arXiv:2012.13747v3 [math.GR] 14 Oct 2021

ON VALENCY PROBLEMS OF SAXL GRAPHS

JIYONG CHEN AND HONG YI HUANG

Abstract. Let G be a permutation group on a set Ω and recall that a base for G is a subset of Ω such that its pointwise stabiliser is trivial. In a recent paper, Burness and Giudici introduced the Saxl graph of G, denoted $\Sigma(G)$, with vertex set Ω and two vertices adjacent if and only if they form a base for G. If G is transitive, then $\Sigma(G)$ is vertex-transitive and it is natural to consider its valency (which we refer to as the valency of G). In this paper we present a general method for computing the valency of any finite transitive group and we use it to calculate the exact valency of every primitive group with stabiliser a Frobenius group with cyclic kernel. As an application, we calculate the valency of every almost simple primitive group with an alternating socle and soluble stabiliser and we use this to extend results of Burness and Giudici on almost simple primitive groups with prime-power or odd valency.

1. Introduction

Let G be a finite permutation group on a set Ω. A *base* for G is a subset of Ω such that its pointwise stabiliser is trivial. The *base size* of G, denoted by $b(G)$, is the minimal size of a base for G. This is a classical notion in permutation group theory and bounds on the base sizes of finite permutation groups have been studied since the nineteenth century, finding a wide range of applications. For example, see [1] for details of the relationship between the base sizes of a group and the metric dimension of a graph, and [35, Section 4] for the application of bases in the computational study of finite groups.

In more recent years, there has been significant interest in determining bounds on the base sizes of finite primitive groups, and almost simple groups in particular (recall that a group G is *almost simple* if $T \leqslant G \leqslant \mathrm{Aut}(T)$ for some non-abelian simple group T, which is the socle of G). Some of this interest has been partly motivated by a well known conjecture of Cameron and Kantor [14, 15], which asserts that there is an absolute constant c such that $b(G) \leqslant c$ for every non-standard almost simple primitive group G (we refer the reader to [4] for the definition of a *non-standard* group). This conjecture was proved by Liebeck and Shalev [31] using probabilistic methods and it is now known that $c = 7$ is the optimal constant (in fact, $b(G) = 7$ if and only if G is the Mathieu group M_{24} acting on 24 points); see the sequence of papers [3, 8, 11, 12] by Burness et al. Furthermore, almost simple primitive groups with $b(G) = 6$ have been determined in [4, Theorem 1]. If G is a soluble primitive group, then a theorem of Seress [34] shows that $b(G) \leqslant 4$ and this has very recently been extended by Burness [5], who has established the bound $b(G) \leqslant 5$ for any finite primitive group G with a soluble point stabiliser (in both cases, the bounds are best possible). In addition, [5, Theorem 2] gives the exact base size for every almost simple primitive group with a soluble stabiliser.

There has been a special interest in studying the permutation groups with base size 2. Indeed, a programme of research initiated by Saxl in the 1990s seeks to determine all the primitive groups G with $b(G) = 2$. In [7], Burness and Giudici introduced the *Saxl graph* of a permutation group $G \leqslant \mathrm{Sym}(\Omega)$, denoted by $\Sigma(G)$, as a tool for studying

Date: October 15, 2021.

Key words and phrases. Bases, Saxl Graphs, Valencies, Subdegrees, Primitive Groups.

these groups. Here the vertex set is Ω and two vertices are adjacent if and only if they form a base for G. Recall that an *orbital graph* of G is a graph with vertices Ω and (α, β) is a directed edge if it is contained in a fixed orbital (an orbit of the associated action of G on $\Omega \times \Omega$) of G. Indeed, $\Sigma(G)$ is the union of all regular orbital graphs of G (a regular orbital is an orbital on which G acts regularly). We refer the reader to [7, Lemma 2.1] for the basic properties of $\Sigma(G)$.

Now assume $G \leqslant \mathrm{Sym}(\Omega)$ is a finite transitive group with point stabiliser H, in which case $\Sigma(G)$ is vertex-transitive. Let $\mathrm{val}(G, H)$ be the valency of $\Sigma(G)$ and observe that $\mathrm{val}(G, H) = r|H|$, where r is the number of regular orbits of H on Ω. It is easy to see that if $\mathrm{val}(G, H) > \frac{1}{2}|\Omega|$, then $\Sigma(G)$ is connected with diameter at most 2. The *Burness-Giudici conjecture* from [7] asserts that $\Sigma(G)$ has diameter at most 2 for every finite primitive group G with $b(G) = 2$ and this provides further motivation for investigating $\mathrm{val}(G, H)$ in this paper. We refer the reader to [10, 16, 28] for some recent work on this conjecture.

We will see another application of $\mathrm{val}(G, H)$ in the following remark.

Remark 1. Another motivation for determining $\mathrm{val}(G, H)$ comes from the study of the bases for primitive groups of *product type* (we refer the reader to [30, p.391, III(b)] for the definition of product type groups). For example, let $X \leqslant \mathrm{Sym}(\Gamma)$ be a base-two primitive group with stabiliser Y, and $G = X \wr P$ acting on the Cartesian product $\Omega = \Gamma^k$ with its product action, where $P \leqslant S_k$ is transitive. Then [1, Theorem 2.13] implies that $b(G) = 2$ if and only if $\mathrm{val}(X, Y)/|Y|$ is at least the distinguishing number of P (see also [7, Corollary 2.9]). Here the *distinguishing number* of P is the smallest size of a partition of $\{1, \dots, k\}$ such that only the identity element of P fixes all the parts of the partition. In particular, $b(X \wr S_k) = 2$ if and only if $\mathrm{val}(X, Y) \geqslant k|Y|$ since the distinguishing number of S_k is k.

Recall that a group H is said to be *Frobenius* if there exists a non-trivial proper subgroup $L < H$ such that $L \cap L^h = 1$ for all $h \in H \backslash L$. The subgroup L is called the *Frobenius complement* of H. The *Frobenius kernel* K is the subgroup comprising the identity element and those elements that are not in any conjugate of L. A well known result [18] states that $H = K{:}L$ is a split extension. It is also easy to show that if K is cyclic, then L is also cyclic.

Our first main result gives an explicit formula for $\mathrm{val}(G, H)$ in the case where G is primitive and H is a Frobenius group with cyclic kernel (see Section 4 for the proof). Here, the *Möbius function* μ is the function defined on the set of positive integers such that $\mu(k) = 0$ if k is not square-free, $\mu(k) = -1$ if k is square-free and has an odd number of prime factors, and $\mu(k) = 1$ otherwise.

Theorem 1. *Suppose G is a finite primitive permutation group with point stabiliser H, where $H = K{:}L$ is Frobenius with cyclic kernel K. Write $L = \langle y \rangle$ and let $\pi(L)$ be the set of divisors d of $|L|$ with $d > 1$. Then*

$$\mathrm{val}(G, H) = |G : H| + |K| - 1 + \frac{|K|}{|L|} \sum_{d \in \pi(L)} \mu(d) |N_G(\langle y^{\frac{|L|}{d}} \rangle)|,$$

where μ is the Möbius function.

We refer the reader to Theorem 4.3 for a more general result, which describes all the subdegrees of G and their associated multiplicities.

In order to prove Theorem 1 we introduce a general method in Section 3 for computing subdegrees and their associated multiplicities of a transitive group, which is a generalisation of [20]. To apply this strategy we need to determine all possible cases $H \cap H^g$ for $g \in G$. This leads us to the following problem, which may be of independent interest.

Problem 1. *Determine the primitive permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ such that there exists $\alpha, \beta \in \Omega$ satisfying $1 \neq G_{\alpha\beta} \lhd G_\alpha$.*

The problem was initially stated by Cameron in [13], where he conjectured that there is no primitive permutation group satisfying the condition in Problem 1. It is straightforward to see that there is no affine primitive group satisfying the condition. We refer the reader to Konygin's work [22, 23, 24, 25, 26] on this problem when G is almost simple or an associated product type primitive group. In particular, no example arises in the case when G has soluble point stabilisers (see [22, Proposition 8]). Recently, however, Spiga [36, Theorem 1.4] first found an example satisfying the condition in Problem 1, which is a primitive group of diagonal type (see [36, Section 5] for the construction). We refer the reader to Remarks 3.3 and 3.4 for further remarks to this problem.

Theorem 1 can be applied to various problems. Our first application concerns the almost simple primitive groups with socle an alternating group. Let G be an almost simple primitive group with $\mathrm{soc}(G) = A_n$ and soluble stabiliser H. Note that $\mathrm{val}(G, H) = 0$ if $b(G) > 2$, and those groups with $b(G) = 2$ are classified in [5]. In the following theorem, μ denotes the Möbius function and ϕ denotes the Euler totient function.

Theorem 2. *Let G be an almost simple primitive group with socle A_n and soluble stabiliser H. If $b(G) = 2$, then $(G, H, \mathrm{val}(G, H))$ is listed in Table 1, where*

$$\mathrm{val}(A_p, \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}) = (p-2)! + p - 1 + p \sum_{1 \neq d \mid \frac{p-1}{2}} \mu(d)\phi(d) d^{\frac{p-1}{d}-1} \left(\frac{p-1}{d} - 1\right)! \quad (1)$$

and

$$\mathrm{val}(S_p, \mathrm{AGL}_1(p)) = (p-2)! + p - 1 + p \sum_{1 \neq d \mid (p-1)} \mu(d)\phi(d) d^{\frac{p-1}{d}-1} \left(\frac{p-1}{d} - 1\right)!. \quad (2)$$

G	H	$\mathrm{val}(G,H)$	Conditions
A_5	S_3	6	
M_{10}	$\mathrm{AGL}_1(5)$	20	
M_{10}	8:2	32	
$\mathrm{PGL}_2(9)$	D_{16}	16	
A_9	$\mathrm{ASL}_2(3)$	432	
A_p	$\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$	see (1)	$p > 5$ is a prime, $p \neq 7, 11, 17, 23$
S_p	$\mathrm{AGL}_1(p)$	see (2)	$p > 5$ is a prime

TABLE 1. The cases $(G, H, \mathrm{val}(G, H))$ in Theorem 2

Next we turn to the primitive groups with prime-power valency Saxl graphs. The following result builds on [7, Proposition 3.1], which describes the transitive groups G with $\mathrm{val}(G, H)$ a prime. The proof of the following result, given in Section 6, is based on the classification of almost simple primitive groups with stabiliser of prime-power order (see Proposition 6.3). Recall that the Johnson graph $J(n, k)$ is a graph with vertices the set of k-subsets of an n-element set, and two vertices are adjacent if they contain exactly $(k-1)$ elements in common.

Theorem 3. *Let G be an almost simple primitive group with stabiliser H. Then $\mathrm{val}(G, H)$ is a prime power if and only if one of the following holds:*

(i) $(G, H) = (\mathrm{M}_{10}, 8{:}2)$ *with* $\mathrm{val}(G, H) = 32$.

(ii) $(G,H) = (\mathrm{PGL}_2(q), D_{2(q-1)})$, *where* $q \geqslant 17$ *is a Fermat prime or* $q = 9$, $\Sigma(G)$ *is isomorphic to* $J(q+1,2)$ *and* $\mathrm{val}(G,H) = 2(q-1)$.

Similarly, for groups with odd valency we obtain Theorem 4, which extends [7, Proposition 3.2] (in particular, Theorem 2 above shows that case (iii) in [7, Proposition 3.2] does not arise). The notation for classical groups follows [21], where $\epsilon = +$ or $-$ indicates the linear or unitary case, respectively. For the proof of Theorem 4 we refer the reader to Section 7.

Theorem 4. *Let* G *be an almost simple primitive group with stabiliser* H *and* $b(G) = 2$. *Then* $\mathrm{val}(G,H)$ *is odd only if one of the following holds:*

(i) $G = \mathrm{M}_{23}$ *and* $H = 23{:}11$.

(ii) $G = \mathrm{L}_r^\epsilon(q).O \leqslant \mathrm{P\Gamma L}_r^\epsilon(q)$ *and* $H = \mathbb{Z}_a{:}\mathbb{Z}_r.O$, *where* $a = \frac{q^r-\epsilon}{(q-\epsilon)(r,q-\epsilon)}$, r *is an odd prime and* $O \leqslant \mathrm{Out}(\mathrm{L}_r^\epsilon(q))$ *has odd order. In addition,* G *is not a subgroup of* $\mathrm{PGL}_r^\epsilon(q)$.

However, it is not known if there are any genuine examples satisfying the conditions in part (ii).

Notation. We will denote by ϕ the Euler totient function and we denote the cyclic group of order n by $\mathbb{Z}_n$. By (a,b) we mean the greatest common divisor $\gcd(a,b)$ of two integers a and b. Our notation for classical groups follows [21]. For example, we use $\mathrm{L}_n(q)$ or $\mathrm{L}_n^+(q)$ to denote $\mathrm{PSL}_n(q)$, and sometimes $\mathrm{PGL}_n^+(q)$ and $\mathrm{P\Gamma L}_n^+(q)$ to represent $\mathrm{PGL}_n(q)$ and $\mathrm{P\Gamma L}_n(q)$ respectively. Similarly, for unitary groups we write $\mathrm{U}_n(q)$ or $\mathrm{L}_n^-(q)$ to represent $\mathrm{PSU}_n(q)$ and we also use $\mathrm{PGL}_n^-(q) = \mathrm{PGU}_n(q)$ and $\mathrm{P\Gamma L}_n^-(q) = \mathrm{P\Gamma U}_n(q)$.

Acknowledgements. This work was partially supported by the National Natural Science Foundation of China (Grant No. 11931005) and the Fundamental Research Funds for the Central Universities (Grant No. 20720210036). The second author is supported by China Scholarship Council for his doctoral studies at the University of Bristol.

Both authors thank Tim Burness, Cai Heng Li and Binzhou Xia for their helpful discussions. They deeply thank Southern University of Science and Technology (SUSTech) for their support and hospitality when some of the work on this paper was undertaken. They also thank Derek Holt, Richard Lyons, Geoffrey Robinson and Gabriel Verret for their comments on Problem 1 on MathOverflow (question 372398 posted by the second author).

2. Preliminaries

2.1. Partially ordered sets and Möbius functions.

At the beginning of this section, we prove two useful lemmas concerning the inversion formula on a partially ordered set. Let $(P,\leqslant)$ be a finite partially ordered set.

Lemma 2.1. *Let* c *be a function from* $P\times P$ *to* $\mathbb{C}$, *such that*

$$c(p_1,p_2) = \begin{cases} 1 & \text{if } p_1 = p_2, \\ 0 & \text{if } p_1, p_2 \text{ are not comparable or } p_1 > p_2. \end{cases}$$

Then there is a unique function $d : P\times P \to \mathbb{C}$ *such that*

$$\sum_{p\in P} c(p_1,p)d(p,p_2) = \sum_{p\in P} d(p_1,p)c(p,p_2) = \begin{cases} 1 & \text{if } p_1 = p_2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since $(P, \leqslant)$ is finite, there is a linear extension $(P, \preceq)$ of it. That is, $(P, \preceq)$ is a totally ordered set, and for any $p_1, p_2 \in P$, $p_1 \preceq p_2$ whenever $p_1 \leqslant p_2$. Suppose that $n = |P|$. Label the elements of P by $p_1, p_2, \ldots, p_n$ such that $p_i \preceq p_j$ whenever $i \leqslant j$. Let $C = [c(p_i, p_j)]_{n\times n}$ be the matrix with $c(p_i, p_j)$ being the entry in the i-th row and j-th column. By the hypothesis on c, we have $c(p_i, p_i) = 1$ for $1 \leqslant i \leqslant n$ and $c(p_i, p_j) = 0$ when $n \geqslant i > j \geqslant 1$. It follows that the matrix C is an upper triangular matrix with diagonal entries all equal to 1. In particular, C is invertible. Suppose $D = [d_{ij}]_{n\times n} = C^{-1}$ and let $d(p_i, p_j) = d_{ij}$ be the (i, j)-entry of D. It is obvious that the function d satisfies those equalities listed in this lemma which is uniquely determined by c. □

Lemma 2.2. *Let c, d be two functions as defined in Lemma 2.1. Suppose that $f, g : P \to \mathbb{C}$ are two functions on P such that*

$$f(q) = \sum_{p\in P} c(q, p)g(p)$$

for each $q \in P$. Then for each $p \in P$,

$$g(p) = \sum_{q\in P} d(p, q)f(q).$$

Proof. For any $p \in P$,

$$\begin{aligned}\sum_{q\in P} d(p, q)f(q) &= \sum_{q\in P} d(p, q) \left(\sum_{x\in P} c(q, x)g(x)\right) \\ &= \sum_{x\in P} \left(\sum_{q\in P} d(p, q)c(q, x)g(x)\right) \\ &= \sum_{x\in P} g(x) \left(\sum_{q\in P} d(p, q)c(q, x)\right).\end{aligned}$$

By Lemma 2.1, the only nonzero term on the right side is $g(p)$, which completes the proof. □

Remark 2.3. If we also assume that $c(p_1, p_2) = 1$ for each pair (p_1, p_2) with $p_1 \leqslant p_2$, then c, d are indeed the zeta function and Möbius function on the order-dual $P^{\downarrow}$ of P, respectively. See [27, Sections 1.1 and 3.1] for more details.

2.2. **Frobenius groups with cyclic kernel.** Let $H = K{:}L$ be a Frobenius group with Frobenius kernel K and Frobenius complement L. Then it is well known that $(|K|, |L|) = 1$ (see for example [33, Theorem 12.6.1]). Suppose K is cyclic. We list the following basic and well-known properties of H, which will be useful later. The proof is straightforward and we refer the reader to [33, Section 12.6] for more properties.

Lemma 2.4. *In terms of the above notation, the following holds.*

(i) *The Frobenius complement L is cyclic.*
(ii) *For any non-trivial subgroup B of L, $N_H(B) = L$.*
(iii) *For any non-trivial subgroup B of H with $B \cap K = 1$, there exists a unique $k \in K$ such that $B^k \leqslant L$.*

3. Our Strategy

Throughout this section, we assume G is a transitive permutation group on a set Ω with stabiliser H. Suppose that $H = G_\alpha$ is the stabiliser of the point $\alpha \in \Omega$.

Definition 3.1. The *multiplicity* of a subdegree n, denoted by $m(G, H, n)$, is the number of suborbits of G of length n.

In particular, we have $\mathrm{val}(G, H) = |H| \cdot m(G, H, |H|)$ and $m(G, H, 1) = 1$.

In order to calculate $\mathrm{val}(G, H)$ and the general $m(G, H, n)$, we need to determine the cardinality of the set $\{g \in G \mid G_\alpha \cap G_{\alpha^g} = A\}$ for any subgroup A of H.

3.1. **Basic enumeration.** Write

$$\delta_H^G(A) := \{g \in G \mid G_\alpha \cap G_{\alpha^g} = A\} = \{g \in G \mid H \cap H^g = A\}.$$

If G and H are clear from the context, we will write $\delta_H(A)$ or $\delta(A)$ for short. In particular, $\delta(1)$ is the set of $g \in G$ such that α^g is adjacent to α in $\Sigma(G)$. We have the following observations on $\delta(A)$.

Lemma 3.2. *With the notation above, the following statements hold:*

(i) $G = \bigcup_{A \leqslant H} \delta(A)$;

(ii) $\mathrm{val}(G, H) = \frac{|\delta(1)|}{|H|}$;

(iii) *For any $h \in H$ and any $A \leqslant H$, $\delta(A^h) = \delta(A)h$.*

Proof. Parts (i) and (ii) follow immediately from the definitions. Let $g \in \delta(A^h)$. Then $H \cap H^g = A^h$ and so $H \cap H^{gh^{-1}} = A$. Conversely, if $g \in \delta(A)$ then $H \cap H^{gh} = A^h$, which implies that $gh \in \delta(A^h)$. Hence, part (iii) holds. □

Note that if $A < H$ and $\delta(A)$ is non-empty, then A is an arc stabiliser of some orbital graph of G. In general, however, for a fixed subgroup A of H, it is not easy to determine whether $\delta(A)$ is empty or not. For example, if G is primitive, it is not known if there exists a non-trivial proper normal subgroup A of H such that $\delta(A)$ is non-empty. Indeed, checking the relevant database in Magma [2], we determine that there is no example of such a primitive group with degree at most 4095. This leads us naturally to the following problem (as stated in the introduction).

Problem 1. *Determine the primitive permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ such that there exists $\alpha, \beta \in \Omega$ satisfying $1 \neq G_{\alpha\beta} \lhd G_\alpha$.*

Here are two remarks concerning Problem 1.

Remark 3.3. Write $H \cap H^g$ as the arc stabiliser $G_{(\alpha,\alpha^g)}$ of the orbital graph associated to the orbital (α, α^g) for some $g \notin G_\alpha = H$. Suppose $1 \neq G_{(\alpha,\alpha^g)} \lhd G_\alpha$. If the edge stabiliser $G_{\{\alpha,\alpha^g\}}$ is strictly larger then $G_{(\alpha,\alpha^g)}$ (that is, the orbital is self-paired and the associated orbital graph is undirected), then there exists $x \in G$ such that $\alpha^x = \alpha^g$ and $\alpha^{gx} = \alpha$. This yields $x \in N_G(G_{(\alpha,\alpha^g)}) = G_\alpha$. Hence, $\alpha = \alpha^x = \alpha^g$, a contradiction. This verifies Problem 1 when $G_{(\alpha,\alpha^g)}$ is a proper subgroup of $G_{\{\alpha,\alpha^g\}}$.

Remark 3.4. Suppose $G \leqslant \mathrm{Sym}(\Omega)$ is primitive and $1 \neq G_{\alpha\beta} \lhd G_\alpha$ for some $\alpha, \beta \in \Omega$. Then by [19, Lemmas 2.1 and 2.2], G_α and $G_\alpha/G_{\alpha\beta}$ have the same simple sections (a section is a quotient group of a subgroup). In particular, G_α and $G_\alpha/G_{\alpha\beta}$ have the same solubility and their orders have same prime divisors. There are some other observations on $G_{\alpha\beta}$ if $1 \neq G_{\alpha\beta} \lhd G_\alpha$ given in MathOverflow (Question 372398). For example, Richard Lyons noted that $G_{\alpha\beta}$ must have even order by analysing on the generalised Fitting subgroups.

With also Lemma 3.2(iii) in mind, we pick a subset $\mathcal{I}$ of $\{A \mid A \leqslant H\}$ such that

$$\bigcup_{A \in \mathcal{I}} \{A^h \mid h \in H\} \supseteq \{A \leqslant H \mid \delta(A) \neq \varnothing\}.$$

This is a set of representatives of possible arc stabilisers A up to conjugacy in H.

Lemma 3.5. *We have*

$$m(G,H,n) = \frac{1}{n} \sum_{A\in\mathcal{I},|A|=\frac{|H|}{n}} \frac{|\delta(A)|}{|N_H(A)|}.$$

Proof. First note that A has exactly $|H:N_H(A)|$ distinct conjugates in H. Thus,

$$m(G,H,n) = \frac{1}{n|H|} \sum_{A\leqslant H,|A|=\frac{|H|}{n}} |\delta(A)| = \frac{1}{n|H|} \sum_{A\in\mathcal{I},|A|=\frac{|H|}{n}} |\delta(A)|\cdot|H:N_H(A)|$$

as required. □

To calculate the multiplicities of subdegrees as well as the valency, we need to find a way to calculate $|\delta(A)|$. For this purpose, we define some new sets. Let $\Delta_H^G(A)$ be the set $\{g \in G \mid H \cap H^g \geqslant A\}$. Again, we write $\Delta_H(A)$ or even $\Delta(A)$ for short if G and H are clear from the context.

Lemma 3.6. *Let $\mathcal{S}$ be a set of representatives of the H-conjugacy classes of subgroups of H.*

(i) $\Delta(A) = \bigcup_{A^x\in\mathcal{S}\cap A^G} HN_G(A^x)x^{-1}$*;*
(ii) *if $A^g \leqslant H$ for some $g \in G$, then $\Delta(A^g) = \Delta(A)g$ and*

$$|\Delta(A^g)| = |\Delta(A)| = \sum_{B\in\mathcal{S}\cap A^G} \frac{|H||N_G(B)|}{|N_H(B)|}.$$

Proof. Firstly, we have

$$\begin{aligned}\Delta(A) &= \{g \in G \mid H \cap H^g \geqslant A\} = \{g \in G \mid A^{g^{-1}} \leqslant H\}\\ &= \bigcup_{C\in A^G,\ C\leqslant H} \{g \in G \mid A^{g^{-1}} = C\}\\ &= \bigcup_{B\in\mathcal{S}\cap A^G} \left(\bigcup_{C\in B^H} \{g \in G \mid A^{g^{-1}} = C\} \right).\end{aligned}$$

For any group $B \in \mathcal{S} \cap A^G$, suppose that $B = A^x \leqslant H$ for some $x \in G$. It follows that

$$\begin{aligned}\bigcup_{C\in B^H} \{g \in G \mid A^{g^{-1}} = C\} &= \bigcup_{h\in H} \{g \in G \mid A^{g^{-1}} = A^{xh}\}\\ &= \bigcup_{h\in H} h^{-1}x^{-1}N_G(A)\\ &= Hx^{-1}N_G(A)\\ &= HN_G(B)x^{-1}.\end{aligned}$$

This gives part (i). Combining the above equations, we obtain that

$$\begin{aligned}|\Delta(A)| &= \sum_{B\in\mathcal{S}\cap A^G} \left| \bigcup_{C\in B^H} \{g \in G \mid A^{g^{-1}} = C\} \right|\\ &= \sum_{B\in\mathcal{S}\cap A^G} |HN_G(B)|.\\ &= \sum_{B\in\mathcal{S}\cap A^G} \frac{|H||N_G(B)|}{|N_H(B)|}.\end{aligned}$$

Note that the right-hand-side remains unchanged if we replace A by $A^g \leqslant H$ for some $g \in G$. This completes the proof. □

By the virtue of Lemma 3.6, $|\Delta(A)|$ can be easily calculated if both normalisers in G and H are known for each subgroup of H. Note that

$$\Delta(A) = \bigcup_{B \geqslant A} \delta(B)$$

is a disjoint union and so

$$|\Delta(A)| = \sum_{B \geqslant A} |\delta(B)|.$$

Now, let $P = (\{A \mid A \leqslant H\}, \leqslant)$ be the partially ordered set on all subgroups of H with the natural inclusion relation. Let $c : P \times P \to \mathbb{C}$ be a function on $P \times P$ such that

$$c(A, B) = \begin{cases} 1 & \text{if } A \leqslant B; \\ 0 & \text{otherwise.} \end{cases}$$

It is obvious that c satisfies the hypothesis in Lemmas 2.1 and 2.2. This implies that

$$|\Delta(A)| = \sum_{B \in P} c(A, B)|\delta(B)| \tag{3}$$

and

$$|\delta(B)| = \sum_{A \in P} \mu_{P^{\downarrow}}(B, A)|\Delta(A)|,$$

where $\mu_{P^{\downarrow}}$ is the Möbius function on the dual partially ordered set $P^{\downarrow}$. This provides a way to compute $|\delta(A)|$ for any subgroup $A \leqslant H$.

3.2. **Reduction.** In the rest of this section, we aim to reduce the size of the partially ordered set P in the calculation of $|\delta(A)|$. By Lemma 3.2(iii), subgroups in the same conjugacy class in H give same cardinalities of $\delta(A)$ and $\Delta(A)$. Hence, it is natural to consider the partially ordered set on the set $\mathcal{I}$. It is easy to make $\mathcal{I}$ into a partially ordered set by defining $A \preceq B$ in $\mathcal{I}$ if there exists an element $h \in H$ such that $A \leqslant B^h$.

Lemma 3.7. *With the notation above, we have the following statements.*

(i) *If η is a function defined on $\mathcal{I} \times \mathcal{I}$ such that $\eta(A, B) = |\{D \in B^H \mid D \geqslant A\}|$, then*

$$|\Delta(A)| = \sum_{B \in \mathcal{I}} \eta(A, B)|\delta(B)|. \tag{4}$$

(ii) *There exists a function $\mu_\eta : \mathcal{I} \times \mathcal{I} \to \mathbb{C}$, such that for each $B \in \mathcal{I}$,*

$$|\delta(B)| = \sum_{A \in \mathcal{I}} \mu_\eta(B, A)|\Delta(A)|.$$

Proof. By (3),

$$\begin{aligned}
|\Delta(A)| &= \sum_{B \in P} c(A, B)|\delta(B)| \\
&= \sum_{B \in \mathcal{I}} \left(\sum_{C \in B^H} c(A, C)|\delta(C)| \right) \\
&= \sum_{B \in \mathcal{I}} \left(\sum_{C \in B^H} c(A, C)|\delta(B)| \right) \\
&= \sum_{B \in \mathcal{I}} \left(\sum_{C \in B^H, C \geqslant A} 1 \right) |\delta(B)| \\
&= \sum_{B \in \mathcal{I}} |\{B^h \mid B^h \geqslant A\}| \cdot |\delta(B)|.
\end{aligned}$$

Thus, part (i) holds. Now, by applying Lemma 2.2, part (ii) holds. □

By Lemma 3.6(ii), $|\Delta(A)| = |\Delta(B)|$ if A and B two subgroups of H which are conjugate in G. Note that A, B are not necessarily conjugate in H. In most cases, however, we still have $|\delta(A)| = |\delta(B)|$, which would simplify (4). To do this, we define $A \sim B$ for $A, B \in \mathcal{I}$ if the following conditions hold (here we adopt the notation of Lemma 3.7):

(E1) $B = A^g$ for some $g \in G$;
(E2) $|N_H(A)| = |N_H(B)|$;
(E3) for any $C \in \mathcal{I} \backslash \{A, B\}$, $\eta(A, C) = \eta(B, C)$ and $\eta(C, A) = \eta(C, B)$.

It is easy to see that $\sim$ is an equivalence relation on $\mathcal{I}$.

Lemma 3.8. *With the notation above, if $A \sim B \in \mathcal{I}$, we have $|\delta(A)| = |\delta(B)|$.*

Proof. Suppose that $\mathcal{I} = \{C_1, C_2, \ldots, C_n\}$, where $A = C_1$ and $B = C_2$, and set $M = [\eta(C_i, C_j)]_{n \times n}$. By the proof of Lemma 2.1, $M^{-1} = [\mu_\eta(C_i, C_j)]_{n \times n}$. Let

$$J = \begin{bmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 1 & 0 & \ldots & 0 \\ & & 0 & 1 & \ldots & 0 \\ & & \vdots & \vdots & \ddots & \vdots \\ & & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

be a permutation matrix. As $A \sim B$, by the definition of $\sim$ we have $J^{-1}MJ = M$ from a straightforward matrix calculation. It follows that $J^{-1}M^{-1}J = M^{-1}$. By Lemma 3.6(ii), we have $|\Delta(C_1)| = |\Delta(A)| = |\Delta(B)| = |\Delta(C_2)|$, which implies

$$\begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} = \begin{bmatrix} |\Delta(C_2)| \\ |\Delta(C_1)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} = J \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix}.$$

Thus,

$$\begin{aligned} \begin{bmatrix} |\delta(C_1)| \\ |\delta(C_2)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix} &= M^{-1} \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} = J^{-1}M^{-1}J \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} \\ &= J^{-1}M^{-1} \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} = J^{-1} \begin{bmatrix} |\delta(C_1)| \\ |\delta(C_2)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix} = \begin{bmatrix} |\delta(C_2)| \\ |\delta(C_1)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix}. \end{aligned}$$

This gives $|\delta(A)| = |\delta(C_1)| = |\delta(C_2)| = |\delta(B)|$. □

Suppose $\tilde{\mathcal{I}}$ is a set of equivalence class representatives of $\mathcal{I}$ with respect to $\sim$. For any subgroup $A \in \mathcal{I}$, let $\tilde{A} = \{B \in \mathcal{I} \mid B \sim A\}$ be the equivalence class containing A.

Lemma 3.9. *We have*

$$m(G, H, n) = \frac{1}{n} \sum_{A \in \tilde{\mathcal{I}}, |A| = \frac{|H|}{n}} \frac{|\delta(A)| \cdot |\tilde{A}|}{|N_H(A)|}.$$

Proof. This is directly given by Lemma 3.5 and the definition of $\sim$. □

Here is a corresponding lemma to Lemma 3.7, which is the main technique we use to determine the valency as well as the multiplicities of subdegrees.

Lemma 3.10. *The following statements hold.*

(i) *If $\tilde{\eta}$ is a function defined on $\tilde{\mathcal{I}} \times \tilde{\mathcal{I}}$ such that*

$$\tilde{\eta}(A, B) = \sum_{C \in \tilde{B}} \eta(A, C),$$

then

$$|\Delta(A)| = \sum_{B \in \tilde{\mathcal{I}}} \tilde{\eta}(A, B)|\delta(B)|$$

and

$$\tilde{\eta}(A, B) = \begin{cases} 1 & \text{if } A = B; \\ \eta(A, B)|\tilde{B}| & \text{otherwise.} \end{cases}$$

(ii) *There exists a function $\mu_{\tilde{\eta}} : \tilde{\mathcal{I}} \times \tilde{\mathcal{I}} \to \mathbb{C}$, such that for each $B \in \tilde{\mathcal{I}}$,*

$$|\delta(B)| = \sum_{A \in \tilde{\mathcal{I}}} \mu_{\tilde{\eta}}(B, A)|\Delta(A)|.$$

Proof. By (4),

$$\begin{aligned} |\Delta(A)| &= \sum_{B \in \mathcal{I}} \eta(A, B)|\delta(B)| \\ &= \sum_{B \in \tilde{\mathcal{I}}} \left(\sum_{C \in \tilde{B}} \eta(A, C)|\delta(C)| \right) \\ &= \sum_{B \in \tilde{\mathcal{I}}} \left(\sum_{C \in \tilde{B}} \eta(A, C) \right) |\delta(B)| \\ &= \sum_{B \in \tilde{\mathcal{I}}} \tilde{\eta}(A, B)|\delta(B)|. \end{aligned}$$

If $A = B$, then

$$\tilde{\eta}(A, A) = \sum_{C \in \tilde{A}} \eta(A, C) = |\{C^h \mid C^h \geqslant A \text{ and } C \sim A\}| = 1.$$

If $A \neq B \in \tilde{\mathcal{I}}$, then

$$\tilde{\eta}(A, B) = \sum_{C \in \tilde{B}} \eta(A, C) = \sum_{C \in \tilde{B}} \eta(A, B) = \eta(A, B)|\tilde{B}|.$$

Thus, part (i) holds. Now, by Lemma 2.2, part (ii) holds. □

Remark 3.11. Suppose $\mathcal{I}$ is the set of subgroups A of H (up to conjugacy in H) such that $\delta(A)$ is non-empty. We can make the corresponding set $\tilde{\mathcal{I}}$ into a partially ordered set $(\tilde{\mathcal{I}}, \preccurlyeq)$ by defining $A \preccurlyeq B$ if and only if $\tilde{\eta}(A, B) > 0$. Then by Szpilrajn's lemma, which asserts that every finite partial order is contained in a total order (see [27, Lemma 1.2.1]), $\tilde{\mathcal{I}}$ can be written as $\{C_1, \ldots, C_n\}$ such that $i \leqslant j$ whenever $C_i \preccurlyeq C_j$. Define an $n \times n$ matrix $M = [\tilde{\eta}(C_i, C_j)]_{n \times n}$. It follows that M is an upper-triangular matrix with diagonal entries all being 1. Now Lemma 2.2 applies, making $M^{-1} = [\mu_{\tilde{\eta}}(C_i, C_j)]_{n \times n}$

and $\mu_{\tilde{\eta}}$ is unique. In the language of matrices, the above equations are exactly

$$\Delta := \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix} = M \begin{bmatrix} |\delta(C_1)| \\ |\delta(C_2)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix}$$
$$= \begin{bmatrix} \tilde{\eta}(C_1, C_1) & \tilde{\eta}(C_1, C_2) & \cdots & \tilde{\eta}(C_1, C_n) \\ \tilde{\eta}(C_2, C_1) & \tilde{\eta}(C_2, C_2) & \cdots & \tilde{\eta}(C_2, C_n) \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{\eta}(C_n, C_1) & \tilde{\eta}(C_n, C_2) & \cdots & \tilde{\eta}(C_n, C_n) \end{bmatrix} \begin{bmatrix} |\delta(C_1)| \\ |\delta(C_2)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix}$$

and

$$\delta := \begin{bmatrix} |\delta(C_1)| \\ |\delta(C_2)| \\ \vdots \\ |\delta(C_n)| \end{bmatrix} = M^{-1} \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix}$$
$$= \begin{bmatrix} \mu_{\tilde{\eta}}(C_1, C_1) & \mu_{\tilde{\eta}}(C_1, C_2) & \cdots & \mu_{\tilde{\eta}}(C_1, C_n) \\ \mu_{\tilde{\eta}}(C_2, C_1) & \mu_{\tilde{\eta}}(C_2, C_2) & \cdots & \mu_{\tilde{\eta}}(C_2, C_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{\tilde{\eta}}(C_n, C_1) & \mu_{\tilde{\eta}}(C_n, C_2) & \cdots & \mu_{\tilde{\eta}}(C_n, C_n) \end{bmatrix} \begin{bmatrix} |\Delta(C_1)| \\ |\Delta(C_2)| \\ \vdots \\ |\Delta(C_n)| \end{bmatrix},$$

where both M and M^{-1} are upper-triangular with diagonal entries all equal to 1. Therefore, to calculate $|\delta(C_1)| = |\delta(1)| = |H| \cdot \mathrm{val}(G, H)$ and the multiplicity of each subdegree, it suffices to determine the matrix M and all the values $|\Delta(C_i)|$. We will adopt the notation introduced in this remark later in the text.

Example 3.12. Let $G = \mathrm{PGL}_3(7)$ be a primitive group with stabiliser $H = \langle x \rangle \times (\langle y \rangle{:}\langle \sigma \rangle) \cong \mathbb{Z}_3 \times (\mathbb{Z}_{19}{:}\mathbb{Z}_3)$. In this case, the only possible arc stabilisers up to conjugacy in H are

$$\mathcal{I} = \{1, \langle \sigma \rangle, \langle x\sigma \rangle, \langle x^2\sigma \rangle, \langle x, \sigma \rangle, H\},$$

in which $\langle x\sigma \rangle$ and $\langle x^2\sigma \rangle$ are conjugate in G. In particular, it is not hard to see that $\langle x\sigma \rangle \sim \langle x^2\sigma \rangle$ by checking conditions (E1)-(E3) and so we have

$$\tilde{\mathcal{I}} = \{1, \langle \sigma \rangle, \langle x\sigma \rangle, \langle x, \sigma \rangle, H\}.$$

The matrix M in Remark 3.11 in this case is

$$M = \begin{bmatrix} 1 & 19 & 38 & 19 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Moreover, we have $\mathcal{S} \cap \langle x\sigma \rangle^G = \{\langle x \rangle, \langle x\sigma \rangle, \langle x^2\sigma \rangle\}$, while $\mathcal{S} \cap A^G = \{A\}$ for any other elements A in $\tilde{\mathcal{I}}$ here. This gives, by applying Lemma 3.6, that

$$\Delta = \begin{bmatrix} |\Delta(1)| \\ |\Delta(\langle \sigma \rangle)| \\ |\Delta(\langle x\sigma \rangle)| \\ |\Delta(\langle x, \sigma \rangle)| \\ |\Delta(H)| \end{bmatrix} = \begin{bmatrix} 5630688 \\ 4104 \\ 6669 \\ 513 \\ 171 \end{bmatrix}.$$

For more details about computing the order of normalisers in a more general setting, one can refer to Corollary 7.4 and Lemma 7.5 (see Section 7). Finally, we have

$$\delta = M^{-1}\Delta = \begin{bmatrix} 5321862 \\ 3591 \\ 6156 \\ 342 \\ 171 \end{bmatrix}.$$

It follows that $\mathrm{val}(G, H) = 5321862/171 = 31122$ by Lemma 3.2. Other multiplicities of subdegrees can be also obtained by applying Lemma 3.9. We refer the reader to Proposition 7.8 for a general statement.

4. Proof of Theorem 1

In this section, we assume G is a primitive permutation group with stabiliser H, and $H = K{:}L$ is a Frobenius group with a cyclic Frobenius kernel K. We aim to determine $\tilde{\mathcal{I}}$ and $\mathrm{val}(G, H)$ in this situation.

As G is a primitive permutation group with stabiliser H, it is well known that H is maximal and core-free in G. The next lemma records some further properties.

Lemma 4.1. *The following statements hold.*

(i) *For any non-trivial subgroup A of K, $N_G(A) = H$.*
(ii) *For any $g \in G$, if $H \cap H^g \leqslant K$ then $H \cap H^g = 1$.*
(iii) *For any proper subgroup M of H with $M \cap K \neq 1$, $\{g \in G \mid M \leqslant H^g\} = H$.*

Proof. (i) Firstly A is a characteristic subgroup of K and $K \lhd H$. This implies $A \lhd H$ and so $N_G(A) \geqslant H$. On the other hand, A is not normal in G because H is core-free. It follows that $N_G(A) = H$ since H is maximal in G.

(ii) If $1 \neq H \cap H^g \leqslant K$ then $g \in N_G(H \cap H^g) = H$ because $H \cap H^g$ is the only subgroup in H with this order. This makes $H \cap H^g = H$, a contradiction.

(iii) It is straightforward to see that every $g \in H$ makes $M \leqslant H^g = H$. If $g \notin H$ satisfies the above, then $1 \neq M \cap K \leqslant M \leqslant H \cap H^g$, a contradiction to (ii). □

Suppose that A is a proper non-trivial subgroup of H. If $A \cap K \neq 1$, then by Lemma 4.1(iii), $\delta_H(A) = \varnothing$. If $A \cap K = 1$, then by Lemma 2.4(iii), there exists $k \in K$ such that $A^k \leqslant L$. Hence, without loss of generality, we set the representatives in $\tilde{\mathcal{I}}$ to be conjugates of subgroups of L together with H. Thus,

$$\mathrm{val}(G, H) = |G : H| - 1 - \frac{1}{|L|} \sum_{1 \neq A \leqslant L} |\delta_H(A)|.$$

It suffices to calculate $|\delta_H(A)|$ for $1 \neq A \leqslant L$, and we can reduce our calculation to the conjugates in L.

Lemma 4.2. *If $1 < A < L$, then*

$$|\delta_H(A)| = |K| \cdot |\delta_L(A)|,$$

while

$$|\delta_H(L)| = |K| \cdot (|\delta_L(L)| - |L|).$$

Proof. For any $1 < A \leqslant L$, by Lemma 2.4(iii),

$$\begin{aligned}|\delta_H(A)| &= \left|\bigcup_{k\in K}\{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L^k\}\right| \\ &= \sum_{k\in K} |\{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L^k\}| \\ &= \sum_{k\in K} |k\{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}| \\ &= |K| \cdot |\{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}|.\end{aligned} \tag{5}$$

Suppose that $1 < A < L$. For any $x \in \delta_L(A)$, it is easy to see that $x \notin H$ and $A^{x^{-1}} < L$. Set $B = H \cap H^x \geqslant L \cap L^x = A > 1$. Since $B \in \tilde{\mathcal{I}}$, $B \cap K = 1$. By Lemma 2.4(iii), there exists a unique $k \in K$ such that $A^k \leqslant B^k \leqslant L$. Note that $A \leqslant L$. By the uniqueness of k, we have $k = 1$ and $B \leqslant L$. Similarly, we have $A^{x^{-1}} \leqslant B^{x^{-1}} \leqslant L$. Therefore $B \leqslant L \cap L^x = A$, and $x \in \{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}$. Conversely, for any $y \in \{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}$, we have $A \leqslant L^y$. Moreover, $A \leqslant L \cap L^y \leqslant H \cap H^y = A$. This implies that $y \in \delta_L(A)$. Thus, $\delta_L(A) = \{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}$. Applying this equality to (5) we conclude that

$$|\delta_H(A)| = |K| \cdot |\{g \in G \mid H \cap H^g = A, A^{g^{-1}} \leqslant L\}| = |K| \cdot |\delta_L(A)|.$$

Now, suppose that $A = L$. Then

$$\begin{aligned}\{g \in G \mid H \cap H^g = L, L^{g^{-1}} \leqslant L\} =& \{g \in G \mid H \cap H^g = L\} \cap \{g \in G \mid L^{g^{-1}} \leqslant L\} \\ =& N_G(L) \cap \{g \in G \mid H \cap H^g = L\} \\ =& N_G(L)\backslash H \\ =& N_G(L)\backslash L \\ =& \delta_L(L)\backslash L.\end{aligned}$$

Applying this equality to (5) we get

$$|\delta_H(L)| = |K| \cdot |\delta_L(L)\backslash L| = |K| \cdot (|\delta_L(L)| - |L|).$$

This completes the proof. $\square$

Write $L = \langle y\rangle$. Let d be a proper divisor of $|L|$. For any $x \in N_G(\langle y^d\rangle)$, it is obvious that $x \in \Delta_L(\langle y^d\rangle)$. Conversely, for any $x \in \Delta_L(\langle y^d\rangle)$, notice that $\langle y^d\rangle$ is the unique subgroup of index d both in L and L^x, $x \in N_G(\langle y^d\rangle)$. It follows that

$$|N_G(\langle y^d\rangle)| = |\Delta_L(\langle y^d\rangle)| = \sum_{e|d} |\delta_L(\langle y^e\rangle)|.$$

It follows by the Möbius inversion formula that

$$|\delta_L(\langle y^d\rangle)| = \sum_{e|d} \mu(e)|N_G(\langle y^{\frac{d}{e}}\rangle)|.$$

Indeed, the function $\mu_{\tilde{\eta}}$ in Lemma 3.10 is exactly the Möbius function on integers in this case.

Considering the number of suborbits of length $d|K|$, it is easy to see that

$$|H| \cdot d|K| \cdot m\,(G, H, d|K|) = \left|\left\{g \in G \mid |H \cap H^g| = \frac{|L|}{d}\right\}\right|.$$

By Lemma 2.4(iii),

$$
\begin{aligned}
m\left(G, H, d|K|\right) &= \frac{1}{d|H|\cdot|K|}\left|\left\{g \in G \mid |H \cap H^g| = \frac{|L|}{d}\right\}\right| \\
&= \frac{1}{d|H|}\left|\{g \in G \mid H \cap H^g = \langle y^d\rangle\}\right| \\
&= \frac{1}{d|H|}\left|\delta_H(\langle y^d\rangle)\right| \\
&= \begin{cases} \frac{1}{d|L|}\left|\delta_L(\langle y^d\rangle)\right| & 1 < d < |L| \\ \frac{1}{|L|}(|\delta_L(L)| - |L|) & d = 1 \end{cases} \\
&= \begin{cases} \frac{1}{d|L|}\sum_{e|d}\mu(e)|N_G(\langle y^{\frac{d}{e}}\rangle)| & 1 < d < |L| \\ \frac{1}{|L|}(|N_G(L)| - |L|) & d = 1. \end{cases}
\end{aligned}
\tag{6}
$$

Now, we are ready to compute $\mathrm{val}(G, H)$. Firstly,

$$
\begin{aligned}
\mathrm{val}(G, H) &= |G : H| - 1 - \frac{1}{|L|}\sum_{1<A\leqslant L}|\delta_H(A)| \\
&= |G : H| - 1 - \frac{|K|}{|L|}\cdot(|\delta_L(L)| - |L|) - \frac{|K|}{|L|}\sum_{1<A<L}|\delta_L(A)| \\
&= |G : H| - 1 - \frac{|K|}{|L|}\cdot\left(-|L| + \sum_{1<A\leqslant L}|\delta_L(A)|\right) \\
&= |G : H| + |K| - 1 - \frac{|K|}{|L|}\sum_{1<A\leqslant L}|\delta_L(A)|.
\end{aligned}
\tag{7}
$$

Moreover,

$$
\begin{aligned}
\sum_{1<A\leqslant L}|\delta_L(A)| &= \sum_{d||L|, d\neq|L|}|\delta_L(\langle y^d\rangle)| \\
&= \sum_{d||L|, d\neq|L|}\sum_{e|d}\mu(e)|N_G(\langle y^{\frac{d}{e}}\rangle)| \\
&= \sum_{e||L|, e\neq|L|}\left(\sum_{\frac{d}{e}|\frac{|L|}{e}, \frac{d}{e}\neq\frac{|L|}{e}}\mu\left(\frac{d}{e}\right)\right)|N_G(\langle y^e\rangle)| \\
&= -\sum_{e||L|, e\neq|L|}\mu\left(\frac{|L|}{e}\right)|N_G(\langle y^e\rangle)| \\
&= -\sum_{1\neq e||L|}\mu(e)|N_G(\langle y^{\frac{|L|}{e}}\rangle)|.
\end{aligned}
\tag{8}
$$

To summarise (6), (7) and (8) we have the following theorem.

Theorem 4.3. *Suppose G is a primitive permutation group with stabiliser H, where $H = K{:}L$ is Frobenius with cyclic kernel K. Then*

$$
\mathrm{val}(G, H) = |G : H| + |K| - 1 + \frac{|K|}{|L|}\sum_{1\neq d||L|}\mu(d)|N_G(\langle y^{\frac{|L|}{d}}\rangle)|,
$$

where $L = \langle y \rangle$ and μ is the Möbius function. Moreover, all the other non-trivial subdegrees are $d|K|$ for proper divisors d of $|L|$, with multiplicities

$$m\left(G,H,d|K|\right)=\begin{cases}\frac{1}{d|L|}\sum_{e|d}\mu(e)|N_G(\langle y^{\frac{d}{e}}\rangle)| & 1<d<|L|\\ \frac{1}{|L|}(|N_G(L)|-|L|) & d=1.\end{cases}$$

5. Alternating and Symmetric Groups

Let G be an almost simple primitive group with stabiliser H. If we have $b(G) = 2$, $\mathrm{soc}(G) = A_n$ and H is soluble, then by [5, 29], (G, H) is exactly one of the pairs given in Table 1. Our aim is to calculate $\mathrm{val}(G, H)$ for each pair listed in Table 1.

There are only two infinite families in Table 1, both of which have a Frobenius stabiliser with cyclic kernel. Hence, Theorem 4.3 can be directly applied. Other valencies in Table 1 can be easily calculated by Magma.

5.1. $G = S_p$ **and** $H = \mathrm{AGL}_1(p)$**.** In this case, $K \cong \mathbb{Z}_p$ and $L = \langle y\rangle \cong \mathbb{Z}_{p-1}$ with y a $(p-1)$-cycle in S_p. Then $y^{\frac{|L|}{d}}$ is a product of $\frac{p-1}{d}$ disjoint d-cycles. We have

$$|N_G(\langle y^{\frac{|L|}{d}}\rangle)|=\phi(d)|C_G(\langle y^{\frac{|L|}{d}}\rangle)|=\phi(d)|\mathbb{Z}_d\wr S_{\frac{p-1}{d}}|=\phi(d)d^{\frac{p-1}{d}}\left(\frac{p-1}{d}\right)!.$$

Therefore, by Theorem 4.3, we have

$$\begin{aligned}\mathrm{val}(S_p,\mathrm{AGL}_1(p))&=\mathrm{val}(G,H)\\&=|G:H|+|K|-1+\frac{|K|}{|L|}\sum_{1\neq d||L|}\mu(d)|N_G(\langle y^{\frac{|L|}{d}}\rangle)|\\&=(p-2)!+p-1+p\sum_{1\neq d|(p-1)}\mu(d)\phi(d)d^{\frac{p-1}{d}-1}\left(\frac{p-1}{d}-1\right)!,\end{aligned}$$

which is exactly (2), and also

$$m(G,H,dp)=\begin{cases}\frac{1}{d(p-1)}\sum_{e|d}\mu(e)\phi(\frac{(p-1)e}{d})\cdot(\frac{(p-1)e}{d})^{\frac{d}{e}}\cdot(\frac{d}{e})! & 1<d<p-1\\ \phi(p-1)-1 & d=1\end{cases}$$

for proper divisors d of $p-1$.

5.2. $G = A_p$ **and** $H = \mathrm{AGL}_1(p)\cap A_p$**.** In this case, $K \cong \mathbb{Z}_p$ and $L = \langle y\rangle \cong \mathbb{Z}_{\frac{p-1}{2}}$ with y a product of two disjoint $\frac{p-1}{2}$-cycles. Then $y^{\frac{|L|}{d}}$ is a product of $\frac{p-1}{d}$ disjoint d-cycles. We have

$$|N_G(\langle y^{\frac{|L|}{d}}\rangle)|=\phi(d)|C_G(\langle y^{\frac{|L|}{d}}\rangle)|=\phi(d)|\mathbb{Z}_d\wr S_{\frac{p-1}{d}}\cap A_p|=\frac{1}{2}\phi(d)d^{\frac{p-1}{d}}\left(\frac{p-1}{d}\right)!.$$

Again by Theorem 4.3, we have

$$\begin{aligned}\mathrm{val}(A_p,\mathrm{AGL}_1(p)\cap A_p)&=\mathrm{val}(G,H)\\&=|G:H|+|K|-1+\frac{|K|}{|L|}\sum_{1\neq d||L|}\mu(d)|N_G(\langle y^{\frac{|L|}{d}}\rangle)|\\&=(p-2)!+p-1+p\sum_{1\neq d|\frac{p-1}{2}}\mu(d)\phi(d)d^{\frac{p-1}{d}-1}\left(\frac{p-1}{d}-1\right)!,\end{aligned}$$

which meets (1), and also

$$m(G,H,dp)=\begin{cases}\frac{1}{d(p-1)}\sum_{e\mid d}\mu(e)\phi(\frac{(p-1)e}{2d})\cdot(\frac{(p-1)e}{2d})^{\frac{2d}{e}}\cdot(\frac{2d}{e})! & 1<d<\frac{p-1}{2}\\ \phi(\frac{p-1}{2})\cdot\frac{p-1}{2}-1 & d=1\end{cases}$$

for proper divisors d of $\frac{p-1}{2}$.

6. Prime-power Valencies

Let G be an almost simple primitive group with stabiliser H. If $\mathrm{val}(G,H)$ is a prime-power, then so is $|H|$ and hence H is soluble. The possibilities for (G,H) given in [29] are presented in Table 2. In the table we use the same notation as in [29], where $G_0 \lhd G$ is minimal such that $H_0 := H \cap G_0$ is maximal in G_0 and $H = H_0.(G/G_0)$.

G_0	H_0	Conditions
$\mathrm{L}_2(q)$	$D_{2(q-1)/(2,q-1)}$	$q \neq 5,7,9,11$
	$D_{2(q+1)/(2,q-1)}$	$q \neq 7,9$
$\mathrm{PGL}_2(7)$	D_{16}	
$\mathrm{PGL}_2(9)$	D_{16}	
$\mathrm{L}_2(9).2 \cong \mathrm{M}_{10}$	$8{:}2$	
$\mathrm{L}_r^{\epsilon}(q)$	$\mathbb{Z}_a{:}\mathbb{Z}_r$	$r \geqslant 3$ prime, $a=\frac{q^r-\epsilon}{(q-\epsilon)(r,q-\epsilon)}$, $G_0 \neq \mathrm{U}_3(3),\mathrm{U}_5(2)$

Table 2. Possible cases of almost simple primitive group G with a maximal subgroup H of prime-power order

Easy applications of Catalan's conjecture (now a theorem proved in [32]) and Zsigmondy's theorem (see [37]) allow us to eliminate some possibilities in Table 2. We record the two theorems below.

Theorem 6.1 (Catalan's conjecture)**.** *The only solution in the natural numbers to*

$$x^a - y^b = 1$$

for $a,b>1$, $x,y>0$ is $(a,b,x,y)=(2,3,3,2)$.

Theorem 6.2 (Zsigmondy)**.** *Let $n>1$, $a>1$ and b be positive integers such that $(a,b)=1$, and $\epsilon=\pm1$. There exists a prime divisor p of an $a^n-\epsilon b^n$ such that p does not divide $a^j-\epsilon b^j$ for all j with $0<j<n$, except exactly in the following cases:*

(i) *$\epsilon=1$, $n=2$, $a+b=2^s$ for some $s\geqslant 2$;*
(ii) *$(\epsilon,n,a,b)=(1,6,2,1)$;*
(iii) *$(\epsilon,n,a,b)=(-1,3,2,1)$.*

In the following proposition, we eliminate some of the possibilities in Table 2 and we classify the almost simple primitive groups with point stabilisers of prime-power order.

Proposition 6.3. *Let G be an almost simple primitive group with stabiliser H. If $|H|$ is a prime power, then H is a 2-group and (G,H) is listed in Table 3.*

Proof. First observe that if $|H|$ is a prime power then so is $|H_0|$. In the first and the second cases in Table 2, we need $q-1$ and $q+1$ to be a prime power, respectively, and thus a power of 2 since H_0 is dihedral. Hence, q is odd, and then Theorem 6.1 can be applied so that q must be a prime of the form $q=2^f\pm1$ for some f (note that $q\neq 9$). Thus, q is a Fermat and a Mersenne prime, respectively. This (together with the case when $(G,H)=(\mathrm{PGL}_2(7),D_{16})$) gives the first four rows in Table 3.

In the last case in Table 2, both a and r are odd. By Theorem 6.2, there exists a prime divisor s of $q^r-\epsilon$ such that s does not divide $q-\epsilon$, except when $(r,q,\epsilon)=(3,2,-1)$,

G	H	Conditions
$\mathrm{L}_2(p)$	D_{p-1}	$p \geqslant 17$ is a Fermat prime
	D_{p+1}	$p \geqslant 31$ is a Mersenne prime
$\mathrm{PGL}_2(p)$	$D_{2(p-1)}$	$p \geqslant 17$ is a Fermat prime
	$D_{2(p+1)}$	$p \geqslant 7$ is a Mersenne prime
$\mathrm{PGL}_2(9)$	D_{16}	
M_{10}	$8{:}2$	
$\mathrm{P\Gamma L}_2(9)$	$8{:}2^2$	

TABLE 3. Almost simple groups G with a maximal subgroup H of prime-power order

in which case G is not almost simple and we do not need to consider it. It follows that s divides ar, and hence $s = r$ because we need ar to be a prime power. However, $q \equiv q^r \equiv \epsilon \pmod r$ gives that $s = r$ divides $q-\epsilon$, leading to a contradiction. Therefore, the last row in Table 2 does not arise. □

Now we calculate the possible cases one by one to prove Theorem 3.

Proposition 6.4. *Let $G = \mathrm{PSL}_2(q)$ with $q \geqslant 13$ odd, and $H \cong D_{q-1}$ a maximal subgroup of G. Then*

$$\mathrm{val}(G,H) = \begin{cases} \frac{1}{4}(q-1)(q+7) & q \equiv 1 \pmod 4 \\ \frac{1}{4}(q-1)(q+5) & q \equiv 3 \pmod 4). \end{cases}$$

Proof. This is given in the proof of [5, Lemma 4.7]. Here we give another proof using the strategy introduced in Section 3.

Note that if $q \equiv 3 \pmod 4$ then Theorem 1 can be directly applied. Thus, we only need to consider the case when $q \equiv 1 \pmod 4$. Observe that the only possible cases for $H \cap H^g$ up to isomorphism are 1, $\mathbb{Z}_2$, $\mathbb{Z}_2^2$ or H, and all involutions in G are conjugate. Write $H = \langle x \rangle{:}\langle y \rangle$.

First suppose $q \equiv 5 \pmod 8$. In this case all subgroups of H that are isomorphic to $\mathbb{Z}_2^2$ are conjugate in H. This implies $\tilde{\mathcal{I}}$ can be chosen as

$$\tilde{\mathcal{I}} = \{1, \langle y \rangle, \langle x^{\frac{q-1}{4}}, y \rangle, H\},$$

which gives the matrix

$$M = \begin{bmatrix} 1 & \frac{q-1}{2} & \frac{q-1}{4} & 1 \\ & 1 & 1 & 1 \\ & & 1 & 1 \\ & & & 1 \end{bmatrix},$$

where the missing entries are zero (and similarly for the matrices presented below). To obtain the values $\Delta(A)$ for $A \in \tilde{\mathcal{I}}$ by Lemma 3.6, it suffices to find $N_G(\langle x^{\frac{q-1}{4}}, y \rangle)$. Other normalisers can be easily determined. Indeed, $N_G(\langle x^{\frac{q-1}{4}}, y \rangle) \cong A_4$. This gives

$$\Delta = \begin{bmatrix} |G| \\ (q-1)^2(\frac{1}{q-1} + \frac{1}{2}) \\ 3(q-1) \\ q-1 \end{bmatrix}$$

and so $\mathrm{val}(G,H)$ follows.

The case $q \equiv 1 \pmod 8$ is slightly different since there are more elements in $\tilde{\mathcal{I}}$. In this case the subgroups $\mathbb{Z}_2^2$ give two conjugacy classes in H, and they are not conjugate in G. It follows that

$$\tilde{\mathcal{I}} = \{1, \langle y\rangle, \langle xy\rangle, \langle x^{\frac{q-1}{4}}, y\rangle, \langle x^{\frac{q-1}{4}}, xy\rangle, H\}$$

is a choice of $\tilde{\mathcal{I}}$, with the matrix

$$M = \begin{bmatrix} 1 & \frac{q-1}{4} & \frac{q-1}{4} & \frac{q-1}{8} & \frac{q-1}{8} & 1 \\ & 1 & 0 & 1 & 0 & 1 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 \\ & & & & 1 & 1 \\ & & & & & 1 \end{bmatrix}.$$

Note also that in this case $N_G(\langle x^{\frac{q-1}{4}}, y\rangle) \cong N_G(\langle x^{\frac{q-1}{4}}, xy\rangle) \cong S_4$ and $N_H(\langle x^{\frac{q-1}{4}}, y\rangle) \cong N_H(\langle x^{\frac{q-1}{4}}, xy\rangle) \cong D_8$. The vector Δ is

$$\Delta = \begin{bmatrix} |G| \\ (q-1)^2(\frac{1}{q-1} + \frac{1}{2}) \\ (q-1)^2(\frac{1}{q-1} + \frac{1}{2}) \\ 3(q-1) \\ 3(q-1) \\ q-1 \end{bmatrix},$$

which gives $\mathrm{val}(G,H)$. □

Corollary 6.5. *Let $p = 2^f + 1 \geqslant 17$ be a Fermat prime, and let $G = \mathrm{PSL}_2(p)$ and $H = D_{p-1}$. Then $\mathrm{val}(G,H) = 2^f(2^{f-2} - 2)$, which is not a prime power.*

Proposition 6.6. *Let $G = \mathrm{PGL}_2(q)$ with $q \geqslant 7$, and $H \cong D_{2(q-1)}$ a maximal subgroup of G. Then the Saxl graph of G with stabiliser H is isomorphic to the Johnson graph $J(q+1, 2)$.*

Proof. We may identify Ω with the set of unordered pairs $\{U, W\}$ of 1-dimensional subspaces of the natural module $V \cong \mathbb{F}_q^2$ with $U \oplus W = V$. It is easy to see that two unordered pairs of 1-dimensional subspaces form a base if and only if they have exactly one 1-dimensional subspace in common. See also [7, Example 2.5] or [17, Table 2]. □

Corollary 6.7. *Let $p = 2^f + 1 \geqslant 17$ be a Fermat prime, and let $G = \mathrm{PGL}_2(p)$ and $H = D_{2(p-1)}$. Then $\mathrm{val}(G,H) = 2^{f+1}$, which is a prime power.*

Proposition 6.8. *Let $G = \mathrm{PSL}_2(q)$ with $q \geqslant 11$ odd, and $H \cong D_{q+1}$ a maximal subgroup of G. Then*

$$\mathrm{val}(G,H) = \begin{cases} \frac{1}{4}(q+1)(q-1) & q \equiv 1 \pmod 4 \\ \frac{1}{4}(q+1)(q-3) & q \equiv 3 \pmod 4. \end{cases}$$

Proof. This follows from the proof of [9, Lemma 7.9]. We note that an argument similar to the proof of Proposition 6.4 can also be applied. □

Corollary 6.9. *Let $p = 2^f - 1 \geqslant 31$ be a Mersenne prime, $G = \mathrm{PSL}_2(p)$ and $H = D_{p+1}$. Then $\mathrm{val}(G,H) = 2^{2f-2} - 2^f$, which is not a prime power.*

Proposition 6.10. *Let $G = \mathrm{PGL}_2(q)$ and $H \cong D_{2(q+1)}$ a maximal subgroup of G. Then $\mathrm{val}(G,H) = 0$.*

Proof. The subdegrees of G are given in [17, Table 2] and there is no regular suborbit. Hence, the Saxl graph is empty. □

Corollary 6.11. *Let $p = 2^f - 1 \geqslant 7$ be a Mersenne prime, $G = \mathrm{PGL}_2(p)$ and $H = D_{2(p+1)}$. Then $\mathrm{val}(G,H) = 0$.*

In view of Table 3, we deduce that the proof of Theorem 3 is complete by combining Corollaries 6.5, 6.7, 6.9 and 6.11.

7. Odd Valencies

A rough classification of almost simple primitive groups with odd valency in [7, Proposition 3.2] gives the following proposition.

Proposition 7.1. *Let G be an almost simple primitive group with stabiliser H such that* $\mathrm{val}(G,H)$ *is odd. Then one of the following holds:*

(i) $G = \mathrm{M}_{23}$ *and* $H = 23{:}11$.
(ii) $G = A_p$ *and* $H = \mathrm{AGL}_1(p) \cap G = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$*, where p is a prime such that* $p \equiv 3 \pmod 4$ *and* $(p-1)/2$ *is composite.*
(iii) $\mathrm{soc}(G) = \mathrm{L}_r^\epsilon(q)$*,* $H \cap \mathrm{soc}(G) = \mathbb{Z}_a{:}\mathbb{Z}_r$ *and* $G \neq \mathrm{soc}(G)$*, where* $a = \frac{q^r-\epsilon}{(q-\epsilon)(r,q-\epsilon)}$*,* $r \geqslant 3$ *is a prime and* $\mathrm{soc}(G) \neq \mathrm{U}_3(3), \mathrm{U}_5(2)$.

Note that the valency of $G = A_p$ with stabiliser $H = \mathrm{AGL}_1(p) \cap A_p$ is given in (1). It follows by this equation that $\mathrm{val}(G,H)$ is odd if and only if 2 divides $\frac{p-1}{2}$. However, it makes $p \equiv 1 \pmod 4$, a contradiction. Therefore, the second case in Proposition 7.1 cannot happen and so there are only two possible cases given in Theorem 4.

In this section we set $G = \mathrm{PGL}_r^\epsilon(q)$ for an odd prime r, and $H = \langle z\rangle{:}\langle\sigma\rangle \cong \mathbb{Z}_a{:}\mathbb{Z}_r$ a maximal subgroup of G, where $a = \frac{q^r-\epsilon}{q-\epsilon}$. If H is a Frobenius group then Theorem 4.3 applies. In general, however, H is not Frobenius but "almost" Frobenius.

Lemma 7.2. *The group* $H = \langle x\rangle \times (\langle y\rangle{:}\langle\sigma\rangle) \cong \mathbb{Z}_{(q-\epsilon,r)} \times F$*, where* $x = z^{a/(q-\epsilon,r)}$ *and F is a Frobenius group.*

Proof. First observe that
$$(q-\epsilon,a) = (q-\epsilon, q^{r-1}+\epsilon q^{r-2}+q^{r-3}+\epsilon q^{r-4}+\cdots+\epsilon q+1) = (q-\epsilon,r),$$
and
$$(q+\epsilon,a) = (q+\epsilon, q^{r-1}+\epsilon q^{r-2}+q^{r-3}+\epsilon q^{r-4}+\cdots+\epsilon q+1) = 1.$$
Since r is an odd prime, $(q-\epsilon,r) = 1$ or r. Hence, we may divide our proof into two cases.

If $(q-\epsilon,r) = 1$, then $(q-\epsilon,a) = 1$. Thus, for any element $z^i \in \langle z\rangle$, $(z^i)^\sigma = z^i$ implies that $z^{i(q-\epsilon)} = 1$. Since $(q-\epsilon,a) = 1$, $z^i = 1$ and σ induces a fixed-point-free automorphism of prime order on $\langle z\rangle$. This implies that H is a Frobenius group.

If $(q-\epsilon,r) = r = (q-\epsilon,a)$, set $\ell = q-\epsilon$. It follows that
$$\begin{aligned}
\frac{a}{r} &= \frac{1}{r}\left(\frac{q^r-\epsilon}{q-\epsilon}\right) = \frac{1}{r}\left(\frac{(\ell+\epsilon)^r-\epsilon}{\ell}\right)\\
&= \frac{1}{r}\left(\sum_{i=1}^{r}\binom{r}{i}\ell^{i-1}\epsilon^{r-i}\right) = \left(\sum_{i=2}^{r}\binom{r}{i}\frac{\ell^{i-1}\epsilon^{r-i}}{r}\right)+1\\
&= \left(\sum_{i=2}^{r-1}\ell^{i-2}\epsilon^{r-i}\frac{\binom{r}{i}}{r}\right)\cdot\ell + \frac{\ell}{r}\cdot\ell^{r-2}+1\\
&\equiv 1 \pmod r.
\end{aligned}$$
This implies $(\frac{a}{r},r) = 1$ and $H = (\langle z^{a/r}\rangle \times \langle z^r\rangle){:}\langle\sigma\rangle$. Furthermore, $(\frac{a}{r}, q-\epsilon)$ divides $(\frac{a}{r},\frac{q-\epsilon}{r})\cdot(\frac{a}{r},r) = 1$, which implies that $(\frac{a}{r},q-\epsilon) = 1$. By an argument similar to the previous case, σ induces a trivial automorphism on $\langle z^{a/r}\rangle$ and a fixed-point-free automorphism on $\langle z^r\rangle$. It follows that $H = \langle z^{a/r}\rangle \times (\langle z^r\rangle{:}\langle\sigma\rangle) = \mathbb{Z}_{(q-\epsilon,r)} \times F$, where F is a Frobenius group. $\square$

In the following lemma, we maintain the notation of Lemma 7.2.

Lemma 7.3. *Suppose $(q-\epsilon, r) = r$. Then there exist preimages $\tilde{x}, \tilde{\sigma} \in \mathrm{GL}_r^{\epsilon}(q)$ of x and σ respectively and a basis of $\mathbb{F}_q^r$ (or $\mathbb{F}_{q^2}^r$ for the case $\epsilon = -$) such that the matrices of $\tilde{x}$ and $\tilde{\sigma}$ under this basis are*

$$\begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \mu & & & \end{bmatrix} \text{ and } \begin{bmatrix} 1 & & & \\ & \lambda & & \\ & & \ddots & \\ & & & \lambda^{r-1} \end{bmatrix}$$

respectively, where $|\mu| = q-\epsilon$, $\lambda = \mu^{(q-1)/r}$ when $\epsilon = +$ and $\lambda = \mu^{(q^2-1)/r}$ when $\epsilon = -$. Furthermore, we have that $\tilde{x}$ is conjugate with $\tilde{x}\tilde{\sigma}^i$ in $\mathrm{GL}_r^{\epsilon}(q)$, where $1 \leqslant i \leqslant r-1$.

Proof. If $\epsilon = +$, then let $V = \mathbb{F}_{q^r}$. We can also view $V \cong \mathbb{F}_q^r$ as an $\mathbb{F}_q$-linear space with additional field structure. For any $b \in \mathbb{F}_{q^r}$, let $\pi_b : V \to V$ be the multiplication of b. That is, $\pi_b(x) = bx$ for all $x \in V$. Let τ be the field automorphism of $\mathbb{F}_{q^r} = V$ which maps x to x^q for all $x \in V$. It is easy to see that both π_b and τ are $\mathbb{F}_q$-linear transformations of V. By [21, Section 4.3], there exist $\omega \in \mathbb{F}_{q^r}$ and a homomorphism ϕ from $\mathrm{GL}(V)$ to $\mathrm{PGL}_r(q)$ such that $\phi(\pi_\omega) = x$, $\phi(\tau) = \sigma$ and $\ker\phi = Z(\mathrm{GL}(V)) \cong \mathbb{F}_q^*$. Note that $\phi^{-1}(\langle x \rangle) = (\ker\phi)\langle \pi_\omega \rangle$ is a cyclic group of order $r(q-1)$. We may assume that π_ω is a generator of $\phi^{-1}(\langle x \rangle)$. It follows that $|\omega| = r(q-1)$. Set $\mu = \omega^r \in \mathbb{F}_q$ and $\lambda = \omega^{q-1} = \mu^{\frac{q-1}{r}}$. We have $|\mu| = q-1$. Now set $\tilde{x} = \pi_\omega$ and $\tilde{\sigma} = \tau$. As $\omega \in \mathbb{F}_{q^r} \backslash \mathbb{F}_q$ and r is a prime, we have $\mathbb{F}_{q^r} = \mathbb{F}_q(\omega)$. This implies that $1, \omega, \ldots, \omega^{r-1}$ form a basis of V. It is easy to see that the matrices of $\tilde{x}$ and $\tilde{\sigma}$ under this basis are as desired. Furthermore, for $1 \leqslant i \leqslant r-1$, let $g_i \in \mathrm{GL}(V)$ be such that the matrix of g_i under the basis described above is

$$\begin{bmatrix} 1 & & & & \\ & \lambda^i & & & \\ & & \lambda^{i(1+2)} & & \\ & & & \ddots & \\ & & & & \lambda^{i(1+2+\cdots+(r-1))} \end{bmatrix}. \tag{9}$$

A simple computation gives $\tilde{x}^{g_i} = \tilde{x}\tilde{\sigma}^i$.

If $\epsilon = -$, then let $V = \mathbb{F}_{q^{2r}}$ with a Hermitian form β such that $\beta(x,y) = xy^{q^r}$. We can also view $V \cong \mathbb{F}_{q^2}^r$ as an $\mathbb{F}_{q^2}$-linear space with additional field structure. Let T be the trace map from $\mathbb{F}_{q^{2r}}$ to $\mathbb{F}_{q^2}$, and $\beta^* = T\beta$ be a Hermitian form over $\mathbb{F}_{q^2}$. That is, (V, β) is a 1-dimensional unitary space, while (V, β^*) is an r-dimensional unitary space. For any $b \in \mathbb{F}_{q^r}$, define $\pi_b : V \to V$ by $x \mapsto bx$, which is the multiplication of b. Let τ be the field automorphism of $\mathbb{F}_{q^r} = V$ which maps x to x^{q^2} for all $x \in V$, and c be an element of order $q^r + 1$ in $\mathbb{F}_{q^{2r}}^*$. It is easy to see that both π_c and τ belong to $\mathrm{GU}_r(q)$. Again, by [21, Section 4.3], there exists a homomorphism ϕ from $\mathrm{GU}_r(q)$ to $\mathrm{PGU}_r(q)$ such that $\phi(\pi_b) = z$ and $\phi(\tau) = \sigma$. Set $\omega = c^{a/r}$ and $\mu = \omega^r$. It follows that $\mu \in \mathbb{F}_{q^2}$. Since $\mathbb{F}_{q^{2r}} = \mathbb{F}_{q^2}(\omega)$, the r elements $1, \omega, \ldots, \omega^{r-1}$ form an $\mathbb{F}_{q^2}$-basis of V. Set $\tilde{x} = \pi_\omega$ and $\tilde{\sigma} = \tau$. It is easy to see that the matrices of $\tilde{x}$ and $\tilde{\sigma}$ under this basis are as desired. Furthermore, for $1 \leqslant i \leqslant r-1$ we have $\tilde{x}^{g_i} = \tilde{x}\tilde{\sigma}^i$, where $g_i \in \mathrm{GU}_r(q)$ is the matrix defined in (9), which completes the proof. $\square$

Suppose $(q-\epsilon, r) = r$. By Lemma 7.2, the subgroups of order r in H, up to conjugacy in H, have representatives $\{\langle x \rangle, \langle x\sigma \rangle, \ldots, \langle x\sigma^{r-1} \rangle, \langle \sigma \rangle\}$. Lemma 7.3 implies that even if they are not conjugate in H, $\langle x \rangle$ and $\langle x\sigma^i \rangle$ are conjugate in G. Therefore, there are only two conjugacy classes in G of subgroups of order r in H, which have representatives $\{\langle x \rangle, \langle \sigma \rangle\}$.

Corollary 7.4. *We have* $|N_G(\langle x,\sigma\rangle)| = r^3$ *if* $(q-\epsilon, r) = r$.

Proof. There are $r+1$ subgroups of $\langle x,\sigma\rangle$ of order r, namely $\langle x\rangle, \langle x\sigma\rangle, \dots, \langle x\sigma^{r-1}\rangle$ and $\langle \sigma\rangle$. The image of matrix g_i in the proof of Lemma 7.3 maps $\langle x\rangle$ to $\langle x\sigma^i\rangle$ and fixes $\langle\sigma\rangle$ by conjugation. It follows that there are two orbits of $N_G(\langle x,\sigma\rangle)$ on the $r+1$ subgroups. They are $\{\langle x\rangle, \langle x\sigma\rangle, \dots, \langle x\sigma^{r-1}\rangle\}$ and $\{\langle\sigma\rangle\}$. The stabiliser of the former is $\langle x,\sigma\rangle$, which has order r^2. Therefore, $N_G(\langle x,\sigma\rangle)$ is of order r^3. □

To obtain the valency, we need to determine $|N_G(\langle\sigma\rangle)|$, which is denoted by N for convenience. Indeed, $N = (r-1)|C_G(\langle\sigma\rangle)|$ and the order of the centralisers are determined in [6]. More specifically, the first three rows in [6, Table B.3] give the linear case and the first five rows in [6, Table B.4] give the unitary case. To see this, observe that σ is conjugate to the matrix

$$\begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}$$

and so if $(q,r) = r$ it is a regular unipotent element, while otherwise it has r distinct eigenvalues in a suitable field extension of $\mathbb{F}_q$. In particular, Lemma 7.3 applies when $(q-\epsilon, r) = r$, making σ diagonalisable over $\mathbb{F}_q$ (or $\mathbb{F}_{q^2}$ for the unitary case). In this case, the third row in [6, Table B.3] and the fifth row in [6, Table B.4] apply. This gives the following lemma on $N = |N_G(\langle\sigma\rangle)|$.

Lemma 7.5. *The following statements hold.*

(i) *If* $(q,r) = r$ *then* $N = (r-1)q^{r-1}$.
(ii) *If* $(q-\epsilon, r) = r$ *then* $N = r(r-1)(q-\epsilon)^{r-1}$.
(iii) *Otherwise,*

$$N = \begin{cases} (r-1)(q^k-1)^{\frac{r-1}{k}} & \text{if } \epsilon = +, \text{ or } \epsilon = - \text{ and } k \equiv 0 \pmod 4, \\ (r-1)(q^{k/2}+1)^{\frac{2r-2}{k}} & \text{if } \epsilon = - \text{ and } k \equiv 2 \pmod 4, \\ (r-1)(q^{2k}-1)^{\frac{r-1}{2k}} & \text{if } \epsilon = - \text{ and } k \text{ odd}, \end{cases}$$

where k *is the smallest integer such that* $r \mid q^k - 1$.

Now we are ready to obtain the valencies as well as the multiplicities of subdegrees.

Proposition 7.6. *If* $(q-\epsilon, r) = 1$*, then subdegrees of* G *with stabiliser* H *are* 1, $|H|$, $|H|/r$ *with multiplicities*

$$1,\ \mathrm{val}(G,H)/|H|,\ (N-r)/r$$

respectively, where

$$\mathrm{val}(G,H) = |G:H| + a - 1 - \frac{aN}{r}.$$

Proof. Combine Theorem 4.3 and Lemma 7.2. □

Proposition 7.7. *If* $(q-\epsilon, r) = r$*, then subdegrees of* $\mathrm{soc}(G) = \mathrm{L}_r^\epsilon(q)$ *with stabiliser* $H \cap \mathrm{L}_r^\epsilon(q)$ *are* 1, a, a/r *with multiplicities*

$$1,\ \mathrm{val}(\mathrm{L}_r^\epsilon(q), H\cap \mathrm{L}_r^\epsilon(q))/a,\ (r-1)(q-\epsilon)^{r-1} - r$$

respectively, where

$$\mathrm{val}(\mathrm{L}_r^\epsilon(q), H\cap \mathrm{L}_r^\epsilon(q)) = |G:H| + \frac{|H|}{r} - 1 - \frac{|H|}{r^2}(r-1)(q-\epsilon)^{r-1}.$$

Proof. Note that $|G:H| = |\,\mathrm{L}_r^\epsilon(q) : H\cap \mathrm{L}_r^\epsilon(q)|$. Again, the result follows by Theorem 4.3, Lemmas 7.2 and 7.5. □

Proposition 7.8. *Suppose $(q-\epsilon, r) = r$. Then subdegrees of G with stabiliser H are 1, $|H|$, a, a/r with multiplicities*

$$1,\ \mathrm{val}(G,H)/|H|,\ m(G,H,a),\ r-1$$

respectively, where

$$\mathrm{val}(G,H) = |G:H| - \frac{|H|}{r^3}(r-1)\left((r-1)\left(\frac{|H|}{r} - r\right) + (q-\epsilon)^{r-1}\right) + \frac{|H|}{r^2} - 1$$

and

$$m(G,H,a) = \frac{1}{r^3}(r(r-1)(q-\epsilon)^{r-1} - r^4 + r^3 - r^2 + (r-1)^2|H|).$$

Proof. First we find the possible arc stabilisers of G with point stabiliser H. If a non-identity element $h \in H \cap H^g \neq H$ then h is of order r, otherwise $g \in N_G(\langle h\rangle) = H$, which leads to a contradiction. This implies that an element in $\mathcal{I}$ has order 1, r, r^2 or $|H|$. Moreover, if $x \in H \cap H^g \neq H$ for some $g \in G$ then $[x, x^g] = 1$ as $Z(H^g) = \langle x^g\rangle$. Thus, we have $x^g \in C_G(\langle x\rangle) = H$, which gives $x^g \in H \cap H^g$, while $x \neq x^g$. It follows that $\langle x\rangle$ cannot be an arc stabiliser. With this in mind and by Lemma 7.3, $\mathcal{I}$ can be chosen as

$$\mathcal{I} = \{1, \langle\sigma\rangle, \langle x\sigma\rangle, \langle x^2\sigma\rangle, \ldots, \langle x^{r-1}\sigma\rangle, \langle x,\sigma\rangle, H\}$$

and a set of representatives of the equivalent relation (E1)-(E3) defined in Section 3 is

$$\tilde{\mathcal{I}} = \{1, \langle\sigma\rangle, \langle x\sigma\rangle, \langle x,\sigma\rangle, H\}.$$

Now the matrix of $\tilde{\eta}$ follows that

$$M = \begin{bmatrix} 1 & \frac{|H|}{r^2} & \frac{(r-1)|H|}{r^2} & \frac{|H|}{r^2} & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

and so

$$M^{-1} = \begin{bmatrix} 1 & -\frac{|H|}{r^2} & -\frac{(r-1)|H|}{r^2} & \frac{(r-1)|H|}{r^2} & -1 + \frac{|H|}{r^2} \\ & 1 & 0 & -1 & 0 \\ & & 1 & -1 & 0 \\ & & & 1 & -1 \\ & & & & 1 \end{bmatrix}.$$

To calculate the values of Δ, Corollary 7.4 and Lemma 7.5 can be applied. Note also that

$$\mathcal{S} \cap \langle x\sigma\rangle = \{\langle x\rangle, \langle x\sigma\rangle, \langle x^2\sigma\rangle, \ldots, \langle x^{r-1}\sigma\rangle\}$$

and $\mathcal{S} \cap A^G = \{A\}$ for any other $A \in \tilde{\mathcal{I}}$ by Lemma 7.3. We finally obtain that

$$\begin{bmatrix} |\Delta(1)| \\ |\Delta(\langle\sigma\rangle)| \\ |\Delta(\langle x\sigma\rangle)| \\ |\Delta(\langle x,\sigma\rangle)| \\ |\Delta(H)| \end{bmatrix} = \begin{bmatrix} |G| \\ N|H|/r^2 \\ |H|^2 \cdot (\frac{1}{|H|} + \frac{r-1}{r^2}) \\ |H| \cdot r^3/r^2 \\ |H| \end{bmatrix} = \begin{bmatrix} |G| \\ |H| \cdot (r-1) \cdot (q-\epsilon)^{r-1}/r \\ |H| + \frac{(r-1)|H|^2}{r^2} \\ r|H| \\ |H| \end{bmatrix}.$$

Now the valencies and multiplicities of subdegrees follow by the matrix operations given in Remark 3.11. □

It is straightforward to deduce Theorem 4 by combining Theorem 2, Propositions 7.1, 7.6-7.8.

References

[1] R. F. Bailey and P. J. Cameron. Base size, metric dimension and other invariants of groups and graphs. *Bull. Lond. Math. Soc.*, 43(2):209–242, 2011.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993).

[3] T. C. Burness. On base sizes for actions of finite classical groups. *J. Lond. Math. Soc. (2)*, 75(3):545–562, 2007.

[4] T. C. Burness. On base sizes for almost simple primitive groups. *J. Algebra*, 516:38–74, 2018.

[5] T. C. Burness. Base sizes for primitive groups with soluble stabilisers. *Algebra Number Theory*, to appear.

[6] T. C. Burness and M. Giudici. *Classical groups, derangements and primes*, volume 25 of *Australian Mathematical Society Lecture Series*. Cambridge University Press, Cambridge, 2016.

[7] T. C. Burness and M. Giudici. On the Saxl graph of a permutation group. *Math. Proc. Cambridge Philos. Soc.*, 168(2):219–248, 2020.

[8] T. C. Burness, R. M. Guralnick, and J. Saxl. On base sizes for symmetric groups. *Bull. Lond. Math. Soc.*, 43(2):386–391, 2011.

[9] T. C. Burness and S. Harper. Finite groups, 2-generation and the uniform domination number. *Israel J. Math.*, 239(1):271–367, 2020.

[10] T. C. Burness and H. Y. Huang. On the Saxl graphs of primitive groups with soluble stabilisers. *arXiv:2105.11861*, 2021.

[11] T. C. Burness, M. W. Liebeck, and A. Shalev. Base sizes for simple groups and a conjecture of Cameron. *Proc. Lond. Math. Soc. (3)*, 98(1):116–162, 2009.

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

[13] P. J. Cameron. Suborbits in transitive permutation groups. In *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 3: Combinatorial group theory*, pages 98–129. Math. Centre Tracts, No. 57, 1974.

[14] P. J. Cameron. Some open problems on permutation groups. In *Groups, combinatorics & geometry (Durham, 1990)*, volume 165 of *London Math. Soc. Lecture Note Ser.*, pages 340–350. Cambridge Univ. Press, Cambridge, 1992.

[15] P. J. Cameron and W. M. Kantor. Random permutations: some group-theoretic aspects. *Combin. Probab. Comput.*, 2(3):257–262, 1993.

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

[17] I. A. Faradžev and A. A. Ivanov. Distance-transitive representations of groups G with $\mathrm{PSL}_2(q) \trianglelefteq G \trianglelefteq \mathrm{P\Gamma L}_2(q)$. *European J. Combin.*, 11(4):347–356, 1990.

[18] F. Frobenius. Über auflösbare gruppen iv, sitz. *Akad. Wiss. Berlin*, 1216(1230):1216–1230, 1901.

[19] M. Giudici, S. P. Glasby, C. H. Li, and G. Verret. Arc-transitive digraphs with quasiprimitive local actions. *J. Pure Appl. Algebra*, 223(3):1217–1226, 2019.

[20] A. A. Ivanov, M. K. Klin, S. V. Tsaranov, and S. V. Shpektorov. On the question of calculation of the subdegrees of transitive permutation groups. *Uspekhi Mat. Nauk*, 38(6(234)):115–116, 1983.

[21] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[22] A. V. Konygin. On primitive permutation groups with a stabilizer of two points normal in the stabilizer of one of them. *Sib. Èlektron. Mat. Izv.*, 5:387–406, 2008.

[23] A. V. Konygin. On primitive permutation groups with a stabilizer of two points that is normal in the stabilizer of one of them: case when the socle is a power of a sporadic simple group. *Proc. Steklov Inst. Math.*, 272(suppl. 1):S65–S73, 2011.

[24] A. V. Konygin. On P. Cameron's question on primitive permutation groups with a stabilizer of two points that is normal in the stabilizer of one of them. *Tr. Inst. Mat. Mekh.*, 19(3):187–198, 2013.

[25] A. V. Konygin. On a question of Cameron on triviality in primitive permutation groups of the stabilizer of two points that is normal in the stabilizer of one of them. *Tr. Inst. Mat. Mekh.*, 21(3):175–186, 2015.

[26] A. V. Konygin. On primitive permutation groups with the stabilizer of two points normal in the stabilizer of one of them: the case when the socle is a power of the group $E_8(q)$. *Tr. Inst. Mat. Mekh.*, 25(4):88–98, 2019.

[27] J. P. S. Kung, G.-C. Rota, and C. H. Yan. *Combinatorics: the Rota way*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2009.

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

[29] C. H. Li and H. Zhang. The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs. *Proc. Lond. Math. Soc. (3)*, 103(3):441–472, 2011.

[30] M. W. Liebeck, C. E. Praeger, and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Austral. Math. Soc. Ser. A*, 44(3):389–396, 1988.

[31] M. W. Liebeck and A. Shalev. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.*, 12(2):497–520, 1999.

[32] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[33] W. R. Scott. *Group theory.* Dover Publications, Inc., New York, second edition, 1987.

[34] Á. Seress. The minimal base size of primitive solvable permutation groups. *Journal of the London Mathematical Society*, 53(2):243–255, 1996.

[35] Á. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

[36] P. Spiga. A generalization of Sims' conjecture for finite primitive groups and two point stabilizers in primitive groups. *J. Group Theory*, to appear.

[37] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

J. Chen, School of Mathematical Sciences, Xiamen University, Xiamen 361005, P.R. China

Email address: cjy1988@pku.edu.cn

H.Y. Huang, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK

Email address: hy.huang@bristol.ac.uk