Proceedings of the Edinburgh Mathematical Society (2019) **62**, 1137–1162
doi:10.1017/S0013091519000130

COPRIME SUBDEGREES OF TWISTED WREATH PERMUTATION GROUPS

ALEXANDER Y. CHUA, MICHAEL GIUDICI AND LUKE MORGAN*

Department of Mathematics and Statistics, Centre for the Mathematics of Symmetry and Computation, The University of Western Australia, 35 Stirling Highway, Crawley, WA 6009, Australia (21506815@student.uwa.edu.au; michael.giudici@uwa.edu.au; luke.morgan@famnit.upr.si)

(Received 31 October 2018; first published online 28 June 2019)

Abstract Dolfi, Guralnick, Praeger and Spiga asked whether there exist infinitely many primitive groups of twisted wreath type with non-trivial coprime subdegrees. Here, we settle this question in the affirmative. We construct infinite families of primitive twisted wreath permutation groups with non-trivial coprime subdegrees. In particular, we define a primitive twisted wreath group $G(m, q)$ constructed from the non-abelian simple group $\mathrm{PSL}(2, q)$ and a primitive permutation group of diagonal type with socle $\mathrm{PSL}(2, q)^m$, and determine many subdegrees for this group. A consequence is that we determine all values of m and q for which $G(m, q)$ has non-trivial coprime subdegrees. In the case where $m = 2$ and $q \notin \{7, 11, 29\}$, we obtain a full classification of all pairs of non-trivial coprime subdegrees.

Keywords: primitive group; twisted wreath group; subdegrees

2010 *Mathematics subject classification:* Primary 20B15; 20H30; 20B05

1. Introduction

If G is a transitive permutation group acting on a finite set Ω and we fix some point $\alpha \in \Omega$, a *subdegree* of G relative to α is defined as the size of a G_α-orbit. These are the sizes of the sets β^{G_α} where $\beta \in \Omega$ or, equivalently, the values of $|G_\alpha : G_\alpha \cap G_\beta|$. The subdegree is said to be *trivial* if it corresponds to the G_α-orbit $\{\alpha\}$, and *non-trivial* otherwise. If G is primitive and not cyclic, and of prime order, then the only subdegree equal to 1 is the trivial subdegree, so all non-trivial subdegrees are greater than 1. The study of subdegrees is a classical topic in permutation group theory. Probably the most famous result is the verification of the Sims conjecture [3] that bounds the order of point stabilizers in primitive groups in terms of the subdegrees.

Primitive groups are classified into eight types by the O'Nan–Scott theorem (following the subdivision in [15]). The primitive groups of twisted wreath type (TW) are the most mysterious and commonly misunderstood. We refer the reader to [1] and [5, § 4.7] for detailed treatments and provide more information in § 2. This paper deals with subdegrees

[*] Corresponding author.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

of twisted wreath groups, a topic that does not appear very often in the literature. The published results include a paper by Giudici, Li, Praeger, Seress and Trofimov [10], which proves bounds on the minimal subdegrees and explicitly constructs such a G_α-orbit of minimal size witnessing the smallest subdegree. A result by Fawcett in her PhD thesis [8, p. 59] shows that if the point stabilizer G_α acts primitively on the set of simple direct factors of the socle of G, then there is a subdegree of size $|G_\alpha|$.

The study of coprime subdegrees dates back to the work of Marie Weiss in 1935, who proved that if G is primitive with coprime subdegrees m and n, then G has a subdegree dividing mn that is greater than or equal to both m and n. Moreover, if G has k pairwise coprime subdegrees then G has rank at least 2^k (see [14, pp. 92–93]). The motivation behind the present paper was a result of Dolfi, Guralnick, Praeger and Spiga [6] that is proven in [7], stating that the maximal size of a set of pairwise coprime non-trivial subdegrees of a finite primitive permutation group is at most 2. Dolfi *et al.* also showed that if a primitive permutation group has a pair of non-trivial coprime subdegrees, then its type is almost simple (AS), product action (PA) or TW. For types AS and PA, they constructed infinite families with non-trivial coprime subdegrees, but only one example for type TW is known.

The initial motivation for the work in this paper was to find infinite families of TW groups with non-trivial coprime subdegrees. To do this, we construct new subdegrees for TW groups, focusing on TW groups which arise from primitive groups of *diagonal type*. In § 2 we provide examples for the structure of two-point stabilizers in twisted wreath groups; this enables us to find sufficient conditions for specified subdegrees of a TW group to exist. The culmination of our work in this section is Theorem 2.12, which gives a sufficient condition to find an infinite family of TW groups having non-trivial coprime subdegrees. Interestingly, the easiest way for the conditions to be satisfied would be to have a factorization of a non-abelian finite simple group as a product of centralizers—which cannot occur because of the validity of the Szep conjecture (see Remark 2.14).

In § 3 we therefore focus on a more specific family of TW groups, which we denote $G(m, q)$. The group $G(m, q)$ is constructed from the non-abelian simple group $\mathrm{PSL}(2, q)$ and a primitive permutation group of diagonal type with socle $\mathrm{PSL}(2, q)^m$. The group $G(2, 7)$ is the example given in [6] of a primitive TW group with non-trivial coprime subdegrees. For the full definition of $G(m, q)$, see § 4. The main reason to focus on $G(m, q)$ is that we have a comprehensive understanding of the subgroup structure of $\mathrm{PSL}(2, q)$ (going back to work of Dickson [4] and Moore [12]), and this allows us to apply results from § 2 to obtain many subdegrees of $G(m, q)$, listed in Table 1. This yields the following theorem, which answers the question of Dolfi *et al.* in the positive.

Theorem 1.1. *Table 2 exhibits infinitely many integers m and prime powers q for which the group $G(m, q)$ has a pair of non-trivial coprime subdegrees.*

As mentioned above, we expect the existence of non-trivial coprime subdegrees to be rare. We therefore go further with our analysis to discover precisely when the group $G(m, q)$ may have non-trivial coprime subdegrees. We obtain the following result.

Theorem 1.2. *The group $G(m, q)$ has non-trivial coprime subdegrees if and only if one of the following holds:*

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Table 1. *Some subdegrees of $G(m,q)$.*

Row	m	q	d
1	$m \geqslant 3$	all	$(q+1)^m$
	$m = 2$	$q \equiv 1 \pmod 4$	$(q+1)^2$
2		$q \equiv 1 \pmod 4$	$\left(\frac{1}{2}q(q+1)\right)^m$
		$q \equiv 3 \pmod 4$	$\left(\frac{1}{2}q(q-1)\right)^m$
3		even	$\left(\frac{1}{2}q(q-1)\right)^m$
4		odd	$(q(q-1))^m$
		odd and $q \geqslant 7$	$(q(q+1))^m$
		even	$(q(q-1))^m$ and $(q(q+1))^m$
5		all	$\left(\frac{1}{(2,q-1)}(q^2-1)\right)^m$
6		$q \equiv \pm 1 \pmod 8$ and q is prime	$\left(\frac{\lvert T\rvert}{24}\right)^m$
7		$q \equiv \pm 1 \pmod{10}$ and q is prime, or $q = p^2$ where $p > 3$ is prime and $p \equiv \pm 3 \pmod{10}$	$\left(\frac{\lvert T\rvert}{60}\right)^m$
8	$m \geqslant 6$	$q = 9$	6^m

Table 2. *Nontrivial coprime subdegrees of $G(m,q)$.*

m	q	d_1	d_2
$m = 2$	$q \equiv 3 \pmod 4$	$\left(\frac{1}{2}q(q-1)\right)^2$	divides $2(q+1)^2$
$m \geqslant 3$	$q \equiv 3 \pmod 4$	$\left(\frac{1}{2}q(q-1)\right)^m$	$(q+1)^m$
$m \geqslant 3$	even	$\left(\frac{1}{2}q(q-1)\right)^m$ or $(q(q-1))^m$	$(q+1)^m$
	$q = 29$	30^m	203^m
	$q = 7$	7^m	24^m
	$q = 11$	11^m	60^m

(1) $q \equiv 3 \pmod 4$ *or* $q = 29$*;*

(2) q *is even and* $m \geqslant 3$*.*

Finally, in § 7 we analyse the $m = 2$ case in more detail to determine all pairs of non-trivial coprime subdegrees.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Table 3. *Classification of non-trivial coprime subdegrees of* $G(2,q)$.

q	H_f	H_g	$\lvert H:H_f\rvert$	$\lvert H:H_g\rvert$
$\equiv 3 \pmod 4$	$P_1\times P_1$	$D_{q+1}\wr S_2$	$2(q+1)^2$	$\left(\frac{1}{2}q(q-1)\right)^2$
7	$C_7\times C_7\leqslant H_f$	$S_4\wr S_2$	divides $2(24^2)$	7^2
11	$C_{11}\times C_{11}\leqslant H_f$	$A_5\wr S_2$	divides $2(60^2)$	11^2
11	$P_1\times P_1$	$A_4\wr S_2$	$2(12^2)$	55^2
19	$P_1\times P_1$	$A_5\wr S_2$	$2(20^2)$	57^2
23	$P_1\times P_1$	$S_4\wr S_2$	$2(24^2)$	253^2
29	$X\times X\leqslant H_f$ where $\lvert P_1:X\rvert=2$	$A_5\wr S_2$	divides $2(60^2)$	203^2
59	$P_1\times P_1$	$A_5\wr S_2$	$2(60^2)$	1711^2

Theorem 1.3. *For $q\notin\{7,11,29\}$ the pair (a,b) is a non-trivial pair of coprime subdegrees of $G(2,q)$ if and only if $(a,b)=(\lvert H:H_g\rvert,\lvert H:H_f\rvert)$ for some pair H_g, H_f appearing in Table 3.*

Remarkably, we find that if $q\equiv 3 \pmod 4$ and $q>19$, then (up to multiplicity) $G(2,q)$ has exactly one pair of non-trivial coprime subdegrees. We make no attempt to investigate the multiplicities of the non-trivial coprime subdegrees, but this in itself is an interesting problem.

2. Twisted wreath groups

We now describe the construction of the twisted wreath product as introduced by Neumann in [**13**]. Let T and H be arbitrary non-trivial groups. For any subset X of H, let T^X denote the set of functions from X to T, which is a group under pointwise multiplication. Let id denote the function defined by $\mathrm{id}(x)=1$ for all $x\in X$. It can be shown that H acts as a group of automorphisms on T^H by $f^x(z)=f(xz)$ for all $f\in T^H$ and $x,z\in H$. Now let L be a subgroup of H, and let R be a set of left coset representatives of L in H. Let $\phi:L\to\mathrm{Aut}(T)$ be a homomorphism. Set

$$N=\{f\in T^H \mid f(z\ell)=f(z)^{\phi(\ell)}\quad \text{for all } z\in H \text{ and } \ell\in L\}.$$

We can show that N is a subgroup of T^H and that $N\cong T^R$. Furthermore, the group N is invariant under the action of H, so H acts as a group of automorphisms on N.

Definition 2.1. We define the twisted wreath product determined from (T,H,ϕ) to be the group $G=N\rtimes H$. The group G acts on $\Omega=N$ with N acting by right multiplication and H acting by automorphisms, that is, $\alpha^{nh}=(\alpha n)^h$ for all $\alpha\in\Omega, n\in N$ and $h\in H$.

Lemma 2.2. *The non-trivial subdegrees of G are the values of $\lvert H:H_f\rvert$ for $f\in N\setminus\{id\}$. Also, if G is primitive, then no non-trivial subdegree of G is equal to 1.*

Proof. We can verify that $G_{\mathrm{id}}=H$, so the non-trivial subdegrees of G are of the form $\lvert G_{\mathrm{id}}:G_{\mathrm{id}}\cap G_f\rvert=\lvert H:H_f\rvert$ for some $f\in N\setminus\{\mathrm{id}\}$. Now suppose that G is primitive. If

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

some non-trivial subdegree of G is equal to 1, then G must have prime order and so either T or H must be trivial, a contradiction. □

The following result from [5, Lemma 4.7A] gives a set of sufficient conditions for a twisted wreath product to be primitive.

Theorem 2.3. *Let T be a non-abelian finite simple group, and suppose that H is a primitive permutation group with point stabilizer L. Suppose that the group of inner automorphisms of T is contained in the image of ϕ, but Im ϕ is not a homomorphic image of H. Then the twisted wreath product determined from (T, H, ϕ) is a primitive group with regular socle N, and $N \cong T^m$ where $m = |H : L|$.*

We will deal with a class of primitive TW groups constructed from a group of diagonal type.

Lemma 2.4. *Let T be a finite non-abelian simple group, let $H = T \wr S_m$ and let $L = \{(x, \dots, x)\sigma \mid x \in T, \sigma \in S_m\}$. Define $\phi : L \to Aut(T)$ by setting $\phi((x, \dots, x)\sigma) = i_x$ for all $x \in T$ and $\sigma \in S_m$, where i_x denotes the automorphism of T induced by conjugation by x. Then the construction in Definition 2.1 yields a primitive TW permutation group $G(m, T)$ with socle isomorphic to $T^{|T|^{m-1}}$ and point stabilizer isomorphic to $T \wr S_m$.*

Proof. The group H acts primitively on the set of right cosets of L. Note that $\mathrm{Inn}(T) = \mathrm{Im}\ \phi$ and that $\mathrm{Inn}(T)$ is not a homomorphic image of H. All the conditions of Theorem 2.3 have been satisfied, so $G(m, T)$ is indeed a primitive group of type TW. Since

$$|H : L| = \frac{|T|^m \cdot m!}{|T| \cdot m!} = |T|^{m-1},$$

the socle is of the form $T^{|T|^{m-1}}$. □

We note that $G(2, \mathrm{PSL}(2, 7))$ is the primitive TW group in [6, pp. 12–14] with non-trivial coprime subdegrees.

Throughout, we will let H, L and ϕ be as defined in Lemma 2.4. Let

$$N = \{f \in T^H \mid f(z\ell) = f(z)^{\phi(\ell)} \text{ for all } z \in H \text{ and } \ell \in L\}$$

be the set of functions that $G(m, T)$ acts on.

We now construct some $g \in N$ which is very similar to the function used by Dolfi *et al.* [6] and Giudici *et al.* [10].

Lemma 2.5. *Let D be a subgroup of H. Suppose there exists $t \in H$ such that $(\eta, \dots, \eta)\sigma \in Z(D^t \cap L)$ with $\eta \neq 1$. Then $g \in T^H$ defined by*

$$g(z) = \begin{cases} \eta^{\phi(\ell)} & \text{if } z = dt\ell, \text{ for some } d \in D \text{ and } \ell \in L, \\ 1 & \text{if } z \in H \setminus DtL \end{cases} \tag{2.1}$$

is well defined. Moreover, g is a non-constant function, $g \in N$ and $D \leqslant \mathbf{C}_H(g)$.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Proof. First, we show that g is well defined. If $z = d_1 t\ell_1 = d_2 t\ell_2$ for $d_1, d_2 \in D$ and $\ell_1, \ell_2 \in L$, then $\ell_2\ell_1^{-1} = t^{-1}d_2^{-1}d_1 t \in D^t \cap L$. Hence $\ell_2 = u\ell_1$ with $u \in D^t \cap L$. Let $u = (\rho, \dots, \rho)\tau$. Since $(\eta, \dots, \eta)\sigma \in Z(D^t \cap L)$, it follows that $(\rho\eta, \dots, \rho\eta)\tau\sigma = (\eta\rho, \dots, \eta\rho)\sigma\tau$. In particular, $\rho\eta = \eta\rho$ and thus $\eta^{\phi(u)} = \eta^{i_\rho} = \eta$. Hence

$$\eta^{\phi(\ell_1)} = \eta^{\phi(u)\phi(\ell_1)} = \eta^{\phi(u\ell_1)} = \eta^{\phi(\ell_2)}$$

and so $g(z)$ does not depend on the representation $z = d_i t\ell_i$ of z.

Next, we show that $g \in N$. If $z = dt\ell$ for $d \in D$ and $\ell \in L$, then

$$g(z\ell_1) = g(dt\ell\ell_1) = \eta^{\phi(\ell\ell_1)} = \eta^{\phi(\ell)\phi(\ell_1)} = g(z)^{\phi(\ell_1)}$$

for each $\ell_1 \in L$. If $z \notin DtL$, then $z\ell \notin DtL$, so $g(z\ell) = 1 = g(z)^{\phi(\ell)}$. Hence $g \in N$. Now suppose for a contradiction that g is constant. Then $\eta^{\phi(\ell)} = \eta^{\phi(1)} = \eta$ for all $\ell \in L$, and since $\mathrm{Inn}(T) \leqslant \mathrm{Im}\ \phi$ we have $\eta \in Z(T) = 1$, a contradiction. Thus, g is non-constant.

Finally, we show that for each $d \in D$ and $z \in H$, we have $g^d(z) = g(dz) = g(z)$, by considering the $z \in DtL$ and $z \notin DtL$ cases. If $z = d_1 t\ell_1$ for $d_1 \in D$ and $\ell_1 \in L$, then $g(dz) = g(dd_1 t\ell_1) = \eta^{\phi(\ell_1)} = g(d_1 t\ell_1) = g(z)$. If $z \notin DtL$, then it also follows that $dz \notin DtL$, so $g(dz) = g(z) = 1$. Thus D centralizes g. □

Lemma 2.6. *Let D be a maximal subgroup of H. If there exists $t \in H$ such that $Z(D^t \cap L)$ contains an element $(\eta, \dots, \eta)\sigma$ with $\eta \neq 1$, then $|H : D|$ is a subdegree of $G(m, T)$.*

Proof. Define g as in Equation (2.1). Then by Lemma 2.5, $D \leqslant \mathbf{C}_H(g)$. Since D is maximal in H, we conclude that $\mathbf{C}_H(g) = D$ or H. If $\mathbf{C}_H(g) = H$, then for each $h \in H$, we have that $g(hz) = g^h(z) = g(z)$, and thus g is a constant function, contradicting $\eta \neq 1$ and Lemma 2.5. So $\mathbf{C}_H(g) = D$. Hence $|H : \mathbf{C}_H(g)| = |H : D|$ is a subdegree of $G(m, T)$. □

Corollary 2.7. *Let K be a maximal subgroup of T and let $D = K \wr S_m$. If there exists $t \in H$ such that $Z(D^t \cap L)$ contains an element $(\eta, \dots, \eta)\sigma$ with $\eta \neq 1$, then $|T : K|^m$ is a subdegree of $G(m, T)$.*

Proof. By Corollary 1.5A and Lemma 2.7A in [5], it follows that D is maximal in H. The result now follows from applying Lemma 2.6. □

Corollary 2.8. *Let K be maximal in T with $Z(K) \neq 1$. Then $|T : K|^m$ is a subdegree of $G(m, T)$.*

Proof. Let $D = K \wr S_m$. Then $D \cap L \cong K \times S_m$, so $Z(D \cap L) \cong Z(K) \times Z(S_m)$. Since $Z(K) \neq 1$, we can apply Corollary 2.7 with $t = 1$, and thus $|T : K|^m$ is a subdegree of $G(m, T)$. □

Corollary 2.9. *Suppose $m \geqslant 3$. Let K be a maximal subgroup of T such that there exists $s \in T \setminus K$ with $Z(K \cap K^s) \neq 1$. Then $|T : K|^m$ is a subdegree of $G(m, T)$.*

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Proof. Let $D = K \wr S_m$ and set $t = (1, \ldots, 1, s)$. Then

$$\begin{aligned} D^t \cap L &= \{(1, \ldots, 1, s^{-1})(k_1, \ldots, k_m)\sigma(1, \ldots, 1, s) \mid k_i \in K, \sigma \in S_m\} \cap L \\ &= \{(1, \ldots, 1, s^{-1})(k_1, \ldots, k_m) \underbrace{(1, \ldots, s, \ldots, 1)}_{s \text{ in the } m^{\sigma^{-1}} \text{th component}} \sigma \mid k_i \in K, \sigma \in S_m\} \cap L. \end{aligned}$$

If $m^{\sigma^{-1}} \neq m$ then, since $m \geqslant 3$, one component of the product will be of the form $k_i s$, while another will be of the form k_j. But $k_i s \neq k_j$ since $s \notin K$, so the product is not in L. So

$$\begin{aligned} D^t \cap L &= \{(1, \ldots, 1, s^{-1})(k_1, \ldots, k_m)(1, \ldots, 1, s)\sigma \mid k_i \in K, m^\sigma = m\} \cap L \\ &= \{(k_1, \ldots, k_{m-1}, k_m^s)\sigma \mid k_i \in K, m^\sigma = m\} \cap L \\ &\cong (K \cap K^s) \times S_{m-1}. \end{aligned}$$

Hence

$$Z(D^t \cap L) \cong Z(K \cap K^s) \times Z(S_{m-1})$$

and since $Z(K \cap K^s) \neq 1$, we can apply Corollary 2.7 to conclude that $|T : K|^m$ is a subdegree of $G(m, T)$. □

Corollary 2.10. *Let K be maximal in T and assume that there exists $s \in T \setminus K$ such that $K \cap K^s \cong C_2$. Then $|T : K|^m$ is a subdegree of $G(m, T)$.*

Proof. If $m \geqslant 3$, we are immediately done by Corollary 2.9 as $K \cap K^s$ is abelian. So suppose $m = 2$ and let $D = K \wr S_2$. Let $M = \{(x, x) \mid x \in T\}$ and set $t = (1, s)$. Then $D^t \cap M \cong K \cap K^s \cong C_2$. Since $M \lhd L$ it follows that $D^t \cap M \lhd D^t \cap L$, and so $D^t \cap M \leqslant Z(D^t \cap L)$. So, by Corollary 2.7, we see that $|T : K|^2$ is a subdegree of $G(m, T)$. □

The following lemma is inspired by the construction in [6] of the subdegree 24^2 in the group $G(2, \mathrm{PSL}(2, 7))$.

Lemma 2.11. *Let γ be a non-trivial element of T. Then*

$$\left(\frac{|T|}{|\mathbf{C}_T(\gamma)|}\right)^m = |\gamma^T|^m$$

is a subdegree of $G(m, T)$.

Proof. Let $D = \mathbf{C}_T(\gamma) \wr S_m$. Define $h \in T^H$ by

$$h(z) = \begin{cases} \gamma^{\phi(\ell)} & \text{if } z = d\ell, \text{ for some } d \in D \text{ and } \ell \in L, \\ 1 & \text{if } z \in H \setminus DL. \end{cases} \tag{2.2}$$

That is, h is defined as in Equation (2.1) with $t = 1$ and $(\gamma, \ldots, \gamma)$ being a non-trivial element in $Z(D \cap L)$. Thus Lemma 2.5 implies that h is well defined, $h \in N$ and $D \leqslant \mathbf{C}_H(h)$. We cannot use maximality as before to conclude that $D = \mathbf{C}_H(h)$, but we can prove this another way. Let $h_1 \in \mathbf{C}_H(h)$ and suppose that $h_1 \notin DL$. Then $\gamma = h(1) =$

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

$h^{h_1}(1) = h(h_1) = 1$, a contradiction. Thus, $h_1 = d\ell$ for some $d \in D$ and $\ell \in L$. Since $D \leqslant \mathbf{C}_H(h)$, we have $\ell = d^{-1}h_1 \in \mathbf{C}_H(h)$. Let $\phi(\ell) = i_x$, that is, $\ell = (x, \ldots, x)\sigma$ for some $x \in T$ and $\sigma \in S_m$. Then $\gamma = h(1) = h^\ell(1) = h(\ell) = \gamma^{i_x}$, so $x \in \mathbf{C}_T(\gamma)$. Hence $\ell \in D$ and $h_1 \in D$, so $D = \mathbf{C}_H(h)$. Thus

$$|H : \mathbf{C}_H(h)| = |H : D| = \left(\frac{|T|}{|\mathbf{C}_T(\gamma)|}\right)^m = |\gamma^T|^m$$

is a subdegree of $G(m, T)$. □

We now explain how the above results could be used to construct infinite families of primitive TW groups with non-trivial coprime subdegrees. If G is a finite group with subgroups A and B, we say $G = AB$ is a *coprime factorization* if $|G : A|$ and $|G : B|$ are coprime. If A and B are maximal in G, we say $G = AB$ is a *maximal coprime factorization.*

Theorem 2.12. *Let $T = AB$ be a maximal coprime factorization of the finite non-abelian simple group T, and suppose $m \geqslant 3$. If there exist $s, t \in T$ such that $Z(A \cap A^s) \neq 1$ and $Z(B \cap B^t) \neq 1$, then the group $G(m, T)$ has non-trivial coprime subdegrees $|T : A|^m$ and $|T : B|^m$.*

Proof. This follows from Corollary 2.8 when s or t lie in K, and from Corollary 2.9 when s or t lie in $T \setminus K$. □

The simple group $T = \mathrm{PSL}(2, 7)$ admits a maximal coprime factorization as $T = AB$ with $A \cong D_8$ and $B \cong F_{21}$. Since B is maximal in T and $N_T(P) \cong S_3$ for P a Sylow 3-subgroup of B, for any involution $t \in N_T(P)$ we have $B \cap B^t = P$. Thus, for $m \geqslant 3$, we can apply the above theorem with $s = 1$ and this choice of t to produce the pair of non-trivial coprime subdegrees $(21^m, 8^m)$ of $G(m, \mathrm{PSL}(2, 7))$. This gives us our first infinite family of coprime subdegrees.

Remark 2.13. Theorem 2.12 is a very powerful result as [6] contains a list of all the maximal coprime factorizations of finite non-abelian simple groups.

Remark 2.14. Let T be a finite non-abelian simple group. If $T = AB$ is a maximal coprime factorization such that both A and B have non-trivial centres, then we have an infinite family of primitive TW groups with non-trivial coprime subdegrees (this is a special case of Theorem 2.12 with $s = t = 1$). It is a conjecture of Szep that T can never be written as AB for any (not necessarily maximal) subgroups A and B of T with non-trivial centre. This conjecture was proven in [9], meaning that, in fact, this idea cannot be used to construct an infinite family.

Remark 2.15. By Lemma 2.11, if there exist two non-trivial conjugacy classes of coprime size, then we have an infinite family of primitive TW groups with non-trivial coprime subdegrees. However, as observed in [9], this is not possible and is an immediate corollary of the Szep conjecture.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

3. Results about $\mathbf{PSL(2,q)}$

We begin with the following standard lemma.

Lemma 3.1. *Let K be a maximal subgroup of a simple group T and let R be a subgroup of K. Let x be the number of conjugates of R in T that are contained in K, and let y be the number of conjugates of K in T whose intersection with K contains R. Then*

$$y = \frac{x \cdot |N_T(R)|}{|K|}.$$

Proof. We will count the number of pairs (X, Y) of subgroups of T, with X conjugate to R, Y conjugate to K, and $X \leqslant Y$. By fixing X and considering the possibilities for Y, and then by fixing Y and considering the possibilities for X, we obtain

$$\begin{aligned}&(\#\text{conjugates of } R \text{ in } T)(\#\text{conjugates of } K \text{ in } T \text{ containing } R)\\ &\quad = (\#\text{conjugates of } R \text{ in } T \text{ that are contained in } K)(\#\text{conjugates of } K \text{ in } T).\end{aligned}$$

Hence

$$\frac{|T|}{|N_T(R)|} \cdot y = x \cdot \frac{|T|}{|N_T(K)|}.$$

Now $K \leqslant N_T(K) \leqslant T$, so by the maximality of K it follows that $N_T(K) = K$ or T. However, the simplicity of T implies that K is not normal in T, so $N_T(K) = K$. Thus

$$y = \frac{x \cdot |N_T(R)|}{|K|}. \qquad \square$$

Corollary 3.2. *We use the same notation as in Lemma 3.1. Also, suppose that there is only one conjugacy class of subgroups isomorphic to R in K. Then*

$$y = \frac{|N_T(R)|}{|N_K(R)|}.$$

Proof. Since there is only one conjugacy class of subgroups isomorphic to R in K, we have that $x = (|K|)/(|N_K(R)|)$ and the result follows. □

We will be working a lot with the projective special linear groups. Information about their subgroups and maximal subgroups will prove to be useful. The list in Dickson [4] is the most commonly cited but contains an error about the number of conjugacy classes of dihedral groups. In particular, it states that for a divisor $d > 2$ of $(q \pm 1)/(2, q-1)$, there is one conjugacy class of subgroups isomorphic to D_{2d} for d odd, and two conjugacy classes if d is even. However, it is actually the case that there are two conjugacy classes for d odd, and one conjugacy class for d even. We point the reader to [12], which states

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

the correct number of conjugacy classes in each case. For the rest of this section we set

$$\begin{aligned} V &= \mathrm{GF}(q)^2 \\ T &= \mathrm{PSL}(2,q) \\ P_1 &= T_{\langle v \rangle}, \quad 0 \neq v \in V. \end{aligned}$$

Thus P_1 is a point stabilizer in the degree $q+1$ action of T on the set $\mathcal{P}_1(V)$ of one-dimensional subspaces of V. We begin with a lemma concerning involutions in cosets of P_1.

Lemma 3.3. *For all $s \in T$ such that $s \notin P_1$, the coset $P_1 s$ contains an involution.*

Proof. With $\langle v \rangle$ the one-dimensional subspace of V stabilized by P_1, let $\langle w \rangle = \langle v \rangle^s$. Since $s \notin P_1$, it follows that $\{v, w\}$ is a basis of V. Take the element $g \in \mathrm{SL}(2,q)$ such that $v^g = w$ and $w^g = -v$. Any element of V can be written as $\alpha v + \beta w$ for some $\alpha, \beta \in \mathrm{GF}(q)$, and we can show that $(\alpha v + \beta w)^{g^2} = -\alpha v - \beta w$, so $g^2 = -I_2$. Thus, the permutation h induced by g on $\mathcal{P}_1(V)$ is an involution and $\langle v \rangle^h = \langle v^g \rangle = \langle w \rangle = \langle v \rangle^s$. Thus, $h \in P_1 s$ and so the coset $P_1 s$ contains an involution. □

The next few lemmas deal with possible intersections of conjugate subgroups of T. We now introduce some notation. Let K be a subgroup of T. For any $R \leqslant K$, let $f(R)$ denote the number of conjugates of K whose intersection with K contains R, and let $g(R)$ denote the number of conjugates of K whose intersection with K is equal to R. Note that for R maximal in K, we have $f(R) = g(R) + 1$.

Lemma 3.4. *Suppose that $q \equiv \pm 1 \pmod{10}$, and q is a prime or $q = p^2$ for some prime $p \equiv \pm 3 \pmod{10}$. Let $K \cong A_5$ be a subgroup of T. If $q > 11$ then there exists $t \in T$ such that $K \cap K^t \cong C_2$.*

Proof. Let $R \cong C_2$ be a subgroup of K. It is easy to calculate that, inside K, R is contained in two subgroups isomorphic to D_{10}, two subgroups isomorphic to D_6 and one subgroup isomorphic to C_2^2. We want to show that $g(R) = f(C_2) - 2g(D_{10}) - 2g(D_6) - f(C_2^2) = f(C_2) - 2f(D_{10}) - 2f(D_6) - f(C_2^2) + 4$ is positive, where the second equality follows from the fact that D_{10} and D_6 are maximal in A_5.

For $R = C_2, D_{10}, D_6$ and C_2^2 there is only one conjugacy class of subgroups isomorphic to R in K, so by Corollary 3.2, we have

$$f(R) = \frac{|N_T(R)|}{|N_K(R)|}.$$

It is easy to prove that $|N_K(C_2)| = 4$, $|N_K(D_{10})| = 10$, $|N_K(D_6)| = 6$ and $|N_K(C_2^2)| = 12$. Choose $\epsilon \in \{-1, 1\}$ such that $(q+\epsilon)/2$ is even. Then we have $N_T(C_2) = D_{q+\epsilon}$, so $|N_T(C_2)| \geqslant q-1$. By looking through the list of maximal subgroups of T, we see that $N_T(C_2^2) \leqslant C_2^2, A_4, S_4$ or $D_{q\pm 1}$. If $C_2^2 \cong D_4 \leqslant N_T(D_4) \leqslant D_{q\pm 1}$, then $N_T(D_4) = N_{D_{q\pm 1}}(D_4) = D_4$ or D_8. So $|N_T(C_2^2)| \leqslant 24$. For $n = 6$ or 10, we use the list of maximal subgroups of T given in [12] to see that $D_n \leqslant N_T(D_n) \leqslant D_{q\pm 1}, A_5$ or S_4. In the last two

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

cases, if D_n is a subgroup, it must be maximal, and hence $N_T(D_n) = D_n$. In the first case, we have $N_T(D_n) = N_{D_{q\pm1}}(D_n) = D_n$ or D_{2n}. So $|N_T(D_n)| \leqslant 2n$ for $n = 6$ and 10.

Putting all this together, we obtain $f(C_2) \geqslant (q-1)/4$, $f(C_2^2) \leqslant \frac{24}{12} = 2$, $f(D_6) \leqslant \frac{12}{6} = 2$ and $f(D_{10}) \leqslant \frac{20}{10} = 2$. It now follows that $g(C_2) \geqslant (q-1)/4 - 2\times 2 - 2\times 2 - 2 + 4 > 0$ for $q > 25$. Taking into account the restrictions on q, it remains to consider the $q = 19$ case in more detail. Here, $f(C_2) = (q+1)/4 = 5$. Also, there is no D_{12} in T, so $N_T(D_6) = D_6$ and $f(D_6) = 1$. Then $g(C_2) \geqslant 5 - 2\times 2 - 2\times 1 - 2 + 4 > 0$, as desired. □

Lemma 3.5. *Suppose that* $q \equiv \pm 1 \pmod 8$ *is prime. Let* $K \cong S_4$ *be a subgroup of* T. *Then there exists* $t \in T$ *such that* $K \cap K^t \cong C_2^2$. *Moreover, if* $q \geqslant 17$, *then there exists* $t \in T$ *such that* $K \cap K^t \cong C_2$.

Proof. Let X be a subgroup of K isomorphic to C_2^2 such that X is not normal in K. Note that there is a unique subgroup Y such that $X < Y < K$. Moreover, $Y \cong D_8$. Thus $g(X) = f(X) - f(D_8)$, which we want to show is positive.

There is only one conjugacy class of subgroups isomorphic to D_8 in K, so by Corollary 3.2 we have

$$f(D_8) = \frac{|N_T(D_8)|}{|N_K(D_8)|} = \frac{|N_T(D_8)|}{8}.$$

From the list of maximal subgroups of T we have $D_8 \leqslant N_T(D_8) \leqslant D_{q\pm1}$ or S_4. In the first case, we have $N_T(D_8) = N_{D_{q\pm1}}(D_8) = D_8$ or D_{16}. In the second case, we have $N_T(D_8) = D_8$, as D_8 is maximal and not normal in S_4. So $|N_T(D_8)| \leqslant 16$. This implies that $f(D_8) \leqslant \frac{16}{8} = 2$.

We claim that $N_T(X) \cong S_4$. There are two conjugacy classes of subgroups isomorphic to S_4 in T, so let J be a subgroup of T isomorphic to S_4 that is not conjugate to K. Let P and Q be the normal subgroups of J and K that are isomorphic to C_2^2, respectively. Now there are two conjugacy classes of subgroups isomorphic to C_2^2 in T. Since the normalizers of P and Q in T (J and K, respectively) are not conjugate, the subgroups P and Q cannot be conjugate. Hence X is conjugate to either P or Q. Thus, the normalizer of X is conjugate to the normalizer of either P or Q, both of which are isomorphic to S_4. This proves that $N_T(X) \cong S_4$.

The conjugacy class of X in K has size 3, so the number of conjugates of X in T contained in K is at least 3. Then Lemma 3.1 implies that

$$f(X) \geqslant \frac{3\cdot 24}{24} = 3.$$

Putting all this together yields $g(X) \geqslant 3 - 2 > 0$. This proves the first part of the lemma.

For the second part of the lemma, we verify the $q = 17$ case by a Magma [2] calculation. We now show that if $q > 17$ then there exists $t \in T$ such that $K \cap K^t = Z$, where Z is a subgroup of X isomorphic to C_2. Since the only subgroups of K that contain Z as a maximal subgroup are X and the subgroups isomorphic to S_3, we need to show that $g(Z) = f(Z) - f(X) - 2g(S_3)$ is positive. Since S_3 is maximal in K, we have $g(S_3) = f(S_3) - 1$, and thus $g(Z) = f(Z) - f(X) - 2f(S_3) + 2$.

There is only one conjugacy class of subgroups isomorphic to Z in T, so the number of conjugates of Z in T that are contained in K is equal to the number of subgroups

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

isomorphic to C_2 in K, which is equal to 9. Now choose $\epsilon \in \{-1, 1\}$ such that $(q+\epsilon)/2$ is even. Then $N_T(Z) \cong D_{q+\epsilon}$. By Lemma 3.1 we have

$$f(Z) = \frac{9(q+\epsilon)}{24} \geqslant \frac{3(q-1)}{8}.$$

There is only one conjugacy class of subgroups isomorphic to S_3 in K, so by Corollary 3.2 we have

$$f(S_3) = \frac{|N_T(S_3)|}{|N_K(S_3)|} = \frac{|N_T(S_3)|}{6}.$$

Now from the list of maximal subgroups of T as given in [12], we have $S_3 \leqslant N_T(S_3) \leqslant D_{q\pm1}, S_4$ or A_5. In the first case, we have $N_T(S_3) = N_T(D_6) = N_{D_{q\pm1}}(D_6) = D_6$ or D_{12}. In the second and third cases, we have $N_T(S_3) = S_3$, as S_3 is maximal and not normal in S_4 and A_5. So $|N_T(S_3)| \leqslant 12$. Thus $f(S_3) \leqslant \frac{12}{6} = 2$.

There are four subgroups isomorphic to C_2^2 in K, and earlier in this proof we calculated $|N_T(X)| = 24$. So by Lemma 3.1 we get

$$f(X) \leqslant \frac{4 \cdot 24}{24} = 4.$$

So $g(Z) \geqslant (3(q-1))/8 - 4 - 2 \times 2 + 2 > 0$ for $q > 17$. Thus the second part of the lemma holds. □

Lemma 3.6. *Let $q = 2^f$ for some $f \geqslant 2$ and suppose that $K \cong D_{2(q+1)}$ is a subgroup of T. Then there exists $t \in T$ such that $K \cap K^t \cong C_2$.*

Proof. Let $y \in K$ be an involution. Since $q+1$ is odd all involutions of K are conjugate and $\mathbf{C}_K(y) = \langle y \rangle$. Moreover, all involutions in T are conjugate and T contains an elementary abelian subgroup of order $2^f \geqslant 4$. Hence there exists $t \in \mathbf{C}_T(y)$ with $t \notin K$. Thus $y \in K \cap K^t \neq K$. We show that $K \cap K^t = \langle y \rangle$. Let $x \in K$ have odd order. Then by the maximality of K in T we have that $K = N_T(\langle x \rangle)$. If we also have $x \in K^t$ then by the same argument we have $K^t = N_T(\langle x \rangle)$, contradicting $K \neq K^t$. Thus $|K \cap K^t|$ is a power of 2 and we are done. □

4. When $T = \mathrm{PSL}(2, q)$

Recall the group $G(m, T)$ defined in Lemma 2.3. From now on, we let $T = \mathrm{PSL}(2, q)$, a non-abelian simple group, so for convenience we write $G(m, q) = G(m, \mathrm{PSL}(2, q))$ where $m \geqslant 2$ and $q \geqslant 4$. Recall $H = T \wr S_m$ and $L = \{(x, \ldots, x)\sigma \mid x \in T, \sigma \in S_m\}$.

The first lemma deals with the $m = 2$ case. We shall write $S_2 = \langle \iota \rangle$, so that $H = T \wr S_2 = (T \times T) \rtimes \langle \iota \rangle$.

Lemma 4.1. *Suppose $m = 2$. Let $D = P_1 \wr S_2 = (P_1 \times P_1) \rtimes \langle \iota \rangle$ and suppose that $t = (1, s) \in H$ such that $s \notin P_1$ is an involution. Then*

$$D^t \cap L \cong D_{2(q-1)/(2,q-1)}$$

and $\iota \notin D^t \cap L$.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Proof. We have $P_1 \cap P_1^s \cong C_{(q-1)/(2,q-1)}$ and $\langle P_1 \cap P_1^s, s\rangle \cong D_{2(q-1)/(2,q-1)}$. Let $M = \{(x,x) \mid x \in T\}$. Then $D^t \cap M \cong P_1 \cap P_1^s$. Moreover, $\iota^{(1,s)} = (s,s)\iota \in D^t \cap L$. Since $|L : M| = 2$, it follows that $|D^t \cap L : D^t \cap M| = 2$ and so

$$D^t \cap L = \langle \{(x,x) \mid x \in P_1 \cap P_1^s\}, (s,s)\iota\rangle \cong \langle P_1 \cap P_1^s, s\rangle \cong D_{2(q-1)/(2,q-1)}.$$

Moreover, note that $\iota \notin D^t \cap L$. □

Theorem 4.2. *Each row of Table 1 gives a triple (m,q,d) such that d is a subdegree of $G(m,q)$. Unless stated otherwise, we assume $m \geqslant 2$ and $q \geqslant 4$.*

Proof. We begin by proving Row 1. When $m \geqslant 3$, this follows from setting $K = P_1$ in Corollary 2.9 and noting that for any $s \in T \setminus P_1$, we have $P_1 \cap P_1^s \cong C_{q-1/(2,q-1)}$, which has non-trivial centre. When $m = 2$ and $q \equiv 1 \pmod 4$, set $D = (P_1 \times P_1) \rtimes \langle\iota\rangle$ and note that P_1 is maximal in T. By Lemma 4.1 there exists $t \in H$ such that $D^t \cap L \cong D_{q-1}$ and $\iota \notin D^t \cap L$. So $Z(D^t \cap L) \cong C_2$ contains an element $(\eta,\eta)\sigma$ with $\eta \neq 1$ and we can finish by Corollary 2.7.

Next, we prove Row 2. Let $\gamma \in T$ be an involution. If $q \equiv 1 \pmod 4$ then $\mathbf{C}_T(\gamma) = D_{q-1}$, and if $q \equiv 3 \pmod 4$ then $\mathbf{C}_T(\gamma) = D_{q+1}$. Hence Lemma 2.11 yields the subdegrees listed.

Row 3 follows from letting $K = D_{2(q+1)}$ in Corollary 2.10 and using Lemma 3.6 to guarantee the existence of $t \in T$ such that $K \cap K^t \cong C_2$.

Now consider Row 4. If q is odd, then there exists $\gamma \in T$ of order $(q+1)/2$. If q is odd and $q \geqslant 7$, then there exists $\gamma \in T$ of order $(q-1)/2$. Finally, if q is even and $\epsilon \in \{-1,1\}$, then there exists $\gamma \in T$ of order $q+\epsilon$. In each of these cases it can be shown that $\mathbf{C}_T(\gamma) = \langle\gamma\rangle$, so by Lemma 2.11 we are done.

To see why Row 5 holds, let Z be the set of elements in $\mathrm{SL}(2,q)$ that are in the centre of $\mathrm{GL}(2,q)$ and set

$$\gamma = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} Z,$$

an element of T. Then $\mathbf{C}_T(\gamma)$ has order q and so Lemma 2.11 implies that

$$\left(\frac{|T|}{q}\right)^m = \left(\frac{q^2-1}{(2,q-1)}\right)^m$$

is a subdegree of $G(m,q)$.

If $m \geqslant 3$, then Row 6 holds by letting $K = S_4$ in Corollary 2.9 and using Lemma 3.5, which guarantees the existence of $t \in T$ such that $K \cap K^t \cong C_2^2$. It remains to consider the $m = 2$ case. The $q = 7$ case is done in [6]. If $q > 7$, then the restrictions on q imply that $q \geqslant 17$, and then by Lemma 3.5 there exists $s \in T$ such that $K \cap K^s \cong C_2$. So by Corollary 2.10 it follows that $|T : K|^2 = (|T|/24)^2$ is a subdegree of $G(2,q)$.

Finally, we consider Rows 7 and 8. Let K be a subgroup of T isomorphic to A_5 (such a subgroup exists and is maximal for the values of q in Row 7). Suppose first that $q \geqslant 19$. By Lemma 3.4, there is $t \in T$ such that $K \cap K^t \cong C_2$ and so Corollary 2.10 shows that Row 7 holds for $q \geqslant 19$. Suppose now that $q \in \{9, 11\}$ and first consider the case where $m \geqslant 6$. By Magma [2], for all $t \in T$ with $t \notin K$, $K \cap K^t = A_4$ if $q = 9$ and

$K \cap K^t \cong S_3$ if $q = 11$. On the other hand, there are $r, s \in T$ such that $K \cap K^r \cap K^s \cong C_3$ if $q = 9$ and $K \cap K^r \cap K^s \cong C_2$ if $q = 11$. By our choice of r and s, we have $K \cap K^r \neq K \cap K^r \cap K^s \neq K \cap K^s$, and so neither of the elements r, s or sr^{-1} can be contained in K. Set $h = (s, r, r, 1 \dots, 1) = (a_1, \dots, a_m)$ and let us compute $D^h \cap L$. Suppose $x = ((k_1, \dots, k_m)\sigma)^h \in D^h \cap L$ for some $k_i \in K$ and $\sigma \in S_m$. Now

$$\begin{aligned} x = ((k_1, \dots, k_m)\sigma)^h &= h^{-1}(k_1, \dots, k_m)\sigma h \\ &= h^{-1}(k_1, \dots, k_m)h^{\sigma^{-1}}\sigma \\ &= (s^{-1}, r^{-1}, r^{-1}, 1, \dots, 1)(k_1, \dots, k_m)(a_{1^\sigma}, \dots, a_{m^\sigma})\sigma \\ &= (s^{-1}k_1a_{1^\sigma}, r^{-1}k_2a_{2^\sigma}, r^{-1}k_3a_{3^\sigma}, k_4a_{4^\sigma}, \dots, k_ma_{m^\sigma})\sigma. \end{aligned}$$

Suppose σ does not fix the set $\{1, \dots, 3\}$. Then, since $m \geqslant 6$, there exist i, j such that $4 \leqslant i, j \leqslant m$ and $a_{i^\sigma} \neq a_{j^\sigma}$. Since $x \in L$, we have $k_ia_{i^\sigma} = k_ja_{j^\sigma}$ and $a_{i^\sigma}(a_{j^\sigma})^{-1} = k_i^{-1}k_j \in K$. But $a_{i^\sigma}(a_{j^\sigma})^{-1} = r, s, sr^{-1}$ or the inverse of one of these, none of which lie in K, a contradiction. Hence σ must fix $\{1, 2, 3\}$ setwise. Suppose now that σ does not fix $\{2, 3\}$ setwise. Then $a_{2^\sigma} \neq a_{3^\sigma}$. Since $x \in L$, we have $r^{-1}k_2a_{2^\sigma} = r^{-1}k_3a_{3^\sigma}$ and $a_{2^\sigma}(a_{3^\sigma})^{-1} = k_3^{-1}k_2 \in K$. But this means that sr^{-1} or $rs^{-1} = (sr^{-1})^{-1}$ lies in K, which is not true, so σ must fix $\{2, 3\}$ setwise. Thus

$$x = (k_1^s, k_2^r, k_3^r, k_4, \dots, k_m)\sigma$$

and so, with $P \cong C_2 \times S_{m-3}$ the subgroup of S_m consisting of all permutations fixing $\{2, 3\}$ and $\{4, \dots, m\}$ setwise, we have

$$\begin{aligned} D^h \cap L &= \{(k_1^s, k_2^r, k_3^r, k_4, \dots, k_m)\sigma \mid k_i \in K, \sigma \in P\} \cap L \\ &\cong (K^s \cap K^r \cap K) \times P. \end{aligned}$$

Since $K \cap K^r \cap K^s = C_2$ or C_3, it follows that $Z(D^t \cap L)$ contains an element $(\eta, \dots, \eta)\sigma$ with $\eta \neq 1$. Thus Corollary 2.7 implies $|T : K|^m = (|T|/60)^m$ is a subdegree of $G(m, q)$.

If $2 \leqslant m \leqslant 5$ and $q = 11$, then computations in Magma [2] show there is $t \in H$ such that $Z(D^t \cap L)$ contains a suitable element to apply Corollary 2.7. For $q = 9$ and $2 \leqslant m \leqslant 5$, there is no such element, hence the restriction $m \geqslant 6$ in Row 8. □

We can also make use of Lemma 2.5 by allowing D not to be maximal in H. In this case we do not get an exact subdegree, but we do prove that there exists a subdegree dividing some number. This will prove to be useful in constructing an infinite family with non-trivial coprime subdegrees.

Lemma 4.3. *Let D be a subgroup of H. Suppose there exists $t \in H$ such that $(\eta, \dots, \eta)\sigma \in Z(D^t \cap L)$ with $\eta \neq 1$. Then $G(m, T)$ has a non-trivial subdegree dividing $|H : D|$.*

Proof. Define g as in Equation (2.1). Then by Lemma 2.5, $D \leqslant \mathbf{C}_H(g)$, so the subdegree $|H : \mathbf{C}_H(g)|$ divides $|H : D|$. To show that this subdegree is non-trivial, it suffices to show that $g \neq \mathrm{id}$, which is true, as by Lemma 2.5 we have that g is non-constant. □

Corollary 4.4. *The group $G(2,q)$ has a non-trivial subdegree dividing $2(q+1)^2$.*

Proof. Let $D = P_1 \times P_1$ and let $t = (1, s)$ for some $s \notin P_1$. Then $D^t \cap L \cong P_1 \cap P_1^s \cong C_{(q-1)/(2,q-1)}$ has non-trivial centre. Since $D^t \cap L \leqslant T^2$, it follows that the conditions in Lemma 4.3 have been satisfied, so $G(2,q)$ has a subdegree dividing $|H : D| = 2(q+1)^2$. □

We now present some infinite families of primitive TW groups with non-trivial coprime subdegrees and so prove Theorem 1.1.

Theorem 4.5. *Each row of Table 2 gives a quadruple (m, q, d_1, d_2) such that d_1 and d_2 are non-trivial coprime subdegrees of $G(m, q)$.*

Proof. This follows from using the data in Lemma 4.2, apart from using Corollary 4.4 to construct the subdegree dividing $2(q+1)^2$ in Row 1. □

5. Characterization results

Recall the action of $H = T \wr S_m$ on $N = \{f \in T^H \mid f(z\ell) = f(z)^{\phi(\ell)} \quad \forall z \in H, \ell \in L\}$, where $L = \{(x, \ldots, x)\sigma \mid x \in T, \sigma \in S_m\}$, and $\phi((x, \ldots, x)\sigma) = i_x$ for all $(x, \ldots, x)\sigma \in L$ (i_x denotes the automorphism induced on T by conjugation by x). We will investigate this action in more detail. Also, define the projection maps $\pi_i : T^m \to T$ for all $1 \leqslant i \leqslant m$ by $\pi_i((t_1, \ldots, t_m)) = t_i$ for all $t_1, \ldots, t_m \in T$.

Lemma 5.1. *Let $f \in T^H$. Then $f \in N$ if and only if*

$$f((t_1, \ldots, t_m)\sigma) = [f((t_1 t_m^{-1}, \ldots, t_{m-1} t_m^{-1}, 1))]^{t_m}$$

for all $t_1, \ldots, t_m \in T$ and $\sigma \in S_m$.

Proof. Let $f \in N$. For all $t_1, \ldots, t_m \in T$ and $\sigma \in S_m$ with $z = (t_1 t_m^{-1}, \ldots, t_{m-1} t_m^{-1}, 1)$ and $\ell = (t_m, \ldots, t_m)\sigma$ we have

$$\begin{aligned} f((t_1, \ldots, t_m)\sigma) &= f(z\ell) \\ &= f(z)^{\phi(\ell)} \\ &= [f((t_1 t_m^{-1}, \ldots, t_{m-1} t_m^{-1}, 1))]^{t_m}. \end{aligned}$$

Conversely, suppose that $f((t_1, \ldots, t_m)\sigma) = [f((t_1 t_m^{-1}, \ldots, t_{m-1} t_m^{-1}, 1))]^{t_m}$ holds for all $t_1, \ldots, t_m \in T$ and $\sigma \in S_m$. Then for any $z = (a_1, \ldots, a_m)\sigma_1 \in H$ and $\ell = (t, \ldots, t)\sigma_2$ we have

$$\begin{aligned} f(z\ell) = f((a_1 t, \ldots, a_m t)\sigma_1\sigma_2) &= [f((a_1 a_m^{-1}, \ldots, a_{m-1} a_m^{-1}, 1))]^{a_m t} \\ &= [f((a_1, \ldots, a_m)\sigma_1)]^t \\ &= f(z)^{\phi(\ell)}, \end{aligned}$$

so $f \in N$. □

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Lemma 5.2. *If for some $f \in N$ we have $T^m \leqslant H_f$, then $f = id$.*

Proof. Define a function $\alpha : T^{m-1} \to T$ by $\alpha((x_1, \dots, x_{m-1})) = f((x_1, \dots, x_{m-1}, 1))$ for all $x_i \in T$. We will use Lemma 5.1 in the following series of manipulations. We have $(t_1, \dots, t_m) \in H_f$ for all $t_1, \dots, t_m \in T$ if and only if for all $t_i, a_i \in T$ and $\sigma \in S_m$ we have

$$\begin{aligned} & f^{(t_1,\dots,t_m)}((a_1, \dots, a_m)\sigma) = f((a_1, \dots, a_m)\sigma) \\ & \iff f((t_1a_1, \dots, t_ma_m)\sigma) = f((a_1, \dots, a_m)\sigma) \\ & \iff [f((t_1a_1a_m^{-1}t_m^{-1}, \dots, t_{m-1}a_{m-1}a_m^{-1}t_m^{-1}, 1))]^{t_m} = f((a_1a_m^{-1}, \dots, a_{m-1}a_m^{-1}, 1)). \end{aligned}$$

This is equivalent to

$$[\alpha((t_1s_1t_m^{-1}, \dots, t_{m-1}s_{m-1}t_m^{-1}))]^{t_m} = \alpha((s_1, \dots, s_{m-1})) \quad \forall\, t_i, s_i \in T.$$

By setting t_m and the s_i to be 1, and varying $t_1, \dots, t_{m-1}$, we see that α is a constant function. Suppose the value of α is always equal to $y \in T$. Then $y = y^{t_m}$ for all $t_m \in T$, so $y \in Z(T) = 1$. Thus $\alpha((x_1, \dots, x_{m-1})) = 1$ for all $x_i \in T$. By Lemma 5.1, we have $f = \text{id}$. □

Lemma 5.3. *Let X be a subgroup of $H = T \wr S_m$ that does not contain T^m. Then $|H : X|$ is divisible by $|T : K|$ for some maximal subgroup K of T.*

Proof. Since T^m is normal in H, it follows that $|X : X \cap T^m|$ divides $|H : T^m|$. Now

$$|H : X| = \frac{|H : X \cap T^m|}{|X : X \cap T^m|} = \frac{|H : T^m||T^m : X \cap T^m|}{|X : X \cap T^m|},$$

so $|H : X|$ is divisible by $|T^m : X \cap T^m|$. It suffices to show that for any proper subgroup Y of T^m, we have that $|T^m : Y|$ is divisible by $|T : K|$ for some maximal subgroup K of T.

Suppose there exists i such that $\pi_i(Y) < T$, and assume without loss of generality that $\pi_1(Y) < T$. Then there exists a maximal subgroup K of T such that $\pi_1(Y) \leqslant K$. So $Y \leqslant K \times T \times \cdots \times T$, and $|T^m : Y|$ is divisible by $|T^m : K \times T \times \cdots \times T| = |T : K|$. Thus we are done in this case. If $\pi_i(Y) = T$ for all i, then $Y \cong T^k$ for some $k < m$. Then $|T^m : Y| = |T|^{m-k}$ is divisible by $|T|$ and thus $|T : K|$ for any maximal subgroup K of T. □

Corollary 5.4. *Let $f \in N \setminus \{id\}$. Then $|H : H_f|$ is divisible by $|T : K|$ for some maximal subgroup K of T.*

Proof. This follows immediately from Lemmas 5.2 and 5.3. □

If $m \geqslant 3$, then the results we have from the previous sections are enough to determine all q such that $G(m, q)$ has non-trivial coprime subdegrees.

Theorem 5.5. *Suppose $m \geqslant 3$. Then $G(m, q)$ has non-trivial coprime subdegrees if and only if either q is even or $q \equiv 3 \pmod 4$ or $q = 29$.*

Proof. By the results in § 4 we see that for all these values of q the group $G(m, q)$ has non-trivial coprime subdegrees. Now suppose that the group $G(m, q)$ has non-trivial

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

coprime subdegrees. Then there exist $f, g \in N \setminus \{\mathrm{id}\}$ such that $|H : H_f|$ and $|H : H_g|$ are coprime. By Corollary 5.4 there exist K_1 and K_2 maximal in T such that $|H : H_f|$ is divisible by $|T : K_1|$ and $|H : H_g|$ is divisible by $|T : K_2|$. Since $|T : K_1|$ and $|T : K_2|$ are coprime, it follows from Lemma 3.16 in [**11**] that $T = K_1K_2$ is a maximal coprime factorization. By the list in [**6**] it follows that either q is even, or $q \equiv 3 \pmod 4$ or $q = 29$. □

6. Maximal subgroups of $H = T \wr S_2$ and $T \times T$

To address the $m = 2$ case, we will need information about the maximal subgroups of $H = T \wr S_2$ and $T \times T$, where T is a non-abelian simple group. The following lemma is part of the proof of the O'Nan–Scott theorem on primitive groups. We separate it out and include a proof for completeness.

Lemma 6.1. *Let X be a maximal subgroup of $H = T \wr S_2 = (T \times T) \rtimes \langle\iota\rangle$. Then up to conjugacy X has one of the following three types:*

(1) $X = T^2 = T \times T$ *and* $|H : X| = 2$;

(2) $X = \langle S, (a, b)\iota\rangle$ *where* $S = \{(t, t^\sigma) \mid t \in T\}$ *for some* $\sigma \in \mathrm{Aut}(T)$ *and* $a, b \in T$ *such that* $(ab)^\sigma = ba$ *and* $\sigma i_b \sigma = i_a$, *and* $|H : X| = |T|$;

(3) $X = K \wr S_2$ *for some K maximal in T, and* $|H : X| = |T : K|^2$.

Proof. Let M be a proper subgroup of H. If $M \leqslant T^2$, then M is contained in the proper subgroup T^2, which is of type (2.1).

If $M \nleqslant T^2$, there exists $(a, b)\iota \in M$ for some $a, b \in T$. Thus $|M : M \cap T^2| = 2$ and $\langle M \cap T^2, (a, b)\iota\rangle = M$. Also note that $((a, b)\iota)^2 = (ab, ba) \in M \cap T^2$. Moreover, for any $t_1, t_2 \in T$ we have $(t_1, t_2)^{(a,b)\iota} = (t_2^b, t_1^a)$, so $\pi_2(M \cap T^2) = (\pi_1(M \cap T^2))^a$.

If $\pi_1(M \cap T^2) = \pi_2(M \cap T^2) = T$, then $M \cap T^2 = T^2$ or $M \cap T^2 \cong T$. If $M \cap T^2 = T^2$, then since M contains an element outside T^2 we must have $M = H$, a contradiction. So $M \cap T^2 \cong T$. Thus $M \cap T^2 = \{(t, t^\sigma) \mid t \in T\} = S$, where $\alpha \in \mathrm{Aut}(T)$. Since $(ab, ba) \in M \cap T^2$, it follows that $(ab)^\sigma = ba$. Since $M \cap T^2 \lhd M$, we have that $(a, b)\iota$ normalizes $M \cap T^2$. If we let i_x denote the automorphism of T induced by conjugation by x, we have $(t, t^\sigma)^{(a,b)\iota} = (t^{\sigma i_b}, t^{i_a}) \in M \cap T^2$ for all $t \in T$, so $\sigma i_b \sigma = i_a$. Thus, M is a subgroup of type (2.2) and since $|M : M \cap T^2| = 2$ we have that $|H : M| = |T|$.

Finally, if $\pi_1(M \cap T^2) < T$, let K be maximal in T such that $\pi_1(M \cap T^2) \leqslant K$. Then $\pi_2(M \cap T^2) \leqslant K^a$. So $M = \langle M \cap T^2, (a, b)\iota\rangle \leqslant \langle K \times K^a, (a, b)\iota\rangle$. Moreover, since $(ab, ba) \in M \cap T^2$ we have that $ab \in K$. Then $(1, ((ab)^{-1})^a)(a, b)\iota = (a, a^{-1})\iota$, so $\langle K \times K^a, (a, b)\iota\rangle = \langle K \times K^a, (a, a^{-1})\iota\rangle$. Now $((K \times K) \rtimes \langle\iota\rangle)^{(1,a)} = \langle K \times K^a, (a, a^{-1})\iota\rangle$, so up to conjugacy K is contained in a subgroup of type (7.1).

Hence each subgroup M of H is contained in a type (2.1), (2.2) or (7.1) subgroup. Observe that a type (i) subgroup cannot be contained in a type (j) subgroup if $i \neq j$, and that a type (i) subgroup cannot be properly contained in another type (i) subgroup. Hence the subgroups stated in the lemma are precisely the maximal subgroups of H. □

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Lemma 6.2. *The maximal subgroups of T^2 are of one of the following two types:*

(1) *$K \times T$ or $T \times K$ for some K maximal in T;*

(2) *$\{(t, t^\sigma) \mid t \in T\}$ where $\sigma \in Aut(T)$.*

Proof. Let M be a proper subgroup of T^2. If $\pi_1(M) < T$, then let K be maximal in T such that $\pi_1(M) \leqslant K$. Then $M \leqslant K \times T$. Similarly, if $\pi_2(M) < T$ then there exists K maximal in T such that $M \leqslant T \times K$. So if there exists i such that $\pi_i(M)$ is a proper subgroup of T, it follows that M is contained in a type (2.1) subgroup. If $\pi_1(M) = \pi_2(M) = T$, then $M \cong T$, so M is equal to (and thus contained in) a type (2.2) subgroup. So in all cases, M is contained in a type (2.1) or (2.2) subgroup.

It is easy to show that a type (i) subgroup cannot be contained in a type (j) subgroup if $i \neq j$, and that a type (i) subgroup cannot be properly contained in another type (i) subgroup. So type (2.1) and type (2.2) subgroups are maximal in T^2. □

7. The $m = 2$ case

We now address the $m = 2$ case. Since $\mathrm{PSL}(2, 4) \cong \mathrm{PSL}(2, 5)$, it follows that $G(2, 4) \cong G(2, 5)$. So, from now on, suppose that $q \neq 5$. Recall that $H = T \wr S_2$ and $L = \{(x, x)\sigma \mid x \in T, \sigma \in S_2\}$.

Lemma 7.1. *Suppose that $|H : H_f|$ and $|H : H_g|$ are non-trivial coprime subdegrees of $G(2, q)$. Let R_1 and R_2 be maximal subgroups of H such that $H_f \leqslant R_1$ and $H_g \leqslant R_2$. Then one of the following holds:*

(1) *R_1 and R_2 are of type (7.1) in Lemma 6.1;*

(2) *after reordering, $R_1 = T^2$ and H_f is contained in a subgroup of type (2.1) in Lemma 6.2, R_2 is of type (7.1) in Lemma 6.1 and $|H : R_2|$ is odd.*

Proof. By Lemma 5.4, neither R_1 nor R_2 can be of type (2.2) as $|T|$ and $|T : K|$ are never coprime for any K maximal in T. If both R_1 and R_2 are of type (7.1) in Lemma 6.1, we obtain the first case. Now assume without loss of generality that R_1 is of type (2.1) and so $R_1 = T^2$. Then by Lemma 5.2 we have $H_f \neq T^2$, so H_f is strictly contained in T^2. Thus H_f is contained in a maximal subgroup of T^2, say M. Then $|H : H_f|$ is divisible by $|H : M|$. If M is of type (2.2) in Lemma 6.2, then $|H : M| = 2|T|$, so by Lemma 5.4 it is not possible for $|H : H_f|$ and $|H : H_g|$ to be coprime. Thus M is of type (2.1) in Lemma 6.2. It is not possible for R_2 to be of type (2.1) or (2.2) as then both $|H : R_1|$ and $|H : R_2|$ will be even. Thus R_2 is of type (7.1) in Lemma 6.1. We note that $|H : R_2|$ is odd since $|H : M|$ is even. □

Lemma 7.2. *Suppose that Case (2.2) of Lemma 7.1 holds. Let H_f be contained in a subgroup of type (2.1) in Lemma 6.2 constructed from K_1. Let R_2 be constructed from K_2. Then the possibilities for K_1 and K_2 are as follows:*

(1) *q is even, $K_1 = D_{2(q+1)}$ and $K_2 = P_1$;*

(2) *$q \equiv 3 \pmod 4$ with $q > 7$, $K_1 = P_1$ and $K_2 = D_{q+1}$;*

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

(3) *$q \in \{7, 23\}$, $K_1 = P_1$ and $K_2 = S_4$;*

(4) *$q \in \{11, 19, 29, 59\}$, $K_1 = P_1$ and $K_2 = A_5$.*

Proof. We need $|H : M| = 2|T : K_1|$ to be coprime to $|H : R_2| = |T : K_2|^2$, where $H_f \leqslant M = T \times K_1$ or $K_1 \times T$. In particular, $|T : K_1|$ must be coprime to $|T : K_2|$ so we can systematically work through the list of maximal coprime factorizations in [**6**], to obtain the possibilities mentioned above. □

We will do some detailed analysis of the possibilities for H_f and H_g when $|H : H_f|$ and $|H : H_g|$ are non-trivial coprime subdegrees of $G(2, q)$. Since $H_f^h = H_{f^h}$ for all $h \in H$, it suffices to consider H_f up to conjugacy in H. We begin with a lemma about subgroups of $T \times P_1$ that will help simplify our casework later.

Lemma 7.3. *Let $q \equiv 3 \pmod 4$. Let X be a subgroup of $M = T \times P_1$ such that $|M : X|$ is coprime to $\frac{1}{2}q(q-1)$. Then $X = M$ or $X = P_1^t \times P_1$ for some $t \in T$.*

Proof. If $\pi_1(X) = T$, then $T = \pi_1(X) \cong X/\mathrm{ker}\pi_1$, so $|X| = |T||\mathrm{ker}\pi_1|$. Now

$$|M : X| = \frac{|T||P_1|}{|T||\mathrm{ker}\pi_1|} = \frac{|P_1|}{|\mathrm{ker}\pi_1|}$$

divides $|P_1| = \frac{1}{2}q(q-1)$, so we must have $X = M$.

Now suppose that $\pi_1(X) < T$. Then $|X| \leqslant |\pi_1(X)||P_1|$. Note that $|M| = |T||P_1| = |P_1|^2(q+1)$, and every prime factor of $|P_1|^2$ is clearly a prime factor of $\frac{1}{2}q(q-1) = |P_1|$, so for $|M : X|$ to be coprime to $\frac{1}{2}q(q-1)$ we require $|X| \geqslant |P_1|^2$. Combining this with $|X| \leqslant |\pi_1(X)||P_1|$ we obtain $|\pi_1(X)| \geqslant |P_1|$. We cannot have $q = 7$ and $\pi_1(X) = S_4$ as then $|M : X|$ would be divisible by $|M : S_4 \times P_1| = 7$, which is not coprime to $\frac{1}{2}q(q-1) = 21$. Similarly, we cannot have $q = 11$ and $\pi_1(X) = A_5$ as then $|M : X|$ would be divisible by $|M : A_5 \times P_1| = 11$, which is not coprime to $\frac{1}{2}q(q-1) = 55$. So it follows from [**12**] that $\pi_1(X) \cong P_1$. Since $|X| \geqslant |P_1|^2$ it follows that $X = P_1^t \times P_1$. □

Lemma 7.4. *If $|H : H_f|$ and $|H : H_g|$ are non-trivial coprime subdegrees of $G(2, q)$, then up to reordering one of the possibilities in Table 4 holds.*

Proof. Suppose that $|H : H_f|$ and $|H : H_g|$ are non-trivial coprime subdegrees of $G(2, q)$. Let R_1 and R_2 be maximal subgroups of H such that $H_f \leqslant R_1$ and $H_g \leqslant R_2$. According to Lemma 7.1, we can split our analysis into two cases.

Case 1. R_1 and R_2 are of type (7.1) in Lemma 6.1 and are constructed from K_1 and K_2, respectively.

Then $|T : K_1|^2$ and $|T : K_2|^2$ are the indices of R_1 and R_2, so they must be coprime. Thus $|T : K_1|$ and $|T : K_2|$ are coprime, so $T = K_1K_2$ is a maximal coprime factorization by Lemma 3.16 in [**11**]. We will work through the list in [**6**], and assume without loss of generality that $K_1 = P_1$.

Subcase 1a. q is even and $K_2 = D_{2(q+1)}$.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Table 4. *Possibilities for H_f and H_g.*

Row	q	H_f	H_g
1a	even	$P_1 \wr S_2$	$C_{q+1} \times C_{q+1} \leqslant H_g$
1b		$P_1 \wr S_2$	$\lvert T \times D_{2(q+1)} : H_g\rvert$ is coprime to $(q+1)^2$
2	$\equiv 3 \pmod 4$	$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$D_{q+1} \wr S_2$
3a	7	$C_7 \times C_7 \leqslant H_f$	$S_4 \wr S_2$
3b		$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$D_8 \wr S_2$
4a	11	$C_{11} \times C_{11} \leqslant H_f$	$A_5 \wr S_2$
4b		$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$A_4 \wr S_2$
5	19	$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$A_5 \wr S_2$
6	23	$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$S_4 \wr S_2$
7	29	$X \times X \leqslant H_f$ where $\lvert P_1 : X\rvert = 2$	$A_5 \wr S_2$
8	59	$P_1 \wr S_2, T \times P_1$ or $P_1 \times P_1$	$A_5 \wr S_2$

Since $|R_1 : H_f|$ is coprime to $|H : R_2| = (\frac{1}{2}q(q-1))^2$ and divides $|R_1| = 2(q(q-1))^2$, it follows that $H_f = R_1$. Since $|H : R_1| = (q+1)^2$, we have that $|H : H_g| = |H : R_2||R_2 : H_g| = (\frac{1}{2}q(q-1))^2|R_2 : H_g|$ is coprime to $(q+1)^2$. Thus $|R_2 : H_g|$ is coprime to $(q+1)^2$ so $C_{q+1} \times C_{q+1} \leqslant H_g$ and we are in Row 1a of Table 4.

Subcase 1b. $q \equiv 3 \pmod 4$ with $q > 7$ and $K_2 = D_{q+1}$.

We have $|H| = |R_1||R_2|$, so $H_f = R_1$ and $H_g = R_2$. Thus we are in Row 2.

Subcase 1c. $q \in \{7, 23\}$ and $K_2 = S_4$.

Suppose $q = 7$. Since $|R_2 : H_g|$ is coprime to $|H : R_1| = 8^2$ and divides $|R_2| = 2(24^2)$, it follows that $|R_2 : H_g|$ is a power of 3. Thus $H_g = R_2$ or $H_g \cong D_8 \wr S_2$. In either case, $|R_1 : H_f|$ is coprime to $|H : R_2| = 7^2$, so H_f contains the subgroup of R_1 isomorphic to $C_7 \times C_7$. If $H_g = R_2$, we are in Row 3a. Furthermore, if $H_g = D_8 \wr S_2$, then since $|R_1 : H_f|$ is coprime to $|H : H_g| = 21^2$ and divides $|R_1| = 2(21^2)$, we must have $|R_1 : H_f| = 1$ or 2. Thus $H_f = R_1$ or $H_f = P_1 \times P_1$ and we are in Row 3b.

If $q = 23$, we have $|H| = |R_1||R_2|$, so $H_f = R_1$ and $H_g = R_2$. Thus we are in Row 6.

Subcase 1d. $q \in \{11, 19, 29, 59\}$ and $K_2 = A_5$.

If $q = 11$, then since $|R_2 : H_g|$ is coprime to $|H : R_1| = 12^2$ and divides $|R_2| = 2(60^2)$, it follows that $|R_2 : H_g|$ must be a power of 5. Thus $H_g = R_2$ or $H_g = A_4 \wr S_2$. In either case, $|R_1 : H_f|$ is coprime to $|H : R_2| = 11^2$, so H_f contains the subgroup of R_1 isomorphic to $C_{11} \times C_{11}$. If $H_g = R_2$, we are in Row 4a. Furthermore, if $H_g = A_4 \wr S_2$, then $|R_1 : H_f|$ is coprime to $|H : H_g| = 55^2$ and divides $|R_1| = 2(55^2)$, so $|R_1 : H_f| = 1$ or 2. Thus $H_f = R_1$ or $H_f = P_1 \times P_1$ and we are in Row 4b.

Suppose $q = 19$. Then $|R_1 : H_f|$ divides $|R_1| = 2(171^2)$ and is coprime to $|H : R_2| = 57^2$, so $|R_1 : H_f| = 1$ or 2. This means that $H_f = R_1$ or $H_f = P_1 \times P_1$. Also, $|R_2 : H_g|$

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

divides $|R_2| = 2(60^2)$ and is coprime to $|H : R_1| = 20^2$, so $|R_2 : H_g|$ is a power of 3. This can only happen if $H_g = R_2$, so we are in Row 5.

If $q = 29$, then since $|R_2 : H_g|$ is coprime to $|H : R_1| = 30^2$ and divides $|R_2| = 2(60^2)$, we must have $H_g = R_2$. Then since $|R_1 : H_f|$ is coprime to $|H : R_2| = 203^2$ and divides $|R_1| = 2(406^2)$, it follows that $|R_1 : H_f|$ is a power of 2. This can only happen if H_f contains the subgroup $X \times X$ of R_1, where X is the index 2 subgroup of P_1, and we get Row 7.

If $q = 59$, we are again in the situation when $|H| = |R_1||R_2|$, so $H_f = R_1$ and $H_g = R_2$. Thus we are in Row 8.

Case 2. $R_1 = T^2$ and H_f is contained in a subgroup M of type (2.1) in Lemma 6.2, and R_2 is of type (7.1) in Lemma 6.1.

Suppose that M is constructed from K_1 and R_2 is constructed from K_2. We work through the possibilities for K_1 and K_2 outlined in Lemma 7.2.

Subcase 2a. q is even, $K_1 = D_{2(q+1)}$ and $K_2 = P_1$.

Since $|R_2 : H_g|$ divides $|R_2| = 2(q(q-1))^2$ and is coprime to $|H : M| = q(q-1)$, it follows that $H_g = R_2$. Since $|H : R_2| = (q+1)^2$, we have that $|H : H_f| = |H : M||M : H_f|$ is coprime to $(q+1)^2$. Thus $|M : H_f|$ is coprime to $(q+1)^2$, so after interchanging f and g we are in Row 1b.

Subcase 2b. Any one of Cases 2, 3 or 4 in Lemma 7.2 holds.

Then $K_1 = P_1$ and $M = T \times P_1$. Hence $|H : H_f| = |H : M||M : H_f| = 2(q+1)$ $|M : H_f|$ is coprime to $|H : H_g| = |H : R_2||R_2 : H_g|$, and so $2(q+1)$ is coprime to $|R_2 : H_g|$. Now $|R_2 : H_g|$ divides $|R_2| = 2|K_2|^2$, and we can check that in all cases apart from Case 3 with $q = 7$ and Case 4 with $q \in \{11, 19\}$, the prime factors of $2|K_2|^2$ are the same as the prime factors of $2(q+1)$. So if we are in Case 2 or 3 with $q = 23$, or Case 4 with $q \in \{29, 59\}$, we must have $H_g = R_2$. We claim that this is also true in Case 4 with $q = 19$. Indeed, $2(q+1) = 20$ is coprime to $|R_2 : H_g|$, which divides $|R_2| = 2(60^2)$, so $|R_2 : H_g|$ is a power of 3, which can only happen if $H_g = R_2$.

Suppose we are in either Case 2 or 3 with $q = 23$, or Case 4 with $q \in \{19, 59\}$. Then from the above argument we have $H_g = R_2 = X \wr S_2$ and $H_f \leqslant M = T \times P_1$. So $|H : H_g| = |T : X|^2$ is coprime to $|M : H_f|$. We can check that in all these cases the prime factors of $|T : X|$ are the same as the prime factors of $\frac{1}{2}q(q-1)$, so by Lemma 7.3 we have $H_f = P_1 \times P_1$ or $H_f = M$. Thus we are in Row 2, 5, 6 or 8.

Consider Case 4 with $q = 29$. We have that $|M : H_f|$ is coprime to $|H : H_g| = 203^2$. Moreover, $|M| = 203^2 \cdot 120$ so $|M : H_f|$ divides 120. This can only happen if H_f contains a subgroup of M isomorphic to $X \times X$ where X has index 2 in P_1, yielding Row 7.

Next, consider Case 3 with $q = 7$. Then $|R_2 : H_g|$ is coprime to $2(q+1) = 16$ and divides $|R_2| = 2(24^2)$, so $|R_2 : H_g|$ is a power of 3. This means that $H_g = R_2$ or $H_g \cong D_8 \wr S_2$. In either case, $|M : H_f|$ is coprime to $|H : R_2| = 7^2$, so H_f contains a subgroup of M isomorphic to $C_7 \times C_7$. If $H_g = D_8 \wr S_2$, then $|M : H_f|$ is coprime to $|H : H_g| = 21^2$ and divides $|M| = 21^2 \cdot 7$, so $|M : H_f|$ is a power of 2 and $H_f = M$ or $H_f = P_1 \times P_1$. Thus we are in Row 3b.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Finally, consider Case 4 with $q = 11$. Then $|R_2 : H_g|$ is coprime to $2(q+1) = 24$ and divides $|R_2| = 2(60^2)$, so $|R_2 : H_g|$ is a power of 5. This means that $H_g = R_2$ or $H_g = A_4 \wr S_2$. In either case, $|M : H_f|$ is coprime to $|H : R_2| = 11^2$, so H_f contains a subgroup of M isomorphic to $C_{11} \times C_{11}$. If $H_g = A_4 \wr S_2$, then $|M : H_f|$ is coprime to $|H : H_g| = 55^2$ and divides $|M| = 55^2 \cdot 12$; it follows that $|M : H_f|$ divides 12. This can only happen if $H_f = M$ or $H_f = P_1 \times P_1$ and we are in Row 4b. □

Now we determine some specific conditions for H_f to contain certain subgroups of H. Recall the action of H on $N = \{f \in T^H \mid f(z\ell) = f(z)^{\phi(\ell)} \quad \forall z \in H, \ell \in L\}$, where $H = (T \times T) \rtimes \langle\iota\rangle$, $L = \{(x, x) \mid x \in T\}\langle\iota\rangle$, and $\phi((x, x)\iota^k) = i_x$ for all $(x, x)\iota^k \in L$ (i_x denotes the automorphism induced on T by conjugation by x).

Lemma 7.5. *Let $f \in N$ and set $\alpha(t) = f((t, 1))$ for all $t \in T$. Let X and Y be subgroups of T. Then $X \times Y \leqslant H_f$ if and only if the following conditions hold:*

- *$\alpha(xt) = \alpha(t)$ for all $x \in X$, $t \in T$;*
- *$\alpha(ty) = \alpha(t)^y$ for all $y \in Y$, $t \in T$.*

In particular, $\alpha(x) = \alpha(1)$ for all $x \in X$.

Proof. We will use Lemma 5.1 here. We have $(x, y) \in H_f$ for all $x \in X$, $y \in Y$ if and only if

$$\begin{aligned}
&f^{(x,y)}((a, b)\iota^k) = f((a, b)\iota^k) \quad \forall a, b \in T, \forall x \in X, \forall y \in Y, \forall k \in \{0, 1\}\\
&\iff f((xa, yb)\iota^k) = f((a, b)\iota^k) \quad \forall a, b \in T, \forall x \in X, \forall y \in Y, \forall k \in \{0, 1\}\\
&\iff f((xab^{-1}y^{-1}, 1))^{yb} = f((ab^{-1}, 1))^b \quad \forall a, b \in T, \forall x \in X, \forall y \in Y\\
&\iff \alpha(xty^{-1})^y = \alpha(t) \quad \forall t \in T, \forall x \in X, \forall y \in Y.
\end{aligned}$$

We claim that this final condition is equivalent to

$$\alpha(xt) = \alpha(t) \quad \text{and} \quad \alpha(t)^y = \alpha(ty) \quad \forall t \in T, x \in X, y \in Y. \tag{7.1}$$

Indeed, if $\alpha(xty^{-1})^y = \alpha(t)$ for all $t \in T$, $x \in X$ and $y \in Y$, we can set $y = 1$ and $x = 1$, respectively, to obtain the equations in (7.1). Conversely, if the equations in (7.1) hold, then for any $t \in T$, $x \in X$ and $y \in Y$ we have

$$\alpha(t) = \alpha(xt) = \alpha(xty^{-1}y) = \alpha(xty^{-1})^y.$$

So $X \times Y \leqslant H_f$ if and only if the equations in (7.1) hold. □

Lemma 7.6. *Let K be a subgroup of T. If a function $\alpha : T \to T$ satisfies $\alpha(kt) = \alpha(t)$ and $\alpha(tk) = \alpha(t)^k$ for all $k \in K$ and $t \in T$, then $K \cap K^t$ is contained in $\mathbf{C}_T(\alpha(t))$ for all $t \in T$.*

Proof. Take any $k \in K \cap K^t$. Then $tkt^{-1} \in K$, so

$$\alpha(t)^k = \alpha(tk) = \alpha((tkt^{-1})t) = \alpha(t).$$

Thus $K \cap K^t \leqslant \mathbf{C}_T(\alpha(t))$. □

Lemma 7.7. *Let $T = PSL(2, q)$ for $q \geqslant 4$. Suppose a function $\alpha : T \to T$ satisfies $\alpha(pt) = \alpha(t)$ and $\alpha(tp) = \alpha(t)^p$ for all $p \in P_1$ and $t \in T$. Then $\alpha(t) = 1$ for all $t \in P_1$.*

Proof. By Lemma 7.6 we get $P_1 \leqslant \mathbf{C}_T(\alpha(1))$. This can only happen if $\alpha(1) = 1$ and so $\alpha(t) = 1$ for all $t \in P_1$. □

Corollary 7.8. *Let $T = PSL(2, q)$ for $q \geqslant 4$. Then there does not exist $f \in N$ such that $H_f = T \times P_1$.*

Proof. Suppose for a contradiction that such an f exists. Set $\alpha(t) = f((t, 1))$ for all $t \in T$. Then by Lemma 7.5 we have $\alpha(xt) = \alpha(t)$ and $\alpha(tp) = \alpha(t)^p$ for all $x \in T$, $p \in P_1$ and $t \in T$. We can apply Lemma 7.7 to get $\alpha(1) = 1$. Then since $\alpha(xt) = \alpha(t)$ for all $x \in T$ and $t \in T$, it follows that α is a constant function, so $\alpha(t) = 1$ for all $t \in T$. This is a contradiction as then $H_f = H$. □

Lemma 7.9. *Let $f \in N$ and set $\alpha(t) = f((t, 1))$ for all $t \in T$. Let K be a maximal subgroup of T. Then $H_f = K \wr S_2 = (K \times K) \rtimes \langle\iota\rangle$ if and only if the following conditions hold:*

- *$\alpha(kt) = \alpha(t)$ for all $k \in K$, $t \in T$;*
- *$\alpha(t) = \alpha(t^{-1})^t$ for all $t \in T$;*
- *there exists $t \in T$ such that $\alpha(t) \neq 1$.*

Proof. By Lemma 7.5 we obtain $K \times K \leqslant H_f$ if and only if

$$\alpha(kt) = \alpha(t) \quad \text{and} \quad \alpha(t)^k = \alpha(tk) \quad \forall t \in T, k \in K. \tag{7.2}$$

We now determine an equivalent set of conditions for $(K \times K)\iota \subseteq H_f$ to hold. By Lemma 5.1 we obtain $(k_1, k_2)\iota \in H_f$ for all $k_1, k_2 \in K$ if and only if

$$\begin{aligned}
&f^{(k_1,k_2)\iota}((a, b)\iota^x) = f((a, b)\iota^x) \quad \forall a, b \in T, \forall k_1, k_2 \in K, \forall x \in \{0, 1\}\\
&\iff f((k_1b, k_2a)\iota^{x+1}) = f((a, b)\iota^x) \quad \forall a, b \in T, \forall k_1, k_2 \in K, \forall x \in \{0, 1\}\\
&\iff f((k_1ba^{-1}k_2^{-1}, 1))^{k_2} = f((ab^{-1}, 1))^{ba^{-1}} \quad \forall a, b \in T, \forall k_1, k_2 \in K\\
&\iff \alpha(k_1tk_2^{-1})^{k_2} = \alpha(t^{-1})^t \quad \forall t \in T, \forall k_1, k_2 \in K.
\end{aligned}$$

We claim that this final condition is equivalent to

$$\alpha(kt) = \alpha(t) \quad \text{and} \quad \alpha(tk^{-1})^k = \alpha(t^{-1})^t \quad \forall t \in T, k \in K. \tag{7.3}$$

Indeed, if $\alpha(k_1tk_2^{-1})^{k_2} = \alpha(t^{-1})^t$ for all $t \in T$ and $k_1, k_2 \in K$, we can set $k_1 = 1$ to obtain the second equation in (7.3). By setting $k_2 = 1$ and comparing this with the equation where $k_1 = k_2 = 1$, we obtain the first equation in (7.3). Conversely, if the equations in (7.3) hold then for any $t \in T$ and $k_1, k_2 \in K$ we have

$$\alpha(k_1tk_2^{-1})^{k_2} = \alpha(tk_2^{-1})^{k_2} = \alpha(t^{-1})^t.$$

So $(K \times K)\iota \subseteq H_f$ if and only if the equations in (7.3) hold.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Putting everything together, we get $(K \times K) \rtimes \langle \iota \rangle \leqslant H_f$ if and only if

$$\alpha(kt) = \alpha(t), \quad \alpha(t)^k = \alpha(tk) \quad \text{and} \quad \alpha(tk^{-1})^k = \alpha(t^{-1})^t \quad \forall t \in T, k \in K. \tag{7.4}$$

Next, we show that these conditions are equivalent to

$$\alpha(kt) = \alpha(t) \quad \text{and} \quad \alpha(t) = \alpha(t^{-1})^t \quad \forall t \in T, k \in K. \tag{7.5}$$

Indeed, (7.5) follows from (7.4) as the first equation is the same in both, and setting $k = 1$ in the third equation of (7.4) yields the second equation in (7.5). Conversely, suppose (7.5) holds. Then

$$\alpha(tk) = \alpha(k^{-1}t^{-1})^{tk} = \alpha(t^{-1})^{tk} = \alpha(t)^k \quad \forall t \in T, k \in K,$$

proving the second equation of (7.4). Also,

$$\alpha(tk^{-1})^k = \alpha(kt^{-1})^{(tk^{-1})k} = \alpha(kt^{-1})^t = \alpha(t^{-1})^t \quad \forall t \in T, k \in K,$$

proving the third equation in (7.4). This proves the claim that $(K \times K) \rtimes \langle \iota \rangle \leqslant H_f$ if and only if the equations in (7.5) hold.

By Lemma 6.1 we have that $(K \times K) \rtimes \langle \iota \rangle$ is maximal in H, and so $H_f = (K \times K) \rtimes \langle \iota \rangle$ if and only if $(K \times K) \rtimes \langle \iota \rangle \leqslant H_f$ and $H_f < H$. Now $H_f < H$ if and only if there exists some $h \in H$ such that $f(h) \neq 1$, by Lemma 2.2. By Lemma 5.1, this is equivalent to the existence of $t \in T$ with $\alpha(t) \neq 1$. Thus, $H_f = (K \times K) \rtimes \langle \iota \rangle$ if and only if the equations in (7.5) hold and there exists $t \in T$ such that $\alpha(t) \neq 1$. □

Lemma 7.10. *Let $T = PSL(2, q)$ where $q \geqslant 4$ and either q is even or $q \equiv 3 \pmod 4$. Then no $f \in N$ exists such that $H_f = P_1 \wr S_2$.*

Proof. Suppose for a contradiction that such an f exists. Define $\alpha : T \to T$ by $\alpha(t) = f((t, 1))$ for all $t \in T$. Then, since $P_1 \times P_1 \leqslant H_f$, Lemma 7.5 implies that $\alpha(pt) = \alpha(t)$ and $\alpha(tp) = \alpha(t)^p$ for all $p \in P_1$ and $t \in T$. By Lemma 7.7 we conclude that $\alpha(t) = 1$ for all $t \in P_1$.

Now let t be an involution in T that is not contained in P_1. By Lemma 7.9 we have $\alpha(t)^t = \alpha(t^{-1})^t = \alpha(t)$, so $t \in \mathbf{C}_T(\alpha(t))$. So Lemma 7.6 implies that $P_1 \cap P_1^t < \langle P_1 \cap P_1^t, t \rangle \leqslant \mathbf{C}_T(\alpha(t))$. Now $X = \langle P_1 \cap P_1^t, t \rangle \cong D_{2(q-1)/(2,q-1)}$, which we can see by observing that t normalizes $P_1 \cap P_1^t \cong C_{q-1/(2,q-1)}$ and consulting the listed subgroups of $\mathrm{PSL}(2, q)$ in [**12**]. Hence if $X \leqslant \mathbf{C}_T(\alpha(t))$ then $\alpha(t) \in Z(X) = 1$ as $q \not\equiv 1 \pmod 4$. By Lemma 3.3 it follows that $\alpha(t) = 1$ for all $t \notin P_1$, as α is constant on the right cosets of P_1 in T. Since we previously showed that $\alpha(t) = 1$ for all $t \in P_1$, we conclude that $\alpha(t) = 1$ for all $t \in T$. But then $H_f = H$, a contradiction, so no such f exists. □

Lemma 7.11. *Let $T = PSL(2, q)$ where $q \geqslant 4$ and either q is even or $q \equiv 3 \pmod 4$. Let $f \in N \setminus \{id\}$. Then whenever $P_1 \times P_1 \leqslant H_f$, we have $P_1 \times P_1 = H_f$.*

Proof. The only proper subgroups of H containing $P_1 \times P_1$ are $T^2, P_1 \times P_1, P_1 \wr S_2, T \times P_1$ and $P_1 \times T$. Recall that the last three were disproved in Lemma 7.10 and Corollary 7.8 by noting that $T \times P_1$ and $P_1 \times T$ are conjugate in H. Finally, we cannot have $H_f = T^2$ by Lemma 5.2. □

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

Remark 7.12. We can now say more about the exact value of the subdegree in Corollary 4.4. If q is even or $q \equiv 3 \pmod 4$ then we claim that the subdegree equals $2(q+1)^2$. Indeed, the proof of Corollary 4.4 implies there exists $f \in N \setminus \{\mathrm{id}\}$ such that $P_1 \times P_1 \leqslant H_f$. Then by Lemma 7.11 we must have $P_1 \times P_1 = H_f$, so the subdegree is $|H : H_f| = 2(q+1)^2$.

Theorem 7.13. *The group $G(2,q)$ has non-trivial coprime subdegrees if and only if $q \equiv 3 \pmod 4$ or $q = 29$. Furthermore, $|H : H_f|$ and $|H : H_g|$ are non-trivial coprime subdegrees if and only if, up to reordering, one of the possibilities in Table 3 holds. Moreover, in each of these cases there exist $f, g \in N$ such that H_f and H_g are as in Table 3.*

Proof. We refer to Table 4, and use Lemmas 7.10 and 7.8 to eliminate all the cases where $H_f = P_1 \wr S_2$ or $H_f = T \times P_1$. This leaves us with the cases in Table 3, and it is easy to check that in each of these cases we obtain non-trivial coprime subdegrees. Thus, if $G(2,q)$ has non-trivial coprime subdegrees, then $q \equiv 3 \pmod 4$ or $q = 29$, and Theorem 4.5 shows that for all these values of q, the group $G(2,q)$ has non-trivial coprime subdegrees. So the first part of this theorem has been proven.

To see that in each of these cases there exist $f, g \in N$ such that H_f and H_g are as shown in Table 3, refer to Remark 7.12 and § 2 and § 4. □

Remark 7.14. Suppose that $q \equiv 3 \pmod 4$. Then $G(2,q)$ has the pair of non-trivial coprime subdegrees $(2(q+1)^2, (\frac{1}{2}q(q-1))^2)$. If $q \neq \{7, 11, 19\}$, this is the only such pair. If $q \in \{7, 11\}$, there are at least two such pairs; if $q = 19$, there are exactly two such pairs, the other pair being $(2(20)^2, 57^2)$.

We have made no attempt to determine the multiplicity of the subdegrees appearing in Table 3 (which we believe would be incredibly difficult); therefore, we have no precise information regarding the multiplicities of the pairs of coprime subdegrees. However, the group $G(2,11)$ has a pair of coprime subdegrees $(288, 3025)$ that occurs with multiplicity at least two—appearing in Row 1 and Row 4 of Table 3. We note that this is a genuine occurrence of multiplicity greater than one, because the 2-point stabilizers giving rise to the suborbits of size 288 are non-isomorphic.

References

1. R. W. Baddeley, Primitive permutation groups with a regular nonabelian normal subgroup, *Proc. Lond. Math. Soc. (3)* **67**(3) (1993), 547–595.
2. W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.
3. P. J. Cameron, C. E. Praeger, J. Saxl and G. M. Seitz, On the Sims conjecture and distance transitive graphs, *Bull. Lond. Math. Soc.* **15**(5) (1983), 499–506.
4. L. E. Dickson, *Linear groups: with an exposition of the Galois field theory*, with an introduction by W. Magnus (Dover Publications, New York, 1958).
5. J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Volume 163 (Springer-Verlag, New York, 1996).
6. S. Dolfi, R. Guralnick, C. E. Praeger and P. Spiga, Coprime subdegrees for primitive permutation groups and completely reducible linear groups, *Israel J. Math.* **195**(2) (2013), 745–772.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press

7. S. Dolfi, R. Guralnick, C. E. Praeger and P. Spiga, On the maximal number of coprime subdegrees in finite primitive permutation groups, *Israel J. Math.* **216**(1) (2016), 107–147.
8. J. Fawcett, *Bases of primitive permutation groups.* PhD thesis, University of Cambridge, 2013.
9. E. Fisman and Z. Arad, A proof of Szep's conjecture on nonsimplicity of certain finite groups, *J. Algebra* **108**(2) (1987), 340–354.
10. M. Giudici, C. H. Li, C. E. Praeger, Á. Seress and V. Trofimov, On minimal subdegrees of finite primitive permutation groups, in *Finite geometries, groups, and computation* (eds A. Hulpke, R. Liebler, T. Penttila and Á. Seress), pp. 75–93 (Walter de Gruyter, Berlin, 2006).
11. I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, Volume 92 (American Mathematical Society, Providence, RI, 2008).
12. E. H. Moore, *The subgroups of the generalized finite modular group*, The Decennial Publications, Volume 9 (University of Chicago Press, 1903).
13. B. H. Neumann, Twisted wreath products of groups, *Arch. Math. (Basel)* **14** (1963), 1–6.
14. P. M. Neumann, Finite permutation groups, edge-coloured graphs and matrices, in *Proc. of the Summer School in Topics in Group Theory and Computation*, University College, Galway, 1973 (ed. M. P. J. Curran), pp. 82–118 (Academic Press, London, 1977).
15. C. E. Praeger, The inclusion problem for finite primitive permutation groups, *Proc. Lond. Math. Soc. (3)* **60**(1) (1990), 68–88.

https://doi.org/10.1017/S0013091519000130 Published online by Cambridge University Press