linear groups. A. Lucchini and E. Detomi (see Theorem 2.8) have proved that the "McIver-Neumann half n bound", which states that $d(G) \leq \frac{n}{2}$ whenever G is a permutation group of degree n, and $(G, n) \neq (S_3, 3)$, holds when one replaces d by d_I. Our first two main results deal with the case when G is transitive and primitive, respectively.

Theorem 1.2. *There exists an absolute constant c_{trans} such that*

$$d(G) \leq \frac{c_{trans} n}{\sqrt{\log n}}$$

whenever G is a transitive permutation group of degree $n \geq 2$.

Theorem 1.3. *There exists an absolute constant c_{prim} such that*

$$d(G) \leq \frac{c_{prim} \log n}{\sqrt{\log \log n}}$$

whenever G is a primitive permutation group of degree $n \geq 3$.

When d_I is replaced by d, Theorem 1.2 is [27, Theorem 1], while Theorem 1.3 is [28, Theorem C].

We now move on to linear groups. For n even, we follow [15] and denote by B_n the completely reducible group $B_n := 3^{n/2} : 2 \leq GL_n(2)$, such that $Z(B_n) = 1$, and $B_n \leq GL_2(2)^{n/2}$ acts completely reducibly on a direct sum of 2-dimensional submodules.

We also require the following definitions.

Definition 1.4. Let $\mathbb{F}$ be a field. An irreducible subgroup R of $GL_n(\mathbb{F})$ is called *imprimitive* if the natural R-module $V \cong \mathbb{F}^n$ has a direct sum decomposition $V = W_1 \oplus W_2 \oplus \ldots \oplus W_r$, where $r > 1$ and R acts on the set $\{W_1, W_2, \ldots, W_r\}$. If no such decomposition exists, then R is *primitive*. If every normal subgroup of R is homogeneous, then we say that R is *quasiprimitive*, while if every characteristic subgroup of R is homogeneous then R is said to be *weakly quasiprimitive*.

A primitive group $R \leq GL_n(\mathbb{F})$ is both quasiprimitive and weakly quasiprimitive, since a decomposition of V into homogeneous components for a normal or characteristic subgroup of R would yield an imprimitivity decomposition for V as given in Definition 1.4. The precise statement of our theorem can now be given as follows.

Theorem 1.5. *Let $\mathbb{F}$ be a field.*

1. *Let $G \leq GL_n(\mathbb{F})$ be finite and completely reducible. Then $d_I(G) \leq 3n/2$. Furthermore, if $|\mathbb{F}| = 2$ then $d_I(G) \leq n/2$, unless $G \cong B_n$ as defined above, in which case we have $d_I(G) = n/2 + 1$; or $G \cong Sp_4(2) \cong S_6$, in which case we have $d_I(G) = 3$. Also, if $|\mathbb{F}| = 3$ then $d_I(G) \leq n$.*

2. *Let $R \leq GL_n(\mathbb{F})$ be finite and weakly quasiprimitive. Also, let $Z = R \cap Z(GL_n(\mathbb{F}))$, and let H be a subnormal subgroup of R. Then $d_I(HZ/Z) \leq 2 \log n$, unless $R = H = Sp_4(2) \cong S_6$, in which case we have $d_I(HZ/Z) = 3$.*

For the case $|\mathbb{F}| = 2$ in Part 1 of Theorem 1.5, and the exceptional case $G \cong B_n$, compare Theorem 2.8 and its exceptional case, which, as mentioned above, is the corresponding result for permutation groups.

If one replaces d_I by d, then the first statement in Part 1 of Theorem 1.5 is proved in [23]. The second half, together with Part 2, is proved in [15, Theorem 1.2].

1.3 Strategy for the proofs and layout of the paper

Let G be a transitive permutation group [respectively irreducible linear group], of degree [resp. dimension] n, and assume that G is imprimitive. Then G may be embedded as a certain

subgroup of a wreath product $R \wr S$, where R is a primitive permutation [resp. linear] group of degree [resp. dimension] r, S is a transitive permutation group of degree s, $rs = n$, and $G\pi = S$, where $\pi : R \wr S \to S$ denotes projection over the top group. Let $B \cong R^s$ be the base group of $R \wr S$. Then $G \cap B^s$ is "built" from submodules of induced G-modules, and non-abelian G-chief factors (see Lemma 3.8). We will use this to bound the contribution of $G \cap B^s$ to the invariable generator number for G. Since $G = (G \cap B^s).(\frac{G}{G \cap B^s})$, we then need to bound $d_I(G/G \cap B^s) = d_I(S)$. This is done by induction to prove Theorem 1.2.

For Theorem 1.3, the affine case of the O'Nan-Scott Theorem is the most difficult to handle, and this requires upper bounds for $d_I(G)$ for an irreducible linear group G. The approach described in the above paragraph then gives us what we need (here, we bound $d_I(G/G \cap B^s)$ by using Theorem 1.2, rather than induction).

Theorem 1.5 Part 1 can easily be reduced to the irreducible case, and we again use the approach described above. For the remaining parts, we use results on the structure of a weakly quasiprimitive linear group from [1], [2], [12] and [28].

The layout of the paper is as follows: in Section 2 we first record some asymptotic results concerning the composition length of finite permutation and linear groups. With the proof strategy outlined above in mind, we will then discuss bounds on the size of a minimal generating set for a submodule of an induced module for a finite group. We close Section 2 with a discussion of the structure of a weakly quasiprimitive linear group, as mentioned above. In Section 3, we partially generalise the module theoretic results from the introduction to certain subgroups of wreath products, while Section 4 consists of upper bounds for the function d_I on various classes of finite groups. Finally, we complete the proof of Theorem 1.5 in Section 5, and Theorems 1.2 and 1.3 in Section 6.

Notation: We will adopt the $\mathbb{ATLAS}$ [6] notation for group names, although we will usually

write $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ for the symmetric and alternating groups of degree n. Furthermore, these groups, and their subgroups, act naturally on the set $\{1, \ldots, n\}$; we will make no further mention of this.

The centre of a group G will be written as $Z(G)$, the Frattini subgroup as $\Phi(G)$, and the Fitting subgroup as $F(G)$. The letters G, H, K and L will usually be used for groups, while V and W will usually be modules. The letter M will usually denote a submodule.

Throughout, we will use the Vinogradov notation $A \ll B$, which means $A = O(B)$. Finally, "log" will always mean log to the base 2.

2   Preliminary results

The purpose of this paper is to study upper bounds for the function d_I on certain classes of finite permutation and linear groups. As mentioned in Section 1, the proofs in the most difficult cases essentially amount to using upper bounds on $d_I(G)$ for subgroups G of wreath products $R \wr S$. Our main strategy for doing this will be to reduce modulo the base group B of $R \wr S$ and

use either induction or previous results to bound $d_I(G/G \cap B)$. In this way, all that remains is to investigate the contribution of $G \cap B$ to $d_I(G)$.

As we will show in Lemma 3.8, the group $G \cap B$ is built, as a normal subgroup of G, from submodules of induced modules for G, and non-abelian chief factors of G. The following lemma shows that, in the abelian case, it therefore suffices to study generator numbers for these submodules as G-modules, rather than their invariable generator numbers as groups themselves. More precisely, we have

Lemma 2.1 ([**7**], **Lemma 2**). *Let G be a group and let N be a normal subgroup of G. Then*

(i) $d_I(G) \leq d_I(G/N) + d_I(N)$.

(ii) *If N is abelian, then $d_I(G) \leq d_I(G/N) + d_G(N)$, where $d_G(N)$ denote the minimal number of generators required to generate N as a G-module;*

Lemma 2.1 also shows that the contribution to $d_I(G)$ of the non-abelian building blocks from $G \cap B$ can be bounded above by $2c_{nonab}(R)$, where $c_{nonab}(R)$ denotes the number of non-abelian chief factors of R.

With the above in mind, the purpose of this section is two-fold: to investigate the number of "building blocks" in $G \cap B$ (this will, in most cases, come down to investigating the chief length of the group R), and to investigate the contribution of each building block to $d_I(G)$. We do this in Sections 2.1 and 2.2 respectively.

2.1 Composition length and invariable generation in permutation and linear groups

In this section we record numerous results concerning invariable generation and composition length in finite permutation and linear groups. We begin with composition length.

Definition 2.2. Let G be a group.

(a) Write $a(G)$ to denote the composition length of G.

(b) Let $a_{ab}(G)$ and $a_{nonab}(G)$ denote the number of abelian and non-abelian composition factors of G, respectively.

(c) Let $c_{nonab}(G)$ denote the number of non-abelian chief factors of G.

The first result is stated slightly differently to how it is stated in [32].

Theorem 2.3 ([**32**], **Theorem 2.10**). *Let R be a primitive permutation group of degree $r \geq 2$. Then $a(R) \ll \log r$.*

Theorem 2.4 ([**28**], **Proposition 9**). *Let $\mathbb{F}$ be a finite field, and let $R \leq GL_r(\mathbb{F})$ be completely reducible. Then $a(R) \ll r \log |\mathbb{F}|$.*

We now consider permutation representations of finite simple groups.

Theorem 2.5 ([21], **Lemma 2.6**). *Let T be a non-abelian finite simple group, and suppose that T is contained in $\mathrm{Sym}(n)$, with $n \geq 2$. Then $|\mathrm{Out}(T)| \ll \log n$.*

Finally, we record a result of Cameron, Solomon and Turull concerning the composition length of a finite permutation group. Note that we only give a simplified version of their result here.

Theorem 2.6 ([3], **Theorem 1**). *Let G be a permutation group of degree $n \geq 2$. Then $a(G) \ll n$.*

We now turn to invariable generation of certain classes of finite groups. We begin with the following general result.

Theorem 2.7 ([22], **Theorem 3.1**). *Let G be a finite group, and let M be a minimal normal subgroup of G. Then $d_I(G) \leq d_I(G/M) + \delta$, where $\delta := 1$ if M is abelian and $\delta := 2$ if M is nonabelian. In particular, $d_I(G) \leq a_{ab}(G) + 2c_{nonab}(G) \leq a(G)$.*

Next, we note the theorem of Lucchini and Detomi mentioned in Section 1.

Theorem 2.8 ([7], **Theorem 1**). *Let G be a subgroup of $\mathrm{Sym}(n)$. Then $d_I(G) \leq \left\lfloor \frac{n}{2} \right\rfloor$, except when $n = 3$ and $G \cong \mathrm{Sym}(3)$.*

We also have the bound for simple groups, which was also mentioned previously.

Theorem 2.9 ([22], **Theorem 5.1** and [13], **Theorem 1.3**). *Let T be a non-abelian finite simple group. Then $d_I(T) \leq 2$.*

Since the outer automorphism group of a nonabelian finite simple group is either isomorphic to a subgroup of $\mathrm{Sym}(4) \times C_f$, or is an extension of at most three cyclic groups, the next corollary follows immediately from Theorem 2.9.

Corollary 2.10. *Let T be a non-abelian finite simple group, and let $H \leq \mathrm{Out}(T)$. Then $d_I(H) \leq 3$. In particular, if $T \leq G \leq \mathrm{Aut}(T)$, then $d_I(G) \leq 5$.*

2.2 Generating submodules of induced modules for finite groups

In this section, we record a number of results from [34, Section 4] concerning generator numbers in submodules of induced modules. We begin with some terminology.

Definition 2.11. Let M be a group, acted on by another group G. A *G-subgroup* of M is a subgroup of M which is stabilised by G. We say that M is *generated as a G-group* by $X \subset M$ and write $M = \langle X \rangle_G$ if no proper G-subgroup of M contains X. We will write $d_G(M)$ for the cardinality of the smallest subset X of M satisfying $\langle X \rangle_G = M$. Finally, write $M^* := M \backslash \{1\}$.

Note that this notation is consistent with our use of $d_G(M)$ in Lemma 2.1.

Definition 2.12. Let G be a group, acting on a set Ω. Write $\chi(G, \Omega)$ for the number of orbits of G on Ω.

To avoid being cumbersome, we will also introduce some notation which will be retained for the remainder of Section 2.2:

- Let G be a finite group.

- Fix a subgroup H of G of index $s \geq 2$.

- Let V be a module for H of dimension a, over a field $\mathbb{F}$.

- Let $K := \mathrm{core}_G(H)$.

- Set $W := V \uparrow_H^G$ to be the induced module.

- Denote the set of right cosets of H in G by Ω.

Next, define the constant b as follows,

$$b := \sqrt{\frac{2}{\pi}}.$$

We also have the following definitions.

Definition 2.13. For a positive integer s with prime factorisation $s = p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t}$, set $\omega(s) := \sum r_i$, $\omega_1(s) := \sum r_i p_i$, $K(s) := \omega_1(s) - \omega(s) = \sum r_i(p_i - 1)$ and

$$\widetilde{\omega}(s) = \frac{s}{2^{K(s)}} \binom{K(s)}{\left\lfloor \frac{K(s)}{2} \right\rfloor}.$$

Definition 2.14. For a positive integer s and a prime p, define s_p to be the p-part of s. Also define $\mathrm{lpp}\,(s) := \max_{p \text{ prime}} s_p$.

The first main result deals with the case when G^Ω contains a soluble transitive subgroup.

Theorem 2.15. *Suppose that G^Ω contains a soluble transitive subgroup, and let M be a submodule of W. Also, denote by $\chi = \chi(K, V^*)$ the number of orbits of K on the non-zero elements of V. Then*

$$d_G(M) \leq \min\{a, \chi\}\, \widetilde{\omega}(s) \leq \min\{a, \chi\} \left\lfloor \frac{bs}{\sqrt{\log s}} \right\rfloor$$

where $b := \sqrt{2/\pi}$. Furthermore, if $s = p^t$, with p prime, then

$$d_G(M) \leq \min\{a, \chi\} \left\lfloor \frac{bp^t}{\sqrt{t(p - 1)}} \right\rfloor.$$

Remark 2.16. If K has infinitely many orbits on the non-zero elements of V, then we assume, in Theorem 2.15, and whenever it is used in the remainder of the paper, that

$$\min\{a, \chi\} = a.$$

We now move on to general finite groups (i.e. those G for which G^Ω does not necessarily contain a soluble transitive subgroup). We retain the notation introduced at the beginning of Section 2.2.

We begin with a definition. Recall the definitions of $\widetilde{\omega}(s)$, s_p, and $\text{lpp}\,(s)$ from Definitions 2.13 and 2.14.

Definition 2.17. For a prime p, set

$$E(s,p) := \min\left\{ \left\lfloor \frac{bs}{\sqrt{(p-1)\log_p s_p}} \right\rfloor , \frac{s}{\text{lpp}\,(s/s_p)} \right\} \text{ and } E_{sol}(s,p) := \min\left\{\widetilde{\omega}(s), s_p\right\}$$

where we take $\left\lfloor bs/\sqrt{(p-1)\log_p s_p} \right\rfloor$ to be ∞ if $s_p = 1$.

The following is quickly proved after examining the functions E_{sol} and E.

Proposition 2.18. *Let p be prime. Then $E_{sol}(s,p) \leq E(s,p)$.*

Remark 2.19. For any finite group G and any G-module M, $d_G(M)$ is bounded above by $\chi(G, M^*)$.

For the remainder of this section, we will make a further assumption: that the field $\mathbb{F}$ has characteristic $p > 0$. The main result for general finite groups reads as follows.

Theorem 2.20. *For a prime $q \neq p$, let P_q be a Sylow q-subgroup of G. Also, let P' be a maximal p'-subgroup of G. Let M be a submodule of W.*

(i) *If G is soluble, then*
$$d_G(M) \leq \min\left\{a, \chi(P' \cap K, V^*)\right\} s_p.$$

(ii) *Let N be a subgroup of G such that N^Ω is soluble, and let s_i, $1 \leq i \leq t$, be the sizes of the orbits of N on Ω. Then*

    (a) *We have*
$$d_G(M) \leq \min\left\{a, \chi(N \cap P' \cap K, V^*)\right\} \times \sum_{i=1}^{t} \widetilde{\omega}(s_i).$$

    (b) *If N is soluble, and P'_N is a p-complement in N, then*
$$d_G(M) \leq \min\left\{a, \chi(P'_N \cap K, V^*)\right\} \times \sum_{i=1}^{t} E_{sol}(s_i, p).$$

(iii) *$d_G(M) \leq \min\left\{a, \chi(P_q \cap K, V^*)\right\} s/s_q.$*

(iv) *Assume that $s_p > 1$. Then*
$$d_G(M) \leq \min\left\{a, \chi(K, V^*)\right\} \left\lfloor \frac{bs}{\sqrt{\log s_p}} \right\rfloor.$$

8

We also record some corollaries from [34].

Corollary 2.21. *Define E' to be E_{sol} if G^Ω contains a soluble transitive subgroup, and $E' := E$ otherwise. Let M be a submodule of W. Then*

(i) $d_G(M) \leq aE'(s, p)$.

(ii) *Suppose that for some $q \neq p$, a Sylow q-subgroup of K acts transitively on the non-identity elements of V. Then*

$$d_G(M) \leq \min\left\{ \left\lfloor \frac{bs}{\sqrt{\log s_p}} \right\rfloor, \frac{s}{s_q} \right\},$$

where the right hand side above is taken to be $\frac{s}{s_q}$ if $s_p = 1$.

Corollary 2.22. *Let M be a submodule of W, and fix $0 < \alpha < 1$.*

(i) *If $s_p \geq s^\alpha$, then $d_G(M) \leq aE(s, p) \leq a\left\lfloor \frac{bs\sqrt{\frac{1}{\alpha}}}{\sqrt{\log s}} \right\rfloor$;*

(ii) *If $s_p \leq s^\alpha$, then $d_G(M) \leq aE(s, p) \leq a\left\lfloor \frac{\frac{1}{1-\alpha}s}{c'\log s} \right\rfloor$;*

(iii) *We have*

$$d_G(M) \leq aE(s, p) \leq \begin{cases} \left\lfloor \frac{2as}{c'\log s} \right\rfloor, & \text{if } 2 \leq s \leq 1260, \\ \left\lfloor \frac{abs\sqrt{2}}{\sqrt{\log s}} \right\rfloor, & \text{if } s \geq 1261. \end{cases}$$

Corollary 2.23. *Let M be a submodule of W. If G contains a soluble subgroup N, acting transitively on Ω, then*

$$d_G(M) \leq \min\left\{ a, \chi(P'_N \cap K, V^*) \right\} E(s, p)$$

where P'_N is a p-complement in N.

2.3 The structure of a weakly quasiprimitive linear group

We close the preliminary section by recording some a series of lemmas from [15, Section 2] concerning the structure of a weakly quasiprimitive linear group (see Definition 1.4).

Lemma 2.24 ([15], Lemma 2.13). *Let $\mathbb{F}$ be a field, and let $R \leq GL_r(\mathbb{F})$ be finite, irreducible and weakly quasiprimitive. Then R has a characteristic subgroup K such that K is isomorphic to a subgroup K_1 of $GL_{r/f}(\mathbb{F}_1)$, for some divisor f of r and some extension $\mathbb{F}_1$ of $\mathbb{F}$, with $[\mathbb{F}_1 : \mathbb{F}] = f$. All characteristic abelian subgroups of K_1 are contained in $Z(GL_{r/f}(\mathbb{F}_1))$, and K_1 is weakly quasiprimitive. Moreover, R/K is abelian of order at most f, and embeds naturally in $\mathrm{Gal}(\mathbb{F}_1 : \mathbb{F})$.*

For a finite, irreducible, weakly quasiprimitive subgroup R of $GL_r(\mathbb{F})$, we define $(f(R), K_1(R))$ to be any pair consisting of a positive integer $f = f(R)$ and a group $K_1 = K_1(R)$ satisfying the conclusion of Lemma 2.24, with f minimal.

We now record some results concerning the generalised Fitting subgroup of a finite group.

Lemma 2.25 ([15], **Lemma 2.14**). *Let L be the generalised fitting subgroup of a finite group R. Then L is a central product of $Z(R)$, the noncentral subgroups $O_{q_i}(R)$ for a set of primes q_i, and a collection of normal subgroups U_j of R. Each U_j is a central product of $u_j \geq 1$ copies of a quasisimple group T_j, and conjugation by R permutes these copies transitively. Also, $C_R(L) = Z(L)$.*

Lemma 2.26 ([15], **Lemma 2.15**). *Let $R \leq GL_r(\mathbb{F})$ be finite and completely reducible, and let L, q_i and U_j be as in Lemma 2.25. Assume that $\mathbb{F}$ is a splitting field for each central factor of L, and let C be a constituent of the natural L-module. Then C decomposes as a tensor product of a one-dimensional module for $Z(R)$, irreducible modules M_{q_i} for each $O_{q_i}(R)$, and irreducible modules M_{U_j} for each U_j.*

Lemma 2.27 ([15], **Lemma 2.16** or [29], **Lemma 1.7**). *Let R be finite with cyclic centre Z, and assume that all abelian characteristic subgroups of R are contained in Z. Then each noncentral $O_q(R)$ is the central product of its intersection with Z and an extraspecial q-group E, of order q^{1+2m} say. If q is odd, then E has exponent q. Any nontrivial absolutely irreducible E-module has dimension q^m, and $R/C_R(O_q(R)) \leq q^{2m}.Sp_{2m}(q)$. Also, $O_q(R/EZ)$ is trivial. Finally, the action of R/EZ on EZ/Z is completely reducible.*

Lemma 2.28 ([15], **Lemma 2.17**). *Let $R \leq GL_r(\mathbb{F})$ be finite and completely reducible, and let L, U_j, u_j, T_j and M_{U_j} be as in Lemmas 2.25 and 2.26. Assume that $\mathbb{F}$ is a splitting field for all central factors of L, and that L acts homogeneously. Then M_{U_j} is a tensor product of u_j copies of some faithful irreducible $\mathbb{F}[T_j]$-module M_{T_j}, of dimension $t_j \geq 2$. Also, writing bars to denote reduction modulo $C_R(U_j)$, $\overline{T_j}$ is a nonabelian simple group, and $\overline{T_j}^{u_j} \leq \overline{R} \leq (\overline{T_j}.A_j) \wr \mathrm{Sym}(u_j)$, where A_j is the subgroup of $\mathrm{Out}(\overline{T_j})$ that stabilises the module M_{T_j}.*

Corollary 2.29. *Let $R \leq GL_r(\mathbb{F})$ be finite and completely reducible, and let U_j, u_j, A_j, T_j and t_j be as in Lemma 2.28. Write bars to denote reduction modulo $C_R(T_j)$.*

1. *If $\overline{T_j} \not\cong P\Omega_8^+(q)$, with q odd, then $A_j \leq N.M$, where $|N| \leq 2$ and M is metacyclic. If $\overline{T_j} \cong P\Omega_8^+(q)$, with q odd, then $A_j \leq N.M$, where N is cyclic and $|M|$ divides 24;*

2. *Assume that $t_j = 2$ for some j. Then $\overline{R} \leq \overline{T_j}^{u_j}.(C_2 \wr \mathrm{Sym}(u_j))$.*

Proof. If $t_j = 2$, then [15, Lemma 2.10] implies that $|A_j| \leq 2$, so (ii) immediately follows. If $\overline{T_j}$ is not $P\Omega_8^+(q)$, with q odd, then part (i) follows from examining the structure of $\mathrm{Out}(\overline{T_j})$ (see [24, Chapter 2]). If $\overline{T_j} = P\Omega_8^+(q)$, with q odd, then $\mathrm{Out}(\overline{T_j})$ modulo its cyclic group of field automorphisms, has order 24, by [24, Theorem 2.1.4 and Proposition 2.7.3]. $\square$

Corollary 2.30. *Let F be a finite field, let $R \leq GL_r(\mathbb{F})$ be irreducible and weakly quasiprimitive, let $f = f(R)$, $K_1 = K_1(R)$, let L be the generalised fitting subgroup of K_1, and let $O_{q_i}(K_1)$, U_j be the central factors of L as in Lemma 2.25. Also, for each q_i let m_i be as in Lemma 2.27, and for each U_j, let u_j and t_j be as in Lemma 2.28. Then*

(i) $\prod_i q_i^{m_i} \prod_j t_j^{u_j}$ *divides* r/f;

(ii) Each q_i divides $|\mathbb{F}|^f - 1$;

Proof. By definition, each characteristic abelian subgroup of K_1 is contained in $Z := Z(GL_r(\mathbb{F}^f))$. Since q_i divides $|Z(O_{q_i}(K_1))|$ and $|Z| = |\mathbb{F}|^f - 1$, part (ii) follows.

Next, extend $\mathbb{F}_1 := \mathbb{F}_{|F|^f}$ so that $\mathbb{F}_1$ is a splitting field for all subgroups of L, and let M_{q_i} and M_{U_j} be as in Lemma 2.26. Then K_1 may no longer be weakly quasiprimitive. In particular, L may no longer be homogeneous, but its irreducible constituents are algebraic conjugates of one another, so they all have the same dimension e. Hence, e divides r/f. Since Lemmas 2.26, 2.27 and 2.28 imply that $e = \prod_i \dim M_{q_i} \prod_j \dim M_{U_j} = \prod_i q_i^{m_i} \prod_j t_j^{u_j}$, part (i) follows. $\qquad\square$

The following is quickly computed using the database of irreducible matrix groups in MAGMA.

Proposition 2.31. *Let $R \leq GL_r(p)$ be primitive. If $(r,p) = (4,2), (4,3), (6,2), (6,3)$ or $(8,2)$, then the list of composition factors of R is contained in one of the lists in Table 1 below.*

Table 1		
(r,p)	Maximum value of $a(R)$ among the primitive irreducible subgroups of $GL_r(p)$	List of composition factors of a primitive irreducible subgroup R of $GL_r(p)$ is contained in one of the lists below
$(4,2)$	4	$[2,2,3,5]$ $(f(R) = 4)$, $[2, A_5]$, $[2, A_6]$, $[A_7]$, $[L_4(2)]$
$(4,3)$	10	$[2,2,2,2,2,2,2,2,3,3]$, $[2,2,2,2,2,2,2,5]$, $[2,2,2,2,2,A_6]$, $[2,2,2,2,2,2,A_5]$, $[2,2,U_4(2)]$, $[2,2,L_4(3)]$
$(6,2)$	8	$[2,3,3,3,7]$, $[2,2,2,2,3,3,3,3]$, $[2,3,3,S]$, $[3,7,S]$, where $S = L_2(7)$, $L_2(8)$, A_6, A_7, $U_3(3)$, A_8, $L_3(4)$, $U_4(2)$, $PSp_6(2)$ or $L_6(2)$
$(6,3)$	7	$[2,2,2,2,3,7,13]$, $[2,2,2,3,3,13]$, $[2,2,2,2,A_5]$, $[2,2,2,2,L_2(7)]$, $[2,2,2,2,2,A_6]$, $[2, L_2(p)]$ ($p = 11, 13$), $[2,2,A_7]$, $[2,2,2,2,U_3(3)]$, $[2,2,2,2,3,L_3(3)]$, $[2,2,3,13,L_2(27)]$, $[2,2,2,L_3(4)]$, $[2, M_{12}]$, $[2,2,2,L_4(3)]$, $[2,2,2,2,U_4(3)]$, $[2,2,2,2,L_3(9)]$, $[2,2,PSp_6(3)]$, $[2,2,L_6(3)]$
$(8,2)$	7	$[2,2,2,3,5,17]$ $(f(R) = 8)$, $[2,2,3,3,5,S]$, $[2,2,3,S,S]$, $[2,3,3,S,S]$, where $S = A_5$, $L_2(7)$, A_6, $L_2(8)$, $L_2(17)$, $L_2(16)$, A_7, $U_4(2)$, A_8, A_9, A_{10}, $PSp_4(4)$, $PSp_6(2)$, $P\Omega_8^+(2)$, $P\Omega_8^-(4)$, $L_4(4)$, $PSp_8(2)$, $L_8(2)$

3 Wreath products

3.1 Wreath products as permutation and linear groups

Let R be a finite group, let S be a permutation group of degree s, and consider the wreath product $R \wr S$, as constructed in [4]. Let B be the base group of $R \wr S$, so that B is isomorphic to

the direct product of s copies of R. Thus, for a subgroup L of R, B contains the direct product of s copies of L: we will denote this direct product by B_L (so that $B_1 = 1$ and $B_R = B$).

Now, for each $1 \leq i \leq s$, set

$$R_{(i)} := \{(g_1, \ldots, g_s) \in B : g_j = 1 \text{ for all } j \neq i\} \trianglelefteq B.$$

Then $R_{(i)} \cong R$, and $B = \prod_{1 \leq i \leq s} R_{(i)}$. Furthermore, $N_{R \wr S}(R_{(i)}) \cong R_{(i)} \times (R \wr \text{Stab}_S(i))$. Hence, we may define the projection maps

$$\rho_i : N_{R \wr S}(R_{(\gamma)}) \to R_{(i)}. \tag{3.1}$$

We also define $\pi : R \wr S \to S$ to be the quotient map by B. This allows us to define a special class of subgroups of $R \wr S$.

Definition 3.1. A subgroup G of $R \wr S$ is called *large* if

(a) $G\rho_i = R_{(i)}$ for all i in $1 \leq i \leq s$, and;

(b) $G\pi = S$.

Remark 3.2. Suppose, in addition, that R is a finite permutation [respectively irreducible linear] group of degree [resp. dimension] $r \geq 1$ [we exclude $r = 1$ in the permutation group case]. If $s > 1$ and G is a large subgroup of $R \wr S$, then G is an imprimitive permutation [resp. linear] group of degree rs, with a system of s blocks, each of cardinality [resp. dimension r]. (G acts on the cartesian product $\{1, \ldots, r\} \times \{1, \ldots, s\}$ in the permutation group case.)

In fact, it turns out that all imprimitive permutation [resp. linear] groups arise as a large subgroup of a certain wreath product.

Theorem 3.3 ([33], Theorem 3.3). *Let G be an imprimitive permutation group on a set Ω_1, and let Δ be a block for G. Also, let $\Gamma := \Delta^G$ be the set of G-translates of Δ, and set $\Omega_2 := \Delta \times \Gamma$. Denote by R and S the permutation groups $\text{Stab}_G(\Delta)^\Delta$, and G^{Δ^G}, on Δ and Γ respectively. Then*

(i) $G \cong G^{\Omega_2}$ is isomorphic to a large subgroup of $R \wr S$, and;

(ii) (G, Ω_1) and (G, Ω_2) are permutation isomorphic.

If G is an imprimitive permutation group, and the block Δ as in Theorem 3.3 is assumed to be a minimal block for G, then the group $R = \text{Stab}_G(\Delta)^\Delta$ is primitive. When Ω is finite we can iterate this process, and deduce the following.

Corollary 3.4. *Let G be a transitive permutation group on a finite set Ω. Then there exist primitive permutation groups $R_1, R_2, \ldots, R_t$ such that G is a subgroup of $R_1 \wr R_2 \wr \ldots \wr R_t$.*

Remark 3.5. The wreath product construction is associative, in the sense that $R \wr (S \wr T) \cong (R \wr S) \wr T$, so the iterated wreath product in Corollary 3.4 is well-defined.

3.2   An application of the results in Section 2.2 to wreath products

We first make the following easy observation.

Proposition 3.6. *Let $A = T_1 \times T_2 \times \ldots \times T_f$, where each T_i is isomorphic to the nonabelian finite simple group T. Suppose that $M \le A$ is a subdirect product of A, and suppose that $M' \trianglelefteq M$ is also a subdirect product of A. Then $M' = M$.*

Proof. We prove the claim by induction on f, and the case $f = 1$ is trivial, so assume that $f > 1$. Since M is subdirect, each $M \cap T_i$ is normal in T_i. If $M = A$, then since the only normal subgroups of A are the groups $\prod_{i \in Y} T_i$, for $Y \subseteq \{1, \ldots, f\}$, the result is clear. So assume that $M \cap T_i = 1$ for some i. Then $M' \cap T_i = 1$, and $M'T_i/T_i$ and MT_i/T_i are subdirect products of $\prod_{j \ne i} T_j$. It follows, using the inductive hypothesis, that $M'T_i = MT_i$. Hence $M' = M$, since $M \cap T_i = 1$, and the proof is complete. $\qquad\square$

We will now fix some notation which will be retained for the remainder of the section.

- Let R be a finite group (we do not exclude the case $R = 1$).

- Let S be a transitive permutation group of degree $s \ge 2$.

- Let G be a large subgroup of the wreath product $R \wr S$ (see Definition 3.1).

- Write $B := R_{(1)} \times R_{(2)} \times \ldots \times R_{(s)}$ for the base group of $R \wr S$.

- write $\pi : G \to S$ for the projection homomorphism onto the top group.

- Let $H := N_G(R_{(1)}) = \pi^{-1}(\mathrm{Stab}_S(1))$.

- Let $\Omega := H \backslash G$.

- Let $K := G \cap B = \mathrm{core}_G(H) = \mathrm{Ker}_G(\Omega)$.

Recall that for a subgroup N of R, $B_N \cong N^s$ denotes the direct product of the distinct S-conjugates of N. In particular, if $N \trianglelefteq R$, then $B_N \trianglelefteq R \wr S$. Throughout, we will view R as a subgroup of B by identifying R with $R_{(1)}$. We also note that

- $|G : H| = s$; and

- $S = G^\Omega$.

In particular, the notation is consistent with the notation introduced at the beginning of Section 2.2.

Remark 3.7. If R is a transitive permutation group, acting on a set Δ, then G is an imprimitive permutation group acting on the set $\Delta \times \{1, 2, \ldots, s\}$, and $H = \mathrm{Stab}_G((\Delta, 1))$. Furthermore $H^\Delta = R$, since G is large (see Remark 3.5).

Our strategy for proving Theorems 1.2 and 1.5 can now be summarised as follows:

Step 1: Show that K is "built" from induced modules for G, and non-abelian G-chief factors.

Step 2: Derive bounds on $d_I(G)$ in terms of the factors from Step 1 and $d_I(S)$.

Step 3: Use the results from Section 2.2, to bound the contributions from the factors in Step 1 to the bound from Step 2.

Step 4: Use induction/previous results to bound $d_I(S)$.

We begin with Step 1.

Lemma 3.8. *Suppose that $R > 1$ and that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a normal series for R, where each factor is either elementary abelian, or a nonabelian chief factor of R. Consider the corresponding normal series $1 := G \cap B_{N_0} \leq G \cap B_{N_1} \leq \ldots \leq G \cap B_{N_e} = G$ for G. Let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$.*

(i) If V_i is elementary abelian, then M_i is a submodule of the induced module $V_i \uparrow_H^G$.

(ii) If V_i is a nonabelian chief factor of R, then M_i is either trivial, or a nonabelian chief factor of G.

For the remainder of this section, suppose that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a chief series for R, and let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$. If V_i is abelian we will also write $|V_i| = p_i^{a_i}$, for p_i prime.

We now have Step 2.

Corollary 3.9. *We have*

$$d_I(G) \leq \sum_{V_i \; abelian} d_G(M_i) + 2c_{nonab}(R) + d_I(S)$$

Proof. We will prove the corollary by induction on $|R|$. If $|R| = 1$ then the bound is trivial, since $G \cong S$ in that case, so assume that $|R| > 1$, and note that

$$G/M_1 \text{ is a large subgroup of } (R/V_1) \wr S. \tag{3.2}$$

Suppose first that V_1 is abelian. Then M_1 is a G-module, so

$$d(G) \leq d_G(M_1) + d_I(G/M_1).$$

by Lemma 2.1. Since $c_{nonab}(R) = c_{nonab}(R/V_1)$, (3.2) and the inductive hypothesis give the result.

So we may assume that V_1 is nonabelian. Then M_1 is either trivial or a minimal normal subgroup of G, by Lemma 3.8 Part (ii). Hence, $d_I(G) \leq d_I(G/M_1) + 2$ by Lemma 2.1. The result now follows, again from (3.2) and the inductive hypothesis. $\square$

Before stating our next corollary, we refer the reader to Definition 2.17 for a reminder of the definitions of the functions E and E_{sol}. The next two corollaries deal with Step 3.

Corollary 3.10. *Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

(i) $d_I(G) \le \sum_{V_i \text{ abelian}} a_i E'(s, p_i) + 2c_{nonab}(R) + d(S)$.

(ii) *Suppose that $|R| = 2$ and $s = 2^m q$, where q is odd, and that S has a tuple of primitive components $X = (R_2, \ldots, R_t)$, where $bl_{X,2}(S) \ge 1$. Let Γ be a full set of blocks for S of size $2^{bl_{X,2}(S)}$, and set $\widetilde{S} := S^\Gamma$. Then*

$$d_I(G) \le \sum_{i=0}^{bl_{X,2}(S)} E'(2^{m-i}q, 2) + d_I(\widetilde{S}).$$

Proof. By Corollary 3.9, we have

$$d_I(G) \le \sum_{V_i \text{ abelian}} d_G(M_i) + 2c_{nonab}(R) + d_I(S).$$

Now, by Corollary 2.21, $d_G(M_i) \le a_i E'(s, p_i)$. This proves (i).

So we consider Part (ii). We will show that

$$d_I(S) \le \sum_{i=1}^{bl_{X,2}(S)} E(2^{m-i}q, 2) + d_I(\widetilde{S}) \tag{3.3}$$

by induction on $bl_{X,2}(S)$. The result will then follow, since $d(G) \le E'(2^m q, 2) + d(S)$ by Part (i). Now, by hypothesis, S has a tuple of primitive components $X = (R_2, \ldots, R_t)$. Also, $|R_2| = 2$ since $bl_{X,2}(S) \ge 1$. Hence, by Theorem 3.3, S is a large subgroup of a wreath product $R_2 \wr S_2$, where either $S_2 = 1$, or S_2 is a transitive permutation group of degree $2^{m-1}q$, with a tuple $Y := (R_3, \ldots, R_t)$ of primitive components. If $S_2 = 1$ then the result follows, since $s = 4$ and $\widetilde{S} = 1$ in that case. So assume that $S_2 > 1$. By Part (i), we have

$$d_I(S) \le E'(2^{m-1}q, 2) + d_I(S_2) \tag{3.4}$$

If $bl_{X,2}(S) = 1$ then $S_2 = \widetilde{S}$ and (3.3) follows from (3.4). So assume that $bl_{X,2}(S) > 1$. Then $bl_{Y,2}(S_2) = bl_{X,2}(S) - 1 \ge 1$. The inductive hypothesis then yields $d_I(S_2) \le \sum_{i=1}^{bl_{Y,2}(S_2)} E(2^{m-1-i}q, 2) + d_I(\widetilde{S}) = \sum_{i=2}^{bl_{X,2}(S)} E(2^{m-i}q, 2) + d_I(\widetilde{S})$. The bound (3.3) now follows immediately from (3.4), which completes the proof. $\square$

The following is immediate from Corollaries 2.22 and 3.10 Part (i).

Corollary 3.11. *Suppose that $|R| \ge 2$. We have*

$$d_I(G) \ll \frac{a_{ab}(R)s}{\sqrt{\log s}} + 2c_{nonab}(R) + d_I(S) \le \frac{a(R)s}{\sqrt{\log s}} + d_I(S).$$

The next corollary will be key in our proof of Theorem 1.2 when G is imprimitive with minimal block size 4.

Corollary 3.12. *Assume that $R = S_4$ or $R = A_4$. Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

$$d_I(G) \leq E'(s, 2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E'(s, 3) + d_I(S).$$

Proof. We have

$$d_I(G) \leq d_G(M_1) + d_G(M_2) + d_G(M_3) + d_I(S) \leq 2E'(s, 2) + E'(s, 3) + d_G(M_3) + d_I(S) \quad (3.5)$$

by Corollaries 3.9 and 2.21 Part (i). Let $\Delta := \{1, 2, 3, 4\}$, so that R is transitive on Δ. We have $V_1 \cong 2^2$, $V_2 \cong 3$, and $V_3 \cong 2$ if $R \cong S_4$. Since K^Δ is a normal subgroup of $H^\Delta = R$ (see Remark 3.7), K^Δ is isomorphic to either 2^2, A_4, or S_4. In the first two cases M_3 is trivial. Hence, since

$$E'(s, 2) \leq \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\},$$

the result follows from (3.5).

So we may assume that $K^\Delta \cong S_4$. Then a Sylow 3-subgroup P_3 of K^Δ acts transitively on the non-identity elements of V_1. Thus, $\chi(P_3 \cap K, V_1^*) = 1$, so

$$d_G(M_1) \leq \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\}$$

by Corollary 2.21 Part (ii), with $(p, q) := (2, 3)$. The result now follows after applying Corollary 2.21 Part (i) to $d_G(M_2)$ and $d_G(M_3)$. $\square$

Corollary 3.13. *Let $s \geq 2$, let $S \leq \mathrm{Sym}(s)$ be transitive, and let $R \leq GL_6(2)$ be primitive and irreducible, with the following properties:*

1. *R has a characteristic subgroup K_1, such that $Z := Z(K_1)$ has order dividing 3, and $\overline{K_1} := K_1/Z$ has shape shape $N.X$, with $N \trianglelefteq \overline{K_1}$ elementary abelian of order 3^2, and $X \leq Sp_2(3)$ completely reducible;*

2. *$|R/K_1| \leq 2$.*

Let G be a large subgroup of the wreath product $R \wr S$, and let $Y \trianglelefteq X$ be the induced action of $(G \cap K_1^s)/(G \cap Z^s)$ on N. Then $d_I(G) \leq E(s, 2) + E(s, 2) + \min\left\{\lfloor bs/\sqrt{\log s_2}\rfloor, s/s_3\right\} + E(s, 3) + \min\left\{\lfloor bs/\sqrt{\log s_3}\rfloor, s/s_2\right\} + E(s, 3) + d_I(S)$, unless $|Y| = 8$, in which case $d_I(G) \leq 4E(s, 2) + \min\left\{\lfloor bs/\sqrt{\log s_3}\rfloor, s/s_2\right\} + E(s, 3) + d_I(S)$. Furthermore, if $s = 2$ then $d_I(G) \leq 6$.

Proof. Since $Y \leq Sp_2(3)$ is completely reducible, $|Y|$ must be 1, 2, 4, 8 or 24. Suppose first that $s \neq 2$. If $|Y|$ is 1, 2 or 4, then R is soluble of order dividing $2^3 3^3$, and the result follows from Corollary 3.10 Part (i), since $E(s, 2) \leq \min\left\{\lfloor bs/\sqrt{\log s_2}\rfloor, s/s_3\right\}$, and $E(s, 3) \leq \min\left\{\lfloor bs/\sqrt{\log s_3}\rfloor, s/s_2\right\}$. If $|Y| = 8$, then Y acts transitively on the nonidentity elements of N, and the result follows from Corollary 2.21 Part (ii) with $(p, q) = (3, 2)$, and Corollary 3.9. If $|Y| = 24$, then a Sylow 2-subgroup of Y acts transitively on the nonidentity elements of N; furthermore, a Sylow 3-subgroup of $Y/Z(Y) \cong A_4$ acts transitively on the

nonidentity elements of the Klein 4-subgroup of $Y/Z(Y)$. The result then follows, again from Corollary 2.21 Part (ii) and Corollary 3.9.

Finally, assume that $s = 2$. We need to prove that G can be invariably generated by 6 elements. Let $M \leq K_1$ such that $M/Z \cong N$. Also, let $H \leq K_1$ such that $M \leq H$ and $H/M = (K_1 \cap Z(Sp_2(3)))/M \leq C_2$. Arguing as in the paragraph above, we have $d_I(G/G \cap H^2) \leq E(2,2) + 2/2_2 + E(2,3) + d_I(S) = 4$ if $|Y| = 24$; $d_I(G/G \cap H^2) \leq E(2,2) + 2E(2,2) + d_I(S) = 4$ if $|Y| = 8$; and $d_I(G/G \cap H^2) \leq E(2,2) + E(2,2) + d_I(S) = 3$ if $|Y| < 8$. Thus, we just need to show that $A := G \cap H^2$ can be generated, as a G-group, by 2 elements if $|Y| \geq 8$, and 3 elements if $|Y| < 8$. Now, by Corollary 2.21 Part (i), $G \cap Z^2$ can be generated, as a G-module, by $E(2,3) = 1$ element; let x be such an element, so that $|x| = 3$. Also, H/Z has shape $N.L$, where $L \leq Z(Sp_2(3))$. Suppose first that $|Y| \geq 8$. Since a Sylow 2-subgroup of $Sp_2(3)$ acts transitively on the nonidentity elements of N, Corollary 2.21 Part (ii) implies that $G \cap M^2/G \cap Z^2$ can be generated, as a G-module, by $2/2_2 = 1$ element. Say $x_1 \in G \cap M^2$ is the preimage of such an element.

Next, suppose that $|Y| < 8$. Then again using Corollary 2.21 Part (ii) $G \cap M^2/G \cap Z^2$ can be generated, as a G-module, by $2E(s,3) = 2$ elements. Say x_1, $x_2 \in G \cap M^2$ are preimages.

Now, using Corollary 2.21 Part (i), $A/G \cap M^2$ can be generated, as a G-module, by $E(2,2) = 1$ element. Say $y \in A$ is the preimage of such an element. Clearly we may assume that $|y|$ is a power of 2. Thus, since $y \in C_{K_1}(x)$, it is now easy to see that $\{x_1, xy\}$ (or $\{x_1, x_2, xy\}$ if $|Y| < 8$) generates A as a G-group, and this completes the proof. $\square$

4 Minimal invariable generator numbers in certain classes of finite groups

In this section, we consider upper bounds for the function d_I on various classes of finite groups. We begin with bounds on $d_I(G)$ for some transitive permutation groups G.

Proposition 4.1. *Let G be a transitive permutation group of degree n.*

(i) *If $n = 6$, then $d_I(G) \leq 2$, except that $d_I(S_6) = 3$;*

(ii) *If $n = 8$, then $d_I(G) \leq 4$, and $d_I(G) = 4$ if and only if $G \cong D_8 \circ D_8$;*

(iii) *If $n = 9$, then $d_I(G) \leq 3$;*

(iv) *If $n = 10$, then $d_I(G) \leq 3$;*

(v) *If $n = 12$, then $d_I(G) \leq 4$;*

(vi) *If $n = 16$, then $d_I(G) \leq 6$;*

(vii) *If $n = 18$, then $d_I(G) \leq 4$.*

Proof. By [22, Lemma 2.1], a subset X of G invariably generates G if and only if th following holds: for each maximal subgroup M of G, at least one element of X acts fixed point freely on the G-cosets of M. Using this, and the database of transitive permutation groups of small degree (see [5]), one can readily check that the result holds in each of the listed cases, using MAGMA. □

Next, we study subgroups of wreath products in which the bottom group is cyclic.

Proposition 4.2. *Let G be a large subgroup in the wreath product $C_m \wr S_3$, where C_m denotes the cyclic group of order m. Then $d_I(G) \leq 4$.*

Proof. Let B be the base group of $W := C_m \wr S_3$, so that $d_I(G) \leq d_G(G \cap B) + d_I(G/G \cap B)$. Since $d_G(G \cap B) \leq d(G \cap B) \leq 3$, we may assume that $G/G \cap B \cong S_3$.

Now, writing B in additive notation, we next set $B_1 := \{(a,b,c) \in B \cap B : a + b + c = 0\} \leq B$. Then B_1 is a W-submodule of B. Furthermore, $W_1 \cong C_m^2$, so $N_1 := G \cap W_1$ is metacyclic. Hence, since Lemma 2.1 gives $d_I(G) \leq d_G(N_1) + d_I(G/N_1)$, it will suffice to prove that $d_i(G/N_1) \leq 2$.

Writing bars to denote reduction modulo N_1, we have $\overline{G} \cong (\overline{G \cap B}).S_3$. Furthermore, it is easily seen that $\overline{G \cap B}$ is cyclic, and is contained in $Z(G)$; write $\overline{G \cap B} = 3^k \times t$, where $(3,t) = 1$, and let x and y be elements of $\overline{G \cap B}$ of order 3^k and t, respectively. Also, let a and b be elements of $\overline{G}$ of 2-power and 3-power order, respectively, which reduce to a 2-cycle and a 3-cycle modulo $\overline{G \cap B}$. Then clearly the set $\{xa, yb\}$ invariably generates G, and the result follows. □

The next two results extend Lemmas 3.3 and 3.4 in [15]; indeed, our proofs use the same techniques as used therein.

Proposition 4.3. *Let G be a subgroup in the wreath product $C_2 \wr \mathrm{Sym}(u)$. Then $d_I(G) \leq u$, and if $d_I(G) = u$, then G is a 2-group and u is even.*

Proof. We prove the claim by induction on u, and the case $u = 1$ is clear, so assume that $u > 1$. Since $G \leq \mathrm{Sym}(2u)$, the claim $d_I(G) \leq u$ follows immediately from Theorem 2.8. So assume that $d_I(G) = u$. We need to show that G is a 2-group and that u is even. Let $\pi : G \to \mathrm{Sym}(u)$ denote the projection over the top group. If $\pi(G)$ is intransitive, with an orbit Δ of size v, then the induced action of G on the preimage of Δ in $\{1, \ldots, 2u\}$ is contained in $C_2 \wr \mathrm{Sym}(v)$, with kernel contained in $C_2 \wr \mathrm{Sym}(u - v)$; hence, the result follows from the inductive hypothesis.

So assume that $\pi(G)$ is transitive. If $\ker(\pi)$ is trivial, then $G \leq \mathrm{Sym}(u)$, so $d_I(G) \leq (u + \delta_{3,u})/2 < u$. Thus, G must be a transitive subgroup of $C_2 \wr \mathrm{Sym}(u)$. If $u = 3$ then $d_I(G) \leq 2$ by direct computation, so we must have $u \neq 3$. Using Corollary 3.10 and Theorem 2.8, we have $u = d_I(G) \leq E(u, 2) + u/2$. Using the definition of the function E, one easily sees that $E(u, 2) < u/2$ unless $u = 2$ or $u = 4$. If $u = 2$ then $G \leq D_8$. If $u = 4$, then $d_I(G) = 4$ implies that $G \cong D_8 \circ D_8$ by Proposition 4.1. The result follows. □

Proposition 4.4. *Let $G \leq S_3^u$. Then $d_I(G) \leq u$, except that $d_I(G) = u + 1$ when $G \cong 3^u : 2$, with $Z(G) = 1$.*

Proof. We prove the claim by induction on u, and the case $u = 1$ is clear, so assume that $u > 1$. Let K be the kernel of the projection of G onto the first $u - 1$ direct factors of $S_3^u := B_1 \times B_2 \times \ldots \times B_u$.

Suppose first that $G/K \cong 3^{u-1} : 2$, with $Z(G/K) = 1$. Then it is easy to see that G/K is invariably generated by a set $\{Kb_1, Kb_2, \ldots, Kb_u\}$, where $|Kb_i| = 3$ for $1 \leq i \leq u - 1$, and $|Kb_u| = 2$. Clearly we can assume that $|K| > 1$. If $K = \langle x \rangle$ with $|x| = 2$, then $|xb_1| = 6$ and $\{xb_1, b_2, \ldots, b_u\}$ invariably generates G. If $|K| = 6$, then we may assume that the projection of b_1 onto B_1 is a 2-cycle, and that the projection of b_u onto B_1 is a 3-cycle. Hence, $\{b_1, b_2, \ldots, b_u\}$ invariably generates G. If $K = \langle y \rangle$, with $|y| = 3$, and G centralises y, then $\{b_1, b_2, \ldots, yb_u\}$ invariably generates G. Finally, if $K = \langle y \rangle$, with $|y| = 3$, and G does not centralise y, then $G \cong 3^u : 2$, with $Z(G) = 1$, and the claim follows.

Finally, assume that G/K is not of the form $3^{u-1} : 2$ with trivial centre. Then, by induction, G/K is invariably generated by a set $\{Kb_1, Kb_2, \ldots, Kb_{u-1}\}$. If K is cyclic then the result is clear, so assume that $K \cong S_3$. Then we may assume that b_1 projects onto a 3-cycle in B_1. Hence, taking b_u to be any 2-cycle in K, it is clear that $\{b_1, b_2, \ldots, b_{u-1}, b_u\}$ invariably generates G. The result follows. $\square$

The following is easily checked using direct computation.

Proposition 4.5. *Let $G \leq GL_n(2)$ be irreducible, and assume that $n \leq 4$ and $d_I(G) > n/2$. Then either $n = 2$ and $G \cong GL_2(2) \cong S_3$; or $n = 3$ and $G \cong 7 : 3$ or $L_3(2)$; or $n = 4$ and $G \cong Sp_4(2) \cong S_6$.*

Lemma 4.6. *Let H and K be groups with no common nontrivial homomorphic image, and let G be a subdirect product of $H \times K$. Then $d_I(G) \leq \max \{d_I(H), d_I(K)\}$.*

Proof. The proof is almost identical to the proof of Lemma 2.4 in [15]; we give the details here for the readers benefit. Let $\{h_1, h_2, \ldots, h_m\}$ and $\{k_1, k_2, \ldots, k_n\}$ be invariable generating sets for H and K respectively, and assume, without loss of generality, that $m \geq n$. Also, let $g_1, g_2, \ldots, g_m \in G$, with $g_i = x_i y_i$ ($x_i \in H$, $y_i \in K$), and let $X = \langle h_1^{x_1} k_1^{y_1}, \ldots, h_n^{x_n} k_n^{y_n}, h_{n+1}^{x_{n+1}}, \ldots, h_m^{x_m} \rangle$. We claim that $X = H \times K = G$. Indeed, if R is any subdirect product of $H \times K$, then $R/[(R \cap H) \times (R \cap K)]$ is a homomorphic image of both H and K. Thus, we must have $R = (R \cap H) \times (R \cap K)$, and hence $R = H \times K$. Since both X and G are subdirect products of $H \times K$, our claim follows. $\square$

Proposition 4.7. *Let G be a subdirect product of $H \times K$, where $1 \neq K$ is a finite group, and H is isomorphic to either S_3, S_6, a nontrivial semidirect product $7 : 3$, or the group $L_3(2)$. Then*

(i) *If $H \neq S_6$, then $d_I(G) \leq d_I(K) + 1$, and if $H = S_6$, then $d_I(G) \leq d_I(K) + 2$.*

(ii) *Suppose that $H = S_3$. If $K = 7 : 3$ or $L_3(2)$, then $d_I(G) = 2$, while if $K = S_6$, then $d_I(G) = 3$.*

(iii) Suppose that $H = S_6$. If $K = 7 : 3$ or $L_3(2)$, then $d_I(G) = 3$, while if $K = S_6$, then $d_I(G) \leq 4$.

(iv) If $H \leq GL_3(2)$ is irreducible, and K is isomorphic to a semidirect product $3^t : 2$, in which the involutions are self-centralising, then $d_I(G) = t + 1$.

(v) If $H \leq GL_4(2)$ is irreducible, and K is isomorphic to a semidirect product $3^t : 2$, in which the involutions are self-centralising, then $d_I(G) = t + 2$.

Proof. We first prove (i). Since $G \leq H \times K$ is subdirect, $G \cap H$ is a normal subgroup of H. If $G \cap H$ is cyclic, then $d_I(G) \leq d_I(K) + 1$, as needed.

So assume that $G \cap H$ is noncyclic, and suppose first that $H \not\cong S_6$. Then $G = H \times K$; let $\{k_1, \ldots, k_t\}$ be an invariable generating set for K. If $H = L_3(2)$, then take x to be any element of H of order 7, and take y to be any element of H of order 4; if $H = 7 : 3$, then take $x, y \in H$ of order 3 and 7 respectively; and if $H = S_3$, then take $x, y \in H$ of order 2 and 3 respectively. Then $\{x, yk_1, \ldots, k_t\}$ invariably generates G. Indeed, if $H = L_3(2)$, then $H = \langle x, x^y \rangle$, since $y \notin N_H(\langle x \rangle)$, and the only proper subgroup of H containing x is of the form $7 : 3$; if $H = 7 : 3$ or S_3, then clearly $H = \langle x, x^y \rangle$. Since our choice of elements, in each case, depended only on the orders, replacing x and y by any H-conjugates yields the same result.

Assume now that $H = S_6$. If $G \cap H < S_6$, then $G \cap H = A_6$, and the result follows from Lemma 2.1 part (i). So assume that $G = H \times K$, and let $x, y, z \in H$ be a 6-cycle, a 5-cycle and a 3-cycle, respectively. Then $\{x, y, z\}$ is an invariable generating set for H. Also, let $g, h, g_1, g_2, \ldots, g_t \in G$. Note that $X := \langle x^g, y^h, (zk_1)^{g_1}, k_2^{g_2} \ldots, k_t^{g_t} \rangle \leq G$ is a subdirect product of G, with $X \cap H > 1$ and $X \cap \neq A_6$ (since $X \cap H$ contains a 6-cycle). Since $X \cap H \trianglelefteq H$, we have $X \cap H = S_6$, so $X = G$ and part (i) follows.

Next, we prove (ii). So assume that $H = S_3$, and take $h_1, h_2 \in H$ of orders 2 and 3 respectively. Assume first that $K = L_3(2)$ or $7 : 3$. It is easily seen that the only subdirect product of $H \times K$, in each case, is the full direct product. So $G = H \times K$. If $K = L_3(2)$, then choose x and y in K of orders 7 and 4 respectively, and if $K = 7 : 3$ then choose x and y in K of orders 3 and 7 respectively. Then one can easily see that $\{h_1 x, h_2 y\}$ is an invariable generating set for G, which gives us what we need. So assume that $K = S_6$, and let x, y and z be cycles in H of length 3, 5 and 6 respectively. Then it is easy to see that x, y and z invariably generate K. If $G \cap H = 1$, then the result is clear. If $G \cap H = A_3$, then take $X = \{x, h_2 y, z\}$, and if $G \cap H = H$, then take $X = \{x, h_2 y, z\}$. Clearly X invariably generates G in each case, and this completes the proof of (ii).

We now consider (iii). So $H = S_6$. If $K = 7 : 3$ or $L_3(2)$ then the result follows from Proposition 4.6, so assume that $K = S_6$. If $G \cap H = 1$, then $d_I(G) = d_I(K) = 3$, so assume that $G \cap H = A_6$ or S_6. Let $k_1, k_2, k_3 \in G$ such that $(G \cap H)k_1$ is a 3-cycle, $(G \cap H)k_2$ is a 5-cycle, and $(G \cap H)k_3$ is a 6-cycle in $G/G \cap H \cong S_6$. Then $\{(G \cap H)k_1, (G \cap H)k_2, (G \cap H)k_3\}$ is an invariable generating set for $G/G \cap H$. Now, since $A_6 \leq G \cap H$, we my assume, by replacing k_1, k_2 by suitable powers, that k_1 and $k_2 \in G$ project onto a 5-cycle and a 3-cycle in H, respectively.

20

If $G \cap H = H$, then choose $h \in H$ to be a 6-cycle in H; otherwise, set $h := 1 \in G \cap H$. Then $\{k_1, k_2, k_3, h\}$ is an invariable generating set for G, and this proves (iii).

Finally, we prove (iv) and (v). So assume that $H \leq GL_n(2)$ is irreducible, where $n = 3$ or 4, and that $K \cong 3^t : 2$ with $Z(K) = 1$. If H and K have no common nontrivial homomorphic images, then the result follows from Proposition 4.6, so assume otherwise. Then, since the only normal subgroups of K are the 3-subgroups, we conclude that H must have a nontrivial homomorphic image of order $3^j 2$, where $j \geq 0$. Using the database of irreducible matrix groups in MAGMA, we have $n = 4$, and $G \cap H \trianglelefteq H$ contains elements x, y and z with $(|x|, 2) = (|y|, 3) = 1$, such that $\{x, y, z\}$ invariably generates $G \cap H$. Choose $k_1, \ldots, k_t, k_{t+1} \in G$, such that $|(G \cap H)k_i| = 3$ for $1 \leq i \leq t$, $|(G \cap H)t_i| = 2$, and $\{(G \cap H)k_1, (G \cap H)k_2, \ldots, (G \cap H)k_t, (G \cap H)k_{t+1}\}$ invariably generates $G/G \cap H \cong K$. Also, let $L := (G \cap H) \times (G \cap K)$, and suppose first that $L = G$. Then $G = H \times K$, since G is subdirect, and hence we may assume that the k_i are elements of K. It now follows easily that $\{z, yk_1, k_2, \ldots, k_t x k_{t+1}\}$ invariably generates G, which gives us hat we need.

So we may assume that $L < G$. Hence, G/L is a common nontrivial homomorphic image of H and K. As mentioned above, we must have $|G : L| = 3^j 2$, some $j \geq 0$. If $G \cap H$ is cyclic, then $d_I(G) \leq d_I(K) + 1 = t + 2$, so assume also that $G \cap H$ is a noncyclic normal subgroup of H. By direct computation, $G/L \cong H/G \cap H \cong K/G \cap K$ is isomorphic to either C_2 or S_3. Furthermore, apart from the case $(H, G \cap H) = (3^2 : 2, 3^2)$, where $|Z(H)| = 3$, for each other pair $(H, G \cap H)$ satisfying these conditions, by direct computation we may choose an invariable generating set $\{x, y\}$ for $G \cap H$ such that $(|x|, 3) = 1$. Then if $\{g_1, \ldots, g_{t-j}\}$ is an invariable generating set for $G \cap K$, then $\{y, xg_1, \ldots, g_{t-j}\}$ is an invariable generating set for L. Also, since $j = 0$ or 1, it is clear that $d_I(G/L) \leq j + 1$. Hence $d_I(G) \leq d_I(G/L) + d_I(L) \leq t + 2$. So we may assume that $(H, G \cap H) = (3^2 : 2, 3^2)$, where $|Z(H)| = 3$; choose an invariable generating set $\{x, y\}$ for $G \cap H$ with $Z(G \cap H) = \langle y \rangle$. Also, take $k_1, k_2, \ldots, k_{t+1}$ to be as in the previous paragraph; by replacing k_{t+1} by k_{t+1}^3 if necessary, we may assume that k_{t+1} projects onto an element of order 2 in H. Hence, $\{x, k_1, k_2, \ldots, yk_{t+1}\}$ is an invariable generating set for G, and this completes the proof. $\square$

Next, we consider the function d_I on direct products of nonabelian simple groups. Wiegold proves in [36, Lemma 2] that if r is the number of direct factors in such a group G, then $d(G) \leq 2 + \lceil \log_{60} r \rceil$. However, in [22], it is shown that this bound fails when one replaces d by d_I. In fact, for each positive integer n, there is a 2-generated group G (which is a direct product of isomorphic nonabelian simple groups), such that $d_I(G) > n$. What we do have, however, is the following.

Theorem 4.8 ([**22**] **Theorem 5.1**). *Let T be a nonabelian simple group.*

(a) *If T is not one of the groups $P\Omega^+(8, 2)$ or $P\Omega^+(8, 3)$, then there are two elements $s, t \in T$ such that $T = \langle s^{g_1}, t^{g_2} \rangle$ for each choice of $g_i \in \text{Aut}(T)$.*

(b) If $T = P\Omega^+(8,2)$ or $P\Omega^+(8,3)$, and if $T \leq A \leq \mathrm{Aut}\,(T)$, then there are elements $t \in T$, $s \in A$, such that $T \leq \langle s^{g_1}, t^{g_2} \rangle$ for each choice of $g_i \in A$.

We now prove a consequence of Theorem 4.8.

Corollary 4.9. *Let $G = T_1 \times T_2 \times \ldots \times T_r$ be a direct product of isomorphic nonabelian simple groups T_i. If r is even then $d_I(G) \leq r$, and if r is odd then $d_I(G) \leq r + 1$.*

Proof. By Theorem 4.8, our claim will follow if we can prove that $d_I(T_1 \times T_2) = 2$. So write $T = T_1$ and assume that $G = T^2$. If T is not $P\Omega^+(8,2)$ or $P\Omega^+(8,3)$, then let $s, t \in T_1$ be as in Theorem 4.8; if $T = P\Omega^+(8,2)$, then by direct computation we can choose $s, t \in T$ such that $|s| \neq |t|$, and T is invariably generated by $\{s,t\}$. We claim that $\{(s,t),(t,s)\}$ invariably generates G. To see this, let (g_1, g_2), $(h_1, h_2) \in G$, and set $X := \langle (s^{g_1}, t^{g_2}),(t^{h_1}, s^{h_2})\rangle$. Let $\rho_i : G \to T_i$ be the projection maps. Then $\rho_i(X) = T_i$ for each i by Theorem 4.8, so either $X = G$, or X is a diagonal subgroup of G.

So assume that X is a diagonal subgroup of G. Then $X = \{(y, y^\alpha) : y \in T_1\}$, for some $\alpha \in \mathrm{Aut}\,(T_1)$. But then, in particular, $t = s^{g_1 \alpha g_2^{-1}}$. This contradicts part (a) of Theorem 4.8 in the case $T \neq P\Omega^+(8,2)$, $P\Omega^+(8,3)$, while the contradiction is clear if T is one of $P\Omega^+(8,2)$, $P\Omega^+(8,3)$; indeed, $|s| \neq |t|$ in these cases. The result now follows. $\square$

We now turn to the symmetric group.

Proposition 4.10. *(i) Let $G \cong S_n$. Then $d_I(G) \leq 2$, except that $d_I(S_6) = 3$;*

(ii) Let $A \cong \mathrm{Aut}\,(A_6)$, $P\Gamma L_2(8)$, $PGL_2(7)$, $PGL_4(3)$ or $L_3(4).m$, where $m = 2$, 3 or 6. Then $d_I(A) \leq 2$.

Proof. (i) If $n \leq 7$ then the result is easy, so assume that $n \geq 8$. Then we can choose a prime p with $n/2 < p < n - 2$ (this is clear for $8 \leq n \leq 11$, and follows from [11, Theorem 1.3] if $n \geq 12$); in particular, p is odd. Let x be any n-cycle in G, and let y be any p-cycle. If n is even, then set $z := 1 \in G$; otherwise, let z be any transposition in G. Then $G = \langle x, yz \rangle$ by Lemma 8.20 and Theorem 8.23 in [20]. This completes the proof.

(ii) We prove the claim by direct computation, using MAGMA. In each of the cases $A = \mathrm{Aut}\,(A_6)$, $P\Gamma L_2(8)$, $PGL_2(7)$, $PGL_4(3)$, $L_3(4).2$, $L_3(4).3 = PGL_3(4)$ or $L_3(4).6$, A has two elements x and y, which invariably generate G. The lists $[|x|, i(x); |y|, i(y)]$, where $i(t)$ denotes the conjugacy class number of the element t of A in MAGMA, is $[8, 11; 10, 13]$, $[7, 8; 9, 11]$, $[6, 6; 8, 9]$, $[26, 39; 40, 43]$, $[5, 8; 14, 14]$, $[15, 18; 21, 22]$ and $[8, 14; 21, 20]$ respectively. $\square$

Proposition 4.11. *Assume that Theorem 1.5 Part 1 holds for $F = \mathbb{F}_2$, and let $G \leq GL_4(3)$ be primitive and irreducible. Then $d_I(G) \leq 4$.*

Proof. Let $f = f(G)$, $K_1 := K_1(G)$. Then $G \leq GL_{4/f}(2^f).f$, $K_1 := G \cap GL_{4/f}(2^f)$ is irreducible and weakly quasiprimitive, and all characteristic abelian subgroups of K_1 lie in the scalar subgroup Z of K_1. Using Lemma 2.25 and Corollary 2.30, we know the possible structures of K_1/Z; we now consider each case.

Suppose first that G has shape $E.X$, where E is extraspecial of order 2^{1+4}, and $X \leq Sp_4(2)$ is completely reducible. Let u be an element of E of order 4, so that $Z = \langle u^2 \rangle$, and let $U = \langle u \rangle^G$. Assume first that G does not centralise U/Z. Then U/Z is a G-submodule of E/Z of dimension d at least 2. Let $Z \leq V \leq E$ such that V/Z is a G-complement for U/Z in E/Z. If $d = 3$ or 4, or if G does not centralise V/Z, then $\langle U, x \rangle^G = E$ for some $x \in V$ and hence, since $d_I(X) \leq 2$ by Theorem 1.5, we have $d_I(G) \leq 4$. So assume that G/Z acts trivially on V/Z. Then $G/U \cong 2^2.S_3$, where the action of S_3 on 2^2 is trivial. It is easy to see that such a group G/U can be invariably generated by 3 elements, and hence $d_I(G) \leq 4$, as needed.

So we may assume that G centralises U/Z. Thus, $\dim(V/Z) = 3$. If V/Z is irreducible as a G-module, then $d_I(G) \leq 4$ again, so assume that V/Z is reducible. Then clearly V/Z is a direct sum $V/Z = S/Z \times T/Z$, where S/Z is a trivial G-module, and T/Z is a 2-dimensional G-module. Hence, $G/V \cong (E/V).(G/E)$, and $G/E \cong S_3$, acting trivially on $E/V \cong U/Z \cong 2$. Now, let x, $y \in G$ such that $|x| = 3$, Ex is a 3-cycle in G/E, and Ey is a 2-cycle. Finally, let v_1, $v_2 \in V$ such that $V/Z = \langle Zv_1, Zv_2 \rangle^G$. Then $\{ux, v_1, v_2, y\}$ in an invariably generating set for G, and this completes the proof in the case $G \leq 2^{1+4}.Sp_4(2)$.

When $f = 1$, the only remaining possibility is $f = 1$ and G/Z is almost simple. Then, using the database of irreducible matrix groups in MAGMA, we have $(G/Z) \leq S_5$, $A_6.2^2$, or $L_4(3).2 = PGL_4(3)$. Each of these groups is invariably 2-generated by Proposition 4.10, so $d_I(G) \leq 4$.

So we may assume that $f = 2$. Then $K_1/Z \leq S_4$ or K_1/Z is almost simple. Since G/K_1 is cyclic, it suffices to prove that $d_I(K_1/Z) \leq 2$, and this is clear when $K_1/Z \leq S_4$. So assume that K_1/Z is almost simple. Again using the database of irreducible matrix groups in MAGMA, we have $(K_1/Z) \leq S_5$, $A_6.2^2$, or $L_4(3).2 = PGL_4(3)$. The claim now follows from Proposition 4.10, and this completes the proof. $\square$

5 Completely reducible linear groups and the proof of Theorem 1.5

Before proceeding to the proof of Theorem 1.5, we need a lemma which is analogous to [15, Lemma 4.1]. We remark that our proof follows the same strategy of the proof of the afore mentioned lemma in [15].

Lemma 5.1. *Let G be a finite group, with a normal elementary abelian subgroup N of order p^m, such that $N = C_G(N)$, and the action of G/N on N is completely reducible. Let H be a subnormal subgroup of G, and assume that Theorem 1.5 holds for $F = \mathbb{F}_p$ and dimensions $n \leq m$. Then*

(i) If $p = 2$, then $d_I(H) \le m$;

(ii) If $p = 3$, then $d_I(H) \le 3m/2$ if $m > 1$, and $d_I(H) \le 2$ if $m = 1$;

(iii) If $p > 3$, then $d_I(H) \le 2m$.

Proof. As shown in the first paragraph of the proof of Lemma 4.1 in [15], it suffices to prove the result for groups G as in the statement of the lemma, rather than their subnormal subgroups.

Let M be the direct sum of the one-dimensional G-submodules of N, so that $|M| = p^l$, for some $l \le m$.

Suppose first that $p = 2$. Then M is a trivial G-module, so $M = Z(G)$ (since N is self-centralising). It follows that G/N acts faithfully on N/M, and hence, by complete reducibility, and since $d_I(M) = l$, it suffices to prove the result for G/M. That is, we may assume that $M = 1$. So all irreducible constituents of N have dimension at least 2, and hence $d_G(N) \le m/2$. The result now follows from Theorem 1.5, unless $G/N \cong B_m$, where $B_m = 3^{m/2} : 2 \le GL_2(2)^{m/2}$ is as defined in Theorem 1.5. In this case, let g_1, g_2, ..., $g_{m/2}$, g be elements of G, with the g_i of 3-power order, and $|Ng| = 2$, such that G/N is invariably generated by Ng_1, ..., $Ng_{m/2}$, Ng. Now, choose a generating set x_1, ..., $x_{m/2}$ for N as a G-module, with $x_1 \in C_G(g_1)$. We claim that the set $\{g_1 x_1, g_2, \ldots, g_{m/2}, g, x_2, \ldots, x_{m/2}\}$ invariably generate G. So let h, h_1, h_2, ..., $h_{m/2}$, y_2 ,..., $y_{m/2}$ be elements of G. We need to prove that $G = H := \langle (g_1 x_1)^{h_1}, g_2^{h_2}, \ldots, g_{m/2}^{h_{m/2}}, g^h, x_2^{y_2}, \ldots, x_{m/2}^{y_{m/2}} \rangle$. Now, $x_1^{h_1} = [(g_1 x_1)^{h_1}]^{|g_1|} \in H$, and $(g_1^2)^{h_1} = [(g_1 x_1)^{h_1}]^2 \in H$ since x_1 centralises g_1, and g_1 has 3-power order. Since $\{Ng_1^2, Ng_2, \ldots, Ng_{m/2}, Ng\}$ is an invariable generating set for G/N, and $\{x_1, x_2, \ldots, x_{m/2}\}$ generates N as a G-module, the claim follows, and hence $d_I(G) \le m$, as needed.

So assume now that $p > 2$, and let L be a G-submodule of N which complements M. Let $C := C_G(L)$. Then $d_I(G/C) \le \epsilon(m - l)$, by Theorem 1.5, where $\epsilon = \epsilon(p) := 1$ if $p = 3$ and $\epsilon := 3/2$ if $p > 3$. Now, C/N acts faithfully on $N/L \cong M$, so $C/N \le GL(M) \cong (p-1)^l$. Hence, $d_I(C/L) \le d_I(C/N) + d_I(M) \le 2l$. Also, if $p = 3$ then C/L is isomorphic to a subgroup of $3^l : 2^l \cong \mathrm{Sym}\,(3)^l$, so Proposition 4.4 implies that $d_I(C/L) \le l + 1$ in that case. Thus, since $d_G(L) \le (m - l)/2$, we have $d_I(G) \le (\epsilon(p) + 1/2)(m - l) + l + \delta(p)$, where $\delta(p) := 1$ if $p = 3$ and $\delta(p) := l$ otherwise. The result now follows, except when $p = 3$ and $l \le 1$. If $l = 0$, then $L = N$ and $d_I(G) \le d_G(L) + d_I(G/N) \le 3m/2$ follows from Theorem 1.5. If $l = 1$ and C/L is cyclic, then we're done. So we may assume that $C/L \cong S_3$. Now let Y be a subset of G, of size $m - 1$, whose image modulo C invariably generates G/C; let x_1, x_2, ..., $x_{(m-1)/2}$ be a generating set for L as a G-module; let σ be an element of C which reduces to a 3-cycle modulo L; and let τ be an element of C of order 2. It is now easy to see that $Y \cup \{\sigma, x_1 \tau, x_2, \ldots, x_{(m-1)/2}\}$ is an invariable generating set for G, and this gives us what we need. $\square$

Proposition 5.2. *Let T be a nonabelian finite simple group, and let H be a subgroup of $\mathrm{Out}\,(T)$. Then $d_I(H) \le 3$.*

Proof. The structures of the outer automorphism groups of the finite simple groups are well known. When T is an alternating group, $|\mathrm{Out}\,(T)| \le 4$. When T is a simple classical group

(see [24, Chapter 2]), $\mathrm{Out}\,(T)$ modulo its (cyclic) group C of field automorphisms is either metacyclic ($T \neq P\Omega_8^+(q)$, for q odd), or isomorphic to S_4 ($T = P\Omega_8^+(q)$). Finally, if T is an exceptional group then [24, Table 5.1.B] implies that $|\mathrm{Out}\,(T)/C| \leq 6$, while if T is a sporadic group then $|\mathrm{Out}\,(T)| \leq 2$, using [24, Table 5.1.C]. The result now follows in each case. $\square$

The preparations are finally complete. We will prove both parts of Theorem 1.5 together by induction on n. If $n = 1$ then G is cyclic, and Parts 1 and 2 clearly hold. So assume, below, that $n > 1$, and that Theorem 1.5 holds for dimensions less than n. We may also assume that for fixed n, the theorem holds for fields of order less than $|F|$.

Proof of Part 2 of Theorem 1.5. Since R is homogeneous, it acts faithfully on each of its irreducible constituents, so we may assume that R is irreducible. Let $f := f(R)$ and $K_1 := K_1(R)$ be as defined after Lemma 2.24, and let K and F_1 be as in Lemma 2.24, so that $K_1 \cong K \leq R$. If $f > 1$, then K_1 satisfies the inductive hypothesis, so $H \cap K_1$ modulo its scalar subgroup can be invariably generated by $2 \log{(r/f)}$ elements. Also, HK/K is abelian of order at most f. Hence, $d_I(H) \leq \log f + 2 \log{(n/f)} + 1 \leq 2 \log n$.

So we may assume that all characteristic abelian subgroups of R are contained in Z. Let q_i, m_i, t_j, T_j, u_j and U_j be as in Corollary 2.30. Then $Z = Z(R)$ is the intersection of the groups $C_R(O_{q_i})$ and $C_R(U_j)$ over all i, j. Thus, since $\log x + \log y = \log xy$, and since $\prod_i q_i^{m_i} \prod_j t_j^{u_j}$ divides n, it will suffice to prove that, for each i, j, each subnormal subgroup of $R/C_R(O_{q_i}(R))$ can be invariably generated by $\log q_i^{m_i}$ elements, and that each subnormal subgroup of $R/C_R(U_j)$ can be invariably generated by $\log s_j^{t_j}$ elements.

To this end, we first consider a subnormal subgroup H of $R/C_R(O_q(R))$, where q is a prime such that $O_q(R)$ is not contained in Z. By Lemma 2.27, $R/C_R(O_q(R))$ has shape $q^{2m}.X$, where X is a completely reducible subgroup of $Sp_{2m}(q)$, for some $m \geq 1$. We need to prove that $d_I(H) \leq 2m \log q$. If $2m < n$, then since Theorem 1.5 (including Part 1) holds for dimensions less than n, we can apply Lemma 5.1 and conclude that $d_I(H) \leq 2\delta m$, where $\delta := 1$ if $q = 2$, $\delta := 3/2$ if $q = 3$ and $\delta := 2$ otherwise. In particular, $\delta \leq \log q$, which gives us what we need. So assume that $2m \geq n$. Since $2m \leq q^m \leq n$, we must have $q = 2$ and $m \leq 2$. If $m = 1$, then $R/C_R(O_q(R)) \leq 2^2.S_3$, and hence every subnormal subgroup of $R/C_R(O_q(R))$ can be invariably generated by 2 elements. If $m = 2$, then $R/C_R(O_q(R)) \leq 2^4.Sp_4(2)$, and hence every subnormal subgroup of $R/C_R(O_q(R))$ can be invariably generated by 4 elements, by Lemma 5.1

Next, let H be a subnormal subgroup of $\overline{R} := R/C_R(U)$, where U is a central product of u copies of a quasisimple group T, and T has a faithful irreducible representation of degree t over F. We need to show here that $d_I(H) \leq 2u \log t$. By Lemma 2.28, $\overline{T}^u \leq \overline{R} \leq \overline{T}^u.(A \wr \mathrm{Sym}\,(u))$, where $A \leq \mathrm{Out}\,(\overline{T})$. Furthermore, $|A| \leq 2$ if $t = 2$. Since $H \cap \overline{T}^u$ is a subnormal subgroup of $\overline{T}^u$, it follows that $H \cap \overline{T}^u \cong \overline{T}^v$ for some $v \leq u$. If $u = 1$, then $\overline{R} \leq \mathrm{Aut}\,(\overline{T})$, so $d_I(H) \leq 5$ by Proposition 5.2 and Corollary 4.9. Using Corollary 4.8 and Proposition 5.2, we get $d_I(H) \leq 2 + 6 + 1 = 9$ if $u = 2$, and $d_I(H) \leq 4 + 9 + 2 = 15$ if $u = 3$. If $u \geq 4$, then Proposition 5.2, Corollary 4.9 and Theorem 2.8 imply that $d_I(H) \leq u + 1 + 3u + u/2 = 9u/2 + 1 < 5u$. If $t > 5$, then $5 < 2 \log t$, and the result follows, so assume that $t \leq 5$. Suppose first that $t = 2$. Then

25

$H/\operatorname{Soc}(H) \le 2 \wr \operatorname{Sym}(u)$, and hence either u is even, or $d_I(H/\operatorname{Soc}(H)) \le u-1$, by Proposition 4.3. If u is even, then $d_I(\operatorname{Soc}(H)) \le u$ by Corollary 4.9. Otherwise, $d_I(\operatorname{Soc}(H)) \le u+1$. Thus, in either case, we have $d_I(H) \le 2u$, as needed.

Suppose next that $t = 3$. Then $|A| \le 3$ by [14, 26], so $d_I(H) \le u + 1 + 3u/2 + \delta_{3,u}/2$ by Theorem 2.8, and this is less than $(2\log 3)u$, except when $u = 1$. But in this case $H \le \overline{T}.A$, so $d_I(H) \le 3 < 2\log 3$ by Corollary 4.9, since A is cyclic, which gives us what we need. Assume now that $t = 4$. Then $|A| = 1, 2$ or 4 by [14, 26], so $H/\operatorname{Soc}(H) \le \operatorname{Sym}(4) \wr \operatorname{Sym}(u) \le \operatorname{Sym}(4u)$, and hence $d_I(H) \le 3u + 1 \le 4u$ using Theorem 2.8 and Corollary 4.9. Finally, suppose that $t = 5$. Then by [14, 26], A is metacyclic, so every subgroup of A can be invariably generated by 2 elements. Hence, if $u = 1$ then $d_I(H) \le 4 < 2\log 5$, and if $u > 1$ then $d_I(H) \le u + 1 + 2u + u/2 + 1/2 \le 9u/2 < 2u\log 5$, again using Corollary 4.8 and Theorem 2.8, as needed. $\qquad\square$

Proof of Part 1 of Theorem 1.5. Define $\epsilon = \epsilon(F)$ to be $1/2$, 1 or $3/2$ according to whether $|F| = 2$, $|F| = 3$ or $|F| > 3$, respectively. We need to prove that $d_I(G) \le \epsilon n$.

Suppose first that G is reducible, let U be an irreducible submodule of the natural module V, and let W be a G-complement for U in V. Then G embeds as a subdirect product of $G^U \times G^W$, where G^U, G^W denote the induced actions of G on U and W respectively. Since the embedding is subdirect, $G/G \cap G^W$ is isomorphic to G^U, and $G \cap G^W$ is a normal subgroup of G^W (here, we are viewing G as a subgroup of $G^U \times G^W$. Thus, $G \cap G^W$ is completely reducible by Clifford's Theorem. Since $d_I(G) \le d_I(G/G \cap G^W) + d_I(G \cap G^W)$, the result now follows from the inductive hypothesis, except when $|F| = 2$ and G has irreducible constituents of dimension 2, 3 or 4. So assume that $|F| = 2$.

Suppose first that $\dim U = 2$, so that $G^U \le S_3$, and $\dim W = n-2$. If $d_I(G^W) \le \lfloor \frac{n-2}{2} \rfloor$, then $d_I(G) \le \frac{n-2}{2} + 1 = \frac{n}{2}$, as needed, by Proposition 4.7 (i). So assume that $d_I(G^W) > \frac{n-2}{2}$. Then Proposition 4.5, together with the inductive hypothesis, implies that G^W is isomorphic to either S_3, B_{n-2}, $7:3$, $L_3(2)$ or $Sp_4(2) \cong S_6$. If $G^W \cong S_3$, then the result follows from Proposition 4.4. If G^W is isomorphic to $7:3$ or $L_3(2)$, then $d_I(G) \le 2$, while if $G^W \cong Sp_4(2)$, then $d_I(G) \le 3$, by Proposition 4.7 (ii). So assume that $G^W \cong B_{n-2}$. If G is the full direct product $G^U \times G^W$, then the result follows from Proposition 4.4. So assume that $G \cap G^U < S_3$. If $|G \cap G^U| = 1$ then $d_I(G) = d_I(K) = \frac{n}{2}$. Otherwise, $|G \cap G^U| = 3$, so $G \cong B_n$ and $d_I(G) = \lfloor \frac{n}{2} \rfloor + 1$.

Assume now that $\dim U = 3$. Then $G^U \cong 7$, $7:3$ or $GL_3(2)$. If $d_I(G^W) \le \lfloor \frac{n-3}{2} \rfloor$, then the result follows from Proposition 4.7 (i). So assume that G^W is isomorphic to one of S_3, $7:3$, $L_3(2)$, $Sp_4(2)$, or B_{n-3}. The result then follows, from Lemma 4.6 if $G^W \cong S_3$, $Sp_4(2)$; Proposition 4.7 (i) if $G^W \cong 7:3, GL_3(2)$; and from part Proposition 4.7 (iv) otherwise.

Finally, suppose that $\dim U = 4$. If $d_I(G^W) \le \lfloor \frac{n-4}{2} \rfloor$, or if $G^W \cong B_{n-4}$, then the result follows, from Proposition 4.7 parts (i) and (v). So assume that $G^W \cong S_3$, $7:3$, $L_3(2)$ or $Sp_4(2)$. If $G^U \not\cong Sp_4(2)$, then $d_I(G) \le d_I(G^U) + 1 = 3$ by Propositions 4.5 and 4.7 (i). If $G^U \cong Sp_4(2)$, then the required upper bound follows from Proposition 4.6 if $G^W \not\cong S_3$, $Sp_4(2)$, and Proposition 4.7 parts (ii) and (iii) otherwise.

So we may assume that G is irreducible. If G is imprimitive, let Δ be a minimal block for G, of dimension r say, let $R := G_\Delta^\Delta$ be the induced action of the stabiliser G_Δ on Δ, and let S be the induced action of G on the set of G-conjugates of Δ. If G primitive, set $\Delta := V$, $r := n$, $R := G$ and $S := 1$. Since G is irreducible, $R \leq GL_r(F)$ is irreducible, and $S \leq \operatorname{Sym}(s)$ is transitive, where $s := n/r$. The minimality of Δ implies also that R is primitive. In particular, each subnormal subgroup of R can be invariably generated by $h(r)$ elements, where $h(r) := 2\log r + 1$ if $|F| > 2$ or if $(r, |F|) := (4, 2)$, and $h(r) := 2\log r$ otherwise, by part 1 of Theorem 1.5. Hence, $d_I(G) \leq h(r)s + (s + \delta_{s,3}/)2$, and this yields $d_I(G) \leq \epsilon rs$, except when $|F| = 2$ and $r \leq 17$; when $|F| = 3$ and $r \leq 7$; and when $|F| > 3$ and $r \leq 3$.

We deal with these exceptional cases as follows. Throughout, we write $f = f(R)$ and $K_1 = K_1(R)$, and we take $F_1 = F_1$ to be a degree f extension of F, as in Lemma 2.24. We also identify K_1 as a characteristic subgroup of R with R/K_1 abelian of order at most f (see Lemma 2.24). If $f = r$, then $d_I(G) \leq 2s + \lfloor s/2 \rfloor$, which is less than $rs/2$ when $r \geq 3$. Thus, in our case by case analysis below, we may assume that if $r \geq 3$, then $f < r$.

1. $r = 1$. If G is primitive then G is cyclic (or trivial when $|F| = 2$), and the result is clear, so assume that G is imprimitive. If $|F| = 2$ then R is trivial, and hence G is reducible, a contradiction. So $|F| > 2$. In any case, R is cyclic, so Proposition 4.2 if $s = 3$, or Theorem 2.8 otherwise, implies that $d_I(G) \leq s + s/2 = 3s/2$. If $|F| = 3$, then Corollary 3.10 yields $d_I(G) \leq E(s, 2) + d_I(S)$. Now, $E(s, 2) \leq s/2$ for all s, so by Theorem 2.8 we may assume that $s = 3$. But in this case $d_I(G) \leq E(3, 2) + 2 = 3$, as needed.

2. $r = 2$. Suppose first that $|F| = 2$, so that $R \leq S_3$. If G is primitive, then $d_I(G) \leq 2$, which gives us what we need. So we may assume that G is imprimitive. Then $d_I(G) \leq E(s, 2) + E(s, 3) + d_I(S)$, by Corollary 3.10. If $s = 3$, and either $R < S_3$ or $S < S_3$, then we get $d_I(G) \leq E(3, 2) + 2$ or $d_I(G) \leq E(3, 2) + E(3, 3) + 1$, which in each case yields $d_I(G) \leq 3$, as needed. If $s = 3$ and $R = S = S_3$, then G is a transitive subgroup of $\operatorname{Sym}(9)$, and the result follows from Proposition 4.1. So assume that $s \neq 3$. Then $d_I(S) \leq s/2$, and the result follows from the bound $d_I(G) \leq E(s, 2) + E(s, 3) + d_I(S)$ if $E(s, 2) + E(s, 3) \leq s/2$. It is easily seen, from the definition of E, that $E(s, 2) + E(s, 3) > s/2$ only when $3 \neq s$ is 2, 4, 6 or 12. However, when $s = 2$, 4 or 6, then G is transitive of degree 6, 12 or 18, respectively (and $G < S_6$ when $s = 2$), so the result follows from Proposition 4.1. When $s = 12$, $d_I(S) \leq 4$ by the same proposition, and hence $d_I(G) \leq E(12, 2) + E(12, 3) + 4 = 11$, which gives us what we need.

Next, assume that $|F| = 3$. Then $R \leq GL_2(3)$. If G is primitive, then G is either cyclic or quaternion of order 8, or isomorphic to SD_{16}, $SL_2(3)$ or $GL_2(3)$. All of these groups are easily seen to be invariably 2-generated, so we may assume that G is imprimitive. Then $d_I(G) \leq 4E(s, 2) + E(s, 3) + d_I(S)$, by Corollary 3.10. Since $E(3, 2) = E(3, 3) = 1$, the case $s = 3$ follows if either $R < GL_2(3)$ or $S < S_3$. Thus we may assume that if $s = 3$, then $R = GL_2(3)$ and $S = S_3$. Then $G/G \cap Z^s \leq S_4 \wr S_3$ is transitive of degree 12, and hence can be invariably generated by 4 elements, by Proposition 4.1. Thus, $d_I(G) \leq E(3, 2) + 4 = 5$,

which gives us what we need. So assume that $s \neq 3$. If s is not 2, 4, 6, 8 or 16, then $4E(s,2) + E(s,3) \leq 3s/2$, so $d_I(G) \leq 2s$ by Theorem 2.8. If $s = 16$, then $d_I(S) \leq 6$ by Proposition 4.1, so $d_I(G) \leq 4E(16,2) + E(16,3) + 6 = 31$, which gives us what we need.

Suppose now that $s = 6$ or 8, and let A_K be the induced action of $G \cap R^s$ on a minimal block. If $A_K < GL_2(3)$, then $d_I(G) \leq \max\{4E(s,2), 3E(s,2) + E(s,3)\} + s/2$, which gives the result in each case. So assume that $R = GL_2(3)$. Then $G/G \cap SL_2(3)^s \leq 2 \wr S$ is transitive of degree $2s$, so by Proposition 4.1, $d_I(G/G \cap SL_2(3)^s)$ is less than or equal to 4 if $s = 6$ and 6 if $s = 8$. Thus, $d_I(G) \leq 3E_{sol}(s,2) + E_{sol}(s,3) + s - 2$, which gives the result in each case.

Finally, suppose that $s = 2$ or 4. Then R/Z is a subgroup of S_4, and if it is intransitive, then it must have order 1, 2 or 6, in which case $d_I(G) \leq 2E(s,2) + E(s,3) + s/2$ by Corollary 3.10 and Theorem 2.8. This yields the result in each case, so assume that $R/Z \leq S_4$ is transitive. Then $G/G \cap Z^s \leq \mathrm{Sym}\, 4 \wr \mathrm{Sym}\,(s)$ is transitive of degree $4s$. Thus, using Proposition 4.1, if $s = 4$ then $d_I(G/G \cap Z^s) \leq 6$, so $d_I(G) \leq E(4,2) + 6 = 8$, as needed. If $s = 2$ and $d_I(G/G \cap Z^s) = 4$, then $G/G \cap Z^s$, and hence G, is a 2-group, by Proposition 4.1 so $d_I(G) = d(G) \leq 2s$ by [22, Proposition 2.4], and [15, Theorem 1.2]. Otherwise, $d_I(G/G \cap Z^s) \leq 3$, so $d_I(G) \leq E(2,2) + 3 = 4$, as needed.

So we may assume that $|F| > 3$. Then either $f = 2$ and R is metacyclic, or $f = 1$ and either $R/Z \leq 2^2.S_3 \cong S_4$, or $R/Z \leq T.2$, for some nonabelian simple group T, by Lemmas 2.27 and 2.28. If G is primitive, then $d_I(G) \leq 3$, since S_4 and T are both invariably 2-generated.

So assume that G is imprimitive. In the case $f = 2$ we have $d_I(G) \leq 2s + s/2 + 1 \leq 3s$, using Theorem 2.8. Otherwise, Corollary 3.10 yields $d_I(G) \leq 3E(s,2) + E(s,3) + s + s/2$. It is easy to see that $3E(s,2) + 9E(s,3) \leq 3s/2$ (from which the result follows), except when $s = 2$ or 4. Furthermore, if $s = 2$ or 4 and $R/Z \leq T.2$ for a nonabelian simple group T, then $d_I(G) \leq E(s,2) + 1 + s/2$, by Corollary 3.10 which is less than $3s$ in each case. Thus, writing bars for reduction modulo Z^s, we may assume that $\overline{R} = R/Z$ has shape $N.X$, where N is elementary abelian of order 4, and $X = 1$, A_3 or S_3. Then $\overline{G}/\overline{G} \cap N^s$ is either transitive of degree s or $3s$. It follows that $d_I(\overline{G}/\overline{G} \cap N^s) \leq s$ in each case, by Proposition 4.1 (since $s = 2$ or 4). It follows that $d_I(G) \leq 2E(s,2) + s + s = 3s$, as needed, in each of the cases $s = 2$ and $s = 4$.

3. $r = 3$. We first consider the case $|F| = 2$. Then $R \leq GL_3(2)$ is primitive and irreducible, so either $R = GL_3(2)$ is simple or $|R|$ divides 21. In particular, $d_I(G) \leq 2$ if G is primitive. So assume that G is imprimitive. Then $d_I(G) \leq E(s,3) + E(s,7) + s/2 + 1$, by Corollary 3.10 and Theorem 2.8, and the result follows since $E(s,p) \leq s/2$ for all primes p.

Assume now that $|F| = 3$. Here $R \leq GL_3(3)$ is primitive and irreducible, so either R has a nonabelian simple normal subgroup T of index at most 2, or R is soluble of order dividing 78 (by direct computation). It follows from Lemma 2.1 part (iii) that

$d_I(G) \leq 3$ if G is primitive. Otherwise, Corollary 3.10 and Theorem 2.8 imply that $d_I(G) \leq E(s,2) + E(s,3) + E(s,13) + s/2 + 1 \leq 2s+1 < 3s$, as needed (since $E(s,p) \leq s/2$ for all primes p).

So assume that $|F| > 3$. Since $f = 1$, either $R/Z \leq 3^2.Sp_2(3)$ or $R/Z \leq T.A$, where T is a nonabelian simple group with a projective irreducible representation of degree 3, and $A \leq \mathrm{Out}\,(T)$. By [14, 26] and [6], $|A| \leq 3$. Thus, G primitive implies that $d_I(G) \leq 3$ by Lemmas 2.1 and 5.1, and Corollary 4.9, in either case. So assume that G is imprimitive. In either case we have $d_I(G) \leq 3E(s,2) + 3E(s,3) + s + d_I(S)$, by Corollary 3.10. Since $E(s,p) \leq s/2$ for all primes p, and $E(3,2) = E(3,3) = 1$, and $d_I(S) \leq (s + \delta_{3,s})/2$, the result follows for all s.

For the remaining cases below, we may assume that $|F| = 2$ or $|F| = 3$.

4. $r = 4$. Suppose first that $|F| = 2$. Then, since $(r, 2^f - 1) = 1$ and $f < r$, Corollary 2.30 implies that R is insoluble. Direct computation then implies that $R \leq GL_4(2)$ is isomorphic to either A_5, S_5, $3.S_5$, A_6, S_6, A_7, S_7 or $L_4(2)$. Suppose first that G is primitive. If $G = S_6$, then $d_I(G) = 3$, as needed, so assume otherwise. Then Corollary 4.9 and Proposition 4.10 yield $d_I(G) \leq 2$ in each case, except when $G \cong 3.S_5$. But in this case, a 5-cycle and a 2-cycle invariably generate G/M, where $M \trianglelefteq G$ of order 3. Clearly any element x of a Sylow 5-subgroup of G reduces to a 5-cycle modulo M, and centralises M. Thus, if $M = \langle z \rangle$, with $|z| = 3$, and $y \in G$ with My a 2-cycle, then $\{xz, y\}$ invariably generates G.

So assume that G is imprimitive. Corollary 3.10 then yields $d_I(G) \leq E(s,2) + E(s,3) + 2 + d_I(S)$, and the result now follows whenever $s \geq 4$, since $E(s,p) \leq s/2$ for all primes p, and $d_I(S) \leq (s + \delta_{s,3})/2$ by Theorem 2.8. If $s = 3$, then $d_I(G) \leq E(3,2) + E(3,3) + 2 + 2 = 6$, as needed. If $s = 2$, then the result follows from using Table 1 and Corollary 3.10, except when $R \cong 3.S_5$. But in this case, if M is a minimal normal subgroup of R of order 3, then since G is large, $G/G \cap M^2$ is isomorphic to a transitive subgroup of $S_5 \wr S_2 \leq S_{10}$. Hence $d_I(G/G \cap M^2) \leq 3$ by Proposition 4.1. Corollary 3.10 then gives $d_I(G) \leq E(2,3) + 3 = 4$ as needed.

Assume now that $|F| = 3$. If G is primitive, then the result follows from Proposition 4.11, so assume that G is imprimitive. Then Corollary 3.10, together with Table 1, yields $d_I(G) \leq \max\{8E(s,2) + 2E(s,3), 7E(s,2) + E(s,5)\} + d_I(S)$. By using Theorem 2.8 (or Proposition 4.1 when $s = 6$), and the definition of the function E, it is easy to see that this yields $d_I(G) \leq 4s$ in all cases, except when $s = 2$ or $s = 4$.

So assume that s is 2 or 4. If R is insoluble, then the result follows easily in each case, using Corollary 3.10 and Table 1, except when R has 6 composition factors of order 2, and one composition factors isomorphic to A_5, and $s = 2$. But in this case, direct computation quickly shows $R/O_2(R) \cong S_5$. Thus, $G/G \cap O_2(R)^2$ is isomorphic to an transitive group of

degree 10, and hence $d_I(G/G \cap O_2(R)) \leq 3$, by Proposition 4.1. It follows from Corollary 3.10 that $d_I(G) \leq 5E(2,2) + 3 = 8$, as needed.

So assume that R is soluble. Since $f < r$, Corollary 2.30 implies that there are two possibilities:

(a) $f = 2$ and $K_1/Z \leq 2^2.S_3 \cong S_4$. Then $d_I(G) \leq 4E(s,2) + E(s,3) + s + s/2$, by Corollary 3.10 and Theorem 2.8. This gives us what we need in each case.

(b) $f = 1$ and R/Z has shape $N.X$, where N is elementary abelian of order 2^4 and $X \leq Sp_4(2) \cong S_6$ is completely reducible. Recall also that $Y := A_K N/N \leq Sp_4(2)$ is also completely reducible, since A_K a normal subgroup of R. By direct computation, the possibilities for $|X|$ and $|Y|$ are $1, 3, 5, 6, 9, 10, 18, 20, 36$ and 72. We also compute, for each possible Y, the number j of orbits of Y on the nonidentity elements of N. Then, by Corollary 3.9 and Theorem 2.20 Part (iv) we have

$$d_I(G) \leq E(s,2) + (i + \min\{j, 4\})\lfloor bs/\sqrt{\log s}\rfloor + kE(s,3) + lE(s,5) + d_I(S) \quad (5.1)$$

where i, k and l denote the number of composition factors of Y of order 2, 3 and 5, respectively. Apart from two cases, this gives us what we need whenever $s = 2$ or $s = 4$.

The two exceptions occur when $|X| = 36$ or 72, and $(|Y|, j) = (36, 3)$ or $(72, 2)$. In these cases, the result follows from (7.1) when $s = 4$, so assume that $s = 2$. Then (by direct computation) X has a core-free subgroup of index 6. Hence, $G/G \cap N^2$ is transitive of degree 12, and hence $d_I(\overline{G}/\overline{G} \cap N^2) \leq 4$ by Proposition 4.1, where bars denote reduction modulo Z^2. Also, since $j = 3$, Corollary 3.9 and Theorem 2.20 Part (iv) imply that $d_{\overline{G}}(N) \leq 3\lfloor 2b\rfloor = 3$. Hence, by Corollary 3.10, we have $d_I(G) \leq d_G(G \cap Z^2) +$
$d_G(\overline{G} \cap N^2) + d_I(\overline{G}/\overline{G} \cap N^2) \leq E(s,2) + 3\lfloor 2b\rfloor + 4 = 8$, which gives us what we need.

5. $r = 5, 7, 11, 13$ or 17. Here, since $f = 1$, all characteristic abelian subgroups of R are contained in $Z(R)$, which has order 1 or 2, depending on whether $|F|$ has order 2 or 3 respectively. Hence, Corollary 2.30 implies that $R/Z \leq T.A$, where T is a nonabelian simple group with a projective irreducible representation M of degree r over F, and A is the subgroup of $\mathrm{Out}(T)$ which stabilises M. Suppose first that $r = 5$ or $r = 7$, and $|F| = 2$. Then direct computation implies that $R = R/Z \cong L_r(2)$. Hence, $d_I(G) \leq 2$ if G is primitive, and $d_I(G) \leq 2 + s/2 + 1/2$ by Corollary 3.10 and Theorem 2.8 if G is imprimitive. This gives the required upper bound in each case.

So we may assume that $(r, |F|) \neq (5, 2), (7, 2)$. If $G = R$ is primitive, then G/Z is almost simple, so $d_I(G) \leq 6$, and $d_I(G) \leq 5$ if $|F| = 2$ by Corollary 4.9 and Proposition 5.2. So assume that G is imprimitive; we will prove that $d_I(G) \leq 5s$, which will give us what we need. To see this, Corollary 3.10, Theorem 2.8 and Proposition 5.2 imply that $d_I(G) \leq 2 + 3s + E(s,2) + (s + \delta_{s,3})/2$. This yields $d_I(G) \leq 5s$, since $E(s,2) \leq s/2$.

6. $r = 6$. Suppose first that $|F| = 2$, and that G is primitive. If G is soluble, then since $f < r$, the only possibility is that $f = 2$, and that $R \leq 3^{1+2}.GL_2(3)$. In this case, it is easily checked by direct computation that $d_I(G) \leq 3$. So assume that G is insoluble. Let a be the number of abelian chief factors of $G \leq GL_6(2)$, and let b be the number of nonabelian chief factors. By Lemma 2.1, $d_I(G) \leq a + 2b$, and by direct computation (using the database of irreducible matrix groups in MAGMA), this gives $d_I(G) \leq 3$, except when G's number i in the MAGMA database is $44, 47, 52, 60, 61$ or 62. Suppose first that $i = 47$. Then G has a normal subgroup $N \cong C_3$ such that $G/N \cong S_6$. Let P be a Sylow 5-subgroup of G, and let $x \in P$ such that Nx is a 5-cycle in S_6. Also, let y and z be elements of G which reduce modulo N to a 3-cycle and a 6-cycle, respectively, and let w be a generator for N. Then, since x centralises w, and Nx, Ny, Nz invariably generates G/N, we see that wx, y, z invariably generates G, as needed. So assume that $i \neq 47$. In each of these cases, G has a subnormal series $1 \trianglelefteq N \trianglelefteq G$, in which one of the factors is cyclic, and the other is isomorphic to either $PGL_2(7)$, $P\Gamma L_2(8)$ or $L_3(4).m$ ($m = 2, 3$ or 6). Thus, $d_I(G) \leq 3$ by Proposition 4.10.

So assume that G is imprimitive. Using Table 1 and Corollary 3.10, if R is insoluble then we have $d_I(G) \leq \max\{E(s,2) + 2E(s,3), E(s,3) + E(s,7)\} + 2 + d_I(S)$. Since $E(s,p)$ and $d_I(S)$ are bounded above by $s/2$, the result follows. So assume that R is soluble. Then, since $f < 6$, Lemma 2.25 implies that $f = 2$ and K_1/Z has shape $N.X$, where N is elementary abelian of order 3^2, and $X \leq Sp_2(3)$ is soluble and completely reducible. It follows from Corollary 3.13 that $d_I(G) \leq 6$ if $s = 2$, as needed, and that

$$d_I(G) \leq E(s,2) + \min\left\{2E(s,3), \lfloor bs/\sqrt{\log s_3}\rfloor, s/s_2\right\} + E(s,2)$$
$$+ \min\left\{2E(s,2), \lfloor bs/\sqrt{\log s_2}\rfloor, s/s_3\right\} + \delta_{s,8}E(s,2) + (1 - \delta_{s,8})E(s,3) + E(s,3) + d_I(S)$$

in general. Using the definition of the function E, one can easily see that this latter bound, together with Theorem 2.8, yields the result whenever $s \geq 3$.

Next, assume that $|F| = 3$. If G is primitive, then $d_I(G) \leq \lfloor 2\log 6\rfloor + 1 = 6$ by Theorem 1.5, as needed. Suppose, then, that G is imprimitive. Using Table 1 and Corollary 3.10, we have

$$d_I(G) \leq \{4E(s,2) + 2E(s,3) + E(s,13), 4E(s,2) + E(s,3) + E(s,7) + E(s,3)\} + d_I(S)$$

Using the definition of the function E, this bound, together with Theorem 2.8 yields the result for all s.

For the remaining cases below we assume that $|F| = 2$.

7. $r = 8$. Since $f < r$, Lemma 2.25 implies that $R \leq GL_8(2)$ is insoluble, and using Table 1, together with Corollary 3.10, we have

$$d_I(G) \leq \max\{2E(s,2) + E(s,3) + 4, E(s,2) + 2E(s,3) + 4, 2E(s,2) + 2E(s,3) + E(s,5) + 2\} + d_I(S)$$

when G is imprimitive. Theorem 2.8, together with the bound $E(s,p) \le s/2$ now gives us what we need.

So we may assume that G is primitive. If $f \ge 4$, then $d_I(G) \le 1 + 2\log 8/f + 1 = 4$ as needed, so assume that $f = 1$ or $f = 2$. Suppose first that $f = 1$. Then $R = R/Z$ is almost simple, with a projective irreducible representation of degree 4 or 8. Hence, $R/\operatorname{Soc}(R)$ is cyclic, using the list in [15, proof of Lemma 4.2], and the result follows from Proposition 5.2 and Corollary 4.9.

So we may assume that $f = 2$. Then $G \le GL_4(4).4$, and $K_1 = G \cap GL_4(4)$ is irreducible and weakly quasiprimitive; let L be the generalised fitting subgroup of K_1. Using the list in [15, proof of Lemma 4.2] and Lemma 2.25, L has l quasisimple central factors, where $l = 1$ or 2. If $l = 1$, then $K_1/Z \cong L_{2^a}(4)$, $PSp_{2^a}(4)$ ($a = 1$ or 2), or $U_4(2)$. In particular, $d_I(G) \le 1 + d_I(K_1/Z) + 1 \le 4$ by Corollary 4.9. So all that remains is the case when L/Z is a direct product of simple groups T_1, T_2, where each T_i has a projective irreducible representation of degree 2 over $\mathbb{F}_4$. By again using the list in [15, proof of Lemma 4.2], we see that $T_i \cong L_2(4) \cong A_5$ for each i. By using the database of irreducible matrix groups in MAGMA, we see that the only possibility for $G \le GL_8(2)$ is to have number $j = 165, 172, 185, 197$ or 203 in the database. However, in each of these cases, we find that either G/L is cyclic, or $d_I(G/L) = 2$ and $Z = 1$. Hence, $d_I(G) \le 2 + d_I(L/Z) = 4$, in each case by Corollary 4.9.

8. $r = 9$. Again, since we are assuming that $f < r$, Lemma 2.25 implies that R is insoluble (since any q_i as in Lemma 2.25 divides r/f and $2^{r/f} - 1$). The database of irreducible matrix groups implies that the list of chief factors of R form a sublist of either $[3, 7, T]$ or $[2, 3, T]$, for a nonabelian simple group T, or $[2, L_2(7) \times L_2(7)]$. Thus, if G is primitive, then $d_I(G) \le 4$ by part (iii) of Lemma 2.1. If G is imprimitive, then Corollary 3.10 gives $d_I(G) \le E(s, 2) + E(s, 3) + E(s, 7) + 2 + d_I(S)$, and the result again follows easily, using Theorem 2.8, and the fact that $E(s, p) \le s/2$.

9. $r = 10, 14$ or 15. As in the cases $r = 8$ and $r = 9$ above, R must be insoluble in each case, by Lemma 2.25. Now, r divides uv, where u and v are prime, so either K_1/Z is almost simple, or $Z = C_1 \cap C_2$ where C_1, C_2 are two normal subgroups of K_1, and K_1/C_i is almost simple, for $i = 1, 2$, whose socles have projective irreducible representations over F_1 of degree u and v respectively over. Also, R/K_1 is cyclic of order 1, u, or v (since $f < r$). Note also that, using Corollary 2.29 and [14, 26], if T is a nonabelian simple group with a projective irreducible representation of degree d, and A is as in Lemma 2.25, then $d \ne 2, 3$ if $f = 1$; $|A| \le 2$ if $d = 2$; $|A| \le 3$ if $d = 3$; and $|A| = 1$ if $d = 5$, using the list in [15, proof of Lemma 4.2] ($*$).

Suppose first that $r = 10$. By ($*$), K_1/Z is an almost simple group, whose socle has a projective irreducible representation of degree 2 or 5 over F_1. Hence, if G is primitive then $d_I(K_1/Z) \le 3$ by ($*$). Thus, $d_I(G) \le d_I(G/K_1) + d_I(K_1/Z) + d_I(Z) \le 5$, as needed.

Otherwise, Corollary 3.10 and $(*)$ imply that $d_I(G) \leq \max\{E(s,2), E(s,5)\} + E(s,2) + s + 2 + s + d_I(S)$. This is less than $5s$, using Theorem 2.8, and the bound $E(s,p) \leq s/2$.

Assume now that $r = 14$ or $r = 15$. It follows, from the first paragraph above and Corollary 3.10, that K_1/Z is almost simple. Hence, $d_I(G) \leq 1 + d_I(K_1/Z) + 1 \leq 7$ if G is primitive. So we my assume that G is imprimitive. Then $d_I(G) \leq \max\{E(s,u), E(s,v)\} + E(s,2) + 2s + 2 + s + d_I(S)$, by Corollary 3.10. By using the bound $E(s,p) \leq s/2$, and the bound of Theorem 2.8, the result now follows.

10. $r = 12$. Suppose first that K_1 has a q-core not contained in Z, for some prime q. Then q divides r/f and $2^f - 1$, so $f = 2$ or $f = 4$. Thus, r/f divides 6, so $q = 3$ is the only possibility. Hence, using Lemma 2.25, we have $K_1/C_{K_1}(O_3(K_1)) \leq 3^2.Sp_2(3)$. The generalised fitting subgroup L of K_1 has at most one another central factor, and if it has such a central factor U, then $f = 2$ and U is insoluble, with $K_1/C_{K_1}(U) \leq T.2$, for a nonabelian simple group T, by Lemmas 2.27 and 2.28. In this case, T has a projective irreducible representation of degree 2 over $\mathbb{F}_4$, so we must have $T = A_5$. Hence, $d_I(K_1/C_{K_1}(U)) = 2$ by Proposition 4.10, and the result now follows if G is primitive, since $Z = C_{K_1}(O_3(K_1)) \cap C_{K_1}(T)$, $d_I(G/K_1) \leq 1$ and every subnormal subgroup of $2^{1+2}.Sp_2(3)$ is invariably 3-generated by direct computation. If G is imprimitive, then Corollary 3.10 implies that

$$d_I(G) \leq 5E(s,2) + 4E(s,3) + E(s,5) + d_I(S)$$

The result now follows, since $E(s,p) \leq s/2$, and $d_I(S) \leq (s + \delta_{s,3})/2$.

So we may assume that all central factors of L are quasisimple. If $f \geq 4$, then $d_I(G) \leq 5s + d_I(S)$ by Part 2 of Theorem 1.5, so we may assume that $f = 1, 2$ or 3 (using Theorem 2.8. Then K_1 has normal subgroups $C_1, \ldots, C_t$, with $t \leq 3$, such that K_1/C_i has shape specified in the following table. Furthermore, in each case, K_1/C_i is either almost simple with a projective irreducible representation over $\mathbb{F}_{2^f}$ of degree t_i dividing r/f, or $f = 3$, $t = 1$, and K_1/C_1 has shape $T_1^2.D_8$, where T_1 is a nonabelian simple group. To list all of the possibilities for the groups K_1/C_i, we use the list in [15, proof of Lemma 4.2]. The possibilities are as follows:

Table 2				
f	K_1/C_1	K_1/C_2	K_1/C_3	
1	A	$L_3(2).2$	-	$A \cong A_m$, S_m, or $L_4(2)$, where $5 \leq m \leq 7$.
1	$T_1.A_1$	-	-	T_1 is a nonabelian simple group, and $A_1 \leq \mathrm{Out}\,(T_1)$.
2	A	A'	-	$A \cong A_5$ or S_5; $A' \cong L_3(4)$, $PGL_3(4)$ or A_6.
2	A	-	-	$A \cong L_6(4).3 = PGL_6(4)$, $PSp_6(4)$, $U_6(3).2$, A_7, M_{22}, $U_4(3).2$, $L_4(4).2$, $U_4(4).2$, $G_2(4)$, J_2, $L_2(13)$.
3	$L_2(8)$	$L_2(8)$	-	T_i is a nonabelian simple group.
3	$T_1^2.D_8$	-	-	T_i is a nonabelian simple group.
3	$T_1.A_1$	-	-	T_1 is a nonabelian simple group, and $A_1 \leq \mathrm{Out}\,(T_1)$ of order at most 4.

Thus, if G is primitive, then $d_I(G/K_1), d_I(K_1/Z) \leq 1 - \delta_{f,1}$, and going through each of the cases in Table 2 above, and applying Corollary 4.8 and Propositions 5.2 and 4.10 where necessary, we get $d_I(G) \leq 6$. If G is imprimitive using Corollary 3.10 we get $d_I(G) \leq 2E(s,2) + 2s + 4 + \max\{E(s,2), E(s,3)\} + d_I(S)$, which is less than or equal to $6s$, using the bound $E(s,p) \leq s/2$ and Theorem 2.8.

11. $r = 16$. If G is primitive, then $d_I(G) \leq 2\log 16 = 8$ by Part 2 of Theorem 1.5, so assume that G is imprimitive. If $f > 1$, then Part 2 of Theorem 1.5 implies that $d_I(G) \leq 7s + d_I(S)$ which is less than $8s$, by Theorem 2.8. So assume that $f = 1$. Then each central factor U_j of the generalised Fitting subgroup L of R is insoluble; let T_j, S_j, t_j, and s_j be as in Lemma 2.28, for $1 \leq j \leq l$. Then $l \leq 4$, $\prod_{i=1}^{l} s_j^{t_j}$ divides 16, and $R/C_R(T_j) \leq S_j^{t_j}.(A_j \wr \mathrm{Sym}\,(t_j))$, where $A_j \leq \mathrm{Out}\,(S_j)$. Furthermore, $|A_j| \leq 2$ if $s_j = 2$. Assume first that $R = R/Z$ has shape $T^4.(2 \wr X)$, where $X \leq S_4$ is the induced action of R on the four direct factors in T^4. If X is intransitive, then $|X|$ has order 1, 2, 3 or 6. If X is transitive, then T^4 is a minimal normal subgroup of R, so T^4 is a chief factor of R. Hence, Corollary 3.10 implies that $d_I(G) \leq \max\{7E(s,2) + E(s,3) + 2, 5E(s,2) + E(s,3) + 8\} + d_I(S)$, and this gives $d_I(G) \leq 8s$, using Theorem 2.8, and the bound $E(s,p) \leq s/2$.

Going through each of the remaining possibilities for the pairs (s_j, t_j) (as in the case $r = 12$ above), and applying Corollary 3.10, we get $d_I(G) \leq \max\{4E(s,2) + 2s + 6, 2E(s,2) + 4s + 4\}$ $+ d_I(S)$, which gives us what we need, using the bounds from Theorem 2.8, and the bound $E(s,p) \leq s/2$.

□

6　The proof of Theorems 1.2 and 1.3

Throughout the remainder of the paper, we will make use of the Vinogradov notation defined in Section 1: recall, $A \ll B$ means that $A = O(B)$. We begin with a useful observation.

Lemma 6.1. *Suppose that $n = ab$, with a and b at least 2. Then*

$$\frac{b \log a}{\sqrt{\log b}} \ll \frac{ab}{\sqrt{\log ab}}$$

where the implied constant is independent of a, b, and n.

Proof. The monotonicity of the function $x/\sqrt{\log x}$ implies that

$$\frac{b \log a}{\sqrt{\log b}} \leq b \log a \leq \frac{ba}{\sqrt{\log a}}.$$

Thus, we have

$$\frac{b \log a}{\sqrt{\log b}} \leq \frac{ba}{\sqrt{\log \max\{a, b\}}} = \frac{n}{\sqrt{\log \max\{a, b\}}}.$$

Since $ab = n$, either a or b must be greater than or equal to $\sqrt{n}$. The result follows. $\square$

Proof of Theorem 1.2. We will prove the theorem by induction on n. For the initial step, assume that G is primitive. Then by Theorems 2.3 and 2.7, we have $d_I(G) \leq a(G) \ll \log n \ll n/\sqrt{\log n}$, as required.

The inductive step concerns imprimitive G. Then G is a large subgroup in a wreath product $R \wr S$, where R is a primitive permutation group of degree $r \geq 2$, S is a transitive permutation group of degree $s \geq 2$, and $rs = n$. In particular, $a(R) \ll \log r$ by Theorem 2.3, and $d_I(S) \ll s/\sqrt{\log s}$ by the inductive hypothesis. Hence, by Corollary 3.11 we have

$$d_I(G) \ll \frac{a(R)s}{\sqrt{\log s}} \ll \frac{s \log r}{\sqrt{\log s}}. \tag{6.1}$$

The result now follows immediately from Lemma 6.1. $\square$

Proposition 6.2. *Let $G \leq GL_m(p)$ be finite and irreducible. Then*

$$d_I(G) \ll \frac{\log p^m}{\sqrt{\log \log p^m}}.$$

Proof. The proof here follows the same strategy as the proof of Theorem 1.2 above. Suppose first that G is primitive. Then $d_I(G) \leq a(2 \log m + 1$ by Theorem 1.5 Part(ii). Since $m \leq \log p^m$, it follows that

$$d_I(G) \ll \log \log p^m \leq \frac{\log p^m}{\sqrt{\log \log p^m}}$$

as needed.

So we may assume that G is imprimitive. Thus, G is a large subgroup in a wreath product $R \wr S$, where $R \leq GL_r(p)$ is primitive, $S \leq \mathrm{Sym}(s)$ is transitive of degree $s \geq 2$, and $rs = n$. Since $a(R) \ll \log p^r$ by Theorem 2.4, and $d_I(S) \ll s/\sqrt{\log s}$ by Theorem 1.2, Corollary 3.11 yields

$$d_I(G) \ll \frac{a(R)s}{\sqrt{\log s}} \ll \frac{s \log p^r}{\sqrt{\log s}}. \tag{6.2}$$

As in the proof of Theorem 1.2 above, the result now follows immediately from Lemma 6.1. $\square$

35

Proof of Theorem 1.3. We will consider each of the cases of the O'Nan-Scott Theorem for primitive permutation groups; the form of the theorem we use is from [25].

(I) G is a subgroup in the affine general linear group $AGL_m(p)$, and $n = p^m$, p prime. Here, G has a unique minimal normal subgroup B, which is elementary abelian of order p^m, and G/B is isomorphic to an irreducible subgroup of $GL_m(p)$. The result now follows from Proposition 6.2 and Lemma 2.1 Part (ii).

(II) G is almost simple. Then $d_I(G) \leq 5$ by Corollary 2.10.

(III) (a) Simple diagonal action. Here, $n = |T|^{k-1}$, where T is a non-abelian finite simple group, and $k \geq 2$. Furthermore, $B := \mathrm{Soc}(G) \cong T^k$, and if $P \leq \mathrm{Sym}(k)$ is the induced action of G on on the direct factors of B, then one of the following holds:

(i) P is primitive, B is the unique minimal normal subgroup of G, and G/B has shape $E.P$ where $E \leq \mathrm{Out}(T)$, or;

(ii) $k = 2$, $P = 1$, and $G \cong B$.

Suppose first that case (i) holds. Then since any subgroup of $\mathrm{Out}(T)$ is invariably 3-generated, Lemma 2.1 and Theorem 1.2 yields

$$d_I(G) \leq 2 + d_I(G/B) \ll 5 + \frac{k}{\sqrt{\log k}} \ll \frac{k}{\sqrt{\log k}}.$$

Since $k \leq \log n$ and $k/\sqrt{\log k}$ is an increasing function, the result follows.

In the second case, $G \cong T^2$, so $d_I(G) \leq 3$ by Corollary 4.9, and the result again follows.

(b) Product action. Let $R \leq \mathrm{Sym}(r)$ be a primitive permutation group of type (II) or (III)(a), and let S be a transitive permutation group of degree s. Then, with the product action, G is a large subgroup of the wreath product $R \wr S$. In particular, $n = r^s$. Hence, we have

$$d_I(G) \ll \frac{a(R)s}{\sqrt{\log s}} + 2c_{nonab}(R) + d_I(S). \tag{6.3}$$

by Corollary 3.11.

Now, by Proposition 2.5, $a_{ab}(R) \ll \log \log r$ and $c_{nonab}(R) = 1$ if R is of type (II). If R is of type (III)(a)(i), then adopting the same notation as used in that case above, we have $a_{ab}(R) = a(R/B)$, and $R/B \leq \mathrm{Out}(T) \times P$ projects onto the primitive group P of degree $k = \log_{|T|}(r) + 1 \ll \log r$. Then

$$a_{ab}(R) = a_{ab}(R/B) \leq \log |\mathrm{Out}(T)| + a_{ab}(P) \ll \log \log r + \log k \ll \log \log r$$

and

$$c_{nonab}(R) = 1 + c_{nonab}(R/B) = 1 + c_{nonab}(P) \ll 1 + \log k \ll \log \log r$$

36

by Proposition 2.5 and Theorem 2.3. Finally, $a_{ab}(R) = 0$ and $c_{nonab}(R) = 2$ if R is of type (III)(a)(ii).

Thus, by (6.3) and Theorem 1.2 we have

$$d_I(G) \ll \frac{s \log \log r}{\sqrt{\log s}} + \frac{s}{\sqrt{\log s}} \ll \frac{s \log \log r}{\sqrt{\log s}}. \tag{6.4}$$

Let $x := \log r$. It now follows immediately from Lemma 6.1 that

$$d_I(G) \ll \frac{xs}{\sqrt{\log xs}} = \frac{\log r^s}{\sqrt{\log \log r^s}}$$

as needed.

(c) Twisted wreath action. Here, G is a semidirect product $T^s \rtimes S$, where S is a transitive permutation group of degree $s \geq 1$, and T is a non-abelian simple group. Furthermore, $n = |T|^s$, and T^s is the unique minimal normal subgroup of G. If $s = 1$, then $d_I(G) = d_I(T) \leq 2$ by Corollary 4.9, so assume that $s \geq 2$. Lemma 2.1 and Theorem 1.2 then give

$$d_I(G) \ll d_I(G/T^s) \ll \frac{s}{\sqrt{\log s}} \leq \frac{\log |T|^s}{\sqrt{\log \log |T|^s}}$$

and the proof is complete.

$\square$

References

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

[2] Aschbacher, M. Finite Group Theory. CUP, Cambridge, 1986.

[3] Cameron, P.J.; Solomon, R.G.; Turull, A. Chains of subgroups in symmetric groups. *J. Algebra* **127** (1989) 340-352.

[4] Cameron, P.J. *Permutation Groups*, London Math. Soc. (Student Texts), vol. 45, CUP, Cambridge, 1999.

[5] Cannon, J.J.; Holt, D.F. The transitive permutation groups of degree up to 32. *Experimental Math.* **17** (2008) 307–314.

[6] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. *An ATLAS of Finite Groups.* Clarendon Press, Oxford, 1985; reprinted with corrections 2003.

[7] Detomi, E.; Lucchini, A. Invariable generation of permutation groups. *Arch. Math.* **104** (2015) 301-309.

[8] Detomi, E.; Lucchini, A. Invariable generation of prosoluble groups. *Israel J. Math.* **211** **(1)** (2016) 481-491.

[9] Dixon, J.D. Random sets which invariably generate the symmetric group. *Discrete Math.* **105** (1992) 25-39.

[10] Eberhard, S.; Ford, K.; Green, B. Invariable generation of the symmetric group. *Duke Math. J.* **166 (8)** (2017) 1573-1590.

[11] El Bachraoui, M. Primes in the interval $[2n, 3n]$. *Int. J. Contemp. Math. Sci.* **1(13)** (2006) 617-621.

[12] Gorenstein, D. Finite Groups. Harper and Row, New York, 1968.

[13] Guralnick, R.M.; Malle, G. Simple groups admit Beauville structures. *J. London Math. Soc.* **85 (3)** (2012) 694721.

[14] Hiss, G.; Malle, G.; Low-dimensional representations of quasi-simple groups. *LMS J. Comput. Math.* **4** (2001) 22-63.

[15] Holt, D.F.; Roney-Dougal, C.M. Minimal and random generation of permutation and matrix groups. *J. Algebra* **387** (2013) 195-223.

[16] Fulman, J., Guralnick, R.: Derangements in simple and primitive groups. In: Ivanov, A.A., Liebeck, M.W., Saxl, J. (eds.) Groups, combinatorics, and Geometry (Durham, 2001), pp. 99121. World Sci. Publ, River Edge, NJ (2003).

[17] Fulman, J., Guralnick, R.: Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the BostonShalev conjecture. Preprint arXiv:1508.00039.

[18] Fulman, J., Guralnick, R.: Derangements in subspace actions of finite classical groups. Trans. Am. Math. Soc. doi:http://dx.doi.org/10.1090/tran/6721.

[19] Fulman, J., Guralnick, R.: Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Am. Math. Soc.* **364** (2012) 30233070.

[20] Isaacs, I.M. *Finite group theory.* Graduate Studies in Mathematics, Volume 92, Amer. Math. Soc., Providence, 2008.

[21] Jaikin-Zapirain, A.; Pyber, L. Random generation of finite and profinite groups and group enumeration. *Ann. of Math.* **173** (2011) 769814.

[22] Kantor, W.M.; Lubotzky, A.; Shalev, A. Invariable generation and the Chebotarev invariant of a finite group. *J. Algebra* **348** (2011) 302-314.

[23] Kovács, L.G.; Robinson, G.R. Generating finite completely reducible linear groups. *Proc. Amer. Math. Soc* (2) **112** (1991) 357-364.

[24] Kleidman, P.; Liebeck, M. W. *The subgroup structure of the finite classical groups.* CUP, Cambridge, 1990.

[25] Liebeck, M.W; Praeger, C.E.; Saxl, J. On the O'Nan-Scott Theorem for finite primitive permutation groups. *J. Austral. Maths. Soc (Series A)* **44** (1988) 389-396.

[26] Lubeck, F. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.* **4** (2001) 135-169.

[27] Lucchini, A.; Menegazzo, F.; Morigi, M. Asymptotic results for transitive permutation groups. *Bull. London. Math. Soc.* **32** (2000) 191-195.

[28] Lucchini, A.; Menegazzo, F.; Morigi, M. Asymptotic results for primitive permutation groups and irreducible linear groups. *J. Algebra* **223** (2000) 154-170.

[29] Lucchini, A.; Menegazzo, F.; Morigi, M. On the number of generators and composition length of finite linear groups. *J. Algebra* **243** (2001) 427-447.

[30] Luczak, T.; Pyber, L. On random generation of the symmetric group. *Combin. Probab. Comput.* **2** (1993) 505-512.

[31] Pemantle, R.; Peres, Y.; Rivin, I. Four random permutations conjugated by an adversary generate S_n with high probability. *Random Structures and Algorithms* **49 (3)** (2016) 409–428.

[32] Pyber, L. Asymptotic results for permutation groups. *Groups and Computation* DIMACS Ser. Discrete Math. Theoret. Computer Sci. **11** (ed. Finkelstein, L. and Kantor, W.M., Amer. Math. Soc., Providence, 1993) 197-219.

[33] Suprunenko, D.A. *Matrix Groups.* Translations of Mathematical Monographs, 45. Amer. Math. Soc., Providence, 1976.

[34] Tracey, G.M. Minimal generation of transitive permutation groups. arXiv:1504.07506.

[35] van der Waerden, B.L. Die seltenheit der gleichungen mit affekt. *Mathematische Annalen* **109** (1934), 1316.

[36] Wiegold, J. Growth sequences in finite groups. *J. Austral. Math. Soc. Ser. A* **25** (1978) 142-144.