# On minimal subdegrees of finite primitive permutation groups

*Michael Giudici, Cai Heng Li, Cheryl E. Praeger,*
*Ákos Seress and Vladimir Trofimov*[*]

**Abstract.** We study the minimal non-trivial subdegrees of finite primitive permutation groups that admit an embedding into a wreath product in product action, giving a connection with the same quantity for the primitive component. We discover that the primitive groups of twisted wreath type exhibit different (but interesting) behaviour from the other primitive types.

2000 Mathematics Subject Classification: 20B15

## 1. Introduction

For a transitive permutation group $G$ on a set $\Omega$, a *suborbit of $G$ relative to a point $\alpha \in \Omega$* is a $G_\alpha$-orbit $\Gamma$, and its size $|\Gamma|$ is the corresponding *subdegree* of $G$. A suborbit $\Gamma$, and the corresponding subdegree, are said to be non-trivial provided $\Gamma \neq \{\alpha\}$. In general, a non-trivial subdegree may be equal to 1. However, if $G$ is primitive and not cyclic of prime order, then $\alpha$ is the unique fixed point of $G_\alpha$, and consequently all non-trivial subdegrees of a non-cyclic primitive permutation group are greater than 1. Let $\mathrm{MinSubDeg}(G)$ denote the minimum of the non-trivial subdegrees of $G$, and note that the transitivity of $G$ implies that the value of $\mathrm{MinSubDeg}(G)$ is independent of the choice of $\alpha$. The aim of this paper is to study $\mathrm{MinSubDeg}(G)$ for several types of finite primitive permutation groups $G$.

The O'Nan–Scott Theorem partitions the finite primitive permutation groups into a number of disjoint types. For several of these types, each group $G$ of the type admits a natural embedding into a wreath product $H \wr S_k$ in its product action on a Cartesian power $\Delta^k$, where $k \geq 2$, $H$ is a primitive permutation group on the smaller set $\Delta$, and $H$ is induced by $G$. The group $H$ is called the *primitive component of $G$ relative to the Cartesian decomposition $\Delta^k$*. The definitions of the product action of a wreath product, and the primitive component are given

---

[*] This work forms a part of a research project funded by an Australian Research Council Discovery Grant. The fourth author is partially supported by the National Security Agency.

formally in Section 2. We study the relationship between $\mathrm{MinSubDeg}(G)$ and $\mathrm{MinSubDeg}(H)$ for these types of primitive groups.

The *socle* of a finite group is the product of its minimal normal subgroups. For each primitive group $G$ having O'Nan–Scott type PA, HC or CD (see Section 2 for definitions of these types), $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k) = \mathrm{Soc}(H)^k$, and for these O'Nan–Scott types complete information about $\mathrm{MinSubDeg}(G)$ in terms of $\mathrm{MinSubDeg}(H)$ and $k$ is given by our first theorem.

**Theorem 1.1.** *Let $G$ be a finite primitive permutation group such that $G \leq H \wr S_k$ acting in product action on $\Delta^k$, with primitive component $H$ and $k \geq 2$. Suppose further that* $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k)$ *and is non-abelian. Then* $\mathrm{MinSubDeg}(G) = k \cdot \mathrm{MinSubDeg}(H)$. *Moreover, let $\delta \in \Delta$ and $\alpha = (\delta, \dots, \delta) \in \Delta^k$, and let $\Gamma$ be a $G_\alpha$-orbit in $\Delta^k \setminus \{\alpha\}$ of minimum length. Then there exists a minimum length $H_\delta$-orbit $\Gamma_0$ in $\Delta \setminus \{\delta\}$ such that either*

- *(a) $\Gamma = \bigcup_{1 \leq i \leq k} \Gamma_i$ where $\Gamma_i$ consists of all $k$-tuples $(\delta_1, \dots, \delta_k)$ such that $\delta_j = \delta$ for $j \neq i$, and $\delta_i \in \Gamma_0$, or*
- *(b) each $k$-tuple in $\Gamma$ has exactly two entries in $\Gamma_0$, with the remaining entries all equal to $\delta$. Moreover, $H \leq H_0 \wr S_\ell$ in product action on $\Delta = \Delta_0^\ell$ with primitive component $H_0$,* $\mathrm{Soc}(H) = \mathrm{Soc}(H_0 \wr S_\ell)$ *(where possibly $\ell = 1$ in which case $H_0 = H$), $|\Gamma_0| = 4\ell$, and $(H_0, |\Delta_0|)$ is one of* $(\mathrm{PGL}(2,7), 21)$, $(\mathrm{PGL}(2,9), 45)$, $(\mathrm{M}_{10}, 45)$, *or* $(\mathrm{P\Gamma L}(2,9), 45)$.

**Corollary 1.2.** *Let $G$ be a finite primitive permutation group of O'Nan–Scott type* PA, HC *or* CD *acting on a set $\Delta^k$ (where $k \geq 2$) with primitive component $H \leq \mathrm{Sym}(\Delta)$. Then* $\mathrm{MinSubDeg}(G) = k \cdot \mathrm{MinSubDeg}(H)$.

**Remark 1.3.** (a) In Theorem 1.1 (b), $G \leq H_0 \wr S_{\ell k}$ in product action with primitive component $H_0$ relative to the decomposition $\Omega = \Delta_0^{\ell k}$. Moreover, for each possibility for $(H_0, |\Delta_0|)$, the stabiliser $(H_0)_{\delta_0}$ (where $\delta_0 \in \Delta_0$) has a unique orbit in $\Delta_0$ of length $\mathrm{MinSubDeg}(H_0) = 4$ (see [4, Lemma 3.1]), and we show in Proposition 3.2 that there are examples of groups $G$ as in (b), corresponding to each group $H_0$, for each even integer $k$.

(b) The study of $\mathrm{MinSubDeg}(G)$ for finite primitive groups $G$ was motivated by problems concerning edge-transitive graphs. Each suborbit $\Gamma$ of a primitive group $G$ on $\Omega$ relative to a point $\alpha$ corresponds to a $G$-orbit $\widehat{\Gamma}$ in $\Omega \times \Omega$, namely $\widehat{\Gamma} := \{(\alpha^g, \beta^g) \mid \beta \in \Gamma,\ g \in G\}$, and this correspondence is bijective. Moreover, for each such $G$-orbit $\widehat{\Gamma}$, its 'pair' $\widehat{\Gamma}^* := \{(\beta, \gamma) \mid (\gamma, \beta) \in \widehat{\Gamma}\}$ is also a $G$-orbit in $\Omega \times \Omega$, and so corresponds to a $G_\alpha$-orbit $\Gamma^*$ in $\Omega$. The suborbits $\Gamma$ and $\Gamma^*$ have the same size, but they are equal if and only if $\widehat{\Gamma} = \widehat{\Gamma}^*$, that is to say, if and only if $\widehat{\Gamma}$ is *symmetric*. In any case the union $\widehat{\Gamma} \cup \widehat{\Gamma}^*$ may be regarded as the set of arcs (ordered pairs of adjacent vertices) of a graph with vertex set $\Omega$ that admits $G$ as an edge-transitive group of automorphisms. The valency of this graph is the subdegree $|\Gamma|$ if $\widehat{\Gamma}$ is symmetric, and is $2|\Gamma|$ otherwise.

The graphs $\widehat{\Gamma} \cup \widehat{\Gamma}^*$ of minimum valency for a given group $G$, as $\Gamma$ ranges over all non-trivial suborbits, arose in [8] in the investigation of limits of convergent sequences of finite vertex-primitive graphs with respect to a certain metric on the space of locally finite, vertex-transitive graphs. The minimum valency graphs for the primitive groups $G$ occuring in Theorem 1.1 can be characterised by extending the arguments used in the proof of that result. If some minimum length non-trivial suborbit $\Gamma$ for $G$, relative to $\alpha$, corresponds to a symmetric $G$-orbit $\widehat{\Gamma}$ in $\Omega \times \Omega$, then all minimum valency graphs will arise from such suborbits. However, if all minimum length non-trivial suborbits $\Gamma$ correspond to non-symmetric $G$-orbits $\widehat{\Gamma}$, then some rather delicate analysis is needed to sort out the possibilities for the minimum valency graphs. The results are given in Theorem 1.4.

A suborbit $\Gamma$ of a transitive permutation group $G$ on $\Omega$, relative to a point $\alpha$, is said to be *symmetric* if the corresponding $G$-orbit $\widehat{\Gamma}$ in $\Omega \times \Omega$ is symmetric. We extend this notion to arbitrary $G_\alpha$-invariant subsets of $\Omega$ as follows. If $\Sigma$ is a $G_\alpha$-invariant subset of $\Omega$, then $\Sigma$ is a union $\bigcup_{i\in I} \Gamma_i$ of some $G_\alpha$-orbits $\Gamma_i$, $i \in I$. We say that $\Sigma$ is *symmetric* if the corresponding union $\widehat{\Sigma} = \bigcup_{i\in I} \widehat{\Gamma}_i$ of $G$-orbits in $\Omega \times \Omega$ is symmetric or, equivalently, if $\Gamma_i^* \subseteq \Sigma$ for all $i \in I$. From Remark 1.3 (b), it is clear that the minimum valency $G$-edge-transitive graphs with vertex set $\Omega$ are those with arc set $\widehat{\Sigma}$, for some symmetric $G_\alpha$-invariant subset $\Sigma \subseteq \Omega \setminus \{\alpha\}$ of minimum length. Thus we define $\mathrm{MinVal}(G)$ to be the minimum length of the symmetric $G_\alpha$-invariant subsets of $\Omega \setminus \{\alpha\}$.

**Theorem 1.4.** *Let* $G, H, k, \alpha, \delta$ *be as in Theorem* 1.1. *Then* $\mathrm{MinVal}(G) = k \cdot \mathrm{MinVal}(H)$. *Let* $\Gamma$ *be a symmetric* $G_\alpha$*-invariant subset of* $\Delta^k \setminus \{\alpha\}$ *of length* $\mathrm{MinVal}(G)$. *Then there exists a symmetric* $H_\delta$*-invariant subset* $\Gamma_0$ *of* $\Delta \setminus \{\delta\}$ *of length* $\mathrm{MinVal}(H)$ *such that either (a) or (b) of Theorem* 1.1 *holds for* $\Gamma, \Gamma_0$, *and if case (b) holds then* $\Gamma$ *is a* $G_\alpha$*-orbit and* $\mathrm{MinVal}(G) = \mathrm{MinSubDeg}(G)$.

This theorem is used in [8] to elucidate the structure of a family of these limit graphs. Minimum valency graphs for primitive groups also arose in the study of finite distance transitive graphs in [13], since a $G$-vertex-primitive, distance-transitive graph must be a graph $\widehat{\Gamma}$ corresponding to one of the smallest two non-trivial subdegrees $|\Gamma|$. Estimates of minimal subdegrees of finite primitive permutation groups also play a role in the analysis of permutation group algorithms for computing a composition series, see [1, 3] and [14, Chapter 6].

There is one O'Nan–Scott type that admits natural embeddings into a wreath product in product action to which Theorem 1.1 does not apply, namely the twisted wreath type TW (defined in Section 2). As with the other types, for every primitive group $G$ of type TW we have $G \le H \wr S_k$ acting on $\Delta^k$, where $H$ is the primitive component of $G$ and $k \ge 2$. However, $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$, while $\mathrm{Soc}(H) \cong T \times T$, so that $\mathrm{Soc}(G)$ is not equal to $\mathrm{Soc}(H \wr S_k)$. The socle of $G$ acts regularly on $\Delta^k$ and $G$ is a semidirect product $\mathrm{Soc}(G) \rtimes P$, for some transitive subgroup $P$ of $S_k$. In fact, for these groups the relationship between $\mathrm{MinSubDeg}(G)$ and $\mathrm{MinSubDeg}(H)$ given in Corollary 1.2 fails spectacularly. For a group $P$, we denote by $\mathrm{MinDeg}(P)$, called the *minimal* *degree of* $P$, the least positive integer $n$ such that $P$ acts faithfully and transitively on a set of size $n$. The analogue of Corollary 1.2 in Theorem 1.5 below gives an inequality relating $\mathrm{MinSubDeg}(G)$ and $\mathrm{MinSubDeg}(H)$, one side of which can be an equality infinitely often. Since $\mathrm{Soc}(G) = T^k$, we can identify the point set with $T^k$ and we take the identity as the point $\alpha$, so that $G_\alpha = P$. In analogy with Theorem 1.1(a), we define a certain collection of points in $T^k\backslash\{1\}$ (see Construction 4.1) and prove that $\mathrm{MinSubDeg}(G)$ is always attained by a $G_\alpha$–orbit containing one of these special points. Further, there is a partial analogy to Theorem 1.1(b), in that we show how to obtain additional minimal length suborbits in certain situations (see also Lemma 4.13).

**Theorem 1.5.** *Let* $G$ *be a finite primitive permutation group of O'Nan–Scott type* TW *and suppose that* $G = \mathrm{Soc}(G) \rtimes P \leq H \wr S_k$ *acting on a set* $\Delta^k$ *(where* $k \geq 2$*) with primitive component* $H \leq \mathrm{Sym}(\Delta)$*. Then*

*(a)* $\max\{\mathrm{MinSubDeg}(H), \mathrm{MinDeg}(P)\} \leq \mathrm{MinSubDeg}(G) \leq k \cdot \mathrm{MinSubDeg}(H)$, *and there are infinitely many examples with* $\mathrm{MinSubDeg}(G) = \mathrm{MinDeg}(P) = \mathrm{MinSubDeg}(H)$.

*(b)* $\mathrm{MinSubDeg}(G)$ *is always attained by a shortest suborbit of the form* $(f_{R,t})^P$*, with* $f_{R,t}$ *as in Construction* 4.1 *for some* $(R, t)$ *in the set* $\mathcal{R}$ *defined there. Moreover,* $\mathrm{MinSubDeg}(G)$ *can sometimes also be attained for suborbits not of this form.*

Thus although there are certain similarities, the behaviour of primitive groups of type TW is different from that of primitive groups of types HC, CD and PA. Moreover, we wonder whether it is perhaps never possible for $\mathrm{MinSubDeg}(G)$ with $G$ of type TW, to achieve the bound of Theorem 1.1.

**Question 1.6.** *Is it true that, for all finite primitive permutation groups* $G = \mathrm{Soc}(G) \rtimes P \leq H \wr S_k$ *of type* TW*, with* $P, H$ *as in Theorem* 1.5*, the inequality* $\mathrm{MinSubDeg}(G) < k \cdot \mathrm{MinSubDeg}(H)$ *holds?*

In Section 2, as promised, we give the information needed about the O'Nan–Scott types and the product action of wreath product groups. Then in Section 3 we prove Theorem 1.1 and Proposition 3.2. In our final Section 4, we not only prove Theorem 1.5, but we also introduce a method that enables us to compute many of the short suborbits of primitive groups of type TW.

## 2. Wreath products in product action, and O'Nan–Scott types

*Wreath products in product action:* The wreath product $W = \mathrm{Sym}(\Delta) \wr S_k$ is the semidirect product $W = \mathrm{Sym}(\Delta)^k \rtimes S_k$ where, for $h = (h_1, \ldots, h_k) \in \mathrm{Sym}(\Delta)^k$

and $\sigma \in S_k$, $\sigma^{-1}h\sigma = (h_{1\sigma^{-1}}, \ldots, h_{k\sigma^{-1}})$. The point set for the product action of $W$ is the Cartesian product $\Omega = \Delta \times \cdots \times \Delta = \Delta^k$ and the action is given by the following, where $h = (h_1, \ldots, h_k) \in \mathrm{Sym}(\Delta)^k$, $\sigma \in S_k$, and $(\delta_1, \ldots, \delta_k) \in \Omega$.

$$\begin{aligned} (h_1, \ldots, h_k) \quad &: \quad (\delta_1, \ldots, \delta_k) \mapsto (\delta_1^{h_1}, \ldots, \delta_k^{h_k}) \\ \sigma \quad &: \quad (\delta_1, \ldots, \delta_k) \mapsto (\delta_{1\sigma^{-1}}, \ldots, \delta_{k\sigma^{-1}}) \end{aligned}$$

*Primitive subgroups of wreath products:* Suppose that $G \leq W$ and $G$ is primitive on $\Omega$. If $G$ projected onto an intransitive subgroup of $S_k$, then the product $M$ of the direct factors of $\mathrm{Sym}(\Delta)^k$ corresponding to a $G$-orbit in $\{1, \ldots, k\}$ would be $G$-invariant and intransitive on $\Delta^k$, and hence $M$ would be an intransitive normal subgroup of the group $MG$, while $MG$ would be primitive since $G$ is primitive. Thus the primitivity of $G$ on $\Omega$ implies that $G$ projects onto a transitive subgroup of $S_k$, and $G$ acts on $\{1, \ldots, k\}$ in the same way that it permutes the entries of the points of $\Omega$.

Let $G_1$ be the stabiliser of the point 1 in this action, so that $G_1 \leq \mathrm{Sym}(\Delta) \times (\mathrm{Sym}(\Delta) \wr S_{k-1})$, and let $H$ denote the image of $G_1$ under the natural homomorphism $\pi_1 : G_1 \to \mathrm{Sym}(\Delta)$ to the first direct factor of this direct product. By [9, 2.2], there is an element $w \in \mathrm{Sym}(\Delta)^k \cap \ker \pi_1$ such that the conjugate $G^w$ lies in $H \wr S_k$. We replace $G$ by $G^w$ and *thereby assume that* $G \leq H \wr S_k$.

The group $G_1$ induces the permutation group $H$ on the set of first entries of points of $\Omega$. It follows from the primitivity of $G$ on $\Omega$ that $H$ is primitive on $\Delta$, and we call $H$ the *primitive component of* $G$ *relative to the decomposition* $\Delta^k$ *of* $\Omega$. Thus the primitive group $G$ satisfies $G \leq H \wr K$ where $H$ is primitive on $\Delta$ and $K$ is transitive on $\{1, \ldots, k\}$.

The converse is not quite true (see [5, Theorem 4.5]): $H \wr K \leq \mathrm{Sym}(\Delta) \wr S_k$ is primitive in its product action on $\Delta^k$ if and only if $H$ is primitive but not regular on $\Delta$, and $K$ is transitive on $\{1, \ldots, k\}$. (A permutation group is *regular* if it is transitive and the only element that fixes a point is the identity element.)

*O'Nan–Scott types:* There are several case subdivisions of finite primitive permutation groups, representing different versions of the so-called O'Nan–Scott Theorem. We use the 8-type subdivision introduced in [12]. There are four types which contain some primitive groups that cannot be embedded into a wreath product in product action. In our notation these are the types HA, AS, HS, SD. These types correspond (approximately) to the *basic primitive groups* defined by Cameron, see [5, Section 4.3, Theorem 4.6]; Cameron calls a finite primitive group $G$ *basic* if $G$ is not a subgroup of a wreath product $\mathrm{Sym}(\Delta) \wr S_k$ in product action on $\Delta^k$, for any $k \geq 2$.

Suppose that $G \leq \mathrm{Sym}(\Omega)$ and $G$ is primitive on $\Omega$. We give minimal defining features for each type, explain the acronym, and make a few comments relevant to embeddability in wreath products in product action.

*The type* HA: $G$ has a non-trivial abelian normal subgroup $N$. Such groups are contained in the *Holomorph of the Abelian group* $N$.

For all groups $G$ of type HA, $\Omega$ can be identified with a finite vector space $V$, $G$ is a group of affine transformations of $V$, and $N$ is the group of translations. Moreover $G = N \rtimes G_0$ where $G_0$ is an irreducible subgroup of $\mathrm{GL}(V)$. Some but not all groups of type HA can be embedded in a wreath product in product action. This occurs if and only if $G_0$ leaves invariant a direct sum decomposition of $V = U \oplus \cdots \oplus U$ as a sum of $k$ subspaces of dimension $\dim(V)/k$; in this case $G \leq H \wr S_k$ with $H$ a primitive group of affine transformations of $U$.

*The type* AS: $G$ has a unique minimal normal subgroup $T$, and $T$ is a non-abelian simple group. Such groups are *Almost Simple.*

Again, it is possible for a primitive group $G$ of type AS to be embedded in a wreath product in product action. However such embeddings are rare, and have been classified in [12, Proposition 6.1 and Table 3]. We point out that for any of these rare embeddings $G \leq H \wr S_k$, where $H$ is the primitive component, $\mathrm{Soc}(G) \neq \mathrm{Soc}(H \wr S_k)$, and in particular Theorem 1.1 does not apply. In particular, these rare primitive groups of type AS that admit such embeddings are not basic according to the definition in [5, page 103], and in fact are counter-examples to [5, Theorem 4.7].

*The types* HS *and* SD*:* $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$ and integer $k \geq 2$, and a stabiliser $\mathrm{Soc}(G)_\alpha \cong T$ is a diagonal subgroup. Either $\mathrm{Soc}(G)$ is a minimal normal subgroup and the type is SD (*Simple Diagonal*), or $k = 2$ and $\mathrm{Soc}(G)$ is the product of two simple normal subgroups of $G$. Here the type is HS (and $G$ is contained in the *Holomorph of the Simple group* $T$).

No primitive group of type HS or SD can be embedded in a wreath product in product action, see [12, Proposition 8.1]. For the other four types, named HC, CD, PA, TW, all groups of these types admit natural embeddings into wreath products in product action.

*The types* HC *and* CD*:* $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$ and integer $k \geq 2$, and a stabiliser $\mathrm{Soc}(G)_\alpha$ is a non-simple subdirect subgroup of $\mathrm{Soc}(G)$. Either $\mathrm{Soc}(G)$ is a minimal normal subgroup and the type is CD (*Compound Diagonal*), or $k$ is even, $k \geq 4$, and $\mathrm{Soc}(G)$ is the product of two isomorphic minimal normal subgroups of $G$. Here the type is HC (and $G$ is contained in the *Holomorph of a 'Compound group'*).

Each group $G$ of type HC or CD admits a natural embedding into $H \wr S_\ell$ in product action with primitive component $H$ being a basic primitive group. For the type HC, $\ell = k/2$ and $H$ is of type HS, while for the type CD, $H$ is of type SD, see [12, Sections 3.5, 3.9, and Proposition 8.1]. In particular $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k)$.

*The type* PA *(Product Action):* $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$ and integer $k \geq 2$ and, for some $\alpha \in \Omega$, the stabiliser $\mathrm{Soc}(G)_\alpha = R^k$, where $1 < R < T$.

Each group $G$ of type PA admits a natural embedding into $H \wr S_k$ in product action with primitive component $H$ of type AS with socle $T$. In particular $\mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k)$, see [12, Section 3.10].

*The type* TW *(Twisted Wreath):* $\mathrm{Soc}(G) = T^k$ for some non-abelian simple group $T$ and integer $k \geq 2$, and a stabiliser $\mathrm{Soc}(G)_\alpha$ is the identity subgroup, that is, $\mathrm{Soc}(G)$ is regular, so that we may identify $\Omega$ with $T^k$.

More details are given about the structure of $G$ in Section 4. In particular, $G \leq \mathrm{Sym}(T) \wr S_k$ in product action on $T^k$, and the primitive component $H$ of $G$ relative to this decomposition is of type HS with $\mathrm{Soc}(H) \cong T \times T$, see [12, Section 3.6]. This means that $\mathrm{Soc}(G) = T^k$ is not equal to $\mathrm{Soc}(H \wr S_k) \cong T^{2k}$.

## 3. Proof of Theorem 1.1 and Theorem 1.4

Let $G, H, k, \Delta^k, \alpha, \delta$ be as in Theorem 1.1. We use the notation introduced in the paragraph preceding the statement of Theorem 1.1. In particular let $N = \mathrm{Soc}(G)$, so that $N = \mathrm{Soc}(H \wr S_k) = M^k$, where $M = \mathrm{Soc}(H)$, and $N_\alpha = M_\delta^k$. Also, by assumption, $N$ is non-abelian, and it follows from the O'Nan–Scott Theorem that for the types where $N = \mathrm{Soc}(G) = \mathrm{Soc}(H \wr S_k)$, we have $N_\alpha \neq 1$, and hence $M_\delta \neq 1$. Before giving a proof of Theorem 1.1, we collect together a few facts about $G$. Recall that $G_1$ denotes the subgroup of index $k$ in $G$ that fixes the first entries of points of $\Delta^k$.

**Lemma 3.1.** *(a) $G_\alpha$ acts transitively on the set $\{1, \ldots, k\}$ of entries of the $k$-tuples in $\Delta^k$.*

*(b) The only fixed points of $N_\alpha$ in $\Delta^k$, and of $M_\delta$ in $\Delta$, are $\alpha$ and $\delta$ respectively.*

*(c) Let $\Gamma$ be a $G_\alpha$-orbit in $\Delta^k \setminus \{\alpha\}$. Then $\Gamma$ contains a point $\gamma = (\gamma_1, \ldots, \gamma_k)$ with $\gamma_1 \neq \delta$. If $L(\gamma)$ denotes the set of all $i$ such that $\gamma_i \neq \delta$, then $u = |L(\gamma)| \leq k$, and $|G_\alpha : (G_1 \cap G_{\alpha\gamma})| = u'|\Gamma|$, where $u'$ is the length of the $G_{\alpha\gamma}$-orbit in $L(\gamma)$ containing the point 1, and in particular $u' \leq u$.*

*(d) With $\gamma, L(\gamma), u$ as in part (c), let $m$ be the minimum of the lengths of the $M_\delta$-orbits in $\Delta \setminus \{\delta\}$, let $d_1$ be the length of the $H_\delta$-orbit containing $\gamma_1$ and, for $j \in L(\gamma) \setminus \{1\}$, let $m_j$ be the length of the $M_\delta$-orbit containing $\gamma_j$. Then $m > 1$, $d_1 \geq \mathrm{MinSubDeg}(H)$, and each $m_j > 1$, and $|G_\alpha : (G_1 \cap G_{\alpha\gamma})| \geq k\, d_1 \cdot \prod_{j \in L(\gamma) \setminus \{1\}} m_j \geq k\, \mathrm{MinSubDeg}(H) m^{u-1}$.*

Proof. (a) As noted in Section 2, $G$ acts transitively on the set $\{1, \ldots, k\}$ of entries of the $k$-tuples in $\Delta^k$, and as $G = NG_\alpha$, so also does $G_\alpha$.

(b) The set $F$ of fixed points of $M_\delta$ in $\Delta$ is a block of imprimitivity for $H$ in $\Delta$, and it follows that the subset $F^k$ of $\Delta^k$ is a block of imprimitivity for $H \wr S_k$, and hence also for $G$. Since $G$ is primitive, we conclude that $F^k = \{\alpha\}$, and hence that $F = \{\delta\}$.

(c) Since $G_\alpha$ fixes $\alpha$, and fixes $\Gamma$ setwise, it follows that $u = |L(\gamma)|$ is independent of the choice of $\gamma \in \Gamma$ and satisfies $1 \leq u \leq k$. By part (a) we may assume that $L(\gamma)$ contains 1, so $\gamma_1 \neq \delta$. Now $G_{\alpha\gamma}$ fixes $L(\gamma)$ setwise and hence contains $G_1 \cap G_{\alpha\gamma}$ as a subgroup of index $u' \leq u$, so $|G_\alpha : (G_1 \cap G_{\alpha\gamma})| = |\Gamma| \cdot u' \leq |\Gamma| \cdot u$.

(d) It follows from part (b) that $m > 1$ and each $m_j > 1$. Let $\Gamma'_0 = \gamma_1^{H_\delta}$, the $H_\delta$-orbit containing $\gamma_1$. Then $d_1 = |\Gamma'_0| \geq \mathrm{MinSubDeg}(H)$. Since $N \leq G_1$ and $N$ is transitive on $\Delta^k$, it follows that $G_1 = (G_1 \cap G_\alpha)N$. Also, since $G_1$ induces the group $H$ on the first entries of points of $\Delta^k$, it follows that $G_1 \cap G_\alpha$ induces the group $H_\delta$ on the first entries of points of $\Delta^k$. This implies that each point of $\Gamma'_0$ occurs the same number, say $v$, times as the first entry of a point of $\gamma^{G_1 \cap G_\alpha}$ (the orbit of $G_1 \cap G_\alpha$ containing $\gamma$), so $|\gamma^{G_1 \cap G_\alpha}| = vd_1$, and

$$|G_\alpha : (G_1 \cap G_{\alpha\gamma})| = k\,|(G_1 \cap G_\alpha) : (G_1 \cap G_{\alpha\gamma})| = k\,|\gamma^{G_1 \cap G_\alpha}| = kvd_1.$$

Thus to complete the proof it is sufficient to show that $v \geq \prod_{j \in L(\gamma)\setminus\{1\}} m_j$. Now $G_1 \cap G_\alpha$ contains the subgroup $X := 1 \times M_\delta^{k-1}$ and each point of the $X$-orbit $\gamma^X$ has first entry $\gamma_1$, so $v \geq |\gamma^X|$. Finally it follows from the definition of the $m_j$ that $|\gamma^X| = \prod_{j \in L(\gamma)\setminus\{1\}} m_j$. □

Proof of Theorem 1.1. Let $\Omega = \Delta^k$. Consider the set $\bigcup_{1 \leq i \leq k} \Gamma_i$, where $\Gamma_i$ consists of all $k$-tuples $(\delta_1, \ldots, \delta_k)$ such that $\delta_j = \delta$ for $j \neq i$, and $\delta_i$ lies in a fixed $H_\delta$-orbit $\Gamma_0$ in $\Delta \setminus \{\delta\}$. By Lemma 3.1, $G_\alpha$ is transitive on entries, and since $G_1$ induces the group $H$ on the first entries of points in $\Omega$, it follows that such a set is a $G_\alpha$-orbit. If $|\Gamma_0| = d := \mathrm{MinSubDeg}(H)$, then this $G_\alpha$-orbit has length $kd$. We will show that the minimum length of the non-trivial $G_\alpha$-orbits is $kd$. In addition we will prove that either all $G_\alpha$-orbits of length $kd$ are of this form, or $(H, |\Delta|)$ is as in (b) and a $G_\alpha$-orbit of length $kd$ is either of this form or is one of the orbits specified in (b).

Suppose that $\Gamma$ is a $G_\alpha$-orbit in $\Omega \setminus \{\alpha\}$ of minimum length. Then $|\Gamma| = \mathrm{MinSubDeg}(G) \leq kd$. By Lemma 3.1, $\Gamma$ contains a point $\gamma = (\gamma_1, \ldots, \gamma_k)$ with $\gamma_1 \neq \delta$, and if $L(\gamma), u, m, d_1$ and the $m_j$ are as in Lemma 3.1 (d), then we have $|G_\alpha : (G_1 \cap G_{\alpha\gamma})| \geq kd_1 \prod_{j \in L(\gamma)\setminus\{1\}} m_j \geq kd_1 m^{u-1} \geq kd2^{u-1}$. On the other hand, by Lemma 3.1 (c), $|G_\alpha : (G_1 \cap G_{\alpha\gamma})| = u'|\Gamma| \leq kdu$. Thus $d_1 = d$, $|\Gamma| = kd$, and either (i) $u = 1$, or (ii) $u = u' = 2$ and the $M_\delta$-orbit containing $\gamma_i$ (where $L = \{1, i\}$) has length 2. In either case, $\mathrm{MinSubDeg}(G) = k \cdot \mathrm{MinSubDeg}(H)$. Moreover, in case (i), $\Gamma$ has the form considered in the previous paragraph, and part (a) holds.

Assume now that case (ii) holds, and in particular that the $M_\delta$-orbit in $\Delta$ containing $\gamma_i$ has length 2. Then, by [4, Theorem 2.3], $H \leq H_0 \wr S_\ell$ in product action on $\Delta = \Delta_0^\ell$, with primitive component $H_0 \leq \mathrm{Sym}(\Delta_0)$ as in part (b), and with $\mathrm{Soc}(H) = \mathrm{Soc}(H_0 \wr S_\ell)$ (possibly with $\ell = 1$ in which case $H_0 = H$). Moreover, by [4, Lemma 3.2] applied to $M = \mathrm{Soc}(H)$, $M_\delta$ has exactly $2\ell$ orbits of length 2 in $\Delta$, and they form a single orbit $\Gamma''_0$ of $H_\delta$ of length $4\ell$. We also have in case (ii) that $|G_{\alpha\gamma} : (G_1 \cap G_{\alpha\gamma})| = u' = 2$, and hence that $G_{\alpha\gamma}$ is transitive on $L = \{1, i\}$. This implies that $\gamma_1$ and $\gamma_i$ lie in the same $H_\delta$-orbit, and hence that $\Gamma_0' = \Gamma_0''$ of length $4\ell$, and part (b) holds. □

Proof of Corollary 1.2. ¿From the brief descriptions of the O'Nan–Scott types in Section 2, it is clear that Theorem 1.1 applies to all finite primitive permutation groups of types PA, HC and CD. Thus Corollary 1.2 is an immediate consequence of Theorem 1.1. □

Now we demonstrate that there are examples in part (b) of Theorem 1.1. By [4, Lemma 3.2], for $(H, \Delta)$ as in Theorem 1.1 (b), there is a unique $H_\delta$-orbit $\Gamma_0$ in $\Delta \setminus \{\delta\}$ that contains $\mathrm{Soc}(H)_\delta$-orbits of length 2, and this orbit $\Gamma_0$ has length $4\ell$. The proof of Theorem 1.1 shows that, in Theorem 1.1 (b), a minimum length $G_\alpha$-orbit $\Gamma$ in $\Delta^k \setminus \{\alpha\}$ has length $4\ell k$, and for $\gamma = (\gamma_1, \ldots, \gamma_k) \in \Gamma$, exactly two entries of $\gamma$ differ from $\delta$ and these two entries lie in $\Gamma_0$. For simplicity, we will construct examples in the case $\ell = 1$, but examples may be obtained by a similar construction for general $\ell$.

**Proposition 3.2.** *Let $(H, \Delta)$ be as in Theorem 1.1 (b) with $H = H_0$ and $\ell = 1$. Let $\Gamma_0$ be the unique $H_\delta$-orbit in $\Delta \setminus \{\delta\}$ of length 4, and let $M = \mathrm{Soc}(H)$ and $h \in H \setminus M$.*

*(a) Suppose that $k$ is even, and $X$ is any transitive subgroup of $S_k$ with $\{1, 2\}$ as a block of imprimitivity. Then the subgroup*

$$G = \langle M^k, (h, h, \ldots, h), X \rangle$$

*of $H \wr S_k$ is primitive on $\Delta^k$ of type PA, and $G_\alpha$ has two orbits of length $4k$ as in Theorem 1.1 (b).*

*(b) Let $G_0 = \langle M^4, (h, 1, h, 1)(1234), (h, 1, h, 1)(24) \rangle \leq H \wr S_4$. Then $G_0$ is primitive on $\Delta^4$ of type PA, and $G_\alpha$ has four orbits of length $16 = 4k$ as in Theorem 1.1 (b).*

The construction in part (b) above can be generalised for any imprimitive subgroup of $S_k$ inducing $D_8$ on a block of length 4.

Proof. Suppose first that $G, H, \Omega$ satisfy the hypotheses of Theorem 1.1, and that there exists a minimum-length $G_\alpha$-orbit $\Gamma$ in $\Omega \setminus \{\alpha\}$ as in Theorem 1.1 (b), with the parameter $\ell = 1$ and $H = H_0$. Then, as discussed in the paragraph preceding the proposition, there is a unique $H_\delta$-orbit $\Gamma_0$ in $\Delta \setminus \{\delta\}$ of minimum length, $|\Gamma_0| = 4$, and setting $M = \mathrm{Soc}(H)$, $M_\delta$ has two orbits in $\Gamma_0$ of length 2. Moreover, if $\gamma = (\gamma_1, \ldots, \gamma_k) \in \Gamma$ then exactly two of the $\gamma_i$ lie in $\Gamma_0$ and the rest are equal to $\delta$. Suppose without loss of generality that $\gamma_1, \gamma_2 \in \Gamma_0$, and set $L = \{1, 2\}$. Then the proof of Theorem 1.1 shows that $4k = |\Gamma| = |G_\alpha : G_{\alpha,L}|.|G_{\alpha,L} : G_{\alpha\gamma}|$, and we have $(M_\delta)^k = \mathrm{Soc}(G)_\alpha \leq G_{\alpha,L}$. Now $\mathrm{Soc}(G)_\alpha$ has four orbits in $\Omega$ consisting of points of the form $(\gamma_1', \gamma_2', \delta, \ldots, \delta)$ with $\gamma_1', \gamma_2' \in \Gamma_0$, and each of these orbits has length 4. Hence $|G_{\alpha,L} : G_{\alpha\gamma}|$ is a multiple of 4. Since $G_\alpha$ is transitive on $\{1, \ldots, k\}$, $|G_\alpha : G_{\alpha,L}| \geq k/2$, and hence is equal to either $k/2$ or $k$. The examples in parts (a) and (b) correspond to the cases $k/2$ and $k$ respectively.

If $|G_\alpha : G_{\alpha,L}| = k/2$, then $L$ is a block of imprimitivity for the action of $G$ on $\{1, \ldots, k\}$, and we must have $|G_{\alpha,L} : G_{\alpha\gamma}| = 8$. If $X$ is any transitive subgroup of $S_k$ for which $L$ is a block of imprimitivity, then the subgroup $G = \langle M^k, (h, h, \ldots, h), X\rangle$ of $H \wr S_k$ is primitive on $\Delta^k$ of type PA and $G_\alpha$ has one orbit of (minimum) length $4k$ as in Theorem 1.1 (a), and two additional orbits of length $4k$ that contain some points of the form $(\gamma_1', \gamma_2', \delta, \ldots, \delta)$, where $\gamma_1', \gamma_2' \in \Gamma_0$.

On the other hand, if $|G_\alpha : G_{\alpha,L}| = k$ then $L$ is not a block of imprimitivity for the action of $G$ on $\{1, \ldots, k\}$. If $k = 4$, we have the following example for this case: $G = \langle M^4, (h, 1, h, 1)(1234), (h, 1, h, 1)(24)\rangle$ is a primitive subgroup of $H \wr S_4$ of type PA, $G_\alpha$ has one orbit of (minimum) length 16 as in Theorem 1.1 (a), two orbits of length 16 as in the previous paragraph corresponding to the block of imprimitivity $\{1, 3\}$ of $D_8$, and two additional orbits of length 16 (and one of length 32) that contain some points of the form $(\gamma_1, \gamma_2, \delta, \delta)$, where $\gamma_1, \gamma_2 \in \Gamma_0$. □

Proof of Theorem 1.4. Let $G, H, k, \alpha, \delta$ be as in Theorem 1.1, and let $\Gamma$ be a symmetric $G_\alpha$-invariant subset of $\Delta^k \setminus \{\alpha\}$ of length $\mathrm{MinVal}(G)$. Then $\Gamma$ is a union $\bigcup_{i\in I} \Sigma_i$, where each $\Sigma_i$ is a $G_\alpha$-orbit in $\Delta^k \setminus \{\alpha\}$. Thus

$$\mathrm{MinVal}(G) = |\Gamma| \geq |I| \cdot \mathrm{MinSubDeg}(G). \tag{3.1}$$

Next let $\Sigma$ be a $G_\alpha$-orbit of length $\mathrm{MinSubDeg}(G)$. Then $\Sigma \cup \Sigma^*$ is a symmetric $G_\alpha$-invariant subset of $\Delta^k \setminus \{\alpha\}$ of length $|\Sigma|$ if $\Sigma$ is symmetric, or $2|\Sigma|$ otherwise, and it follows that

$$\mathrm{MinVal}(G) \leq |\Sigma \cup \Sigma^*| \leq 2\,\mathrm{MinSubDeg}(G) \tag{3.2}$$

and similarly $\mathrm{MinVal}(H) \leq 2\,\mathrm{MinSubDeg}(H)$. Hence, for the $G_\alpha$-invariant subset $\Gamma = \bigcup_{i\in I} \Sigma_i$ in the previous paragraph, the set $I$ has size at most 2.

Now let $\Phi_0$ be a symmetric $H_\delta$-invariant subset of $\Delta \setminus \{\delta\}$ of length $\mathrm{MinVal}(H)$, and let $\Phi$ be the subset of $\Delta^k \setminus \{\alpha\}$ constructed as in Theorem 1.1 (a) using $\Phi_0$ as the set $\Gamma_0$. Then $\Phi$ is a symmetric $G_\alpha$-invariant subset of $\Delta^k \setminus \{\alpha\}$ and hence $k \cdot |\Phi_0| = |\Phi| \geq \mathrm{MinVal}(G)$. Thus

$$\mathrm{MinVal}(G) \leq k \cdot \mathrm{MinVal}(H) \leq 2k \cdot \mathrm{MinSubDeg}(H). \tag{3.3}$$

Suppose first that there is a symmetric $G_\alpha$-orbit $\Sigma$ of length $\mathrm{MinSubDeg}(G)$. Then every symmetric $G_\alpha$-invariant subset of $\Delta^k \setminus \{\alpha\}$ of length $\mathrm{MinVal}(G)$ is a single symmetric $G_\alpha$-orbit of length $\mathrm{MinSubDeg}(G)$. Hence by Theorem 1.1, $\mathrm{MinVal}(G) = k \cdot \mathrm{MinSubDeg}(H)$ and all such $\Gamma$ must satisfy (a) or (b) of that theorem. In case (a), since $\Gamma$ is symmetric it follows that the $H_\delta$-orbit $\Gamma_0$ involved is also symmetric, and hence $\mathrm{MinVal}(G) = k \cdot \mathrm{MinVal}(H)$. Also, in case (b), it follows from [4, Lemma 3.2] that in this case also $\Gamma_0$ is symmetric (see also the discussion before Proposition 3.2) so again we find that $\mathrm{MinVal}(G) = k \cdot \mathrm{MinVal}(H)$. Thus

Theorem 1.4 is proved in this case. We may therefore assume that all $G_\alpha$-orbits of length $\mathrm{MinSubDeg}(G)$ are non-symmetric.

Suppose next that $\Gamma = \Sigma_1 \cup \Sigma_2$ is a symmetric $G_\alpha$-invariant subset of length $\mathrm{MinVal}(G)$ in $\Delta^k \setminus \{\alpha\}$, where $\Sigma_2 \neq \Sigma_1$. Then by (3.1) and (3.2), $|\Sigma_1| = |\Sigma_2| = \mathrm{MinSubDeg}(G)$, $\Sigma_1^* = \Sigma_2$, and $\mathrm{MinVal}(G) = 2\,\mathrm{MinSubDeg}(G)$. Moreover, by Theorem 1.1, and since the $\Sigma_i$ are not symmetric, it follows as above that Theorem 1.1 (a) holds for each $\Sigma_i$. Thus for each $i \in I$ there exists an $H_\delta$-orbit $\Gamma_{i0}$ of length $\mathrm{MinSubDeg}(H)$ such that $\Sigma_i = \bigcup_{1\le j\le k} \Sigma_{ij}$, where $\Sigma_{ij}$ consists of all $k$-tuples $(\delta_1, \ldots, \delta_k)$ such that $\delta_\ell = \delta$ for $\ell \neq j$ and $\delta_j \in \Gamma_{i0}$. Then since $\Gamma$ is symmetric it follows that $\Gamma_{10}^* = \Gamma_{20}$, and hence (a) holds for $\Gamma$ with $\Gamma_0 = \Gamma_{10} \cup \Gamma_{20}$. Also, by Theorem 1.1, $\mathrm{MinVal}(G) = 2\,\mathrm{MinSubDeg}(G) = 2k \cdot \mathrm{MinSubDeg}(H)$ and applying (3.3) we conclude that $\mathrm{MinVal}(H) = 2\,\mathrm{MinSubDeg}(H)$ so that Theorem 1.4 is proved in this case also.

Thus we may assume in addition that each symmetric $G_\alpha$-invariant subset $\Gamma$ of $\Delta^k \setminus \{\alpha\}$ of length $\mathrm{MinVal}(G)$ is a $G_\alpha$-orbit. Then, since all $G_\alpha$-orbits of length $\mathrm{MinSubDeg}(G)$ are non-symmetric, we have $\mathrm{MinVal}(G) > \mathrm{MinSubDeg}(G)$.

By Lemma 3.1 (c), $\Gamma$ contains a point $\gamma = (\gamma_1, \ldots, \gamma_k) \in \Gamma$ with $\gamma_1 \neq \delta$. Let $L(\gamma)$ denote the set of all $i$ such that $\gamma_i \neq \delta$ and $u = |L(\gamma)|$. If $u = 1$ then $\Gamma$ is as in Theorem 1.1 (a) for some symmetric $H_\delta$-invariant subset $\Gamma_0$ of $\Delta \setminus \{\delta\}$, so $\mathrm{MinVal}(G) = |\Gamma| = k\,|\Gamma_0| \geq k \cdot \mathrm{MinVal}(H)$, and equality holds by (3.3). If $u = 1$ for all such $\Gamma$ then Theorem 1.4 is proved. Thus we may assume that $u \geq 2$ for some $\Gamma$. Then by Lemma 3.1 (c) and (3.3),

$$|G_\alpha : (G_1 \cap G_{\alpha\gamma})| = |\Gamma| \cdot u' \leq ku'\mathrm{MinVal}(H) \leq 2ku'\,\mathrm{MinSubDeg}(H) \tag{3.4}$$

and $u' \leq u$, while by Lemma 3.1 (d) (using the notation there),

$$|G_\alpha : (G_1 \cap G_{\alpha\gamma})| \geq k\ \mathrm{MinSubDeg}(H) \cdot \prod_{i \in L\setminus\{1\}} m_i \geq k\,\mathrm{MinSubDeg}(H) m^{u-1}. \tag{3.5}$$

If $m = 2$ then by [4, Lemma 3.2] there is a symmetric $H_\delta$-orbit $\Gamma_0$ of length $\mathrm{MinSubDeg}(H)$, and $\Gamma_0$ can be used as in Theorem 1.1 (a) to construct $G_\alpha$-orbits of length $\mathrm{MinSubDeg}(G)$ that are symmetric since $\Gamma_0$ is symmetric. However we are assuming that all such suborbits are non-symmetric, and hence $m \geq 3$. Thus $3^{u-1} \leq m^{u-1} \leq 2u' \leq 2u$, and hence $u = u' = 2$ and $m \leq 4$. Without loss of generality $L(\gamma) = \{1, 2\}$. By Lemma 3.1 (c), since $u' = 2$, it follows that $G_{\alpha\gamma}$ contains an element $g$ that interchanges positions 1 and 2 in the $k$-tuples in $\Delta^k$, say $g = (h_1, \ldots, h_k)\sigma$ where $\sigma \in S_k$ and $\sigma$ interchanges 1 and 2. Since $g$ fixes $\gamma$ we have $\gamma_1^{h_1} = \gamma_2$ and $\gamma_2^{h_2} = \gamma_1$, and since $g$ fixes $\alpha$ each of the $h_i$ must fix $\delta$. In particular, $\gamma_1$ and $\gamma_2 = \gamma_1^{h_1}$ lie in the same $H_\delta$-orbit. Moreover, since $\Gamma$ is a symmetric $G_\alpha$-orbit, $G$ also contains an element $g' = (h'_1, \ldots, h'_k)\sigma'$ that interchanges $\alpha$ and $\gamma$. Since $g'$ maps $\gamma$ to $\alpha$ we have that $\gamma_1^{h'_1} = \gamma_2^{h'_2} = \delta$ and $h'_i$ fixes $\delta$ for all $i > 2$. Let $j$ be such that $j^{\sigma'} = 1$. Then since $g'$ maps $\alpha$ to $\gamma$ we have that $\delta^{h'_j} = \gamma_1$. In particular this means that $j \leq 2$. If $j = 1$ then $h'_1$ interchanges $\delta$ and $\gamma_1$, while if $j = 2$ then $h'_2 h_1$ interchanges $\delta$ and $\gamma_2$. In either case, since the points $\gamma_1$ and $\gamma_2$ lie in the same $H_\delta$-orbit in $\Delta \setminus \{\delta\}$, the $H$-orbit $(\delta, \gamma_1)^H$ in $\Delta \times \Delta$

is symmetric. Hence in (3.5), we can replace $\mathrm{MinSubDeg}(H)$ by $\mathrm{MinVal}(H)$, and combining with (3.4) we obtain $m^{u-1} \le u$, which is impossible. Thus the proof of Theorem 1.4 is complete. $\square$

## 4. Proof of Theorem 1.5

We define a twisted wreath product by following the description in [15, page 269]. Let $T$ be a finite non-abelian simple group, $P$ a group with a proper subgroup $Q$ and let $\phi : Q \to \mathrm{Aut}(T)$ be a homomorphism. We define the *complete base group* $\mathcal{B}$ to be the set of maps $f : P \to T$ under pointwise multiplication and so $\mathcal{B} \cong T^{|P|}$. The group $P$ acts on $\mathcal{B}$ by

$$f^p(x) = f(px) \text{ for all } x, p \in P, f \in \mathcal{B}.$$

We define $\mathcal{X}$ to be the semidirect product $\mathcal{B} \rtimes P$ with respect to this action. Define the *$\phi$–base group*

$$B_\phi = \{f : P \to T \mid f(pq) = f(p)^{\phi(q)} \text{ for all } p \in P, q \in Q\}. \tag{4.1}$$

This group is isomorphic to $T^k$ where $k = |P : Q|$. Also $B_\phi$ is normalised by $P$, and so $B_\phi$ and $P$ generate the subgroup $X_\phi = B_\phi \rtimes P$ of $\mathcal{X}$ which we call the *twisted wreath product* $T \,\mathrm{twr}_\phi\, P$ of $T$ by $P$ with respect to $\phi$. This group $X_\phi$ acts faithfully and transitively on $\Omega = B_\phi$ as follows: each element of $X_\phi$ is of the form $f' \cdot p$ with $f' \in B_\phi$ and $p \in P$, and maps $f \in B_\phi$ to $(f \cdot f')^p$, where $(f \cdot f')^p(x) = f(px) \cdot f'(px)$ (for $x \in P$). The subgroup $B_\phi \le X_\phi$ is regular, and $B_\phi = \mathrm{Soc}(X_\phi)$.

The action is primitive if and only if $\mathrm{Inn}(T) \leqslant \phi(Q)$, $\phi^{-1}(\mathrm{Inn}(T))$ is a core free subgroup of $P$, and $\phi$ extends to no larger subgroup of $P$ (see [2]). Under these conditions, $X_\phi$ is primitive of type TW and, as described in Section 2, $X_\phi \le H \wr P \le \mathrm{Sym}(T) \wr S_k$ in product action on $\Omega = T^k$. The primitive component $H$ is the semidirect product $H = T \rtimes \phi(Q)$, acting on $T$. The orbits of the stabilizer $H_1$ of $1 \in T$ are the conjugacy classes of $T$ under $\phi(Q)$ and so $\mathrm{MinSubDeg}(H) = \mathcal{C}_{\phi(Q)}(T)$, the length of the shortest non-trivial conjugacy class of $T$ under $\phi(Q)$.

For $f \in B_\phi$ and $R \le P$, let $f^R = \{f^p \mid p \in R\}$ denote the $R$-orbit containing $f$. The suborbit $f^P$ of $X_\phi$ containing $f$ has length $|P : C_P(f)|$. For $p \in P$, $p \in C_P(f)$ if and only if $f^p(x) = f(px) = f(x)$ for all $x \in P$. Note that if $f(px) = f(x)$ for some $x \in P$, then $f(py) = f(y)$ for all $y \in xQ$, since $y = xq$ for some $q \in Q$ and so $f(py) = f(pxq) = f(px)^{\phi(q)} = f(x)^{\phi(q)} = f(xq) = f(y)$. Thus to check that $f^p = f$ it is sufficient to check that $f(px) = f(x)$ for all $x$ in some left transversal for $Q$ in $P$. We have the following important construction of elements in $B_\phi$.

**Construction 4.1.** Let $t \in T \backslash \{1\}$ and $R < P$ such that $\phi(Q \cap R) \leqslant C_{\mathrm{Aut}(T)}(t)$. We define the element $f = f_{R,t}$ as follows. For each $x \in R$ and $q \in Q$ let $f(xq) = t^{\phi(q)}$, and for each $x \in P \backslash RQ$ let $f(x) = 1$. This function $f$ is well-defined since if $xq = x'q'$, with $x, x' \in R$ and $q, q' \in Q$, then $q'q^{-1} = (x')^{-1}x \in Q \cap R$, and hence $\phi(q'q^{-1})$ centralises $t$, whence $t^{\phi(q)} = t^{\phi(q')}$. Also it follows from the definition that $f \in B_\phi$. We also define the following set

$$\mathcal{R} = \{(R,t) \mid t \in T, R < P, R \cap Q \leqslant \phi^{-1}(C_{\phi(Q)}(t))\}.$$

We now show that $R$ stabilises $f_{R,t}$.

**Lemma 4.2.** *Suppose that* $X_\phi = T \operatorname{twr}_\phi P$ *is primitive with primitive component* $H = T \rtimes \phi(Q)$ *and let* $(R,t) \in \mathcal{R}$. *Then* $f_{R,t}$ *is the unique element* $f \in B_\phi$ *such that* $f(x) = t$ *for all* $x \in R$ *and* $f(x) = 1$ *for all* $x \notin RQ$. *Moreover,* $R \leq C_P(f_{R,t})$ *and the subdegree* $|(f_{R,t})^P|$ *divides* $|P : R|$.

Proof. Let $f_{R,t}$ as obtained by Construction 4.1. Since $R \cup (P\backslash RQ)$ contains a set of coset representatives for $Q$ in $P$, any function in $B_\phi$ agreeing with $f_{R,t}$ on $R \cup (P\backslash RQ)$, is equal to $f_{R,t}$. Hence the first part of the lemma follows.

Let $f = f_{R,t}$ and let $r \in R$. Then for all $x \in R$, we have $rx \in R$ and so $f^r(x) = f(rx) = t$. Moreover, for all $x \notin RQ$ we have $rx \notin RQ$ and so $f^r(x) = f(rx) = 1$. Then as $f$ is the unique such element of $B_\phi$ it follows that $f^r = f$. Thus $R \leqslant C_P(f)$ and so the stabiliser in $P$ of $f$ contains $R$, whence $|f^P|$ divides $|P : R|$. □

We now show that the elements $f_{R,t}$ determine the minimum subdegree of $X_\phi$.

**Lemma 4.3.** *Let* $X_\phi = T \operatorname{twr}_\phi P$ *be a primitive permutation group acting on its base group* $B_\phi$. *Then* $\mathrm{MinSubDeg}(X_\phi) = \min\{|(f_{R,t})^P| \mid (R,t) \in \mathcal{R}\}$. *Moreover, for some* $(R,t) \in \mathcal{R}$, $\mathrm{MinSubDeg}(X_\phi) = |(f_{R,t})^P| = |P : R| \leq k \cdot \mathrm{MinSubDeg}(H)$.

Proof. Let $f \in B_\phi$ such that $|f^P| = \mathrm{MinSubDeg}(X_\phi)$. As $|f^P| > 1$, $f \neq 1$ and so there exists $p \in P$ such that $1 \neq f(p) = f^p(1)$. Hence there exists $p \in P$ such that $t = f^p(1) \neq 1$. Let $R$ be the stabiliser in $P$ of $f^p$. Let $q \in Q \cap R$. Then $t = f^p(1) = (f^p)^q(1) = f^p(q) = (f^p(1))^{\phi(q)} = t^{\phi(q)}$. Hence $\phi(Q \cap R) \leqslant C_{\phi(Q)}(t)$. Define $f_{R,t}$ as given by Construction 4.1. Then by Lemma 4.2, the subdegree $|(f_{R,t})^P|$ divides $|P : R|$. However, $|P : R| = |f^P| = \mathrm{MinSubDeg}(X_\phi)$ and so $|(f_{R,t})^P| = |P : R|$. Thus the first parts of the lemma hold.

Let $t \in T$ with $|t^{\phi(Q)}| = \mathcal{C}_{\phi(Q)}(T)$, the length of the smallest nontrivial conjugacy class of $T$ under $Q$, and $R = \phi^{-1}(C_{\phi(Q)}(t)) \leqslant Q$. Then $|(f_{R,t})^P| \leq |P : R| = k \cdot \mathrm{MinSubDeg}(H)$, and hence we obtain $\mathrm{MinSubDeg}(X_\phi) \leq k \cdot \mathrm{MinSubDeg}(H)$. □

Note that Lemma 4.3 does not assert that all minimal length suborbits are of the form $(f_{R,t})^P$, and indeed this need not be the case, see Lemma 4.13 and Example 4.14.

We now establish lower bounds on $\mathrm{MinSubDeg}(X_\phi)$.

**Lemma 4.4.** *Suppose that* $X_\phi = T \operatorname{twr}_\phi P$ *is primitive with primitive component* $H = T \rtimes \phi(Q)$. *Then* $\mathrm{MinSubDeg}(X_\phi) \geq \mathrm{MinSubDeg}(H)$.

Proof. Fix a set $\{c_1, c_2, \ldots, c_k\}$ of left coset representatives for $Q$ in $P$ with $c_1 \in Q$, and identify $B_\phi = \mathrm{Soc}(X_\phi)$ with $T^k = T_1 \times \cdots \times T_k$, by the map $f \mapsto$

$(f(c_1),\dots,f(c_k))$. Let $\alpha \in B_\phi$ denote the function $f(c_1)=\cdots=f(c_k)=1$, so $\alpha = 1_{B_\phi}$ and $P=(X_\phi)_\alpha$. Let $P_i$ denote the stabilizer of $T_i$ in the conjugation action of $P$ on $\{T_1,\dots,T_k\}$. We have $P_1=Q$, since $Q \leqslant P_1$ by (4.1), and $|P:P_1| = k = |P:Q|$. Moreover, it follows from (4.1) that the subgroup of $\mathrm{Aut}(T_1)$ induced by the conjugation action of $P_1$ is $\phi(Q)$.

Let $f \in B_\phi$ be arbitrary, satisfying $f(c_1)\neq 1$. Then $|f^P| \geq |f^{P_1}|$, and this latter quantity is at least $\mathcal{C}_{\phi(Q)}(T)$ since the functions in $f^{P_1}$ have at least so many different first coordinates. Since any $g \in B_\phi \setminus \{\alpha\}$ satisfies $g(c_i)\neq 1$ for some $i$, it follows that $|g^P| \geq |g^{P_i}| \geq \mathcal{C}_{\phi(Q)}(T)$. Hence $\mathrm{MinSubDeg}(X_\phi) = \min\{|f^P| \mid f \in B_\phi \setminus \{\alpha\}\} \geq \mathcal{C}_{\phi(Q)}(T) = \mathrm{MinSubDeg}(H)$. □

We can determine a necessary and sufficient condition for equality to hold in Lemma 4.4.

**Lemma 4.5.** *Suppose that $X_\phi = T\,\mathrm{twr}_\phi\, P$ is primitive with primitive component $H = T \rtimes \phi(Q)$ and let $f \in B_\phi$. Then $|f^P| = \mathrm{MinSubDeg}(H)$ if and only if $f = f_{R,t}$ as obtained by Construction 4.1, where $|t^{\phi(Q)}| = \mathrm{MinSubDeg}(H)$, $R$ is transitive on $\{1,\dots,k\}$ and $R \cap Q = \phi^{-1}(C_{\phi(Q)}(t))$.*

Proof. Suppose first that $f = f_{R,t}$ as stated in the lemma. Then

$$\begin{aligned}|P:R| &= \frac{k|Q:R\cap Q|}{|R:R\cap Q|}\\ &= |Q:R\cap Q| && \text{since } R \text{ is transitive}\\ &= \mathcal{C}_{\phi(Q)}(T) && \text{since } R\cap Q = \phi^{-1}(C_{\phi(Q)}(t))\\ &= \mathrm{MinSubDeg}(H).\end{aligned}$$

By Lemma 4.2, $|f^P|$ divides $|P:R|$ and so by Lemma 4.4, equality holds.

Conversely, suppose that $|f^P| = \mathrm{MinSubDeg}(H)$. As $|f^P|>1$, $f\neq 1$ and so there exists $p\in P$ with $1\neq f(p) = f^p(1)$. Hence there exists $p \in P$ such that $t = f^p(1)\neq 1$.

Now $(f^p)^P = f^P$ and so $\mathrm{MinSubDeg}(H) = |(f^p)^P| \geq |(f^p)^Q|$. However, for $q \in Q$, $f^{pq}(1) = f^p(q) = (f^p(1))^{\phi(q)} = t^{\phi(q)}$. So $|(f^p)^Q| \geq \mathcal{C}_{\phi(Q)}(t) \geq \mathrm{MinSubDeg}(H)$. Hence $(f^p)^P = (f^p)^Q$ and $|t^{\phi(Q)}| = \mathrm{MinSubDeg}(H)$.

Let $R$ be the stabiliser in $P$ of $f^p$. Since $(f^p)^P = (f^p)^Q$ it follows that $Q$ is transitive on $(f^p)^P$. Hence $P = RQ$ and so $R$ is transitive on $\{1,\dots,k\}$.

For all $r\in R$, $r^{-1}$ fixes $f^p$ and so $f^p(r) = f^{pr^{-1}}(1) = f^p(1) = t$. Then as $P = RQ$ it follows from (4.1) that the set of values taken by $f$ is contained in $t^{\phi(Q)}$. Hence $f(1)\neq 1$ and we can choose $p=1$, that is, $f(r)=t$ for all $r\in R$. Let $g \in R\cap Q$. Since $g\in R$ we have $f^g = f$, and in particular, $f(g)=t$. On the other hand, since $g\in Q$ and using (4.1), $f(g) = f(1)^{\phi(g)} = t^{\phi(g)}$, and it follows that $g \in \phi^{-1}(C_{\phi(Q)}(t))$. Thus $\phi(Q\cap R) \leqslant C_{\phi(Q)}(t)$. Since $P = RQ$, Lemma 4.2 implies that $f_{R,t}$ is the unique element of $B_\phi$ which evaluates to $t$ at each element of $R$. Hence $f = f_{R,t}$. By assumption $\mathrm{MinSubDeg}(H) = |f^P|$, which by the definition of $R$ is equal to

$$\begin{aligned}|P:R| &= \frac{|P:Q||Q:Q\cap R|}{|R:Q\cap R|}\\ &= \frac{k}{k}|Q:\phi^{-1}(C_{\phi(Q)}(t)||\phi^{-1}(C_{\phi(Q)}(t)):Q\cap R|\\ &= \mathrm{MinSubDeg}(H)|\phi^{-1}(C_{\phi(Q)}(t)):Q\cap R|.\end{aligned}$$

Hence $R\cap Q=\phi^{-1}(C_{\phi(Q)}(t))$ and the proof is complete. □

The following general construction will be used to obtain examples exhibiting this behaviour.

**Construction 4.6.** Let $Q$ be an almost simple group with socle $T$ and let $t$ be an element from the smallest $Q$–conjugacy class of $T$. Then $Q$ acts faithfully on a set of size $n=|t^Q|$. Let $P=S_n$, $k=|P:Q|$ and $\phi:Q\to\mathrm{Aut}(T)$ such that $\phi(q)$ is conjugation by $q$. This allows us to construct $X_\phi=T\,\mathrm{twr}_\phi\,P$. Suppose that $\phi$ does not extend to any overgroup of $Q$ in $P$. Then the action of $X_\phi$ on $B_\phi\cong T^k$ is primitive with primitive component $H=T\rtimes\phi(Q)$ (see [11]), and it follows from the definition of $t$ that $n=\mathrm{MinSubDeg}(H)$. Let $R=S_{n-1}$. Since $Q$ is a transitive subgroup of $P$ in its action on $n$ points, $P=RQ$ and hence $R$ acts transitively on $[P:Q]$. Furthermore, $R\cap Q=\phi^{-1}(C_{\phi(Q)}(t))$. Thus we may apply Construction 4.1 and obtain an element $f=f_{R,t}$. By Lemma 4.2, $|f^P|$ divides $|P:R|$. However, $|P:R|=n=\mathrm{MinSubDeg}(H)=\mathrm{MinDeg}(P)$ and so by Lemma 4.4, $\mathrm{MinSubDeg}(X_\phi)=\mathrm{MinSubDeg}(H)=\mathrm{MinDeg}(P)$.

We now provide examples of groups $Q$ to which we can apply Construction 4.6.

**Example 4.7.** Let $p\equiv 3\pmod 4$ be a prime and let $Q=\mathrm{PGL}(2,p)$. Then the smallest $Q$-conjugacy class in $T=\mathrm{PSL}(2,p)$ is the set of involutions. Let $t$ be an involution. Then $|t^Q|=p(p-1)/2$ and $C_Q(t)=D_{2(p+1)}$. Thus $C_Q(t)$ is a maximal subgroup of $Q$. Let $n=p(p-1)/2$. Then as $Q=\mathrm{Aut}(T)$ and $Q$ is a primitive subgroup of $S_n$, it follows that $N_{S_n}(Q)=Q$. By [10], if $p\equiv 7\pmod 8$ then $Q$ is a maximal subgroup of $A_n$ while if $p\equiv 3\pmod 8$ then $Q$ is a maximal subgroup of $S_n$. Hence, as $N_{S_n}(Q)=Q$, the only possible overgroups of $Q$ in $P$ are $A_n$ or $S_n$. However, neither of these two groups have $\mathrm{PGL}(2,p)$ as a homomorphic image and so it follows that $\phi:Q\to\mathrm{Aut}(T)$ does not extend to any larger subgroup of $P=S_n$. Hence we can use Construction 4.6 to obtain a primitive group $X_\phi=T\,\mathrm{twr}_\phi\,P$ such that $\mathrm{MinSubDeg}(X_\phi)=\mathrm{MinSubDeg}(H)=\mathrm{MinDeg}(P)$.

**Example 4.8.** Let $Q=T=J_1$ and $t$ be one of the 1463 involutions. Then $C_Q(t)$ is a maximal subgroup of $Q$ and by [10], $Q$ is a maximal subgroup of $A_{1463}$. Moreover, as $Q=\mathrm{Aut}(T)$ it follows that $N_{S_{1463}}(Q)=Q$. Thus the only overgroups of $Q$ in $P=S_{1463}$ are $A_{1463}$ and $P$. As neither group has $J_1$ as a homomorphic image, it follows that $\phi:Q\to\mathrm{Aut}(T)$ does not extend to any larger subgroup of $P$. Hence we can use Construction 4.6 to obtain a primitive group $X_\phi=T\,\mathrm{twr}_\phi\,P$ such that $\mathrm{MinSubDeg}(X_\phi)=\mathrm{MinSubDeg}(H)=\mathrm{MinDeg}(P)$.

**Example 4.9.** Let $Q = T = M_{11}$ and $t$ be one of the 165 involutions. Then $C_Q(t)$ is a maximal subgroup of $Q$ and as $Q = \mathrm{Aut}(T)$ it follows that $N_{S_{165}}(Q) = Q$. Then by [10], the only overgroups of $Q$ in $P = S_{165}$ are $A_{11}, S_{11}, A_{165}$ and $S_{165}$. Since none of these four subgroups have $M_{11}$ as a homomorphic image it follows that $\phi : Q \to \mathrm{Aut}(T)$ does not extend to any larger subgroup of $P$. Hence we can use Construction 4.6 to obtain a primitive group $X_\phi = T \,\mathrm{twr}_\phi\, P$ such that $\mathrm{MinSubDeg}(X_\phi) = \mathrm{MinSubDeg}(H) = \mathrm{MinDeg}(P)$.

We also have another lower bound on $\mathrm{MinSubDeg}(X_\phi)$ which, together with Lemma 4.4, establishes the lower bound for the first assertion of Theorem 1.5.

**Lemma 4.10.** *Suppose that* $X_\phi = T \,\mathrm{twr}_\phi\, P$ *is primitive. Then* $\mathrm{MinSubDeg}(X_\phi) \geq \mathrm{MinDeg}(P)$.

Proof. Using the notation introduced in the proof of Lemma 4.4, for any $f \in B_\phi \setminus \{\alpha\}$ the group $P$ acts transitively on $f^P$ by definition. Hence if we prove that $P$ acts faithfully on $f^P$ then it follows that $\mathrm{MinSubDeg}(X_\phi) = \min\{|f^P| : f \in B_\phi \setminus \{\alpha\}\} \geq \mathrm{MinDeg}(P)$.

The subgroup $F := \langle f^P \rangle$ of $B_\phi$ is normalised by $P$, and hence the product $FP$ is a subgroup satisfying $P < FP \leq X_\phi$. Since $X_\phi$ is primitive, the stabiliser $P$ is maximal and hence $FP = X_\phi$, which implies that $F = B_\phi$. Suppose that some $p \in P$ acts trivially on $f^P$. Then $p$ centralises a generating set of $B_\phi$, so $p$ centralises $B_\phi$. However, $C_{X_\phi}(B_\phi)$ is normal in $X_\phi$ since $B_\phi$ is normal, and $C_{X_\phi}(B_\phi)$ intersects $B_\phi$ trivially. Thus, since $B_\phi$ is the unique minimal normal subgroup of $X_\phi$, it follows that $C_{X_\phi}(B_\phi) = 1$. Hence $p = 1$. □

The following example provides an instance where $\mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = \max\{\mathrm{MinDeg}(P), \mathrm{MinSubDeg}(H)\}$, but $\mathrm{MinDeg}(P) \neq \mathrm{MinSubDeg}(H)$.

**Example 4.11.** Let $p$ be a prime with $p \equiv \pm 1 \pmod 5$, let $P = \mathrm{PSL}(2,p)$, $T = A_5$, $Q \cong A_5$, and let $\phi$ be an isomorphism between $Q$ and $\mathrm{Inn}(A_5)$. Moreover, let $R$ be a maximal parabolic subgroup of $P$. Then $R \cap Q$ is trivial, or a cyclic subgroup $\langle t \rangle$ for some $t \in Q$. In any case, there exists $t \in Q$ with $R \cap Q \leq \langle t \rangle$, and for this $t$, we have, by Lemma 4.2, $|f_{R,t}^P| \leq |P : R| = p + 1$. If $p > 11$ then $\mathrm{MinDeg}(P) = p+1$, and it follows from Lemma 4.10 that $\mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = \mathrm{MinDeg}(P) = p + 1 > \mathrm{MinSubDeg}(H) = 12$. If $p = 11$, then $\mathrm{MinDeg}(P) = 11$ and so by Lemma 4.4, $\mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = 12 = \mathrm{MinSubDeg}(H)$.

We now give another construction of elements in $B_\phi$ which allows us to construct minimal length suborbits other than $(f_{R,t})^P$.

**Construction 4.12.** Let $R < P$ and choose a set $S = \{s_1, \ldots, s_l\}$ of representatives for the $(R, Q)$–double cosets in $P$. Suppose that for each $s_i$, there exists $t_i \in T$ such that $\phi(R^{s_i} \cap Q) \leqslant C_{\mathrm{Aut}(T)}(t_i)$. We define the element $f = f_{R,S,t_1,\ldots,t_l} \in B_\phi$ as follows. For all $x \in Rs_i$, let $f(x) = t_i$ and for each $q \in Q$ let $f(xq) = f(x)^{\phi(q)} = t_i^{\phi(q)}$. Note that this is well defined, since if $xq \in Rs_i$, then $q \in R^{s_i} \cap Q$ and so $\phi(q)$

centralises $t_i$. Thus $f \in B_\phi$. Note also, that if $s_1 \in R$ then $f_{R,S,t_1,1,\ldots,1} = f_{R,t}$ as yielded by Construction 4.1.

**Lemma 4.13.** *Suppose that* $X_\phi = T \operatorname{twr}_\phi P$ *is primitive with primitive component* $H = T \rtimes \phi(Q)$. *Let* $S = \{s_1, \ldots, s_l\}$ *be a set of representatives for the* $(R, Q)$*-double cosets in* $P$ *and let* $t_1, \ldots, t_l \in T$ *such that* $\phi(R^{s_i} \cap Q) \leqslant C_{\mathrm{Aut}(T)}(t_i)$. *Then the element* $f_{R,S,t_1,\ldots,t_l} \in B_\phi$ *obtained from Construction* 4.12 *is the unique element* $f \in B_\phi$ *such that for each* $i = 1, \ldots, l$, $f(x) = t_i$ *for all* $x \in Rs_i$. *Furthermore,* $R \leqslant C_P(f_{R,S,t_1,\ldots,t_l})$ *and if* $(f_{R,t_1})^P$ *is a minimal length nontrivial suborbit and at least one of* $t_2, \ldots, t_l$ *is nontrivial then* $(f_{R,S,t_1,\ldots,t_l})^P$ *is also a minimal length suborbit which is not of the form* $(f_{R',t})^P$ *for any* $(R', t) \in \mathcal{R}$.

Proof. Since $Rs_1 \cup \ldots \cup Rs_l$ contains a set of left coset representatives for $Q$ in $P$, it follows that $f_{R,S,t_1,\ldots,t_l}$ is the unique element $f \in B_\phi$ such that for all $i = 1, \ldots, l$ and $x \in Rs_i$, we have $f(x) = t_i$.

Let $f = f_{R,S,t_1,\ldots,t_l}$ and let $r \in R$ be arbitrary. Let $i \in \{1, \ldots, l\}$ and let $x \in Rs_i$. Then $rx \in Rs_i$ and so $f^r(x) = f(rx) = t_i$. As this is true for all $i$, it follows by the uniqueness of $f$, that $f^r = f$ and so $R \leqslant C_P(f)$. If $(f_{R,t_1})^P$ is a minimal length nontrivial suborbit then $t_1 \neq 1$ and by Lemma 4.2, $R$ is the stabiliser of $f_{R,t_1}$ in $P$. We have just proved that $R$ fixes $f$, and hence, by the minimality of $|(f_{R,t_1})^P|$, and Lemma 4.3, it follows that $R = C_P(f)$ and $|f^P| = |(f_{R,t_1})^P|$. Finally we prove that $f^P$ does not contain $f_{R',t}$ for any $(R', t) \in \mathcal{R}$. Suppose to the contrary that $f_{R',t} \in f^P$ for some $(R', t) \in \mathcal{R}$. Then, by Lemmas 4.2 and 4.3, and the minimality of $|f^P|$, it follows that $R'$ is the stabiliser of $f_{R',t}$ in $P$. Since $R$ is the stabiliser of $f$ it follows that $R' = R^p$ for some $p \in P$. However, $f_{R',t}$ is nontrivial on a single double $(R', Q)$-coset in $P$, whereas, by assumption, $f$ is nontrivial on at least two double $(R, Q)$-cosets. Hence $(f_{R,S,t_1,\ldots,t_l})^P$ is not of the form $(f_{R',t})^P$, for any $(R', t) \in \mathcal{R}$. □

**Example 4.14.** Let $P$, $T$, $Q$, $\phi$, $R$ and $t$ be as in Example 4.11. Note that for $p > 11$, we have $\mathrm{MinSubDeg}(X_\phi) > \mathrm{MinSubDeg}(H)$. When $p > 60$, $R$ is intransitive on the set of left cosets of $Q$ in $P$. Choose a set $S = \{s_1, s_2, \ldots, s_l\}$ of representatives for the $(R, Q)$-double cosets in $P$ with $s_1 = 1$. Then for each $s_i$, $R^{s_i} \cap Q$ is either trivial or cyclic, and so for each $i \geq 2$, there exists $t_i \neq 1$ with $\phi(R^{s_i} \cap Q) \leqslant C_{\phi(Q)}(t_i)$. Then by Lemma 4.13, $(f_{R,S,t,t_2,\ldots,t_l})^P$ is a minimal length suborbit which is not of the form $(f_{R',s})^P$ for any $(R', s) \in \mathcal{R}$.

Our next two examples give infinite families of twisted wreath product groups $(G_n)_{n\geq 0}$ where $\mathrm{MinSubDeg}(G_n)/\mathrm{MinSubDeg}(H_n) \to 1$ as $n \to \infty$ with exceptional behaviour for the example in Example 4.15 involving $A_6$ and for the example in Example 4.16 involving $A_7$.

**Example 4.15.** Let $P = A_n$ for some $n \geq 6$, let $Q = T = A_{n-1}$, and let $\phi(q)$ be the conjugation by $q$ for all $q \in Q$. Then the primitive component is $H \cong A_{n-1} \rtimes A_{n-1}$. Let $t = (1, 2, 3)$ and let $R = C_P(t) \cong A_3 \times A_{n-3}$. Then by Lemma 4.2, $|(f_{R,t})^P| \leq 2\binom{n}{3}$. In fact, equality holds here, as there is no larger subgroup of $P$ whose intersection with $Q$ centralises $t$. By [6, Theorem 5.2A], when $n > 6$, there is no $S \leqslant P$, with $|S| > |R|$ such that $S \cap Q$ centralises some nontrivial element of $T$. Moreover, when $n > 6$ $\mathrm{MinSubDeg}(H) = 2\binom{n-1}{3}$ and so in this case

$$\mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = |f_{R,t}^P| = \frac{n}{n-3}\,\mathrm{MinSubDeg}(H).$$

If $n = 6$ then $|(f_{R,t})^P| = 40$ and $\mathrm{MinSubDeg}(H) = 12$. However, computations in *GAP* [7] show that there are suborbits of lengths 36, 24, and 15 in $A_5 \,\mathrm{twr}_\phi\, A_6$. A suborbit of length 15 is the suborbit containing $f_{R,t}$, where $R = \langle (1,3,2,4)(5,6), (1,3,5)(2,4,6)\rangle \cong (S_2 \wr S_3) \cap A_6$ and $t = (1,3)(2,4)$.

**Example 4.16.** Let $P = A_n$ for some $n \geq 7$, $T = A_{n-2}$, $Q = (S_{n-2} \times S_2) \cap A_n \cong S_{n-2}$, and let $\phi(q)$ be the conjugation by $q$ for all $q \in Q$. Then the primitive component is $H \cong A_{n-2} \rtimes S_{n-2}$. Let $t = (1,2,3)$ and let $R = C_P(t) \cong A_3 \times A_{n-3}$. By Lemma 4.2, $|(f_{R,t})^P| \leq 2\binom{n}{3}$. In fact, equality holds here as there is no larger subgroup of $P$ whose intersection with $Q$ centralises $t$. If $n \geq 8$ then $2\binom{n}{3}$ is the minimal non-trivial suborbit length in $A_{n-2} \,\mathrm{twr}_\phi\, A_n$ because by [6, Theorem 5.2A], there is no larger subgroup $S \leqslant P$, with $|S| > |R|$ such that $S \cap Q$ centralises some nontrivial element of $T$. Hence in this case we have $\mathrm{MinSubDeg}(H) = 2\binom{n-2}{3}$ and $\mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = |(f_{R,t})^P| = \frac{n(n-1)}{(n-3)(n-4)}\,\mathrm{MinSubDeg}(H)$. When $n = 7$ we have $\mathrm{MinSubDeg}(H) = 15$. Moreover, for the subgroup $S = \langle (1,2)(4,5), (1,3,5)(4,6,7)\rangle \cong \mathrm{PSL}(3,2)$ and element $s = (1,5)(2,4)$, we have $\phi(S \cap Q) = C_{\phi(Q)}(s)$ and so $|(f_{S,s})^P| = |P : S| = 15 = \mathrm{MinSubDeg}(T \,\mathrm{twr}_\phi\, P) = \mathrm{MinSubDeg}(H)$.

PROOF OF THEOREM 1.5. Part (a) follows follows immediately from Lemmas 4.2, 4.4 and 4.10, and from Example 4.7. Part (b) follows from Lemma 4.3 and Example 4.14. □

## References

[1] László Babai, Eugene M. Luks and Ákos Seress, Computing composition series in primitive groups, in: Groups and Computation, DIMACS Series on Discrete Math. and Theor. Computer Science **11**, AMS 1993, pp. 1–16.

[2] R. W. Baddeley, Primitive permutation groups with a regular non-abelian normal subgroup, *Proc. London Math. Soc. (3)* **67** (1993) 547–595.

[3] Robert Beals and Ákos Seress, Computing composition factors of small base groups in almost linear time, in: Proc. 24th Symp. on Theor. Comp. Science 1992, pp. 116–125.

[4] Anton Betten, Anne Delandtsheer, Alice C. Niemeyer and Cheryl E. Praeger, On a theorem of Wielandt for finite primitive permutation groups, *J. Group Theory* **6** (2003), 415–420.

[5] Peter J. Cameron, *Permutation groups*, London Math. Soc. Student Texts **45**, Cambridge Univ. Press, 1999.

[6] J. D. Dixon and B. Mortimer, *Permutation groups*, Springer-Verlag, New York, 1996.

[7] The GAP Group. GAP–Groups, Algorithms, and Programming, Version 4.3 (2002). (`http://www.gap-system.org`).

[8] Michael Giudici, Cai Heng Li, Cheryl E. Praeger, Ákos Seress and Vladimir Trofimov, On limit graphs of finite vertex-primitive graphs, preprint, 2004.

[9] L. G. Kovács, Primitive subgroups of wreath products in product action, *Proc. London Math. Soc. (3)* **68** (2) (1989), 306–322.

[10] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), 365–383.

[11] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, On the O'Nan–Scott Theorem for finite primitive permutation groups, *J. Austral. Math. Soc. (A)* **44** (1988), 389–396.

[12] Cheryl E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. London Math. Soc.* (3) **60** (1990), 68–88.

[13] Cheryl E. Praeger, Jan Saxl and Kasuhiro Yokoyama, Distance transitive graphs and finite simple groups, *Proc. London Math. Soc.* (3) **55** (1987), 1–21.

[14] Ákos Seress, *Permutation Group Algorithms*, Cambridge Univ. Press, 2003.

[15] Michio Suzuki, *Group theory. I*, Springer-Verlag, Berlin, 1982.

Michael Giudici, School of Mathematics,The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia

Email: giudici@maths.uwa.edu.au

Cai Heng Li, School of Mathematics,The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia

Email: li@maths.uwa.edu.au

Cheryl E. Praeger, School of Mathematics,The University of Western Australia, 35 Stirling Highway, Crawley WA 6009, Australia

Email: praeger@maths.uwa.edu.au

Ákos Seress, The Ohio State University, Department of Mathematics, Columbus, OH 43210, USA

Email: akos@math.ohio-state.edu

Vladimir Trofimov, Institute of Mathematics and Mechanics, Russian Academy of Sciences, S. Kovalevskoy, 16, 620219, Ekaterinburg, Russia

Email: trofimov@imm.uran.ru