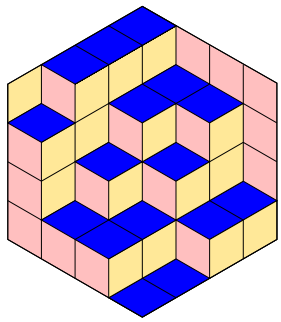


ALGEBRAIC COMBINATORICS

Timothy C. Burness & Hong Yi Huang

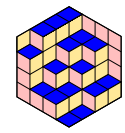
On the Saxl graphs of primitive groups with soluble stabilisers

Volume 5, issue 5 (2022), p. 1053-1087.

https://doi.org/10.5802/alco.238

Algebraic Combinatorics is published by The Combinatorics Consortium and is a member of the Centre Mersenne for Open Scientific Publishing
www.tccpublishing.org www.centre-mersenne.org
e-ISSN: 2589-5486

Algebraic Combinatorics
Volume 5, issue 5 (2022), p. 1053–1087
https://doi.org/10.5802/alco.238



On the Saxl graphs of primitive groups with soluble stabilisers

Timothy C. Burness & Hong Yi Huang

Abstract Let G be a transitive permutation group on a finite set Ω and recall that a base for G is a subset of Ω with trivial pointwise stabiliser. The base size of G, denoted $b(G)$, is the minimal size of a base. If $b(G) = 2$ then we can study the Saxl graph $\Sigma(G)$ of G, which has vertex set Ω and two vertices are adjacent if and only if they form a base. This is a vertex-transitive graph, which is conjectured to be connected with diameter at most 2 when G is primitive. In this paper, we combine probabilistic and computational methods to prove a strong form of this conjecture for all almost simple primitive groups with soluble point stabilisers. In this setting, we also establish best possible lower bounds on the clique and independence numbers of $\Sigma(G)$ and we determine the groups with a unique regular suborbit, which can be interpreted in terms of the valency of $\Sigma(G)$.

1. Introduction

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω with point stabiliser H and recall that a *base* for G is a subset of Ω with trivial pointwise stabiliser. In turn, the *base size* of G, denoted $b(G)$, is the minimal size of a base. This is a classical concept in permutation group theory, which arises naturally in a wide range of contexts. There is a long history of studying bases, which stretches all the way back to the nineteenth century, and there are many applications and connections to other areas of algebra and combinatorics. We refer the reader to the survey articles [3, 34] and [8, Section 5] for further details.

Historically, there has been a focus on studying bases for finite primitive permutation groups and there have been several major advances in this direction in recent years. For example, a number of highly influential conjectures due to Babai, Cameron, Kantor and Pyber from the 1990s have been resolved, which in turn has opened up new directions of research. For instance, Seress [39] proved that $b(G) \leqslant 4$ if G is a finite soluble primitive group, which established a strong form of Pyber's base size conjecture in this setting (in [37], Pyber conjectured that there exists an absolute constant c such that $b(G)$ is at most $c \log_n |G|$ for every primitive group G of degree n and the proof was finally completed in [22]). Seress' theorem has recently been extended in [9], where the main result shows that $b(G) \leqslant 5$ for every finite primitive

Manuscript received 23rd August 2021, revised 14th March 2022, accepted 16th March 2022.

Keywords. Saxl graph, primitive group, base, soluble stabiliser.

Acknowledgements. Both authors thank Eamonn O'Brien for his assistance with several computations in this paper. The second author thanks the China Scholarship Council for supporting his doctoral studies at the University of Bristol and he thanks the Southern University of Science and Technology (SUSTech) for their generous hospitality during a visit in 2021.

group with soluble point stabilisers (it is worth noting that the bounds in [9] and [39] are best possible). Moreover, the exact base size is computed in [9] for all almost simple primitive groups with soluble point stabilisers (recall that G is *almost simple* if there exists a non-abelian simple group G_0 such that $G_0 \trianglelefteqslant G \leqslant \mathrm{Aut}(G_0)$; here G_0 is the *socle* of G).

Further motivation stems from an ambitious project initiated by Jan Saxl in the 1990s. Here the main aim is to classify all the base-two finite primitive permutation groups, where a group G is said to be *base-two* if $b(G) = 2$. These groups arise naturally in many applications of bases to other problems. For example, see [18] on the classification of extremely primitive groups and [14] for applications concerning the 2-generation properties of almost simple groups. Although a complete classification of the base-two primitive groups remains out of reach, there has been some significant progress. For instance, we refer the reader to [25, 24] for work of Fawcett on diagonal-type groups and twisted wreath products, respectively, and there are various partial results for affine-type groups (see [26, 27, 29, 30], for example). Similarly, we refer the reader to [9, 13, 12, 16] for results towards a classification of the base-two almost simple groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two finite transitive permutation group with point stabiliser H. In [11], Burness and Giudici define the *Saxl graph* $\Sigma(G)$ of G as follows: the vertex set is Ω and two vertices are joined by an edge if and only if they form a base for G. Clearly, $\Sigma(G)$ is vertex-transitive and it is easy to see that $\Sigma(G)$ is connected if G is primitive (as discussed in [11], if G is imprimitive then $\Sigma(G)$ can have arbitrarily many connected components). In addition, $\Sigma(G)$ is a complete graph if and only if G is a Frobenius group. Various problems concerning the valency and connectedness properties of Saxl graphs are investigated in [11] and we refer the reader to [20] for further results on the valency of $\Sigma(G)$ when G is primitive.

A number of open problems concerning Saxl graphs are presented in [11] and the aim of this paper is to address some of these questions for the permutation groups in the collection denoted $\mathcal{G}$, which is defined as follows:

$$\mathcal{G} = \{\textit{finite almost simple primitive base-two groups with soluble point stabilisers}\}.$$

This is a natural collection to consider in this setting because one of the main results in [9] provides a complete classification of the groups in $\mathcal{G}$. We will also need to highlight the following subcollection, where G_0 denotes the socle of G and H is a point stabiliser:

$$\mathcal{L} = \{G \in \mathcal{G} \,:\, G_0 = \mathrm{L}_2(q),\ H \text{ is of type } \mathrm{GL}_1(q) \wr S_2 \text{ or } \mathrm{GL}_1(q^2)\}.$$

In terms of Aschbacher's subgroup structure theorem [1], the subgroups H in the definition of $\mathcal{L}$ comprise the collections denoted $\mathcal{C}_2$ and $\mathcal{C}_3$.

Perhaps the most intriguing open problem in this area is [11, Conjecture 4.5], which asserts that if G is primitive, then any two vertices in $\Sigma(G)$ have a common neighbour. In particular, this implies that the diameter of $\Sigma(G)$ is at most 2 for every base-two finite primitive group G. Evidence for the conjecture is presented in [11, Sections 4-6], where it is verified in several special cases. Our first main result establishes [11, Conjecture 4.5] for the groups in $\mathcal{G}$. This extends recent work of Chen and Du [19], who have shown that $\Sigma(G)$ has diameter 2 for every base-two almost simple primitive group with socle $\mathrm{L}_2(q)$.

Theorem 1.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$. Then any two vertices in $\Sigma(G)$ have a common neighbour. In particular, $\Sigma(G)$ has diameter 2.*

REMARK 1.2. It is straightforward to extend our methods in order to establish [11, Conjecture 4.5] for all base-two almost simple primitive groups with socle $\mathrm{L}_2(q)$; we refer the reader to Theorem 4.22.

Next we turn to the clique number of $\Sigma(G)$, which is denoted $\omega(G)$. Recall that this is the maximal size of a complete subgraph. By Theorem 1.1 we immediately deduce that $\omega(G) \geqslant 3$ for every group G in $\mathcal{G}$ and we can establish a stronger lower bound.

THEOREM 1.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$ with socle G_0 and assume that either $G \in \mathcal{G} \setminus \mathcal{L}$ or $G \leqslant \mathrm{PGL}_2(q)$. Then $\omega(G) \geqslant 4$, with equality if and only if $G = A_5$ and Ω is the set of 2-element subsets of $\{1, \ldots, 5\}$.*

REMARK 1.4. Let us record a couple of comments on the statement of Theorem 1.3.

(a) First note that if $G = A_5$ and Ω is the set of 2-element subsets of $\{1, \ldots, 5\}$, then $\Sigma(G)$ is the complement of the Petersen graph, which also coincides with the Johnson graph $J(5, 2)$.

(b) We expect that the bound $\omega(G) \geqslant 5$ also holds for the groups $G \in \mathcal{L}$ with $G \not\leqslant \mathrm{PGL}_2(q)$, but we have not been able to verify this in all cases. Here the main difficulty involves constructing an explicit clique of size 5 when G contains field automorphisms, working with a suitable geometric description of Ω (for example, if H is of type $\mathrm{GL}_1(q) \wr S_2$, then we may identify Ω with the set of pairs of distinct 1-dimensional subspaces of the natural module for G_0). With the aid of MAGMA [4], we have verified the bound $\omega(G) \geqslant 5$ for all groups in $\mathcal{L}$ with $5 < q < 1000$, but the general case remains open. We refer the reader to Remarks 4.11 and 4.21 for further details on the difficulties that arise.

For our next result, recall that the *independence number* of $\Sigma(G)$, denoted $\alpha(G)$, is the maximal size of a co-clique (in other words, it is the clique number of the complement of $\Sigma(G)$). By applying work of Magaard and Waldecker [35, 36], we will prove the following result.

THEOREM 1.5. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$. Then either $\alpha(G) \geqslant 4$, or $G = A_5$, Ω is the set of 2-element subsets of $\{1, \ldots, 5\}$ and $\alpha(G) = 2$.*

As explained in [11, Remark 2.2], the Saxl graph $\Sigma(G)$ can be viewed as the *generalised orbital graph* corresponding to the regular suborbits of G. In particular, $\Sigma(G)$ is an orbital graph of G if and only if G has a unique regular suborbit (recall that the base-two condition implies that G has at least one regular suborbit), which in turn is equivalent to the property that G acts arc-transitively on $\Sigma(G)$. The following result completely determines when a group in $\mathcal{G}$ has a unique regular suborbit.

THEOREM 1.6. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$ with point stabiliser H. Then G has a unique regular suborbit if and only if*

(i) *$G = \mathrm{PGL}_2(q)$, $H = D_{2(q-1)}$ and $q \geqslant 4$, $q \neq 5$; or*
(ii) *(G, H) is one of the cases listed in Table 1.*

REMARK 1.7. Some comments on the statement of Theorem 1.6 are in order:

(a) In the second column of Table 1 we record the *type of H*. If G is a group of Lie type, then this gives an approximate description of the structure of H, which is consistent with usage in [28] when G is a classical group. For example, the notation in the first row indicates that H is the stabiliser in G of an orthogonal decomposition $V = V_1 \perp V_2$ of the natural module for G_0, where the V_i are nondegenerate 4-dimensional subspaces of plus-type. In

G	Type of H	Comments
$P\Omega_8^+(3).2^2$	$O_4^+(3) \wr S_2$	Both groups of this shape
$\Omega_8^+(2).3$	$O_2^-(2) \times GU_3(2)$	
$SO_7(3)$	$O_4^+(3) \perp O_3(3)$	
$PSp_6(3)$	$Sp_2(3) \wr S_3$	
$PGL_4(3)$	$O_4^+(3)$	
$U_4(3).[4]$	$GU_1(3) \wr S_4$	$G \neq G_0.\langle \delta^2, \phi \rangle$
$U_4(3)$	$GU_2(3) \wr S_2$	
$L_3(4).D_{12}$	$GL_1(4^3)$	
$L_3(4).2$	$GU_3(2)$	$G \neq P\Sigma L_3(4)$
$U_3(5).S_3$	$GU_1(5) \wr S_3$	
$U_3(4)$	$GU_1(4) \wr S_3$	
$L_2(11).2$	$2_-^{1+2}.O_2^-(2)$	
$L_2(9).2$	$GL_1(9^2)$	$G = M_{10}$
$L_2(5)$	$GL_1(5^2)$	
$G_2(3).2$	$SL_2(3)^2$	
S_7	$AGL_1(7)$	
$J_2.2$	$5^2{:}(4 \times S_3)$	
M_{11}	$2.S_4$	

TABLE 1. Groups in $\mathcal{G}$ with a unique regular suborbit

the final three rows of the table, we present the precise structure of H in the second column.

(b) In the first row of the table, there are two non-isomorphic groups G of the form $G_0.2^2$, up to conjugacy in $\mathrm{Aut}(G_0)$. In both cases, G has a unique regular suborbit.

(c) Suppose $G = G_0.[4]$, where $G_0 = U_4(3)$ and H is of type $GU_1(3) \wr S_4$. Note that there are three groups of this form up to conjugacy in $\mathrm{Aut}(G_0)$, namely $G_0.4 = PGU_4(3)$ and two groups of shape $G_0.2^2$. As recorded in [5, Table 8.10], H is not maximal when $G = G_0.\langle \delta^2, \phi \rangle = G_0.2^2$, but in the other two cases H is maximal and G has a unique regular suborbit (here we are adopting the notation for automorphisms from [5]).

(d) Suppose $G = G_0.2$, where $G_0 = L_3(4)$ and H is of type $GU_3(2)$. There are three groups of this form; each contains a maximal subgroup of the given type, but $b(G) = 2$ if and only if $G = G_0.2_1$ or $G_0.2_3$, and in both cases G has a unique regular suborbit. Equivalently, $G = G_0.2$ has a unique regular suborbit if and only if $G \neq P\Sigma L_3(4)$.

Probabilistic and computational methods play a key role in the proofs of our main theorems and we will introduce the relevant results we will need in Section 2. One of our main tools is Proposition 2.2, which implies that if $G \leqslant \mathrm{Sym}(\Omega)$ is a finite transitive base-two group and $Q(G) < 1/4$, then $\omega(G) \geqslant 5$ and any four vertices in $\Sigma(G)$ have a common neighbour. Here $Q(G)$ is the probability that a random pair of points in Ω do not form a base for G (so the condition $b(G) = 2$ implies that $Q(G) < 1$). In view of Theorems 1.1 and 1.3, this explains why one of our main aims is to establish the bound $Q(G) < 1/4$ whenever possible, using upper bounds on fixed point ratios to do this. This approach turns out to be effective for the groups in $\mathcal{G} \setminus \mathcal{L}$. Indeed, Theorem 3.1 shows that if G is such a group then $Q(G) \geqslant 1/4$ if and only if G is one of the finitely many groups recorded in Tables 2 and 3 (this is the main content of Section 3). The latter groups are small enough to be amenable to computational methods and we refer the reader to Section 2.2 for more details.

However, the groups in $\mathcal{L}$ behave rather differently and this explains why they need to be handled separately (see Section 4). For example, if $G = \mathrm{PGL}_2(q)$ and $H = D_{2(q-1)}$ then G has a unique regular suborbit and we deduce that

$$Q(G) = 1 - \frac{4(q-1)}{q(q+1)}.$$

In particular, $Q(G)$ tends to 1 as q tends to infinity, whence Proposition 2.2 is not going to be useful in this situation.

The proof of Theorem 1.1 will be completed in Section 5 and proofs of Theorems 1.3 and 1.5 are presented in Section 6. Finally, the proof of Theorem 1.6 is given in Section 7.

Notation. Our notation is fairly standard. Given a finite group G and a positive integer n, we write C_n, or just n, for a cyclic group of order n and G^n for the direct product of n copies of G. An unspecified extension of G by a group H will be denoted by $G.H$; if the extension splits then we sometimes write $G{:}H$. We use $[n]$ for an unspecified soluble group of order n. If X is a subset of G, then $i_n(X)$ is the number of elements of order n in X. We adopt the standard notation for simple groups of Lie type from [28]. In particular, $\mathrm{L}_n^\varepsilon(q)$ denotes $\mathrm{PSL}_n(q)$ (when $\varepsilon = +$) and $\mathrm{PSU}_n(q)$ (when $\varepsilon = -$). We write $\mathrm{P\Omega}_n^\varepsilon(q)$ for the simple orthogonal groups, which differs from the notation used in the Atlas [21]. All logarithms are base two.

2. Preliminaries

In this section, we present the main probabilistic and computational methods that will be used in the proofs of our main theorems.

2.1. Probabilistic methods. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive permutation group on a finite set Ω with point stabiliser H. Here we recall a powerful probabilistic approach for bounding the base size of G, which was originally introduced by Liebeck and Shalev [33] in their innovative proof of a conjecture of Cameron and Kantor on bases for almost simple primitive groups.

Fix a positive integer c and let $Q(G,c)$ be the probability that a randomly chosen c-tuple of points in Ω does not form a base for G, that is

$$Q(G,c) = \frac{|\{(\alpha_1,\ldots,\alpha_c) \in \Omega^c \,:\, \bigcap_i G_{\alpha_i} \neq 1\}|}{|\Omega|^c} \tag{1}$$

and note that $b(G) \leqslant c$ if and only if $Q(G,c) < 1$. Clearly, a subset $\{\alpha_1,\ldots,\alpha_c\} \subseteq \Omega$ is not a base for G if and only if there exists an element $x \in G$ of prime order fixing each α_i. Now the probability that x fixes a randomly chosen element of Ω is given by the *fixed point ratio*

$$\mathrm{fpr}(x) = \frac{|C_\Omega(x)|}{|\Omega|} = \frac{|x^G \cap H|}{|x^G|},$$

where $C_\Omega(x)$ is the set of fixed points of x on Ω, whence

$$Q(G,c) \leqslant \sum_{x \in \mathcal{P}} \mathrm{fpr}(x)^c = \sum_{i=1}^{k} |x_i^G| \cdot \mathrm{fpr}(x_i)^c =: \widehat{Q}(G,c),$$

where $\mathcal{P} = \bigcup_i x_i^G$ is the set of elements of prime order in G.

The following elementary result is [7, Lemma 2.1] and it provides a useful tool for estimating $\widehat{Q}(G,c)$.

Lemma 2.1. *Suppose $x_1, \ldots, x_m$ represent distinct conjugacy classes in G such that $\sum_i |x_i^G \cap H| \leqslant A$ and $|x_i^G| \geqslant B$ for all i. Then*

$$\sum_{i=1}^{m} |x_i^G| \cdot \mathrm{fpr}(x_i)^c \leqslant B(A/B)^c$$

for every positive integer c.

In this paper, we are interested in the case $c = 2$ and we define

$$Q(G) \coloneqq Q(G,2), \quad \widehat{Q}(G) \coloneqq \widehat{Q}(G,2) \tag{2}$$

so $b(G) = 2$ if and only if $Q(G) < 1$. As noted in [11, Section 3.3], we have

$$Q(G) = 1 - \frac{r|H|}{n} \tag{3}$$

where $n = |G : H| = |\Omega|$ and r is the number of regular suborbits of G.

Suppose $b(G) = 2$ and set

$$t(G) = \max\{m \in \mathbb{N} \,:\, Q(G) < 1/m\}.$$

The following key result is [11, Lemma 3.6].

Proposition 2.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a transitive group on a finite set Ω and assume $t(G) \geqslant 2$. Then the following hold:*

(i) *Any $t(G)$ vertices in the Saxl graph $\Sigma(G)$ have a common neighbour.*
(ii) *The clique number of $\Sigma(G)$ is at least $t(G) + 1$.*

In particular, the conclusion to Theorem 1.1 holds if $Q(G) < 1/2$. Similarly, the bound $\omega(G) \geqslant 5$ in Theorem 1.3 on the clique number of $\Sigma(G)$ holds if $Q(G) < 1/4$. Let us also observe that if $Q(G) < 1/4$ then G has a unique regular suborbit only if

$$|H|^2 \leqslant |G| < \frac{4}{3}|H|^2.$$

By definition, each group G in the collection $\mathcal{G}$ satisfies the bound $Q(G) < 1$ and in view of the above observations, one of our main aims is to show that $Q(G) < 1/4$ in most cases (see Theorem 3.1). This will reduce the proofs of Theorems 1.1 and 1.3 to a small number of specific cases that require closer attention.

It turns out that there are two infinite families in $\mathcal{G}$ that will require special attention. This is the collection denoted $\mathcal{L}$ in the introduction, which comprises the groups with socle $G_0 = \mathrm{L}_2(q)$ and point stabiliser H of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$. More precisely, $\mathcal{L}$ also contains any groups in $\mathcal{G}$ that are permutation isomorphic to one of these almost simple primitive groups with socle $\mathrm{L}_2(q)$. In particular, let us observe that if $G \in \mathcal{G} \setminus \mathcal{L}$ then

$$G_0 \notin \{A_5, A_6, \mathrm{L}_3(2), \mathrm{Sp}_4(2)', {}^2G_2(3)'\} \cup \{\mathrm{L}_2(q) \,:\, q \leqslant 9\}. \tag{4}$$

Remark 2.3. The rationale for isolating the groups in $\mathcal{L}$ becomes clear when we consider the probability $Q(G)$ defined above. For example, by inspecting the relevant proofs in [9], it is easy to check that if $G \in \mathcal{G} \setminus \mathcal{L}$ then $Q(G) \to 0$ as $|G| \to \infty$ (in particular, there are only finitely many groups of this form with $Q(G) \geqslant 1/4$). However, the groups in $\mathcal{L}$ behave differently and they need to be handled separately. For example, if $G = \mathrm{L}_2(q)$ and q is odd, then by inspecting the proofs of [9, Lemmas 4.7 and 4.8] we see that

$$Q(G) = \begin{cases} 1 - \frac{(q-1)(q+a)}{2q(q+1)} \text{ if } H = D_{q-1} \\ \\ 1 - \frac{(q+1)(q-b)}{2q(q-1)} \text{ if } H = D_{q+1} \end{cases}$$

where $(a,b) = (7,1)$ if $q \equiv 1 \pmod 4$, otherwise $(a,b) = (5,3)$. Therefore, in both cases we get $Q(G) \to 1/2$ as q tends to infinity. Similarly, as noted in Section 1, if $G = \mathrm{PGL}_2(q)$ then $Q(G) \to 1$ when q is odd and $H = D_{2(q-1)}$. As a consequence, we cannot appeal to Proposition 2.2 in these cases and we will need to adopt a constructive approach to establish our main results (see Sections 4.1 and 4.2).

2.2. Computational methods. We will apply computational methods to establish our main results when G is a sporadic group, or a small degree symmetric or alternating group, or a low rank group of Lie type defined over a suitably small field. We mainly use Magma V2.25-7 [4] to do the computations, noting that the GAP Character Table Library [6] is an important tool for the analysis of sporadic groups.

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two almost simple primitive group with socle G_0 and soluble point stabiliser H. Our initial aim is to construct G as a permutation group of an appropriate degree (note that this will not necessarily be the permutation representation of G on Ω). To do this, we typically use the Magma function `AutomorphismGroupSimpleGroup` to obtain $A = \mathrm{Aut}(G_0)$ as a permutation group and then we identify G by inspecting the subgroups of A containing G_0. We then construct H as a subgroup of G in this permutation representation via the command `MaximalSubgroups(G:IsSolvable:=true)`, which returns a set of representatives of the G-classes of soluble maximal subgroups of G. In a handful of cases (due to the size of G), this approach is ineffective and a different method is needed in order to construct H. For example, we may identify $H = N_G(K)$ for some specific p-subgroup K of G (for instance, see [9, Example 2.4]).

The next key step is to estimate $Q(G)$, with the aim of determining the groups with $Q(G) \geqslant 1/4$ (this is the content of Theorem 3.1). First we focus on $\widehat{Q}(G)$, recalling that $Q(G) \leqslant \widehat{Q}(G)$ (see (2)). It is straightforward to implement an algorithm in Magma to compute $\widehat{Q}(G)$ precisely, using the functions `ConjugacyClasses` and `IsConjugate` to find a set of representatives of the conjugacy classes in H and to test conjugacy in G, respectively. This allows us to compute $|x^G \cap H|$ for each $x \in H$ of prime order, which is the main step in calculating the contribution to $\widehat{Q}(G)$ from the elements in the G-class of x. Note that this approach can be implemented without determining a set of representatives of the conjugacy classes in G, which can be an expensive operation in terms of time and memory. Let us also observe that $\widehat{Q}(G)$ can be computed precisely if we have access to the character tables of G and H, in addition to the fusion map from H-classes to G-classes. For example, this approach works well when G is a sporadic group, using the character table data stored in the GAP Character Table Library [6] (see the proof of Proposition 3.4).

In some cases, it turns out that we can work effectively with a crude bound

$$\widehat{Q}(G) \leqslant \widetilde{Q}(G) \tag{5}$$

where the contribution to $\widetilde{Q}(G)$ from all the elements in G of order r (for a fixed prime r) with $|x^G| = m$ is given by

$$\frac{1}{m}\left(\sum_{i=1}^{\ell} |y_i^H|\right)^2$$

and $y_1, \ldots, y_\ell$ represent the distinct H-classes of elements of order r with $|y_i^G| = m$. Notice that no `IsConjugate` commands are needed to compute $\widetilde{Q}(G)$, which can be a significant saving.

If $\widehat{Q}(G) \geqslant 1/4$ then we need to either compute a better upper bound on $Q(G)$, or we need to determine $Q(G)$ precisely. In view of (3), it suffices to bound (or compute)

the number r of regular suborbits of G. To do this, we work with double cosets, noting that if R is a complete set of (H,H) double coset representatives in G, then

$$r = |\{x \in R \,:\, |HxH| = |H|^2\}|. \tag{6}$$

If $|G:H|$ is not prohibitively large (for example, if $|G:H| < 10^7$), then we can use the Magma function `DoubleCosetRepresentatives` to determine R and then compute r. If $|G:H|$ is large, then we may be able to use the `DoubleCosetCanonical` function to identify sufficiently many distinct double cosets of size $|H|^2$ so that the corresponding lower bound on r forces $Q(G) < 1/4$. Similarly, we may be able to find a set S of distinct (H,H) double coset representatives so that

$$\sum_{x \in S} |HxH| > |G| - |H|^2$$

and thus $r = |\{x \in S \,:\, |HxH| = |H|^2\}|$. It is straightforward to implement all of these methods in Magma.

3. Random bases

In this section we will prove the following theorem, which will be a key ingredient in the proofs of Theorems 1.1 and 1.3. We adopt the notation $\mathcal{G}$ and $\mathcal{L}$ introduced above. In particular, we recall that the socle G_0 of a group in $\mathcal{G} \setminus \mathcal{L}$ satisfies the restrictions in (4).

Theorem 3.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G} \setminus \mathcal{L}$ with socle G_0 and point stabiliser H. Then either $Q(G) < 1/4$, or (G,H) is one of the cases in Tables 2 and 3.*

Remark 3.2. We make several comments concerning Theorem 3.1.

(a) In Table 2 we record the relevant cases where G_0 is non-classical (as previously noted, the condition $G \in \mathcal{G} \setminus \mathcal{L}$ implies that $G_0 \neq A_5, A_6$ or ${}^2G_2(3)'$).
(b) The cases with G_0 classical are listed in Table 3. As before, the *type of H* provides an approximate description of the group theoretic structure of H (the precise structure can be read off from [28]).
(c) In both tables, the number of regular suborbits of G is listed in the third column.
(d) We use the standard Atlas [21] notation for describing the almost simple groups of the form $\mathrm{L}_4(3).2$. In particular, $\mathrm{L}_4(3).2_2$ and $\mathrm{L}_4(3).2_3$ contain involutory graph automorphisms x with $C_{G_0}(x) = \mathrm{PSp}_4(3).2$ and $\mathrm{PSO}_4^-(3).2$, respectively.
(e) Suppose $G = G_0.S_3$, where $G_0 = \mathrm{L}_3(4)$ and H is of type $\mathrm{GL}_1(3^4)$. There are two groups of this form, up to conjugacy in $\mathrm{Aut}(G_0)$, and we find that $r = 6$ and $Q(G) = 17/80$ if $G = G_0.\langle \delta, \phi \rangle$, whereas $r = 3$ and $Q(G) = 97/160$ if $G = G_0.\langle \delta, \gamma \rangle$. Here we are using the notation for automorphisms in [5], where δ, ϕ and γ denote diagonal, field and graph automorphisms, respectively. We adopt similar notation to describe the relevant groups with $G_0 = \mathrm{U}_4(3)$ or $\mathrm{P\Omega}_8^+(3)$ (in the latter case, γ is an involutory graph automorphism).

3.1. Alternating and sporadic groups.

Proposition 3.3. *The conclusion to Theorem 3.1 holds if G_0 is an alternating group.*

Proof. Let $G_0 = A_m$ be the socle of G. If $m \leqslant 12$ then the result is easily checked using Magma [4] (see Section 2.2), so let us assume $m \geqslant 13$. By inspecting [31, Table

G	H	r	$Q(G)$
A_9	$\mathrm{ASL}_2(3)$	2	17/35
S_7	$\mathrm{AGL}_1(7)$	1	13/20
M_{11}	$2.S_4$	1	39/55
M_{12}	$A_4 \times S_3$	13	16/55
$\mathrm{M}_{12}.2$	$S_4 \times S_3$	4	31/55
J_1	19:6	9	257/770
	$D_6 \times D_{10}$	34	443/1463
J_2	$5^2{:}D_{12}$	2	59/84
$\mathrm{J}_2.2$	$5^2{:}(4 \times S_3)$	1	59/84
$\mathrm{J}_3.2$	$3^{2+1+2}{:}8.2$	3	886/1615
	$2^{2+4}{:}(S_3 \times S_3)$	10	457/969
HS.2	$5^{1+2}.[2^5]$	3	106/231
McL.2	$2^{2+4}{:}(S_3 \times S_3)$	228	9419/28875
He.2	$2^{4+4}.(S_3 \times S_3).2$	5	23011/29155
Suz	$3^{2+4}{:}2.(A_4 \times 2^2).2$	16	7529/25025
Suz.2	$3^{2+4}{:}2.(S_4 \times D_8)$	4	16277/25025
HN	$5^{1+4}{:}2^{1+4}.5.4$	47	332152/1066527
HN.2	$5^{1+4}{:}2^{1+4}.5.4.2$	22	34457/96957
${}^2B_2(8)$	13:4	7	7/20
${}^2B_2(8).3$	13:12	2	31/70
${}^2F_4(2)'$	$5^2{:}4A_4$	6	27/52
${}^2F_4(2)$	$5^2{:}4S_4$	3	27/52
$G_2(3)$	$(\mathrm{SL}_2(3) \circ \mathrm{SL}_2(3)).2$	4	563/819
$G_2(3).2$	$(\mathrm{SL}_2(3) \circ \mathrm{SL}_2(3)).2.2$	1	691/819

TABLE 2. The groups in $\mathcal{G} \setminus \mathcal{L}$ with $Q(G) \geqslant 1/4$, part I

14] and [9, Table 4] we deduce that m is a prime and $H = \mathrm{AGL}_1(m) \cap G$, in which case

$$|H| \leqslant m(m-1) = a, \ \ |x^G| \geqslant \frac{m!}{((m-1)/2)!2^{(m-1)/2}} = b$$

for all $x \in H$ of prime order (minimal if x is an involution, noting that x has at most one fixed point on $\{1, \ldots, m\}$). In view of Lemma 2.1, this gives $\widehat{Q}(G) < a^2/b < 1/4$ and the result follows. □

PROPOSITION 3.4. *The conclusion to Theorem* 3.1 *holds if G_0 is a sporadic group.*

Proof. First recall that the maximal subgroups of G have been classified up to conjugacy, with the exception of the Monster group $\mathbb{M}$, where the problem of determining all the almost simple maximal subgroups is still open. In particular, the possibilities for (G, H) are known and [40] is a convenient reference. In addition, the groups with $b(G) \geqslant 3$ are listed in [9, Table 4].

First assume G is not the Baby Monster $\mathbb{B}$ nor the Monster $\mathbb{M}$. Here we first use the GAP Character Table Library [6] to identify the relevant groups with $\widehat{Q}(G) \geqslant 1/4$. Indeed, in each case the character table of G is available in [6] and we can use the `Maxes` function to access the character table of the maximal subgroup H. Moreover, [6] also stores the fusion map from H-classes to G-classes and this allows us to compute precise fixed point ratios and subsequently determine the exact value of $\widehat{Q}(G)$.

This reduces the problem to a small number of cases that require further attention. To handle these groups, we adopt the method described in Section 2.2 to compute $Q(G)$ precisely. First we use the function `AutomorphismGroupSimpleGroup` to construct G as a permutation group and we obtain H via the `MaximalSubgroups` function

G	Type of H	r	$Q(G)$
$\mathrm{L}_4(3)$	$\mathrm{O}_4^+(3)$	6	131/195
$\mathrm{L}_4(3).2_3$	$\mathrm{O}_4^+(3)$	3	131/195
$\mathrm{L}_4(3).2_2$	$\mathrm{O}_4^+(3)$	2	457/585
$\mathrm{L}_4(3).2_1 = \mathrm{PGL}_4(3)$	$\mathrm{O}_4^+(3)$	1	521/585
$\mathrm{L}_3(9).2^2$	$\mathrm{GL}_1(9) \wr S_3$	48	4093/12285
$\mathrm{L}_3(5)$	$\mathrm{GL}_1(5) \wr S_3$	30	199/775
$\mathrm{L}_3(5).2$	$\mathrm{GL}_1(5) \wr S_3$	13	1379/3875
	$\mathrm{GL}_1(5^3)$	13	791/2000
$\mathrm{L}_3(4).2 \neq \mathrm{P\Sigma L}_3(4)$	$\mathrm{GU}_3(2)$	1	17/35
$\mathrm{L}_3(4).6$	$\mathrm{GL}_1(4^3)$	5	11/32
$\mathrm{L}_3(4).S_3 = G_0.\langle\delta,\gamma\rangle$	$\mathrm{GL}_1(4^3)$	3	97/160
$\mathrm{L}_3(4).D_{12}$	$\mathrm{GL}_1(4^3)$	1	59/80
$\mathrm{L}_3(3)$	$\mathrm{GL}_1(3^3)$	2	11/24
	$\mathrm{O}_3(3)$	5	19/39
$\mathrm{L}_3(3).2$	$\mathrm{O}_3(3)$	2	23/39
$\mathrm{L}_2(17)$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	3	5/17
$\mathrm{L}_2(13).2$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	2	43/91
$\mathrm{L}_2(11).2$	$2_-^{1+2}.\mathrm{O}_2^-(2)$	1	31/55
$\mathrm{U}_4(5).2^2$	$\mathrm{GU}_1(5) \wr S_4$	409	361747/1421875
$\mathrm{U}_4(4)$	$\mathrm{GU}_1(4) \wr S_4$	80	259/884
$\mathrm{U}_4(4).2$	$\mathrm{GU}_1(4) \wr S_4$	30	1661/3536
$\mathrm{U}_4(4).4$	$\mathrm{GU}_1(4) \wr S_4$	15	1661/3536
$\mathrm{U}_4(3)$	$\mathrm{GU}_2(3) \wr S_2$	1	187/315
$\mathrm{U}_4(3).2 = \mathrm{U}_4(3).\langle\delta^2\phi\rangle$	$\mathrm{GU}_1(3) \wr S_4$	4	1811/2835
$\mathrm{U}_4(3).2^2 \neq \mathrm{U}_4(3).\langle\delta^2,\phi\rangle$	$\mathrm{GU}_1(3) \wr S_4$	1	2323/2835
$\mathrm{U}_4(3).4$	$\mathrm{GU}_1(3) \wr S_4$	1	2323/2835
$\mathrm{U}_3(9).2$	$\mathrm{GU}_1(9) \wr S_3$	40	1913/5913
$\mathrm{U}_3(9).4$	$\mathrm{GU}_1(9) \wr S_3$	20	1913/5913
$\mathrm{U}_3(8).2$	$\mathrm{GU}_1(8) \wr S_3$	78	1097/4256
$\mathrm{U}_3(8).S_3$	$\mathrm{GU}_1(8) \wr S_3$	19	205/448
$\mathrm{U}_3(8).6$	$\mathrm{GU}_1(8) \wr S_3$	25	2437/8512
$\mathrm{U}_3(8).(3 \times S_3)$	$\mathrm{GU}_1(8) \wr S_3$	6	2069/4256
$\mathrm{U}_3(7)$	$\mathrm{GU}_1(7) \wr S_3$	27	4381/14749
$\mathrm{U}_3(7).2$	$\mathrm{GU}_1(7) \wr S_3$	10	7069/14749
$\mathrm{U}_3(5).3$	$\mathrm{GU}_1(5) \wr S_3$	3	551/875
	$3^{1+2}.\mathrm{Sp}_2(3)$	5	67/175
$\mathrm{U}_3(5).S_3$	$\mathrm{GU}_1(5) \wr S_3$	1	659/875
	$3^{1+2}.\mathrm{Sp}_2(3)$	2	443/875
$\mathrm{U}_3(4)$	$\mathrm{GU}_1(4) \wr S_3$	1	133/208
$\mathrm{PSp}_6(3)$	$\mathrm{Sp}_2(3) \wr S_3$	1	853/1365
$\mathrm{Sp}_4(4).4$	$\mathrm{O}_2^-(4) \wr S_2$	2	103/153
$\mathrm{P\Omega}_8^+(3)$	$\mathrm{O}_4^+(3) \wr S_2$	12	45041/61425
$\mathrm{P\Omega}_8^+(3).2 = \mathrm{PSO}_8^+(3)$	$\mathrm{O}_4^+(3) \wr S_2$	4	151507/184275
$\mathrm{P\Omega}_8^+(3).2 = \mathrm{P\Omega}_8^+(3).\langle\gamma\rangle$	$\mathrm{O}_4^+(3) \wr S_2$	3	53233/61425
$\mathrm{P\Omega}_8^+(3).3$	$\mathrm{O}_4^+(3) \wr S_2$	3	16379/20475
$\mathrm{P\Omega}_8^+(3).2^2$	$\mathrm{O}_4^+(3) \wr S_2$	1	167891/184275
$\mathrm{P\Omega}_8^+(3).4$	$\mathrm{O}_4^+(3) \wr S_2$	2	151507/184275
$\mathrm{P\Omega}_8^+(3).S_4$	$\mathrm{O}_2^-(3) \wr S_4$	823	17810761/44778825
$\Omega_8^+(2).3$	$\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$	1	2071/2800
$\Omega_7(3)$	$\mathrm{O}_4^+(3) \perp \mathrm{O}_3(3)$	5	1945/2457
$\mathrm{SO}_7(3)$	$\mathrm{O}_4^+(3) \perp \mathrm{O}_3(3)$	1	11261/12285

TABLE 3. The groups in $\mathcal{G} \setminus \mathcal{L}$ with $Q(G) \geqslant 1/4$, part II

	G_0	Type of H
(a)	$G_2(3)$	$\mathrm{SL}_2(3)^2$
(b)	${}^3D_4(2)$	$3 \times \mathrm{SU}_3(2)$
(c)	${}^2F_4(2)'$	$\mathrm{SU}_3(2)$
(d)	$F_4(2)$	$\mathrm{SU}_3(2)^2$
(e)	${}^2E_6(2)$	$\mathrm{SU}_3(2)^3$
(f)	$E_8(2)$	$\mathrm{SU}_3(2)^4$

TABLE 4. The groups in $\mathcal{G} \setminus \mathcal{L}$, G_0 exceptional, $H \neq N_G(T)$

(for $G_0 = \mathrm{HN}$ and $H \cap G_0 = 5^{1+4}.2^{1+4}.5.4$ we construct H using the generators given in the Web Atlas [41]). Next we use `DoubleCosetRepresentatives` to construct a complete set R of (H, H) double coset representatives and this allows us to calculate $Q(G)$ via (3) and (6) (we thank Eamonn O'Brien for his assistance with this computation in the special case where $G_0 = \mathrm{HN}$ and $H \cap G_0 = 5^{1+4}.2^{1+4}.5.4$). In this way, we can read off the groups with $Q(G) \geqslant 1/4$ and they are recorded in Table 2.

Finally, suppose $G = \mathbb{B}$ or $\mathbb{M}$. If $G = \mathbb{B}$ then $H = [3^{11}].(S_4 \times 2S_4)$ or 47:23; in both cases we can use [6] and the `Maxes` function as above to show that $\widehat{Q}(G) < 1/4$. Similarly, if $G = \mathbb{M}$ then $H = 13^{1+2}{:}(3 \times 4S_4)$ or 41:40 and once again we can use [6] to verify the bound $\widehat{Q}(G) < 1/4$ (here we use `NamesOfFusionSources` in place of `Maxes` since the latter is not available for $\mathbb{M}$). □

3.2. EXCEPTIONAL GROUPS. Next let us turn to the groups in $\mathcal{G} \setminus \mathcal{L}$ where G_0 is an exceptional group of Lie type over $\mathbb{F}_q$ with $q = p^f$ for a prime p. As noted in the proof of [9, Proposition 7.1], the condition $b(G) = 2$ implies that H is a maximal rank subgroup (that is, H contains a maximal torus of G). More precisely, either $H = N_G(T)$ for some maximal torus T of G_0 (see [32, Table 5.2]), or (G, H) is one of the cases recorded in Table 4. Recall that $G_0 \neq {}^2G_2(3)' \cong \mathrm{L}_2(8)$ since $G \in \mathcal{G} \setminus \mathcal{L}$.

LEMMA 3.5. *The conclusion to Theorem* 3.1 *holds if G_0 is an exceptional group of Lie type and H is the normaliser of a maximal torus.*

Proof. The possibilities for H are recorded in [32, Table 5.2] and [18, Proposition 4.2] states that $b(G) = 2$ whenever H is the normaliser of a maximal torus (soluble or otherwise). We proceed by carefully inspecting the proof of [18, Proposition 4.2] in the relevant cases with H soluble.

If $G_0 = E_8(q)$ then one checks that the bound on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.3] is sufficient and we note that H is insoluble when $G_0 = E_7(q)$.

Next assume $G_0 = E_6^{\varepsilon}(q)$. Here the proof of [18, Lemma 4.11] yields $\widehat{Q}(G) < q^{-1}$ if $q \geqslant 5$, so we may assume $q \leqslant 4$ and

$$N_L(H_0) = (q^2 + \varepsilon q + 1)^3.3^{1+2}.\mathrm{SL}_2(3),$$

where $H_0 = H \cap G_0$, $L = \mathrm{Inndiag}(G_0)$ and $(q, \varepsilon) \neq (2, -)$. One checks that the upper bound on $\widehat{Q}(G)$ presented in the proof of [18, Lemma 4.11] is sufficient unless $\varepsilon = +$ and $q \leqslant 3$. If $q = 3$ then H does not contain any long root elements (see [18, Corollary 2.13], for example) and by bounding the contribution to $\widehat{Q}(G)$ from the remaining elements of prime order, as in the proof of [18, Lemma 4.11], we deduce that $\widehat{Q}(G) < 1/4$.

Now suppose $(q, \varepsilon) = (2, +)$. As explained in the proof of [18, Lemma 4.11], we can use MAGMA to construct H as a subgroup of $E_7(8)$ (see [17, Example 1.11] for the details). Let $i_m(H)$ denote the number of elements in H of order m. If $x \in H$ has odd prime order then $|x^G| > 2^{31} = b_1$ and we calculate that $i_3(H) = 11438$ and

$i_7(H) = 342$, so Lemma 2.1 implies that the contribution to $\widehat{Q}(G)$ from elements of odd prime order is less than a_1^2/b_1, where $a_1 = 11780$. Now assume $x \in H$ is an involution. We find that H_0 contains $a_2 = 441$ involutions, so the contribution from these elements is less than a_2^2/b_2, where $b_2 = 2^{21}$. Similarly, there are $a_3 = 406$ involutions $x \in H_0.2 \setminus H_0$, each of which acts on G_0 as a graph automorphism. Therefore $|x^G| > \frac{1}{3}2^{25} = b_3$ and we conclude that

$$\widehat{Q}(G) < \sum_{i=1}^{3} a_i^2/b_i < \frac{1}{4}. \tag{7}$$

Next assume $G_0 = F_4(q)$, so q is even and G contains graph automorphisms (see [32, Table 5.2]). By applying the bounds on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.15] we immediately reduce to the case $q = 2$. Here $G = F_4(2).2$ and we may assume $H = 7^2{:}(3 \times 2.S_4)$ is the normaliser of a Sylow 7-subgroup of G. The upper bound on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.15] is larger than $1/2$, but we can use Magma to construct G and H as permutation groups of degree 139776 (more precisely, we use `AutomorphismGroupSimpleGroup` to construct G and we find H by taking the normaliser of a Sylow 7-subgroup). Then by considering the fusion of H-classes in G we calculate that

$$\widehat{Q}(G) = \frac{541861}{29328998400}$$

and the result follows.

Now suppose $G_0 = G_2(q)$, so $p = 3$, $q \geqslant 9$ and G contains graph automorphisms (see [32, Table 5.2]). By arguing as in the proof of [18, Lemma 4.21] we reduce to the cases $q \in \{9, 27\}$. Suppose $q = 27$ and note that $|H_0| \leqslant 12(q+1)^2 = a_1$. Let $x \in H$ be an element of prime order. If $x \in H_0$ then $|x^G| \geqslant q^3(q^3-1)(q+1) = b_1$ (as noted in the proof of [18, Lemma 4.21]), whereas if x is a field automorphism then $|x^G| > q^{28/3} = b_2$ and H contains at most $a_2 = 24(q+1)^2$ such elements. Similarly, if x is an involutory graph automorphism then $|x^G| = q^3(q^3-1)(q+1) = b_3$ and there are at most $a_3 = 12(q+1)^2$ such elements in H. It is straightforward to check that (7) holds. Finally, suppose $q = 9$. First we use Magma to construct $G = G_2(9).4 = \mathrm{Aut}(G_0)$ as a permutation group of degree 132860 and we note that $H = N_G(K)$, where K is either a Sylow ℓ-subgroup of G_0 (with $\ell \in \{5, 13, 73\}$) or $K = C_8 \times C_8$. In each case, it is straightforward to construct H and verify the bound $\widehat{Q}(G) < 1/4$.

To complete the proof of the lemma, we may assume G_0 is one of the twisted groups ${}^3D_4(q)$, ${}^2F_4(q)'$, ${}^2G_2(q)$ ($q \geqslant 27$) or ${}^2B_2(q)$. First assume $G_0 = {}^3D_4(q)$, in which case there are three possibilities for H and one checks that the bound on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.24] is sufficient if $q \geqslant 9$. Suppose $q = 8$ and let $x \in H$ be an element of prime order, which implies that $x \in H_0.3$. Then $|x^G| > 8^{14} = b_1$ and $3|H_0| \leqslant 383688 = a_1$, whence $\widehat{Q}(G) < a_1^2/b_1 < 1/4$. The same conclusion holds when $q = 7$ since $|H| \leqslant 233928$ and $|x^G| > 7^{14}$ for all $x \in H$ of prime order. The remaining groups with $q \leqslant 5$ can be handled using Magma. In each case, we can use `AutomorphismGroupSimpleGroup` to construct G and we obtain H as the normaliser in G of an appropriate Sylow ℓ-subgroup of G_0. For example, if $q = 5$ then the three possibilities for H correspond to the primes $\ell \in \{7, 31, 601\}$. In every case, it is straightforward to verify the bound $\widehat{Q}(G) < 1/4$.

Next assume $G_0 = {}^2F_4(q)'$. The case $q = 2$ can be checked using Magma and we note that $Q(G) > 1/4$ when $H \cap G_0 = 5^2{:}4A_4$ (as recorded in Table 2). For $q \geqslant 8$, the upper bound on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.26] is sufficient (note that in the upper bound on $|H|$ given in the proof of this lemma, the $2\log q$ factor can be replaced

by $|\mathrm{Out}(G_0)| = \log q$). The case $G_0 = {}^2G_2(q)$ is very similar. Indeed, if $q \geqslant 3^5$ then the upper bound on $\widehat{Q}(G)$ in the proof of [15, Lemma 4.37] is good enough, while the case $q = 27$ can be handled using Magma, noting that $H = N_G(K)$ with K a Sylow ℓ-subgroup of G_0 for $\ell \in \{7, 19, 37\}$. Finally, let us assume $G_0 = {}^2B_2(q)$. If $q \geqslant 2^9$ then the bounds in the proof of [15, Lemma 4.39] are good enough. If $q = 2^7$ and $x \in H$ is a field automorphism of order 7 then $|x^G| > q^4$ and by arguing as in the proof of [15, Lemma 4.39] we deduce that $\widehat{Q}(G) < 1/4$. The remaining cases with $q \in \{8, 32\}$ can be checked using Magma and we find that $Q(G) < 1/4$ unless $q = 8$ and $H \cap G_0 = 13{:}4$. The latter case is recorded in Table 2. □

Proposition 3.6. *The conclusion to Theorem* 3.1 *holds if G_0 is an exceptional group of Lie type.*

Proof. In view of the previous lemma, we may assume G is one of the groups listed in Table 4. In cases (a), (b) and (c) we can use Magma to prove the result (we get $Q(G) < 1/4$ in cases (b) and (c), while $Q(G) \geqslant 1/4$ in (a)). In (d), the upper bound on $\widehat{Q}(G)$ in the proof of [18, Lemma 4.16] is insufficient. But as explained in [17, Example 1.4], we can use Magma to construct G and H and then it is straightforward to verify the bound $\widehat{Q}(G) < 1/4$.

Finally, let us consider cases (e) and (f). In (e) we observe that 2 and 3 are the only prime divisors of $|H|$ and we deduce that $\widehat{Q}(G) < 1/4$ by applying the relevant bounds presented in Case 1 in the proof of [18, Lemma 4.12]. Similarly, in case (f) we note that the only prime divisors of $|H|$ are 2 and 3. If x is a long root element, then

$$|x^G \cap H| = 4|y^L| = 36 = a_1, \;\; |x^G| > 2^{58} = b_1,$$

where y is a long root element in $L = \mathrm{SU}_3(2)$. If not, then $|x^G| > 2^{92} = b_2$ and we note that $|H| = 104485552128 = a_2$. By applying Lemma 2.1 we deduce that

$$\widehat{Q}(G) < a_1^2/b_1 + a_2^2/b_2 < \frac{1}{4}$$

and the result follows. □

In order to complete the proof of Theorem 3.1, we may assume G_0 is a classical group. It will be convenient to partition the proof into various subsections according to the socle G_0. The cases that we need to consider are recorded in the following result, which is an immediate consequence of [31] and [9, Theorem 2].

Theorem 3.7. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G} \setminus \mathcal{L}$ with socle G_0 classical and point stabiliser H. Then (G, H) is one of the cases in Table* 5.

Note that in the final column of Table 5 we list necessary conditions for the existence of a group in $\mathcal{G} \setminus \mathcal{L}$ with the given socle and point stabiliser. In general, these conditions are not sufficient and we refer the reader to [5, 28] and [9] for a precise description of the conditions that are needed to ensure that G has a maximal subgroup of the given type and a base of size 2. We also refer the reader to [10, Chapter 3] for detailed information on the conjugacy classes of elements of prime order in G.

3.3. Linear groups. In this section we assume $G_0 = \mathrm{L}_n(q)$. Recall that the condition $G \notin \mathcal{L}$ implies that $q \geqslant 11$ if $n = 2$, and $q \geqslant 3$ if $n = 3$.

Proposition 3.8. *The conclusion to Theorem* 3.1 *holds if $G_0 = \mathrm{L}_n(q)$.*

Proof. First assume n is a prime and H is of type $\mathrm{GL}_1(q^n)$. By applying the upper bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.4] we immediately reduce to the cases where $(n, q) = (7, 2)$, or $n = 5$ and $q \leqslant 5$, or $n = 3$ and $q \leqslant 19$. With the aid of Magma, it is straightforward to compute $Q(G)$ precisely in each of these cases and

G_0	Type of H	Conditions
$\mathrm{L}_n(q)$	$\mathrm{GL}_1(q^n)$	$n \geqslant 3$ prime, $G \neq \mathrm{L}_3(3).2$
	$\mathrm{GL}_2(q) \wr S_{n/2}$	$n \in \{6,8\}$, $q = 3$
	$\mathrm{GL}_1(q) \wr S_n$	$n \in \{3,4\}$, $q \geqslant 5$
	$\mathrm{O}_4^+(q)$	$(n,q) = (4,3)$, $G \neq \mathrm{Aut}(G_0)$
	$\mathrm{O}_3(q)$	$(n,q) = (3,3)$
	$3^{1+2}.\mathrm{Sp}_2(3)$	$n = 3$, $p = q \equiv 1 \pmod 3$
	$\mathrm{GL}_2(3)$	$n = 2$, $q = 3^f$, $f \geqslant 3$ prime
	$2_-^{1+2}.\mathrm{O}_2^-(2)$	$n = 2$, $q = p \geqslant 11$
$\mathrm{U}_n(q)$	$\mathrm{GU}_1(q^n)$	$n \geqslant 3$ prime
	$\mathrm{GU}_1(q) \wr S_n$	$n \in \{3,4\}$, $q \geqslant 3$, $(n,q) \neq (3,3)$
	$\mathrm{GU}_2(q) \wr S_{n/2}$	$n \in \{4,6,8\}$, $q = 3$
	$\mathrm{GU}_3(q) \wr S_{n/3}$	$n \in \{9,12\}$, $q = 2$
	$3^{1+2}.\mathrm{Sp}_2(3)$	$n = 3$, $q = p \equiv 2 \pmod 3$
	$\mathrm{GU}_3(2)$	$n = 3$, $q = 2^f$, $f \geqslant 3$ prime
$\mathrm{PSp}_n(q)$	$\mathrm{Sp}_2(q) \wr S_{n/2}$	$n \in \{6,8\}$, $q = 3$
	$\mathrm{O}_2^\epsilon(q) \wr S_2$	$(n,p) = (4,2)$, $q \geqslant 4$
	$\mathrm{O}_2^-(q^2)$	$(n,p) = (4,2)$, $q \geqslant 4$
$\mathrm{P}\Omega_n^+(q)$	$\mathrm{O}_4^+(q) \wr S_{n/4}$	$n \in \{12,16\}$, $q = 3$
	$\mathrm{O}_4^+(q) \wr S_2$	$(n,q) = (8,3)$, $\lvert G : G_0 \rvert < 6$
	$\mathrm{O}_2^\epsilon(q) \wr S_4$	$n = 8$, $q \geqslant 3$
	$\mathrm{O}_2^-(q) \times \mathrm{GU}_3(q)$	$(n,q) = (8,2)$, $G = G_0.3$
	$\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$	$n = 8$
$\Omega_n(q)$	$\mathrm{O}_4^+(q) \perp \mathrm{O}_3(q)$	$(n,q) = (7,3)$

TABLE 5. The groups in $\mathcal{G} \setminus \mathcal{L}$ with G_0 classical

the result quickly follows (note that the condition $b(G) = 2$ implies that $G \neq \mathrm{L}_3(3).2$). In particular, we find that $Q(G) \geqslant 1/4$ only if $n = 3$ and $q \leqslant 5$ (the precise exceptions are recorded in Table 3).

Next assume $n \in \{3,4\}$, $q \geqslant 5$ and H is of type $\mathrm{GL}_1(q) \wr S_n$. First assume $n = 3$. By inspecting the proof of [9, Lemma 6.5] we deduce that $\widehat{Q}(G) < 1/4$ if $q \geqslant 43$. If $29 \leqslant q \leqslant 41$ then G does not contain field automorphisms of order 2 or 3, nor graph-field automorphisms of order 2, so we may set $a_8 = a_9 = 0$ in the bound on $\widehat{Q}(G)$ presented in the proof of [9, Lemma 6.5]. One checks that this modified bound yields $\widehat{Q}(G) < 1/4$. For $7 \leqslant q \leqslant 27$ we can use MAGMA to show that $Q(G) < 1/4$ in the usual manner, with the single exception of the case $G = \mathrm{Aut}(G_0)$ with $q = 9$, where $Q(G) = 4093/12285$. Finally, for $q = 5$ we calculate that $Q(G) = 199/775$ if $G = G_0$, otherwise $Q(G) = 1379/3875$; both cases are recorded in Table 3. Similarly, if $n = 4$ then the result follows by combining explicit MAGMA computations for $q \in \{5,7,8\}$ with the upper bound on $\widehat{Q}(G)$ presented in the proof of [9, Lemma 6.6] for $q \geqslant 9$ (in every case we get $Q(G) < 1/4$). The case where $n = 3$ and H is of type $3^{1+2}.\mathrm{Sp}_2(3)$ is entirely similar, working with the bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.11].

Now let us turn to the relevant groups with $G_0 = \mathrm{L}_2(q)$. If $q = 3^f$ with $f \geqslant 3$ a prime and H is a subfield subgroup of type $\mathrm{GL}_2(3)$, then the bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 4.9] is sufficient if $f \geqslant 7$, while the cases $f \in \{3,5\}$ are easily checked using MAGMA. Similarly, if $q = p \geqslant 11$ and H is of type $2_-^{1+2}.\mathrm{O}_2^-(2)$ then the bound in the proof of [9, Lemma 4.10] is good enough if $q \geqslant 71$ and we can use MAGMA to handle the cases with $q < 71$.

There are four remaining cases to consider. If $G_0 = \mathrm{L}_3(3)$ with H of type $\mathrm{O}_3(3)$ then we compute $Q(G) = 19/39$ if $G = G_0$, whereas $Q(G) = 23/39$ for $G = G_0.2$. Next suppose $G_0 = \mathrm{L}_4(3)$ and H is of type $\mathrm{O}_4^+(3)$. Here the condition $b(G) = 2$ implies that $G \neq \mathrm{Aut}(G_0)$ and using Magma one checks that $Q(G) > 1/4$ in each case (the precise value of $Q(G)$ is recorded in Table 3). The case $G_0 = \mathrm{L}_6(3)$ with H of type $\mathrm{GL}_2(3) \wr S_3$ can be handled using Magma, working with the function `MaximalSubgroups` to construct H. Finally, suppose $G_0 = \mathrm{L}_8(3)$ and H is of type $\mathrm{GL}_2(3) \wr S_4$. Here the `MaximalSubgroups` function is ineffective, but we can construct H by observing that $H = N_G(K)$ with $|K| = 2^{11}$, as noted in the proof of [9, Proposition 6.3] (also see [9, Example 2.4]). It is straightforward to check that $\widehat{Q}(G) < 1/4$. □

3.4. Unitary groups.

Proposition 3.9. *The conclusion to Theorem* 3.1 *holds if* $G_0 = \mathrm{U}_n(q)$ *with* $n \geqslant 3$.

Proof. First assume n is a prime and H is of type $\mathrm{GU}_1(q^n)$. For $n \geqslant 5$, one checks that the upper bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.4] is sufficient unless $n = 5$ and $q \leqslant 5$. Suppose $n = 5$, so $q \geqslant 3$ by the maximality of H. If $q = 5$ then it is easy to improve the given bound in [9] in order to show that $\widehat{Q}(G) < 1/4$ (for example, we can use the fact that $|H| \leqslant 10(5^5 + 1)/6$). For $q = 4$ we observe that $H = N_G(K)$, where K is a Sylow 41-subgroup of G, so it is straightforward to construct H in Magma and verify the bound $\widehat{Q}(G) < 1/4$ (note that it suffices to check this for $G = \mathrm{Aut}(G_0)$). The case $q = 3$ can also be checked using Magma (using `MaximalSubgroups` to construct H, or noting that H is the normaliser of a Sylow 61-subgroup). Similarly, if $n = 3$ then $q \geqslant 4$ and the bound in the proof of [9, Lemma 6.4] is sufficient for $q \geqslant 23$ (for $q = 32$, we note that $|x^G| \geqslant |G_0 : \mathrm{U}_3(2)|$ if x is a field automorphism of order 5); the remaining cases with $q \leqslant 19$ can be verified using Magma.

Next suppose $G_0 = \mathrm{U}_3(q)$ and H is of type $\mathrm{GU}_1(q) \wr S_3$ with $q \geqslant 4$. For $q \geqslant 43$ it is easy to check that the upper bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.5] is sufficient. The same estimates are also good enough when $29 \leqslant q \leqslant 41$, noting that in each case G does not contain any field or graph-field automorphisms of order 2 or 3. For $11 \leqslant q \leqslant 27$ we can use Magma to verify the bound $\widehat{Q}(G) < 1/4$. We find that there are examples with $Q(G) \geqslant 1/4$ when $q \leqslant 9$; they are easily identified using Magma and they are recorded in Table 3. The case where $G_0 = \mathrm{U}_4(q)$ and H is of type $\mathrm{GU}_1(q) \wr S_4$ is similar. Here $q \geqslant 3$ and the bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.5] is good enough for $q \geqslant 9$. If $q \in \{7, 8\}$ then one can check that $Q(G) < 1/4$ using Magma. In the same way, we find that there are exceptions to this bound when $q \in \{3, 4, 5\}$ and each of these cases is listed in Table 3.

Next assume $n \in \{4, 6, 8\}$, $q = 3$ and H is of type $\mathrm{GU}_2(q) \wr S_{n/2}$. If $n = 4$ then $G = G_0$ is the only group with $b(G) = 2$ (see [9, Table 7]) and with the aid of Magma we calculate that $Q(G) = 187/315$. Next assume $n = 6$. Here $H = N_G(K)$ for some subgroup K of G_0 of order 2^{10} and it is straightforward to check that $\widehat{Q}(G) < 1/4$ (see [9, Example 2.4] and the proof of [9, Proposition 6.3]). Similarly, if $n = 8$ then $H = N_G(K)$ with $|K| = 2^{13}$ and once again one checks that $\widehat{Q}(G) < 1/4$. (Note that in both cases, it suffices to check the bound for $G = \mathrm{Aut}(G_0)$.)

Now assume $n \in \{9, 12\}$, $q = 2$ and H is of type $\mathrm{GU}_3(q) \wr S_{n/3}$. As noted in the proof of [9, Proposition 6.3], if $n = 9$ then $H = N_G(K)$ with $|K| = 3^8$ and we can use Magma to verify the bound $\widehat{Q}(G) < 1/4$.

For $n = 12$ we find that the bound presented in the proof of [9, Proposition 6.3] does not give $\widehat{Q}(G) < 1/4$ and a more accurate estimate is required. To do this, it

suffices to improve the upper bound on the contribution to $\widehat{Q}(G)$ from elements of order 3.

As in the proof of [9, Proposition 6.3], we may view H as the stabiliser in G of an orthogonal decomposition

$$V = V_1 \perp V_2 \perp V_3 \perp V_4$$

of the natural module, where each V_i is a nondegenerate 3-space. Suppose $x \in H$ has order 3. If some conjugate of x induces a nontrivial permutation of the V_i, then $|x^G| > 2^{89} = b_1$ and we note that $|H| < 2^{42} = a_1$. Following the argument in [9], the contribution from the remaining elements of order 3 in H with $|x^G| > 2^{69} = b_2$ is less than a_2^2/b_2, where $a_2 = 2^{31}$. As explained in the proof of [9, Proposition 6.3], the contribution from the elements with $|x^G| \leqslant 3.2^{62}$ is less than $2\sum_{i=3}^{7} a_i^2/b_i$, where the integers a_i and b_i are defined as in the proof in [9]. Finally, if $3.2^{62} < |x^G| \leqslant 2^{69}$ then one can check that x is of the form $[I_8, \omega I_4]$, where $\omega \in \mathbb{F}_4$ is a primitive cube root of unity. Here we calculate

$$|x^G \cap H| \leqslant 2\binom{4}{2}m + \binom{4}{2}m^2 + 2\binom{4}{2}m^3 + m^4 = 42480 = a_0$$

where $m = \frac{1}{3}|\mathrm{GU}_3(2) : \mathrm{GU}_2(2)| = 12$. Therefore, the contribution to $\widehat{Q}(G)$ from elements of order 3 is less than

$$a_1^2/b_1 + a_2^2/b_2 + 2\left(a_0^2/b_0 + \sum_{i=3}^{7} a_i^2/b_i\right) < \frac{1}{20}$$

where $b_0 = 3.2^{62}$. Finally, the estimates in the proof of [9, Proposition 6.3] imply that the contribution to $\widehat{Q}(G)$ from involutions is also less than $1/20$ and the result follows.

To complete the proof of the proposition, we may assume $n = 3$ and either $q = p \equiv 2 \pmod 3$ and H is of type $3^{1+2}.\mathrm{Sp}_2(3)$, or $q = 2^f$ with $f \geqslant 3$ a prime and H is a subfield subgroup of type $\mathrm{GU}_3(2)$. Suppose H is of type $3^{1+2}.\mathrm{Sp}_2(3)$. Here the proof of [9, Lemma 6.11] gives the result for $q > 29$ and we can use Magma to handle the cases with $q \leqslant 29$, noting that there are exceptions to the bound $Q(G) < 1/4$ when $q = 5$ (as recorded in Table 3). Finally, let us assume H is of type $\mathrm{GU}_3(2)$, so $q = 2^f$ with $f \geqslant 3$ odd. If $f \geqslant 7$ then the bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.10] is sufficient, while the cases with $f \in \{3, 5\}$ can be handled using Magma. □

3.5. Symplectic groups. Next assume $G_0 = \mathrm{PSp}_n(q)$ with $n \geqslant 4$. Recall that $(n, q) \neq (4, 2)$ since $G \notin \mathcal{L}$.

Proposition 3.10. *The conclusion to Theorem* 3.1 *holds if* $G_0 = \mathrm{PSp}_n(q)$ *with* $n \geqslant 4$.

Proof. First assume $n \in \{6, 8\}$, $q = 3$ and H is of type $\mathrm{Sp}_2(q) \wr S_{n/2}$. If $n = 6$ then the condition $b(G) = 2$ implies that $G = G_0$ and using Magma we calculate that $Q(G) = 853/1365$, so this case is listed in Table 3. For $n = 8$ we use the functions `AutomorphismGroupSimpleGroup` and `MaximalSubgroups` to construct G and H, and we apply `DoubleCosetCanonical` to establish the existence of sufficiently many regular H-orbits in order to force $Q(G) < 1/4$ (see (3)). Indeed, for $G = G_0$ we get $r \geqslant 3113$, while $r \geqslant 1557$ for $G = G_0.2$.

Finally let us assume $G_0 = \mathrm{Sp}_4(q)$ with $q \geqslant 4$ even and H of type $\mathrm{O}_2^{\epsilon}(q) \wr S_2$ or $\mathrm{O}_2^{-}(q^2)$. Here H is maximal only if G contains graph automorphisms and with the aid of Magma one checks that if $q \leqslant 2^5$ then either $\widehat{Q}(G) < 1/4$ or $q = 4$, $G = \mathrm{Aut}(G_0)$ and H is of type $\mathrm{O}_2^{-}(q) \wr S_2$. In the latter case we have $Q(G) = 103/153$ as recorded in Table 3. For the remainder, we may assume $q \geqslant 2^6$.

Suppose H is of type $\mathrm{O}_2^{\epsilon}(q) \wr S_2$, so $H_0 = (C_{q-\varepsilon})^2{:}D_8$. By applying the upper bound in the proof of [9, Lemma 6.9], we deduce that $\widehat{Q}(G) < 1/4$ if $q \neq 2^7$. So

let us assume $q = 2^7$ and write $\widehat{Q}(G) = \alpha_1 + \alpha_2$, where α_1 is the contribution from involutory graph automorphisms. The proof of [9, Lemma 6.9] gives $\alpha_2 < 2^{-6}$, so it remains for us to estimate α_1. If $\varepsilon = -$ then $H \leqslant (C_{129})^2{:}(SD_{16} \times C_7)$ and it follows that every involution in H is contained in $H \cap G_0 = (C_{129})^2{:}D_8$, whence $\alpha_1 = 0$ and the result follows. Now assume $\varepsilon = +$, so $H \leqslant (C_{127})^2{:}(D_{16} \times C_7)$. Since there are exactly 4 involutions in $D_{16} \setminus D_8$, we deduce that $\alpha_1 \leqslant d^2/b$ with $d = 4.127^2$ and $b = |G_0 : {}^2B_2(q)| = 34626060288$. One checks that the resulting bound on $\widehat{Q}(G)$ is good enough.

To complete the proof, let us assume $q \geqslant 2^6$ and H is of type $\mathrm{O}_2^-(q^2)$, so

$$H_0 = \mathrm{O}_2^-(q^2).2 = C_{q^2+1}{:}C_4$$

and we will estimate the contribution to $\widehat{Q}(G)$ from the various elements of prime order (the details in this case were omitted in the proof of [9, Lemma 6.9]). First let $x \in H$ be a unipotent involution. Then x embeds in G as an involution of type c_2 (in the notation of Aschbacher and Seitz [2]), whence

$$|x^G \cap H| = i_2(H_0) = q^2 + 1 = a_1, \;\; |x^G| = (q^2-1)(q^4-1) = b_1.$$

If x is semisimple, then $|x^G| \geqslant |\mathrm{Sp}_4(q) : \mathrm{GU}_1(q^2)| = q^4(q^2-1)^2 = b_2$ and we note that there are at most $a_2 = q^2 + 1$ such elements in H. Next suppose x is a field automorphism of odd order. Then $|x^G| > q^{20/3} = b_3$ and H contains fewer than $4(q^2+1)\log q = a_3$ such elements. Finally, suppose x is an involutory field or graph automorphism (note that G cannot contain elements of both types). If $\log q$ is even then every involution in H is contained in H_0, so we may assume $\log q$ is odd and x is a graph automorphism. Then $|x^G| = q^2(q+1)(q^2-1) = b_4$ and we note that $|x^G \cap H| \leqslant |H_0| = 4(q^2+1) = a_4$. Therefore, by applying Lemma 2.1 we deduce that

$$\widehat{Q}(G) < \sum_{i=1}^{3} a_i^2/b_i + \alpha a_4^2/b_4,$$

where $\alpha = 1$ if $\log q$ is odd, otherwise $\alpha = 0$, and we conclude that $\widehat{Q}(G) < 1/4$. □

3.6. Orthogonal groups. In order to complete the proof of Theorem 3.1, we may assume $G_0 = \mathrm{P}\Omega_n^\varepsilon(q)$ with $n \geqslant 7$.

Proposition 3.11. *The conclusion to Theorem* 3.1 *holds if* $G_0 = \mathrm{P}\Omega_n^\varepsilon(q)$ *with* $n \geqslant 7$.

Proof. By inspecting Table 5 we observe that either n is even and $\varepsilon = +$, or $(n,q) = (7,3)$. First assume $n \in \{12, 16\}$, $q = 3$ and H is of type $\mathrm{O}_4^+(q) \wr S_{n/4}$. For $n = 16$, the upper bound in the proof of [9, Proposition 6.3] gives $\widehat{Q}(G) < 1/4$. On the other hand, if $n = 12$ then we can construct G and H in Magma (see [9, Example 2.4]) and it is straightforward to check that $\widehat{Q}(G) < 1/4$. The relevant cases with $G_0 = \Omega_7(3)$ or $\Omega_8^+(2)$ can also be handled using Magma and the exceptions with $Q(G) \geqslant 1/4$ are recorded in Table 3.

To complete the proof, we may assume $G_0 = \mathrm{P}\Omega_8^+(q)$ with $q \geqslant 3$. Suppose $q = 3$ and H is of type $\mathrm{O}_4^+(3) \wr S_2$, noting that $|G : G_0| < 6$ since $b(G) = 2$. Even though $|G : H| = 14926275$ is large, we can still analyse this case in the usual way using Magma, working with a set of (H,H) double coset representatives to compute r (and hence $Q(G)$) via (6). The results are presented in Table 3.

Next assume H is of type $\mathrm{O}_2^{\varepsilon'}(q) \wr S_4$. If $q \in \{3,4\}$ then $\varepsilon' = -$ and using Magma one can check that either $Q(G) < 1/4$, or $q = 3$, $G = \mathrm{Aut}(G_0)$, $r = 823$ and

$$Q(G) = \frac{17810761}{44778825}.$$

For example, if $q = 3$ and $G = G_0.A_4$ then using `DoubleCosetCanonical` we can verify the bound $r \geqslant 3075$, which forces $Q(G) < 1/4$. We thank Eamonn O'Brien for his assistance with the precise calculation of r when $G = \mathrm{Aut}(G_0)$. For $q \geqslant 5$, we seek to apply the upper bound on $\widehat{Q}(G)$ presented in the proof of [9, Lemma 6.7]. If $q \geqslant 9$ then

$$\widehat{Q}(G) < 2q^{-1} + q^{-2} + q^{-3} + q^{-7} < \frac{1}{4}$$

and the result follows. One can check that the bounds in the proof of [9, Lemma 6.7] are also sufficient when $q \in \{7, 8\}$, so we may assume $q = 5$. Here we have $H = N_G(K)$, where $K < G_0$ has order 2^9 if $\varepsilon' = +$, otherwise $|K| = 3^4$. We now construct H as in [9, Example 2.4] and one checks that $\widehat{Q}(G) < 1/4$.

Finally, let us assume H is of type $\mathrm{O}_2^-(q^2) \times \mathrm{O}_2^-(q^2)$ with $q \geqslant 3$. If $q \geqslant 11$ then the upper bound on $\widehat{Q}(G)$ in the proof of [9, Lemma 6.8] is sufficient. On the other hand, if $q \leqslant 9$ then we can construct H in Magma, noting that $H = N_G(K)$ with K a Sylow ℓ-subgroup of G_0 and ℓ an odd prime divisor of $q^2 + 1$. In this way, it is straightforward to check that $\widehat{Q}(G) < 1/4$ and the result follows. □

This completes the proof of Theorem 3.1.

4. Two-dimensional linear groups

In this section we turn to the groups in $\mathcal{L}$, so $G_0 = \mathrm{L}_2(q)$, $q \geqslant 4$ and H is of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$. Note that these special cases coincide with the $\mathcal{C}_2$-actions and $\mathcal{C}_3$-actions of G, respectively, where a point stabiliser H is a maximal subgroup of G in the collection labelled $\mathcal{C}_i$ in Aschbacher's subgroup structure theorem [1]. The goal of this section is to establish our main theorems in these cases (we will handle Theorem 1.5 in Section 6.2).

Recall that $\Sigma(G)$ denotes the Saxl graph of G. A key ingredient in our proof of Theorem 1.1 for the groups in $\mathcal{L}$ is the following recent result of Chen and Du [19].

Theorem 4.1 (Chen & Du, [19]). *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive group with socle $G_0 = \mathrm{L}_2(q)$ and $b(G) = 2$. Then $\Sigma(G)$ has diameter 2.*

This establishes a special case of a conjecture in [11], which asserts that $\Sigma(G)$ has diameter at most 2 for every finite primitive permutation group G with $b(G) = 2$. In fact, [11, Conjecture 4.5] states that the following even stronger property holds in this general setting:

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour.*

In view of Theorem 4.1, in order to establish this for the groups we are considering in this section, it suffices to show that if $\{\alpha, \beta\}$ is a base for G, then there exists $\gamma \in \Omega$ such that $\{\alpha, \gamma\}$ and $\{\beta, \gamma\}$ are bases.

Let us fix some notation. Let V be the natural module for G_0 and write $q = p^f$, where p is a prime. Fix a basis $\{e_1, e_2\}$ for V and write $\mathbb{F}_q^\times = \langle \mu \rangle$. Let $\delta \in \mathrm{PGL}_2(q)$ be the image (modulo scalars) of the diagonal matrix $\mathrm{diag}(\mu, 1) \in \mathrm{GL}_2(q)$, which induces a diagonal automorphism on G_0. Similarly, let ϕ be a field automorphism of order f such that $(ae_1 + be_2)^\phi = a^p e_1 + b^p e_2$ for all $a, b \in \mathbb{F}_q$ and note that

$$\mathrm{Aut}(G_0) = \langle G_0, \delta, \phi \rangle$$

and $\mathrm{P\Sigma L}_2(q) = \langle G_0, \phi \rangle$. For $g \in \mathrm{Aut}(G_0)$, if we write $\ddot{g}$ for the coset $G_0 g$, then

$$\mathrm{Out}(G_0) = \{\ddot{g} : g \in \mathrm{Aut}(G_0)\} = \langle \ddot{\delta} \rangle \times \langle \ddot{\phi} \rangle = C_{(2,q-1)} \times C_f.$$

As before, if H is a subgroup of G, then we set $H_0 = H \cap G_0$.

It is convenient to use computational methods to handle the cases where q is small. To this end, we present the following result. Note that $\mathrm{L}_2(9).2 = \mathrm{M}_{10}$ in part (ii)(b). Also recall that we write $\omega(G)$ for the clique number of $\Sigma(G)$.

PROPOSITION 4.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a finite almost simple primitive group with socle $G_0 = \mathrm{L}_2(q)$ and point stabiliser H of type $\mathrm{GL}_1(q) \wr S_2$ or $\mathrm{GL}_1(q^2)$. If $b(G) = 2$ and $q \leqslant 27$, then the following hold:*

(i) *Property $(\star)$ holds.*
(ii) *G has a unique regular suborbit if and only if one of the following holds:*
  (a) *$G = \mathrm{PGL}_2(q)$, $q \geqslant 4$, $q \neq 5$ and $H = D_{2(q-1)}$; or*
  (b) *$(G, H) = (\mathrm{L}_2(5), D_6)$ or $(\mathrm{L}_2(9).2, 5{:}4)$.*
(iii) *$\omega(G) \geqslant 4$, with equality if and only if $G = \mathrm{L}_2(4) \cong \mathrm{L}_2(5)$ and $H = D_6$.*

Proof. To verify $(\star)$, we proceed as in Section 5, working with the MAGMA functions `AutomorphismGroupSimpleGroup` and `MaximalSubgroups` to construct G and H. We then use `DoubleCosetRepresentatives` to determine a set R of (H, H) double coset representatives and for each $x \in R$ we find an element $y \in G$ such that $H \cap H^y = H^x \cap H^y = 1$, which establishes $(\star)$. In the same way, we can count the number of elements $x \in R$ with $|HxH| = |H|^2$, which coincides with the number of regular suborbits of G (the existence of a unique regular suborbit in (ii)(a) was noted in [11, Example 2.5]). Finally, we can use the MAGMA code presented in Section 6.1 to verify the bound on $\omega(G)$ in part (iii). □

4.1. $\mathcal{C}_2$-ACTIONS. Here H is of type $\mathrm{GL}_1(q) \wr S_2$, so $H_0 = D_{2(q-1)/h}$ and $|\Omega| = \frac{1}{2}q(q+1)$, where $h = (2, q-1)$. We may identify $\Omega = G/H$ with the set of unordered pairs of distinct 1-dimensional subspaces of the natural module V for G_0. The maximality of H implies that $q \geqslant 4$ and $q \neq 5$ (see [5, Table 8.1], for example); in view of Proposition 4.2, we may assume that $q > 27$. By [9, Lemma 4.7] we have $b(G, H) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) < G$.

As noted in [11, Example 2.5], if $G = \mathrm{PGL}_2(q)$ then $\Sigma(G)$ is isomorphic to the *Johnson graph* $J(q+1, 2)$; the vertices of this graph correspond to the 2-element subsets of a set of size $q+1$, with two vertices joined by an edge if they have nonempty intersection. This observation immediately implies that $(\star)$ holds, G has a unique regular suborbit and $\Sigma(G)$ has clique number q. Therefore, for the remainder of this section we will assume that q is odd and $G \cap \mathrm{PGL}_2(q) = G_0$. Then as noted in the proof of [9, Lemma 4.7], this implies that one of the following holds:

(a) $G = \langle G_0, \phi^j \rangle$ for some j in the range $0 \leqslant j < f$; or
(b) $G = \langle G_0, \delta\phi^j \rangle$ with $0 < j < f$ and $f/(f, j)$ even.

Set $\alpha, \beta \in \Omega$, where $\alpha = \{\langle e_1 \rangle, \langle e_2 \rangle\}$ and $\beta = \{\langle u \rangle, \langle v \rangle\}$. Let us assume q is odd and suppose $G = \mathrm{P\Sigma L}_2(q) = \langle G_0, \phi \rangle$. Notice that if $u = e_1$ and $v = be_1 + e_2$, then α and β are fixed by the image in G of an element

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \phi \in \langle \mathrm{SL}_2(q), \phi \rangle$$

with $a^2 = b^{p-1}$. Similarly, the pointwise stabiliser of $\{\alpha, \beta\}$ is nontrivial if $u = e_2$. Therefore, $\{\alpha, \beta\}$ is a base for G only if $\langle u \rangle = \langle e_1 + be_2 \rangle$ and $\langle v \rangle = \langle e_1 + ce_2 \rangle$ for distinct nonzero scalars $b, c \in \mathbb{F}_q$.

In Lemma 4.4 below we present necessary and sufficient conditions on the scalars b and c to ensure that $\{\alpha, \beta\}$ is a base for $\mathrm{P\Sigma L}_2(q)$. To do this, we need the following more general result. Note that the condition in part (iii) is equivalent to the non-containment of bc^{-1} in a proper subfield of $\mathbb{F}_q$.

Lemma 4.3. *Suppose $G \cap \mathrm{PGL}_2(q) = G_0$ with q odd and set*

$$\alpha = \{\langle e_1\rangle, \langle e_2\rangle\}, \quad \beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$$

with $b \neq c$. Then $\{\alpha, \beta\}$ is a base for G if the following conditions are satisfied:

(i) *$bc \neq 0$;*
(ii) *$-bc^{-1}$ is a non-square in $\mathbb{F}_q$; and*
(iii) *$b^{p^k-1} \neq c^{p^k-1}$ for all $0 < k < f$.*

Proof. Suppose b and c satisfy the three given conditions and let us assume

$$x = AB^i\phi^j \in \langle \mathrm{GL}_2(q), \phi\rangle$$

fixes α and β, where $A \in \mathrm{SL}_2(q)$, $B = \mathrm{diag}(\mu, 1)$, $0 \leqslant i < q-1$ and $0 \leqslant j < f$, with $j > 0$ if $i > 0$. It suffices to show that $x = \pm I_2$. Since x fixes α, the matrix of A with respect to the basis $\{e_1, e_2\}$ is either diagonal or anti-diagonal.

First assume x fixes the two 1-spaces comprising α, so $A = \mathrm{diag}(a, a^{-1})$ is diagonal. If x also fixes the two spaces in β, then

$$(e_1 + be_2)^x = a\mu^i e_1 + a^{-1}b^{p^j}e_2 = \eta_1(e_1 + be_2)$$
$$(e_1 + ce_2)^x = a\mu^i e_1 + a^{-1}c^{p^j}e_2 = \eta_2(e_1 + ce_2)$$

for some $\eta_1, \eta_2 \in \mathbb{F}_q^\times$. Therefore

$$a^2\mu^i = b^{p^j-1} = c^{p^j-1} \tag{8}$$

and thus (iii) implies that $j = 0$, so $i = 0$ and $a^2 = 1$, which gives $x = \pm I_2$ as required. Similarly, if x interchanges the spaces in β, then

$$a^2\mu^i = b^{p^j}c^{-1} = c^{p^j}b^{-1}. \tag{9}$$

Here $b^{p^{2j}-1} = c^{p^{2j}-1}$, so (iii) implies that $2j = 0$ or f. Suppose $2j = 0$, so $i = 0$ and $a^2 = bc^{-1} = cb^{-1}$ and thus $bc^{-1} = \pm 1$. But $b \neq c$, so $bc^{-1} = -1$, which is incompatible with (ii). Now assume $2j = f$, so $q \equiv 1 \pmod 4$ and -1 is a square in $\mathbb{F}_q$. In addition, (9) gives $(bc^{-1})^{p^{f/2}+1} = 1$, so $bc^{-1} \in \langle \mu^{p^{f/2}-1}\rangle$ and thus bc^{-1} is a square. Therefore, $-bc^{-1}$ is a square, which once again is incompatible with (ii).

Now assume $A = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$ is anti-diagonal. If x fixes both spaces in β then

$$(e_1 + be_2)^x = ab^{p^j}e_1 - a^{-1}\mu^i e_2 = \eta_1(e_1 + be_2)$$
$$(e_1 + ce_2)^x = ac^{p^j}e_1 - a^{-1}\mu^i e_2 = \eta_2(e_1 + ce_2)$$

for some $\eta_1, \eta_2 \in \mathbb{F}_q^\times$. This gives

$$-a^2\mu^{-i} = b^{-p^j-1} = c^{-p^j-1}. \tag{10}$$

Here $b^{p^{2j}-1} = c^{p^{2j}-1}$ and thus $2j = 0$ or f by (iii). If $2j = 0$ then $i = 0$ and $-a^2 = b^{-2} = c^{-2}$, which implies that $bc^{-1} = \pm 1$. As noted above, this is incompatible with (ii). Now assume $2j = f$, so $q \equiv 1 \pmod 4$ and -1 is a square in $\mathbb{F}_q$ once again. Then (10) gives $(bc^{-1})^{p^{f/2}+1} = 1$ and as above we deduce that bc^{-1} is a square. Hence, $-bc^{-1}$ is also a square, which contradicts (ii).

Finally, suppose A is anti-diagonal as above and assume x interchanges the 1-spaces in β. Here we get

$$-a^2\mu^{-i} = b^{-p^j}c^{-1} = c^{-p^j}b^{-1}, \tag{11}$$

so $b^{p^j-1} = c^{p^j-1}$ and the condition in (iii) implies that $j = 0$ and $i = 0$. Therefore $-bc^{-1} = (ab)^2$, which is incompatible with (ii).

We conclude that if the scalars b and c satisfy the conditions in (i), (ii) and (iii), then $\{\alpha, \beta\}$ is a base. □

LEMMA 4.4. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and set α and β as in Lemma* 4.3*. Then $\{\alpha, \beta\}$ is a base for G if and only if the scalars b and c satisfy the conditions* (i)–(iii) *in Lemma* 4.3*.*

Proof. By Lemma 4.3, it suffices to show that if any of the conditions in (i), (ii) or (iii) fail to hold, then there exists an element $x \neq \pm I_2$ in $\Sigma\mathrm{L}_2(q) = \langle \mathrm{SL}_2(q), \phi \rangle$ that fixes α and β. We proceed by inspecting the proof of Lemma 4.3, noting that $i = 0$ in each of the equations (8)–(11).

As explained in the discussion preceding Lemma 4.3, if $bc = 0$ then $\{\alpha, \beta\}$ is not a base. Next assume $-bc^{-1}$ is a square in $\mathbb{F}_q$, say $d^2 = -bc^{-1}$. Then setting $a = db^{-1}$ gives $-a^2 = b^{-1}c^{-1}$ and we get a solution to (11) with $j = 0$. Finally, suppose $b^{p^k-1} = c^{p^k-1}$ for some $0 < k < f$ and choose $a \in \mathbb{F}_q$ with $a^2 = b^{p^k-1}$. Then (8) is satisfied and we conclude that $x = \mathrm{diag}(a, a^{-1})\phi^k$ fixes α and β. □

Let us record three corollaries of Lemma 4.4. The first result allows us to reduce our main problems to the special case $G = \mathrm{P\Sigma L}_2(q)$.

COROLLARY 4.5. *Suppose $G \cap \mathrm{PGL}_2(q) = G_0$ and q is odd. Then the Saxl graph $\Sigma(G)$ contains $\Sigma(\mathrm{P\Sigma L}_2(q))$ as a subgraph.*

Proof. Let $\{\alpha, \beta\}$ be a base for $\mathrm{P\Sigma L}_2(q)$ with $\alpha = \{\langle e_1 \rangle, \langle e_2 \rangle\}$ as usual. As explained in the discussion preceding Lemma 4.3, we have $\beta = \{\langle e_1 + be_2 \rangle, \langle e_1 + ce_2 \rangle\}$ for nonzero scalars b and c, which must satisfy the conditions in (i), (ii), and (iii) of Lemma 4.3 (see Lemma 4.4). Then Lemma 4.3 implies that $\{\alpha, \beta\}$ is a base for G and the result follows. □

COROLLARY 4.6. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and set*

$$\beta = \{\langle e_1 + be_2 \rangle, \langle e_1 + ce_2 \rangle\}, \quad \gamma = \{\langle e_1 + b'e_2 \rangle, \langle e_1 + c'e_2 \rangle\}$$

where b, c, b', c' are nonzero scalars with $b \neq c$ and $b' \neq c'$. Then $\{\beta, \gamma\}$ is a base for G if and only if

$$\{b', c'\} = \left\{ \frac{b(c-b)+dc}{c-b+d}, \frac{b(c-b)+ec}{c-b+e} \right\}$$

for scalars $d, e \in \mathbb{F}_q$ with $d, e \neq b - c$ satisfying conditions (i)–(iii) *in Lemma* 4.3*.*

Proof. Since G acts primitively on Ω, it follows that the normal subgroup G_0 is transitive. Therefore, $\beta = \alpha^g$ for some $g \in G_0$ and we note that g maps the set of neighbours of α in $\Sigma(G)$ to the set of neighbours of β. More precisely, we can take g to be the image of the matrix

$$\begin{pmatrix} 1 & (c-b)^{-1} \\ b & c(c-b)^{-1} \end{pmatrix} \in \mathrm{SL}_2(q).$$

Suppose $\{\beta, \gamma\}$ is a base, so $\gamma = \delta^g$ for some neighbour δ of α. By Lemma 4.4, we have $\delta = \{\langle e_1 + de_2 \rangle, \langle e_1 + ee_2 \rangle\}$ for scalars $d, e \in \mathbb{F}_q$ satisfying the conditions in (i), (ii), and (iii) of Lemma 4.3 and by applying g we get

$$\gamma = \{\langle (1+d(c-b)^{-1})e_1 + (b+dc(c-b)^{-1})e_2 \rangle, \langle (1+e(c-b)^{-1})e_1 + (b+ec(c-b)^{-1})e_2 \rangle\}.$$

Here the coefficients $1 + d(c-b)^{-1}$ and $1 + e(c-b)^{-1}$ are nonzero, so $d, e \neq b - c$ and we deduce that γ has the required form.

Conversely, if γ has the given form then $\gamma = \delta^g$ for some $\delta \in \Omega$ with $\{\alpha, \delta\}$ a base and it follows that $\{\beta, \gamma\}$ is a base. □

Corollary 4.7. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and let m be the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Then $\Sigma(G)$ has valency $m(q-1)/2$ and thus G has exactly $m/2f$ regular suborbits on Ω.*

Proof. We consider the neighbours of $\alpha = \{\langle e_1\rangle, \langle e_2\rangle\}$.

Suppose $\beta = \{\langle e_1 + b_0 e_2\rangle, \langle e_1 + e_2\rangle\}$. By Lemma 4.4, $\{\alpha, \beta\}$ is a base if and only if $-b_0$ is a non-square that is not contained in any proper subfield of $\mathbb{F}_q$. Therefore, there are m choices for β. More generally, if $\beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$ with $c \neq 0$, then $\{\alpha, \beta\}$ is a base if and only if $b = cb_0$ for some b_0 as above. Since there are $q-1$ choices for c and we can interchange the two spaces comprising β, we conclude that $\Sigma(G)$ has valency $m(q-1)/2$. Since $|H| = (q-1)f$, it follows that G has precisely $m/2f$ regular suborbits on Ω. □

We are now in a position to prove our first main result for the $\mathcal{C}_2$-actions of groups with socle $G_0 = \mathrm{L}_2(q)$. The following proposition extends Theorem 4.1 by establishing the main conjecture of [11] for these groups.

Proposition 4.8. *Property $(\star)$ holds if $G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q) \wr S_2$.*

Proof. We may assume $q > 27$. Recall that $b(G) = 2$ if and only if G does not contain $\mathrm{PGL}_2(q)$ as a proper subgroup. If $G = \mathrm{PGL}_2(q)$, then $\Sigma(G)$ is isomorphic to the Johnson graph $J(q+1, 2)$ and we immediately deduce that $(\star)$ holds (as noted in [11, Example 3.9]).

For the remainder, we may assume that $G \cap \mathrm{PGL}_2(q) = G_0$ and q is odd. In view of Corollary 4.5, we only need to consider the group $G = \mathrm{P\Sigma L}_2(q)$. Fix $\alpha = \{\langle e_1\rangle, \langle e_2\rangle\}$ as before. By Theorem 4.1, it suffices to show that if $\{\alpha, \beta\}$ is a base, then there exists $\gamma \in \Omega$ such that both $\{\alpha, \gamma\}$ and $\{\beta, \gamma\}$ are bases.

By Lemma 4.4 we have $\beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\}$, where $b, c \in \mathbb{F}_q$ are nonzero scalars such that $-bc^{-1}$ is a non-square and is not contained in any proper subfield of $\mathbb{F}_q$. Set $\gamma = \{\langle e_1 - be_2\rangle, \langle e_1 - ce_2\rangle\} \in \Omega$ and note that $\{\alpha, \gamma\}$ is a base by Lemma 4.3. By Corollary 4.6, $\{\beta, \gamma\}$ is a base if and only if there exists $d, e \in \mathbb{F}_q$ with $d, e \neq b - c$ such that

$$\{-b, -c\} = \left\{ \frac{b(c-b) + dc}{c - b + d}, \frac{b(c-b) + ec}{c - b + e} \right\} \tag{12}$$

and d, e satisfy the conditions in (i), (ii), and (iii) of Lemma 4.3.

Set $d = \frac{2b(b-c)}{b+c}$ and $e = \frac{b^2 - c^2}{2c}$. Then $d, e \neq b - c$, (12) holds and $de \neq 0$. In addition,

$$-de^{-1} = -bc^{-1}\left(\frac{2c}{b+c}\right)^2 = -4(bc^{-1} + cb^{-1} + 2)^{-1}$$

and we immediately deduce that $-de^{-1}$ is a non-square in $\mathbb{F}_q$.

Finally, we claim that de^{-1} is not contained in a proper subfield of $\mathbb{F}_q$. To do this, it suffices to show that $\eta = bc^{-1} + cb^{-1}$ is not contained in such a subfield. With this aim in mind, it will be useful to observe that

$$\begin{aligned} \eta^{p^k} - \eta &= (bc^{-1})^{p^k} + (bc^{-1})^{-p^k} - bc^{-1} - (bc^{-1})^{-1} \\ &= (bc^{-1})^{-p^k}((bc^{-1})^{p^k+1} - 1)((bc^{-1})^{p^k-1} - 1) \end{aligned}$$

for $1 \leqslant k < f$, so η is contained in the subfield $\mathbb{F}_{p^k}$ of $\mathbb{F}_q$ if and only if this expression is 0. Now since b and c satisfy the condition in part (iii) of Lemma 4.3, it follows that $(bc^{-1})^{p^k-1} - 1 \neq 0$, whence $\eta \in \mathbb{F}_{p^k}$ if and only if $(bc^{-1})^{p^k+1} = 1$. If the latter equality holds, then $bc^{-1} \in \mathbb{F}_{p^{2k}}$ and thus $2k = f$. In particular, this implies that both -1 and bc^{-1} are squares, which contradicts (ii) in Lemma 4.3.

This justifies the claim and we conclude that d and e satisfy the conditions in parts (i), (ii), and (iii) of Lemma 4.3. In particular, $\{\beta, \gamma\}$ is a base and the result follows. □

Next we turn to the problem of determining when G has a unique regular suborbit on Ω. We will need the following number-theoretic result, where ϕ and $\gamma = 0.57721...$ denote Euler's totient function and Euler's constant, respectively.

LEMMA 4.9. *For every integer $n \geqslant 3$,*

$$\phi(n) > \frac{n}{e^{\gamma} \log\log n + \frac{3}{\log\log n}}.$$

Proof. See [38, Theorem 15]. □

PROPOSITION 4.10. *Suppose $G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q) \wr S_2$. Then G has a unique regular suborbit if and only if $G = \mathrm{PGL}_2(q)$ and $q \geqslant 4$, $q \neq 5$.*

Proof. In view of Proposition 4.2, we may assume $q > 27$ and we recall that $G = \mathrm{PGL}_2(q)$ has a unique regular suborbit. For the remainder we may assume q is odd and $G \cap \mathrm{PGL}_2(q) = G_0$; our aim is to show that G has at least two regular suborbits. By Corollary 4.5, we may assume that $G = \mathrm{P\Sigma L}_2(q)$, in which case G has $m/2f$ regular suborbits by Corollary 4.7, where m is the number of non-squares in $\mathbb{F}_q$ that are not contained in any proper subfield of $\mathbb{F}_q$. Any primitive element of $\mathbb{F}_q$ has this property and there are $\phi(q-1)$ such elements in $\mathbb{F}_q$. By applying the lower bound in Lemma 4.9 we deduce that $\phi(q-1) \geqslant 4f$ for all $q > 27$ and the result follows. □

Finally, we turn to the clique number of $\Sigma(G)$. If $G = \mathrm{PGL}_2(q)$ then $\omega(G) = q$ since $\Sigma(G)$ is isomorphic to the Johnson graph $J(q+1, 2)$, whence $\omega(G) \geqslant q$ if $G \leqslant \mathrm{PGL}_2(q)$ and the conclusion to Theorem 1.3 holds. For $5 < q < 1000$ we have used the computational approach described in Section 6.1 to verify the bound $\omega(\mathrm{P\Sigma L}_2(q)) \geqslant 5$ (in view of Corollary 4.5, this implies that $\omega(G) \geqslant 5$ whenever $5 < q < 1000$ is odd and $G \cap \mathrm{PGL}_2(q) = G_0$). We expect $\omega(G) \geqslant 5$ for all $q > 5$, but we have not been able to prove this.

REMARK 4.11. Let us say more about the difficulties that arise when trying to construct a clique of size 5 when $G = \mathrm{P\Sigma L}_2(q)$. By Proposition 4.8 we see that $\omega(G) \geqslant 3$. More precisely, $\{\alpha, \beta, \gamma\}$ is a clique of size 3, where

$$\alpha = \{\langle e_1\rangle, \langle e_2\rangle\},\ \beta = \{\langle e_1 + be_2\rangle, \langle e_1 + ce_2\rangle\},\ \gamma = \{\langle e_1 - be_2\rangle, \langle e_1 - ce_2\rangle\}$$

and $b, c \in \mathbb{F}_q^{\times}$ satisfy the conditions in parts (i), (ii), and (iii) of Lemma 4.3. Similarly, if we choose different scalars $b', c' \in \mathbb{F}_q^{\times}$ then we can construct another clique $\{\alpha, \beta', \gamma'\}$, where $\beta' = \{\langle e_1 + b'e_2\rangle, \langle e_1 + c'e_2\rangle\}$ and $\gamma' = \{\langle e_1 - b'e_2\rangle, \langle e_1 - c'e_2\rangle\}$. Then $\{\alpha, \beta, \beta', \gamma, \gamma'\}$ is a clique of size 5 if $\{\beta, \beta'\}$ and $\{\beta, \gamma'\}$ are bases. So in view of Corollary 4.6, we need to find scalars $d, e \neq b - c$ satisfying conditions (i)–(iii) in Lemma 4.3 such that

$$\{b', c'\} = \left\{ \frac{b(c-b) + dc}{c - b + d}, \frac{b(c-b) + ec}{c - b + e} \right\},$$

together with another pair of scalars $d', e' \neq b - c$ satisfying the same conditions with

$$\{-b', -c'\} = \left\{ \frac{b(c-b) + d'c}{c - b + d'}, \frac{b(c-b) + e'c}{c - b + e'} \right\}.$$

Here the main difficulty arises in verifying the required conditions in Lemma 4.3. For example, if we fix b' and c', then we need to show that de^{-1} is not contained in a proper subfield of $\mathbb{F}_q$, which is not an easy condition to check. At the same time,

we also need to verify the corresponding condition for $d'e'^{-1}$, which is an additional complication.

4.2. $\mathcal{C}_3$-actions. In this section we assume H is of type $\mathrm{GL}_1(q^2)$, so $H_0 = D_{2(q+1)/h}$ and $|\Omega| = \frac{1}{2}q(q-1)$, where $h = (2, q-1)$. By Proposition 4.2 we may assume $q > 27$ and we note that [9, Lemma 4.8] gives $b(G) \leqslant 3$, with equality if and only if $\mathrm{PGL}_2(q) \leqslant G$. Therefore, we may assume q is odd and $G \cap \mathrm{PGL}_2(q) = G_0$, so either

(a) $G = \langle G_0, \phi^j \rangle$ for some j in the range $0 \leqslant j < f$; or
(b) $G = \langle G_0, \delta\phi^j \rangle$ with $0 < j < f$ and $f/(f, j)$ even.

Following [9], it will be helpful to identify G_0 with the unitary group $X_0 = \mathrm{U}_2(q)$ and H with a maximal subgroup of type $\mathrm{GU}_1(q) \wr S_2$. We may then identify Ω with the set of orthogonal pairs of nondegenerate 1-dimensional subspaces of the natural module U for X_0, which is defined over $\mathbb{F}_{q^2}$. As in the proof of [9, Lemma 4.8], fix an orthonormal basis $\{u, v\}$ for U and set $\alpha = \{\langle u \rangle, \langle v \rangle\} \in \Omega$. For each nonzero scalar $b \in \mathbb{F}_{q^2}$ with $b^{q+1} \neq -1$ we define

$$\omega_b = \{\langle u + bv \rangle, \langle u - b^{-q}v \rangle\} \in \Omega.$$

Then

$$\Omega = \{\alpha\} \cup \{\omega_b \,:\, b \in \mathbb{F}_{q^2}^\times,\, b^{q+1} \neq -1\}$$

and we note that $\omega_b = \omega_{-b^{-q}}$. We will abuse notation by writing ϕ for the field automorphism of X_0 that corresponds to the map $\eta \mapsto \eta^p$ on $\mathbb{F}_{q^2}$ and we will assume that

$$(au + bv)^\phi = a^p u + b^p v$$

for all $a, b \in \mathbb{F}_{q^2}$. We define $\Sigma\mathrm{U}_2(q) = \langle \mathrm{SU}_2(q), \phi \rangle$ and $\mathrm{P}\Sigma\mathrm{U}_2(q) = \langle X_0, \phi \rangle = X_0.f$, noting that $X_0 \cap \langle \phi \rangle = \langle \phi^f \rangle$. In this setting, the two cases we need to consider are as described in (a) and (b) above, with G_0 replaced by X_0. Note that in (b), the diagonal automorphism δ is the image of a diagonal matrix $\mathrm{diag}(\lambda^{q-1}, 1) \in \mathrm{GU}_2(q)$ with respect to the basis $\{u, v\}$ for U, where $\mathbb{F}_{q^2}^\times = \langle \lambda \rangle$.

We begin with the following result, which is the analogue of Lemma 4.3 for the $\mathcal{C}_3$-actions we are considering here. Note that the sufficient condition in the lemma is equivalent to the non-containment of $b^{\frac{1}{2}(q+1)}$ in a proper subfield of $\mathbb{F}_{q^2}$.

Lemma 4.12. *Suppose $G \cap \mathrm{PGL}_2(q) = G_0$ with q odd. Then $\{\alpha, \omega_b\}$ is a base for G if*

$$b^{\frac{1}{2}(q+1)(p^k-1)} \neq 1 \tag{13}$$

for all $0 < k < 2f$.

Proof. Suppose b satisfies the condition in (13) for all $0 < k < 2f$ and let us assume

$$x = AB^i\phi^j \in \langle \mathrm{GU}_2(q), \phi \rangle$$

fixes α and ω_b, where $A \in \mathrm{SU}_2(q)$, $B = \mathrm{diag}(\lambda^{q-1}, 1)$, $0 \leqslant i < q+1$, $0 \leqslant j < 2f$ with $j \neq f$, and $j > 0$ if $i > 0$. In order to prove that $\{\alpha, \omega_b\}$ is a base for G, it suffices to show that if x fixes α and ω_b, then $i = j = 0$ and $A = \pm I_2$. So let us assume x fixes α and ω_b, which means that A is either diagonal or anti-diagonal with respect to the basis $\{u, v\}$ for the natural $\mathrm{SU}_2(q)$-module U.

First assume $A = \mathrm{diag}(a, a^{-1})$ is diagonal, so $a^{q+1} = 1$. If x fixes the two spaces in ω_b, then

$$(u + bv)^x = a\lambda^{i(q-1)}u + a^{-1}b^{p^j}v = \eta_1(u + bv)$$
$$(u - b^{-q}v)^x = a\lambda^{i(q-1)}u - a^{-1}b^{-qp^j}v = \eta_2(u - b^{-q}v)$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^\times$, whence

$$a^2\lambda^{i(q-1)} = b^{p^j-1} = b^{q(1-p^j)}. \tag{14}$$

Since $a^{q+1} = 1$ we get $(b^{q+1})^{(p^j-1)} = 1$, which implies that $(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = 1$ and thus $2j = 0$ or $2f$ are the only possibilities. But we are assuming $j \neq f$, hence $j = 0$ and thus $i = 0$. Therefore, (14) gives $a^2 = 1$ and we conclude that $x = \pm I_2$.

Similarly, if x interchanges the spaces in ω_b, then

$$(u + bv)^x = a\lambda^{i(q-1)}u + a^{-1}b^{p^j}v = \eta_1(u - b^{-q}v)$$
$$(u - b^{-q}v)^x = a\lambda^{i(q-1)}u - a^{-1}b^{-qp^j}v = \eta_2(u + bv)$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^\times$ and we deduce that

$$-a^2\lambda^{i(q-1)} = b^{p^j+q} = b^{-qp^j-1}. \tag{15}$$

In particular, since $a^{q+1} = 1$, it follows that

$$(b^{q+1})^{\frac{1}{2}(p^{j+f}+1)} = (-1)^{\frac{1}{2}(q+1)}\lambda^{\frac{1}{2}i(q^2-1)} = (-\lambda^{i(q-1)})^{\frac{1}{2}(q+1)}$$

and thus

$$(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = (b^{q+1})^{\frac{1}{2}(p^{2(j+f)}-1)} = (-\lambda^{i(q-1)})^{\frac{1}{2}(q+1)(p^{j+f}-1)} = 1.$$

Since (13) holds and $j \neq f$ we deduce that $j = 0$ is the only possibility, implying $i = 0$. Then (15) gives $b^{q+1} = b^{-q-1}$ and thus $b^{q+1} = \pm 1$. By construction we have $b^{q+1} \neq -1$ (since $\omega_b \in \Omega$), while (13) implies that $b^{q+1} \neq 1$. Therefore, we have reached a contradiction and this case does not arise.

Now let us assume x interchanges the two spaces in α, so

$$A = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$$

is anti-diagonal and $a^{q+1} = 1$. If x fixes the spaces in ω_b, then

$$(u + bv)^x = ab^{p^j}u - a^{-1}\lambda^{i(q-1)}v = \eta_1(u + bv)$$
$$(u - b^{-q}v)^x = -ab^{-qp^j}u - a^{-1}\lambda^{i(q-1)}v = \eta_2(u - b^{-q}v)$$

for some $\eta_1, \eta_2 \in \mathbb{F}_{q^2}^\times$ and we get

$$-a^2\lambda^{-i(q-1)} = b^{-p^j-1} = b^{q+qp^j}. \tag{16}$$

This implies that $(b^{q+1})^{\frac{1}{2}(p^{2j}-1)} = 1$, which leads to a contradiction as above. Finally, suppose x interchanges the two spaces in ω_b. Here we get

$$a^2\lambda^{i(q-1)} = b^{q-p^j} = b^{qp^j-1} \tag{17}$$

and thus $(b^{q+1})^{\frac{1}{2}(p^{f+j}-1)} = \lambda^{\frac{1}{2}i(q^2-1)} = \pm 1$ and so $(b^{q+1})^{\frac{1}{2}(p^{2(f+j)}-1)} = 1$. It follows that $j = 0$ and $i = 0$, so $(b^{q+1})^{\frac{1}{2}(p^f-1)} = 1$ and this is incompatible with (13). □

LEMMA 4.13. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd. Then $\{\alpha, \omega_b\}$ is a base for G if and only if (13) holds for all $0 < k < 2f$.*

Proof. By Lemma 4.12, it suffices to show that if the condition in (13) fails to hold, then $\{\alpha, \omega_b\}$ is not a base for G. So let us assume k is an integer such that $0 < k < 2f$ and

$$b^{\frac{1}{2}(q+1)(p^k-1)} = 1.$$

If $k \neq f$ then by setting $j = k$ we deduce that (14) holds with $a = b^{(p^k-1)/2}$ and $i = 0$, otherwise (17) holds with $a = b^{(q-1)/2}$ and $i = j = 0$. In both cases we conclude that $\{\alpha, \omega_b\}$ is not a base and the result follows. □

Remark 4.14. By inspecting the proofs of Lemmas 4.12 and 4.13, we deduce that if $G = G_0$ and q is odd, then $\{\alpha, \omega_b\}$ is a base for G if and only if b is a non-square in $\mathbb{F}_{q^2}$. The same criterion was established in the proof of [14, Theorem 10] for $q \equiv 3 \pmod 4$ and we note that a very similar argument can be used to reach the same conclusion when $q \equiv 1 \pmod 4$. In addition, we refer the reader to [14, Lemma 7.9] for a complete list of the subdegrees of $G = G_0$ when $q \geqslant 11$ is odd.

We can now reduce our main problems to the special case $G = \mathrm{P\Sigma L}_2(q)$.

Corollary 4.15. *Suppose $G \cap \mathrm{PGL}_2(q) = G_0$ and q is odd. Then the Saxl graph $\Sigma(G)$ contains $\Sigma(\mathrm{P\Sigma L}_2(q))$ as a subgraph.*

Proof. If $\{\alpha, \omega_b\}$ is a base for $\mathrm{P\Sigma L}_2(q)$, then Lemma 4.13 implies that (13) holds and thus $\{\alpha, \omega_b\}$ is a base for G by Lemma 4.12. □

The following technical result is a key observation.

Corollary 4.16. *Let $G = \mathrm{P\Sigma L}_2(q)$ with q odd and let $b, c \in \mathbb{F}_{q^2}^\times$ be scalars such that $b^{q+1}, c^{q+1} \neq -1$ and $c \notin \{b, -b^{-q}\}$. Then $\{\omega_b, \omega_c\}$ is a base for G if and only if*

$$\frac{ba_1^{-2}(b + b^{-q}) + b^{-q}d}{a_1^{-2}(b + b^{-q}) - d} \in \{c, -c^{-q}\}$$

for scalars $a_1, d \in \mathbb{F}_{q^2}$ satisfying all of the following conditions:

(i) $a_1^{q+1} = 1 + b^{q+1}$;
(ii) $d^{q+1} \neq -1$ *and* $d \notin \{a_1^{-2}(b + b^{-q}), -b^{q+1}a_1^{-2}(b + b^{-q})\}$;
(iii) $d^{\frac{1}{2}(q+1)(p^k-1)} \neq 1$ *for all* $0 < k < 2f$.

Proof. Choose $a_1 \in \mathbb{F}_{q^2}$ such that $a_1^{q+1} = 1 + b^{q+1}$ and set $a_2 = -(b + b^{-q})a_1^{-1}$ (note that a_1 exists since $1 + b^{q+1} \in \mathbb{F}_q$). Then $a_2^{q+1} = 1 + b^{-(q+1)}$ and we deduce that both $a_1^{-1}(u + bv)$ and $a_2^{-1}(u - b^{-q}v)$ are unit vectors. Let $g \in X_0 = \mathrm{U}_2(q)$ be the image of the matrix

$$A = \begin{pmatrix} a_1^{-1} & a_2^{-1} \\ ba_1^{-1} & -b^{-q}a_2^{-1} \end{pmatrix} \in \mathrm{SU}_2(q),$$

which is expressed in terms of the basis $\{u, v\}$ for U. Note that $\alpha^g = \omega_b$.

First assume $\{\omega_b, \omega_c\}$ is a base for G, so $\omega_c = \omega_d^g$ for some neighbour ω_d of α in $\Sigma(G)$. Then $d^{q+1} \neq -1$ and Lemma 4.13 implies that d satisfies the condition in (iii). By applying g we get

$$(u + dv)^g = (a_1^{-1} + a_2^{-1}d)u + (ba_1^{-1} - b^{-q}a_2^{-1}d)v.$$

Since $\omega_c \neq \alpha$, the coefficients of u and v in this expression are nonzero and we deduce that d satisfies the remaining conditions in (ii). In particular,

$$\langle u + dv \rangle^g = \left\langle u + \frac{ba_1^{-1}a_2 - b^{-q}d}{a_1^{-1}a_2 + d}v \right\rangle = \left\langle u + \frac{ba_1^{-2}(b + b^{-q}) + b^{-q}d}{a_1^{-2}(b + b^{-q}) - d}v \right\rangle$$

$$\langle u - d^{-q}v \rangle^g = \left\langle u + \frac{ba_1^{-2}(b + b^{-q}) - b^{-q}d^{-q}}{a_1^{-2}(b + b^{-q}) + d^{-q}}v \right\rangle$$

and we conclude that if $\{\omega_b, \omega_c\}$ is a base for G then all of the required conditions are satisfied.

Conversely, if c has the given form for scalars a_1 and d satisfying all of the given conditions, then $\{\alpha, \omega_d\}$ is a base for G (via the condition in (iii)) and $\omega_c = \omega_d^g$ for some $g \in G_0$ with $\omega_b = \alpha^g$. Therefore, $\{\omega_b, \omega_c\}$ is also a base for G. □

We are now in a position to extend Theorem 4.1 by establishing $(\star)$ for the $\mathcal{C}_3$-actions of groups with socle $\mathrm{L}_2(q)$.

PROPOSITION 4.17. *Property* $(\star)$ *holds if* $G_0 = \mathrm{L}_2(q)$ *and* H *is of type* $\mathrm{GL}_1(q^2)$.

Proof. We may assume $q > 27$ (see Proposition 4.2) and we recall that $b(G) = 2$ if and only if q is odd and $G \cap \mathrm{PGL}_2(q) = G_0$. In view of Corollary 4.15, we may assume that $G = \mathrm{P\Sigma L}_2(q)$. By Theorem 4.1, it suffices to show that if $\{\alpha, \omega_b\}$ is a base for G, then there exists $c \in \mathbb{F}_{q^2}^\times$ with $c^{q+1} \neq -1$ such that both $\{\alpha, \omega_c\}$ and $\{\omega_b, \omega_c\}$ are also bases. Note that $b^{q+1} \neq -1$ and b satisfies the condition in (13) for all $0 < k < 2f$ (see Lemma 4.13).

We claim that all of the above properties hold with $c = -b$. Clearly, we have $c^{q+1} = b^{q+1} \neq -1$ and $c^{\frac{1}{2}(q+1)(p^k-1)} \neq 1$ for all $0 < k < 2f$, so $\{\alpha, \omega_c\}$ is a base. It remains to prove that $\{\omega_b, \omega_c\}$ is a base.

As in Corollary 4.16, fix a scalar $a_1 \in \mathbb{F}_{q^2}^\times$ such that $a_1^{q+1} = 1 + b^{q+1}$ and set

$$d = \frac{2ba_1^{-2}(b + b^{-q})}{b - b^{-q}} \in \mathbb{F}_{q^2}^\times.$$

Then

$$c = \frac{ba_1^{-2}(b + b^{-q}) + b^{-q}d}{a_1^{-2}(b + b^{-q}) - d}$$

and it remains to show that d satisfies all the conditions in parts (ii) and (iii) of Corollary 4.16.

If $d \in \{a_1^{-2}(b+b^{-q}), -b^{q+1}a_1^{-2}(b+b^{-q})\}$ then $b^{q+1} = -1$, which is a contradiction. In addition, if we write $\alpha^g = \omega_b$ as in the proof of Corollary 4.16, then $\langle u + dv\rangle = \langle u+cv\rangle^{g^{-1}}$ and $\langle u-d^{-q}v\rangle = \langle u-c^{-q}v\rangle^{g^{-1}}$. Since $c^{q+1} \neq -1$, we have $u+cv \neq u-c^{-q}v$ and thus $u + dv \neq u - d^{-q}v$. Therefore, $d^{q+1} \neq -1$ and we conclude that d satisfies all of the conditions in part (ii) of Corollary 4.16.

Finally, we need to show that

$$d^{\frac{1}{2}(q+1)} = \pm 2\left(b^{\frac{1}{2}(q+1)} - b^{-\frac{1}{2}(q+1)}\right)^{-1}$$

is not contained in a proper subfield of $\mathbb{F}_{q^2}$. Set $e = b^{\frac{1}{2}(q+1)}$, which is not in a proper subfield by Lemma 4.13, and note that it suffices to show that $e - e^{-1}$ is also not contained in a proper subfield. Fix an integer $0 < k < 2f$ and observe that

$$(e - e^{-1})^{p^k} - (e - e^{-1}) = e^{-p^k}(e^{p^k+1} + 1)(e^{p^k-1} - 1),$$

so $e - e^{-1} \in \mathbb{F}_{p^k}$ if and only if this expression is 0. In view of (13), this holds if and only if $e^{p^k+1} = -1$. So let us assume this relation holds. Then $e^{p^{2k}-1} = (-1)^{p^k-1} = 1$ and thus $2k = 0$ or $2f$. If $2k = 2f$ then $k = f$ and so $e^{q+1} = e^{p^k+1} = -1$. This implies that

$$-1 = e^{q+1} = b^{\frac{1}{2}(q+1)^2} = b^{\frac{1}{2}(q^2+1)}b^q = -b^{q+1}$$

and so b is a square, which is incompatible with (13). Therefore $k = 0$, so $e^2 = -1$ and $e - e^{-1} = -2e^{-1}$. The result now follows since Lemma 4.13 implies that e^{-1} is not contained in a proper subfield of $\mathbb{F}_{q^2}$. □

PROPOSITION 4.18. *Suppose* $G_0 = \mathrm{L}_2(q)$ *and* H *is of type* $\mathrm{GL}_1(q^2)$. *Then* G *has a unique regular suborbit if and only if* $G = \mathrm{L}_2(5)$ *or* $\mathrm{L}_2(9).2 = \mathrm{M}_{10}$.

Proof. In view of Proposition 4.2 and Corollary 4.15, we may assume $q > 27$ is odd and $G = \mathrm{P\Sigma L}_2(q)$. Let r be the number of regular suborbits of G. If q is a prime then $G = G_0$ and [14, Lemma 7.9] gives $r = (q-\ell)/4$, where $q \equiv \ell \pmod 4$ with $\ell \in \{1, 3\}$. For the remainder, we may assume $q > p$.

Let λ be a primitive element of $\mathbb{F}_{q^2}$. Then by Lemma 4.12, we see that $\{\alpha, \omega_\lambda\}$ is a base for G. Therefore, the valency of $\Sigma(G)$ is at least $\phi(q^2 - 1)/2$, where ϕ is Euler's

function and thus $r \geqslant \phi(q^2-1)/2f(q+1)$ since $|H| = f(q+1)$. By applying the lower bound in Lemma 4.9 we deduce that

$$\frac{\phi(q^2-1)}{2f(q+1)} \geqslant 2$$

for $q > 27$ and the desired result follows. □

Finally, we consider the clique number $\omega(G)$ of $\Sigma(G)$. Our main result is the following, which establishes a strong form of Theorem 1.3 when $G = G_0$ is simple.

Proposition 4.19. *Suppose $G = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q^2)$, where q is odd. Then $\omega(G) \geqslant \frac{1}{2}(q-1)$.*

Proof. Let b be a non-square in $\mathbb{F}_{q^2}$ with $b^{q+1} \neq -1$. Then bx is a non-square for all $x \in \mathbb{F}_q$ and thus $\{\alpha, \omega_{bx}\}$ is a base for G if and only if $(bx)^{q+1} \neq -1$ (see Remark 4.14). We claim that

$$C = \{\alpha\} \cup \{\omega_{bx} \,:\, x \in \mathbb{F}_q^\times,\, (bx)^{q+1} \neq -1\}$$

is a clique in $\Sigma(G)$ with $|C| \geqslant \frac{1}{2}(q-1)$.

To see this, first note that if $x \in \mathbb{F}_q^\times$ and $(bx)^{q+1} = -1$, then $b^{q+1} = -x^{-2}$ and there are at most two possibilities for x. Let us also observe that if $y = -b^{-(q+1)}x^{-1}$ then $by = -(bx)^{-q}$ and thus $\omega_{bx} = \omega_{by}$. This shows that $|C| \geqslant 1 + \frac{1}{2}(q-3) = \frac{1}{2}(q-1)$.

To complete the proof of the proposition, it suffices to show that $\{\omega_{bx}, \omega_{by}\}$ is a base for all distinct points ω_{bx}, ω_{by} in C. To this end, set $c = bx$ and note that c is a non-square such that $c^{q+1} \neq -1$ and $by = cyx^{-1} \in c\mathbb{F}_q^\times$. In this way, the problem is reduced to showing that $\{\omega_b, \omega_{by}\}$ is a base for all $y \in \mathbb{F}_q^\times$ with $(by)^{q+1} \neq -1$ and $by \neq -b^{-q}$ (the latter condition forces $\omega_b \neq \omega_{by}$).

By Corollary 4.16, it suffices to show that there exist scalars $a_1, d \in \mathbb{F}_{q^2}^\times$ such that

$$by = \frac{ba_1^{-2}(b + b^{-q}) + b^{-q}d}{a_1^{-2}(b + b^{-q}) - d}, \tag{18}$$

where $a_1^{q+1} = 1 + b^{q+1}$ and d satisfies the conditions in parts (ii) and (iii) of the corollary. In fact, in view of Remark 4.14, we can replace the condition in (iii) by the property that d is a non-square.

Let $a_1 \in \mathbb{F}_{q^2}^\times$ be any scalar such that $a_1^{q+1} = 1 + b^{q+1}$, noting that a_1 exists since $b^{q+1} \in \mathbb{F}_q$. Since $by \neq -b^{-q}$, it follows that $b^{-(q+1)} + y \neq 0$ and we may define

$$d = \frac{ba_1^{-2}(1 + b^{-(q+1)})(y-1)}{b^{-(q+1)} + y}.$$

Since $b^{q+1} \neq -1$ we see that $d \neq a_1^{-2}(b + b^{-q})$ and by rearranging we deduce that (18) holds. In particular, since $by \neq 0$ we have $d \neq -b^{q+1}a_1^{-2}(b + b^{-q})$. If $d^{q+1} = -1$, then $(y-1)^2 = -b^{q+1}(b^{-(q+1)} + y)^2$, which forces $(b^{q+1}y^2 + 1)(b^{q+1} + 1) = 0$. But this is false because $b^{q+1}y^2 = (by)^{q+1} \neq -1$ and $b^{q+1} \neq -1$, whence $d^{q+1} \neq -1$ and d satisfies all of the conditions in part (ii) of Corollary 4.16. Finally, let us observe that a_1^{-2} is a square and $\frac{(1+b^{-(q+1)})(y-1)}{b^{-(q+1)}+y} \in \mathbb{F}_q$, which is also a square. Therefore, d is a non-square since b is a non-square. We conclude that $\{\omega_b, \omega_{by}\}$ is a base for G and this completes the proof of the proposition. □

Corollary 4.20. *If $G = G_0 = \mathrm{L}_2(q)$ and H is of type $\mathrm{GL}_1(q^2)$, then either $\omega(G) \geqslant 5$, or $q = 5$ and $\omega(G) = 4$.*

Proof. By Proposition 4.2 we may assume $q > 27$. Now apply Proposition 4.19. □

REMARK 4.21. As for the $\mathcal{C}_2$-actions from the previous section, we have been unable to extend Corollary 4.20 to the base-two groups with $G \neq G_0$. Using a computational approach (see Section 6.1), it is straightforward to show that $\omega(\mathrm{P\Sigma L}_2(q)) \geqslant 5$ when $5 < q < 1000$ and we expect $\omega(G) \geqslant 5$ for all $q > 5$.

In order to illustrate some of the difficulties that arise, let us assume $G = \mathrm{P\Sigma L}_2(q)$. As explained in the proof of Proposition 4.17, if $b \in \mathbb{F}_{q^2}$ is a scalar such that $b^{q+1} \neq -1$ and (13) holds for all $0 < k < 2f$, then $\{\alpha, \omega_b, \omega_{-b}\}$ a clique of size 3. Similarly, we can choose a different scalar c such that $\{\alpha, \omega_c, \omega_{-c}\}$ is a clique and we can seek to combine these sets to construct a clique $\{\alpha, \omega_b, \omega_{-b}, \omega_c, \omega_{-c}\}$ of size 5. For this approach to work, we need $\{\omega_b, \omega_c\}$ and $\{\omega_b, \omega_{-c}\}$ to be bases, which imposes various conditions on c. For example, we need the scalars

$$d = \frac{(c-b)a_1^{-2}(b+b^{-q})}{b^{-q}+c}, \quad e = \frac{-(b+c)a_1^{-2}(b+b^{-q})}{b^{-q}-c}$$

to satisfy all the conditions in parts (ii) and (iii) of Corollary 4.16, where $a_1 \in \mathbb{F}_{q^2}$ is chosen so that $a_1^{q+1} = 1 + b^{q+1}$. These conditions are difficult to check and we have been unable to establish the existence of scalars b and c with the desired properties in full generality.

4.3. AN EXTENSION. In this section we take the opportunity to establish [11, Conjecture 4.5] for all base-two almost simple primitive groups G with socle $G_0 = \mathrm{L}_2(q)$. This extends the main theorem of [19], which shows that $\Sigma(G)$ has diameter 2.

THEOREM 4.22. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a base-two almost simple primitive permutation group with socle $G_0 = \mathrm{L}_2(q)$. Then any two vertices in $\Sigma(G)$ have a common neighbour.*

Proof. The groups with $q \leqslant 11$ can be handled using MAGMA [4] (see Section 5 below), so let us assume $q > 11$. By combining Proposition 2.2 with Theorem 3.1, we may assume that either $G \in \mathcal{L}$ or a point stabiliser H is insoluble. So in view of Propositions 4.8 and 4.17, we may assume H is insoluble. By inspecting [5, Tables 8.1 and 8.2], one of the following holds:

(a) $H = S_5$ or A_5, $q \in \{p, p^2\}$ and $p \equiv \pm 1, \pm 3 \pmod{10}$;
(b) H is a subfield subgroup of type $\mathrm{GL}_2(q_0)$, where $q = q_0^k$, k is a prime and $q_0 \geqslant 4$.

First consider case (a) and recall that we write $i_m(H)$ for the number of elements of order m in H. In view of Proposition 2.2, it suffices to show that $\widehat{Q}(G) < 1/2$ (see Section 2.1). We refer the reader to [10, Section 3.2] for detailed information on the conjugacy classes of elements of prime order in G.

Let $x \in H$ be an element of prime order m and note that $m \in \{2, 3, 5\}$. If $m = 2$ then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_1$ (minimal if x is an involutory field automorphism) and we note that $i_2(H) \leqslant 25 = a_1$. Similarly, if $m \in \{3, 5\}$ then $|x^G| \geqslant q(q-1) = b_2$ and $i_3(H) + i_5(H) = 44 = a_2$. Therefore, Lemma 2.1 implies that

$$\widehat{Q}(G) \leqslant a_1^2/b_1 + a_2^2/b_2 \tag{19}$$

and we deduce that $\widehat{Q}(G) < 1/2$ if $q \geqslant 197$. The remaining cases with $q < 197$ can be verified using MAGMA.

Finally, let us consider the subfield subgroups in (b). First assume $k = 2$. We claim that $b(G) \geqslant 3$. If p is odd then

$$|\Omega| = |G_0 : \mathrm{PGL}_2(q_0)| = \frac{1}{2}q_0(q_0^2+1)$$

and the claim follows since $b(G) \geqslant \log_{|\Omega|} |G| > 2$. Similarly, if $p = 2$ and $G \neq G_0$ then $|\Omega| = q_0(q_0^2+1)$ and

$$b(G) \geqslant \frac{\log |G|}{\log |\Omega|} \geqslant \frac{\log 2q_0^2(q_0^4-1)}{\log q_0(q_0^2+1)} > 2.$$

Finally, suppose $p = 2$ and $G = G_0$. Here $\log_{|\Omega|} |G| < 2$ and the subdegrees of G are recorded in [23, p.354]. By inspection, we see that G does not have a regular suborbit and thus $b(G) \geqslant 3$.

Next assume $k \geqslant 5$ and let $x \in H$ be an element of prime order. If x is an involutory field automorphism of G_0, then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_1$ and we note that there are at most $a_1 = q_0^{1/2}(q_0+1)$ such elements in H. In each of the remaining cases, we have $|x^G| \geqslant \frac{1}{2}q(q-1) = b_2$ and we observe that $|H| \leqslant q_0(q_0^2-1)\log q = a_2$. By applying Lemma 2.1 we deduce that (19) holds and this gives $\widehat{Q}(G) < 1/2$ as required.

To complete the proof, we may assume $k = 3$. This case requires a more refined treatment. First let $x \in H \cap \mathrm{PGL}_2(q)$ be an element of prime order m. If x is unipotent (so $m = p$) then $|x^G| \geqslant \frac{1}{2}(q^2-1) = b_1$ and we note that there are exactly $a_1 = q_0 - 1$ such elements in H. Similarly, if x is a semisimple involution then $|x^G| \geqslant \frac{1}{2}q(q-1) = b_2$ and we have $i_2(\mathrm{PGL}_2(q_0)) = q_0^2 = a_2$. Next suppose $m \neq p$ and $m \geqslant 3$, so m divides $q_0^2 - 1$ and there are $\frac{1}{2}(m-1)$ distinct G_0-classes of such elements in G (and the same number of $\mathrm{L}_2(q_0)$-classes in $H \cap \mathrm{PGL}_2(q)$). If $\{x_1, \ldots, x_t\}$ is a set of representatives of the distinct G-classes of these elements, then there exist positive integers k_i such that $\sum_i k_i = \frac{1}{2}(m-1)$ and

$$|x_i^G \cap H| = k_i q_0(q_0+\varepsilon), \quad |x_i^G| = k_i q_0^3(q_0^3+\varepsilon),$$

where $\varepsilon = 1$ if m divides $q_0 - 1$, otherwise $\varepsilon = -1$ (here $|x_i^{G_0}| = |x_i^{\mathrm{PGL}_2(q)}| = q_0^3(q_0^3+\varepsilon)$ and k_i denotes the number of distinct G_0-classes that are fused under the action of field automorphisms in G). Therefore, the contribution to $\widehat{Q}(G)$ from elements of order m is equal to

$$\sum_{i=1}^{t} \frac{(k_i q_0(q_0+\varepsilon))^2}{k_i q_0^3(q_0^3+\varepsilon)} = \frac{1}{2}(m-1) \cdot \frac{(q_0+\varepsilon)^2}{q_0(q_0^3+\varepsilon)}.$$

If m divides $q_0 + 1$ then $m - 1 \leqslant q_0$ and there are at most $\log(q_0+1)$ possibilities for m, so the total contribution to $\widehat{Q}(G)$ from these elements is at most

$$f_1(q_0) = \log(q_0+1) \cdot \frac{1}{2}q_0 \cdot \frac{(q_0-1)^2}{q_0(q_0^3-1)}.$$

Similarly, the contribution from the elements with m dividing $q_0 - 1$ is no more than

$$f_2(q_0) = \log(q_0-1) \cdot \frac{1}{2}(q_0-2) \cdot \frac{(q_0+1)^2}{q_0(q_0^3+1)}.$$

Finally, let us assume $x \in G$ is a field automorphism of order m. As above, if $m = 2$ then $|x^G| \geqslant \frac{1}{2}q^{1/2}(q+1) = b_3$ and there are at most $a_3 = q_0^{1/2}(q_0+1)$ of these elements in H. Next suppose $m = 3$. Here $|x^G| \geqslant q_0^2(q_0^4+q_0^2+1) = b_4$ and we may assume $H = C_G(x)$, which implies that H contains at most

$$2\left(1 + i_3(\mathrm{L}_2(q_0))\right) \leqslant 2\left(1 + \frac{|\mathrm{GL}_2(q_0)|}{(q_0-1)^2}\right) = 2q_0(q_0+1) + 2 = a_4$$

such elements. If $m = 5$ then $|x^G| > q_0^{36/5} = b_5$ and there are at most $8q_0^{12/5} = a_5$ of these elements in H. Finally, if $m \geqslant 7$ then $|x^G| > q_0^{54/7} = b_6$ and we observe that $|H| \leqslant q_0(q_0^2-1)\log q = a_6$.

Set $\alpha = 1$ if $q_0 = q_1^2$ for some q_1, otherwise $\alpha = 0$. Similarly, let $\beta = 1$ if $q_0 = q_1^5$ and $\gamma = 1$ if $q_0 = q_1^m$ for some prime $m \geqslant 7$ (otherwise $\beta = 0$ and $\gamma = 0$, respectively). Then by bringing all of the above estimates together, we conclude that

$$\widehat{Q}(G) < f_1(q_0) + f_2(q_0) + \left(a_1^2/b_1 + a_2^2/b_2 + a_4^2/b_4\right) + \alpha a_3^2/b_3 + \beta a_5^2/b_5 + \gamma a_6^2/b_6$$

and one checks that this upper bound is less than $1/2$ for all $q_0 \geqslant 7$. Finally, the cases with $q_0 \in \{4, 5\}$ can be checked using Magma. □

5. Proof of Theorem 1.1

In this section we complete the proof of Theorem 1.1. Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$ with socle G_0 and point stabiliser H. Recall that our goal is to show that the Saxl graph $\Sigma(G)$ has the following property:

($\star$) *Any two vertices in $\Sigma(G)$ have a common neighbour*

which immediately implies that $\Sigma(G)$ has diameter 2. In view of Propositions 2.2, 4.8 and 4.17, we may assume $G \in \mathcal{G} \setminus \mathcal{L}$ and $Q(G) \geqslant 1/2$, so the relevant groups can be determined by inspecting Tables 2 and 3 (see Theorem 3.1). In every one of these cases, we can verify property ($\star$) using Magma.

To do this, we first construct G and H using the functions

`AutomorphismGroupSimpleGroup` and `MaximalSubgroups`.

Next we identify a set R of (H, H) double coset representatives and then for each $x \in R$ we seek an element $y \in G$ (by random search) such that $H \cap H^y = H^x \cap H^y = 1$. Notice that ($\star$) holds if and only if such an element y exists for each $x \in R$. As demonstrated by the following example, it is easy to implement this approach in Magma.

Example 5.1. Suppose $G_0 = \Omega_8^+(2)$, $G = G_0.3$ and H is of type $\mathrm{O}_2^-(2) \times \mathrm{GU}_3(2)$. Here $Q(G) = 2071/2800 > 1/2$ and so this is one of the cases we need to consider. We proceed as follows, noting that G has a unique conjugacy class of maximal subgroups of order 11664:

```
G:=AutomorphismGroupSimpleGroup("O+",8,2);
S:=LowIndexSubgroups(G,2);
G:=S[1];
M:=MaximalSubgroups(G:OrderEqual:=11664);
H:=M[1]`subgroup;
R,T:=DoubleCosetRepresentatives(G,H,H);
z:=0;
for x in R do
  if exists(y){y : y in G | #(H meet H^y) eq 1 and #(H^x meet H^y) eq 1}
    then z:=z+1;
  end if;
end for;
z eq #R;
```

This returns `true` and we conclude that ($\star$) holds. An entirely similar approach is effective for all of the relevant groups in Tables 2 and 3.

6. Proof of Theorems 1.3 and 1.5

Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group in $\mathcal{G}$ with socle G_0 and point stabiliser H. Let $\omega(G)$ and $\alpha(G)$ denote the clique and independence numbers of $\Sigma(G)$, respectively.

6.1. Clique number. In view of Proposition 2.2 and Theorem 3.1, together with our work in Sections 4.1 and 4.2, it remains to verify the bound $\omega(G) \geqslant 5$ for the groups appearing in Tables 2 and 3. With the aid of Magma, this is a straightforward exercise, working with a suitable permutation representation of G and H. For example, the following function for checking the bound $\omega(G) \geqslant 5$ can be used effectively in every case. This uses the fact that $\omega(G) \geqslant 5$ if and only if there exist elements $x_2, \ldots, x_5$ in G such that $H^{x_i} \cap H^{x_j} = 1$ for all distinct $i, j \in \{1, \ldots, 5\}$, where $x_1 = 1$.

```
clique:=function(G,H);
exists(x2){y : y in G | #(H meet H^y) eq 1};
exists(x3){y : y in G | #(H meet H^y) eq 1 and #(H^x2 meet H^y) eq 1};
exists(x4){y : y in G | #(H meet H^y) eq 1 and #(H^x2 meet H^y) eq 1
  and #(H^x3 meet H^y) eq 1};
exists(x5){y : y in G | #(H meet H^y) eq 1 and #(H^x2 meet H^y) eq 1
  and #(H^x3 meet H^y) eq 1 and #(H^x4 meet H^y) eq 1};
return "omega(G) is at least 5";
end function;
```

6.2. Independence number. Now let us turn to the independence number $\alpha(G)$ of $\Sigma(G)$. Here we apply work of Magaard and Waldecker [35, 36] and we begin with the following trivial observation.

Lemma 6.1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a permutation group and let c be a positive integer. Then $\alpha(G) \leqslant c$ only if every $(c+1)$-point stabiliser in G is trivial.*

Proposition 6.2. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a group in $\mathcal{G}$ with socle G_0 and point stabiliser H. Then $\alpha(G) = 2$ if and only if $G = A_5$ and Ω is the set of 2-element subsets of $\{1, \ldots, 5\}$.*

Proof. First assume $G = G_0$ is simple. We apply [35, Theorem 3.20], which gives a complete list of all the finite simple transitive groups with the property that every 3-point stabiliser is trivial. The theorem implies that $G = \mathrm{L}_2(q)$, ${}^2B_2(q)$ or $\mathrm{L}_3(4)$, and by inspection (using [9, Theorem 2]) we deduce that $G = \mathrm{L}_2(4)$ with $H = D_6$ is the only example with G primitive and $b(G) = 2$. Here $\Sigma(G)$ is the Johnson graph $J(5, 2)$ and $\alpha(G) = 2$ (note that G is permutation isomorphic to A_5 acting on the set of 2-element subsets of $\{1, \ldots, 5\}$).

Now assume $G \neq G_0$. Then $G_0 \leqslant \mathrm{Sym}(\Omega)$ is a transitive group and every 3-point stabiliser is trivial, so as above the possibilities for G_0 and Ω are described in [35, Theorem 3.20] and by appealing to [35, Theorem 1.3] we see that $G_0 = \mathrm{L}_2(q)$ with $q = p^f$. More precisely, either p is odd and $G = \mathrm{PGL}_2(q)$ or $G_0.2 = \langle G_0, \delta\phi^{f/2} \rangle$ (in the notation of Section 4), or $p = 2$, f is a prime and $G = \mathrm{Aut}(G_0)$. The cases with $q \in \{4, 5\}$ can be checked using Magma [4] and we find that there are no groups $G \neq G_0$ with $\alpha(G) = 2$. Finally, let us assume $q \geqslant 7$, in which case the relevant possibilities are labelled (a)–(d) in [35, Theorem 3.20(1)]. In (a) and (d), it is easy to check that $b(G_0) > 2$, while the groups in (b) and (c) are imprimitive. Therefore, none of these cases arise and the proof is complete. □

Proposition 6.3. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be a group in $\mathcal{G}$ with socle G_0 and point stabiliser H. Then $\alpha(G) \neq 3$.*

Proof. Seeking a contradiction, suppose $\alpha(G) = 3$, in which case every 4-point stabiliser is trivial. We may also assume that there exists a nontrivial 3-point stabiliser. If $G = G_0$ then the possibilities for G are described in [36, Theorem 1.1(i)], but we find that there are no compatible examples with G primitive, H soluble and $b(G) = 2$. The cases with $G \neq G_0$ are recorded in [36, Theorem 1.2] and once again we see that there are no valid examples. □

This completes the proof of Theorems 1.3 and 1.5.

7. Proof of Theorem 1.6

In this final section we prove Theorem 1.6 on the groups $G \in \mathcal{G}$ with a unique regular suborbit. If $G \in \mathcal{L}$ then we refer the reader to Propositions 4.10 and 4.18, so we may assume $G \in \mathcal{G} \setminus \mathcal{L}$. If $Q(G) \geqslant 1/4$ then we can simply read off the relevant groups in Tables 2 and 3, so we may assume $Q(G) < 1/4$. Then in view of (3), it follows that G has a unique regular suborbit only if

$$|H|^2 > \frac{3}{4}|G|,$$

where H is a point stabiliser. The following result reveals that there are no such groups and this completes the proof of Theorem 1.6.

Proposition 7.1. *Let G be a group in $\mathcal{G} \setminus \mathcal{L}$ with point stabiliser H. If $Q(G) < 1/4$ then $|H|^2 \leqslant \frac{3}{4}|G|$.*

Proof. First assume $G_0 = A_m$ is an alternating group. If $m \leqslant 12$ then it is easy to verify the desired bound with the aid of Magma. On the other hand, if $m > 12$ then by inspecting [31, Table 14] and [9, Table 4] we deduce that m is a prime, $H = \mathrm{AGL}_1(m) \cap G$ and we have

$$\frac{|H|^2}{|G|} \leqslant \frac{m(m-1)}{(m-2)!} < \frac{3}{4}$$

as required. Similarly, if G_0 is a sporadic group then the possibilities for G and H can be determined by combining the information in Table 2 and [9, Table 4] with the tables of maximal subgroups in [40]. In each case, it is a straightforward exercise to show that $|H|^2 \leqslant \frac{3}{4}|G|$.

Next suppose G_0 is an exceptional group of Lie type. Then either $H = N_G(T)$ for some maximal torus T of G_0 (see [32, Table 5.2]), or (G, H) is recorded in Table 4. One can now verify the bound $|H|^2 \leqslant \frac{3}{4}|G|$ by inspection. For example, if $G_0 = {}^2B_2(q)$ with $q = 2^f$ and $f \geqslant 3$ odd, then $|G| \geqslant q^2(q^2+1)(q-1)$ and by inspecting [32, Table 5.2] we deduce that $|H| \leqslant 4(q+\sqrt{2q}+1)\log q$. A routine calculation shows that $|H|^2 \leqslant \frac{3}{4}|G|$.

Finally, let us assume G_0 is a classical group. Then (G, H) is one of the cases recorded in Table 5 and once again the result follows by inspection (recall that in each case, the precise structure of H is given in [28]). For instance, if $G_0 = \mathrm{L}_4^{\varepsilon}(q)$ and H is of type $\mathrm{GL}_1^{\varepsilon}(q) \wr S_4$ with $q \geqslant 3$, then $|H| \leqslant 48(q+1)^3 \log q$ and the result follows since $|G| > \frac{1}{8}q^{15}$. In fact, one can check that the only case in Table 5 with $|H|^2 > \frac{3}{4}|G|$ is where $G = \mathrm{PGSp}_6(3)$ and H is of type $\mathrm{Sp}_2(3) \wr S_3$. But $b(G) = 3$ in this case (see [9, Table 7]), so this is not a group in $\mathcal{G}$. □

References

[1] Michael Aschbacher, *On the maximal subgroups of the finite classical groups*, Invent. Math. **76** (1984), no. 3, 469–514.

[2] Michael Aschbacher and Gary M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63** (1976), 1–91.

[3] Robert F. Bailey and Peter J. Cameron, *Base size, metric dimension and other invariants of groups and graphs*, Bull. Lond. Math. Soc. **43** (2011), no. 2, 209–242.

[4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, vol. 24, 1997, Computational algebra and number theory (London, 1993), pp. 235–265.

[5] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society Lecture Note Series, vol. 407, Cambridge University Press, Cambridge, 2013.

[6] T. Breuer, *The GAP Character Table Library, Version 1.3.1*, April 2020, `http://www.math.rwth-aachen.de/~Thomas.Breuer/ctbllib`, GAP package.

[7] Timothy C. Burness, *On base sizes for actions of finite classical groups*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 545–562.

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

[9] ———, *Base sizes for primitive groups with soluble stabilisers*, Algebra Number Theory **15** (2021), no. 7, 1755–1807.

[10] Timothy C. Burness and Michael Giudici, *Classical groups, derangements and primes*, Australian Mathematical Society Lecture Series, vol. 25, Cambridge University Press, Cambridge, 2016.

[11] ———, *On the Saxl graph of a permutation group*, Math. Proc. Cambridge Philos. Soc. **168** (2020), no. 2, 219–248.

[12] Timothy C. Burness, Robert M. Guralnick, and Jan Saxl, *On base sizes for symmetric groups*, Bull. Lond. Math. Soc. **43** (2011), no. 2, 386–391.

[13] ———, *Base sizes for $\mathcal{S}$-actions of finite classical groups*, Israel J. Math. **199** (2014), no. 2, 711–756.

[14] Timothy C. Burness and Scott Harper, *Finite groups, 2-generation and the uniform domination number*, Israel J. Math. **239** (2020), no. 1, 271–367.

[15] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. (3) **98** (2009), no. 1, 116–162.

[16] Timothy C. Burness, E. A. O'Brien, and Robert A. Wilson, *Base sizes for sporadic simple groups*, Israel J. Math. **177** (2010), 307–333.

[17] Timothy C. Burness and Adam R. Thomas, *Computations concerning the classification of extremely primitive groups*, `http://seis.bristol.ac.uk/~tb13602/epcomp.pdf`.

[18] ———, *The classification of extremely primitive groups*, Int. Math. Res. Not. IMRN (2022), no. 13, 10148–10248.

[19] Huye Chen and Shaofei Du, *On the Burness-Giudici conjecture*, 2020, `https://arxiv.org/abs/2008.04233`.

[20] Jiyong Chen and Hong Yi Huang, *On valency problems of Saxl graphs*, J. Group Theory **25** (2022), no. 3, 543–577.

[21] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker, and Robert A. Wilson, ATLAS *of finite groups*, Oxford University Press, Eynsham, 1985.

[22] Hülya Duyan, Zoltán Halasi, and Attila Maróti, *A proof of Pyber's base size conjecture*, Adv. Math. **331** (2018), 720–747.

[23] 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** (1990), no. 4, 347–356.

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

[25] ———, *Bases of twisted wreath products*, J. Algebra **607** (2022), 247–271.

[26] Joanna B. Fawcett, Jürgen Müller, E. A. O'Brien, and Robert A. Wilson, *Regular orbits of sporadic simple groups*, J. Algebra **522** (2019), 61–79.

[27] Joanna B. Fawcett, Eamonn A. O'Brien, and Jan Saxl, *Regular orbits of symmetric and alternating groups*, J. Algebra **458** (2016), 21–52.

[28] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990.

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

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

[31] Cai Heng Li and Hua Zhang, *The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs*, Proc. Lond. Math. Soc. (3) **103** (2011), no. 3, 441–472.

[32] Martin W. Liebeck, Jan Saxl, and Gary M. Seitz, *Subgroups of maximal rank in finite exceptional groups of Lie type*, Proc. London Math. Soc. (3) **65** (1992), no. 2, 297–325.

[33] Martin W. Liebeck and Aner Shalev, *Simple groups, permutation groups, and probability*, J. Amer. Math. Soc. **12** (1999), no. 2, 497–520.

[34] ———, *Bases of primitive permutation groups*, in Groups, combinatorics & geometry (Durham, 2001), World Sci. Publ., River Edge, NJ, 2003, pp. 147–154.

[35] Kay Magaard and Rebecca Waldecker, *Transitive permutation groups where nontrivial elements have at most two fixed points*, J. Pure Appl. Algebra **219** (2015), no. 4, 729–759.

[36] ———, *Transitive permutation groups with trivial four point stabilizers*, J. Group Theory **18** (2015), no. 5, 687–740.

[37] László Pyber, *Asymptotic results for permutation groups*, in Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 197–219.
[38] J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
[39] Ákos Seress, *The minimal base size of primitive solvable permutation groups*, J. London Math. Soc. (2) **53** (1996), no. 2, 243–255.
[40] Robert A. Wilson, *Maximal subgroups of sporadic groups*, in Finite simple groups: thirty years of the atlas and beyond, Contemp. Math., vol. 694, Amer. Math. Soc., Providence, RI, 2017, pp. 57–72.
[41] Robert A. Wilson et al., *A World-Wide-Web Atlas of finite group representations*, `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

Timothy C. Burness, School of Mathematics, University of Bristol, Bristol, BS8 1UG (UK)
E-mail : `t.burness@bristol.ac.uk`

Hong Yi Huang, School of Mathematics, University of Bristol, Bristol, BS8 1UG (UK)
E-mail : `hy.huang@bristol.ac.uk`