Minimal and random generation of permutation and matrix groups

Derek F. Holt and Colva M. Roney-Dougal

November 27, 2012

Abstract

We prove explicit bounds on the numbers of elements needed to generate various types of finite permutation groups and finite completely reducible matrix groups, and present examples to show that they are sharp in all cases. The bounds are linear in the degree of the permutation or matrix group in general, and logarithmic when the group is primitive. They can be combined with results of Lubotzky to produce explicit bounds on the number of random elements required to generate these groups with a specified probability. These results have important applications to computational group theory. Our proofs are inductive and largely theoretical, but we use computer calculations to establish the bounds in a number of specific small cases.

MSC Classification: 20B05, 20H20, 20P05.

1 Introduction and Main Theorems

For a group G, we denote by $d(G)$ the minimal size of a generating set for G. In this paper we prove various bounds on $d(G)$, when G is either a permutation group on $n < \infty$ points, or a finite subgroup of $\mathrm{GL}_n(F)$ for $n < \infty$ and an arbitrary field F. Using these, we derive bounds on the number of random elements needed to generate G with failure probability less than ϵ, for any given $\epsilon \in (0, 1)$. All of our results make use of the classification of finite simple groups. All logarithms will be to the base 2 unless otherwise indicated.

We start with our main result for permutation groups. By a result of P. M. Neumann, published in [5, Theorem 4.1], the smallest possible upper bound for arbitrary subgroups H of S_n is $d(H) \leq n/2$, except when $n = 3$ and $H \cong \mathrm{S}_3$. In Section 6, we improve on this for subnormal subgroups of primitive groups, as follows.

Theorem 1.1 *Let H be a subnormal subgroup of a primitive permutation group G of degree n. Then $d(H) \leq \log n$ unless $n = 3$ and $H \cong \mathrm{S}_3$.*

This bound is sharp, since elementary abelian 2-groups acting regularly are normal subgroups of primitive groups. For *primitive* subgroups H of S_n, it is proved in [21] that $d(H) = O(\log n/\sqrt{\log \log n})$, but no attempt is made to estimate the constant.

Turning now to finite completely reducible matrix groups G of dimension n, it is proved in [16] that the smallest possible upper bound is $d(G) \leq 3n/2$. We improve this result under various extra hypotheses on the field F.

For an arbitrary field F, a subgroup G of $\mathrm{GL}_n(F)$ is *homogeneous* if its associated FG-module is completely reducible with all of its constituents isomorphic. The group G is *quasiprimitive* if all of its normal subgroups are homogeneous, and *weakly quasiprimitive* if all of its characteristic subgroups are homogeneous. Primitive linear groups are quasiprimitive, because otherwise the homogeneous components of some normal subgroup of G would form an imprimitive direct sum decomposition.

For n even, let $B_n \leq \mathrm{GL}_n(2)$ be the group of shape $3^{n/2}{:}2$ in which the involutions are self-centralising, such that $B_n \leq \mathrm{GL}_2(2)^{n/2}$, and B_n acts completely reducibly on a direct sum of 2-dimensional submodules. Our main result for matrix groups is as follows.

Theorem 1.2 *1. Let $G \leq \mathrm{GL}_n(F)$ be finite, and suppose that either G is completely reducible, or $\mathrm{Char}F = p$ and $O_p(G) = 1$. If F does not contain a primitive fourth root of unity then $d(G) \leq n$. Furthermore, if $|F| = 2$ and $n > 3$ then $d(G) \leq n/2$, unless $G = B_n$, as defined above, when $d(G) = n/2 + 1$.*

2. Let H be a subnormal subgroup of a finite weakly quasiprimitive subgroup G of $\mathrm{GL}_n(F)$, and let $Z = Z(\mathrm{GL}_n(F))$. Then $d(HZ/Z) \leq 2\log n$. Furthermore, if $|F| = 2$, then $d(H) \leq 2$ when $n \leq 5$ or $n = 7$, and $d(H) \leq 3$ when $n \leq 17$.

We now observe that, apart possibly from the $d(H) \leq 3$ bounds for $n \leq 17$ when $|F| = 2$, the bounds in Theorem 1.2 are best possible. First note that if $q \equiv 3 \bmod 4$ and $G \leq \mathrm{GL}_n(q)$ is a direct sum of $n/2$ copies of $Q_8 \leq \mathrm{GL}_2(q)$, then $d(G) = n$, so the first bound is best possible. If $G \leq \mathrm{GL}_n(2)$ is a direct sum of $n/2$ copies of $\mathrm{GL}_2(2) \cong \mathrm{S}_3$ for $n > 2$, then $d(G) = n/2$, so the general bound in Part 1 for $|F| = 2$ is also best possible.

Better asymptotic bounds than those in Part 1 are known for *irreducible* subgroups G of $\mathrm{GL}_n(q)$: it is proved in [21] that $d(G) = O(n \log q/\sqrt{\log n})$, but no attempt is made to estimate the constant.

An extraspecial subgroup $G = 2^{1+2m} \leq \mathrm{GL}_{2^m}(q)$ for odd q is weakly quasiprimitive (and is also a normal subgroup of a primitive group) with $d(GZ/Z) = 2m$, so the bound in Part 2 is also best possible. This example is not quasiprimitive (and hence is not primitive), and in Section 5 we prove the following, better bound for quasiprimitive groups.

Theorem 1.3 *Let $G \leq \mathrm{GL}_n(F)$ be finite and quasiprimitive. Then*

$$d(G) \leq 1 + \lceil (2\log_3 2)\, \log n \rceil.$$

For $k \geq 1$, we construct primitive groups $G \leq \mathrm{GL}_{3^k}(F)$ with $d(G) = 2k + 1$ over fields F that contain a primitive 12th root of unity, as tensor products of k copies of $3^{1+2}.Q_8$ in dimension 3, and a cyclic group of order 4 in dimension 1. So this result is also best possible for primitive groups. It is an improvement of [22, Theorem B], which states that if $G \leq \mathrm{GL}_n(F)$ is finite and quasiprimitive then $d(G) \leq c \log n$, with c about 6.

We move on now to random generation. Our study was motivated by the need for explicit upper bounds on the number of random elements that we need to choose from a permutation or matrix group G in order to ensure that we generate G with high probability. Such bounds have immediate applications to computational group theory, and in particular to the computation of *composition trees* for matrix groups over finite fields and

large base permutation groups, as described in [18] and [25]. Note that it is reasonable to assume, in such circumstances, that we know whether G is a completely reducible matrix group, or is a subnormal subgroup of a primitive permutation or matrix group.

For $\epsilon \in (0,1)$, we write $d^\epsilon(G)$ for the number of independent uniformly-distributed random elements of G required to generate G with failure probability at most ϵ. Results proved in [8] and [20] show that $d^\epsilon(G)$ is not much larger than $d(G)$. More precisely, the proof of Proposition 1.2 of [20] shows that, if $t \in \mathbb{R}$ is such that $\zeta(t) \leq 1+\epsilon$, where $\zeta(t)$ is the Riemann Zeta function, then

$$d^\epsilon(G) \leq d(G) + 2\log\log|G| + t + 2.$$

Elementary estimates show that $1+2^{-t} < \zeta(t) < 1+1/(2^{t-1}-1)$ for $t > 1$, so t increases logarithmically with $1/\epsilon$. The following corollary of Neumann's result, Theorems 1.1, 1.2 and the above equation is immediate.

Corollary 1.4 *Let $\epsilon \in (0,1)$ be given, and let t be such that $\zeta(t) \leq 1+\epsilon$.*

1. *Let $G \leq \mathrm{S}_n$ be arbitrary, with $n \geq 4$. Then:*
   (a) *$d^\epsilon(G) < n/2 + 2(\log n + \log\log n) + t + 2$;*
   (b) *if G is a subnormal subgroup of a primitive group, then $d^\epsilon(G) < 3\log n + 2\log\log n + t + 2$.*
2. *Let $G \leq \mathrm{GL}_n(q)$ be completely reducible. Then:*
   (a) *$d^\epsilon(G) < 3n/2 + 4\log n + 2\log\log q + t + 2$;*
   (b) *if $q \not\equiv 1 \bmod 4$ then $d^\epsilon(G) < n + 4\log n + 2\log\log q + t + 2$;*
   (c) *if $q = 2$ and $n \geq 4$ then $d^\epsilon(G) < n/2 + 4\log n + t + 2$;*
   (d) *if G is a subnormal subgroup of a weakly quasiprimitive group then $d^\epsilon(G) < 6\log n + 2\log\log q + t + 3$.*

The correctness of Part 2(c) for B_n follows from $\log\log|B_n| + 1 < 4\log n$.

Notation In general we will use the $\mathbb{ATLAS}$ [6] notation for group names. However, we will write C_n for a cyclic group of order n when this improves readability, and we will write $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$ in place of S_n and A_n if the group is acting on n points.

Layout of paper and background material In Section 2 we collect a variety of preliminary results, then in Section 3 we prove minimal generation results for some specific families of groups, which will be used in later sections. In Section 4 we prove Theorem 1.2, and in Section 5 we prove Theorem 1.3. Finally in Section 6 we prove Theorem 1.1.

For some arguments, we shall need to know which almost simple groups have projective representations of small degrees. For projective representations of simple groups S, this information can be gleaned from [19] for representations of groups of Lie type in their own characteristic(s), and from [12] for all other cases. We can then use [6, 14] to find the stabilisers of these representations in $\mathrm{Aut}(S)$, which enables us to find the required projective representations of almost simple groups. We shall generally omit the details of such calculations and simply list the almost simple groups that can occur. In several of our proofs, we used computer calculations for small cases. We did these in MAGMA [4], and our code is available on request.

2 Preliminary results

Our first result is [5, Theorem 4.1] and is actually due to Peter Neumann. The second is [5, Lemma 4.2] and, according to Neumann, is due to Wielandt and others.

Proposition 2.1 *Let $G \leq \mathrm{S}_n$. Then $d(G) \leq n/2$, except that $d(G) = 2$ when $n = 3$ and $G \cong \mathrm{S}_3$. If G is transitive and $n \geq 5$, then either $d(G) < n/2$, or $n = 8$ and $G \cong D_8 \circ D_8$.*

Lemma 2.2 *Let p be a prime and let the p-group P be a transitive subgroup of $\mathrm{Sym}(p^m)$ with $m \geq 1$. Then $d(P) \leq 1 + (p^{m-1} - 1)/(p - 1)$ $(\leq p^{m-1})$.*

Proposition 2.3 ([16]) *Let G be a finite and completely reducible subgroup of $\mathrm{GL}_n(F)$. Then $d(G) \leq 3n/2$.*

We now collect some easy facts about minimal generation for future use.

Lemma 2.4 *Let G and K be finitely generated, with $G = \langle g_1, \ldots, g_s \rangle$ and $K = \langle k_1, \ldots, k_t \rangle$. If $K \neq 1$ and there exist $a, b \in G$ such that $\langle a, [a, b] \rangle = G$, then $d(G \times K) \leq t + 1$. If G and K have no common nontrivial homomorphic images then $d(G \times K) \leq \max\{s, t\}$.*

Proof: For the first claim, $G \times K = \langle a, bk_1, k_2, \ldots, k_t \rangle$. For the second, assume that $s \geq t$. The only subdirect product of $G \times K$ is the direct product, so $G \times K = \langle g_1 k_1, \ldots, g_t k_t, g_{t+1} \ldots, g_s \rangle$. □

Lemma 2.5 *Let G be a finite group with a normal elementary abelian subgroup N such that the conjugation action of G/N on N is faithful and irreducible. Then $d(G) \leq \max(2, d(G/N))$.*

Proof: Let $G/N = \langle g_1 N, \ldots, g_k N \rangle$ with $k = d(G/N)$. If $k \leq 1$ then $d(G) \leq 2$, so assume that $k > 1$. Let $\mathcal{C}$ be the set of complements of N in G. If the result is false, then $\langle g_1 n_1, \ldots, g_k n_k \rangle \in \mathcal{C}$ for every choice of $n_1, \ldots, n_k \in N$. Since these complements are all distinct, $|\mathcal{C}| \geq |N|^k$. But there are $|H^1(G/N, N)|$ conjugacy classes of complements and each such class contains exactly $|N|$ complements, so $|\mathcal{C}| \leq |H^1(G/N, N)||N|$. By [3, Theorem A], $|H^1(G/N, N)| < |N|$, which is a contradiction when $k \geq 2$. □

Let G be a finite group, and let $P \in \mathrm{Syl}_p(G)$. We define $d_p(G) := d(P)$.

Lemma 2.6 (Lemma 2.1(b) and Corollary 2.2 (b) of [11]) *Let p be a prime and let S be a normal p-subgroup of the finite group G. Then $d(G) \leq \max\{d(G/S), d_p(G)+1\}$. Furthermore, if no G-composition factor of S is a nontrivial one-dimensional G-module (which is always the case when $p = 2$), then $d(G) \leq \max\{d(G/S), d_p(G)\}$.*

A group X is *almost simple* if $Y \leq X \leq \mathrm{Aut}(Y)$ for some nonabelian simple group Y.

Lemma 2.7 *Let X be a finite almost simple group with socle Y. Then $d(X) \leq 3$, and if $d(X/Y) \leq 2$ then $d(X) = 2$. If X has a projective representation of degree less than 12, then $d(X) \leq 2$. If G is quasisimple with $G/Z(G) \cong Y$ then $d(G) = d(Y)$.*

PROOF: The first part is proved in [7]. By [7, Corollary to Theorem 1], the only almost simple groups that are not 2-generated are extensions of $\mathrm{L}_d(q)$ with $d \geq 4$ and of $\mathrm{O}_d^+(q)$ with $d \geq 6$ that (in both cases) contain diagonal, graph and field automorphisms. The smallest degree of a representation of such a group is 12. The final claim is clear, since any generating set for Y must lift to a generating set for G. □

Lemma 2.8 *If S is a finite nonabelian simple group then $d(S^2) = 2$. Furthermore, $d(\mathrm{L}_3(2)^3) = d(\mathrm{SL}_2(7)^3) = 2$.*

PROOF: Let $S = \langle x, y \rangle$, where $|y| \neq |xy|$. It follows from [24] that such a generating set exists for $G \neq \mathrm{U}_3(3)$, and by direct computation otherwise. Then $\langle (x,x), (y,xy) \rangle = S^2$.

For $\mathrm{L}_3(2)$ with $|x| = 2$, $|y| = 3$ and $|xy| = 7$, it is straightforward to check that $\langle (x,y,xy), (y,x,x) \rangle \cong \mathrm{L}_3(2)^3$, and similarly for $\mathrm{SL}_2(7)$. □

Lemma 2.9 ([26, Lemma 2]) *The direct product of r nonabelian finite simple or quasisimple groups can be generated by $2 + \lceil \log_{60} r \rceil$ elements.*

Lemma 2.10 *Let G be a finite subgroup of $\mathrm{PGL}_2(F)$ for some field F, such that the inverse image of G in $\mathrm{GL}_2(F)$ is completely reducible. Then either G is cyclic or dihedral, or G is isomorphic to A_4, S_4, $\mathrm{L}_2(q)$ or $\mathrm{PGL}_2(q)$ for some prime power $q \geq 4$.*

PROOF: Since any finite completely reducible subgroup of $\mathrm{PGL}_2(F)$ is isomorphic to a completely reducible subgroup of $\mathrm{PGL}_2(q)$ for some finite q, the result follows from the classification of subgroups of $\mathrm{PGL}_2(q)$ [13, Satz II.8.27]. □

Corollary 2.11 *Let G be a finite completely reducible subgroup of $\mathrm{GL}_2(F)$ where F does not contain a primitive fourth root of 1. Then $d(G) \leq 2$.*

PROOF: This follows easily from Lemma 2.4 and the fact that G is a direct product of a double cover of one of the groups listed in Lemma 2.10 (or of the group itself if $\mathrm{char}(F) = 2$) with a cyclic subgroup of odd order. □

The following can be checked by direct computation.

Lemma 2.12 *Let G be an irreducible subgroup of $\mathrm{GL}_n(2)$, with $n \leq 3$. If $d(G) > n/2$ then (n, G) is one of the following: $(2, \mathrm{S}_3)$, $(3, 7{:}3)$, $(3, \mathrm{L}_3(2))$.*

Lemma 2.13 *Let $G \leq \mathrm{GL}_n(F)$ be finite, irreducible and weakly quasiprimitive, with an abelian characteristic subgroup not contained in $Z(\mathrm{GL}_n(F))$. Then G has a characteristic subgroup K such that $K \cong K_1 \leq \mathrm{GL}_{n/f}(F_1)$, for some divisor f of n and some extension F_1 of F. All characteristic abelian subgroups of K_1 are contained in $Z(\mathrm{GL}_{n/f}(F_1))$, and K_1 is weakly quasiprimitive. Furthermore, G/K is abelian of order at most f, and embeds naturally in $\mathrm{Gal}(F_1 \mid F)$.*

PROOF: All assertions are from the second paragraph of the proof of [22, Lemma 3.1]. Here $K = C_G(A)$, where A is an abelian characteristic subgroup of G that is maximal, subject to not being contained in $Z(\mathrm{GL}_n(F))$. □

We finish this section with several results on the generalised Fitting subgroup of a matrix group. The claims in Lemma 2.14 can all be found in [2, Chapter 11]; the set of primes r_i and the collection of normal subgroups T_i are possibly empty.

Lemma 2.14 *Let L be the generalised Fitting subgroup of a finite group G. Then L is a central product of $Z(G)$, the noncentral subgroups $O_{r_i}(G)$ for distinct primes r_i, and a collection of normal subgroups T_i of G. Each T_i is a central product of t_i copies of a quasisimple group S_i, and G permutes these copies transitively. Also, $C_G(L) = Z(L)$.*

The following is immediate from [10, Chapter 3, Theorems 7.1 and 7.2].

Lemma 2.15 *Let $G \leq \mathrm{GL}_n(F)$ be finite, and let L, r_i and T_i be as in Lemma 2.14. Assume that F is a splitting field for each central factor of L, and let C be a constituent of the natural L-module. Then C is a tensor product of a one-dimensional $Z(G)$-module, irreducible modules M_{r_i} for each $O_{r_i}(G)$, and irreducible modules M_{T_i} for each T_i.*

The next result is largely taken from [22, Lemma 1.7], with additional claims from, for example, [10, Chapter 5, Theorem 5.5].

Lemma 2.16 *Let G be finite with cyclic center Z, and assume that all abelian characteristic subgroups of G are contained in Z. Each noncentral $O_r(G)$ is the central product of $O_r(G) \cap Z$ and an extraspecial r-group E, of order r^{1+2m} say. If r is odd then E has exponent r. Any nontrivial absolutely irreducible E-module has dimension r^m, and $G/C_G(O_r(G)) \leq r^{2m}.\mathrm{Sp}_{2m}(r)$. The action of G/EZ on EZ/Z is completely reducible.*

The next result follows from [1, (3.17)] and [10, Chapter 3, Theorems 7.1 and 7.2].

Lemma 2.17 *Let $G \leq \mathrm{GL}_n(F)$ be finite, and let L, T_i, t_i, S_i and M_i be as in Lemmas 2.14 and 2.15. Assume that F is a splitting field for all central factors of L, and that L acts homogeneously. Then M_{T_i} is a tensor product of t_i copies of some faithful irreducible FS_i-module M_{S_i}. Also, $G/C_G(T_i) \leq A \wr \mathrm{Sym}(t_i)$, where A is the subgroup of $\mathrm{Aut}(S_i/Z(S_i))$ that stabilises the module M_{S_i}.*

3 Minimal generation of certain families of groups

In this section we will prove bounds on the sizes of generating sets of several families of groups, for use in the proofs of the main theorems.

The following results will be used frequently. In particular, the proposition enables us to handle the case of imprimitive groups with blocks of size 1 in the proof of Theorem 1.2. In the next three proofs we denote the cyclic group of order n by C_n, for clarity.

Lemma 3.1 *Let p be a prime, let $P \leq \mathrm{Sym}(p^m)$ be a transitive p-group with $m \geq 1$, let R be the ring of integers modulo p^k for some $k \geq 1$, let M be the permutation module of P over R, and let N be a submodule of M. Then N is generated as an RP-module by at most $2p^{m-1}$ elements, and by at most p^{m-1} elements if $k = 1$.*

PROOF: We prove this first in the case $m = 1$, so $P \cong C_p$. Let $W := C_{p^k} \wr C_p$, let B be the base group of W, and let A be a complement of B in W. Then we can identify M with B and N with a subgroup C of B with $C \trianglelefteq W$. Let $X := CA \leq W$. Now W has a faithful irreducible complex monomial representation ρ of degree p. If $C \leq Z(W)$ then C is cyclic and the result holds, so suppose not. Then X is nonabelian, so the restriction of ρ to X must remain irreducible. We can now apply [17, Lemma 5] to conclude that $d_X(C) \leq 2$ and $d_X(C) \leq 1$ when $k = 1$, where $d_X(C) := d(C/C \cap \Phi(X))$. Hence we can generate X with two (or one when $k = 1$) elements of C together with an element of A, from which it follows that C is generated as a normal subgroup of X by at most two elements in general, or one element when $k = 1$, which implies the result.

In the general case, let g be an element of order p in P that acts fixed-point-freely. As an $R\langle g\rangle$-module, M has a descending chain $M = M_0 > M_1 > \cdots > M_{p^{m-1}} = 0$ of submodules, corresponding to the orbits of g. Let $N_i = M_i \cap N$ for $0 \leq i \leq p^{m-1}$. Then it follows from the case $P \cong C_p$ that each N_{i-1}/N_i is generated by at most two elements as an $R\langle g\rangle$-module (or at most one when $k = 1$), from which the result follows. □

Proposition 3.2 *Let t be a positive integer not divisible by 4, and let $G \leq C_t \wr \mathrm{Sym}(n)$ for some $n \geq 1$. Then $d(G) \leq n$. Furthermore, if $t = 2$ and $d(G) = n$, then G is a 2-group.*

PROOF: Let ρ be the natural map from G to $\mathrm{Sym}(n)$ and let $B := \ker(\rho)$. The case $n = 1$ is easy, so assume inductively that $n > 1$. If $\mathrm{Im}(\rho)$ is intransitive with an orbit of length $m < n$, then G has a homomorphism to $C_t \wr \mathrm{Sym}(m)$ with kernel contained in $C_t \wr \mathrm{Sym}(n-m)$ so the result follows by induction. Hence we may assume that $\mathrm{Im}(\rho)$ is transitive. Let Z be the diagonal subgroup of the base group of $C_t \wr \mathrm{Sym}(n)$ and let $Y := B \cap Z$; so $Y \leq Z(G)$.

If G is a p-group for some prime p, then $n = p^m$ and, since 4 does not divide t, it follows from Lemma 3.1 that $G \cap B$ is generated as a normal subgroup of G by at most $p^{m-1}(p-1)$ elements. Hence, from Lemma 2.2, $d(G) \leq p^{m-1}(p-1) + p^{m-1} = p^m$. This completes the proof for all p-groups, including intransitive ones.

In the general case, let $P \in \mathrm{Syl}_p(G)$ for a prime p dividing $|G|$, so that $d(P) \leq n$. We claim that $d(PZ/Z) < n$ when p is odd. This is clear if p does not divide t, so assume that it does. We use essentially the trick from [16, Section 2]. First embed $C_t \wr \mathrm{Sym}(n)$, and hence also G, in the natural way into $C_{pt} \wr \mathrm{Sym}(n)$, and let Z_p be a Sylow p-subgroup of the diagonal subgroup of the base group (that is, the centre) of $C_{pt} \wr \mathrm{Sym}(n)$. Then $d(PZ_p) \leq n$, by the previous paragraph applied to PZ_p. But PZ_p contains elements of Z_p that do not lie in the Frattini subgroup of PZ_p, and hence $d(PZ_p/Z_p) < d(PZ_p)$ and, since $PZ_p/Z_p \cong P/(P \cap Z_p) = P/(P \cap Z) \cong PZ/Z$, we get $d(PZ/Z) < n$ as claimed.

Now, $d(G/B) \leq n$ by Proposition 2.1. We apply Lemma 2.6, once for each prime dividing $|B|$, to show that $d(G/Y) \leq n$. For odd primes we do this using $d(PZ/Z) < n$ for $P \in \mathrm{Syl}_p(G)$. If $p = 2$ then $d(PZ/Z) \leq n$, but the stronger conclusion of Lemma 2.6 holds. Now, since $Y \leq Z(G)$, no G-composition factor of Y is a nontrivial G-module, and hence Lemma 2.6 applied to primes dividing $|Y|$ implies that $d(G) \leq n$ as required.

Suppose now that $t = 2$ and $d(G) = n$, and regard G as a subgroup of $\mathrm{Sym}(2n)$. If G is intransitive, then its intersection with the base group of the wreath product is trivial,

so $G \cong \rho(G)$, and then $d(G) \leq n/2 < n$ (or $d(G) = 2 < 3$), a contradiction. Thus G is a transitive subgroup of $\mathrm{Sym}(2n)$, and it follows from Proposition 2.1 that either $2n \leq 4$ or $G = D_8 \circ D_8 \leq C_2 \wr \mathrm{Sym}(4)$, and in either case G is a 2-group. □

Note that $C_4 \wr \mathrm{Sym}(2)$ has subgroups G with $d(G) = 3$, so the assumption on t in the above proposition is necessary.

Lemma 3.3 *Let $G \leq X := \mathrm{S}_3^t$ for some $t \geq 1$. Then $d(G) \leq t$, except that $d(G) = t + 1$ when $|G| = 2 \times 3^t$ and $Z(G) = 1$.*

Proof: The proof is by induction on t, and the case $t = 1$ is clear, so suppose that $t > 1$.

Let K be the kernel of the projection of G onto the first $t - 1$ direct factors of X. By the inductive hypothesis $d(G/K) \leq t-1$, except that $d(G/K) = t$ when $|G/K| = 2 \times 3^{t-1}$ and $Z(G/K) = 1$. The result is immediate if $|K| = 1$ so assume that $|K| = 2, 3$ or 6.

Suppose first that $|G/K| = 2 \times 3^{t-1}$ and $Z(G/K) = 1$. Then $G/K = \langle x_1K, \ldots, x_tK \rangle$, where $|x_iK| = 3$ for $i < t$ and $|x_tK| = 2$. We explain how to choose x_1 and x_t to get $G = \langle x_1, \ldots, x_t \rangle$. If $|K| = 2$ then choose x_1 of order 6. If $|K| = 6$ then choose both x_1 and x_t of order 6. If $|K| = 3$ and x_t centralises K then choose x_t of order 6. If $|K| = 3$ and x_t inverts K, then $|G| = 2 \times 3^t$, $Z(G) = 1$ and $d(G) = t + 1$.

Otherwise $d(G/K) \leq t - 1$ and the result is clear except when $|K| = 6$. In that case choose the inverse image in G of one of the generators of G/K to project onto a 3-element in K and then take an involution in K as the extra generator, to get $d(G) \leq t$. □

Lemma 3.4 *Let $X = X_1 \times \cdots \times X_t = \mathrm{S}_4^t$ for some $t \geq 1$ and suppose that $G \leq X$, $O_2(X) \leq G$, and a Sylow 3-subgroup of G projects onto Sylow 3-subgroups of at least $t-1$ of the direct factors of X. Then $d(G) \leq t + 1$.*

Proof: The proof is by induction on t, and the case $t = 1$ is easy, so assume that $t > 1$.

We may assume that $P \in \mathrm{Syl}_3(G)$ projects onto X_t. Let $K = G \cap X_t$ be the kernel of the projection of G onto $X_1 \times \cdots \times X_{t-1}$. Then by the inductive hypothesis, there exist $x_1, \ldots, x_t \in G$ with $G/K = \langle x_1K, \ldots, x_tK \rangle$. Since $K \lhd G$ and P projects onto X_t, $|K| \neq 8$, and hence $|K| \in \{4, 12, 24\}$, since $O_2(X) \leq G$. If $|K| = 4$ then $G = \langle x_1, \ldots, x_{t+1} \rangle$, where $x_{t+1} \in K$ and $|x_{t+1}| = 2$, again because P projects onto X_t. Otherwise, by interchanging x_1 and x_2 or by replacing x_1 by x_1x_2, we can assume that x_1 induces an even permutation on X_t. Then, by multiplying x_1 by a suitable element of K, we may assume that the projection x_1' of x_1 onto X_t has order 3. We now choose $x_{t+1} \in K$ such that $K = \langle x_{t+1}, [x_1', x_{t+1}] \rangle$, to give $G = \langle x_1, \ldots, x_{t+1} \rangle$. □

The remaining lemmas in this section will be used to prove Theorem 1.3.

Lemma 3.5 *Let $G = \mathrm{L}_2(q)$ with $q \geq 5$ odd, and let f be whichever of $(q \pm 1)/2$ is odd. Let $\mathcal{C}$ be a G-conjugacy class of elements of order f.*

1. *For all $x \in \mathcal{C}$ there exists $y \in \mathcal{C}$ with $\langle x, y \rangle = G$.*
2. *For $t \geq 2$ when $q > 5$, and $t > 2$ when $q = 5$, G^t can be generated by t elements whose projections onto all direct factors of G^t lie in $\mathcal{C}$.*

PROOF: For $q \leq 11$, we verify Part 1, and Part 2 for $t = 2$ (or $t = 3$ when $q = 5$), using MAGMA, so assume for now that $q \geq 13$. Suppose first that $f = (q-1)/2$, so $|\mathcal{C}| = q(q+1)$, and each of the $q(q+1)/2$ subgroups H of G of order f contain precisely two, inverse, elements of $\mathcal{C}$. Let $x \in \mathcal{C}$. Then $|\langle x, H\rangle| = q(q-1)/2$ for $2(q-1)$ of these subgroups H. Using [13, Satz II.8.27] and the fact that $q \geq 13$, we see that, if H is any subgroup of order f such that $x \notin H$ and $|\langle x, H\rangle| \neq q(q-1)/2$, then $\langle x, H\rangle = G$. So there are $q^2 - 3q + 2$ elements $y \in \mathcal{C}$ with $\langle x, y\rangle = G$, which proves Part 1.

Let $y_1 \neq y_2$ be such elements, and let $X_{y_1,y_2} := \langle (x,x), (y_1,y_2)\rangle \leq G^2$. Either $X_{y_1,y_2} = G^2$, or it is a diagonal subgroup of G^2, and the latter occurs when there exists $\phi \in \mathrm{Aut}(G)$ with $\phi(x) = x$, $\phi(y_1) = y_2$. There are precisely $2f = |C_{\mathrm{P\Gamma L}_2(q)}(x)|$ elements $\phi \in \mathrm{Aut}(G)$ with $\phi(x) = x$. Since $q^2 - 3q + 2 > 2f$, for all y_1 there exists y_2 with $X_{y_1,y_2} = G^2$.

Using similar arguments for $f = (q+1)/2$ with $q \geq 13$, we can prove Part 1, and Part 2 with $t = 2$. This completes the proof of Part 2 for $t = 2$, and for $t = 3$ when $q = 5$.

We prove the rest of Part 2 by induction. Let $X := G^{t+1} = G^t \times G$, choose t suitable generators for G^t, and let them project onto some fixed $x \in \mathcal{C}$ in the final direct factor of X. Adjoin an additional generator that is equal to one of the existing generators of G^t and projects onto $y \in \mathcal{C}$ in the final direct factor, where $G = \langle x, y\rangle$. Then the subgroup of X generated by these $t+1$ elements projects onto and has nontrivial intersection with the final factor so, by simplicity of G, it contains this factor and hence equals X. □

Lemma 3.6 *Let $q \geq 4$, let $t > 1$, and let $S := \mathrm{L}_2(q)^t \trianglelefteq G \leq \mathrm{PGL}_2(q) \wr \mathrm{Sym}(t)$. Then $d(G) \leq \lfloor (2\log_3 2)t \rfloor$.*

PROOF: Let $Q = G/S$. We first deal with q even. If $t = 2$ or 3 and Q is trivial then the result follows from Lemmas 2.8 and 2.9. If $t = 2$ and $Q \cong \mathrm{S}_2$ then choose one generator of G outside of S that squares into an element of order $q-1$ of both factors of S, and a second generator that projects onto suitable elements of order $(q+1)$ in each factor. If $t = 3$ and $Q \cong \mathrm{S}_3$ then let $\overline{a}, \overline{b}$ be involutions generating Q. Then G is generated by their pre-images a, b where $a^2 = (a_1, a_2, a_3)$ and $b^2 = (b_1, b_2, b_3)$, with $|a_1| = |a_2| = q-1$, $|b_2| = |b_3| = q+1$, $a_3 = b_1 = 1$. If $t > 3$ or $t = 3$ and Q is cyclic then, by Theorem 1.1, $d(Q) \leq t/2$. By Lemma 2.9, $d(S) \leq 2 + \lceil \log_{60}(t) \rceil$, so $d(G) \leq t/2 + 2 + \lceil \log_{60} t \rceil < (2\log_3 2)t$.

Now assume that q is odd, let $f = (q \pm 1)/2$ with f odd, and let $\mathcal{C}$ be an $\mathrm{L}_2(q)$-conjugacy class of elements of order f. By Lemma 3.2, $d(Q) \leq t$, and $d(Q) \leq t-1$ unless Q is a 2-group.

Each element of $\mathrm{L}_2(q)$ of order f is centralised by an involution in $\mathrm{PGL}_2(q) \setminus \mathrm{L}_2(q)$. Let $\mathcal{X}$ be the set of elements of S for which the projections onto all direct factors of S lie in $\mathcal{C}$. Then the centraliser $C_G(x)$ of any $x \in \mathcal{X}$ supplements S in G. Hence, if $\overline{g} \in Q$ has order a power of 2, then some inverse image of g in G powers into x. The result now follows from Lemma 3.5 when Q is a 2-group (and hence when $d(Q) = t$), except for $(t, q) = (2, 5)$ which we check in MAGMA.

So we may assume that $d(Q) \leq t-1$. Then, using Lemma 2.9, we may generate G by choosing $t-1$ generators for Q together with $2 + \lceil \log_{60} t \rceil$ generators for S. This is fewer than $(2\log_3 2)t$ provided that $t \geq 8$. Furthermore, it follows from [23, Corollary to Theorem 4 and table in Section 14] that if $q \geq 4$ then $d(S) = 2$ for all $t \leq 19$ (note that

$d(\mathrm{A}_5^{20}) = 3$), and the result now follows except when $t = 3$, $d(Q) = 2$ and 3 divides $|Q|$ (so that Q is transitive on the factors). In that case, we can choose one of the generators of Q to have 2-power order, then choose an inverse image that powers into an element of $\mathcal{X}$. We choose the preimage of the second generator of Q arbitrarily. Finally, we choose one further generator from one of the $\mathrm{L}_2(q)$ factors. □

Lemma 3.7 *Let S be a finite nonabelian simple group, and suppose that $T \leq \mathrm{Aut}(S)$ has socle S and a faithful projective representation of degree s. Let $G \leq T \wr \mathrm{Sym}(t)$ for some $t \geq 1$ where $S^t \leq G$. Then $d(G) \leq \lfloor (2 \log_3 s)\, t \rfloor$, except that $d(G) = 2$ when $(s, t) = (2, 1)$.*

Proof: Let K be the intersection of G with the base group of the wreath product. By Proposition 2.1, $d(G/K) \leq t/2$, except when $t = 3$ and $G/K \cong \mathrm{S}_3$. By Lemma 2.7, $d(K) \leq 3t$, so $d(G) \leq 7t/2$ (or 11 when $t = 3$), which is at most $\lfloor (2 \log_3 s)\, t \rfloor$ when $s \geq 8$.

By Lemma 2.7, if $s \leq 7$ then $d(G) \leq 5t/2$ (or 8 when $t = 3$ and $G/K \cong \mathrm{S}_3$). This is at most $\lfloor (2 \log_3 s)\, t \rfloor$ when $s \geq 5$, and also when $s = 4$ except in the case $t = 3$, $G/K \cong \mathrm{S}_3$. If $t = 1$ then the result is clear, so assume that $t > 1$.

If $s = 2$ then the result follows from Lemma 3.6. If $s = 3$, then $|T/S| \leq 3$ by [12, 19]. By Lemmas 2.9 and 2.8, $d(S^t) \leq 2 + \lceil \log_{60} t \rceil$ or 2 when $t = 2$, and by Proposition 3.2 $d(G/S^t) \leq t$, so the result follows.

Suppose finally that $s = 4$, $t = 3$ and $G/K \cong \mathrm{S}_3$. Then $|T/S| = 1, 2$ or 4, by [12, 19]. It can be shown using Lemma 2.6 and Lemma 3.1 with $p = 2$ that $d(G/S^3) \leq 5$. Since G/K acts transitively on the factors of K, we generate G by adjoining two generators of one factor, to give $d(G) \leq 7$. □

4 The proof of Theorem 1.2

The proof of both parts together is by induction on n. For fixed n, we may also assume that the result is true for all finite fields $\mathbb{F}_q$ with $q < |F|$ and, for a given n and F, for all groups of order less than $|G|$. To ground the induction, note that if $n = 1$, then G is cyclic and is trivial when $|F| = 2$: so both Part 1 and Part 2 are true.

4.1 The proof of Part 2 of Theorem 1.2

We begin with a lemma which is also used in the proof of Theorem 1.1.

Proposition 4.1 *Let the finite group G have a normal elementary abelian subgroup N with $|N| = p^m$, where $C_G(N) = N$ and the induced conjugation action of G/N on N is completely reducible. Let H be a subnormal subgroup of G. Assume that Theorem 1.2 holds for $F = \mathbb{F}_p$ and dimensions $n \leq m$. Then:*

(i) if $p = 2$ then $d(H) \leq m$;

(ii) if $p \equiv 3 \bmod 4$ then $d(H) \leq 3m/2$ if $m > 1$, and $d(H) \leq 2$ if $m = 1$;

(iii) if $p \equiv 1 \bmod 4$ then $d(H) \leq 2m$.

PROOF: We regard N as a faithful completely reducible $\mathbb{F}_pG/N$-module. Suppose that H is actually normal in G. Then $H \cap N$ is an $\mathbb{F}_pG/N$-submodule of N and hence has a complement $C \leq N$ with $C \lhd G$. Thus $[H, C] \leq H \cap C = 1$, and so $C_G(N) = N$ implies that $C_H(H \cap N) = H \cap N$. Also $H/(H \cap N) \cong HN/N \trianglelefteq G/N$ and so by Clifford's theorem H and $H \cap N$ satisfy the same hypotheses as G and N with a possibly smaller value of m. So it suffices to prove the result for $H = G$.

Let $M \cong p^l$ be the sum of the one-dimensional submodules of N.

Suppose that $p = 2$. By complete reducibility, $M = Z(G)$ and G/N acts faithfully on N/M. Since $d(M) = l$, it suffices to prove the result for G/M; so assume that $M = 1$. So all $\mathbb{F}_pG/N$-constituents of N have dimension at least 2. By Theorem 1.2, if $m > 3$ and $G/N \neq B_m$, then $d(G/N) \leq m/2$ and, by choosing one generator from each constituent of N, we get $d(G) \leq m$. If $m \leq 3$ and $d(G/N) > m/2$, then G/N is listed in Lemma 2.12, and the result can be checked by direct computation. If $m > 3$ and $G/N = B_m$ then N is a direct sum of $m/2$ constituents of dimension 2. We multiply one of the generators of G modulo N of order 3 by an element of order 2 that it centralises in N to get $d(G) \leq m$.

Now suppose that $p \equiv 3 \bmod 4$, let L be an $\mathbb{F}_pG/N$-complement of M in N, and let $K = C_G(L)$. Then K/N acts faithfully on $N/L \cong M$, and so $K/N \leq (p-1)^l$. By Lemma 2.6, $d(K/L) \leq l+1$. Also, G/K acts faithfully and completely reducibly on L and so $d(G/K) \leq m - l$ by Theorem 1.2. Hence, by taking $d(G/K)$ generators for G modulo K, together with the $l + 1$ generators for K/L, and one element from each irreducible constituent of L, we get $d(G) \leq l + 1 + 3(m - l)/2$. This is at most $3m/2$ except when $l \leq 1$. If $l = 0$ then $d(G) \leq 3m/2$. If $l = 1$, then either K/L is cyclic and the result follows, or K/L is isomorphic to a 2-generator subgroup of $p.(p - 1)$. In this case we multiply a generator of K modulo L of order dividing $p - 1$ by a generator of one of the constituents of L to reduce the number of generators and get $d(G) \leq 3m/2$.

The proof when $p \equiv 1 \bmod 4$ is similar but easier, using Proposition 2.3. □

Lemma 4.2 *Let H be a subnormal subgroup of a weakly quasiprimitive group $G \leq \mathrm{GL}_n(2)$. If $n \leq 5$ or $n = 7$ then $d(H) \leq 2$, and if $n \leq 17$ then $d(H) \leq 3$.*

PROOF: Since G is homogeneous, without loss of generality G is irreducible. We use the MAGMA database of irreducible subgroups of $\mathrm{GL}_n(2)$ to verify that $d(H) \leq 2$ when $n \leq 5$ or $n = 7$. It remains to prove that $d(H) \leq 3$ when $6 \leq n \leq 17$ and $n \neq 7$.

By Lemma 2.13, we may consider G as a subgroup of $\mathrm{GL}_m(2^e).e$ with $n = me \leq 17$, where $R := G \cap \mathrm{GL}_m(2^e)$ is irreducible, weakly quasiprimitive and has no nonscalar characteristic abelian subgroups. If $m = 1$, then $d(H) \leq 2$, so assume that $m > 1$. Let $K = R \cap Z(\mathrm{GL}_m(2^e))$, so K is cyclic of order dividing $2^e - 1$. By Lemmas 2.14 and 2.16 the generalised Fitting subgroup L of R is a central product of K, extraspecial groups, and quasisimple groups. These central factors may not act absolutely irreducibly, but L is homogeneous by weak quasiprimitivity, and m is a multiple of the product of the degrees of the associated absolutely irreducible representations of the factors.

Using [12, 19], we list the almost simple groups that can arise as sections of R/K in terms of the degree d of their absolutely irreducible projective representations in characteristic 2. Such representations with $d > 8$ can only be involved if $n = m = d$ and

$G \leq \mathrm{GL}_n(2)$ is almost simple, in which case $d(H) \leq 3$ by Lemma 2.7. So we may assume that $d \leq 8$. The table below contains the isomorphism types of $X/Z(X)$ for conjugacy class representatives of the subgroups $X \leq \mathrm{GL}_d(2^f)$ with $d \leq 8$ and $df \leq 17$, where X is the largest subgroup of $\mathrm{GL}_d(2^f)$ containing and normalising X^∞ such that $X/Z(X)$ is almost simple, and X^∞ is absolutely irreducible.

d	$X/Z(X)$	d	$X/Z(X)$
2	$\mathrm{L}_2(2^f)$ $(2 \leq f \leq 8)$	6	$\mathrm{L}_6(2)$, $\mathrm{S}_6(2)$, $\mathrm{S}_7, \mathrm{S}_8, \mathrm{U}_4(2).2$,
3	$\mathrm{L}_3(2^f)$ $(f = 1, 3, 5)$, $\mathrm{PGL}_3(4)$,		$\mathrm{U}_3(3).2 \leq \mathrm{L}_6(2)$, $\mathrm{PGL}_6(4)$, $\mathrm{S}_6(4)$,
	$\mathrm{A}_6 \leq \mathrm{L}_3(4)$, $\mathrm{PGL}_3(16)$,		$\mathrm{U}_6(2).3, \mathrm{A}_7$, $\mathrm{M}_{22}, \mathrm{U}_4(3).2, \mathrm{L}_4(4).2$,
	$\mathrm{U}_3(4) \leq \mathrm{L}_3(16)$		$\mathrm{U}_4(4).2$, $\mathrm{G}_2(4)$, J_2, $\mathrm{L}_2(13) \leq \mathrm{PGL}_6(4)$
4	$\mathrm{L}_4(2^f)$, $\mathrm{S}_4(2^f)$ $(f \leq 4)$,	7	$\mathrm{L}_7(2^f)$ $(f \leq 2)$, $\mathrm{U}_7(2) \leq \mathrm{L}_7(4)$
	$\mathrm{S}_5, \mathrm{A}_7 \leq \mathrm{L}_4(2)$, $\mathrm{U}_4(2) \leq \mathrm{L}_4(4)$,	8	$\mathrm{L}_8(2^f), \mathrm{S}_8(2^f)$ $(f \leq 2)$,
	$\mathrm{Sz}(8) \leq \mathrm{L}_4(8)$, $\mathrm{U}_4(4) \leq \mathrm{L}_4(16)$		$\mathrm{O}_8^+(2).2$, $\mathrm{O}_8^-(2).2, \mathrm{L}_2(17), \mathrm{A}_9, \mathrm{S}_9$,
5	$\mathrm{L}_5(2^f)$ $(f \leq 3)$,		$\mathrm{S}_{10}, \mathrm{L}_2(7).2, \mathrm{S}_6(2) \leq \mathrm{PGL}_8(2)$,
	$\mathrm{U}_5(2)$, $\mathrm{L}_2(11) \leq \mathrm{L}_5(4)$		$\mathrm{U}_8(2), \mathrm{O}_8^+(4).2, \mathrm{O}_8^-(4).2, \mathrm{A}_6.2_2$,
			$\mathrm{S}_6(4), \mathrm{U}_3(4).2, \mathrm{L}_3(4).3.2 \leq \mathrm{PGL}_8(4)$

All of these groups are 2-generated by Lemma 2.7. If L/K is simple, then R/K is one of the groups above, and we can check directly that $d(R) \leq 2$. So $d(G) \leq 3$ and $d(H) \leq 3$.

Suppose next that L/K is a direct product of simple groups. Since the representations of the groups $\mathrm{L}_2(2^f)$ with $d = 2$ have degree at least 4 over $\mathbb{F}_2$, a representation over $\mathbb{F}_2$ of a central product of $\mathrm{L}_2(2^f)$ with another group in the list with absolute dimension d has degree at least $4d$. Clearly, a representation of a central product of two groups with absolute dimension $d, d_1 \geq 3$ has dimension at least $3d$. Hence, since $n \leq 17$, the examples with $d \geq 6$ cannot arise in such a product. Furthermore, R/K is either a subdirect product of two of the groups listed above with $d \leq 5$, or else $R/K \leq \mathrm{A}_5 \wr \mathrm{Sym}(b) \leq \mathrm{PGL}_{2^b}(4)$ (with $b \in \{2, 3\}$), $\mathrm{L}_2(8) \wr \mathrm{Sym}(2) \leq \mathrm{L}_4(8)$, $R/K \leq \mathrm{L}_2(16) \wr \mathrm{Sym}(2) \leq \mathrm{PGL}_4(16)$, $R/K \leq \mathrm{L}_3(2) \wr \mathrm{Sym}(2) \leq \mathrm{PGL}_9(2)$, or $R/K \leq S \wr \mathrm{Sym}(2) \leq \mathrm{PGL}_{16}(2)$ with S one of the subgroups of $\mathrm{PGL}_4(2)$ on the list. In each of these cases, $d(R/K) \leq 2$. If R/K has no nontrivial cyclic quotient of odd order then $d(G) \leq 3$. The only other possibility is $\mathrm{A}_5 \wr \mathrm{Alt}(3) \leq \mathrm{PGL}_4(8)$ with $R = (\mathrm{A}_5 \wr \mathrm{Alt}(3)) \times 3$. We check directly that $d(R) \leq 2$, so $d(G) \leq 3$ and $d(H) \leq 3$.

Suppose finally that a factor D of L is an extraspecial p-group. Then D is homogenous, and $\gcd(m, 2^e - 1) \equiv 0 \mod p$. Hence $p = 3$ and $e = 2$ or 4, so $n = 6$ or 12.

If $n = 6$, then $G \leq 3^{1+2}.Q_8.\mathrm{S}_3 \leq \mathrm{GL}_3(4).2$. We calculate in MAGMA that all subnormal subgroups H of irreducible weakly quasiprimitive groups G satisfy $d(H) \leq 3$.

If $n = 12$, then there are two possibilities. The first is $G \leq \mathrm{GL}_6(4).2$ and $L \cong 3^{1+2} \times \mathrm{L}_2(4)$. Then G is contained in the subdirect product of index 2 in $3^{1+2}.Q_8.\mathrm{S}_3 \times \mathrm{L}_2(4).2$, and so H is either isomorphic to one of the groups with $n = 6$ or is the subdirect product of one of these groups with $\mathrm{L}_2(4).2 \cong \mathrm{S}_5$. In either case, $d(H) \leq 3$. The second possibility is $G \leq \mathrm{GL}_3(16).4$ and $3^{1+2} \trianglelefteq G$. We check in MAGMA that all subnormal subgroups of all weakly quasiprimitive subgroups of $\mathrm{GL}_3(16).4$ are 3-generated. □

Proof of Theorem 1.2, Part 2: Let $H \leq \mathrm{GL}_n(F)$ be a subnormal subgroup of a weakly quasiprimitive group G. Let Z be the centre of $\mathrm{GL}_n(F)$: the scalar matrices. We

shall prove by induction on n that $d(HZ/Z) \leq 2\log n$. The sharper results for $n \leq 17$ when $|F| = 2$ follow from Lemma 4.2.

Since G is homogeneous, we may assume that G is irreducible. If G has an abelian nonscalar characteristic subgroup, then let K, K_1 and f be as in Lemma 2.13. Notice that K_1 satisfies the inductive hypothesis, and that $d(HK/K) \leq \log f$. By the inductive hypothesis, $H \cap K_1$ modulo its scalar subgroup requires at most $2\log(n/f)$ generators, so $d(H) \leq 1 + 2\log(n/f) + \log f \leq 2\log n$ as required.

So we may assume that all abelian characteristic subgroups of G are contained in Z. In particular, $Z(G) = G \cap Z$. Let L be the generalised Fitting subgroup of G, and let r_i, T_i, t_i, and S_i be as given in Lemma 2.14. Since L is characteristic in G, it is homogeneous, and therefore acts faithfully on each of its constituents. We now extend the field F to make it a splitting field for all subgroups of L. After doing this, G might not remain weakly quasiprimitive, but we shall make no further use of this property of G. In particular, L may no longer be homogeneous, but its irreducible constituents all have the same dimension m and are algebraic conjugates of one another, so L still acts faithfully on them. We shall actually prove that $d(HZ/Z) \leq 2\log m$, so we may assume that L is irreducible and hence $n = m$. Let M_{r_i} and M_{T_i} be as in Lemma 2.15. Then n is at least the product of the dimensions of the M_{r_i} and the M_{T_i}.

Our strategy is as follows. We prove that all subnormal subgroups A_i of $G/C_G(O_{r_i}(G))$ satisfy $d(A_i) \leq 2\log(\deg(M_{r_i}))$, and that all subnormal subgroups A_i of $G/C_G(T_i)$ satisfy $d(A_i) \leq 2\log(\deg(M_{T_i}))$. Since $C_G(L) = G \cap Z$, the sum of these $d(A_i)$ is an upper bound for $d(HZ/Z)$. Since $\log xy = \log x + \log y$, this will complete the proof.

We first consider $G/C_G(O_r(G))$ for r prime, with $O_r(G) = (O_r(G) \cap Z) \circ E$ for some extraspecial r-group E, by Lemma 2.16. By Lemma 2.16, $G/C_G(O_r(G))$ is a subgroup of an extension of an elementary abelian group N of order r^{2m} by $\mathrm{Sp}_{2m}(r)$, for some m. Also, the action of GZ/EZ on EZ/Z is completely reducible. Now, $2m \leq r^m = \deg(M_r) \leq n$, and $2m < n$ unless $r = 2$ and $m \leq 2$. If $r = 2$ then $|F| > 2$, so we may assume by the inductive hypothesis (see the beginning of this section) that Part 1 is true for dimensions up to $2m$ and for the field $\mathbb{F}_r$. Let H be a subnormal subgroup of $G/C_G(O_r(G))$. Then Proposition 4.1 yields $d(H) \leq 2m$ when $r = 2$, $d(H) \leq 3m$ when $r = 3$, and $d(H) \leq 4m$ for all $r \geq 5$, which gives $d(H) \leq 2\log(\deg(M_r))$ in all cases.

Now consider $\overline{G} := G/C_G(T)$ for T a central product of t copies of a quasisimple group S, and for a faithful irreducible FT-module M_T, and let H be a subnormal subgroup of $\overline{G}$. By Lemma 2.17 $\dim M_T = s^t$ with s being the dimension of the faithful irreducible FS-module M_S, and $\overline{G}$ has a normal subgroup K_1 with $\overline{S}^t \leq K_1 \leq \mathrm{Aut}(\overline{S})^t$ and $\overline{G}/K_1 \leq \mathrm{Sym}(t)$. Since $\mathrm{Soc}(\overline{G}) = \overline{S}^t$ has trivial centraliser in $\overline{G}$, it follows that $\mathrm{Soc}(H) = \overline{S}^u$ for some $u \leq t$, and H has a subnormal subgroup K such that $\overline{S}^u \leq K \leq \mathrm{Aut}(\overline{S})^u$ and $H/K \leq \mathrm{Sym}(u)$. By Proposition 2.1, $d(H/K) \leq t/2$, except when $t = 3$ and $H/K \cong \mathrm{S}_3$.

If $s = 2$ then $|\mathrm{Aut}(\overline{S})/\overline{S}| \leq 2$ by Lemma 2.10. So $H/\mathrm{Soc}(H) \leq 2 \wr \mathrm{Sym}(t) \leq \mathrm{S}_{2t}$, and $d(H/\mathrm{Soc}(H)) \leq t$ by Lemma 2.1. The result now follows by Lemma 2.7 if $t = 1$, by Lemma 2.8 if $t = 2$, and by Lemma 2.9 for $t \geq 3$. If $s = 3$ then the second part of Lemma 2.7 gives $d(K) \leq 2t$, so $d(H) \leq 5t/2$ (or 8 when $t = 3$), which is less than $2\log(\dim M_T)$. In general, $d(K) \leq 3t$ by Lemma 2.7, and hence $d(H) \leq 7t/2 = 7\log_s(\dim M_T)/2$ (or 11 when $t = 3$), which is less than $2\log(\dim M_T)$ for $s > 3$. □

4.2 The proof of Part 1 of Theorem 1.2

We begin with a sequence of lemmas concerning imprimitive matrix groups $G \leq \mathrm{GL}_f(F) \wr \mathrm{Sym}(n/f) < \mathrm{GL}_n(F)$ for small values of f. Note that the case $f = 1$ has already been dealt with in Proposition 3.2. In each case, let B be a minimal-dimensional block of imprimitivity for G, with $\dim B = f$, $b = n/f$, let $H = G^B_B$, so that H is primitive, let K be the kernel of the action of G on the block system, and let $Z = Z(\mathrm{GL}_f(F))$. We shall use the fact that G embeds into $H \wr \overline{G}$, where $\overline{G}$ is the induced permutation action of G on the block system. This follows, for example, from [13, p. 413, Hauptsatz 1.4]. In the following proofs we sometimes write C_k for the cyclic group of order k.

Lemma 4.3 *Let $G \leq \mathrm{GL}_n(F)$ be finite, irreducible, and imprimitive with minimal blocks of dimension 2, and assume that F does not contain a primitive fourth root of unity. Then $d(G) \leq n$, and if $|F| = 2$ then $d(G) \leq n/2$.*

Proof: Fix an imprimitive action of G on $b = n/2$ blocks. First assume that $|F| = 2$, so that $G \leq \mathrm{S}_3 \wr \mathrm{Sym}(b)$. Let $P \in \mathrm{Syl}_3(G)$. Then G has a permutation representation of degree $3b$, and so by applying Lemma 2.2 to the nontrivial orbits of P on the block system, we get $d_3(G) \leq b$, and $d_3(G) < b$ unless $P \leq K$. Let $S = P \cap K$. Then $S \lhd G$ and $G/S \leq C_2 \wr (G/K)$, so $d(G/S) \leq n/2$ by Proposition 2.1. Now Lemma 2.6 gives $d(G) \leq n/2$ unless $P \leq K$ and $d(P) = b$. In that case, we can generate G with generators of G modulo P together with a single generator of P, so we get the result unless $d(G/S) = n/2$. But by Proposition 2.1, this can happen only if $n \leq 4$ (in which case $n = 4$ and $G/S \cong D_8$, assuming $n > 2$), or $n = 8$ and $G/S \cong D_8 \circ D_8$. In either case, the generators of G modulo S have nontrivial centralisers in P, so we can multiply one of them by an element that it centralises in P to reduce the number of generators to $n/2$.

Suppose now that F has no primitive fourth root of unity. The possibilities for H/Z are listed in Lemma 2.10. Suppose first that H is not soluble. Then H has a subgroup H_1 of index at most 2, where $H_1 \cong S \times Z'$ with $S = \mathrm{SL}_2(q)$ for some $q \geq 4$, and Z' is a subgroup of Z of odd order and index at most 2 in Z. So K has a normal subgroup N isomorphic to $S^c \times Y$ for some $c \leq b$ and $Y \leq Z^b$, and $G/N \leq C_2 \wr \mathrm{Sym}(b) \leq \mathrm{S}_{2b}$. Thus $d(G/N) \leq b$ by Proposition 2.1. It follows from Lemma 2.8 ($c = 2$) and Lemma 2.9 ($c > 2$) that $d(\mathrm{SL}_2(q)^c) \leq c \leq b$. Since $d(Y) \leq b$, and Y and $\mathrm{SL}_2(q)^c$ have no common nontrivial quotients, Lemma 2.4 implies that $d(N) \leq b$, and hence $d(G) \leq 2b = n$.

When H is soluble, our strategy will be to prove that $d(P) < n$ or $d(P) \leq n$ for all Sylow p-subgroups P of G, and then to use Lemma 2.6 (once for each prime power layer of K) to extend $d(G/K) < n$ to $d(G) \leq n$.

If H/Z is cyclic or dihedral (including C_2^2) then, since H is primitive, H is semilinear, and either cyclic, or of shape $C_t.C_2$ for some t. If $p \neq 2$ then $d(P) \leq b < n$ by Proposition 3.2, so by Lemma 2.6 it suffices to show that $d(P) \leq n$ for $P \in \mathrm{Syl}_2(G)$. A Sylow 2-subgroup of H has a normal cyclic subgroup of index at most 2, so P has a normal subgroup Q which is abelian of rank at most b, and $P/Q \leq C_2 \wr \mathrm{Sym}(b) \leq \mathrm{S}_{2b}$. So $d(Q) \leq n/2$ and $d(P/Q) \leq n/2$ by Proposition 2.1, and hence $d(P) \leq n$.

When $H/Z \cong \mathrm{A}_4$ or S_4, a Sylow 2-subgroup of H is semidihedral of order 16 or quaternion of order 8 or 16, and therefore has structure $C_t.C_2$, as in the previous paragraph. Therefore $d(P) \leq n$ for $p = 2$, and $d(P) < n$ for all primes $p \neq 2$ except possibly $p = 3$

when 3 divides $|Z|$. So let $p = 3$, so that $P \leq (C_3 \times C_{3^k}) \wr \mathrm{Sym}(b)$ for some k, and let $Q = P \cap K$. If the projection of P onto $\mathrm{Sym}(b)$ is transitive, then two applications of Lemma 3.1 (one with $N = P \cap C_3^b$ and one with $N = P \cap C_{3^k}^b$) show that Q can be generated as a P-module by at most $b/3 + 2b/3 = b$ elements. More generally, if the projection of P onto $\mathrm{Sym}(b)$ has nontrivial orbits of total length $c > 1$, then by considering the image and kernel of this projection, we can show that Q can be generated as a P-module by at most $c + 2(b - c)$ elements. Since $P/Q \leq \mathrm{S}_c$, Proposition 2.1 (and the fact that $P \ncong \mathrm{S}_3$) gives $d(P) \leq 3c/2 + 2(b - c) < 2b = n$, and the result follows as before using Lemma 2.6.

It remains to deal with the case when P projects trivially onto $\mathrm{Sym}(b)$, and $d(P) = n$. We now regard G as an abstract subgroup of $X := (Z \circ \mathrm{S}_4) \wr \mathrm{Sym}(b)$. We use the same trick as in the proof of Proposition 3.2. The centre of X is the diagonal subgroup of the subgroup Z^b of its base group. We embed X in a group X' with $|X' : X| = 3$, where X' is the central product of X and a cyclic group of order $3|Z|$. Let Z_3 be a Sylow 3-subgroup of $Z(X')$. Then $PZ_3 \leq (C_3 \times C_{3^{k+1}})^b$ so $d(PZ_3) = n$. But Z_3 contains elements outside of the Frattini subgroup of PZ_3, so $d(PZ_3/Z_3) < n$. Hence $d(P/(P \cap Z(G))) < n$, and Lemma 2.6 implies that $d(G/Z(G)) \leq n$. Then, applying Lemma 2.6 again to the primes dividing $|Z(G)|$ gives $d(G) \leq n$. □

Recall H, B, K and Z, from the beginning of this subsection.

Lemma 4.4 *Let $G \leq \mathrm{GL}_n(F)$ be finite, irreducible, and either imprimitive with minimal blocks of dimension 3, or primitive with $n = 3$. Assume that F does not contain a primitive fourth root of unity. Then $d(G) \leq n$. In addition, if $n > 3$ and $|F| = 2$ then $d(G) \leq n/2$.*

Proof: Let $b = n/3$ be the number of blocks. We first prove the stronger result for $|F| = 2$, so $n > 3$ implies that $b > 1$. Then $H \leq 7{:}3$ or $H = \mathrm{L}_3(2)$. If $b = 2$ then the result can easily be checked computationally. If $b \geq 3$ then the result follows from Lemma 2.9 or 2.8 for $H = \mathrm{L}_3(2)$ and from Lemma 2.6 for $H \leq 7{:}3$.

Assume from now on that F contains no primitive fourth roots of unity. By checking the lists [12, 19] of almost simple groups that can arise, we can show that $d(S) \leq 2$ for all subnormal subgroups S of H when H/Z is almost simple, and the same applies when H is semilinear. In those cases we get $d(G) \leq n$ immediately.

Thus we assume that H is primitive, not semilinear, and not almost simple, so that $H/Z \leq 3^2.\mathrm{SL}_2(3)$ by Lemmas 2.14 and 2.16. Regard G as a subgroup of $X := (Z \circ (3^{1+2}.\mathrm{SL}_2(3))) \wr \mathrm{Sym}(b)$, and let N be the intersection of G with the subgroup $(Z \circ 3^{1+2})^b$ of the base group of the wreath product. Then $G/N \leq \mathrm{SL}_2(3) \wr \mathrm{Sym}(b)$, and since all subgroups of $\mathrm{SL}_2(3)$ are 2-generated, $d(G/N) \leq 2b + (b - 1) < n$.

We want to use Lemma 2.6 to show that $d(G) \leq n$. Let p be a prime and $P \in \mathrm{Syl}_p(G)$. If $p > 3$, then $d(P) < n$. Suppose that $p = 2$. Since F contains no primitive fourth roots of unity, a Sylow 2-subgroup of H is a subgroup of $Q_8 \times 2$, and so P satisfies $d(P) \leq d(P \cap (Q_8 \wr \mathrm{Sym}(b))) + d(C_2^b)$. As in the arguments for $H/Z \cong \mathrm{A}_4$ in the proof of Lemma 4.3 we get $d(P \cap (Q_8 \wr \mathrm{Sym}(b))) \leq 2b$, so $d(P) \leq 3b = n$.

It remains to deal with $P \in \mathrm{Syl}_3(G)$. A Sylow 3-subgroup Q of H is a central product of L and C_{3^k} for some k, where L has the structure 3^{1+2} or $3^{1+2}.3$. Now all subgroups of Q/C_{3^k} are 2-generated, and hence all subgroups of Q are 3-generated. Let ρ be the

projection of G onto $\mathrm{Sym}(b)$; so $K = \ker(\rho)$. Then P embeds into $Q \wr \rho(P)$, where Q has a normal series of length 4 with cyclic factors, at least 3 of which are of order 3. If $\rho(P)$ has an orbit O of length 3^m for some $m \geq 1$ then it follows from Lemma 3.1 that we can generate the restriction of $P \cap K$ to O, as a normal subgroup of P by at most $5 \cdot 3^{m-1}$ elements, and hence generate the restriction of P to O by at most $2 \cdot 3^m$ elements by Lemma 2.2. On the other hand, a projection of $P \cap K$ onto a factor of the base group that is fixed by $\rho(P)$ could require up to 3 generators. Arguing in this way, we find that $d(P) < n$ except possibly when P has trivial image in $\mathrm{Sym}(b)$, so that $P \leq K$. In this instance, $P \leq (L \circ C_{3^k})^b$, and we proceed exactly as in the final paragraph of the proof of Lemma 4.3 to deduce that $d(G) \leq n$. □

Recall H, B, K and Z, from the beginning of this subsection.

Lemma 4.5 *Let $G \leq \mathrm{GL}_n(F)$ be finite, irreducible, and either imprimitive with minimal blocks of dimension 4, or primitive in dimension 4. Assume that F does not contain a primitive fourth root of unity, and that Part 1 of Theorem 1.2 holds in dimension less than n. Then $d(G) \leq n$. In addition, if $|F| = 2$ then $d(G) \leq n/2$.*

Proof: We first prove the stronger result when $|F| = 2$. We can show (by using the database of irreducible groups in MAGMA, for example) that either (i) H is a primitive subgroup of 15:4; or (ii) $H = (3 \times \mathrm{L}_2(4))$ or $(3 \times \mathrm{L}_2(4)).2$; or (iii) $S \trianglelefteq H \leq S.2$ with S simple. Case (i) is straightforward, using up to three applications of Lemma 2.6. In Case (ii), there is a normal subgroup N of G contained in K with $N \cong 3^{c_1} \times \mathrm{L}_2(4)^{c_2}$ for $c_1, c_2 \leq b$, and $G/N \leq 2 \wr \mathrm{Sym}(b)$. The case $b = 1$ is easy, and for $b > 1$ Lemmas 2.9 and 2.4 give $d(N) \leq b$, and Proposition 2.1 gives $d(G/N) \leq b$, so $d(G) \leq 2b$ as required. The proof for Case (iii) is similar.

We assume from now on that F contains no primitive fourth root of 1. The lists [12, 19] of almost simple groups that can arise show that $d(S/Z) \leq 2$ for all subnormal subgroups S of H when H/Z is almost simple. So, if H/Z is almost simple, then $d(S) \leq 3$, and $d(G) \leq n$. So assume that H/Z is not almost simple.

Suppose first that H is semilinear of degree f. If $f = 4$ then H is metacyclic, which we can handle easily, so assume that $H \leq \mathrm{GL}_2(E).2$ for some field E with $|E : F| = 2$. Let $H_1 = H \cap \mathrm{GL}_2(E)$ and $Z_1 = H_1 \cap Z(\mathrm{GL}_2(E))$. Since we are assuming that H/Z is not almost simple, H_1/Z_1 is cyclic, dihedral, or isomorphic to A_4 or S_4 by Lemma 2.10. We reduce as in Lemma 4.3 to showing that $d(P) \leq n$ for $P \in \mathrm{Syl}_2(G)$. Let $Q \in \mathrm{Syl}_2(H)$. Then Q (and hence also all subnormal subgroups of Q) has a normal series of length at most 4, with all factors cyclic, and at most two factors having order greater than 2. Using similar arguments as in the previous lemmas, for a nontrivial orbit of P on the blocks, we apply Lemma 3.1 up to four times to the cyclic sections of H, where $k = 1$ in Lemma 3.1 for the cyclic sections of order 2. This gives $d(\overline{P}) \leq 7\overline{n}/8$ for the induced action of $\overline{P}$ of P on the subspace of dimension $\overline{n}$ corresponding to this nontrivial orbit. On the other hand, a subnormal subgroup of P acting trivially on a block requires at most 4 generators for its action on this block, so we get $d(P) \leq n$ as required.

So we may assume that H is not semilinear, so that in particular H has no nonscalar abelian characteristic subgroups. Now Lemma 2.16 applies to H: let L be the generalised Fitting subgroup of $H \leq \mathrm{GL}_4(F)$. We have already considered quasisimple L.

If L is an extraspecial p-group then $p = 2$ and $H/Z \leq 2^4.S$ for some $S \leq \mathrm{GO}_4^{\pm}(2)$, since F contains no primitive fourth root of 1. All Sylow subgroups of $\mathrm{GO}_4^{\pm}(2)$ are 2-generated, so we reduce to showing that $d(P) \leq n$ for $P \in \mathrm{Syl}_2(G)$. The Sylow 2-subgroups of $\mathrm{GO}_4^+(2)$ and $\mathrm{GO}_4^-(2)$ are both isomorphic to D_8, and $Q \in \mathrm{Syl}_2(H)$ is a subgroup of a group of shape $2^{1+4}.D_8$. The action of $D_8 \leq \mathrm{GO}_4^{\pm}(2)$ on 2^4 stabilises a one-dimensional submodule, and hence Q has a nonscalar abelian normal subgroup. Since 2^{1+4} is absolutely irreducible and not semilinear, so is Q, and so the action of Q is imprimitive. Since Q is imprimitive, P is not primitive, so P is either imprimitive with block size 1 or 2 or reducible. Furthermore, if P is reducible then P is completely reducible, since $\mathrm{char}F \neq 2$. If P is imprimitive with block size 1 then the result follows from Proposition 3.2, and if P is imprimitive with block size 2 then the result follows from Lemma 4.3. If P is reducible then, since we are assuming that Part 1 of Theorem 1.2 holds in dimensions less than n, we can apply it to the action of P on an irreducible constituent and to the kernel of this action on the remaining consitutents to get $d(P) \leq n$ as required.

Otherwise L is a tensor product of two two-dimensional groups, which are both primitive and not semilinear. Thus H is a subgroup of $H_1 \otimes H_2$ or $H_1 \wr \mathrm{Sym}(2)$, where $H_1, H_2 \leq \mathrm{GL}_2(F)$. Consulting Lemma 2.10, either $\mathrm{L}_2(q) \leq H_i/(H_i \cap Z) \leq \mathrm{PGL}_2(q)$ for some q, or $\mathrm{A}_4 \leq H_i/(H_i \cap Z) \leq \mathrm{S}_4$. If $H_i/(H_i \cap Z) \leq \mathrm{S}_4$ for $i = 1, 2$, then $H/Z \leq 2^4.S$, which we dealt with in the preceding paragraph, and otherwise it is routine to show that all subnormal subgroups of H are 3-generated. □

Proof of Theorem 1.2, Part 1: If $\mathrm{Char}F = p$ and $O_p(G) = 1$, then G embeds into the direct sum of its actions on its irreducible constituents, and its image under this embedding is completely reducible. So we may assume that G is completely reducible and by Clifford's theorem we immediately reduce to the case when G is irreducible, except when $|F| = 2$ and G has irreducible constituents of dimensions 2 or 3. In these exceptional cases G is a subdirect product of $H \times K$, where $H \leq \mathrm{GL}_t(2)$ with $t = 2$ or 3, and $K \leq \mathrm{GL}_{n-t}(2)$. By Lemma 2.12, we reduce to $H \cong \mathrm{S}_3$ with $t = 2$, or $H \cong 7{:}3$ or $\mathrm{L}_3(2)$ with $t = 3$. In each of these cases, by Lemma 2.4, if $G = H \times K$, then $d(G) \leq d(K) + 1$. Furthermore, if G is a proper subdirect product of $H \times K$, then either $G \cong K$ or the kernel of the projection of G onto K is cyclic, so again $d(G) \leq d(K) + 1$.

Suppose first that $H \cong \mathrm{S}_3$. If $d(K) \leq \lfloor (n-2)/2 \rfloor$ then $d(G) \leq \lfloor (n-2)/2 \rfloor + 1 = \lfloor n/2 \rfloor$, and the result follows, so assume that $K \in \{B_{n-2}, 7{:}3, \mathrm{L}_3(2)\}$. In each case, if G is equal to the full direct product, then in fact $d(G) = d(K) = \lfloor n/2 \rfloor$. Thus we assume that G is a proper subdirect product, so $K \cong B_{n-2}$. If $G \cong K$ then $d(G) = d(K)$. Otherwise, the kernel of the projection of G onto K has order 3, so $G \cong 3^{n/2}{:}2 = B_n$ and $d(G) = n/2 + 1$.

Otherwise $H \leq \mathrm{GL}_3(2)$, and $d(K) \leq \lfloor (n-1)/2 \rfloor$, with strict inequality unless $K \in \{B_{n-3}, 7{:}3, \mathrm{L}_3(2)\}$. Furthermore, $d(G) \leq d(K) + 1$, with $d(G) = d(K)$ if $K = B_{n-3}$ by Lemma 2.4. Therefore $d(G) \leq n/2$, as required.

Thus we may now assume that G is irreducible. If G is imprimitive, then we choose a block system preserved by G such that the dimension f of the blocks is minimal, and let $b > 1$ be the number of blocks. Let B be a block, let $H = G_B^B$, and let K be the kernel of the action of G on the block system. If H is reducible then so is G, contrary to assumption. The minimality of f implies that H is primitive and hence weakly quasiprimitive. If G is

primitive then let $H = K = G$, $b = 1$, $n = f$.

Suppose that $f = 1$. If $|F| = 2$, then H is trivial and G is reducible, a contradiction. Otherwise, H is cyclic. If F contains no fourth root of 1, then $t := |H|$ is not divisible by 4, and the result follows from Proposition 3.2. So we assume from now on that $f > 1$.

The action of K on each individual block is isomorphic to a normal subgroup of H, and so K has a descending normal series of length b in which the factors are isomorphic to subnormal subgroups of H.

Since H is weakly quasiprimitive, each of the b factors K_i of the descending normal series of K satisfies $d(K_i) \leq 2\log f + 1$ and $d(K_i) \leq 2\log f$ if $|F| = 2$, by Theorem 1.2 (2).

Hence, by Proposition 2.1, $d(G) \leq n(2\log f + 3/2)/f$ and $d(G) \leq n(2\log f + 1/2)/f$ if $|F| = 2$, except that we need to add $1/2$ to these estimates when $b = 3$ and $G/K \cong \mathrm{S}_3$. The bound for $|F| = 2$ is at most $n/2$ for $f \geq 18$ and the general bound is less than n for $f \geq 8$, including when $b = 3$ in both cases.

We deal first with the smaller values of f when $|F| = 2$. If $f = 2$, 3 or 4, then the result follows from Lemma 4.3, Lemma 4.4, or Lemma 4.5. The only primitive subgroups of $\mathrm{GL}_5(2)$ are of shape 31, $31 : 5$, or $\mathrm{L}_5(2)$, and we easily get $d(K) \leq 5$ and hence $d(G) \leq 7 < n/2$ when $f = 5$, $b = 3$ and $G/K \cong \mathrm{S}_3$. If $f \geq 7$, or $f = 5$ and $G/K \ncong \mathrm{S}_3$ then we get the result from the second statement of Part 2.

Suppose, therefore, that $f = 6$. If all subnormal subgroups of H are 2-generated, then we get $d(G) \leq n/2$ immediately. We can check in MAGMA that if L is a subnormal subgroup of a primitive subgroup of $\mathrm{GL}_6(2)$ then $d(L) \leq 3$, and that all candidates for H with subnormal subgroups that are not 2-generated are subgroups of $3^{1+2}.\mathrm{GL}_2(3) \cong 3^{1+2}.Q_8.D_6$ that contain 3^{1+2}. It is easily checked that all subgroups of $\mathrm{GL}_2(3)$ are 2-generated so, by applying Lemma 2.6 with $S = O_3(K)$, it is sufficient to check that $P \in \mathrm{Syl}_3(G)$ satisfies $d(P) < n/2$. If $|H|$ is not divisible by 81, then since all subgroups of 3^{1+2} are 2-generated, $d(P \cap K) \leq 2b = n/3$. Lemma 2.2 gives that $d(PK/K) \leq b/3 < b/2 = n/12$, and hence $d(P) < n/2$ as required. If, on the other hand, $|H|$ is divisible by 81, then $H \cong 3^{1+2}.\mathrm{SL}_2(3)$ or $H \cong 3^{1+2}.\mathrm{GL}_2(3)$. These groups do have 3-generated 3-subgroups, but none of these is the Sylow 3-subgroup of a subnormal subgroup of H. Hence again $d(P \cap K) \leq n/3$ and the result follows.

We now deal with the cases where F does not contain a primitive fourth root of 1 and $2 \leq f \leq 7$. The case $f = 2$ is covered by Corollary 2.11 and Lemma 4.3. The cases $f = 3$ and $f = 4$ follow from Lemmas 4.4 and 4.5, respectively, so assume that $f \in \{5, 6, 7\}$. The fact that all almost simple groups are 3-generated settles the cases when H/Z is almost simple. The semilinear case is straightforward when $f = 5$ or 7, and it can be verified that all subgroups of $5^2{:}\mathrm{SL}_2(5)$ and $7^2{:}\mathrm{SL}_2(7)$ are 3-generated, so in the normaliser of extraspecial group cases H is 4-generated and $d(G) \leq n$.

So suppose $f = 6$. The semilinear cases with field extensions of degree 6 and 3 are easy. For an extension field E of F, completely reducible subgroups of $\mathrm{GL}_3(E)$ are 4-generated by Proposition 2.3, and hence subgroups of $\mathrm{GL}_3(E).2$ are 5-generated, which deals with the final semilinear case. The remaining possibility is that H is a central product of primitive subgroups of $\mathrm{GL}_2(F)$ and $\mathrm{GL}_3(F)$. Since (from the case $f = 2$ and 3) these are 2- and 3-generated respectively, the result follows in this case too. □

5 The proof of Theorem 1.3

Before proceeding to this proof we need a few more lemmas.

Lemma 5.1 *Let $G \leq \mathrm{Sp}_{2m}(q)$ be completely reducible, let N be the natural G-module, and let $M = C_N(G)$. Then M is nondegenerate under the symplectic form.*

PROOF: Let $x \in M$. Then G stabilises both $\langle x \rangle$ and $\langle x \rangle^\perp$, so stabilises $N/(\langle x \rangle^\perp) = \langle y \rangle$. Since G is completely reducible, $\langle y \rangle$ is a G-submodule. If $g \in G$ and $yg = \lambda y$ then $(x, y) = (xg, yg) = \lambda(x, y)$, so $\lambda = 1$ and $y \in M$. Thus M is nondegenerate. □

Lemma 5.2 *Let N be the natural module for a completely reducible subgroup G of $\mathrm{Sp}_{2m}(q)$ and let M be an irreducible submodule of N. Then either*
(i) $N = M \oplus L$ with $G/C_G(M)$ naturally isomorphic to a subgroup of $\mathrm{Sp}(M)$ and $G/C_G(L)$ naturally isomorphic to a subgroup of $\mathrm{Sp}(L)$; or
(ii) there is an irreducible submodule M' of N with $N = M \oplus M' \oplus L$, $C_G(M) = C_G(M')$, $G/C_G(M) \leq \mathrm{GL}(M)$ and $G/C_G(L) \leq \mathrm{Sp}(L)$.

PROOF: Since M is an irreducible G-module, the restriction to M of the symplectic form preserved by G is either nondegenerate or totally singular.

If M is nondegenerate, then $N = M \oplus L$, where $L = M^\perp$ is also nondegenerate, and $G \leq H := \mathrm{Sp}(M) \times \mathrm{Sp}(L) \leq \mathrm{Sp}_{2m}(q)$. Hence $C_H(M) = \mathrm{Sp}(L)$ and $C_H(L) = \mathrm{Sp}(M)$.

If M is totally singular, then by [15, Lemma 4.1.12] there exist spaces M' and L such that M' is totally singular, $M \oplus M'$ is nondegenerate, and $(M \oplus M')^\perp = L$. Thus L is nondegenerate Also by [15, Lemma 4.1.12], $G \leq H := \mathrm{GL}(M) \times \mathrm{Sp}(L) \leq \mathrm{Sp}_{2m}(q)$. Hence, $C_H(M) = C_H(M') = \mathrm{Sp}(L)$ and $C_H(L) = \mathrm{GL}(M)$. □

Lemma 5.3 *Let N be the natural module for a subgroup G of $\mathrm{Sp}_{2m}(2)$ with $m > 1$, and suppose that $M := C_N(G)$ has dimension at most 2. Then N can be generated as a G-module by at most m elements.*

PROOF: The assumption $\dim M \leq 2$ implies that $\mathrm{Soc}(N)$ has at most two one-dimensional constituents. Since G preserves a symplectic form, N is self-dual, and so $\mathrm{Soc}(N) \cong N/\mathrm{Rad}(N)$, and $N/\mathrm{Rad}(N)$ has at most two one-dimensional constituents. The number of generators of N as a G-module is equal to the number of generators of $N/\mathrm{Rad}(N)$, which is at most the number of its irreducible constituents. But if $N/\mathrm{Rad}(N)$ has a one-dimensional and also a higher dimensional constituent, then we can replace the generators from these two constituents by their sum, and the result now follows since $m > 1$. □

The estimates related to $O_2(G)$ in Theorem 1.3 will be derived from the following.

Lemma 5.4 *Let X be of shape $N.H \leq 2^{2m}.\mathrm{Sp}_{2m}(2)$, with $N \trianglelefteq X$ elementary abelian of order 2^{2m} and H a completely reducible subgroup of $\mathrm{Sp}_{2m}(2)$, and assume that $|Z(X)| \leq 4$. Then $d(X) \leq \lceil (2 \log_3 2)\, m \rceil$.*

PROOF: The assumptions imply that $Z(X) \leq N$. The proof is by induction on m. If $m = 1$ then $X \leq \mathrm{Sym}(4)$ and $d(X) = 2 = \lceil (2 \log_3 2)\, m \rceil$. So assume that $m > 1$.

Let M be a minimal normal subgroup of X with $M \leq N$ and $|M|$ maximal. Now $m > 1$ and $|Z(X)| \leq 4$, so $\dim M > 1$. Let $K = C_H(M)$. Then by Lemma 5.2 either (i) $N = M \times L$ with $\dim M = 2k$, $L \lhd X$, $H/K \leq \mathrm{Sp}_{2k}(2)$; or (ii) $N = M \times M' \times L$ with $M', L \lhd X$, $\dim M = \dim M' = k$, $K = C_H(M')$, and $H/K \leq \mathrm{GL}_k(2)$. In both cases $\dim L = 2(m-k)$, and if $k < m$ then K acts faithfully and completely reducibly as a subgroup of $\mathrm{Sp}_{2(m-k)}(2)$ on L.

Suppose first that $\dim M > 2$. Then, since M is an irreducible module for H/K and all irreducible subgroups of $\mathrm{GL}_3(2)$ are 2-generated, Theorem 1.2 Part 1 gives $d(H/K) \leq k$ in Case (i) and $d(H/K) \leq \lceil k/2 \rceil$ in Case (ii). In Case (i), Lemma 2.5 then gives $d(M.(H/K)) \leq k$, whereas in Case (ii) it gives $d(M.(H/K)) \leq \lceil k/2 \rceil$ and so $d((M \times M').(H/K)) \leq \lceil k/2 \rceil + 1 \leq k$. The result now follows if $k = m$. If $k < m$ then we can write $L = L_1 \times L_2 \times L_3$ with each $L_i \trianglelefteq H$, where $L_1 \times L_2$ and L_2 are generated by the 1-dimensional constituents of L under the actions of K and H respectively. By Lemma 5.1, L_2 and $L_1 \times L_2$ are both non-degenerate under the symplectic form preserved by H and hence so are L_1 and $L_1^{\perp} = L_2 \times L_3$. Thus, if $|L_1| = 2^{2t}$, then $L_2 L_3.K \leq 2^{2(m-k-t)}.\mathrm{Sp}_{2(m-k-t)}(2)$, and $L_2 L_3.K$ satisfies the hypotheses of the lemma. Hence, by the inductive hypothesis, $d(L_2 L_3.K) \leq \lceil (2 \log_3 2)\,(m-k-t) \rceil$. Since L_1 can be generated as an H-module by at most t elements, $d(X) \leq k + d(L_2 L_3.K) + t$, as required.

So we have reduced to the case where the irreducible H-constituents of N have dimension at most 2, and there are at most two of dimension 1. But then X satisfies the hypotheses of Lemma 3.4, and the result follows. □

The estimates for $O_p(G)$ for p odd in Theorem 1.3 will be derived from the following.

Lemma 5.5 *Let X be of shape $N.H \leq p^{2m}.\mathrm{Sp}_{2m}(p)$, with p an odd prime, $N \trianglelefteq X$ elementary abelian of order p^{2m}, and H a completely reducible subgroup of $\mathrm{Sp}_{2m}(p)$. Then $d(X) \leq \lfloor (2 \log_3 p)\, m \rfloor$, except that $d(X) \leq \lfloor (2 \log_3 p)\, m \rfloor + 1$ when $|H| = 2$ and either: $p = 3$ and $Z(X) = 1$; or $p = 5$ and $m = 1$.*

PROOF: The proof is by induction on m. Suppose first that all irreducible H-submodules of N have dimension 1. Then $H \leq (p-1)^{2m}$, so $d(H) \leq 2m$ and $d_p(X) = 2m$. Now Lemma 2.6 gives $d(X) \leq 2m + 1 \leq \lfloor (2 \log_3 p)\, m \rfloor + 1$, and $d(X) \leq \lfloor (2 \log_3 p)\, m \rfloor$ except when $p = 3$ or when $p = 5$ and $m = 1$. When $p = 3$ the result follows from Lemma 3.3, and it is easily checked when $p = 5$ and $m = 1$.

Otherwise, let M be a minimal normal subgroup of X with $M \leq N$ and $|M|$ maximal. Then $\dim M > 1$, since at least one irreducible H-submodule of N has dimension greater than 1. Let $K = C_H(M)$. Then by Lemma 5.2 either (i) $N = M \times L$ with $\dim M = 2k$, $L \lhd X$, $H/K \leq \mathrm{Sp}_{2k}(p)$; or (ii) $N = M \times M' \times L$ with $M', L \lhd X$, $\dim M = \dim M' = k$, $K = C_H(M')$, and $H/K \leq \mathrm{GL}_k(p)$. In both cases $\dim L = 2(m-k)$, and if $k < m$ then K acts faithfully and completely reducibly as a subgroup of $\mathrm{Sp}_{2(m-k)}(p)$ on L.

Suppose that $p \equiv 3 \bmod 4$. In Case (i), Theorem 1.2.1 gives $d(H/K) \leq 2k$, and then Lemma 2.5 gives $d(M.(H/K)) \leq 2k$, and in Case (ii), Theorem 1.2.1 gives $d(H/K) \leq k$, and Lemma 2.5 gives $d((M \times M').(H/K)) \leq k + 1$. The result now follows by applying the inductive hypothesis to $L.K$ except in Case (i) when $p = 3$, $d(L.K) = 2(m-k) + 1$

and $|K| = 2$, when we get $d(X) \leq 2m + 1$. In that situation, we can choose $2k$ of the generators to be inverse images in X of generators of $M.(H/K)$, a further $2(m-k)$ to generate L and one, x_K say, of order 2 that maps onto a generator of K. Note that K is central in H and $C_X(x_K)$ is a complement of L in X. We choose the inverse image x of one of the generators of $M.(H/K)$ to be the product of an element in $C_X(K)$ with an element y of order 3 in L. Then $[x, x_K] = y^{-1}$, and so one of our generators in L is redundant, and $d(X) \leq 2m$ as required.

Suppose then that $p \equiv 1 \bmod 4$. In Case (ii), we get $d(H/K) \leq 3k/2$ from Proposition 2.3 and then, by Lemma 2.5, $d((M \times M').(H/K)) \leq 3k/2+1 \leq 2k$. The result follows immediately if $k = m$, and by applying the inductive hypothesis to $d(L.K)$ otherwise.

In Case (i), if $k < m$ then we get the result by applying the inductive hypothesis to $d(M.(H/K))$ and $d(L.K)$, and dealing with the case when $p = 5$ and $m - k = 1$ in a similar way to the exceptional case for $p = 3$: note that if $k = 1$ and $p = 5$ then the irreducibility of M implies that we are not in the exceptional case.

Suppose finally that we are in Case (i) and L is trivial; that is, H acts irreducibly on N. By Lemma 2.5, $d(X) \leq d(H)$, so it is enough to prove that $d(H) \leq \lfloor (2 \log_3 p)\, m \rfloor$. If the action of H on N is primitive then put $B = N$, $K = S = H$ and $f = 2m$. Otherwise, let $B < N$, with $\dim B = f$, be a minimal block of imprimitivity under the action of H, let S be the stabiliser in H of B, and let K be the stabiliser of the block system. So S acts irreducibly and primitively on B, and B must either be totally singular or non-degenerate under the symplectic form preserved by H. If B is totally singular, then all subspaces of N preserved by K are totally singular, and Lemma 5.2 together with Proposition 2.3 give $d(K) \leq 3m/2$. Now Proposition 2.1 applied to $H/K \leq \mathrm{S}_{2m/f}$ gives $d(H/K) \leq m$, so $d(H) \leq 5m/2 \leq \lfloor (2 \log_3 p)\, m \rfloor$, as required.

If B is non-degenerate, then S^B is symplectic and primitive with $K^B \trianglelefteq S^B$. So we can apply Part 2 of Theorem 1.2 to the action of K on the blocks of imprimitivity and conclude that $d(K) \leq (2 \log f + 1)2m/f$. Then applying Proposition 2.1 to $H/K \leq \mathrm{S}_{2m/f}$ gives $d(H) \leq (2 \log f + 3/2)2m/f$ (but replace the 3/2 by 5/3 when $2m/f = 3$). This proves the result except when $f = 2$ and $p = 5$. But all subgroups of $\mathrm{Sp}_2(5) = \mathrm{SL}_2(5)$ are 2-generated, so we get $d(K) \leq 2m$ in that case, and the result follows. □

For a normal subgroup N of G, we define $d_G(N)$ to be the smallest k such that there exist k elements of N with the property that they, together with any set of elements of G that generate G modulo N, generate G. (This is not a standard definition, and is not the same usage as in [17], as used in the proof of Lemma 3.1.) Then $d(G) \leq d(G/N) + d_G(N)$. If $K \trianglelefteq N \trianglelefteq G$ with $K \trianglelefteq G$, then we write $d_G(N/K)$ for $d_{G/K}(N/K)$.

Proof of Theorem 1.3: The proof has the same general structure as that of Part 2 of Theorem 1.2. But since we are proving a tighter bound, we have to work harder.

We may assume that G is irreducible. If G has a noncentral abelian characteristic subgroup then we define K and f as in Lemma 2.13, and otherwise we put $G = K$ and $f = 1$. Then $n = fn'$ for some n', where $K \leq \mathrm{GL}_{n'}(F')$, $Z(K)$ is cyclic, and F' is a degree f extension of F. So

$$d(G) \leq d(G/K) + 1 + d_G(K/Z(K)) \leq \log f + 1 + d_G(K/Z(K)).$$

Let L be the generalised Fitting subgroup of K, and let r_i, T_i and S_i be as in Lemma 2.14. It suffices to prove that $d_G(K/Z(K)) \leq \lceil (2\log_3 2)\log n' \rceil$, which we shall do, as in Theorem 1.2, by estimating the contributions to $d_G(K/Z(K))$ coming from the central factors $O_{r_i}(K)$ and T_i of L.

More precisely, let the central factors of L be $L_1, \ldots, L_k$, where the factors $O_{r_i}(K)$ in order of increasing r_i come first, and let $M_0 = 1$ and $M_i = L_1 \cdots L_i$ for $1 \leq i \leq k$. We derive upper bounds for $d_G(C_K(M_{i-1})/C_K(M_i))$ for $1 \leq i \leq k$ and sum them to get an upper bound for $d_G(K/Z(K))$.

In the estimates for these individual contributions, we call examples in which the floor of the expression involved in the upper bound is exceeded by 1 *adverse ceiling* examples. If we combine two adverse ceiling examples coming from different components of L, then we need to reduce the size of their combined set of generators by 1 in order to avoid exceeding the bound for $d_G(K)$. We shall complete the proof by considering such cases.

$\mathbf{O_2(K)}$ Suppose that $A := O_2(K)$ is nonscalar. Then by Lemmas 2.14 and 2.16 A is the central product of an extraspecial group E of order 2^{2m+1} for some $m > 0$, and the cyclic group $Z(A)$. So $N := A/Z(A)$ is elementary abelian of order 2^{2m}, and the conjugation action of G on N preserves a symplectic form, in which the restriction to K acts completely reducibly. We need to prove that $d_G(K/C_K(A)) \leq \lceil (2\log_3 2)\, m \rceil$.

Let M' and M be the fixed subspaces of the actions of G and K on N; so $M' \leq M \leq N$. We claim that $|M'| \leq 4$. To see this, let I be the inverse image of M' in A. If $|M'| > 4$ then $d(I) \geq 3$, so by [10, Chapter 5, Theorem 4.10] I has a noncyclic abelian subgroup S. We may assume that $Z(A) < S$, then $[S, G] \leq Z(A)$ implies $S \trianglelefteq G$. But a faithful representation of a noncyclic abelian group cannot be homogeneous, so this contradicts the quasiprimitivity of G and proves the claim.

Since the action of K on N is completely reducible, by Lemma 5.1 M is nondegenerate under the symplectic form preserved by G, and its complement $M^\perp$ in N is also nondegenerate. Now the induced conjugation action of G on M has fixed space M' of dimension at most 2 and hence, by Lemma 5.3, if $\dim M > 2$ then M is generated by at most $(\dim M)/2$ elements as a G-module.

Now $AC_K(A)/C_K(A)$ is isomorphic to N as a G-module under the conjugation action, and $K/C_K(A) \cong N.H$, where H is a completely reducible subgroup of $\mathrm{Sp}_{2m}(2)$, with fixed subspace G-isomorphic to M. If $\dim M > 2$, then $d_G(K/C_K(A)) \leq (\dim M)/2 + d(M^\perp.H)$. Hence the required bound $d_G(K/C_K(A)) \leq \lceil (2\log_3 2)\, m \rceil$ follows by applying Lemma 5.4 to $N.H$ if $\dim M \leq 2$, and to $M^\perp.H$ if $\dim M > 2$.

$\mathbf{O_p(K)}$ for odd p Recall from Lemma 2.14 that, for odd primes p, $B := O_p(K)$ is a central product of its intersection with $Z(K)$ and an extraspecial group of exponent p. Since G is quasiprimitive, it has no noncyclic normal abelian subgroups, and it follows that $BZ(K)/Z(K)$ has no nontrivial cyclic subgroups that are normal in $G/Z(K)$.

Lemma 5.5 provides the estimates required for proof of Theorem 1.3 except when $|H| = 2$ and either $p = 3$ and $Z(X) = 1$, or $p = 5$ and $m = 1$, when we need to reduce the number of generators by 1.

In the proof of Theorem 1.3, if we apply Lemma 5.5 for $p = 3$ then, as explained earlier, we actually apply it with $X = K/C_K(B)$ if $O_2(K)$ is scalar or, if $O_2(K)$ is nonscalar, with $X = C_K(O_2(K))C_K(B)/C_K(B)$. In the case when $d(X) = d(N.H) = \lfloor (2\log_3 p)\, m \rfloor + 1$,

the $2m+1$ generators of X consist of $2m$ generators of N and one of H. The fact that $B/Z(K)$ has no nontrivial cyclic subgroups that are normal in $G/Z(K)$ means that under the action of G we may reduce the number of generators that lie in N and hence $d_G(X) \leq \lfloor (2\log_3 p)\, m \rfloor$, which is what we need for the proof of Theorem 1.3. We handle the exceptional case when $p = 5$ similarly.

Insoluble factors of L Next consider $\overline{G} = G/C_G(T)$, with T a central product of t copies of a quasisimple group S. By Lemma 2.17, $\overline{G} \leq A \wr \mathrm{Sym}(t)$, where A is the subgroup of $\mathrm{Aut}(\overline{S})$ that stabilises the module M_S. The bound that we require for $d(G/C_G(T))$ then follows from Lemma 3.7.

Adverse ceiling combinations In Lemma 3.7 the only adverse ceiling examples are of dimension 2. We verify that, for any prime powers q_1, q_2, any subgroup of $\mathrm{PGL}_2(q_1) \times \mathrm{PGL}_2(q_2)$ that contains $\mathrm{L}_2(q_1) \times \mathrm{L}_2(q_2)$ is 2-generated, which deals with the case when two such instances arise in G.

The other possibility is that there is one such instance of $\mathrm{L}_2(q)$ or $\mathrm{PGL}_2(q)$ in dimension 2, together with $d_G(K/C_K(O_2(K))) > \lfloor (2\log_3 2)\, m \rfloor$, where $|O_2(K)/Z(O_2(K))| = 2^{2m}$. In that case, we choose an inverse image of one of our generators of $K/C_G(O_2(K))$ such that either it or its square projects onto an element of order $(q-1)/2$ in $\mathrm{L}_2(q)$, and then we need just one additional generator from $\mathrm{L}_2(q)$ or $\mathrm{PGL}_2(q)$. □

6 The proof of Theorem 1.1

For this proof we assume that the reader is familiar with the O'Nan–Scott Theorem (see, for example, [9, Theorem 4.1A]).

Proof of Theorem 1.1: If G is of affine type, then this is Proposition 4.1.

If G is almost simple then $n \geq 5$. From Lemma 2.7, we get $d(G) \leq 3$ in general, and the classification of primitive groups of small degree [9, Appendix B] yields $d(G) = 2$ for $n < 8$. The same clearly applies to any subnormal subgroup H of G, so the result follows.

Otherwise, for some $e > 1$, there exists a nonabelian simple group S with $S^e \leq G \leq \mathrm{Aut}(S) \wr \mathrm{Sym}(e)$ (up to isomorphism). Let $N = G \cap \mathrm{Aut}(S)^e$. Then G/N is isomorphic to a subgroup of S_e and by Proposition 2.1 $d(G/N) \leq e/2$ unless $e = 3$ and $G/N \cong \mathrm{S}_3$. So by Lemma 2.7, $d(G) \leq 7e/2$, unless $e = 3$ when $d(G) \leq 11$, and the same applies to any subnormal subgroup H of G.

If G is of diagonal type or twisted wreath product type, then $n = |S|^{e-1}$ or $|S|^e$, respectively, and hence $\log n \geq (e-1)\log|S|$. The smallest values of $|S|$ are 60 and 168. Therefore $d(H) \leq \log n$, except possibly when $|S| = 60$ and $e = 2$, but in that case $d(\mathrm{Aut}(S)) = 2$, so $d(H) \leq 5$.

If G is of product action type then $e = e_1 e_2$ with $e_2 > 1$, and $n = f^{e_2}$ for some f. Furthermore, there exists a primitive group K of degree f, with socle S^{e_1}, such that $G \leq K \wr \mathrm{Sym}(e_2)$ with the product action. The group K is of diagonal type if $e_1 > 1$ and is almost simple if $e_1 = 1$.

If K is of diagonal type then $f = |S|^{e_1 - 1}$ so $\log n = (e_1 - 1)e_2 \log|S|$. This is larger than $7e/2$ except when $|S| = 60$ and $e_1 = 2$, but in that case $d(H) \leq 5e/2$.

If K is almost simple, then $n = f^e$ and $f \geq 5$. If $f > 12$ then $\log n \geq 7e/2$ (or 11 when $e = 3$). From the lists of primitive groups of small degree in [9, Appendix B], we find that all almost simple groups with primitive permutation representations of degree at most 12 have outer automorphism groups with at most two generators, so if $f \leq 12$ then $d(H) \leq 5e/2$ (or 8 when $e = 3$), and the result follows except when $f = 5$, or $f = 6$ and $e = 3$. If $f = 5$ or 6, then $G/\mathrm{Soc}(G) \leq 2 \wr \mathrm{Sym}(e)$, so $d(G/\mathrm{Soc}(G)) \leq e$ by Proposition 2.1, whereas $d(\mathrm{Soc}(G)) \leq 2 + \lceil \log_{60} e \rceil$ by Lemma 2.9. So $d(G) \leq 2 + e + \lceil \log_{60} e \rceil$, and the same bound holds for $d(H)$. The result follows except when $e = 2$ and $f = 5$, but $d(\mathrm{A}_5^2) = 2$, so we are done. □

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] Aschbacher, M.; Guralnick, R. Some applications of the first cohomology group. *J. Algebra* **90** (1984) 446–460.

[4] Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997) 235–265.

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

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

[7] Dalla Volta, F.; Lucchini, A. Generation of almost simple groups. *J. Algebra* **178** (1995) 194–223.

[8] Detomi, E.; Lucchini, A. Crowns and factorization of the probabilistic zeta function of a finite group. *J. Algebra* **265** (2003) 651–668.

[9] Dixon, J.D.; Mortimer B. *Permutation Groups*. Graduate Texts in Mathematics, 163. Springer, New York, 1996.

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

[11] Guralnick, R. M. On the number of generators of a finite group. *Arch. Math. (Basel)* **53** (1989) 521–523.

[12] Hiss, G.; Malle G. Low dimensional representations of quasi-simple groups. *LMS J. Comput. Math.* **4** (2001) 22–63. [Corrigenda: *LMS J. Comput. Math.* **5** (2002) 95–126].

[13] Huppert, B. *Endliche Gruppen I.* Grundlehren Math. Wiss. 134. Springer-Verlag, Berlin, Heidelberg, New York, 1967

[14] Jansen, C. H.; Lux, K.; Parker, R.A; Wilson, R. A. *An Atlas of Brauer characters.* The Clarendon Press, OUP, New York, 1995.

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

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

[17] Isaacs, I.M. The number of generators of a linear p-group. *Canad. J. Math.* **24** (1972) 851–858.

[18] Leedham-Green, C.R. The computational matrix group project. In *Groups and computation, III (Columbus, OH, 1999)*, Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, 229–247.

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

[20] Lubotzky, A. The expected number of random elements to generate a finite group. *J. Algebra* **257** (2002) 452–459.

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

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

[23] Holt, D.; Macbeath, M. Certain maximal characteristic subgroups of the free group of rank 2. *Comm. Algebra* **25** (1997) 1047–1077.

[24] Malle, G.; Saxl, J.; Weigel T. Generation of classical groups *Geom. Dedicata* **49** (1994) 85–116.

[25] Neunhöffer, M; Seress, Á. A data structure for a uniform approach to computations with finite groups. In *ISSAC '06: Proceedings of the 2006 international symposium on symbolic and algebraic computation* (2006) 254–261.

[26] Wiegold, J. Growth sequences of finite groups, III. *J. Austral. Math. Soc. Ser. A* **25** (1978) 142–144.

Addresses:

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK.
e-mail: D.F.Holt@warwick.ac.uk

Mathematical Institute, University of St Andrews, St Andrews, Fife KY16 9SS, UK.
email: colva@mcs.st-and.ac.uk