ON BASE SIZES FOR PRIMITIVE GROUPS OF PRODUCT TYPE

TIMOTHY C. BURNESS AND HONG YI HUANG

ABSTRACT. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite permutation group and recall that the base size of G is the minimal size of a subset of Ω with trivial pointwise stabiliser. There is an extensive literature on base sizes for primitive groups, but there are very few results for primitive groups of product type. In this paper, we initiate a systematic study of bases in this setting. Our first main result determines the base size of every product type primitive group of the form $L \wr P \leqslant \mathrm{Sym}(\Omega)$ with soluble point stabilisers, where $\Omega = \Gamma^k$, $L \leqslant \mathrm{Sym}(\Gamma)$ and $P \leqslant S_k$ is transitive. This extends recent work of Burness on almost simple primitive groups. We also obtain an expression for the number of regular suborbits of any product type group of the form $L \wr P$ and we classify the groups with a unique regular suborbit under the assumption that P is primitive, which involves extending earlier results due to Seress and Dolfi. We present applications on the Saxl graphs of base-two product type groups and we conclude by establishing several new results on base sizes for general product type primitive groups.

1. INTRODUCTION

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite permutation group and recall that a subset of Ω is a *base* for G if its pointwise stabiliser in G is trivial. We write $b(G)$ for the *base size* of G, which is the minimal size of a base for G. This classical invariant has been studied intensively for many decades, finding a wide range of applications and connections to a diverse range of problems in group theory and related areas (we refer the reader to the survey articles [1, 31] and [5, Section 5] for more details). Determining the base size of a given group is a fundamental problem in permutation group theory.

There is an extensive literature on bases for primitive groups, stretching all the way back to the nineteenth century. In recent years, further motivation for studying bases in this setting stems from a circle of highly influential conjectures of Babai, Cameron, Kantor and Pyber proposed in the 1990s, all of which have now been resolved. For example, a conjecture of Pyber [34] asserts that there is an absolute constant c such that $b(G)$ is at most $c \log_n |G|$ for every primitive permutation group of degree n (note that $b(G) \geqslant \log_n |G|$ is a trivial lower bound). The proof of Pyber's conjecture, which was finally completed by Duyan, Halasi and Maróti in [17], relies heavily on the O'Nan-Scott theorem, which describes the finite primitive groups in terms of the structure and action of the socle of the group. Following [28], this theorem divides the primitive groups into five families, as briefly described in Table 1 (in the table, T denotes a non-abelian finite simple group).

In this paper, we initiate a systematic study of bases for product type primitive groups, noting that there are very few existing results in the literature when compared to the other families of primitive groups identified by the O'Nan-Scott theorem. Recall that if $G \leqslant \mathrm{Sym}(\Omega)$ is such a group, then $G \leqslant L \wr S_k$ acts on $\Omega = \Gamma^k$ with its product action, where $k \geqslant 2$ and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle T, which is either almost simple or diagonal type (see Table 1). Moreover, G has socle T^k and the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is transitive. In particular, we have $T^k \trianglelefteq G \leqslant L \wr P$ and thus $b(G) \leqslant b(L \wr P)$.

Type	Description
I	Affine: $G = V{:}H \leqslant \mathrm{AGL}(V)$, $H \leqslant \mathrm{GL}(V)$ irreducible
II	Almost simple: $T \leqslant G \leqslant \mathrm{Aut}(T)$
III	Diagonal type: $T^k \leqslant G \leqslant T^k.(\mathrm{Out}(T) \times P)$, $P \leqslant S_k$ primitive, or $k = 2$, $P = 1$
IV	Product type: $G \leqslant L \wr P$, L primitive of type II or III, $P \leqslant S_k$ transitive
V	Twisted wreath product

TABLE 1. The types of finite primitive groups in the O'Nan-Scott theorem

In [22], Halasi et al. prove an explicit version of Pyber's conjecture for finite primitive groups, establishing the general bound

$$b(G) \leqslant 2\frac{\log|G|}{\log|\Omega|} + 22$$

when G is a product type group (the original form of Pyber's conjecture in this setting, with unspecified constants, was established in [12]). Bases for product type groups of the form $G = L \wr P$ are also considered by Bailey and Cameron in [1]. In order to state their main result (which imposes no conditions on L or P), let $D(P)$ denote the *distinguishing number* of P, which is the minimal number of parts in a distinguishing partition for the action of P on $\{1, \ldots, k\}$ (recall that a partition is a distinguishing partition if the intersection of the setwise stabilisers of the parts in P is trivial). In addition, for a positive integer m, let $\mathrm{reg}(L, m)$ be the number of regular orbits of L in its coordinatewise action on Γ^m (note that $\mathrm{reg}(L, m) \geqslant 1$ if and only if $m \geqslant b(L)$). Then [1, Theorem 2.13] states that

$$b(L \wr P) \leqslant m \text{ if and only if } \mathrm{reg}(L, m) \geqslant D(P). \tag{1}$$

In studying product type groups $G \leqslant L \wr P$ as above, there is a natural distinction to make between the full wreath product $L \wr P$ and its proper (primitive) subgroups. As in [1], we mainly focus on groups of the form $G = L \wr P$ in this paper, although we will study the general case in Section 6.

Primitive groups with soluble point stabilisers is another common theme throughout the paper. This is partly motivated by the main theorem of [4], which states that $b(G) \leqslant 5$ for every finite primitive permutation group G with soluble point stabilisers (this extends a well known theorem of Seress [38], which establishes the bound $b(G) \leqslant 4$ in the more restrictive setting where G itself is soluble). Moreover, [4, Theorem 2] determines the exact base size of every almost simple primitive group with soluble stabilisers and it is natural to seek an extension of this result to product type groups (as a consequence of the O'Nan-Scott theorem, every primitive group with soluble stabilisers is either almost simple, affine, or product type).

In order to describe some of our main results, it will be convenient to write $\mathcal{S}$ for the set of finite almost simple primitive groups with soluble point stabilisers (as noted above, the precise base size of each group in $\mathcal{S}$ is computed in [4]). Let $G \leqslant L \wr P$ be a product type primitive group as above with soluble point stabiliser H, so $L \in \mathcal{S}$ and G has socle T^k, where T is the socle of L (see Remark 2.5). Since $G = T^k H$, it follows that H induces P on the set of factors of T^k and thus P is soluble. It is easy to see that $b(L \wr P) \geqslant b(L)$ and thus (1) implies that $b(L \wr P) = b(L)$ if and only if $\mathrm{reg}(L, b(L)) \geqslant D(P)$. By [38, Theorem 1.2], the solubility of P implies that $D(P) \leqslant 5$ and as a consequence we deduce that $b(L \wr P) = b(L)$ if $\mathrm{reg}(L, b(L)) \geqslant 5$. This leads us naturally to the problem of determining the groups $L \in \mathcal{S}$ with $\mathrm{reg}(L, b(L)) \leqslant 4$, which is addressed in Theorem 1 below (note that the relevant tables are presented at the end of the paper in Section 7).

Theorem 1. *Let L be a finite almost simple primitive group with soluble point stabiliser J. Then $\mathrm{reg}(L, b(L)) \leqslant 4$ if and only if (L, J) is one of the cases in Table 4 or 5.*

Remark 1. Suppose L is a group as in Theorem 1 with $b(L) = 2$, so $\mathrm{reg}(L, b(L)) = r(L)$ is the number of regular suborbits of L. By the theorem, it follows that $r(L) \leqslant 4$ if and only if (L, J) is one of the cases in Table 4. This extends [10, Theorem 4], which determines the groups L of this form with $r(L) = 1$.

The proof of Theorem 1 will be given in Section 3 and it features a combination of probabilistic and computational methods. In particular, the argument relies on the statement and proof of [4, Theorem 2], with [10, Theorem 3.1] as another key ingredient. The relevant computations will be described in Section 2.3.

An ambitious project initiated by Jan Saxl in the 1990s seeks to determine the primitive groups G with $b(G) = 2$ and there has been some significant progress towards this goal in several special cases. For example, we refer the reader to Fawcett's work [18, 19] on diagonal type groups and twisted wreath products, while various papers have investigated this problem for affine groups (for instance, see Lee's recent work [25, 26] on affine groups with quasisimple point stabilisers). The almost simple primitive groups have also been intensively studied and the base-two groups with socle an alternating group or sporadic group [8, 11] have been determined. In addition, a complete solution for almost simple groups with soluble point stabilisers is presented in [4, Theorem 2].

Our next result constitutes the first step towards a classification of the base-two product type primitive groups.

Theorem 2. *Let $G = L \wr P$ be a product type primitive group with soluble point stabiliser $J \wr P$. Then $b(G) = 2$ if and only if $b(L) = 2$ and either*

(i) *(L, J) is not one of the cases in Table 4; or*

(ii) *$D(P) \leqslant r(L) \leqslant 4$ and $(L, J, r(L))$ is one of the cases in Table 4.*

More generally, we have the following.

Theorem 3. *Let $G = L \wr P$ be a product type primitive group with soluble point stabiliser $J \wr P$. Then either*

(i) *$b(G) = b(L)$; or*

(ii) *$b(G) = b(L) + 1$, $\mathrm{reg}(L, b(L)) < D(P)$ and $(L, J, \mathrm{reg}(L, b(L)))$ is one of the cases in Table 4 or 5.*

Next let $r(G)$ be the number of regular suborbits of an arbitrary product type primitive group of the form $G = L \wr P$, noting that $b(G) = 2$ if and only if $r(G) \geqslant 1$. In the following result, we determine a formula for $r(G)$, which turns out to have some interesting applications. Here t_m denotes the number of (unordered) distinguishing partitions with m non-empty parts for the action of P on $\{1, \ldots, k\}$, so $t_m \geqslant 1$ if and only if $D(P) \leqslant m$.

Theorem 4. *Let $G = L \wr P$ be a product type primitive group on $\Omega = \Gamma^k$. Then*

$$ r(G) = \frac{1}{|P|} \sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m. $$

In general, it is difficult to compute t_m precisely, but this can be achieved in some special cases, which then allows us to simplify the given expression for $r(G)$. For example, see Corollaries 4.6 and 4.7. Notice that we have a trivial upper bound $t_m \leqslant S(k, m)$, which is the total number of partitions of $\{1, \ldots, k\}$ into m non-empty parts (a Stirling number of the second kind). In fact, this bound is best possible. For instance, if $P = C_k$ has prime order, then $t_m = S(k, m)$ for all $m \geqslant 2$. On the other hand, if $\Pi = \{\pi_1, \ldots, \pi_m\}$ is a distinguishing partition for P, then $P_{\{\Pi\}} \leqslant S_m$ is a permutation group on the set of parts comprising Π and thus $t_m \geqslant |P|/m!$. Note that $t_m = |P|/m!$ only if each part has the same size in every distinguishing partition for P into m parts. For example, if $P = S_k$ and

$m = k$, then $t_m = 1 = |P|/m!$ since the partition of $\{1, \ldots, k\}$ into singletons is the only distinguishing partition for P.

As an immediate corollary of Theorem 4, we obtain the following result on product type groups with a unique regular suborbit.

Corollary 5. *Let $G = L \wr P$ be a product type primitive group. Then $r(G) = 1$ if and only if $r(L) = D(P)$ and $t_{D(P)} = |P|/D(P)!$.*

In [37], Seress classifies the primitive groups $P \leqslant S_k$ with $D(P) = 2$, which is equivalent to the property that P has a regular orbit on the power set of $\{1, \ldots, k\}$. Using a similar approach, we will show that $(k, P) = (2, S_2)$ is the only example with a unique regular orbit on the power set (see Corollary 4.14), which we then use to determine the primitive groups P with $t_{D(P)} = |P|/D(P)!$. This allows us to establish the following refinement of Corollary 5 in the case where P is primitive.

Theorem 6. *Let $G = L \wr P$ be a product type primitive group with $P \leqslant S_k$ primitive. Then $r(G) = 1$ if and only if $r(L) = D(P)$ and one of the following holds:*

    (i) *$P = S_k$ and $D(P) = k$.*

    (ii) *$P = A_5$, $k = 6$ and $D(P) = 3$.*

    (iii) *$P = \mathrm{P\Gamma L}_2(8)$, $k = 9$ and $D(P) = 3$.*

    (iv) *$P = \mathrm{AGL}_3(2)$, $k = 8$ and $D(P) = 4$.*

In a different direction, we can use Theorem 4 to establish several new results on the Saxl graphs of base-two product type primitive groups. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group with $b(G) = 2$. The *Saxl graph* of G, denoted $\Sigma(G)$, was introduced by Burness and Giudici in [6]; the vertices of $\Sigma(G)$ are labelled by the elements of Ω, with two vertices joined by an edge if and only if they form a base for G. It is easy to see that if G is primitive, then $\Sigma(G)$ is vertex-transitive and connected. In this case, we write $\mathrm{val}(G)$ to denote the valency of $\Sigma(G)$, noting that $\mathrm{val}(G) = |H|r(G)$ with H a point stabiliser.

Our main result on the valency of Saxl graphs of product type groups is Corollary 7 below, which extends earlier work in [6] and [15]. For part (i), recall that a connected graph is *Eulerian* if and only if every vertex has even degree.

Corollary 7. *Let $G = L \wr P$ be a base-two product type primitive group with Saxl graph $\Sigma(G)$. Then the following hold:*

    (i) *$\Sigma(G)$ is Eulerian.*

    (ii) *$\mathrm{val}(G)$ is a prime power if and only if $L = \mathrm{M}_{10}$, $J = SD_{16}$, P is a 2-group and $t_2 \geqslant 1$ is a 2-power.*

Note that $\mathrm{val}(G)$ is a prime power only if $|H| = |J|^k|P|$ is a prime power, which implies that both J and P are soluble. In particular, $\mathrm{val}(G)$ is a prime power only if $L \in \mathcal{S}$. Let us also observe that there are genuine examples in part (ii), where P is a 2-group and t_2 is a 2-power. For example, if $P = C_8{:}(C_2 \times C_2)$ is the holomorph of the cyclic group C_8 in its natural action on 8 points, then $t_2 = 16$. We refer the reader to Remark 5.3 for further comments.

One of the main open problems concerning the Saxl graphs of base-two primitive groups is a conjecture of Burness and Giudici [6, Conjecture 4.5]. In order to state this, let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group with $b(G) = 2$. For $\alpha \in \Omega$, let

$$\Sigma(\alpha) = \{\gamma \in \Omega : \{\alpha, \gamma\} \text{ is a base for } G\}$$

be the set of neighbours of α in $\Sigma(G)$ (note that $\Sigma(\alpha)$ is the union of the regular G_α-orbits on Ω). Then [6, Conjecture 4.5] asserts that

$$\Sigma(\alpha) \cap \Sigma(\beta) \text{ is non-empty for all } \alpha, \beta \in \Omega.$$

That is, any two vertices in $\Sigma(G)$ have a common neighbour and thus the diameter of $\Sigma(G)$ is at most 2. Some initial evidence for the veracity of this conjecture is presented in Sections 4–6 in [6]. In addition, it has been verified for all groups with socle $L_2(q)$ and for all almost simple groups with soluble point stabilisers (see [14] and [10], respectively). Some positive results for affine groups are given in [27].

By considering this conjecture for primitive wreath products, we deduce that it is equivalent to the following (a priori, stronger) statement.

Conjecture 8. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with $b(G) = 2$ and let $\alpha, \beta \in \Omega$. Then $\Sigma(\alpha)$ meets every regular G_β-orbit on Ω.*

In particular, this asserts that $|\Sigma(\alpha) \cap \Sigma(\beta)| \geqslant r(G)$ for all $\alpha, \beta \in \Omega$. We will present some evidence for Conjecture 8 in Section 5.2. For example, we will show that the conclusion holds for the action of $L_2(q)$ on the set of pairs of 1-dimensional subspaces of the natural module $\mathbb{F}_q^2$ (see Proposition 5.12).

In the final part of the paper, we consider general product type groups of the form $G \leqslant L \wr P$. The analysis of bases in this setting is significantly more difficult and there are very few (if any) existing results in the literature that are tailored to this particular situation. As a starting point, we seek a partial extension of Theorem 2 by determining the base-two groups in certain families of product type primitive groups of the form

$$T \wr P < G < L \wr P \tag{2}$$

with soluble point stabilisers. Here P is soluble and L is almost simple with soluble point stabilisers. In addition, we may assume G induces L on each copy of Γ in the Cartesian product $\Omega = \Gamma^k$, so both L and P are uniquely determined by G (see Remarks 2.4 and 2.5).

Our main results are Theorems 6.4 and 6.11. For instance, the following result in the special case $k = b(L) = 2$ is stated as Theorem 6.4 in Section 6.

Theorem 9. *Let G be a product type primitive group as in (2), where $k = b(L) = 2$ and G has soluble point stabilisers. Then $b(G) \leqslant 3$, with equality if and only if $|L \wr P : G| = 2$ and one of the following holds, where J is a point stabiliser in L:*

  (i) $(L, J) = (\mathrm{M}_{10}, 5{:}4)$.
  (ii) $(L, J) = (\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$.
  (iii) $L = \mathrm{PGU}_4(3)$ and J is of type $\mathrm{GU}_1(3) \wr S_4$.

Further observations on the base-two problem for general product type primitive groups are presented at the end of Section 6.

Notation. Let G be a finite group and let n be a positive integer. We will write C_n, or just n, for a cyclic group of order n and G^n will denote the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits then we may write $G{:}H$. We use $[n]$ for an unspecified soluble group of order n (in addition, we will sometimes write $[n]$ to denote the set $\{1, \ldots, n\}$, but this should not cause any confusion). We adopt the standard notation for simple groups of Lie type from [23]. All logarithms in this paper are in base 2.

Organisation. We begin in Section 2 by recording some preliminary results that will be needed in the proofs of our main results, together with some details of the computational methods that we will use in this paper. This includes work of Seress [37, 38] on the distinguishing number of permutation groups, which we will combine with a key result of Bailey and Cameron [1] on bases for product type groups (see Theorem 2.6). Next in Section 3 we focus on the product type groups of the form $G = L \wr P$ with soluble point stabilisers and we will prove Theorems 1, 2 and 3. Our main results on regular suborbits are presented in Section 4 and we investigate applications involving the Saxl graphs of

product type groups in Section 5. Finally, in Section 6 we consider general product type groups with $G \leqslant L \wr P$, focussing on the case where G contains P. The relevant tables referred to in the statement of Theorem 1 are presented in Section 7.

2. Preliminaries

In this section we record some preliminary results, which will be needed in the proofs of our main theorems. Throughout this section, $G \leqslant \mathrm{Sym}(\Omega)$ denotes a finite transitive permutation group of degree n with point stabiliser H. Let $b(G)$ be the base size of G.

2.1. **Distinguishing number.** Let $\Pi = \{\pi_1, \ldots, \pi_m\}$ be a partition of Ω into m non-empty parts. Then Π is called a *distinguishing partition* for G if its stabiliser $\bigcap_{i=1}^{m} G_{\{\pi_i\}}$ is trivial, where $G_{\{\pi_i\}}$ is the setwise stabiliser of π_i in G. The *distinguishing number* of G, denoted $D(G)$, is defined to be the smallest number m such that there exists a distinguishing partition for G with m parts. For example, $D(G) = 1$ if and only if G is trivial, whereas $D(G) \leqslant 2$ if and only if G has a regular orbit on the power set of Ω. At the other end of the spectrum, S_n and A_n have distinguishing numbers n and $n-1$, respectively.

We will need the following theorem due to Seress [38, Theorem 1.2], which gives a best possible upper bound on $D(G)$ when G is soluble.

Theorem 2.1. *If G is soluble, then $D(G) \leqslant 5$.*

Remark 2.2. It is worth noting that for each $d \in \{2, 3, 4, 5\}$, there are infinitely many soluble transitive permutation groups G with $D(G) = d$. For example, if $t \in \{2, 3, 4\}$ and $m \geqslant 2$, then $D(G) = t + 1$ for the natural action of $G = S_t \wr C_m$ of degree tm (see [38, p.244]). And by Theorem 2.3 below, there are infinitely many soluble primitive groups G with $D(G) = 2$.

The following result on the distinguishing number of primitive groups, which is also due to Seress [37, Theorem 2], will be useful later.

Theorem 2.3. *Let G be a primitive group of degree n. Then either $D(G) = 2$ or one of the following holds:*

  (i) *$G = S_n$ or A_n.*
  (ii) *G is one of 43 groups listed in [37, Theorem 2], each with $n \leqslant 32$ and $D(G) \in \{3, 4\}$.*

The precise distinguishing numbers of the groups arising in case (ii) of Theorem 2.3 were determined by Dolfi (see [16, Lemma 1]).

2.2. **Product type groups.** Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a finite primitive group with socle T and point stabiliser J, which is either almost simple or diagonal type (see Table 1). Let $k \geqslant 2$ be an integer and consider the product action of $L \wr S_k$ on the Cartesian product $\Omega = \Gamma_1 \times \cdots \times \Gamma_k = \Gamma^k$:

$$(\gamma_1, \ldots, \gamma_k)^{(z_1, \ldots, z_k)\sigma} = \left(\gamma_{1^{\sigma^{-1}}}^{z_{1^{\sigma^{-1}}}}, \ldots, \gamma_{k^{\sigma^{-1}}}^{z_{k^{\sigma^{-1}}}} \right),$$

where $\gamma_i \in \Gamma$, $z_i \in L$ and $\sigma \in S_k$. Since this action is faithful and primitive, we can view $L \wr S_k$ as a product type primitive group on Ω, with socle T^k and point stabiliser $J \wr S_k$. More generally, a subgroup $G \leqslant L \wr S_k$ is a primitive group of product type if G has socle T^k and the subgroup $P \leqslant S_k$ induced by the conjugation action of G on the set of factors of T^k is transitive. Therefore

$$T^k \trianglelefteq G \leqslant L \wr P. \tag{3}$$

Remark 2.4. Let $G_1 = \{(z_1, \ldots, z_k)\sigma \in G : 1^\sigma = 1\}$ and let $L_1 \leqslant L \leqslant \mathrm{Sym}(\Gamma_1)$ be the group induced by G_1 on Γ_1. Then by a theorem of Kovács [24, (2.2)], we may replace G by a conjugate G^x for some $x \in \prod_{i=1}^k \mathrm{Sym}(\Gamma_i) < \mathrm{Sym}(\Omega)$ so that $G \leqslant L_1 \wr P$ and G induces L_1 on each factor Γ_i of Ω. Since $L_1 \leqslant \mathrm{Sym}(\Gamma_1)$ is primitive, we are free to assume that $L_1 = L$, so (3) holds and the groups L and P are uniquely determined by G. This observation will be relevant when we consider general product type groups with $G < L \wr P$ in Section 6.

Remark 2.5. Consider the special case where $G \leqslant L \wr P$ is a product type primitive group with soluble point stabiliser $H = G_\alpha$, where $\alpha = (\gamma, \ldots, \gamma) \in \Omega$ for some $\gamma \in \Gamma$. By the transitivity of the socle T^k on Ω, we have $G = T^k H$ and thus H induces P on the set of factors of T^k. Therefore, P is soluble. In addition, we have $(T_\gamma)^k = (T^k)_\alpha \leqslant H$, so T_γ is soluble and thus L is almost simple (indeed, if L is a diagonal type group with socle $T = S^m$ for some non-abelian simple group S, then $T_\gamma \cong S$ is insoluble). In particular, $L/T \leqslant \mathrm{Out}(T)$ is soluble. Now the primitivity of L implies that $L = TL_\gamma$, so $L_\gamma/T_\gamma \cong L/T$ is soluble and we conclude that L_γ is soluble.

Given a positive integer m, let $\mathrm{reg}(L, m)$ be the number of regular L-orbits with respect to the natural coordinatewise action of L on the Cartesian product Γ^m. Note that $\mathrm{reg}(L, 2) = r(L)$ is the number of regular suborbits of L on Γ.

As explained in the introduction, in this paper we are primarily interested in product type primitive groups of the form $G = L \wr P$ as above. In this setting, the following theorem of Bailey and Cameron (see [1, Theorem 2.13]) will be an essential tool.

Theorem 2.6. *Let $G = L \wr P$ be a product type primitive group. Then $b(G) \leqslant m$ if and only if $\mathrm{reg}(L, m) \geqslant D(P)$. In particular, $b(G) = 2$ if and only if $r(L) \geqslant D(P)$.*

2.3. **Computational methods.** To conclude this preliminary section, we briefly describe some of the main computational methods that we will use in this paper, working with MAGMA [2] (version V2.26-6). Here we focus on the computations arising in the proof of Theorem 1 in Section 3, so let $L \leqslant \mathrm{Sym}(\Gamma)$ be a finite primitive almost simple permutation group with socle T and point stabiliser J. Note that the primitivity of L implies that T acts transitively on Γ.

2.3.1. *Regular orbits on Γ^2.* First assume $b(L) = 2$ and let $r(L)$ (respectively, $r(T)$) be the number of regular suborbits of L (respectively, T) on Γ. As explained in [10, Section 2.2], we can compute $r(L)$ by working with double cosets. Indeed, if R is a complete set of (J, J) double coset representatives in L, then

$$r(L) = |\{x \in R : |JxJ| = |J|^2\}|.$$

Similarly, if R_0 is a complete set of (J_0, J) double coset representatives, where $J_0 = J \cap T$, then

$$r(T) = |\{x \in R_0 : |J_0 x J| = |J_0||J|\}|.$$

It is straightforward to compute these numbers using MAGMA. We first construct L as a permutation group (not necessarily with respect to the action on Γ) and we then construct J as a maximal subgroup. To do this, we will typically use the functions

<div align="center"><code>AutomorphismGroupSimpleGroup</code> and <code>MaximalSubgroups</code>.</div>

The latter returns a set of representatives of the conjugacy classes of maximal subgroups of L, but it is not effective in a handful of cases we need to consider. To get around this difficulty, we can exploit the fact that $J = N_L(K)$ for a suitable p-subgroup K of T (for instance, see [4, Example 2.4]). If $|\Gamma| = |L : J|$ is not prohibitively large (for example, if $|\Gamma| < 10^7$), then we can use the function <code>DoubleCosetRepresentatives</code> to determine R and R_0, which then allows us to compute $r(L)$ and $r(T)$.

2.3.2. *Regular orbits on Γ^3 and Γ^4.* In the proof of Theorem 1 we will also need to compute $\mathrm{reg}(L, b(L))$ in a number of cases with $b(L) = 3$ or 4. Fix $\gamma \in \Gamma$ and set $J = L_\gamma$. Decompose $\Gamma = \Lambda_1 \cup \cdots \cup \Lambda_t$ as a disjoint union of J-orbits and fix $\lambda_i \in \Lambda_i$ and $K_i = J_{\lambda_i}$.

Suppose $b(L) = 3$. Then every regular L-orbit on Γ^3 is represented by an element of the form $(\gamma, \lambda_i, \beta)$, where β is contained in a regular orbit of K_i on Γ. Therefore,

$$\mathrm{reg}(L, 3) = \sum_{i=1}^{t} r_i, \tag{4}$$

where r_i is the number of regular orbits of K_i on Γ.

Now assume $b(L) = 4$. Fix $i \in \{1, \ldots, t\}$. Let $\Lambda_{i,1}, \ldots, \Lambda_{i,m_i}$ be the orbits of K_i on Γ and for each $j \in \{1, \ldots, m_i\}$ set $K_{i,j} = (K_i)_{\omega_j} = J_{\lambda_i} \cap J_{\omega_j}$ for some fixed $\omega_j \in \Lambda_{i,j}$. Notice that every regular L-orbit on Γ^4 is represented by an element of the form $(\gamma, \lambda_i, \omega_j, \beta)$, where β is in a regular orbit of $K_{i,j}$ on Γ. Therefore, if $r_{i,j}$ denotes the number of regular orbits of $K_{i,j}$ on Γ, then

$$\mathrm{reg}(L, 4) = \sum_{i=1}^{t} \sum_{j=1}^{m_i} r_{i,j}. \tag{5}$$

Once again, we can implement this approach in MAGMA in order to compute $\mathrm{reg}(L, b(L))$. As before, we first construct L and J, and then we work with the function `CosetAction` to construct L as a permutation group on Γ, which then allows us to construct stabilisers and their orbits. This can be expensive (in terms of time and memory) if $|\Gamma|$ is large, but in the proof of Theorem 1, we only need to apply this method when $|\Gamma| < 5 \times 10^6$ and no special difficulties arise.

3. Soluble stabilisers

In this section, we assume $G = L \wr P$ is a product type primitive group on $\Omega = \Gamma^k$, with socle T^k and soluble point stabiliser $J \wr P$. In particular, P is soluble and $L \leqslant \mathrm{Sym}(\Gamma)$ is almost simple with socle T and soluble point stabiliser J (so we have $L \in \mathcal{S}$ in terms of our notation in Section 1). We will prove Theorems 1, 2 and 3.

We begin with a useful observation in this setting.

Lemma 3.1. *Let $G = L \wr P$ be a product type primitive group with soluble point stabilisers. Then either*

    (i) $\mathrm{reg}(L, b(L)) \geqslant D(P)$ *and* $b(G) = b(L)$*; or*

    (ii) $\mathrm{reg}(L, b(L)) < D(P)$ *and* $b(G) = b(L) + 1$*.*

Proof. First recall that $b(G) \geqslant b(L)$, which shows that (i) follows from Theorem 2.6. Now assume $\mathrm{reg}(L, b(L)) < D(P)$, so $b(G) \geqslant b(L) + 1$. By [1, Corollary 2.14], we have

$$b(G) \leqslant b(L) + \lceil \log_m D(P) \rceil,$$

where $m = |\Gamma|$ is the degree of L. Since P is soluble, we have $D(P) \leqslant 5$ by Theorem 2.1, while $m \geqslant 5$ since L is almost simple. Therefore, $\lceil \log_m D(P) \rceil = 1$ and thus $b(G) \leqslant b(L) + 1$ as required. $\square$

Remark 3.2. In general, if $G = L \wr P$ does not have soluble point stabilisers, then the difference $b(G) - b(L)$ can be arbitrarily large. For example, if m is a positive integer and $k > \mathrm{reg}(L, m)$, then $b(L \wr S_k) > m$ by Theorem 2.6.

3.1. **Base-two groups.** Here we will prove Theorem 2, which completely describes the product type primitive groups $G = L \wr P$ as above with $b(G) = 2$. As recorded in Theorem 2.6, we have $b(G) = 2$ if and only if $r(L) \geqslant D(P)$, while Theorem 2.1 implies that $D(P) \leqslant 5$. Therefore, we immediately deduce that $b(G) = 2$ if $r(L) \geqslant 5$ and so we are interested in determining the groups $L \in \mathcal{S}$ with $1 \leqslant r(L) \leqslant 4$.

With this aim in mind, the following result establishes Theorem 1 in the special case where $b(L) = 2$ (the proof of Theorem 1 will be completed in Proposition 3.10 below). Recall that Table 4 is presented in Section 7 at the end of the paper.

Proposition 3.3. *Let $L \leqslant \mathrm{Sym}(\Gamma)$ be an almost simple primitive group with socle T and soluble point stabiliser J. Then $1 \leqslant r(L) \leqslant 4$ if and only if (L, J) is one of the cases in Table 4.*

Proof. Following [10], let $\mathcal{G}$ be the set of base-two almost simple primitive groups with soluble point stabilisers and note that the groups in $\mathcal{G}$ are determined in [4]. Let us also define $\mathcal{L}$ to be the set of classical groups in $\mathcal{G}$ with socle $\mathrm{L}_2(q)$ such that J is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$ (in other words, J is the normaliser of a maximal torus). Given $L \in \mathcal{G}$ as in the statement of the proposition, let

$$\mathcal{P}(L) = \frac{|\{(\alpha, \beta) \in \Gamma^2 \,:\, L_\alpha \cap L_\beta = 1\}|}{|\Gamma|^2} = \frac{|J|^2 r(L)}{|L|} \tag{6}$$

be the probability that a random pair of points in Γ form a base for L (so the condition $b(L) = 2$ implies that $\mathcal{P}(L) > 0$).

First assume $L \in \mathcal{G} \backslash \mathcal{L}$ and $\mathcal{P}(L) \leqslant 3/4$. By [10, Theorem 3.1], the possibilities for (L, J) are recorded in [10, Tables 2 and 3], together with the precise value of $r(L)$. Therefore, it is a routine exercise to read off the cases with $r(L) \leqslant 4$, all of which are listed in Table 4.

Next suppose $L \in \mathcal{G} \setminus \mathcal{L}$ and $\mathcal{P}(L) > 3/4$, in which case $4|J|^2 r(L) > 3|L|$. We will establish the following claim, which extends [10, Proposition 7.1] and immediately implies that $r(L) \geqslant 5$.

Claim. If $L \in \mathcal{G} \setminus \mathcal{L}$ and $\mathcal{P}(L) > 3/4$, then $16|J|^2 \leqslant 3|L|$.

To prove the claim, we consider each possibility for T in turn. First assume $T = A_m$ is an alternating group. With the aid of MAGMA [2], it is straightforward to verify the claim when $m \leqslant 12$. Now assume $m > 12$. As noted in the proof of [10, Proposition 7.1], m is a prime and $J = \mathrm{AGL}_1(m) \cap L$, which implies that

$$\frac{|J|^2}{|L|} \leqslant \frac{m(m-1)}{(m-2)!} < \frac{3}{16}$$

as required. The sporadic groups are also straightforward. Here the possibilities for J can be read off from [42], noting that we may exclude the cases in [10, Table 2] and [4, Table 4] since we are assuming $\mathcal{P}(L) > 3/4$.

Next assume T is an exceptional group of Lie type over $\mathbb{F}_q$. As noted in the proof of [4, Proposition 7.1], either $J = N_L(R)$ for some maximal torus R or T (see [30, Table 5.2]), or (L, J) is one of the cases in [10, Table 4]. In addition, we may exclude the relevant cases in [10, Table 2]. The claim now follows by inspection. For example, suppose $T = {}^2B_2(q)$ and $J = N_L(R)$ is the normaliser of a maximal torus, where $q = 2^f$ with $f \geqslant 3$ odd. Here

$$|J| \leqslant 4(q + \sqrt{2q} + 1)\log q, \quad |L| \geqslant |T| = q^2(q^2 + 1)(q - 1)$$

and the claim follows if $f \geqslant 5$. On the other hand, if $f = 3$ then the condition $\mathcal{P}(L) > 3/4$ implies that $J \cap T = 7{:}2$ or $5{:}4$, whence $|J| \leqslant 60$, $|L| \geqslant 29120$ and once again the desired bound holds.

To complete the proof of the claim, we may assume T is a classical group over $\mathbb{F}_q$ and we note that the possibilities for L and J are recorded in [10, Table 5]. In each case, the precise structure of J is given in [23, Chapter 4] and the claim follows by inspection. For example, suppose $T = \mathrm{L}_3^\epsilon(q)$ and J is of type $\mathrm{GL}_1^\epsilon(q) \wr S_3$. If $q \geqslant 19$, then the bounds $|L| > \frac{1}{6}q^8$ and $|J| \leqslant 12(q+1)^2 \log q$ are sufficient. For the remaining groups with $q \leqslant 17$, excluding the cases with $\mathcal{P}(L) \leqslant 3/4$ recorded in [10, Table 3], we can verify the bound by working with the exact orders of L and J. All of the other cases are very similar and

we omit the details. This justifies the claim and we have now completed the proof of the proposition for the groups in $\mathcal{G} \setminus \mathcal{L}$.

Finally, let us assume $L \in \mathcal{L}$, so L has socle $T = \mathrm{L}_2(q)$. Write $q = p^f$, where p is a prime. If $q \leqslant 81$ then it is a routine exercise to determine all the groups with $r(L) \leqslant 4$ using MAGMA [2] (see Section 2.3.1) and one can check that all the relevant cases have been recorded in Table 4. For the remainder, we may assume $q > 81$.

First assume J is of type $\mathrm{GL}_1(q) \wr S_2$. Here [4, Lemma 4.7] implies that $b(L) = 2$ if and only if $\mathrm{PGL}_2(q)$ is not a proper subgroup of L. If $L = \mathrm{PGL}_2(q)$ then $r(L) = 1$ (see [6, Example 2.5]) and so this case is recorded in Table 4. Now assume $L \cap \mathrm{PGL}_2(q) = T$ and q is odd. By [10, Lemmas 4.3 and 4.4], we have $r(L) \leqslant 4$ only if $r(\mathrm{P\Sigma L}_2(q)) \leqslant 4$. By arguing as in the proof of [10, Proposition 4.10], we see that $r(\mathrm{P\Sigma L}_2(q)) = m/2f$, where m is the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Since every generator of the multiplicative group $\mathbb{F}_q^\times$ has this property, it follows that $m \geqslant \phi(q-1)$, where ϕ is Euler's totient function. In particular, $r(L) \leqslant 4$ only if $\phi(q-1) \leqslant 8f$. By applying the lower bound on $\phi(q-1)$ in [10, Lemma 4.9] (the original reference is [36, Theorem 15]), we find that $\phi(q-1) > 8f$ for every prime-power q with $q > 81$, whence $r(L) \geqslant 5$ and no additional cases arise.

Finally, suppose J is of type $\mathrm{GL}_1(q^2)$, so $b(L) = 2$ if and only if L does not contain $\mathrm{PGL}_2(q)$ (see [4, Lemma 4.8]). Therefore, we may assume q is odd and by combining Lemmas 4.12 and 4.13 in [10], we observe that $r(L) \leqslant 4$ only if $r(\mathrm{P\Sigma L}_2(q)) \leqslant 4$. By arguing as in the proof of [10, Proposition 4.18], we deduce that $r(L) \leqslant 4$ only if $\phi(q^2-1) \leqslant 8f(q+1)$. But one can check that the bound in [10, Lemma 4.9] yields $\phi(q^2-1) > 8f(q+1)$ for every prime-power q with $q > 81$, and so once again we conclude that $r(L) \geqslant 5$. This completes the proof of the proposition. $\square$

Remark 3.4. Let (L, J) be one of the cases recorded in Table 4. In the fourth column of the table we give $r(T)$, which is the number of regular suborbits of T on $\Gamma = L/J$. Note that each regular suborbit of L is a union of $|L : T|$ regular suborbits of T, so $r(T) \geqslant r(L) \cdot |L : T|$. If $L = \mathrm{PGL}_2(q)$ and J is of type $\mathrm{GL}_1(q) \wr S_2$ then

$$ r(L) = 1, \quad r(T) = \begin{cases} 1 & q \text{ even} \\ (q+a)/4 & q \text{ odd} \end{cases} $$

where $a = 7$ if $q \equiv 1 \pmod 4$, otherwise $a = 5$ (see the proof of [4, Lemma 4.7]). For each of the remaining cases in Table 4, we can compute the exact value of $r(T)$ by proceeding as in Section 2.3.1. This information will be useful in Section 6 (see the proof of Theorem 6.4, for example).

As a corollary we obtain the following result, which establishes Theorem 2.

Theorem 3.5. *Let $G = L \wr P$ be a product type primitive group with soluble point stabiliser $J \wr P$. If $b(L) = 2$, then either*

(i) $b(G) = 2$; or

(ii) $b(G) = 3$, $r(L) < D(P)$ and $(L, J, r(L))$ is one of the cases in Table 4.

Proof. We may assume $b(G) \geqslant 3$. Then Lemma 3.1 implies that $b(G) = 3$ and $r(L) < D(P)$, where $D(P) \leqslant 5$ by Theorem 2.1. Now apply Proposition 3.3. $\square$

3.2. **The general case.** In this section, we complete the proof of Theorem 1 and we establish Theorem 3. As before, $G = L \wr P$ is a product type primitive group with soluble point stabiliser $J \wr P$. Here $L \in \mathcal{S}$ and our first aim is to determine all the groups with $\mathrm{reg}(L, b(L)) \leqslant 4$.

Set $b = b(L)$ and $r = \mathrm{reg}(L, b)$. Let $\mathcal{P}$ be the probability that a random b-tuple of points in Γ is a base for L. It is straightforward to show that

$$\mathcal{P} = \frac{|J|^b r}{|L|^{b-1}}, \tag{7}$$

which is a generalisation of the expression in (6) for the special case $b = 2$. This immediately yields the following observation.

Lemma 3.6. *If $\mathcal{P} > 4|J|^b/|L|^{b-1}$ then $r \geqslant 5$.*

In general, it is difficult to compute $\mathcal{P}$ precisely, but there is a method to obtain an upper bound on the complementary probability $\mathcal{Q} = 1 - \mathcal{P}$, which will typically be sufficient for our purposes. In order to do this, let $x_1, \ldots, x_m$ be a complete set of representatives of the conjugacy classes of elements in L of prime order and let

$$\mathrm{fpr}(x_i) = \frac{|C_\Gamma(x_i)|}{|\Gamma|} = \frac{|x_i^L \cap J|}{|x_i^L|}$$

be the *fixed point ratio* of x_i on Γ, where $C_\Gamma(x_i)$ is the set of points in Γ fixed by x_i. Then it is straightforward to show that $\mathcal{Q} \leqslant \widehat{\mathcal{Q}}$, where

$$\widehat{\mathcal{Q}} = \sum_{i=1}^m |x_i^L| \cdot \mathrm{fpr}(x_i)^b. \tag{8}$$

This was originally observed and applied by Liebeck and Shalev in their proof of a conjecture of Cameron and Kantor on bases for almost simple primitive groups (see [32, Theorem 1.3]) and it provides a powerful approach for bounding the probability $\mathcal{Q}$. In particular, we deduce that $r \geqslant 5$ if

$$\widehat{\mathcal{Q}} < 1 - \frac{4|J|^b}{|L|^{b-1}}. \tag{9}$$

Three special cases arise in the proof of Proposition 3.10 below and it is convenient to handle them separately from the main argument. Note that in the following lemma, J is the normaliser of a non-split maximal torus of T.

Lemma 3.7. *Suppose $T = \mathrm{L}_2(q)$ and J is of type $\mathrm{GL}_1(q^2)$, where $q \geqslant 11$. Then $b(L) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) \leqslant L$. Moreover, if $b(L) = 3$ then $\mathrm{reg}(L, 3) \geqslant 5$.*

Proof. The base size of L is determined in [4, Lemma 4.8] and so for the remainder we may assume $\mathrm{PGL}_2(q) \leqslant L$. Write $q = p^f$ with p a prime and note that $J \cap \mathrm{PGL}_2(q) = D_{2(q+1)}$. It suffices to verify the inequality in (9) (with $b = 3$), so we need to consider the contributions to $\widehat{\mathcal{Q}}$ from the elements $x \in L$ of prime order; the argument below closely follows the proof of [4, Lemma 4.6]. Note that $\mathrm{fpr}(x) = 0$ if $x^L \cap J$ is empty, so we are only interested in the relevant L-classes that meet J. Let $x \in J$ be an element of prime order r and let $i_r(X)$ be the number of elements of order r in X.

First assume $r = 2$, so x is either semisimple or unipotent (according to the parity of p) since $\mathrm{fpr}(x) = 0$ if x is an involutory field automorphism. Then

$$|x^L \cap J| \leqslant i_2(D_{2(q+1)}) \leqslant q + 2 = a, \quad |x^L| \geqslant \frac{1}{2}q(q-1) = b,$$

so the contribution to $\widehat{\mathcal{Q}}$ from involutions is at most $\alpha_1 = b(a/b)^3$.

Now suppose r is odd, so either r divides $q + 1$ and x is semisimple, or $q = q_0^r$ is an r-th power and x is a field automorphism. If x is semisimple, then $|x^T \cap J| = 2$, $|x^T| = q(q-1)$ and we note that L has $(r-1)/2$ distinct T-classes of such elements. Therefore, the combined contribution to $\widehat{\mathcal{Q}}$ from semisimple elements of odd order is at most

$$\sum_{r \in \pi} \frac{1}{2}(r-1) \cdot \frac{8}{q^2(q-1)^2} < \frac{4\log(q+1)}{q(q-1)^2} = \alpha_2,$$

where π is the set of odd prime divisors of $q+1$ (here we are using the fact that $|\pi|$ is at most $\log(q+1)$, recalling that all logarithms in this paper are in base 2).

Finally, suppose $q = q_0^r$ and x is a field automorphism of order r. Here

$$|x^L \cap J| = \frac{q+1}{q_0+1}, \quad |x^L| = \frac{q(q^2-1)}{q_0(q_0^2-1)}$$

and we note that there are $r - 1$ distinct T-classes of field automorphisms of order r in $\mathrm{Aut}(T)$. If $q_0 = 2$ then $q = 2^r$ and the contribution from field automorphisms is

$$(r-1) \cdot \frac{4(2^r+1)}{3.2^{2r}(2^r-1)^2} < 2^{-r} = q^{-1}.$$

And for $q_0 \geqslant 3$ we get

$$\sum_{r \in \pi'} (r-1) \cdot \frac{q_0^2(q_0-1)^2}{q^2(q-1)^2} \cdot \frac{q+1}{q_0+1} < \sum_{r \in \pi'} (r-1) \cdot 3q^{-3\left(1-\frac{1}{r}\right)} < q^{-1}\log\log q = \alpha_3,$$

where π' is the set of odd prime divisors of $f = \log_p q$.

By combining the above estimates, we conclude that $\widehat{\mathcal{Q}} \leqslant \alpha_1 + \alpha_2 + \alpha_3$ and it is straightforward to check that the bound in (9) holds for all $q \geqslant 11$. $\qquad\square$

Lemma 3.8. *Suppose $T = {}^2B_2(q)$ and $J \cap T = [q^2]{:}C_{q-1}$ is a Borel subgroup. Then $b(L) = 3$ and either $G = {}^2B_2(8){:}3$ and $\mathrm{reg}(L,3) = 2$, or $\mathrm{reg}(L,3) \geqslant 5$.*

Proof. Here $q = 2^f$, $f \geqslant 3$ is odd and $|\Gamma| = q^2 + 1$. In addition, $b(L) = 3$ by [4, Theorem 1.2]. The cases with $q \leqslant 2^7$ can be checked directly using MAGMA (see Section 2.3.2) and so we may assume $f \geqslant 9$. As before, it suffices to show that the inequality in (9) is satisfied (with $b = 3$). Set $J_0 = J \cap T$ and let χ be the permutation character $1_{J_0}^T$, which can be expressed as the sum of the trivial and Steinberg characters of T. The character table of T is given in [40].

First let $x \in T$ be an element of prime order r. If $r = 2$ then $\chi(x) = 1$, so $\mathrm{fpr}(x) = 1/(q^2+1)$ and we have $|x^L| = (q^2+1)(q-1)$. Similarly, if r divides $q - 1$ then $\chi(x) = 2$, $|x^L| = q^2(q^2+1)$ and we note that there are at most $(q-2)/2$ distinct T-classes of such elements. Therefore, the contribution to $\widehat{\mathcal{Q}}$ from unipotent and semisimple elements is at most

$$\alpha_1 = \frac{q-1}{(q^2+1)^2} + \frac{1}{2}(q-2) \cdot \frac{8q^2}{(q^2+1)^2}.$$

Finally, suppose $x \in L$ is a field automorphism of prime order r and note that r is odd since f is odd. Then

$$|x^T| = \frac{q^2(q^2+1)(q-1)}{q^{2/r}(q^{2/r}+1)(q^{1/r}-1)} = f(q,r)$$

and $C_{J_0}(x)$ is a Borel subgroup of $C_T(x) = {}^2B_2(q^{1/r})$, so

$$|x^T \cap J_0 x| = \frac{q^2(q-1)}{q^{2/r}(q^{1/r}-1)} = g(q,r).$$

There are $r - 1$ distinct T-classes of field automorphisms of order r in $\mathrm{Aut}(T)$, so the combined contribution to $\widehat{\mathcal{Q}}$ from field automorphisms is

$$\beta = \sum_{r \in \pi} (r-1) \cdot g(q,r)^3 f(q,r)^{-2}, \qquad (10)$$

where π is the set of prime divisors of $f = \log q$. Set

$$e(q,r) = (r-1) \cdot g(q,r)^3 f(q,r)^{-2}. \qquad (11)$$

If $q = 2^9$ or 2^{11} then it is straightforward to check that $\beta < 1/25$. Now assume $q \geqslant 2^{13}$. If $f = r$ then $\beta = e(q,r)$ and one checks that this is less than $q^{-1/2}$. Now assume f is

composite, so $q^{1/r} \geqslant 8$ for each $r \in \pi$. Here $f(q,r) > q^{5(1-1/r)}$ and $g(q,r) < 2q^{3(1-1/r)}$, which implies that $e(q,r) < 8(r-1)q_0^{1-r} < 4q^{-1/2}$. Since $|\pi| < \log \log q$, we deduce that

$$\beta < 4q^{-1/2} \log \log q.$$

By combining the above estimates, we conclude that $\widehat{\mathcal{Q}} \leqslant \alpha_1 + \alpha_2$ for $q \geqslant 2^9$, where $\alpha_2 = 1/25$ if $q \in \{2^9, 2^{11}\}$, otherwise $\alpha_2 = 4q^{-1/2} \log \log q$. It is now routine to verify that the bound in (9) is satisfied for all $q \geqslant 2^9$. □

Note that in the statement of the next lemma we assume $q \geqslant 27$. Indeed, if $q = 3$ then $T = {}^2G_2(q)' \cong \mathrm{L}_2(8)$ and $J \cap T$ corresponds to a Borel subgroup of $\mathrm{L}_2(8)$ (if $G = T$, then $b(L) = 3$ and $\mathrm{reg}(L, 3) = 1$, otherwise $b(L) = 4$ and $\mathrm{reg}(L, 4) = 2$).

Lemma 3.9. *Suppose* $T = {}^2G_2(q)$ *and* $J \cap T = [q^3]{:}C_{q-1}$ *is a Borel subgroup, where* $q \geqslant 27$. *Then* $b(L) = 3$ *and* $\mathrm{reg}(L, 3) \geqslant 5$.

Proof. Here $q = 3^f$, $f \geqslant 3$ is odd, $|\Gamma| = q^3 + 1$ and $b(L) = 3$ by [4, Theorem 1.2]. The case $q = 27$ can be checked directly using MAGMA and so we may assume $f \geqslant 5$. We now proceed as in the proof of the previous two lemmas, working with fixed point ratio estimates to derive a suitable upper bound on $\widehat{\mathcal{Q}}$ which allows us to verify the inequality in (9) (with $b = 3$). As before, set $J_0 = J \cap T$ and let $\chi = 1_{J_0}^T$ be the permutation character. Once again, χ is the sum of the trivial and Steinberg characters of T (the character table of T is presented in [41]).

First let $x \in T$ be an element of prime order r. If $r = 3$ then $\chi(x) = 1$ and thus $\mathrm{fpr}(x) = 1/(q^3 + 1)$. In addition, we calculate that there are precisely $(q^3 + 1)(q^2 - 1)$ elements in T of order 3 (forming three distinct conjugacy classes). Next assume r divides $q - 1$. If $r = 2$ then $|x^L| = q^2(q^2 - q + 1)$ (there is a unique class of involutions in T) and we have $\chi(x) = q + 1$, so $\mathrm{fpr}(x) = 1/(q^2 - q + 1)$. Now suppose r is an odd prime divisor of $q - 1$. Here $\chi(x) = 2$, so $\mathrm{fpr}(x) = 2/(q^3 + 1)$ and $|x^T| = q^3(q^3 + 1)$. Since there are at most $(q-3)/2$ distinct T-classes of such elements, we conclude that the contribution to $\widehat{\mathcal{Q}}$ from unipotent and semisimple elements is at most

$$\alpha_1 = \frac{q^2 - 1}{(q^3 + 1)^2} + \frac{q^2}{(q^2 - q + 1)^2} + \frac{1}{2}(q - 3) \cdot \frac{8q^3}{(q^3 + 1)^2}.$$

Now assume $x \in L$ is a field automorphism of prime order r, so r is odd and we have

$$|x^T| = \frac{q^3(q^3 + 1)(q - 1)}{q^{3/r}(q^{3/r} + 1)(q^{1/r} - 1)} = f(q, r)$$

and

$$|x^T \cap J_0 x| = \frac{q^3(q - 1)}{q^{3/r}(q^{1/r} - 1)} = g(q, r).$$

Therefore, the combined contribution to $\widehat{\mathcal{Q}}$ from field automorphisms is β, as defined in (10). Define $e(q, r)$ as in (11).

If $f = r$ then $\beta = e(q, r) < q^{-1}$ for all $q \geqslant 3^5$. Now assume f is composite, so $q^{1/r} \geqslant 27$ for each $r \in \pi$. Then one checks that $f(q, r) > q^{7(1-1/r)}$ and $g(q, r) < 2q^{4(1-1/r)}$, which implies that $e(q, r) < 8(r-1)q_0^{-2(r-1)} < 4q^{-1}$. Since $|\pi| < \log \log q$, we conclude that $\beta < \alpha_2 = 4q^{-1} \log \log q$ for all $q \geqslant 3^5$.

Therefore, $\widehat{\mathcal{Q}} \leqslant \alpha_1 + \alpha_2$ and it is now straightforward to verify the bound in (9). □

We are now in a position to prove the following result. When combined with Proposition 3.3, this completes the proof of Theorem 1. Recall that Table 5 is given in Section 7.

Proposition 3.10. *Let* $L \leqslant \mathrm{Sym}(\Gamma)$ *be an almost simple primitive group with socle* T *and soluble point stabiliser* J. *If* $b(L) \geqslant 3$ *then* $\mathrm{reg}(L, b(L)) \leqslant 4$ *if and only if* (L, J) *is one of the cases in Table 5.*

Proof. Set $b = b(L)$, $r = \mathrm{reg}(L, b)$ and recall that $b \leqslant 5$ by the main theorem of [4]. The proof of [4, Theorem 8.2] gives $r \geqslant 5$ if $b = 5$, so we may assume $b \in \{3, 4\}$ and we note that the possibilities for L and J are recorded in [4, Tables 4–7]. Recall that $r \geqslant 5$ if (9) holds, where $\widehat{\mathcal{Q}}$ is defined in (8).

For most of the cases appearing in [4, Tables 4–7], an explicit upper bound on $\widehat{\mathcal{Q}}$ is given in [4] and we can usually use this to verify the inequality in (9). However, this approach is not always effective because the given upper bound on $\widehat{\mathcal{Q}}$ is either too large, or is not defined. As explained below, in these remaining cases we will typically use MAGMA to directly compute r, implementing the approach described in Section 2.3.2. We divide the remainder of the proof into three cases.

Case 1. $b(L) = 4$.

First assume $b = 4$. By inspecting the relevant tables in [4], we see that $T = \mathrm{L}_2(q)$ with J of type P_1 (a Borel subgroup of L) is the only infinite family that arises. Let us first consider this special case. For $q > 32$, an explicit upper bound on $\widehat{\mathcal{Q}}$ is presented as a function of q in the proof of [4, Lemma 4.4] and it is a routine exercise to check that the bound in (9) is satisfied. The remaining groups with $q \leqslant 32$ can be handled using MAGMA, which allows us to compute r precisely. In particular, the groups with $r \leqslant 4$ are recorded in Table 5. We can apply the same computational approach to handle all the remaining groups with $b = 4$ appearing in [4, Tables 4–7], considering each group in turn.

Case 2. $b(L) = 3$, J *non-parabolic.*

To complete the proof, we may assume $b = 3$. We begin by assuming L is not a group of Lie type in a parabolic action, so either

    (a) $T = \mathrm{L}_2(q)$ and J is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$; or

    (b) (L, J) is one of a finite number of sporadic cases in [4, Tables 4 and 7].

First let us consider the cases in (a), noting that the precise base size of L is recorded in [4, Lemmas 4.7 and 4.8]. The groups with $q \leqslant 37$ can be handled using MAGMA and we find that $r \leqslant 4$ if and only if (L, J, r) is one of the following:

$$(\mathrm{L}_2(4), D_{10}, 2),\ (\mathrm{L}_2(4).2, 5{:}4, 1),\ (\mathrm{L}_2(4).2, D_{12}, 4),\ (\mathrm{PGL}_2(5), D_{12}, 4),$$

all of which are recorded in Table 5 with $L = A_5$ or S_5 (see Remark 7.1). If J is of type $\mathrm{GL}_1(q) \wr S_2$ and $q > 37$, then the proof of [4, Lemma 4.6] yields the upper bound $\widehat{\mathcal{Q}} < 2q^{-1/2}$ and we deduce that (9) holds. For J of type $\mathrm{GL}_1(q^2)$, we refer the reader to Lemma 3.7.

Next let us turn to the groups in (b) above. Here we apply computational methods, after first dividing the groups into two subcollections according to the size of Γ. By inspection, one can check that $|\Gamma| \geqslant 5 \times 10^6$ if and only if $T = \mathrm{P}\Omega_8^+(3)$ and J is of type $\mathrm{O}_4^+(3) \wr S_2$, or $T \in \{\mathrm{Fi}_{22}, \mathrm{Fi}_{23}\}$ and J is the 3-local subgroup of L recorded in [4, Table 4]. Here we can use MAGMA to compute $\widehat{\mathcal{Q}}$ precisely, which then allows us to verify the bound in (9) (see [10, Section 2.2] for further details). In each of the remaining cases, we can apply the usual approach to compute r, as explained in Section 2.3.2.

Case 3. $b(L) = 3$, J *parabolic.*

For the remainder of the proof, we may assume L is a group of Lie type over $\mathbb{F}_q$, J is a maximal parabolic subgroup and $b = 3$. Write $q = p^f$, where p is a prime, and let ϕ be a field automorphism of T of order f.

First assume L is an exceptional group. Here the possibilities for (L, J) are recorded in [4, Table 5] and by inspection we see that one of the following holds:

    (a$'$) $T = G_2(q)$ and $J \cap T = [q^6]{:}C_{q-1}^2$, where $p = 3$ and $L \not\leqslant \langle T, \phi \rangle$.

    (b$'$) $T = {}^2B_2(q)$ and $J \cap T = [q^2]{:}C_{q-1}$.

(c′) $T = {}^2G_2(q)$ and $J \cap T = [q^3]{:}C_{q-1}$, where $q \geqslant 27$.

(d′) (L, J) is one of a finite number of sporadic cases in [4, Table 5] with $q \leqslant 3$.

Consider case (a′). If $q \geqslant 27$, then the explicit upper bound on $\widehat{\mathcal{Q}}$ presented in the proof of [4, Lemma 5.9] is sufficient, while the groups with $q \in \{3, 9\}$ can be handled directly using MAGMA (note that if $q = 9$ then we can construct J by observing that $J = N_L(K)$ for some subgroup $K < T$ of order 9^6). For (b′) and (c′) we refer the reader to Lemmas 3.8 and 3.9. The cases in (d′) can all be handled computationally using MAGMA. First assume $L = F_4(2).2$ and $J = [2^{22}].S_3^2.2$, in which case $|\Gamma| = 21928725$. Here we construct L as a permutation group of degree 139776 and we use the fact that $J = N_L(K)$ with $|K| = 2^{22}$ to construct J (here the function `MaximalSubgroups` is not effective). We then compute $\widehat{\mathcal{Q}}$ and we check that (9) holds (given the size of Γ, this appears to be the most efficient way to handle this case). We use a similar method in the case where $T = {}^3D_4(3)$ and $T \cap J = [3^{11}]{:}(26 \circ \mathrm{SL}_2(3)).2$. All of the remaining cases in (d′) can be handled in the usual fashion and we can compute r precisely. In this way, we deduce that $r \leqslant 4$ if and only if $L = G_2(3)$ and $J = [3^5]{:}\mathrm{GL}_2(3)$, in which case $r = 4$.

Finally, let us assume L is a classical group and J is a parabolic subgroup. By inspecting [4, Table 6], we see that one of the following holds:

(a″) $T = \mathrm{L}_2(q)$ and J is of type P_1.

(b″) $T = \mathrm{L}_3(q)$ and J is of type $P_{1,2}$.

(c″) $T = \mathrm{U}_3(q)$ and J is of type P_1.

(d″) $T = \mathrm{PSp}_4(q)$ and $J \cap T = [q^4]{:}C_{q-1}^2$, where $q \geqslant 4$ is even and $L \not\leqslant \langle T, \phi \rangle$.

(e″) (L, J) is one of a finite number of sporadic cases in [4, Table 6] with $q \leqslant 3$.

First consider case (a″). Here [4, Lemma 4.5] implies that $b(L) = 3$ if and only if $L \leqslant \mathrm{PGL}_2(q)$, or $q = p^f$ is odd, f is even and $L = \langle T, \delta\phi^{f/2} \rangle = T.2$, where $\mathrm{PGL}_2(q) = \langle T, \delta \rangle$. In other words, either L is sharply 3-transitive on Γ and thus $r = 1$, or q is odd, $L = T$ and $r = 2$.

In cases (b″), (c″) and (d″), an explicit upper bound on $\widehat{\mathcal{Q}}$ is presented in the proofs of [4, Lemmas 5.6–5.8]. Using this bound, one can check that (9) holds for $q > 128, 32, 32$, respectively. Consider case (c″) for example. For $q > 10^4$, the bound

$$\widehat{\mathcal{Q}} < 8q^{-1/2}\log\log q + 4q^{-1} + q^{-3}$$

from the proof of [4, Lemma 5.7] is sufficient. Similarly, for $9 \leqslant q \leqslant 10^4$, we can use a more accurate upper bound on $\widehat{\mathcal{Q}}$ in [4] to reduce our analysis to the groups with

$$q \in \{3, 4, 5, 7, 8, 9, 16, 27, 32\}$$

and at this point, we can use MAGMA to compute r precisely (here it is convenient to note that the standard permutation representation of L in MAGMA corresponds to the action of L on Γ). We find that there are several cases with $r \leqslant 4$, all of which have been listed in Table 5. Cases (b″) and (d″) can be handled in the same way. Similarly, we can use MAGMA to compute r for each group in case (e″). □

This completes the proof of Theorem 1. By combining Theorems 1 and 2 with Lemma 3.1, we obtain Theorem 3 as an immediate corollary.

4. REGULAR SUBORBITS

In this section, we will derive an expression for the number of regular suborbits of a product type primitive group of the form $G = L \wr P$ acting on $\Omega = \Gamma^k$, which we denote by $r(G)$. This is the content of Theorem 4, which yields Corollary 5 as an immediate application. We then go on to establish Theorem 6, which describes the groups $G = L \wr P$ with $r(G) = 1$ and $P \leqslant S_k$ primitive. The latter result relies on our classification of the

primitive groups $P \leqslant S_k$ with a unique regular orbit on the power set of $[k]$ (see Corollary 4.14), which extends earlier work of Seress [37] and Dolfi [16].

The proof of Theorem 2.6 in [1] involves a specific construction, which can be used to describe the pairs of points in Ω that form a base for $G = L \wr P$. This yields the following result, which is [6, Lemma 2.8]. The proof of this lemma was omitted in [6], but here we give the details because the argument will be needed in our proof of Theorem 4 below.

Lemma 4.1. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$ and let $\alpha = (\alpha_1, \ldots, \alpha_k)$ and $\beta = (\beta_1, \ldots, \beta_k)$ be elements in Ω. Define a partition Π of $\{1, \ldots, k\}$ such that i and j are in the same part if and only if (α_i, β_i) and (α_j, β_j) are in the same L-orbit on Γ^2. Then $\{\alpha, \beta\}$ is a base for G if and only if each $\{\alpha_i, \beta_i\}$ is a base for L and Π is a distinguishing partition for P.*

Proof. Let $\mathcal{A}$ be the set of $k \times 2$ arrays of elements in Γ such that

(A1) each row of the array is an ordered base for L; and

(A2) the partition of $\{1, \ldots, k\}$ with respect to L-orbits on rows is a distinguishing partition for P.

Let $\mathcal{B}$ be the set of ordered pairs of bases for G and let A be an array in $\mathcal{A}$. We claim that the two columns of A form a base for G, so there is a natural map $f : \mathcal{A} \to \mathcal{B}$.

To justify the claim, let $\alpha = (\alpha_1, \ldots, \alpha_k)$ and $\beta = (\beta_1, \ldots, \beta_k)$ be the two columns of A and suppose $x \in G_\alpha \cap G_\beta$. Write $x = z\sigma$, where $z = (z_1, \ldots, z_k) \in L^k$ and $\sigma \in P$. If $i^\sigma = j$, then $(\alpha_i, \beta_i)^{z_i} = (\alpha_j, \beta_j)$ and thus (α_i, β_i) and (α_j, β_j) are in the same L-orbit. It follows that σ fixes the partition given by (A2), so $\sigma = 1$ since this is a distinguishing partition for P. Hence, $z_i \in L_{\alpha_i} \cap L_{\beta_i} = 1$ by (A1) and thus $x = 1$ as required.

In order to prove the lemma, it suffices to show that f is a bijection. It is clear that f is injective. To show that f is surjective, let A be a $k \times 2$ array of elements in Γ and assume the two columns of A form a base for G. We need to show that A satisfies the conditions labelled (A1) and (A2) above.

Suppose there is a row of A that does not form an ordered base for L. There there exists a non-trivial element in L fixing both entries, which implies that there is a non-trivial element in L^k stabilising the two columns of A pointwise. But this is incompatible with the fact that the two columns of A form a base for G, whence (A1) is satisfied.

Now let us turn to (A2). As we have just noted, each row of A is an ordered base for L of size 2. Now L acts on the set of such bases, so we can use the rows of A to construct a partition Π of $\{1, \ldots, k\}$, where i and j are in the same part if and only if the i-th and j-th rows of A are in the same L-orbit. We need to show that Π is a distinguishing partition for P. Without loss of generality, we may assume that any two rows of A in the same L-orbit are equal (with this assumption, note that the two columns of A still form a base for G). Let $\sigma \in P$ and note that σ permutes the rows of A. Now any two rows of A are equal if and only if they are in the same part of Π, so if σ fixes Π then σ must fix every entry of A. In particular, this implies that σ fixes the two columns of A, which form a base for G. Hence, $\sigma = 1$ and thus Π is a distinguishing partition. Therefore, property (A2) also holds and we conclude that f is surjective. $\qquad\square$

We will now use this lemma to calculate $r(L \wr P)$. In order to do this, we need the following definition.

Definition 4.2. *Let $P \leqslant S_k$ be a permutation group of degree k and let $1 \leqslant m \leqslant k$ be an integer. We will write t_m for the number of (unordered) distinguishing partitions for the action of P on $[k]$ into m non-empty parts.*

Remark 4.3. Note that $t_m > 0$ if and only if $m \geqslant D(P)$. In general, it is rather difficult to compute t_m precisely, but this is possible in some special cases. For example, if $P = S_k$ then $D(P) = k$ and $t_k = 1$ since the partition of $[k] = \{1, \ldots, k\}$ into singletons is clearly

the only distinguishing partition for P. Similarly, if $P = A_k$ then $D(P) = k - 1$ and we have $t_{k-1} = k(k-1)/2$. As discussed in Section 1, if $m \geqslant D(P)$ then

$$\frac{|P|}{m!} \leqslant t_m \leqslant S(k, m), \tag{12}$$

where $S(k, m)$ denotes the number of partitions of $[k]$ into m non-empty parts (a Stirling number of the second kind).

The following result is Theorem 4.

Theorem 4.4. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$. Then*

$$r(G) = \frac{1}{|P|} \sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m.$$

Proof. Set $r = r(L)$ and $D = D(P)$. If $r < D$ then Theorem 2.6 gives $b(G) \geqslant 3$, so $r(G) = 0$ and the result follows (note that each summand in the given expression is 0 in this situation). Now assume $r \geqslant D$ and adopt the notation in the proof of Lemma 4.1, where we showed that $|\mathcal{A}| = |\mathcal{B}|$. In view of (6), we see that $|\mathcal{B}| = |G|r(G)$ and so we just need to count the number of $k \times 2$ arrays satisfying (A1) and (A2).

Let A be an arbitrary $k \times 2$ array satisfying (A1) and (A2), where Π is the partition of $\{1, \ldots, k\}$ corresponding to (A2). Let m be the number of parts in Π, so $D \leqslant m \leqslant k$ and there are precisely t_m possibilities for Π in total. Each part comprising Π corresponds to a distinct regular L-orbit on Γ^2. Since there are r such orbits, it follows that there are $m!\binom{r}{m}$ different ways to label the rows of A by regular L-orbits on Γ^2. In addition, since each of these L-orbits has length $|L|$, there are $|L|^k$ possibilities for A with respect to each choice of labelling of rows by regular L-orbits. To summarise, we deduce that

$$|G|r(G) = |\mathcal{A}| = \sum_{m=D}^{k} m! \binom{r}{m} t_m |L|^k,$$

and the result follows since $|G| = |L|^k |P|$. $\qquad\square$

Remark 4.5. Notice that Theorem 4.4 holds for any group of the form $G = L \wr P$ with its product action on $\Omega = \Gamma^k$, where $L \leqslant \mathrm{Sym}(\Gamma)$ is transitive. In particular, there is no need to impose any conditions on P (for example, if $P = 1$ then $r(G) = r(L)^k$).

We now present several corollaries of Theorem 4. Further applications will be discussed in the next section.

Corollary 4.6. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$, where $P = S_k$. Then $r(G) = \binom{r(L)}{k}$.*

Proof. This is an immediate application of Theorem 4, noting that for $P = S_k$ we have $D(P) = k$ and $t_k = 1$. $\qquad\square$

The next corollary is [6, Proposition 3.5]; here we give a short proof, as an application of Theorem 4.

Corollary 4.7. *Let $G = L \wr P$ be a product type primitive group acting on $\Omega = \Gamma^k$, where $P = C_k$ and k is a prime. Then $r(G) = (r(L)^k - r(L))/k$.*

Proof. Set $r = r(L)$ and note that $D(P) = 2$, so Theorem 2.6 implies that $r(G) \geqslant 1$ if and only if $r \geqslant 2$. Now any partition of $[k]$ into at least two parts is a distinguishing partition for P, so for $m \geqslant 2$ we observe that t_m coincides with the total number of partitions of

$[k]$ into m parts. In other words, $t_m = S(k, m)$ is a Stirling number of the second kind. Therefore,

$$\sum_{m=2}^{k} m! \binom{r}{m} t_m = \sum_{m=2}^{k} m! \binom{r}{m} S(k, m) = r^k - r,$$

where the final equality follows from a basic property of Stirling numbers of the second kind (see [39, p.75], for example). By applying Theorem 4, we conclude that $r(G)k = r^k - r$. $\square$

For the remainder of Section 4, we focus our attention on the groups with $r(G) = 1$. As a starting point, we establish Corollary 5.

Corollary 4.8. *Let $G = L \wr P$ be a product type primitive group. Then $r(G) = 1$ if and only if $r(L) = D(P)$ and $t_{D(P)} = |P|/D(P)!$.*

Proof. Set $r = r(L)$ and $D = D(P)$. If $r = D$ and $t_D = |P|/D!$ then Theorem 4 yields $r(G) = 1$. On the other hand, if $r(G) = 1$ then $r \geqslant D$ by Theorem 2.6 and we have $D!t_D \geqslant |P|$ (see (12)), whence

$$1 = r(G) = \frac{1}{|P|} \sum_{m=D}^{k} m! \binom{r}{m} t_m \geqslant \frac{1}{|P|} D! \binom{r}{D} t_D \geqslant 1.$$

Therefore $r = D$ and $t_D = |P|/D!$ as required. $\square$

In view of the corollary, we are interested in understanding the condition

$$t_{D(P)} = \frac{|P|}{D(P)!}. \tag{13}$$

As previously noted (see Remark 4.3), $P = S_k$ has this property, but $P = A_k$ does not. Our proof of Theorem 6 relies on the classification of the primitive groups with this property, which is stated as Proposition 4.19 below.

Fix an integer $m \in \{1, \ldots, k\}$ and let

$$\mathcal{P}_m([k]) = \{(\pi_1, \ldots, \pi_m) : \pi_i \subseteq [k], \pi_i \cap \pi_j = \emptyset \text{ for } i \neq j, \bigcup_i \pi_i = [k]\}$$

be the set of ordered partitions of $[k]$ into m parts, where some of the parts are allowed to be the empty set. Note that we may identify $\mathcal{P}_2([k])$ with the power set of $[k]$. Then P acts naturally on $\mathcal{P}_m([k])$ via

$$(\pi_1, \ldots, \pi_m)^\sigma = (\pi_1^\sigma, \ldots, \pi_m^\sigma)$$

and we see that $(\pi_1, \ldots, \pi_m)$ is in a regular P-orbit if and only if $\{\pi_1, \ldots, \pi_m\}$ is a distinguishing partition for P. The following lemma, which is an immediate consequence of this observation, will be useful.

Lemma 4.9. *Let $P \leqslant S_k$ be a transitive group of degree k. Then $t_{D(P)} = |P|/D(P)!$ if and only if P has a unique regular orbit on $\mathcal{P}_{D(P)}([k])$.*

Suppose (13) holds and $\{\pi_1, \ldots, \pi_{D(P)}\}$ is a distinguishing partition for P. Then the unique regular P-orbit on $\mathcal{P}_{D(P)}([k])$ is represented by $(\pi_1, \ldots, \pi_{D(P)})$ and all $D(P)!$ rearrangements of this ordered partition are in the same P-orbit. Therefore, the π_i all have the same size and thus $D(P)$ must divide k.

Since we are focussing on the case where $P \leqslant S_k$ is primitive, we have a special interest in the groups with $D(P) = 2$ (see Theorem 2.3). Here Lemma 4.9 implies that (13) holds if and only if P has a unique regular orbit on the power set of $[k]$ and we will classify the primitive groups with this property (see Corollary 4.14 below). This can be viewed as a natural extension of the main theorem of [37] (stated here as Theorem 2.3), which determines the primitive groups $P \leqslant S_k$ with a regular orbit on the power set of $[k]$. It also extends earlier work of Dolfi [16], where the primitive groups with a unique regular orbit on $\mathcal{P}_3([k])$ or $\mathcal{P}_4([k])$ are classified.

For the remainder of this section, define

$$X = \{\Lambda \subseteq [k] \,:\, |\Lambda| \neq k/2\} \tag{14}$$

and note that P has a natural action on X. Of course, if k is odd then X coincides with the power set of $[k]$.

Lemma 4.10. *If P has a regular orbit on X, then $t_2 > |P|/2$.*

Proof. If Λ is in a regular orbit of P on X, then its complement $[k] \setminus \Lambda$ is also contained in a regular P-orbit. Therefore, P has at least two regular orbits on $\mathcal{P}_2([k])$ and thus $t_2 > |P|/2$ by Lemma 4.9. $\qquad\square$

Clearly, if $D(P) = 2$ and k is odd, then P has a regular orbit on X and thus $t_2 > |P|/2$ by the lemma. Therefore, we are interested in the case where $D(P) = 2$ and k is even, so

$$|X| = 2^k - \binom{k}{k/2}.$$

Lemma 4.11. *We have $|X| \geqslant 2^{k-1}$.*

Proof. We may assume k is even, so it suffices to show that

$$\binom{k}{k/2} \leqslant 2^{k-1}.$$

To do this, we will use the following bounds on $m!$ (valid for all $m \geqslant 1$), which are a consequence of Stirling's approximation (see [35]):

$$\sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{1/(12m+1)} < m! < \sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{1/12m}.$$

Therefore, for $k \geqslant 4$ we have

$$\binom{k}{k/2} = \frac{k!}{(k/2)!^2} < \frac{\sqrt{2\pi k} \left(\frac{k}{e}\right)^k e^{1/12k}}{\left(\sqrt{\pi k} \left(\frac{k}{2e}\right)^{k/2} e^{1/(6k+1)}\right)^2} = \left(\frac{2\sqrt{2}}{\sqrt{\pi k}} e^{\frac{1}{12k} - \frac{2}{6k+1}}\right) 2^{k-1} < 2^{k-1}$$

and the result follows, noting that the case $k = 2$ is clear. $\qquad\square$

Let $\mu(P)$ be the *minimal degree* of P, which is the minimal number of points in $[k]$ moved by a non-identity element of P.

Lemma 4.12. *If k is even and $|P| < 2^{\mu(P)/2-1}$, then P has a regular orbit on X.*

Proof. We follow the proof of the main theorem of [13]. Suppose P has no regular orbit on X, which means that each set in X is fixed (setwise) by some prime order element of P. Therefore,

$$|X| = \left| \bigcup_{\sigma \in \mathcal{R}} C_X(\sigma) \right| \leqslant \sum_{\sigma \in \mathcal{R}} |C_X(\sigma)|,$$

where $\mathcal{R}$ is the set of prime order elements in P and $C_X(\sigma)$ is the set of fixed points of σ on X. If $\sigma \in P$ has prime order r, then σ has cycle-shape $(r^m, 1^{k-mr})$ on $[k]$ for some $m \geqslant 1$ and it is easy to see that

$$|C_X(\sigma)| \leqslant 2^{k-m(r-1)} \leqslant 2^{k-(r-1)\mu(P)/r} \leqslant 2^{k-\mu(P)/2}$$

since $\mu(P) \leqslant mr$ and $r \geqslant 2$. By applying Lemma 4.11 we deduce that

$$2^{k-1} \leqslant |X| \leqslant 2^{k-\mu(P)/2}|P|$$

and thus $|P| \geqslant 2^{\mu(P)/2-1}$. $\qquad\square$

We will use Lemma 4.12 and the O'Nan-Scott theorem to prove the following result.

Proposition 4.13. *Let $P \leqslant S_k$ be a primitive group with $D(P) = 2$. Then P has no regular orbit on X if and only if $(k, P) = (2, S_2)$ or $(16, 2^4{:}O_4^-(2))$.*

We then obtain the following as an immediate corollary.

Corollary 4.14. *Let $P \leqslant S_k$ be a primitive group. Then P has a unique regular orbit on the power set of $[k]$ if and only if $(k, P) = (2, S_2)$.*

Proof. Suppose P has a unique regular orbit on the power set of $[k]$, so $D(P) = 2$ and P has no regular orbit on X by Lemma 4.10. If $(k, P) = (16, 2^4{:}O_4^-(2))$ then one checks that P has two regular orbits on the power set of $[k]$. Now apply Proposition 4.13. $\square$

We now focus on the proof of Proposition 4.13, considering each family of primitive groups in turn (see Table 1).

Lemma 4.15. *Let $P \leqslant S_k$ be a primitive group of type III, IV or V. Then P has a regular orbit on X.*

Proof. First assume that P is of type III, so $P \leqslant S^m.(\mathrm{Out}(S) \times S_m)$ is a diagonal type group, S is a non-abelian simple group and $k = s^{m-1}$, where $s = |S|$ and $m \geqslant 2$. Now $|P| < s^{m+1}m!$ and [7, Theorem 4] gives $\mu(P) \geqslant 2k/3$, so in view of Lemma 4.12, it suffices to show that

$$f(s, m) := \frac{2^{\frac{1}{3}s^{m-1}-1}}{s^{m+1}m!} > 1.$$

If we fix s, then it is easy to check that $f(s, m)$ is an increasing function of m, whence

$$f(s, m) \geqslant f(s, 2) = \frac{2^{\frac{1}{3}s-1}}{2s^3} > 1$$

for all $s \geqslant 60$ and the result follows.

Next assume $P \leqslant S_m \wr S_t$ is a product type primitive group of degree $k = m^t$, where $m \geqslant 5$ and $t \geqslant 2$. As explained in the proof of [37, Lemma 4], there exists a subset $\Lambda \subseteq \{1, \ldots, k\}$ such that $P_{\{\Lambda\}} = 1$ and

$$|\Lambda| = \ell + \sum_{i=1}^{t}(m-2)^{i-1}m^{t-i},$$

where $\ell = 3m - 5$ if $t \geqslant 3$, otherwise $\ell = 2m - 3$. If m is odd then $k = m^t$ is odd and thus $\Lambda \in X$. On the other hand, if m is even, then $k/2 = m^t/2$ is even and $|\Lambda|$ is odd, so $\Lambda \in X$ once again.

Finally, suppose P is a primitive group of type V, so $P = S^m.Q$ is a twisted wreath product, where S is a non-abelian simple group and $Q \leqslant S_m$ is transitive. Here we can embed P in a product type primitive group $R = S^2 \wr S_m \leqslant \mathrm{Sym}([k])$ and the result follows since we have already shown that R has a regular orbit on X (see [28, Remark 2(ii)] for the containment of P in R). $\square$

Next, we turn to the primitive groups of affine type. The following result extends [37, Lemma 7].

Lemma 4.16. *Consider the natural action of $P = \mathrm{AGL}_d(p)$ on $k = p^d$ points, where $d \geqslant 1$, p is a prime and $(d, p) \neq (1, 2)$. Then either P has a regular orbit on X, or $D(P) > 2$ and one of the following holds:*

   (i) *$p = 2$ and $d \in \{2, 3, 4, 5\}$.*
   (ii) *$d = 1$ and $p \in \{3, 5, 7\}$.*
   (iii) *$d = 2$ and $p = 3$.*

Proof. First assume p is odd, so $k = p^d$ is also odd. Then as previously noted, P has a regular orbit on X if and only if $D(P) = 2$, and the groups with $D(P) > 2$ can be read off from [37, Lemma 7]. For the remainder, we may assume $p = 2$.

As noted in the proof of [37, Lemma 7], we have $\mu(P) = 2^{d-1}$ and thus

$$|P| < 2^{d^2+d-1} < 2^{\mu(P)/2-1}$$

for $d \geqslant 9$. Therefore, Lemma 4.12 implies that P has a regular orbit on X if $d \geqslant 9$. For $d = 6, 7, 8$, we can use MAGMA to construct P as a permutation group on $[k]$ and by random search we can find a subset $\Lambda \in X$ with $P_{\{\Lambda\}} = 1$ and $|\Lambda| = 16, 16, 17$, respectively. Finally, if $d \in \{3, 4, 5\}$ then $D(P) > 2$ by [37, Lemma 7], and similarly $D(P) = 4$ when $d = 2$. $\qquad\square$

We can now complete the analysis of primitive groups of affine type.

Lemma 4.17. *Let $P \leqslant \mathrm{AGL}_d(p)$ be a primitive affine group of degree $k = p^d$, where $d \geqslant 1$, p is a prime and $D(P) = 2$. Then P has no regular orbit on X if and only if one of the following holds:*

(i) $k = 2$ *and* $P = S_2$.
(ii) $k = 16$ *and* $P = 2^4{:}\mathrm{O}_4^-(2)$.

Proof. We may assume $p = 2$ and $d \geqslant 2$. If $d \geqslant 6$ then Lemma 4.16 implies that $\mathrm{AGL}_d(2)$, and hence P, has a regular orbit on X. Therefore, we may assume $d \in \{2, 3, 4, 5\}$ and $P < \mathrm{AGL}_d(2)$.

If $d = 5$ then $P = 2^5{:}31$ or $2^5{:}(31{:}5)$ and in both cases we can use MAGMA to find a subset of $[32]$ of size 5 with trivial setwise stabiliser in P. Next assume $d = 4$. We can use the MAGMA database of primitive groups to construct each possibility for P; there are 19 such groups, up to permutation isomorphism, and 15 with $D(P) = 2$. In all but one of these cases, we can use random search to find a set in X with trivial setwise stabiliser in P. The exception is the group $P = 2^4{:}\mathrm{O}_4^-(2)$ recorded in case (ii). Here $k = 16$, $D(P) = 2$ and every subset of $[16]$ with trivial setwise stabiliser has size 8, so this is a genuine exception. Finally, if $d \in \{2, 3\}$ then $P = 2^3{:}7$ is the only group with $D(P) = 2$ and it is easy to check that there is a subset of size 3 with trivial setwise stabiliser in P. $\qquad\square$

Finally, we deal with the case where P is an almost simple primitive group.

Lemma 4.18. *Let $P \leqslant S_k$ be an almost simple primitive group with $D(P) = 2$. Then P has a regular orbit on X.*

Proof. Let R be the socle of P and write Q for the stabiliser of a point in $\Omega = [k]$. For the convenience of the reader, we divide the proof into several cases.

Case 1. R is an alternating group.

First assume $R = A_m$ is an alternating group. The case $m = 6$ can be handled using MAGMA, so we may assume $m \neq 6$ and thus $P = S_m$ or A_m. There are now three cases to consider, according to the action of Q on $\{1, \ldots, m\}$.

First assume Q is intransitive, in which case we may identify Ω with the set of t-element subsets of $\{1, \ldots, m\}$ for some $2 \leqslant t < m/2$ (note that $t \neq 1$ since we are assuming $D(P) = 2$). Suppose $m \geqslant t + 5$. If $t \geqslant 4$ then the proof of [37, Lemma 9] shows that there exists a subset Λ of Ω such that $P_{\{\Lambda\}} = 1$ and $|\Lambda| = 2(m - t + 1) < k/2$, so P has a regular orbit on X. Similarly, if $t = 2, 3$ then we can take $|\Lambda| = m - t + 1$. On the other hand, if $m < t + 5$ then $(m, t) = (7, 3)$ or $(5, 2)$, noting that $P = A_5$ in the latter case (since $D(P) > 2$ when $P = S_5$). Here it is straightforward to check that Ω has a subset of size 4 with trivial setwise stabiliser in P.

Next assume Q acts primitively on $\{1, \ldots, m\}$. By the main theorem of [33] we have $|Q| < 4^m$ and [7, Theorem 4] implies that $\mu(P) \geqslant 2k/3$. By combining these bounds and

applying Lemma 4.12, noting that $k = |P : Q|$, we deduce that P has a regular orbit on X if $m \geqslant 14$. For $7 \leqslant m \leqslant 13$ we can use MAGMA to determine the possibilities for Q and it is routine to check that $|P| < 2^{k/3-1}$ unless $(k, P, Q) = (15, A_8, \mathrm{AGL}_3(2))$ or $(15, A_7, \mathrm{L}_3(2))$. In the former case we have $D(P) > 2$, while $D(P) = 2$ in the latter and the result follows since $k = 15$ is odd. Finally, if $m = 5$ then one can check that $D(P) > 2$.

To complete the argument when $R = A_m$, we may assume Q acts imprimitively on $\{1, \ldots, m\}$. Here we may identify Ω with the set of partitions of $\{1, \ldots, m\}$ into b sets of size a, where $a, b \geqslant 2$ and $m = ab \geqslant 8$ (we have already considered the case $m = 6$). Therefore, $k = m!/(a!^b b!)$ and the main theorem of [21] gives $\mu(P) \geqslant k/2$, so it suffices to show that $|P| < 2^{k/4-1}$ (see Lemma 4.12). First assume $m = 8$. If $(a, b) = (2, 4)$ then it is easy to check that $|P| < 2^{k/4-1}$. On the other hand, if $(a, b) = (4, 2)$ then $D(P) = 2$ and the result follows since $k = 35$ is odd. Now assume $m \geqslant 9$. Here $m! < 2^{m^2/4-1}$ and so it suffices to show that $k \geqslant m^2$. This is clear if $a \geqslant 3$ since $k \geqslant \binom{m}{3} > m^2$ for $m \geqslant 9$. Finally, for $a = 2$ it remains to show that

$$f(b) := \frac{(2b)!}{b! 2^b 4b^2} > 1$$

for all $b \geqslant 5$. It is easy to verify that this is an increasing function, so $f(b) \geqslant f(5) > 1$ and the result follows.

Case 2. R is a sporadic group.

Next assume R is a sporadic simple group. First observe that $D(P) > 2$ if $R = \mathrm{M}_{22}$ and $k = 22$, so this case does not arise and thus $\mu(P) \geqslant 2k/3$ by [7, Theorem 4]. Therefore, it suffices to show that $|P| < 2^{k/3-1}$. Let ℓ be the minimal index of a core-free subgroup of P, which can be read off from [42]. If P is not a Mathieu group, then it is straightforward to show that $|P| < 2^{\ell/3-1}$ and the result follows. On the other hand, if P is a Mathieu group then the cases with $D(P) > 2$ are determined in [37, Lemma 12]; by excluding these groups, it is easy to check that $|P| < 2^{k/3-1}$ as required.

Case 3. R is a group of Lie type.

For the remainder, we may assume R is a simple group of Lie type over $\mathbb{F}_q$, where $q = p^f$ and p is a prime. As before, let ℓ be the minimal index of a core-free subgroup of P and note that ℓ is recorded in [20, Table 4].

First assume R is an exceptional group of Lie type. By [29, Proposition 2] and [7, Theorem 4], we have $|P| < k^5$ and $\mu(P) \geqslant 2k/3$, so it suffices to show that $k^5 < 2^{k/3-1}$. The latter bound holds for $k \geqslant 104$ and by inspecting [20, Table 4] we reduce to the case where $R = {}^2B_2(8)$ and Q is a Borel subgroup of P. Here $k = 65$ and $|P| \leqslant 3|R| < 2^{k/3-1}$, so once again Lemma 4.12 implies that P has a regular orbit on X.

Finally, let us assume R is a classical group. Due to isomorphisms between some of the low dimensional groups, we may assume R is one of the following:

$$\mathrm{L}_n(q),\ n \geqslant 2;\ \mathrm{U}_n(q),\ n \geqslant 3;\ \mathrm{PSp}_n(q),\ n \geqslant 4;\ \mathrm{P}\Omega_n^\varepsilon(q),\ n \geqslant 7.$$

We may also assume that R is not isomorphic to an alternating group. By [21, Corollary 1] we have $\mu(P) \geqslant 3k/7$.

First assume $n \geqslant 4$ and observe that $|P| < q^{n^2}$. By carefully inspecting [20, Table 4] we see that $\ell > q^{n-2}$ and thus $\mu(P) > \frac{3}{7} q^{n-2}$. Now, if $n \geqslant 12$ or $q \geqslant 19$ then

$$q^{n^2} < 2^{\frac{3}{14} q^{n-2}-1}$$

and we deduce that $|P| < 2^{\mu(P)/2-1}$, which implies that P has a regular orbit on X (in fact, if $q \geqslant 3$ then the same bound holds for all $n \geqslant 8$). This leaves us with finitely many groups to consider. In each of these remaining cases, it is routine to check that $|P| < 2^{3\ell/14-1}$

with the exception of the following possibilities for (R, k):

$$(\mathrm{L}_4(5), 156), (\mathrm{L}_4(3), 40), (\mathrm{U}_4(3), 112), (\mathrm{U}_4(2), 40), (\mathrm{U}_4(2), 36),$$

$$(\mathrm{Sp}_6(2), 36), (\Omega_8^+(2), 120), (\Omega_8^-(2), 136).$$

(Here we also exclude the relevant groups with $D(P) > 2$, as recorded in [37, Lemma 12], together with the groups where $D(P) = 2$ and k is odd.) In each of these cases, we can use MAGMA to construct P as a permutation group on $[k]$ and then find a subset in X by random search with trivial setwise stabiliser in P.

Finally, let us assume $n \in \{2, 3\}$. If $R = \mathrm{L}_3(q)$ then $\ell = q^2 + q + 1$ and

$$|P| \leqslant 2q^3(q^2 - 1)(q^3 - 1) \log q < 2^{3\ell/14-1}$$

for $q \geqslant 13$. The remaining groups with $q < 13$ can be dealt with using MAGMA as above. Similarly, if $R = \mathrm{U}_3(q)$ then the problem is quickly reduced to the groups with $q \leqslant 5$, each of which can be handled in the usual fashion with the aid of MAGMA. Finally, suppose $R = \mathrm{L}_2(q)$. If $q \geqslant 113$ then $\ell = q + 1$ and one can check that

$$|P| \leqslant q(q^2 - 1) \log q < 2^{3\ell/14-1},$$

which implies that P has a regular orbit on X. The remaining groups with $q < 113$ can be handled using MAGMA; either the bound $|P| < 2^{3k/14-1}$ is satisfied and we conclude via Lemma 4.12, or we construct P as a permutation group on $[k]$ and then use random search to find a set in X with trivial setwise stabiliser in P. □

This completes the proof of Proposition 4.13 and we are now in a position to classify the primitive groups P with $t_{D(P)} = |P|/D(P)!$.

Proposition 4.19. *Let $P \leqslant S_k$ be a primitive group. Then $t_{D(P)} = |P|/D(P)!$ if and only if $P = S_k$, or $(k, P, D(P)) = (6, A_5, 3)$, $(9, \mathrm{P\Gamma L}_2(8), 3)$ or $(8, \mathrm{AGL}_3(2), 4)$.*

Proof. Set $D = D(P)$. As previously noted, if $P = S_k$ then $D = k$ and $t_D = |P|/D!$, whereas $t_D > |P|/D!$ if $P = A_k$. Now assume $P \neq A_k, S_k$ and recall that $D \leqslant 4$ (see Theorem 2.3). If $D = 2$ then Corollary 4.14 applies, so we may assume $D \in \{3, 4\}$. By Lemma 4.9, $t_D = |P|/D!$ if and only if P has a unique regular orbit on $\mathcal{P}_D([k])$ and these groups can be read off by inspecting parts (a) and (c) in [16, Lemma 1]. □

Finally, observe that Theorem 6 now follows by combining Corollary 5 and Proposition 4.19.

5. SAXL GRAPHS

In this section we use Theorem 4 to study the valency and connectedness properties of the Saxl graphs of base-two product type primitive groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive permutation group with $b(G) = 2$ and point stabiliser H. Recall that the vertices of the *Saxl graph* of G, denoted $\Sigma(G)$, are labelled by the elements of Ω, with α and β joined by an edge if and only if $\{\alpha, \beta\}$ is a base for G. Then $\Sigma(G)$ is vertex-transitive with valency $\mathrm{val}(G) = r|H|$, where $r = r(G)$ is the number of regular suborbits of G. In addition, it is easy to see that $\Sigma(G)$ is connected if G is primitive. This concept was initially introduced and studied by Burness and Giudici in [6].

5.1. **Valency.** Recall that a graph is *Eulerian* if it contains an Eulerian cycle, which is a cycle that uses each edge exactly once. A celebrated theorem of Euler asserts that a connected graph is Eulerian if and only if the degree of every vertex is even. In particular, the Saxl graph of a base-two primitive group G is Eulerian if and only if $\mathrm{val}(G)$ is even.

A complete classification of the finite primitive groups with an Eulerian Saxl graph remains out of reach and some genuine exceptions have been identified. For example, if

$G = \mathrm{M}_{23}$ and $H = 23{:}11$, then the action of G on G/H is primitive with $b(G) = 2$ and the corresponding Saxl graph is non-Eulerian (indeed, we compute $r = 159$, so $\mathrm{val}(G) = r|H|$ is odd). The problem for almost simple primitive groups is studied in [6, Proposition 3.2] and subsequently extended in [15, Theorem 4].

As another application of Theorem 4, the following result establishes part (i) of Corollary 7. It can be viewed as an extension of [6, Proposition 3.4].

Proposition 5.1. *Let* $G = L \wr P$ *be a base-two product type primitive group acting on* $\Omega = \Gamma^k$. *Then* $\Sigma(G)$ *is Eulerian.*

Proof. By Theorem 4 we have

$$\sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m = r(G)|P| \tag{15}$$

and each summand on the left hand side of this equality is even since $D(P) \geqslant 2$. Therefore, at least one of $r(G)$ or $|P|$ is even, so $\mathrm{val}(G) = r(G)|H|$ is even and the result follows. $\square$

The finite transitive groups G such that $\Sigma(G)$ has prime valency are determined in [6, Proposition 3.1]. For almost simple primitive groups, this is extended in [15, Theorem 3], which classifies all the groups of this form with the property that $\mathrm{val}(G)$ is a prime power (in each case, $\mathrm{val}(G)$ is a 2-power).

In our next result, which gives part (ii) of Corollary 7, we extend the analysis to product type primitive groups of the form $G = L \wr P$.

Proposition 5.2. *Let* $G = L \wr P$ *be a base-two product type primitive group acting on* $\Omega = \Gamma^k$ *with point stabiliser* $J \wr P$. *Then* $\mathrm{val}(G)$ *is a prime power if and only if* $L = \mathrm{M}_{10}$, $J = SD_{16}$, P *is a 2-group and* $t_2 \geqslant 1$ *is a 2-power.*

Proof. Suppose $\mathrm{val}(G) = p^a$ with p a prime. Then J and P are p-groups, so J is soluble and thus L is almost simple. By [15, Proposition 6.3], the possibilities for (L, J) are recorded in [15, Table 3] and we deduce that $p = 2$. By Theorem 4, we see that (15) holds and thus

$$\sum_{m=D(P)}^{k} m! \binom{r(L)}{m} t_m$$

is a 2-power. This observation immediately implies that $D(P) = 2$, otherwise each summand is divisible by 3. In addition, $r(L) \equiv 2 \pmod 3$ because the binomial coefficient $\binom{r(L)}{2}$ must be indivisible by 3. By inspecting [15, Table 3], we now consider each possibility for (L, J) in turn.

First assume $L = \mathrm{L}_2(q)$ and $J = D_{q-1}$, where $q \geqslant 17$ is a Fermat prime. Then $q \equiv 1 \pmod 4$ and so $r(L) = (q+7)/4$ by the proof of [4, Lemma 4.7]. If we write $q = 2^m + 1$ then $r(L) = 2^{m-2} + 2$ and thus $r(L) \not\equiv 2 \pmod 3$, so this case does not arise. Now suppose $L = \mathrm{L}_2(q)$ and $J = D_{q+1}$ with $q = 2^m - 1 \geqslant 31$ a Mersenne prime. Here $q \equiv 3 \pmod 4$ and $r(L) = (q-3)/4$ by the proof of [9, Lemma 7.9]. Therefore $r(L) = 2^{m-2} - 1$ and once again we deduce that $r(L) \not\equiv 2 \pmod 3$.

Finally, let us turn to the remaining cases in [15, Table 3]. If $L = \mathrm{PGL}_2(q)$ and $J = D_{2(q-1)}$ with $q \geqslant 17$ a Fermat prime, then $r(L) = 1$ (see Table 4) and thus $b(G) \geqslant 3$. The case where $L = \mathrm{PGL}_2(q)$ and $J = D_{2(q+1)}$ with $q \geqslant 7$ a Mersenne prime can be immediately excluded since $b(L) = 3$ by [4, Theorem 2]. The handful of remaining possibilities can be checked using MAGMA [2], implementing the approach presented in Section 2.3.1 to compute $r(L)$. In this way, we find that $r(L) \equiv 2 \pmod 3$ if and only if $L = \mathrm{M}_{10}$ and $J = SD_{16}$, where we observe that $r(L) = 2$.

We conclude that $L = \mathrm{M}_{10}$ with $J = SD_{16}$ is the only possibility. Here Theorem 4 implies that $|P|r(G) = 2t_2$ and thus t_2 is a 2-power (note that $t_2 = 1$ if and only if $P = S_2$). This completes the proof of the proposition. $\square$

Remark 5.3. There are genuine examples in Proposition 5.2, where $P \leqslant S_k$ is a transitive 2-group and t_2 is a 2-power. For example, we can take $(k, P) = (2, S_2)$ or $(4, C_2 \times C_2)$, where $t_2 = 1$ or 4, respectively. By inspecting the MAGMA database of transitive groups, we find that there are 165 groups of degree $k \leqslant 16$ with the desired property. For example, t_2 is a 2-power for 156 of the 1427 transitive 2-groups of degree 16.

5.2. Connectedness. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group with $b(G) = 2$ and recall that the Saxl graph $\Sigma(G)$ is connected in this situation, so it is natural to consider its diameter. Given $\alpha \in \Omega$, let $\Sigma_G(\alpha)$ (or just $\Sigma(\alpha)$ if the corresponding group G is clear from the context) be the set of neighbours of α in $\Sigma(G)$, so

$$\Sigma(\alpha) = \{\beta \in \Omega \, : \, G_\alpha \cap G_\beta = 1\}$$

is the union of the regular G_α-orbits on Ω.

One of the main open problems concerning the connectedness of $\Sigma(G)$ is the following conjecture of Burness and Giudici (see [6, Conjecture 4.5]).

Conjecture 5.4. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group with $b(G) = 2$. Then any two vertices in $\Sigma(G)$ have a common neighbour.*

In other words, the conjecture asserts that the following property is satisfied:

$$\Sigma(\alpha) \cap \Sigma(\beta) \text{ is non-empty for all } \alpha, \beta \in \Omega. \tag{$\star$}$$

In particular, this implies that $\Sigma(G)$ has diameter at most 2 for every finite primitive group G with $b(G) = 2$ (this weaker assertion is stated as [6, Conjecture 4.4]).

Remark 5.5. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite transitive group and let $\mathcal{P}(G) = \mathrm{val}(G)/|\Omega|$ be the probability that a random pair of points in Ω form a base for G. If $\mathcal{P}(G) > 1/2$ then $\mathrm{val}(G) > |\Omega|/2$ and thus the neighbourhoods of any two points in Ω must have a non-empty intersection. Therefore, $(\star)$ holds if $\mathcal{P}(G) > 1/2$ (this is a special case of [6, Lemma 3.6(i)]).

As we highlighted in Section 1, Conjecture 5.4 has been verified in various special cases. For example, every primitive group of degree at most 4095 has the desired property (this has been checked computationally, using the MAGMA database of primitive groups). In addition, it has been verified for all almost simple primitive groups with socle $\mathrm{L}_2(q)$ or with soluble point stabilisers (see [14] and [10]). For the almost simple groups with socle an alternating group A_n, the proof is reduced in [6, Section 5] to the case where each point stabiliser acts imprimitively on $\{1, \ldots, n\}$. Computational methods are used in [6, Section 6] to verify the conjecture for many almost simple sporadic groups and there are asymptotic results of Fawcett (see [19, Theorem 1.4] and [18, Theorem 1.5]), which give the desired conclusion for almost all sufficiently large primitive groups of diagonal and twisted wreath type. Recent work of Lee and Popiel [27] shows that the conjecture holds for many affine groups of the form $G = VH$, where H is a quasisimple sporadic group.

This demonstrates that there is a growing body of evidence pointing towards the veracity of Conjecture 5.4. However, there are very few (if any) results in the literature for product type primitive groups.

Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a finite primitive group (of any type), let $P \leqslant S_k$ be transitive with $k \geqslant 2$ and consider the product action of $G = L \wr P$ on $\Omega = \Gamma^k$. If L is non-regular on Γ, then $G \leqslant \mathrm{Sym}(\Omega)$ is primitive and it is clear that $b(G) = 2$ only if $b(L) = 2$ for the action of L on Γ. The following result reveals the relationship between property $(\star)$ for G and L in this setting.

Lemma 5.6. *Let $G = L \wr P$ be a base-two primitive group in its product action on $\Omega = \Gamma^k$ and assume G satisfies $(\star)$. Then $\Sigma_L(\alpha)$ meets at least $D(P)$ regular L_β-orbits for all $\alpha, \beta \in \Gamma$.*

Proof. Suppose there exists $\alpha, \beta \in \Gamma$ such that the given condition on $\Sigma(L)$ does not hold. We claim that the elements $\rho = (\alpha, \ldots, \alpha)$ and $\sigma = (\beta, \ldots, \beta)$ in Ω have no common neighbour in $\Sigma(G)$, which implies that G does not satisfy $(\star)$.

Seeking a contradiction, suppose $(\gamma_1, \ldots, \gamma_k) \in \Sigma_G(\rho) \cap \Sigma_G(\sigma)$. For each i, Lemma 4.1 implies that $\{\alpha, \gamma_i\}$ and $\{\beta, \gamma_i\}$ are bases for L, so γ_i is contained in both $\Sigma_L(\alpha)$ and a regular L_β-orbit. In addition, the lemma implies that the pairs (β, γ_i) for $1 \leqslant i \leqslant k$ represent at least $D(P)$ distinct L-orbits on Γ^2, whence $\{\gamma_1, \ldots, \gamma_k\}$ meets at least $D(P)$ distinct regular L_β-orbits. But this means that $\Sigma_L(\alpha)$ meets at least $D(P)$ regular L_β-orbits and we have reached a contradiction. □

In order to state our next result, we define the following condition for a base-two group $G \leqslant \mathrm{Sym}(\Omega)$:

$$\Sigma(\alpha) \text{ meets every regular } G_\beta\text{-orbit for all } \alpha, \beta \in \Omega. \qquad (\star\star)$$

Note that if this holds, then $|\Sigma(\alpha) \cap \Sigma(\beta)| \geqslant r(G)$ for all $\alpha, \beta \in \Omega$, so it can be viewed as a stronger form of the condition in $(\star)$.

As a special case of Lemma 5.6, we obtain the following corollary.

Corollary 5.7. *Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a base-two primitive group and consider the primitive product action of $G = L \wr S_{r(L)}$ on $\Omega = \Gamma^k$. If G satisfies $(\star)$, then L satisfies $(\star\star)$.*

This observation leads us to propose the following strengthening of Conjecture 5.4, which is stated as Conjecture 8 in Section 1.

Conjecture 5.8. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive permutation group with $b(G) = 2$. Then $(\star\star)$ holds.*

As noted above, this asserts that any two vertices in $\Sigma(G)$ have at least $r(G)$ common neighbours, and it coincides with Conjecture 5.4 when $r(G) = 1$. In fact, by taking $G = L \wr S_{r(L)}$ as in Corollary 5.7, where $L \leqslant \mathrm{Sym}(\Gamma)$ is an arbitrary primitive group with $b(L) = 2$, we deduce the following result.

Proposition 5.9. *Conjectures 5.4 and 5.8 are equivalent.*

Remark 5.10. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite primitive group with $b(G) = 2$ and point stabiliser H. Let R be a set of (H, H) double coset representatives in G and set

$$S = \{x \in R : |HxH| = |H|^2\}.$$

Then observe that $(\star\star)$ holds if for all $x \in R$ and all $y \in S$, there exists $z \in HyH$ such that $H \cap H^z = H^x \cap H^z = 1$. This approach for verifying $(\star\star)$ can be implemented in Magma and by using the primitive groups database, we have checked that it holds for every base-two primitive group of degree $n \leqslant 4095$.

Remark 5.11. Let $G = V{:}H$ be a primitive affine group with $b(G) = 2$, where $V = (\mathbb{F}_p)^d$ and $H = G_0 \leqslant \mathrm{GL}_d(p)$ is the stabiliser of the zero vector. Set $r = r(G)$ and let $\Lambda_1, \ldots, \Lambda_r$ be the regular orbits of H on V. In [27, Lemma 2.3], Lee and Popiel observe that G satisfies $(\star)$ if and only if every non-zero vector in V is of the form $v_1 + v_2$, where v_1 and v_2 are contained in regular H-orbits. The same argument shows that $(\star\star)$ holds if and only if for all non-zero vectors $v \in V$ and all $i \in \{1, \ldots, r\}$ we can write $v = u_i + w_i$ with $u_i \in \Lambda_i$ and $w_i \in \Lambda_j$ for some j.

The following proposition shows that $(\star\star)$ holds for an infinite family of primitive groups G with $r(G) \geqslant 2$ (by inspecting [3, Table 8.1], we note that G is primitive if q is even, or if $q \geqslant 13$).

Proposition 5.12. *Let $G = \mathrm{L}_2(q)$, where $q \geqslant 4$, and consider the action of G on $\Omega = G/H$, where H is a subgroup of type $\mathrm{GL}_1(q) \wr S_2$. Then G satisfies $(\star\star)$.*

Proof. First assume q is even. As noted in [6, Example 2.5], G satisfies $(\star)$, which coincides with $(\star\star)$ since $r(G) = 1$.

For the remainder, we may assume q is odd, so $H = D_{q-1}$ and [4, Lemma 4.7] implies that $b(G) = 2$. As in [10, Section 4.1], we may identify Ω with the set of unordered pairs of distinct 1-dimensional subspaces of $V = \mathbb{F}_q^2$.

Fix a basis $\{e_1, e_2\}$ for V and set $\beta = \{\langle e_1 \rangle, \langle e_2 \rangle\} \in \Omega$. Note that if $x \in G_\beta$, then x is the image (modulo scalars) of an element $A \in \mathrm{SL}_2(q)$ of the form

$$A = \begin{pmatrix} \lambda & \\ & \lambda^{-1} \end{pmatrix} \text{ or } \begin{pmatrix} & \lambda \\ -\lambda^{-1} & \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_q^\times$, where the matrices are presented with respect to the basis $\{e_1, e_2\}$. We first determine the regular G_β-orbits (as recorded in Remark 3.4, G_β has $(q+a)/4$ regular orbits, where $a = 7$ if $q \equiv 1 \pmod 4$, otherwise $a = 5$). Fix an element $\gamma \in \Omega$.

Suppose $\gamma = \{\langle e_1 \rangle, \langle e_1 + se_2 \rangle\}$ for some $s \in \mathbb{F}_q^\times$. Then an easy calculation shows that $\{\beta, \gamma\}$ is a base for G and the regular G_β-orbit containing γ is

$$R_1 = \{\{\langle e_1 \rangle, \langle e_1 + ce_2 \rangle\} \ : \ c \in \mathbb{F}_q^\times\}.$$

Similarly, if $\gamma = \{\langle e_2 \rangle, \langle e_1 + se_2 \rangle\}$ for some $s \in \mathbb{F}_q^\times$, then $\{\beta, \gamma\}$ is also a base for G and

$$R_2 = \{\{\langle e_2 \rangle, \langle e_1 + ce_2 \rangle\} \ : \ c \in \mathbb{F}_q^\times\}$$

is the regular G_β-orbit containing γ.

Now suppose $\gamma = \{\langle e_1 + se_2 \rangle, \langle e_1 + te_2 \rangle\}$, where $s, t \in \mathbb{F}_q^\times$ are distinct. By arguing as in the proof of [10, Lemma 4.3] we calculate that $\{\beta, \gamma\}$ is a base for G if and only if $-st^{-1}$ is a non-square in $\mathbb{F}_q$. So let us assume $-st^{-1}$ is non-square and suppose $A \in \mathrm{SL}_2(q)$ fixes β. If $A = \mathrm{diag}(\lambda, \lambda^{-1})$, then

$$\gamma^A = \{\langle e_1 + \lambda^{-2}se_2 \rangle, \langle e_1 + \lambda^{-2}te_2 \rangle\},$$

whereas

$$\gamma^A = \{\langle e_1 - \lambda^{-2}s^{-1}e_2 \rangle, \langle e_1 - \lambda^{-2}t^{-1}e_2 \rangle\}$$

if $A = \begin{pmatrix} & \lambda \\ -\lambda^{-1} & \end{pmatrix}$. It follows that the regular G_β-orbit containing γ is

$$R_{s,t} = \{\{\langle e_1 + \lambda^2 se_2 \rangle, \langle e_1 + \lambda^2 te_2 \rangle\} : \lambda \in \mathbb{F}_q^\times\} \cup \{\{\langle e_1 - \lambda^2 s^{-1}e_2 \rangle, \langle e_1 - \lambda^2 t^{-1}e_2 \rangle\} : \lambda \in \mathbb{F}_q^\times\}.$$

We conclude that

$$\{R_1, R_2, R_{s,t} \ : \ s, t \in \mathbb{F}_q^\times, \ s \ne t \text{ and } -st^{-1} \text{ is a non-square in } \mathbb{F}_q\}$$

is the set of regular G_β-orbits. Note that we are not claiming that the orbits denoted $R_{s,t}$ are all distinct.

Fix an element $\alpha \in \Omega$ with $\alpha \ne \beta$ and let $\Sigma(\alpha)$ be the set of neighbours of α in the Saxl graph $\Sigma(G)$. In order to verify $(\star\star)$, we need to show that $\Sigma(\alpha)$ meets every regular G_β-orbit. There are several cases to consider.

First assume $\alpha = \{\langle e_1 \rangle, \langle e_1 + be_2 \rangle\}$ for some $b \in \mathbb{F}_q^\times$. It is easy to see that each $\gamma \in R_1 \setminus \{\alpha\}$ is contained in $\Sigma(\alpha)$ and we also have $\{\langle e_2 \rangle, \langle e_1 + be_2 \rangle\} \in R_2 \cap \Sigma(\alpha)$. Now consider $R_{s,t}$, where $s, t \in \mathbb{F}_q^\times$ are distinct and $-st^{-1}$ is non-square. Note that either $-bs$ or bt^{-1} is a square in $\mathbb{F}_q$, so there are two cases to consider. If $-bs = \mu^2$ is a square then $b = -\mu^2 s^{-1}$ and

$$\{\langle e_1 - \mu^2 s^{-1}e_2 \rangle, \langle e_1 - \mu^2 t^{-1}e_2 \rangle\} \in R_{s,t} \cap \Sigma(\alpha).$$

On the other hand, if $bt^{-1} = \mu^2$ then $b = \mu^2 t$ and

$$\{\langle e_1 + \mu^2 se_2 \rangle, \langle e_1 + \mu^2 te_2 \rangle\} \in R_{s,t} \cap \Sigma(\alpha).$$

Therefore, $\Sigma(\alpha)$ meets every regular G_β-orbit as required.

A very similar argument applies when $\alpha = \{\langle e_2 \rangle, \langle e_1 + be_2 \rangle\}$ for some $b \in \mathbb{F}_q^\times$ and we omit the details.

Finally, let us assume $\alpha = \{\langle e_1 + s_0 e_2 \rangle, \langle e_1 + t_0 e_2 \rangle\}$, where $s_0, t_0 \in \mathbb{F}_q^\times$ are distinct. Note that $\{\langle e_i \rangle, \langle e_1 + s_0 e_2 \rangle\} \in R_i \cap \Sigma(\alpha)$ for $i = 1, 2$, so it just remains to show that $\Sigma(\alpha)$ meets each $R_{s,t}$. As before, either $-s_0 s$ or $s_0 t^{-1}$ is a square in $\mathbb{F}_q^\times$ and we can repeat the above argument in order to construct an element in $R_{s,t} \cap \Sigma(\alpha)$. $\square$

A weaker form of Conjecture 5.4 asserts that the Saxl graph of any base-two primitive group has diameter at most 2 (see [6, Conjecture 4.4]). Our final result in this section highlights the relationship between this assertion and Conjecture 5.8.

Proposition 5.13. *Let $L \leqslant \mathrm{Sym}(\Gamma)$ be a finite base-two primitive group. If the Saxl graph of every finite base-two primitive group has diameter at most 2, then either $r(L) = 1$, or L satisfies $(\star\star)$.*

Proof. We may assume $r = r(L) \geqslant 2$. Fix $\alpha, \beta \in \Gamma$. We need to show that $\Sigma(\alpha)$ meets all r regular L_β-orbits on Γ. Set $\Omega = \Gamma^r$, $P = S_r$ and consider $G = L \wr P \leqslant \mathrm{Sym}(\Omega)$, which is a base-two product type primitive group by Theorem 2.6. Fix $\rho = (\alpha, \ldots, \alpha)$ and $\sigma = (\beta, \ldots, \beta)$ in Ω.

First observe that $D(P) = r \geqslant 2$, so $\{\rho, \sigma\}$ is not a base for G by Lemma 4.1. Therefore, our hypothesis implies that there exists $\tau = (\gamma_1, \ldots, \gamma_r) \in \Omega$ such that both $\{\rho, \tau\}$ and $\{\sigma, \tau\}$ are bases for G (otherwise the distance between ρ and σ in $\Sigma(G)$ is at least 3). By applying Lemma 4.1 again, we deduce that each γ_i is contained in $\Sigma_L(\alpha) \cap \Sigma_L(\beta)$. Moreover, the γ_i are contained in distinct regular L_β-orbits since the only distinguishing partition for the action of P on $[r]$ is the partition into singletons. The result follows. $\square$

6. General product type groups

Up to now, we have focussed on product type groups of the form $G = L \wr P$. As one might expect, the study of bases in the general setting $G \leqslant L \wr P$ is more difficult and this is essentially unchartered territory. In this final section, we take the first steps in this direction by focussing on the special case where $P \leqslant G$, which already turns out to be rather challenging. Our main results are Theorems 6.4 and 6.11, which describe the groups with $b(G) = 2$ in certain families of product type groups with soluble point stabilisers. Note that Theorem 6.4 is stated as Theorem 9 in Section 1.

6.1. **Preliminaries.** Let us fix the set-up and notation we will work with throughout this section. As before, $G \leqslant L \wr P \leqslant \mathrm{Sym}(\Omega)$ is a product type primitive group on $\Omega = \Gamma_1 \times \cdots \times \Gamma_k = \Gamma^k$, with socle $T_1 \times \cdots \times T_k = T^k$ and point stabiliser H. Here $k \geqslant 2$, $P \leqslant S_k$ is transitive and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with socle T and point stabiliser J, which is either almost simple or diagonal type. In addition, we may assume P is the permutation group on $[k] = \{1, \ldots, k\}$ induced by the conjugation action of G on the set of k factors of the socle T^k. In view of Remark 2.4, we may (and will) also assume that L is the group induced by G on Γ_1. In particular, this means that both L and P are uniquely determined by G. As explained in Remark 2.5, if H is soluble then J and P are also soluble.

Since the case $G = L \wr P$ has been studied in Sections 3-5, we will assume $G < L \wr P$. More importantly, we will also assume that G contains P, which means that we adopt the following hypothesis for the remainder of this section (in particular, note that $L \neq T$).

Hypothesis 6.1. *$G \leqslant \mathrm{Sym}(\Omega)$ is a product type primitive group with $T \wr P < G < L \wr P$.*

In the setting of Hypothesis 6.1, we introduce some new notation. Given an element $g = (g_1, \ldots, g_k) \in L^k \cap G$, let $\tau(g)$ be the number of coordinates of g that are contained in T and set

$$\tau(G) = \max\{\tau(g) : g \in (L^k \cap G) \setminus T^k\} \in \{0, 1, \ldots, k-1\}. \tag{16}$$

For example, if $L = \langle T, x \rangle$ and $G = \langle T^k, (x, \ldots, x), P \rangle$, then $\tau(G) = 0$. Note that if $\tau(G) = k - 1$ and G satisfies Hypothesis 6.1, then $|L : T|$ is composite (indeed, if $|L : T|$ is a prime then we get $G = L \wr P$).

As before, let $r(L)$ and $r(T)$ denote the number of regular suborbits of L and T on Γ, respectively (recall that T acts transitively on Γ since L is primitive).

We begin with the following result, which gives a sufficient condition for a group satisfying Hypothesis 6.1 to admit a base of size 2.

Proposition 6.2. *Assume Hypothesis 6.1 and let $m \in \{1, \ldots, D(P)\}$ be minimal such that there exists a distinguishing partition $\{\pi_1, \ldots, \pi_{D(P)}\}$ for P with $|\bigcup_{i=1}^{m} \pi_i| > \tau(G)$. Then $b(G) = 2$ if*

    (i) $r(L) \geqslant m$; *and*

    (ii) $r(T) \geqslant m(|L : T| - 1) + D(P)$.

Proof. Suppose the bounds in (i) and (ii) are satisfied. Set $D = D(P)$ and fix an element $\alpha = (\alpha_0, \ldots, \alpha_0) \in \Omega$ for some $\alpha_0 \in \Gamma$. Since $r(L) \geqslant m$, we may choose elements $\gamma_1, \ldots, \gamma_m$ in Γ that are contained in distinct regular L_{α_0}-orbits. Now each of these L_{α_0}-orbits is a union of $|L : T|$ regular T_{α_0}-orbits, so the bound in (ii) implies that we can find additional points $\gamma_{m+1}, \ldots, \gamma_D$ in Γ such that each element in $\{\gamma_1, \ldots, \gamma_D\}$ is contained in a distinct regular T_{α_0}-orbit. Define $\beta = (\beta_1, \ldots, \beta_k) \in \Omega$, where $\beta_j = \gamma_i$ if $j \in \pi_i$. We claim that $\{\alpha, \beta\}$ is a base for G.

Let $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1, \ldots, z_k) \in L^k \cap G$ and $\sigma \in P$. Recall that $\tau(z)$ denotes the number of coordinates z_i that are contained in T and observe that $z \in T^k$ if $\tau(z) > \tau(G)$ (see (16)). By Lemma 4.1, we see that $\{\alpha, \beta\}$ is a base for $T \wr P$, so it suffices to show that $\tau(z) > \tau(G)$.

Fix $j \in \pi_1$ and notice that $z_j \in L_{\alpha_0}$ since x fixes α. Next observe that the j^σ-th coordinate of β^x is $\beta_j^{z_j} = \gamma_1^{z_j}$, which is equal to $\beta_{j^\sigma} \in \{\gamma_1, \ldots, \gamma_D\}$ since x fixes β. By construction, none of the elements $\gamma_2, \ldots, \gamma_D$ are contained in the L_{α_0}-orbit of γ_1, whence $\beta_{j^\sigma} = \gamma_1$ and thus $z_j \in L_{\alpha_0} \cap L_{\gamma_1} = 1$. In the same way, we deduce that $z_j = 1$ for all $j \in \bigcup_{i=1}^{m} \pi_i$ and thus $\tau(z) \geqslant |\bigcup_{i=1}^{m} \pi_i| > \tau(G)$. The result follows. $\qquad\square$

Remark 6.3. Note that Proposition 6.2 can be applied when $G = L \wr P$ and $L \neq T$. Here $\tau(G) = k - 1$, so $m = D(P)$ and the proposition asserts that $b(G) = 2$ if $r(L) \geqslant D(P)$ and $r(T) \geqslant |L : T|$. Here the condition $r(L) \geqslant D(P)$ coincides with the one in Theorem 2.6, while the bound $r(T) \geqslant |L : T|$ always holds when $b(L) = 2$. So in some sense, Proposition 6.2 can be viewed as a generalisation of Theorem 2.6 for base-two groups. However, it is worth noting that there are groups with $b(G) = 2$ that do not satisfy the bounds labelled (i) and (ii) in the proposition. For example, the proof of Theorem 6.4 shows that there are groups G satisfying Hypothesis 6.1 with $k = m = 2$, $r(L) = 1$ and $b(G) = 2$.

Let G be a group satisfying Hypothesis 6.1 and note that $b(G) = 2$ only if $b(T \wr P) = 2$, so we are interested in the groups with $b(T) = 2$. Moreover, in view of [1, Theorem 2.13], we may assume $r(T) \geqslant D(P)$. Recall that if H is soluble, then L is almost simple with soluble point stabilisers and as a consequence of [4, Theorem 2] we observe that $b(L) \in \{2, 3\}$. So in the case where G has soluble point stabilisers, as in the two main results of this section, there are two cases to consider according to the base size of L on Γ. To simplify the analysis, we will focus on the groups with $b(L) = 2$, which allows us to bring Proposition 6.2 into play. However, it is worth noting that there are groups of this form with $b(L) = 3$ and $b(G) = 2$. Indeed, we refer the reader to Example 6.12 at the end of the section for an infinite family of groups G with soluble point stabilisers where we have $b(L) = 3$ and $b(G) = 2$.

6.2. **Base-two groups with $k = 2$.** Our first main result is Theorem 6.4 below, which is stated as Theorem 9 in Section 1. Here we assume $k = b(L) = 2$, so $P = S_2$ and $D(P) = 2$.

If $r(L) \geqslant 2$ then $b(L \wr P) = 2$ by Theorem 2.6, so we may as well assume $r(L) = 1$. Define $\tau(G)$ as in (16) and note that $\tau(G) \in \{0, 1\}$. If $\tau(G) = 0$, then $m = 1$ in Proposition 6.2 and we deduce that $b(G) = 2$ if $r(T) \geqslant |L : T| + 1$ (recall that the slightly weaker bound $r(T) \geqslant |L : T|$ always holds when $b(L) = 2$). On the other hand, if $\tau(G) = 1$ then $m = 2$ and thus Proposition 6.2 is not useful when $r(L) = 1$. Also recall that $|L : T|$ is composite if $\tau(G) = 1$ (otherwise $G = L \wr P$).

Theorem 6.4. *Assume Hypothesis 6.1, where $k = b(L) = 2$, H is soluble and J is a point stabiliser in L. Then $b(G) \leqslant 3$, with equality if and only if $|L \wr P : G| = 2$ and one of the following holds:*

    (i) *$(L, J) = (\mathrm{M}_{10}, 5{:}4)$ or $(\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$.*

    (ii) *$L = \mathrm{PGU}_4(3)$ and J is of type $\mathrm{GU}_1(3) \wr S_4$.*

Proof. Here $P = S_2$ and $D(P) = 2$. By Lemma 3.1 we have $b(L \wr P) \leqslant b(L) + 1$ and thus $b(G) \leqslant 3$. As explained in Remark 2.5, we note that J is soluble and thus L is almost simple. If $r(L) \geqslant 2$ then $b(L \wr P) = 2$ by Theorem 2.6, so we may assume $r(L) = 1$ and then inspect the possibilities for (L, J) recorded in Table 4. As discussed above, Proposition 6.2 implies that $b(G) = 3$ only if $r(T) = |L : T|$ or $\tau(G) = 1$, so there are two cases to consider.

First assume $r(T) = |L : T|$. By inspecting Table 4, we see that $(L, J) = (\mathrm{M}_{10}, 5{:}4)$ or $(L, J) = (\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$, so in both cases we have $|L : T| = 2$ and $|L \wr P : G| = 2$. More precisely, if we write $L = \langle T, a \rangle$ then we may assume $G = \langle T^2, (a, a), P \rangle$. Using MAGMA, we can construct G as a permutation group on $\Omega = \Gamma^2$ with point stabiliser H and we can then find a complete set R of (H, H) double coset representatives. In both cases, it is routine to check that $|HxH| < |H|^2$ for all $x \in R$ and we conclude that $b(G) = 3$ as claimed.

For the remainder, let us assume $\tau(G) = 1$ and recall that $|L : T| \geqslant 4$ is composite since G is a proper subgroup of $L \wr P$. By inspecting Table 4 we deduce that there are four possibilities for (L, J):

    (a) $L = \mathrm{U}_3(5){:}S_3$ and J is of type $\mathrm{GU}_1(5) \wr S_3$.

    (b) $L = \mathrm{L}_3(4){:}D_{12}$ and J is of type $\mathrm{GL}_1(4^3)$.

    (c) $L = \mathrm{P\Omega}_8^+(3){:}2^2$ and J is of type $\mathrm{O}_4^+(3) \wr S_2$.

    (d) $L = \mathrm{U}_4(3){:}[4]$ and J is of type $\mathrm{GU}_1(3) \wr S_4$.

In cases (a) and (b), we can use MAGMA to check that $b(G) = 2$ (here we construct G and H as above, and then we use random search to find an element $g \in G$ with $H \cap H^g = 1$). Now let us turn to cases (c) and (d), so $|L : T| = 4$ and $|L \wr P : G| \in \{2, 4, 8\}$. In fact, one can check that the condition $\tau(G) = 1$ forces $|L \wr P : G| = 2$. More precisely, if $L = T{:}\langle a, b \rangle = T{:}2^2$ then up to permutation isomorphism, we may assume that

$$G = \langle T^2, (a, a), (b, 1), P \rangle. \tag{17}$$

Similarly, if $L = \mathrm{PGU}_4(3) = T{:}\langle a \rangle$, then we can take

$$G = \langle T^2, (a, a), (a^2, 1), P \rangle. \tag{18}$$

First assume $L = T{:}\langle a, b \rangle = T{:}2^2$, so (17) holds and $T = \mathrm{P\Omega}_8^+(3)$ or $\mathrm{U}_4(3)$. We claim that $b(G) = 2$. To see this, fix $\alpha_0 \in \Gamma$ and let $\gamma_1, \ldots, \gamma_t$ be representatives of the regular T_{α_0}-orbits on Γ, where $t = r(T)$ (as recorded in Table 4, we have $t = 12$ if $T = \mathrm{P\Omega}_8^+(3)$ and $t = 11$ for $T = \mathrm{U}_4(3)$). We may assume that $L_{\alpha_0} \cap L_{\gamma_1} = 1$ and $|L_{\alpha_0} \cap L_{\gamma_2}| = 2$ (the existence of γ_2 can be checked using MAGMA). Now $T_{\alpha_0} \cap T_{\gamma_2} = 1$, so without loss of generality we may assume that $\{\alpha_0, \gamma_2\}$ is a base for $T{:}\langle b \rangle$. Suppose $x = (z_1, z_2)\sigma \in G$ fixes $\alpha = (\alpha_0, \alpha_0)$ and $\beta = (\gamma_1, \gamma_2)$, where $z_1, z_2 \in L$ and $\sigma \in P$. Then $z_i \in L_{\alpha_0}$ for $i = 1, 2$ and we note that $\sigma = 1$ since γ_1 and γ_2 are contained in distinct L_{α_0}-orbits. Therefore,

$z_1 \in L_{\alpha_0} \cap L_{\gamma_1} = 1$ and thus $z_1 = 1$. From the description of G in (17), it follows that $z_2 \in T{:}\langle b \rangle$ fixes α_0 and γ_2, whence $z_2 = 1$ and thus $x = 1$. This justifies the claim.

Finally, let us assume $L = \mathrm{PGU}_4(3) = T{:}\langle a \rangle$, so the structure of G is given in (18). We claim that $b(G) = 3$. As before, fix $\alpha_0 \in \Gamma$ and set $\alpha = (\alpha_0, \alpha_0)$ and $\beta = (\gamma_1, \gamma_2)$, where γ_1 and γ_2 are contained in regular T_{α_0}-orbits. It suffices to show that the pointwise stabiliser of α and β in G is non-trivial. It will be useful to observe that a given element $(z_1, z_2) \in L^2$ is contained in G if and only if $z_1 z_2 \in T{:}\langle a^2 \rangle$.

First assume $\{\alpha_0, \gamma_1\}$ is not a base for L. Then using MAGMA we see that $|L_{\alpha_0} \cap L_{\gamma_1}| \in \{2, 4\}$, so there is an involution $y \in L$ fixing α_0 and γ_1. Since every involution in L is contained in $T{:}\langle a^2 \rangle$, it follows that $(y, 1) \in G$ fixes α and β. An entirely similar argument applies if $\{\alpha_0, \gamma_2\}$ is not a base for L.

Finally, suppose $\{\alpha_0, \gamma_1\}$ and $\{\alpha_0, \gamma_2\}$ are both bases for L, which means that γ_1 and γ_2 are contained in the unique regular L_{α_0}-orbit on Γ. Therefore, there exists $z_1 \in L_{\alpha_0}$ such that $\gamma_1^{z_1} = \gamma_2$ and thus $(z_1, z_1^{-1})\sigma \in G$ is a non-trivial element fixing α and β, where $\sigma = (1, 2) \in P$. This completes the proof of the theorem. $\qquad\square$

6.3. **Base-two groups with $\tau(G) = 0$.** For the remainder of Section 6, we will continue to assume that Hypothesis 6.1 holds and $b(L) = 2$, but we will not impose any conditions on k. In exchange, we will focus on the groups with $\tau(G) = 0$ (see (16)), which is a natural restriction on the structure of G. In particular, this means that if $x = z\sigma \in G$, where $z = (z_1, \ldots, z_k) \in L^k \cap G$ and $\sigma \in P$, then either $z \in T^k$ or $z_j \in L \setminus T$ for all j.

Our main result in this setting is Theorem 6.11 and the proof will require several preliminary results. We begin with an easy corollary of Proposition 6.2.

Corollary 6.5. *Assume Hypothesis 6.1, where $b(L) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then*
$$|L : T| \leqslant r(T) \leqslant |L : T| + D(P) - 2.$$

Proof. This follows immediately from Proposition 6.2, noting that $m = 1$ in the statement of the proposition. $\qquad\square$

Remark 6.6. Let us apply Corollary 6.5 in the case where H is soluble. Suppose $b(G) \geqslant 3$, so $r(T) \leqslant |L : T| + D(P) - 2$ by the corollary. Now $r(T) \geqslant r(L)|L : T|$ and the solubility of P implies that $D(P) \leqslant 5$ (see Theorem 2.1), whence
$$(r(L) - 1)|L : T| \leqslant D(P) - 2 \leqslant 3$$
and either $r(L) = 1$, or $r(L) = 2$ and $|L : T| \in \{2, 3\}$. In particular, the possibilities for (L, J) can be read off from Table 4 and we find that $r(L) = 2$, $|L : T| \in \{2, 3\}$ and $r(T) \leqslant |L : T| + 3$ if and only if one of the following holds:

(a) $L = \mathrm{L}_3(3).2$ and J is of type $\mathrm{O}_3(3)$.
(b) $L = \mathrm{L}_2(27).3$ and J is of type $\mathrm{GL}_1(27^2)$.
(c) $(L, J) = (\mathrm{M}_{10}, SD_{16})$.

Note that if P is primitive (as in Theorem 6.11), then $D(P) \leqslant 4$ by Theorem 2.3, so the corollary implies that $r(T) \leqslant |L : T| + 2$ and this eliminates cases (a) and (b).

In order to state our next result, we define the following condition on the group $P \leqslant S_k$, with respect to a fixed integer m in the range $D(P) \leqslant m \leqslant k$:

$$\begin{array}{c} \textit{If } \{\pi_1, \ldots, \pi_m\} \textit{ is a distinguishing partition for } P, \\ \textit{then for all } i, \textit{ there exists } \rho \in P \textit{ such that } \pi_i \cap \pi_i^\rho \textit{ is empty.} \end{array} \qquad (\dagger)$$

Note that if there exists a distinguishing partition $\{\pi_1, \ldots, \pi_m\}$ for P with $|\pi_i| > k/2$ for some i, then $\pi_i \cap \pi_i^\rho$ is non-empty for all $\rho \in P$ and thus (P, m) does not satisfy $(\dagger)$.

Remark 6.7. Recall that t_m is the number of (unordered) distinguishing partitions for P with m non-empty parts. As noted in Section 4, if $t_m = |P|/m!$ then any two parts in such a partition are in the same P-orbit and thus (P, m) satisfies the condition in $(\dagger)$.

Proposition 6.8. *Assume Hypothesis 6.1, where $b(L) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then (†) holds for all $D(P) \leqslant m \leqslant \min\{k, r(T)\}$.*

Proof. This is similar to the proof of Proposition 6.2. Suppose there exists a distinguishing partition $\{\pi_1, \ldots, \pi_m\}$ for P such that $D(P) \leqslant m \leqslant r(T)$ and $\pi_1 \cap \pi_1^\rho$ is non-empty for all $\rho \in P$. Fix $\alpha_0 \in \Gamma$. Since $r(T) \geqslant m$, we can choose elements $\gamma_1, \ldots, \gamma_m$ that are contained in distinct regular T_{α_0}-orbits on Γ, so each pair $\{\alpha_0, \gamma_i\}$ is a base for T. In addition, we may assume that $\{\alpha_0, \gamma_1\}$ is a base for L. Define $\alpha = (\alpha_0, \ldots, \alpha_0)$ and $\beta = (\beta_1, \ldots, \beta_k)$ as elements of Ω, where $\beta_j = \gamma_i$ if $j \in \pi_i$. In order to prove the proposition, it suffices to show that $\{\alpha, \beta\}$ is a base for G.

Let $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1, \ldots, z_k) \in L^k \cap G$ and $\sigma \in P$. Note that each z_j is contained in L_{α_0}. If $z \in T^k$ then $x \in T \wr P$ and thus $x = 1$ since we know that $\{\alpha, \beta\}$ is a base for $T \wr P$ by Lemma 4.1. Therefore, since $\tau(G) = 0$, we may assume $z_j \in L \setminus T$ for all j.

Since $\pi_1 \cap \pi_1^\sigma$ is non-empty, there exists $j \in \pi_1$ such that $j^\sigma \in \pi_1$. Then $\beta_j = \gamma_1$ and by considering the j^σ-th coordinate of β^x we deduce that $\gamma_1 = \beta_{j^\sigma} = \beta_j^{z_j} = \gamma_1^{z_j}$. Therefore, $z_j \in L_{\alpha_0} \cap L_{\gamma_1} = 1$ and thus $z_j = 1$, which contradicts the fact that $z_j \in L \setminus T$. The result follows. $\qquad\square$

Notice that P is primitive in the statement of Theorem 6.11. Therefore, in view of Theorem 2.3, we have a special interest in the case $D(P) = 2$, which means that P has a regular orbit on the power set of $[k] = \{1, \ldots, k\}$. This leads us naturally to consider the following condition, which coincides with (†) when $m = 2$:

$$\begin{array}{c} \textit{If the setwise stabiliser of } \Lambda \subseteq [k] \textit{ in } P \textit{ is trivial,} \\ \textit{then } \Lambda^\sigma = [k] \setminus \Lambda \textit{ for some } \sigma \in P. \end{array} \qquad (\ddagger)$$

Clearly, if $D(P) = 2$ then (‡) holds only if k is even and every subset of $[k]$ with trivial setwise stabiliser in P has size $k/2$. In other words, (‡) holds only if P has no regular orbit on the set X defined in (14). Therefore, if P is primitive and $D(P) = 2$, then Proposition 4.13 implies that (‡) holds if and only if $(k, P) = (2, S_2)$ or $(16, 2^4{:}O_4^-(2))$. We will return to this observation in the proof of Theorem 6.11 below.

The following result is an immediate corollary of Proposition 6.8.

Corollary 6.9. *Assume Hypothesis 6.1, where $b(L) = D(P) = 2$ and $\tau(G) = 0$. If $b(G) \geqslant 3$, then (‡) holds.*

The final ingredient for the proof of Theorem 6.11 is provided by the following lemma.

Lemma 6.10. *Assume Hypothesis 6.1, where $b(L) = |L : T| = 2$, $\tau(G) = 0$ and $P = S_{r(T)}$. Then $b(G) \geqslant 3$.*

Proof. Set $k = r(T)$ and fix $\alpha_0 \in \Gamma$. Recall that an element $z = (z_1, \ldots, z_k) \in L^k$ is contained in G if and only if $z \in T^k$ or $z_i \in L \setminus T$ for all i. In view of Lemma 4.1, it suffices to show that $\alpha = (\alpha_0, \ldots, \alpha_0)$ and $\beta = (\gamma_1, \ldots, \gamma_k)$ do not form a base for G, where the γ_i are contained in distinct regular T_{α_0}-orbits.

Since $|L : T| = 2$, each regular L_{α_0}-orbit is a union of two regular T_{α_0}-orbits. This allows us to define $r = r(L)$ distinct pairs $\{s, t\} \subseteq \{1, \ldots, k\}$, where $\{s, t\}$ is a pair if and only if γ_s and γ_t are in the same regular L_{α_0}-orbit. Let $\{s_1, t_1\}, \ldots, \{s_r, t_r\}$ be the pairs arising in this way. For each $i \in \{1, \ldots, r\}$, there exist $z_{s_i}, z_{t_i} \in L_{\alpha_0}$ such that $\gamma_{s_i}^{z_{s_i}} = \gamma_{t_i}$ and $\gamma_{t_i}^{z_{t_i}} = \gamma_{s_i}$. In addition, if $\ell \notin \{s_1, t_1, \ldots, s_r, t_r\}$ then there exists $1 \neq z_\ell \in L_{\alpha_0}$ such that $\gamma_\ell^{z_\ell} = \gamma_\ell$. By construction, all of the elements z_{s_i}, z_{t_i} and z_ℓ are contained in $L \setminus T$. Therefore, if we define $z = (z_1, \ldots, z_k) \in L^k$, then $z \in G$. Finally, we note that $1 \neq z\sigma \in G_\alpha \cap G_\beta$, where $\sigma = (s_1, t_1) \cdots (s_r, t_r) \in P$, and we conclude that $\{\alpha, \beta\}$ is not a base for G. $\qquad\square$

$r(T)$	L	Type of J	Conditions
2	M_{10}	$5{:}4$	
	$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	
3	$\mathrm{L}_3(4).2$	$\mathrm{GU}_3(2)$	$L \neq \mathrm{P\Sigma L}_3(4)$
	$\mathrm{PGL}_2(11)$	$2^{1+2}_-.\mathrm{O}^-_2(2)$	
	$\mathrm{PGL}_2(7)$	D_{12}	
4	$\mathrm{PGL}_2(q)$	$D_{2(q-1)}$	$q \in \{9, 11\}$
	$G_2(3).2$	$\mathrm{SL}_2(3)^2$	
	S_7	$\mathrm{AGL}_1(7)$	
	M_{10}	SD_{16}	

TABLE 2. The groups (L, J) in Theorem 6.11

Theorem 6.11. *Assume Hypothesis 6.1, where $b(L) = 2$, P is primitive, $\tau(G) = 0$ and H is soluble. Then $b(G) \leqslant 3$, with equality if and only if (L, J) is one of the cases in Table 2 and either $r(T) < D(P)$, or $P = S_k$, $k \in \{2, 3, 4\}$ and $r(T) = D(P) = k$.*

Proof. First note that L is almost simple with soluble point stabiliser J, and P is also soluble (see Remark 2.5). By Lemma 3.1 we have $b(L \wr P) \leqslant b(L) + 1$ and thus $b(G) \leqslant 3$. Since P is primitive, Theorem 2.3 implies that either $D(P) = 2$, or one of the following holds:

(a) $D(P) = 3$ and $(k, P) = (4, A_4)$, $(3, S_3)$ or one of 8 cases listed in [37, Theorem 2] with P soluble.

(b) $D(P) = 4$ and $(k, P) = (4, S_4)$.

First assume $r(T) < D(P)$. Here [1, Theorem 2.13] gives $b(T \wr P) \geqslant 3$, so $b(G) = 3$ and the possibilities for (L, J) can be read off from Table 4, noting that $L \neq T$ since we are assuming G satisfies Hypothesis 6.1. In this way, we obtain the cases recorded in Table 2 with $r(T) \in \{2, 3\}$.

For the remainder, we will assume $r(T) \geqslant D(P)$. We now divide the proof into three cases, according to $D(P)$.

Case 1. $D(P) = 2$.

First assume $D(P) = 2$. By combining Theorem 2.6 and Corollary 6.5, we deduce that $b(G) = 3$ only if $r(L) = 1$ and $r(T) = |L : T|$. Therefore, by inspecting Table 4 we see that $(L, J) = (\mathrm{M}_{10}, 5{:}4)$ or $(\mathrm{J}_2.2, 5^2{:}(4 \times S_3))$ are the only possibilities, and in both cases we have $|L : T| = 2$. If $b(G) = 3$ then Corollary 6.9 implies that the condition (‡) holds, which means that P has no regular orbit on the set X defined in (14). In addition, since P is soluble, Proposition 4.13 implies that $(k, P) = (2, S_2)$ and we conclude that $b(G) = 3$ via Lemma 6.10.

Case 2. $D(P) = 3$.

Next assume $D(P) = 3$, so the possibilities for (k, P) are described in case (a) above. Suppose $b(G) = 3$ and first observe that Proposition 6.8 implies that (†) holds with $m = 3$. By considering the cases in (a), with the aid of MAGMA it is straightforward to check that (†) holds with $m = 3$ if and only if $(k, P) = (3, S_3)$, $(4, A_4)$ or $(9, \mathrm{AGL}_2(3))$.

Next observe that $r(T) = |L : T|$ or $|L : T| + 1$ by Corollary 6.5. Therefore, $r(L) = 1$ and by inspecting Table 4 we deduce that (L, J) is one of the three cases recorded in Table 2 with $r(T) = |L : T| + 1 = 3$. In particular, if $(k, P) = (3, S_3)$ then $b(G) = 3$ in both cases by Lemma 6.10. We now consider the two remaining possibilities for (k, P) in turn.

Suppose $(k, P) = (9, \mathrm{AGL}_2(3))$. Using MAGMA, we can find a distinguishing partition $\{\pi_1, \pi_2, \pi_3\}$ for P such that $|\pi_i| = i + 1$ for all i. Let (L, J) be one of the relevant cases

in Table 2 and fix $\alpha_0 \in \Gamma = L/J$. Since $r(T) = 3$, there exist points $\gamma_1, \gamma_2, \gamma_3$ that are contained in distinct regular T_{α_0}-orbits on Γ. In addition, we may assume that $\{\alpha_0, \gamma_1\}$ is not a base for L, whereas γ_2 and γ_3 are in the unique regular L_{α_0}-orbit on Γ. Set $\alpha = (\alpha_0, \ldots, \alpha_0)$ and $\beta = (\beta_1, \ldots, \beta_k)$ in $\Omega = \Gamma^k$, where $\beta_j = \gamma_i$ if $j \in \pi_i$. We claim that $\{\alpha, \beta\}$ is a base for G, which is incompatible with our assumption that $b(G) = 3$. To see this, suppose $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1, \ldots, z_k) \in L^k \cap G$ and $\sigma \in P$. Suppose $j \in \pi_1$, so $\beta_j = \gamma_1$. Since γ_2 and γ_3 are not in the L_{α_0}-orbit of γ_1, it follows that $\beta_j^{z_j} = \gamma_1$. Therefore, σ fixes π_1 and $\pi_2 \cup \pi_3$ (setwise). As a consequence, since $|\pi_2| = 3$ and $|\pi_3| = 4$, we deduce that there exists $j \in \pi_3$ such that $j^\sigma \in \pi_3$. Therefore, $z_j \in L_{\alpha_0} \cap L_{\gamma_3}$ and thus $z_j = 1$. At this point, the condition $\tau(G) = 0$ forces $z \in T^k$ and thus Lemma 4.1 implies that $x = 1$. Therefore, $\{\alpha, \beta\}$ is indeed a base for G and so the case $(k, P) = (9, \mathrm{AGL}_2(3))$ is eliminated.

An almost identical argument also eliminates the case $(k, P) = (4, A_4)$, working with a distinguishing partition $\{\pi_1, \pi_2, \pi_3\}$ for P with $|\pi_1| = |\pi_2| = 1$ and $|\pi_3| = 2$. We omit the details.

Case 3. $D(P) = 4$.

Finally, let us assume $D(P) = 4$ and $b(G) = 3$, in which case $(k, P) = (4, S_4)$ (see case (b) above) and Corollary 6.5 implies that $|L : T| \leqslant r(T) \leqslant |L : T| + 2$. Therefore $r(T) \leqslant 2|L : T|$ and thus $r(L) \in \{1, 2\}$. By inspecting Table 4, we deduce that either (L, J) is one of the cases in Table 2 with $r(T) = |L : T| + 2 = 4$, or $L = \Omega_8^+(2){:}3$ and J is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$. In the former case, Lemma 6.10 shows that $b(G) = 3$, so it just remains to eliminate the latter possibility.

Suppose $L = T{:}\langle a \rangle = \Omega_8^+(2){:}3$ and J is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$, so $r(L) = 1$ and $r(T) = 5$. Since $|L : T| = 3$ is a prime and we are assuming that $\tau(G) = 0$ and $P = S_4$, it follows that

$$G = \langle T^4, (a, a, a, a), P \rangle,$$

so an element $(z_1, z_2, z_3, z_4) \in L^4$ is contained in G if and only if each z_i is in the same coset of T in L. Fix $\alpha_0, \gamma_1, \ldots, \gamma_4 \in \Gamma$, where the γ_i are contained in distinct regular T_{α_0}-orbits and $\{\alpha_0, \gamma_i\}$ is a base for L if and only if $i \in \{1, 2\}$. Notice that if $i \in \{3, 4\}$ then $|L_{\alpha_0} \cap L_{\gamma_i}| = 3$, which implies that the L_{α_0}-orbit and T_{α_0}-orbit of γ_i are equal (in particular, γ_3 and γ_4 are in distinct L_{α_0}-orbits). Set $\alpha = (\alpha_0, \alpha_0, \alpha_0, \alpha_0)$ and $\beta = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ in $\Omega = \Gamma^4$. We claim that $\{\alpha, \beta\}$ is a base for G.

Assume $x \in G_\alpha \cap G_\beta$ and write $x = z\sigma$, where $z = (z_1, z_2, z_3, z_4) \in L^4 \cap G$ and $\sigma \in P$. Since none of the points γ_1, γ_2 and γ_4 are in the same L_{α_0}-orbit as γ_3, we deduce that $3^\sigma = 3$. Similarly, $4^\sigma = 4$. Suppose $\sigma = (1, 2)$. Then $\gamma_1^{z_1} = \gamma_2$ and $\gamma_2^{z_2} = \gamma_1$, which implies that $z_1, z_2 \in L \setminus T$. Moreover, $z_1 z_2 \in L_{\alpha_0} \cap L_{\gamma_1} = 1$, so $z_1 = z_2^{-1}$ and we deduce that z_1 and z_2 are contained in different cosets of T in L. But this means that $z \notin G$ and we have reached a contradiction. This forces $\sigma = 1$. Finally, since $\{\alpha_0, \gamma_1\}$ is a base for L we deduce that $z_1 = 1$ and thus $z \in T^4$. Since each $\{\alpha_0, \gamma_i\}$ is a base for T, we conclude that $z = 1$ and the proof of both the claim and the theorem is complete. $\qquad\square$

6.4. **Final remarks.** We conclude by briefly discussing the general problem of determining the base-two product type groups with soluble point stabilisers. Let $G \leqslant L \wr P$ be such a group with socle T^k, and adopt all the usual notation as before. The case where $G = L \wr P$ is handled in Theorem 2, so we may assume $G < L \wr P$ and $b(L \wr P) \geqslant 3$. Continuing with the main theme of Section 6, let us also assume that Hypothesis 6.1 holds. Here $L \neq T$ and $b(G) = 2$ only if $b(T \wr P) = 2$, so $r(T) \geqslant D(P)$ and we deduce that $b(L) \in \{2, 3\}$ as a consequence of [4, Theorem 2]. In this setting, we have handled the cases

   (a) $b(L) = k = 2$ (see Theorem 6.4); and
   (b) $b(L) = 2$, P is primitive and $\tau(G) = 0$ (see Theorem 6.11).

So even under the assumption $b(L) = 2$, there is more work to be done here and it would be interesting to see if it is possible to relax the conditions on P and $\tau(G)$ in case (b). For example, it might be fruitful to consider the groups with $\tau(G) = k - 1$ as a starting point.

As the following example demonstrates, we can also find base-two groups under Hypothesis 6.1 when $b(L) = 3$.

Example 6.12. Take $L = \mathrm{P\Gamma L}_2(q) = T{:}\langle a, b \rangle = T{:}2^2$ and let J be a maximal subgroup of type $\mathrm{GL}_1(q) \wr S_2$, where $q = p^2$, $p \geqslant 3$ is a prime and $\mathrm{PGL}_2(q) = T{:}\langle a \rangle$ and $\mathrm{P\Sigma L}_2(q) = T{:}\langle b \rangle$. By [4, Lemma 4.7] we have $b(L) = 3$ and $b(\mathrm{PGL}_2(q)) = b(\mathrm{P\Sigma L}_2(q)) = 2$. Set $(k, P) = (2, S_2)$ and consider

$$G = \langle T^2, (a, a), (b, b), P \rangle$$

as a primitive product type group on $\Omega = \Gamma^2$, where $\Gamma = L/J$.

We may identify Γ with the set of distinct pairs of 1-dimensional subspaces of the natural module for T. Given this identification, a precise description of the 2-element bases for $\mathrm{PGL}_2(q)$ and $\mathrm{P\Sigma L}_2(q)$ is presented in [10, Section 4.1] and this allows us to choose bases $\{\alpha_0, \gamma_1\}$ and $\{\alpha_0, \gamma_2\}$ for $\mathrm{PGL}_2(q)$ and $\mathrm{P\Sigma L}_2(q)$, respectively, where γ_1 and γ_2 are contained in distinct L_{α_0}-orbits. In addition, notice that $\{\alpha_0, \gamma_2\}$ is a base for $T{:}\langle ab \rangle$ by [10, Lemma 4.5]. Set $\alpha = (\alpha_0, \alpha_0)$ and $\beta = (\gamma_1, \gamma_2)$. We claim that $\{\alpha, \beta\}$ is a base for G and thus $b(G) = 2$. To see this, suppose $x = (z_1, z_2)\sigma \in G$ fixes α and β. Then each z_i is contained in L_{α_0} and thus $\sigma = 1$ since γ_1 and γ_2 are in distinct L_{α_0}-orbits. Since $x \in G$, we may write $z_i = t_i c$ with $t_i \in T$ and $c \in \{1, a, b, ab\}$. If $c = 1$ then $z_i \in T_{\alpha_0} \cap T_{\gamma_i} = 1$ and thus $x = 1$. If $c = a$ then $z_1 \in \mathrm{PGL}_2(q)_{\alpha_0} \cap \mathrm{PGL}_2(q)_{\gamma_1} = 1$, which is a contradiction since $z_1 \in L \setminus T$. An entirely similar argument applies if $c \in \{b, ab\}$ and the proof of the claim is complete.

Notice that $|L : T| = 4$ in Example 6.12. By the following result, there are no examples with $b(L) = 3$, $|L : T| = 2$ and $b(G) = 2$. Here there is no need to assume that G has soluble point stabilisers and it is worth noting that the same proof goes through under the weaker hypothesis $T^k < L^k \cap G$.

Proposition 6.13. *Assume Hypothesis 6.1, with $b(L) \geqslant 3$ and $|L : T| = 2$. Then $b(G) \geqslant 3$.*

Proof. We may as well assume $b(T) = 2$. Fix $\alpha_0 \in \Gamma$ and set $\alpha = (\alpha_0, \ldots, \alpha_0) \in \Omega$. It suffices to show that $\{\alpha, \beta\}$ is not a base for G, where $\beta = (\gamma_1, \ldots, \gamma_k)$ and each γ_i is contained in a regular T_{α_0}-orbit. Since $b(L) \geqslant 3$, for each i there exists $x_i \in L \setminus T$ fixing both α_0 and γ_i.

Fix $z = (z_1, \ldots, z_k) \in (L^k \cap G) \setminus T^k$ and define a subset A of $[k]$ such that $i \in A$ if and only if $z_i \notin T$. Note that A is non-empty since $z \notin T^k$. Set $y = (y_1, \ldots, y_k) \in L^k$, where $y_i = x_i$ if $x \in A$, otherwise $y_i = 1$, and observe that y is non-trivial and it fixes α and β. Finally, since $|L : T| = 2$ we deduce that $yz \in T^k \leqslant G$, so $y \in G_\alpha \cap G_\beta$ and the result follows. $\square$

By the proposition, if G has soluble point stabilisers and $b(L) = 3$, then $b(G) = 2$ only if $b(T) = 2$, $r(T) \geqslant D(P)$ and $|L : T| \geqslant 3$. Since L is almost simple, the possibilities for (L, J) can be read off from [4, Tables 4-7], noting that $b(T) = 2$ only if $\log_m |T| < 2$, where $m = |\Gamma|$. In [4, Table 4], we deduce that the only possibility is $L = A_6.2^2$ with $J = [32]$ or $D_{20}.2$ (here L is isomorphic to $\mathrm{P\Gamma L}_2(9)$ and J is of type $\mathrm{GL}_1(9) \wr S_2$ or $\mathrm{GL}_1(9^2)$, respectively). One can check that no examples arise in [4, Tables 5 and 6], while the relevant possibilities for (L, J) in [4, Table 7] are recorded in Table 3 (here we implicitly assume the additional condition $|L : T| \geqslant 3$). For the values of $r(T)$ in the first two rows, we have $(a, b) = (7, 1)$ if $q \equiv 1 \pmod 4$, otherwise $(a, b) = (5, 3)$ (see Remark 3.4 and the proof of [9, Lemma 7.9]).

It is straightforward to check that none of these possibilities correspond to cases in Table 5, which implies that $\mathrm{reg}(L, 3) \geqslant 5$ and we obtain the following result via Theorem 2.6.

T	Type of J	$r(T)$	Conditions
$L_2(q)$	$GL_1(q) \wr S_2$	$(q+a)/4$	q odd, $PGL_2(q) < L$
	$GL_1(q^2)$	$(q-b)/4$	q odd, $PGL_2(q) \leqslant L$
$L_3(4)$	$GU_3(2)$	3	
$L_4(3)$	$O_4^+(3)$	6	$L = T.2^2$
$U_4(3)$	$GU_1(3) \wr S_4$	11	$L = T.D_8$
$\Omega_8^+(2)$	$O_2^-(2) \times GU_3(2)$	5	$L = T.S_3$
$P\Omega_8^+(3)$	$O_4^+(3) \wr S_2$	12	$|L : T| \geqslant 6$

TABLE 3. The groups (L, J) in Proposition 6.14(ii)

Proposition 6.14. *Assume Hypothesis 6.1 and H is soluble. Then $b(G) = 2$ only if one of the following holds:*

(i) *$b(L) = 2$ and either $b(L \wr P) = 2$, or $b(L \wr P) = 3$, $r(L) < D(P)$ and (L, J) is one of the cases in Table 4.*

(ii) *$b(L) = b(L \wr P) = 3$ and (L, J) is one of the cases in Table 3, where $r(T) \geqslant D(P)$ and $|L : T| \geqslant 3$.*

The study of bases for product type groups becomes rather more complicated if we drop Hypothesis 6.1 and this will be the focus of a future paper. As an illustration, we close with the following example.

Example 6.15. Let $G \leqslant L \wr P$ be a product type primitive group on $\Omega = \Gamma^3$, where $P = S_3$ and $L \leqslant \mathrm{Sym}(\Gamma)$ is a primitive group with point stabiliser J. As before, we may assume G induces L on each factor of Ω, and P on the set of factors of the socle T^3. Take $L = PGL_2(11) = T{:}\langle a \rangle = T.2$ and $J = S_4$, so $b(L) = 2$, $r(L) = 1$ and $r(T) = 3$ (see Table 4, noting that J is of type $2_-^{1+2}.O_2^-(2)$).

First assume G contains P and note that there are three possibilities, namely $L \wr P$, $\langle T^3, (a, a, a), P \rangle$ and $\langle T^3, (a, a, 1), P \rangle$. For the full wreath product $G = L \wr P$, Theorem 3 implies that $b(G) = 3$ since $r(L) < D(P)$. Similarly, if $G = \langle T^3, (a, a, a), P \rangle$ then $\tau(G) = 0$ (see (16)) and thus $b(G) = 3$ by Theorem 6.11, while a MAGMA calculation gives $b(G) = 3$ if $G = \langle T^3, (a, a, 1), P \rangle$.

Now assume G does not contain P, so $|P \cap G| \in \{1, 2, 3\}$. With the aid of MAGMA, we find that there are 8 product type primitive groups of this form, up to permutation isomorphism. More precisely, there are 3 groups with $P \cap G = 1$ and in each case $b(G) = 2$. There are also 3 groups with $|P \cap G| = 2$ and here we find that $b(G) = 3$. Finally, let G_1 and G_2 be the two remaining groups with $|P \cap G_i| = 3$. For one of them, say G_1, we have $\langle G_1, P \rangle = L \wr P$ and $b(G_1) = 3$. On the other hand, $\langle G_2, P \rangle$ has index 4 in $L \wr P$ and one can check that $b(G_2) = 2$.

7. THE TABLES

Here we present Tables 4 and 5, which arise in the statement of Theorems 1, 2 and 3.

Let $L \leqslant \mathrm{Sym}(\Gamma)$ be an almost simple primitive group with socle T and soluble point stabiliser J (in terms of the notation introduced in Section 1, this means that $L \in \mathcal{S}$). Let $b(L)$ be the base size of L and let $\mathrm{reg}(L, b(L))$ be the number of regular orbits of L on the Cartesian product $\Gamma^{b(L)}$. By Theorem 1, we have $\mathrm{reg}(L, b(L)) \leqslant 4$ if and only if (L, J) is one of the cases recorded in Tables 4 and 5. Note that if $b(L) = 2$ then $\mathrm{reg}(L, b(L)) = r(L)$ is the number of regular suborbits of L on Γ (and similarly, $r(T)$ is the number of regular suborbits of T).

Remark 7.1. Suppose T is a classical group over $\mathbb{F}_q$. Then due to the existence of isomorphisms between various low-dimensional classical groups (see [23, Proposition 2.9.1],

for example), we may assume T is one of the following:

$$\mathrm{L}_n(q),\ n \geqslant 2;\ \mathrm{U}_n(q),\ n \geqslant 3;\ \mathrm{PSp}_n(q),\ n \geqslant 4;\ \mathrm{P\Omega}_n^\varepsilon(q),\ n \geqslant 7.$$

Furthermore, in order to avoid unnecessary repetition, we will exclude the groups with socle

$$\mathrm{L}_2(4),\ \mathrm{L}_2(5),\ \mathrm{L}_2(9),\ \mathrm{L}_3(2),\ \mathrm{L}_4(2),\ \mathrm{PSp}_4(2)',\ \mathrm{PSp}_4(3),\ {}^2G_2(3)',\ G_2(2)'$$

in Tables 4 and 5. This is consistent with [4] (see [4, Remark 9.1]) and it is justified by the existence of the following well known isomorphisms:

$$\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5,\ \mathrm{L}_2(9) \cong \mathrm{PSp}_4(2)' \cong A_6,\ \mathrm{L}_3(2) \cong \mathrm{L}_2(7),$$

$$\mathrm{L}_4(2) \cong A_8,\ \mathrm{PSp}_4(3) \cong \mathrm{U}_4(2),\ {}^2G_2(3)' \cong \mathrm{L}_2(8),\ G_2(2)' \cong \mathrm{U}_3(3).$$

So for example, a reader who is interested in the groups with socle $\mathrm{L}_4(2)$ should inspect the tables for any cases with $L = S_8$ or A_8.

In both tables we refer to the *type* of J. If L is a classical group, then this provides an approximate description of the structure of J, which is consistent with its usage in [23], where the precise structure of J is determined. For example, in the first row of Table 4 we have $L = \mathrm{PGL}_2(q)$ and J is of type $\mathrm{GL}_1(q) \wr S_2$, which indicates that J is the stabiliser in L of a direct sum decomposition $V = V_1 \oplus V_2$ of the natural module for L, where the V_i are 1-dimensional subspaces (see [23, Proposition 4.2.9] for the precise structure). In Table 5 we use the standard P_m notation for maximal parabolic subgroups, where P_m is the stabiliser of a totally singular m-dimensional subspace of the natural module. For $T = \mathrm{L}_n(q)$, we also use $P_{1,n-1}$ for the stabiliser of a flag of subspaces $0 < V_1 < V_{n-1} < V$ of V, where $\dim V_i = i$ (again, this notation is consisted with [23]). For the remaining groups where L is not classical, we record the precise structure of J in the third column of both tables. In addition, in Table 4 we use the standard notation δ, ϕ, γ, etc. for automorphisms of a simple classical group (see [3, Section 1.7.2]).

Remark 7.2. Let us record some additional comments on Tables 4 and 5.

(i) In the first row of Table 4 we have $L = \mathrm{PGL}_2(q)$ and $J = D_{2(q-1)}$ is a subgroup of type $\mathrm{GL}_1(q) \wr S_2$. In view of Remark 7.1, we may assume $q \geqslant 7$ and $q \neq 9$. More precisely, J is non-maximal when $q = 5$, while the cases $q = 4$ and 9 are recorded as $(L, J) = (A_5, D_6)$ and $(A_6.2, D_{16})$ in Table 4. As noted in Remark 3.4 we have

$$r(T) = \begin{cases} 1 & q \text{ even} \\ (q + a)/4 & q \text{ odd} \end{cases}$$

where $a = 7$ if $q \equiv 1 \pmod 4$, otherwise $a = 5$.

(ii) Consider the first row in Table 5 with $b(L) = 3$. Here $L = \mathrm{L}_2(q).2$, $J = P_1$ is a Borel subgroup and $q = p^f$ is odd, so in view of Remark 7.1, we may assume $q \neq 5, 9$. Then $\mathrm{reg}(L, b(L)) = 1$ if and only if L is sharply 3-transitive, which means that either $L = \mathrm{PGL}_2(q)$, or f is even and $L = T.\langle \delta\phi^{f/2} \rangle$.

(iii) Up to isomorphism, there are three almost simple groups of the form $\mathrm{L}_4(3).2$, one of which is $\mathrm{PGL}_4(3)$. In addition, we have $\mathrm{L}_4(3).2_2$ and $\mathrm{L}_4(3).2_3$, which contain involutory graph automorphisms x with $C_T(x) = \mathrm{PGSp}_4(3)$ and $\mathrm{PSO}_4^-(3).2$, respectively.

(iv) In the fourth column of Table 5 we record $\mathrm{reg}(L, b(L))$. In a few cases, this is presented as $r_1, r_2, \ldots$, which means that $\mathrm{reg}(L, b(L)) = r_i$ when q is contained in the i-th set appearing in the fifth column. For example, if $L = \mathrm{P\Gamma L}_2(q)$ and $J = P_1$, then $\mathrm{reg}(L, b(L)) = 3$ if $q = 16$ and $\mathrm{reg}(L, b(L)) = 2$ if $q = 8$.

$r(L)$	L	Type of J	$r(T)$	Comments
1	$\mathrm{PGL}_2(q)$	$\mathrm{GL}_1(q) \wr S_2$	See Remark 7.2(i)	$q \geqslant 7,\ q \neq 9$
	$\mathrm{P\Omega}_8^+(3).2^2$	$\mathrm{O}_4^+(3) \wr S_2$	12	Both groups of this shape
	$\Omega_8^+(2).3$	$\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$	5	
	$\mathrm{SO}_7(3)$	$\mathrm{O}_4^+(3) \perp \mathrm{O}_3(3)$	5	
	$\mathrm{PSp}_6(3)$	$\mathrm{Sp}_2(3) \wr S_3$	1	
	$\mathrm{PGL}_4(3)$	$\mathrm{O}_4^+(3)$	6	
	$\mathrm{U}_4(3).[4]$	$\mathrm{GU}_1(3) \wr S_4$	11	$L \neq T.\langle \delta^2, \phi \rangle$
	$\mathrm{U}_4(3)$	$\mathrm{GU}_2(3) \wr S_2$	1	
	$\mathrm{L}_3(4).D_{12}$	$\mathrm{GL}_1(4^3)$	44	
	$\mathrm{L}_3(4).2$	$\mathrm{GU}_3(2)$	3	$L \neq \mathrm{P\Sigma L}_3(4)$
	$\mathrm{U}_3(5).S_3$	$\mathrm{GU}_1(5) \wr S_3$	11	
	$\mathrm{U}_3(4)$	$\mathrm{GU}_1(4) \wr S_3$	1	
	$\mathrm{PGL}_2(11)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	3	
	$G_2(3).2$	$\mathrm{SL}_2(3)^2$	4	
	S_7	$\mathrm{AGL}_1(7)$	4	
	$A_6.2$	D_{16}	4	$L = \mathrm{PGL}_2(9)$
	$A_6.2$	$5{:}4$	2	$L = \mathrm{M}_{10}$
	A_5	D_6	1	
	$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	2	
	M_{11}	$2.S_4$	1	
2	$\mathrm{P\Omega}_8^+(3).4$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{L}_4(3).2_2$	$\mathrm{O}_4^+(3)$	6	
	$\mathrm{Sp}_4(4).4$	$\mathrm{O}_2^-(4) \wr S_2$	9	
	$\mathrm{L}_3(3)$	$\mathrm{GL}_1(3^3)$	2	
	$\mathrm{L}_3(3).2$	$\mathrm{O}_3(3)$	5	
	$\mathrm{U}_3(5).S_3$	$3^{1+2}.\mathrm{Sp}_2(3)$	21	
	$\mathrm{L}_2(27).3$	$\mathrm{GL}_1(27) \wr S_2$	8	
		$\mathrm{GL}_1(27^2)$	6	
	$\mathrm{PGL}_2(13)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	6	
	$\mathrm{L}_2(11)$	$\mathrm{GL}_1(11^2)$	2	
	$^2B_2(8).3$	$13{:}12$	7	
	A_9	$\mathrm{ASL}_2(3)$	2	
	$A_6.2$	SD_{16}	4	$L = \mathrm{M}_{10}$
	J_2	$5^2{:}D_{12}$	2	
3	$\mathrm{P\Omega}_8^+(3).3$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{P\Omega}_8^+(3).2$	$\mathrm{O}_4^+(3) \wr S_2$	12	$L = T.\langle \gamma \rangle$
	$\mathrm{L}_4(3).2_3$	$\mathrm{O}_4^+(3)$	6	
	$\mathrm{L}_3(4).S_3$	$\mathrm{GL}_1(4^3)$	44	$L \neq \mathrm{P\Gamma L}_3(4)$
	$\mathrm{PGU}_3(5)$	$\mathrm{GU}_1(5) \wr S_3$	11	
	$\mathrm{L}_2(25).2$	$\mathrm{GL}_1(25) \wr S_2$	8	$L = \mathrm{P\Sigma L}_2(25)$
		$\mathrm{GL}_1(25^2)$	6	$L \neq \mathrm{PGL}_2(25)$
	$\mathrm{L}_2(17)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	3	
	$\mathrm{L}_2(13)$	$\mathrm{GL}_1(13^2)$	3	
	$^2F_4(2)$	$5^2{:}4S_4$	6	
	$\mathrm{J}_3.2$	$3^{2+1+2}{:}8.2$	10	
	$\mathrm{HS}.2$	$5^{1+2}.[2^5]$	9	
4	$\mathrm{PSO}_8^+(3)$	$\mathrm{O}_4^+(3) \wr S_2$	12	
	$\mathrm{U}_4(3).2$	$\mathrm{GU}_1(3) \wr S_4$	11	$L \neq T.\langle \delta^2 \phi \rangle$
	$\mathrm{L}_2(25).2$	$\mathrm{GL}_1(25) \wr S_2$	8	$L = T.\langle \delta \phi \rangle$
	$\mathrm{L}_2(q)$	$\mathrm{GL}_1(q^2)$	4	$q = 17, 19$
	$G_2(3)$	$\mathrm{SL}_2(3)^2$	4	
	$\mathrm{M}_{12}.2$	$S_4 \times S_3$	13	
	$\mathrm{Suz}.2$	$3^{2+4}{:}2.(S_4 \times D_8)$	16	

TABLE 4. The groups $L \in \mathcal{S}$ with $b(L) = 2$ and $r(L) \leqslant 4$

$b(L)$	L	Type of J	$\operatorname{reg}(L, b(L))$	Comments
4	$\mathrm{L}_3(3)$	P_1, P_2	1	
	$\mathrm{P\Gamma L}_2(q)$	P_1	3, 2	$q \in \{16\}, \{8\}$
	$A_6.2^2$	$3^2{:}SD_{16}$	3	
	S_5	S_4	1	
3	$\mathrm{L}_2(q).2$	P_1	1	See Remark 7.2(ii)
	$\mathrm{L}_2(q)$	P_1	$2 - \delta_{2,p}$	$q \geqslant 7$, $q \neq 9$
	$\mathrm{P\Omega}_8^+(3)$	P_2	3	
	$\Omega_7(3)$	P_2	3	
	$\mathrm{PSp}_6(3)$	P_2	3	
	$\mathrm{L}_4(3).2$	$P_{1,3}$	3	$L \neq \mathrm{PGL}_4(3)$
	$\mathrm{U}_4(3).2$	P_1	1	$L \not< \mathrm{PGU}_4(3)$
	$\mathrm{U}_4(3)$	P_1	3	
	$\mathrm{Aut}(\mathrm{L}_3(q))$	$P_{1,2}$	4, 3, 1	$q \in \{3, 25, 27, 64\}, \{32\}, \{8, 9, 16\}$
	$\mathrm{L}_3(16).(2 \times 4)$	$P_{1,2}$	4	
	$\mathrm{L}_3(16).D_{12}$	$P_{1,2}$	2	
	$\mathrm{L}_3(16).12$	$P_{1,2}$	3	
	$\mathrm{L}_3(4).2^2$	$P_{1,2}$	4	
	$\mathrm{L}_3(4).6$	$P_{1,2}$	4	
	$\mathrm{Aut}(\mathrm{U}_3(q))$	P_1	4, 3, 2, 1	$q \in \{27\}, \{7, 32\}, \{5, 9, 16\}, \{3, 4, 8\}$
	$\mathrm{U}_3(16).4$	P_1	4	
	$\mathrm{U}_3(9).2$	P_1	4	
	$\mathrm{U}_3(8).S_3$	P_1	4	
	$\mathrm{U}_3(8).6$	P_1	3	
	$\mathrm{U}_3(8).3^2$	P_1	2	
	$\mathrm{U}_3(4).2$	P_1	2	
	$\mathrm{U}_3(4)$	P_1	4	
	$\mathrm{U}_3(3)$	P_1	3	
	$\mathrm{L}_2(7)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	1	
	$^2B_2(8).3$	$[8^2]{:}7.3$	2	
	$G_2(3)$	$[3^5]{:}\mathrm{GL}_2(3)$	4	
	S_7	$S_4 \times S_3$	1	
	$A_6.2$	$3^2{:}Q_8$	1	$L = \mathrm{PGL}_2(9)$
		$\mathrm{AGL}_1(9)$	1	$L = \mathrm{M}_{10}$
	A_6	$(S_3 \wr S_2) \cap L$	2	
	S_5	$S_3 \times S_2$	4	
		$5{:}4$	1	
	A_5	A_4	1	
		D_{10}	2	

TABLE 5. The groups $L \in \mathcal{S}$ with $b(L) \in \{3, 4\}$ and $\operatorname{reg}(L, b(L)) \leqslant 4$

REFERENCES

[1] R.F. Bailey and P.J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc. **43** (2011), 209–242.

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

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

[4] T.C. Burness, *Base sizes for primitive groups with soluble stabilisers*, Algebra Number Theory **15** (2021), 1755–1807.

[5] T.C. Burness, *Simple groups, fixed point ratios and applications*, in Local representation theory and simple groups, 267–322, EMS Ser. Lect. Math., Eur. Math. Soc., Zürich, 2018.

[6] T.C. Burness and M. Giudici, *On the Saxl graph of a permutation group*, Math. Proc. Cambridge Philos. Soc. **168** (2020), 219–248.

[7] T.C. Burness and R.M. Guralnick, *Fixed point ratios for finite primitive groups and applications*, submitted (2021), arXiv:2112.03967.

[8] T.C. Burness, R.M. Guralnick and J. Saxl, *On base sizes for symmetric groups*, Bull. Lond. Math. Soc. **43** (2011), 386–391.

[9] T.C. Burness and S. Harper, *Finite groups, 2-generation and the uniform domination number*, Israel J. Math. **239** (2020), 271–367.

[10] T.C. Burness and H.Y. Huang, *On the Saxl graphs of primitive groups with soluble stabilisers*, Algebr. Comb., to appear.

[11] T.C. Burness, E.A. O'Brien and R.A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–333.

[12] T.C. Burness and Á. Seress, *On Pyber's base size conjecture*, Trans. Amer. Math. Soc. **367** (2015), 5633–5651.

[13] P.J. Cameron, P.M. Neumann and J. Saxl, *On groups with no regular orbits on the set of subsets*, Arch. Math. **43** (1984), 295–296.

[14] H. Chen and S. Du, *On the Burness-Giudici conjecture*, submitted (2020), arXiv:2008.04233.

[15] J. Chen and H.Y. Huang, *On valency problems of Saxl graphs*, J. Group Theory **25** (2022), 543–577.

[16] S. Dolfi, *Orbits of permutation groups on the power set*, Arch. Math. **75** (2000), 321–327.

[17] H. Duyan, Z. Halasi and A. Maróti, *A proof of Pyber's base size conjecture*, Adv. Math. **331** (2018), 720–747.

[18] J.B. Fawcett, *Bases of twisted wreath products*, J. Algebra **607** (2022), 247–271.

[19] J.B. Fawcett, *The base size of a primitive diagonal group*, J. Algebra **375** (2013), 302–321.

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

[21] R.M. Guralnick and K. Magaard, *On the minimal degree of a primitive permutation group*, J. Algebra **207** (1998), 127–145.

[22] Z. Halasi, M.W. Liebeck and A. Maróti, *Base sizes of primitive groups: bounds with explicit constants*, J. Algebra **521** (2019), 16–43.

[23] P.B. Kleidman and M.W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Math. Soc. Lecture Note Series, vol. 129, Cambridge University Press, 1990.

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

[25] M. Lee, *Regular orbits of quasisimple linear groups I*, J. Algebra **586** (2021), 1122–1194.

[26] M. Lee, *Regular orbits of quasisimple linear groups II*, J. Algebra **586** (2021), 643–717.

[27] M. Lee and T. Popiel, *Saxl graphs of primitive affine groups with sporadic point stabilisers*, submitted (2021), arXiv:2108.02470.

[28] M.W. Liebeck, C.E. Praeger and J. Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. **44** (1988), 389–396.

[29] M.W. Liebeck and J. Saxl, *Maximal subgroups of finite simple groups and their automorphism groups*, in Proceedings of the International Conference on Algebra, Part 1 (Novosibirsk, 1989), 243–259, Contemp. Math., 131, Part 1, Amer. Math. Soc., Providence, RI, 1992.

[30] M.W. Liebeck, J. Saxl and G.M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. London Math. Soc. **65** (1992), 297–325.

[31] M.W. Liebeck and A. Shalev, *Bases of primitive permutation groups*, in Groups, combinatorics & geometry (Durham, 2001), 147–154, World Sci. Publ., River Edge, NJ, 2003.

[32] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), 497–520.

[33] C.E. Praeger and J. Saxl, *On the orders of primitive permutation groups*, Bull. London Math. Soc. **12** (1980), 303–307.

[34] L. Pyber, *Asymptotic results for permutation groups*, in Groups and Computation (eds. L. Finkelstein and W. Kantor), DIMACS Series, vol. 11, pp.197–219, 1993.

[35] H. Robbins, *A remark on Stirling's formula*, Amer. Math. Monthly **62** (1955), 26–29.

[36] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[37] Á. Seress, *Primitive groups with no regular orbits on the set of subsets*, Bull. London Math. Soc. **29** (1997), 697–704.

[38] Á. Seress, *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. **53** (1996), 243–255.

[39] R.P. Stanley, *Enumerative combinatorics. Volume 1*, Second edition. Cambridge Studies in Advanced Mathematics, 49. Cambridge University Press, 2012.

[40] M. Suzuki, *On a class of doubly transitive groups*, Ann. of Math. **75** (1962), 105–145.

[41] H.N. Ward, *On Ree's series of simple groups*, Trans. Amer. Math. Soc. **121** (1966), 62–89.

[42] R.A. Wilson, *Maximal subgroups of sporadic groups*, in Finite simple groups: thirty years of the Atlas and beyond, 57–72, Contemp. Math., 694, Amer. Math. Soc., Providence, RI, 2017.

T.C. Burness, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: t.burness@bristol.ac.uk

H.Y. Huang, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK
Email address: hy.huang@bristol.ac.uk