On Valency Problems of Saxl Graphs of Almost Simple Primitive Groups with Soluble Stabiliser

Hongyi Huang

Supervisor: Cai Heng Li, Department of Mathematics

[ABSTRACT]: Let G be a permutation group acting on Ω. A base of G is a subset of Ω such that its point-wise stabiliser is trivial. The Saxl graph is a graph whose vertex set is Ω and two vertices are adjacent if they form a base. The valency of Saxl graph of G is also called the valency of G, denoted by $\mathrm{val}(G)$. In this paper we determine the valencies of almost simple primitive groups with socle A_n and soluble stabiliser. We also completely classify almost simple primitive groups G with $\mathrm{val}(G)$ a prime power, which is based on the classification of finite simple groups.

[Keywords]: Bases, Saxl Graphs, Almost Simple Primitive Groups

Contents

1 Preliminaries

1.1 Permutation Groups

A subgroup G of the symmetric group $\mathrm{Sym}(\Omega)$ is said to be a *permutation group* acting on Ω. We assume Ω is finite from now on, and hence G is finite. For $\omega \in \Omega$, the *stabiliser* G_ω of ω in G is given by $G_\omega = \{g \in G \mid \omega^g = \omega\}$. It is straightforward to see that $G_\omega \leqslant G$, and if $G_\omega = \{1\}$ for all $\omega \in \Omega$, we say G is *semiregular* on Ω.

An *orbit* ω^G of G on Ω is a subset of Ω such that $\omega^G = \{\omega^g \mid g \in G\}$ for some $\omega \in \Omega$. It is also easy to see that orbits of G give a partition of Ω into equivalent classes and $|\omega^G| = |G : G_\omega|$. An orbit of G_ω acting on $\Omega \backslash \{\omega\}$ is called a *suborbit* of G, the length of which is called a *subdegree* of G. Further, if G has only one orbit on Ω, we say G is *transitive* on Ω. A transitive semiregular group is called a *regular* group.

Let G be a transitive group on Ω. Then all the stabilisers are conjugate, and the action of G on Ω is equivalent to the action of G on $[G : G_\omega]$ by right multiplications. Hence, by considering a transitive group action, we may equivalently consider the corresponding coset action.

Note that an action of G on Ω induces an action of G on $\Omega \times \Omega$ given by $(\omega_1, \omega_2)^g = (\omega_1^g, \omega_2^g)$. An *orbital* of G acting on Ω is an orbit of G on $\Omega \times \Omega$. Let G be transitive on Ω. Then $\{(\omega, \omega) : \omega \in \Omega\}$ is an orbital. An orbital is *self-paired* if (ω_1, ω_2) and (ω_2, ω_1) are both in the orbital for all (equivalently, for some, if G is transitive) (ω_1, ω_2) in the orbital. The number of orbitals of G is said to be the *rank* of G. If G is of rank 2 then G is said to be 2-*transitive*.

A permutation group G is said to be k-*transitive* if G is transitive on the set of all k-tuples of distinct elements of Ω, where the action is component-wise. Note that G is $(k-1)$-transitive if G is k-transitive ($k \geqslant 2$). The classification of 2-transitive groups has been done. The soluble case is done in [1] and the insoluble case is done in [2], and so this kind of permutation groups are known (a complete list is given in many places, for example [3]). A permutation group is said to be *sharply k-transitive* if also the intersection of stabilisers of k distinct elements is trivial. A permutation group is said to be *Frobenius* if some non-trivial element fixes a point and no non-trivial element fixes more than two points.

Let G be a transitive permutation group. A *block system* $\mathcal{B} = \{B_1, \ldots, B_k\}$ of G on Ω is a G-invariant partition of Ω. That is, for any $i \in \{1, \ldots, k\}$ and $g \in G$, $B_i^g = B_j$ for some $j \in \{1, \ldots, k\}$. Each element in $\mathcal{B}$ is called a *block*. Note that there are always two block systems of G: $k = 1$ or $k = |\Omega|$ – these two block systems are said to be trivial. G is said to be *imprimitive* if there exists a non-trivial block system, and *primitive* otherwise. We have

Proposition 1.1. *Let G be a transitive permutation group.*

(i) If G is 2-transitive then G is primitive.

(ii) If G is primitive then every non-trivial normal subgroup of G is transitive.

(iii) G is primitive if and only if the stabiliser G_ω is maximal.

Proof. If G is 2-transitive then every two distinct points cannot be in a block unless the block is Ω itself. This gives (i). Orbits of a normal subgroup of G form a block system of G and (ii) holds. If H is such that $G_\omega < H < G$ then ω^H is a block. Conversely, if G is imprimitive, then the stabiliser of a block lies strictly between G_ω and G. Hence, (iii) holds. $\square$

The classification of primitive groups into types will be given in Theorem 1.11. A transitive group is said to be *quasi-primitive* if every non-trivial normal subgroup of G is transitive. By Proposition 1.1 (ii), a primitive group is quasi-primitive.

1.2 Transitive Graphs

Let Γ be a simple undirected graph, we write by $V\Gamma$ its vertex set and by $E\Gamma$ its edge set. For convenience, we denote $v \sim w$ if vertices v and w are adjacent. An *automorphism* of Γ is a permutation of vertices preserving edges, that is, a permutation $g \in \mathrm{Sym}(V\Gamma)$ such that $v \sim w$ if and only if $v^g \sim w^g$. All such automorphisms of Γ form a subgroup of $\mathrm{Sym}(V\Gamma)$. This group is called the *automorphism group* of Γ, denoted by $\mathrm{Aut}(\Gamma)$.

Let $G \leqslant \mathrm{Aut}(\Gamma)$. Note that G is a permutation group on $V\Gamma$. We say Γ is *G-vertex-transitive* if G is transitive on $V\Gamma$. Also, we say Γ is *G-edge-transitive* (or *G-arc-transitive*) if the induced action of G on $E\Gamma$ (or the set of arcs of Γ) is transitive. Similar definitions can be defined for other kinds of permutation groups, such as regular groups and semiregular groups.

If Γ is a regular graph, we call the *valency* of Γ, denoted by $\mathrm{val}(\Gamma)$, the number of adjacent vertices with a fixed vertex.

Recall that an orbital of a permutation group G acting on Ω is an orbit of G with the induced action on $\Omega \times \Omega$. Let $\mathcal{O}$ be an orbital of G. Then we can define a graph whose vertex set is Ω and (ω_1, ω_2) is a directed edge if $(\omega_1, \omega_2) \in \mathcal{O}$. This graph is called an *orbital graph* of G on Ω with orbital $\mathcal{O}$. An orbital graph is undirected if and only if the corresponding orbital is self-paired. A *generalised orbital graph* of a group G acting on Ω is a union of some orbital graphs of G.

Let G be a group, H a subgroup of G and S a subset of $G \backslash H$. The coset graph $\Gamma = \mathrm{Cos}(G, H, HSH)$ is a graph whose vertex set is $[G : H]$ and (Hx, Hy) is a directed edge if $yx^{-1} \in HSH$. It is easy to see that this graph is well-defined. We have the following observations on coset graphs.

Proposition 1.2. *Let* $\Gamma = \mathrm{Cos}(G, H, HSH)$. *Then*

1. $G \leqslant \mathrm{Aut}(\Gamma)$ *and* H *(as a group) is the stabiliser of* H *(as a vertex).*

2. Γ *is undirected if and only if* $HSH = (HSH)^{-1} = HS^{-1}H$.

3. Γ *is connected if and only if* $\langle H, S \rangle = G$.

Coset graphs and orbital graphs give a more group theoretic view of transitive graphs. Indeed, we have

Proposition 1.3. *Let* Γ *be a graph. Then*

1. Γ *is vertex-transitive if and only if* Γ *is isomorphic to a coset graph, if and only if* Γ *is isomorphic to a generalised orbital graph.*

2. Γ *is arc-transitive if and only if* Γ *is isomorphic to an orbital graph, if and only if* Γ *is isomorphic to a coset graph* $\mathrm{Cos}(G, H, HSH)$ *with* $|S| = 1$.

In particular, when $H = 1$, the coset graph $\mathrm{Cos}(G, H, HSH)$ becomes a Cayley graph $\mathrm{Cay}(G, S)$. In general, a *Cayley graph* $\mathrm{Cay}(G, S)$ of a group G and a subset S of $G \backslash \{1\}$ is a graph whose vertex set is G and (x, y) is a directed edge if $yx^{-1} \in S$.

Proposition 1.4. *A graph* Γ *is a Cayley graph if and only if there is a regular subgroup of* $\mathrm{Aut}(\Gamma)$.

1.3 Some Products of Groups

Let G be a group and H, K subgroups of G. The subset HK of G is defined by $HK := \{hk \mid h \in H, k \in K\}$. An easy exercise in group theory gives that HK is a subgroup of G if and only if $HK = KH$. If $HK \leqslant G$, then we say HK is a *product* of subgroups H and K.

Now we focus on different cases of H and K in G.

If H is normal in G and $H \cap K = 1$, then HK is said to be a *semi-direct product* of H by K. In this case, we usually write $H{:}K$ instead of HK. If H is normal in G and K induces a subgroup of $\mathrm{Aut}(H)$ by conjugation, then HK is a semi-direct product, and vice versa. Further, if also $K \lhd G$, then HK is said to be a *direct product* of H and K in G. In this case, we write $H \times K = HK$.

Note that for any group X, $\mathrm{Aut}(X^n)$ has a subgroup isomorphic to $\mathrm{Sym}(n)$ by permuting coordinates. If $H = X^n$ for some subgroup X of G and $n \geqslant 2$, and further K induces a subgroup (by conjugation) of $\mathrm{Sym}(n)$ by φ, then we say $HK = X^n K$ is a *wreath product* of X by K, denoted by $X \wr_{\varphi} K$. If there is no ambiguity on φ, we will write $X \wr K$.

If H and K are commutative, that is, for any $h \in H$ and $k \in K$, $hk = kh$, then HK is said to be a *central product*, denoted by $H \circ K$.

We will also denote by $H.K$ a group which has a normal subgroup that is isomorphic to H and the corresponding quotient group (over H) is isomorphic to K. This group is also called an *extension* of K by H.

1.4 Soluble Groups

Let G be a finite group. A *composition series* of G is a series

$$G = H_1 \rhd H_2 \rhd \cdots \rhd H_n = 1$$

such that each H_{i+1} is a maximal normal subgroup of H_i, or equivalently each quotient group H_i/H_{i+1}, which is called a *composition factor*, is simple. Jordan-Hölder theorem states that any two composition series of G have the same length and the same composition factors up to permutation.

A group G is called *soluble* if each composition factor of G is abelian. Equivalently,

G is soluble if and only if the derived series of G is such that

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(m)} = 1.$$

Soluble groups play a significant role in the study of group theory. Many famous theorems give sufficient conditions for solubility based on the group orders. For example

Theorem 1.5 (Burnside, 1904)**.** *Every group of order $p^a q^b$ for some primes p, q and $a, b \geqslant 0$ is soluble.*

Theorem 1.6 (Feit–Thompson, 1963)**.** *Every group of odd order is soluble.*

Corollary 1.7. *Every group with a cyclic Sylow 2-subgroup is soluble.*

Let π be a subset of the set of prime divisors of $|G|$. A Hall π-subgroup of G is a subgroup whose order is a product of primes in π and is coprime with its index. Denote by π' the complement of π in the set of prime divisors of $|G|$.

Theorem 1.8 (Hall, 1928)**.** *A finite group is soluble if and only if its Hall π-subgroup exists for any set of prime divisors π.*

1.5 Linear Groups

Suppose V is a vector space. Denote by $\mathrm{GL}(V)$ the group of all invertible linear transformations on V, which is called the *general linear group* on V. From now on we suppose V is a finite dimensional vector space over a finite field $\mathbb{F}_q$, where q is a prime power. In this case, we write $\mathrm{GL}_n(q)$ for $\mathrm{GL}(V)$ with $\dim V = n$. The order of $\mathrm{GL}_n(q)$ is

$$|\,\mathrm{GL}_n(q)| = \prod_{k=0}^{n-1}(q^n - q^k) = q^{n(n-1)/2}\prod_{k=1}^{n}(q^k - 1).$$

$\mathrm{GL}_n(q)$ is abelian if and only if $n = 1$, in which case $\mathrm{GL}_1(q) \cong \mathbb{Z}_{q-1}$.

Denote by $\mathrm{SL}_n(q)$ the subgroup of $\mathrm{GL}_n(q)$ of all operators in $\mathrm{GL}_n(q)$ of determinant 1, which is called the *special linear group* of $\mathbb{F}_q^n$. The order of $\mathrm{SL}_n(q)$ is

$$|\,\mathrm{SL}_n(q)| = \frac{|\,\mathrm{GL}_n(q)|}{q-1}.$$

When $n = 1$, the special linear group is trivial. For $n \geqslant 2$, $\mathrm{SL}_n(q)$ is perfect (that is, $\mathrm{SL}_n(q)$ is equal to its derived subgroup) except when $(n, q) = (2, 2)$ or $(2, 3)$.

The centre of $\mathrm{GL}_n(q)$ is the group of all non-zero scalar multiples of identity, which has order $q-1$. The *projective general linear group* of $\mathrm{GL}_n(q)$, denoted by $\mathrm{PGL}_n(q)$, is the quotient group of $\mathrm{GL}_n(q)$ by its centre. The order of $\mathrm{PGL}_n(q)$ is

$$|\mathrm{PGL}_n(q)| = \frac{|\mathrm{GL}_n(q)|}{|Z(\mathrm{GL}_n(q))|} = \frac{|\mathrm{GL}_n(q)|}{q-1}.$$

Note that $\mathrm{PGL}_n(q)$ and $\mathrm{SL}_n(q)$ have the same order. Indeed, these two groups are not isomorphic when $n \geqslant 2$: $\mathrm{PGL}_n(q)$ is centreless but $\mathrm{SL}_n(q)$ is not. The centre of $\mathrm{SL}_n(q)$ is $\mathrm{SL}_n(q) \cap Z(\mathrm{GL}_n(q))$, which has order $\gcd(2, q-1)$. Denote $\mathrm{PSL}_n(q)$ by the quotient group of $\mathrm{SL}_n(q)$ by its centre, which is called the *projective special linear group* and has order

$$|\mathrm{PSL}_n(q)| = \frac{|\mathrm{SL}_n(q)|}{|Z(\mathrm{SL}_n(q))|} = \frac{|\mathrm{GL}_n(q)|}{(q-1)\gcd(n, q-1)}.$$

When $n \geqslant 2$, $\mathrm{PSL}_n(q)$ is simple unless $(n, q) = (2, 2)$ or $(2, 3)$.

The *affine general linear group* $\mathrm{AGL}_n(q)$ is the group of all affine transformations of $\mathbb{F}_q^n$. We have $\mathrm{AGL}_n(q) = \mathbb{F}_q^+ {:} \mathrm{GL}_n(q)$. This group is 2-transitive on $\mathbb{F}_q^n$. In particular, when $n = 1$, $\mathrm{AGL}_1(q) \cong \mathbb{Z}_q{:}\mathbb{Z}_{q-1}$. Similarly we have the *affine special linear group* $\mathrm{ASL}_n(q) = \mathbb{F}_q^+ {:} \mathrm{SL}_n(q)$.

1.6 Bases and Saxl Graphs

Let G be a permutation group acting on a set Ω. Then $\Delta \subseteq \Omega$ is called a *base* if the point-wise stabiliser $G_{(\Delta)} = 1$. The *base size* $b(G)$ of G is the size of smallest base of G, and a base Δ is said to be a *base size set* if $|\Delta| = b(G)$. Here are some easy observations.

Proposition 1.9. *Let G be a transitive permutation group on Ω.*

(a) G is regular if and only if $b(G) = 1$, if and only if every non-empty subset of Ω is a base.

(b) G is Frobenius if and only if every 2-subset of Ω is a base size set. In this case $b(G) = 2$.

(c) G is sharply k-transitive if and only if every k-subset of Ω is a base size set. In this case $b(G) = k$.

For a permutation group G with $b(G) = 2$ we can define a graph called Saxl graph, named after Jan Saxl who proposed determining all the base-two primitive groups. This concept was first introduced by Timothy Burness and Michael Giudici in [4].

The *Saxl graph* $\Sigma = \Sigma(G)$ of a permutation group G acting on Ω is defined by $V\Sigma = \Omega$ and two vertices are adjacent if they form a base. That is, $E\Sigma = \{\{\alpha, \beta\} \mid \alpha, \beta \in V\Sigma, G_\alpha \cap G_\beta = 1\}$. It is easy to see that Saxl graphs are undirected. Moreover, if $b(G) \geqslant 3$ then $\Sigma(G)$ is empty and if $b(G) = 1$ then $\Sigma(G)$ is complete. Hence, to characterize Saxl graphs, we only need to consider those permutation groups G with $b(G) = 2$.

Proposition 1.10 ([4])**.** *Let G be a transitive permutation group on Ω with $b(G) = 2$ and let $\Sigma(G)$ be the Saxl graph of G.*

(i) $\Sigma(G)$ is G-vertex-transitive.

(ii) $\Sigma(G)$ is complete if and only if G is Frobenius.

(iii) $\Sigma(G)$ is connected if G is primitive.

(iv) $\Sigma(G)$ is G-edge-transitive if G is 2-homogeneous.

(v) $\Sigma(G)$ is G-arc-transitive if G is 2-transitive.

(vi) $\Sigma(G)$ is G-arc-semiregular.

(vii) $\Sigma(G)$ has valency $r|G_\alpha|$, where r is the number of regular suborbits of G.

Proof. For any $g \in G$, $\{\alpha, \beta\}$ is a base of G if and only if $\{\alpha^g, \beta^g\}$ is a base. Then G preserves edges of $\Sigma(G)$ and so (i) holds. (ii) is clear by the definition of Frobenius groups. Connected components of $\Sigma(G)$ forms a block system of G on Ω, which gives (iii). A permutation group is said to be k-homogeneous if it is transitive on the k-sets of permuted points. This immediate gives (iv). (v) is also clear by the definition of 2-transitive groups. An arc of $\Sigma(G)$ is an ordered base of G, and by the definition of bases, the stabiliser is trivial. This gives (vi). Moreover, the edge stabilisers are of order 2. Finally, $\{\alpha, \beta\}$ is a base if and only if G_α acts regularly on β^{G_α}. Thus, the neighbours of α in $\Sigma(G)$ is a union of the regular orbits of G_α and so (vii) follows. □

Many problems are still open on parameters of Saxl graphs, some of which are listed in [4]. The most famous problem in this area is the Burness-Giudici Conjecture.

Conjecture 1 (Burness-Giudici [4]). *Let G be a finite primitive permutation group with $b(G) = 2$ and Saxl graph $\Sigma(G)$. Then either $\Sigma(G)$ is complete or of diameter 2.*

We will later discuss the valency of $\Sigma(G)$ in more detail. For convenience, by the *valency* of a permutation group G, denoted by $\mathrm{val}(G)$, we mean the valency of the Saxl graph of G and by $\mathrm{val}(G, H)$ the valency of G with specific stabiliser H. The valency of G is also the number of orbital graphs with valency $|H|$.

1.7 O'Nan-Scott Theorem on Primitive Groups

Recall that a permutation group G acting on Ω is primitive if there is no non-trivial G-invariant partition of Ω, or equivalently the stabiliser is maximal. The following theorem gives a classification by types of finite primitive groups.

Theorem 1.11 (O'Nan-Scott Theorem [5]). *Let G be a finite primitive group. Then G is of one of the following eight types:*

1. *if G has two minimal normal subgroups, then*
   - (a) *G is of type HS (holomorph simple) if the minimal normal subgroups are simple;*
   - (b) *G is of type HC (holomorph compound) otherwise;*
2. *if G has a unique abelian minimal normal subgroup, then G is of type HA (holomorph affine);*
3. *if G has a unique non-abelian simple minimal normal subgroup, then G is of type AS (almost simple);*
4. *if G has a unique minimal normal subgroup $M \cong T^k$ with $k \geqslant 2$, where T is non-abelian simple, then*
   - (a) *if M is regular on Ω, then G is of type TW (twisted wreath);*
   - (b) *if there exists $N \lhd M$ such that N is regular and $M_\omega \cong T$, then G is of type SD (simple diagonal);*
   - (c) *if there exists $N \lhd M$ such that N is regular and $M_\omega \cong T^l$ with $l \geqslant 2$, then G is of type CD (compound diagonal);*

(d) if every proper normal subgroup of M is intransitive, then G is of type PA (product action).

The definitions of above types are introduced below:

HS: a group G such that $T{:}\,\mathrm{Inn}(T) \leqslant G \leqslant T{:}\,\mathrm{Aut}(T)$, where T is a non-abelian simple group.

HC: a group G such that $T^k{:}\,\mathrm{Inn}(T^k) \leqslant G \leqslant T^k{:}\,\mathrm{Aut}(T^k)$, where T is a non-abelian simple group and $k \geqslant 2$.

HA: a subgroup of $\mathrm{AGL}(d,p)$ containing all translations and the stabiliser is irreducible in $\mathrm{GL}(d,p)$.

AS: a group G such that $\mathrm{Inn}(T) \lesssim G \lesssim \mathrm{Aut}(T)$ for some non-abelian simple group T, or equivalently a group with non-abelian simple *socle* (subgroup generated by all minimal normal subgroups).

TW: a group constructed by a twisted wreath product.

SD: a group $T^k \lhd G \leqslant T^k.(\mathrm{Out}(T) \times S_k) \leqslant \mathrm{Sym}(\Omega)$, where Ω is the right cosets of the diagonal subgroup $\{(t,\ldots,t) \mid t \in T\}$ of T^k and the action is by right multiplication, such that G induces a primitive subgroup of S_k.

CD: a group $G \leqslant H \wr S_k$ acting on Ω^k with H a primitive group of type SD acting on Ω and G induces a transitive subgroup of S_k.

PA: a group $G \leqslant H \wr S_k$ acting on Ω^k with H a primitive group of type AS acting on Ω and G induces a transitive subgroup of S_k.

Cheryl E Praeger generalised O'Nan-Scott Theorem in [6]: any finite quasi-primitive group is one of the above eight types. This theorem is also called O'Nan-Scott-Praeger Theorem.

1.8 Aschbacher's Theorem on Classical Groups

Similar to O'Nan-Scott Theorem on maximal subgroups of symmetric groups, Aschbacher's theorem classifies maximal subgroups of finite classical groups into types.

Theorem 1.12 (Aschbacher [7]). *Let $H \leqslant \mathrm{GL}_n(q)$ with $n \geqslant 2$ be such that $\mathrm{SL}_n(q)$ is not contained in H. Then either H lies in at least one of the classes of subgroups of $\mathrm{GL}_n(q)$ listed in Table 1 or the following hold:*

1. *H is not in $\mathscr{C}_8$,*
2. *$H/Z(H)$ is almost simple, and*
3. *$\mathbb{F}_q^n$ is an absolutely irreducible projective representation of $H/Z(H)$, which is not realisable over a proper subfield of $\mathbb{F}_q$.*

Class	Description
$\mathscr{C}_1$	Stabilisers of subspaces
$\mathscr{C}_2$	Stabilisers of direct sum decompositions $V = \bigoplus_{i=1}^m V_i$, $n = m \dim V_i$
$\mathscr{C}_3$	Stabilisers of extension fields of $\mathbb{F}_q$ of prime degree
$\mathscr{C}_4$	Stabilisers of tensor product decompositions $V = V_1 \otimes V_2$
$\mathscr{C}_5$	Stabilisers of subfields of $\mathbb{F}_q$ of prime index
$\mathscr{C}_6$	Normalisers of symplectic-type or extra-special groups
$\mathscr{C}_7$	Stabilisers of tensor product decompositions $V = \bigotimes_{i=1}^m V_i$, $n = (\dim V_i)^m$
$\mathscr{C}_8$	Stabilisers of non-degenerate classical forms on V

Table 1: Descriptions of classes in Aschbacher's theorem

1.9 Classification of Finite Simple Groups (CFSG)

Theorem 1.13 (CFSG). *Every finite simple group is isomorphic to one of the following groups:*

1. *a cyclic group $\mathbb{Z}_p$ of order p, where p is a prime;*
2. *an alternating group A_n for $n \geqslant 5$;*
3. *a group of Lie type:*
   (a) *linear: $\mathrm{PSL}_n(q)$ for $n \geqslant 3$ or $q \geqslant 4$;*

(b) *symplectic:* $\mathrm{PSp}_{2n}(q)$ *for* $n \geqslant 2$, *except* $\mathrm{PSp}_4(2)$*;*

(c) *unitary:* $\mathrm{PSU}_n(q)$ *for* $n \geqslant 3$, *except* $\mathrm{PSU}_3(2)$*;*

(d) *orthogonal:* $\mathrm{P\Omega}_{2n+1}(q)$ *for* $n \geqslant 3$ *and* q *odd; or* $\mathrm{P\Omega}^{\pm}_{2n}(q)$ *for* $n \geqslant 4$*;*

(e) *exceptional:* $G_2(q)$ *for* $q \geqslant 3$*;* $F_4(q)$*;* $E_6(q)$*;* ${}^2E_6(q)$*;* $E_7(q)$*;* $E_8(q)$*;* ${}^3D_4(q)$*;* ${}^2B_2(2^{2n+1}) = \mathrm{Sz}(2^{2n+1})$*;* ${}^2G_2(3^{2n+1}) = \mathrm{Ree}(3^{2n+1})$*;* ${}^2F_4(2^{2n+1}) = \mathrm{Ree}(2^{2n+1})$*;* ${}^2F_4(2)'$,

where n *is a positive integer and* q *is a prime power;*

4. *one of 26 sporadic simple groups:* M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, Co_1, Co_2, Co_3, McL, HS, Suz, J_1, J_2, J_3, J_4, Fi_{22}, Fi_{23}, Fi'_{24}, $\mathbb{M}$, $\mathbb{B}$, Th, HN, He, O′N, Ly *and* Ru.

There are also some repetitions in the above list. The only repetitions are:

- $\mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5$;
- $\mathrm{PSL}_2(9) \cong A_6$;
- $\mathrm{PSL}_4(2) \cong A_8$;
- $\mathrm{PSL}_3(2) \cong \mathrm{PSL}(2,7)$;
- $\mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$.

The notation of these groups can vary: for example, some authors use $L^+_n(q)$ or $L_n(q)$ for $\mathrm{PSL}_n(q)$, and $L^-_n(q)$ or $U_n(q)$ for $\mathrm{PSU}_n(q)$. We will also use those later.

1.10 Almost Simple Groups and Outer Automorphisms

Recall that a group G is called almost simple if there exists a non-abelian simple group T such that $\mathrm{Inn}(T) \lesssim G \lesssim \mathrm{Aut}(T)$, or equivalently $\mathrm{soc}(G)$ is non-abelian simple. The *outer automorphism group* of a group H is given by the quotient group $\mathrm{Out}(H) := \mathrm{Aut}(H)/\mathrm{Inn}(H)$. For a simple group T, as its centre is trivial, we have $\mathrm{Inn}(T) \cong T/Z(T) \cong T$ and so $\mathrm{Aut}(T) \cong T.\mathrm{Out}(T)$.

For A_n ($n \geqslant 5$), the automorphism group is S_n for $n \neq 6$ and $S_6.2$ for $n = 6$.

For finite simple groups of Lie type, the outer automorphisms only come from three different types: diagonal automorphisms, field automorphisms and graph automorphisms.

The diagonal automorphisms are given by the conjugation of diagonal matrices. It gives a cyclic subgroup of outer automorphism group unless the corresponding simple group is $\mathrm{P}\Omega^{+}_{2n}(q)$ for n even and q odd.

The field automorphisms of a finite simple group of Lie type over a finite field $\mathbb{F}_{p^f}$ forms a cyclic group $\langle \phi \rangle \cong \mathbb{Z}_f$, where $\phi : x \mapsto x^p$ is a field automorphism of $\mathbb{F}_{p^f}$.

A graph automorphism is an automorphism of the corresponding Dynkin diagram (for Chevalley groups). The relation of Chevalley groups and Dynkin diagrams is listed in Table 2.

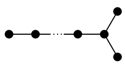
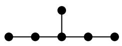
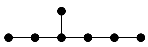
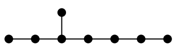
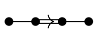
Group	Dynkin diagram	Condition
$\mathrm{PSL}_{n+1}(q)$	A_n	$n \geqslant 1$
$\mathrm{P}\Omega_{2n+1}(q)$	B_n 	$n \geqslant 3$
$\mathrm{PSp}_{2n}(q)$	C_n 	$n \geqslant 2$
$\mathrm{P}\Omega^{+}_{2n}(q)$	D_n 	$n \geqslant 4$
$E_6(q)$	E_6 	
$E_7(q)$	E_7 	
$E_8(q)$	E_8 	
$F_4(q)$	F_4 	
$G_2(q)$	G_2 	

Table 2: Corresponding Dynkin diagrams of Chevalley groups

Outer automorphism groups of finite simple groups of Lie type are given in Table 3 and Table 4. Conditions are given in the tables as well as in Theorem 1.13.

Among 26 sporadic simple groups, only M_{12}, M_{22}, HS, J_2, McL, Suz, He, HN, Fi_{22}, Fi'_{24}, O′N and J_3 have outer automorphism groups of order 2. Other sporadic simple groups have trivial outer automorphism groups.

1.11 Known Results on Valencies

The classification of permutation groups with prime valency has been done in [4]. Indeed, this is an easy exercise of permutation groups.

T	$\mathrm{Out}(T)$	Conditions
$\mathrm{PSL}_n(p^f)$	$\mathbb{Z}_{(n,p^f-1)}{:}(\mathbb{Z}_f \times \mathbb{Z}_2)$	$n > 2$
	$\mathbb{Z}_{(2,p^f-1)} \times \mathbb{Z}_f$	$n = 2$
$\mathrm{PSp}_{2n}(p^f)$	$\mathbb{Z}_2.\mathbb{Z}_f$	$p \neq 2$
	$\mathbb{Z}_f.\mathbb{Z}_2$	$p = 2$, $n = 2$
	$\mathbb{Z}_f$	$p = 2$, $n > 2$
$\mathrm{PSU}_n(q)$	$\mathbb{Z}_{(n,q+1)}.\mathbb{Z}_f$	$q^2 = p^f$
$\mathrm{P}\Omega_{2n+1}(p^f)$	$\mathbb{Z}_{(2,p^f-1)}.\mathbb{Z}_f$	
$\mathrm{P}\Omega^+_{2n}(p^f)$	$\mathbb{Z}^2_{(2,p^f-1)}.\mathbb{Z}_f.S_3$	$n = 4$
	$\mathbb{Z}^2_{(2,p^f-1)}.\mathbb{Z}_f.\mathbb{Z}_2$	$n > 4$ even
	$\mathbb{Z}_{(4,p^{nf}-1)}.\mathbb{Z}_f.\mathbb{Z}_2$	n odd
$\mathrm{P}\Omega^-_{2n}(q)$	$\mathbb{Z}_{(4,q^n+1)}.\mathbb{Z}_f$	$q^2 = p^f$

Table 3: Outer automorphism groups $\mathrm{Out}(T)$ of finite simple classical groups T

Theorem 1.14. *Let G be a transitive permutation group on Ω with $b(G) = 2$. Then G has prime valency p if and only if G is one of the following:*

(i) $G = \mathbb{Z}_p \wr \mathbb{Z}_2$ acting imprimitively on $2p$ points and $\Sigma(G) \cong K_{p,p}$.

(ii) $G = S_3$ with the natural action, $p = 2$ and $\Sigma(G) \cong K_3$.

(iii) $G = \mathrm{AGL}_1(2^f)$ with the natural action, where $p = 2^f - 1$ is a Mersenne prime and $\Sigma(G) \cong K_{p+1}$.

Proof. This is given in [4]. □

The classification of almost simple primitive group in which a point stabiliser has odd order has been done in [8]. Let G be an almost simple primitive permutation group. We can use the classification in [8] to classify those G with $\Sigma(G)$ having odd valency, which is based on CFSG.

Theorem 1.15. *Let G be a non-abelian almost simple group with socle T, and H a maximal subgroup of G of odd order. Then T and H are listed in Table 5.*

T	$\mathrm{Out}(T)$	Condition
$G_2(p^f)$	$\mathbb{Z}_f$	$p \neq 3$
	$\mathbb{Z}_f.\mathbb{Z}_2$	$p = 3$
$F_4(p^f)$	$\mathbb{Z}_f$	$p \neq 2$
	$\mathbb{Z}_f.\mathbb{Z}_2$	$p = 2$
$E_6(p^f)$	$\mathbb{Z}_{(3,p^f-1)}.\mathbb{Z}_f.\mathbb{Z}_2$	
${}^2E_6(q)$	$\mathbb{Z}_{(3,q+1)}.\mathbb{Z}_f$	$q^2 = p^f$
$E_7(p^f)$	$\mathbb{Z}_{(2,p^f-1)}.\mathbb{Z}_f$	
$E_8(p^f)$	$\mathbb{Z}_f$	
${}^3D_4(q)$	$\mathbb{Z}_f$	$q^3 = p^f$
${}^2B_2(2^{2n+1})$	$\mathbb{Z}_{2n+1}$	
${}^2G_2(3^{2n+1})$	$\mathbb{Z}_{2n+1}$	
${}^2F_4(2^{2n+1})$	$\mathbb{Z}_{2n+1}$	
${}^2F_4(2)'$	$\mathbb{Z}_2$	

Table 4: Outer automorphism groups $\mathrm{Out}(T)$ of finite simple exceptional groups T

T	$H \cap T$	Conditions
$L_2(q), q = p^f$	$\mathbb{Z}_p^f{:}\mathbb{Z}_{(p^f-1)/2}$	p prime, $q \equiv 3 \pmod 4$
A_p	$\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$	p prime, $p \equiv 3 \pmod 4$, $p \neq 7, 11, 23$
$L_n^\epsilon(q)$, $\epsilon = \pm 1$	$\mathbb{Z}_a{:}\mathbb{Z}_n$	$a = \frac{q^n-\epsilon}{(q-\epsilon)(n,q-\epsilon)}$, $n \geqslant 3$ prime, $T \neq U_3(3), U_5(2)$
M_{23}	23:11	
Th	31:15	
$\mathbb{B}$	47:23	

Table 5: Primitive almost simple groups with odd order point stabiliser

It follows the classification of almost simple primitive groups of odd valencies.

Theorem 1.16 ([4])**.** *Let G be an almost simple primitive permutation group on Ω with socle T, point stabiliser H. If $b(G) = 2$ and $\mathrm{val}(G)$ is odd, then one of the following holds:*

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

(ii) $G = A_p$ *and* $H = \mathrm{AGL}_1(p) \cap G = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$*, where p is a prime such that* $p \equiv 3 \pmod 4$ *and* $(p-1)/2$ *is composite.*

(iii) $T = L_n^{\epsilon}(q)$, $H \cap T = \mathbb{Z}_a{:}\mathbb{Z}_n$ *and* $G \neq T$*, where* $a = \frac{q^n-\epsilon}{(q-\epsilon)(n,q-\epsilon)}$, $n \geqslant 3$ *is a prime and* $T \neq U_3(3), U_5(2)$.

However, we will later show that the second case cannot happen in Theorem 2.7, and so Theorem 1.16 becomes

Theorem 1.17. *Let G be an almost simple primitive permutation group on Ω with socle T, point stabiliser H. If $b(G) = 2$ and $\mathrm{val}(G)$ is odd, then one of the following holds:*

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

(ii) $T = L_n^{\epsilon}(q)$, $H \cap T = \mathbb{Z}_a{:}\mathbb{Z}_n$ *and* $G \neq T$*, where* $a = \frac{q^n-\epsilon}{(q-\epsilon)(n,q-\epsilon)}$, $n \geqslant 3$ *is a prime and* $T \neq U_3(3), U_5(2)$.

1.12 Some Results in Number Theory

Some results in number theory are useful in finite group theory, especially in finite classical groups because the orders of underlying fields are prime power.

Theorem 1.18 (Catalan's conjecture)**.** *The only solution in the natural numbers of*

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

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

Catalan's conjecture is now a theorem proved by Mihăilescu in [9].

Theorem 1.19 (Zsigmondy [10])**.** *Let a and n be integers greater than 1. There exists a prime divisor p of $a^n - 1$ such that p does not divide $a^j - 1$ for all j, $0 < j < n$, except exactly in the following cases:*

1. $n = 2,\ a = 2^s - 1,\ s \geqslant 2.$

2. $n = 6,\ a = 2.$

There is a useful corollary in the later classification.

Corollary 1.20. *Suppose n is an odd prime and q is a prime power. Then there is no positive integer solution (n, q, k) to*

$$\frac{q^n - 1}{q - 1} = n^k.$$

Proof. Let (n, q, k) be a solution. By Zsigmondy's Theorem, there exists a prime divisor p of $q^n - 1$ such that p does not divide $q - 1$. Hence, p divides $\frac{q^n-1}{q-1} = n^k$ and so $p = n$. However, that means $q \equiv q^n \equiv 1 \pmod{n}$ and thus n divides $q-1$, a contradiction. □

Similarly, we have

Theorem 1.21 (Zsigmondy's theorem for sums [10]). *Let $a > b > 0$ be coprime integers and $n \geqslant 1$. Then there exists a prime divisor p of $a^n + b^n$ such that p does not divide $a^j + b^j$ for all j, $0 < j < n$, except $(n, a, b) = (3, 2, 1)$.*

Corollary 1.22. *Suppose n is an odd prime and q is a prime power. Then the only positive integer solution (n, q, k) to*

$$\frac{q^n + 1}{q + 1} = n^k$$

is $(3, 2, 1)$.

2 Almost Simple Primitive Groups with Soluble Stabilisers

The classification of almost simple primitive groups with soluble stabilisers has been done in [11]. The work in the remaining of this section is based on this paper. Valencies of almost simple primitive groups with socle A_n and soluble stabiliser will be given in Table 7, which deduces Theorem 1.17, and the complete classification of almost simple primitive groups with prime-power valencies will be given in Theorem 2.16.

2.1 Alternating and Symmetric Groups

Let G be an almost simple primitive group with $\mathrm{soc}(G) = A_n$ for $n \geqslant 5$ and soluble stabiliser H. Then by [11], (G, H) are classified in Table 6.

G	H
A_5	S_3, A_4
S_5	D_{12}, S_4
A_6	S_4, S_4, $3^2{:}4$
$A_6.2 \cong \mathrm{M}_{10}$	$\mathrm{AGL}_1(5)$, $8{:}2$, $\mathrm{PSU}_3(2)$
$A_6.2 \cong \mathrm{PGL}_2(9)$	D_{20}, D_{16}, $\mathrm{AGL}_1(9)$
S_6	$S_4 \times S_2$, $S_4 \times S_2$, $S_3 \wr S_2$
A_7	$3{:}S_4$
S_7	$S_3 \times S_4$
A_8	$A_4^2.2^2$
S_8	$(2 \wr S_4).2$, $A_4^2.D_8$
A_9	$\mathrm{ASL}_2(3)$, $3^3{:}S_4$
S_9	$\mathrm{AGL}_2(3)$, $3^3{:}2^2.D_{12}$
A_{12}	$3^4{:}2^3{:}S_4$, $2^6{:}3^3{:}S_4$
S_{12}	$3^4.2 \wr A_4.2$, $2^6.3^3.A_4.2^2$
A_{16}	$2^8.3^4.2^3.S_4$
S_{16}	$2^8.3^4.2 \wr A_4.2$
A_p	$\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$, $p \geqslant 5$ is a prime, $p \neq 7, 11, 17, 23$
S_p	$\mathrm{AGL}_1(p)$, $p \geqslant 5$ is a prime

Table 6: Almost simple primitive group G with $\mathrm{soc}(G) = A_n$ for $n \geqslant 5$ and soluble stabiliser H up to conjugacy

Our aim is to calculate $\mathrm{val}(G)$ with stabiliser H listed in Table 6.

2.1.1 $G = S_p$ and $H = \mathrm{AGL}_1(p)$

We first consider the case when $G = S_p$ and $H = \mathrm{AGL}_1(p)$.

Lemma 2.1. *Let p be a prime. Then a subgroup of $\mathrm{AGL}_1(p)$ either contains the unique Sylow p-subgroup of $\mathrm{AGL}_1(p)$ or is contained in a stabiliser for some element in $\mathbb{F}_p$.*

Proof. Note that $\mathrm{AGL}_1(p)$ is soluble, all Hall p'-groups (in this case, cyclic groups of order $p-1$) are conjugate, and that the stabiliser of a vector in $\mathrm{AGL}_1(p)$ is isomorphic to $\mathbb{Z}_{p-1}$. If a subgroup does not contain the Sylow p-subgroup, then it is contained in a Hall p'-subgroup and hence stabilises one element. □

For convenience, now we denote $H_i = \langle h_i \rangle$ the stabiliser of $i \in \{1, \ldots, p\}$.

Corollary 2.2. *If $g \in G$ is such that $H \cap H^g \neq 1$, then either $g \in H$ or $H \cap H^g = \langle h_i \rangle \cap \langle h_j^g \rangle \leqslant H_i$ for unique $i, j \in \{1, \ldots, p\}$.*

Proof. Note that $H \cong \mathrm{AGL}_1(p)$ is a maximal subgroup of S_p, the normaliser of its Sylow p-subgroup in S_p is H itself. Hence, $H \cap H^g$ contains the Sylow p-subgroup of H if and only if $g \in H$. By Lemma 2.1, $H \cap H^g \leqslant H$ for $g \notin H$ is a subgroup of a stabiliser H_i. Therefore, $H \cap H^g = \langle h_i \rangle \cap \langle h_j^g \rangle$ for some $i, j \in \{1, \ldots, p\}$. This (i, j) is unique, as stabilisers of two different elements intersect trivially since $\mathrm{AGL}_1(p)$ acts sharply 2-transitively on $\mathbb{F}_p$. □

To calculate the valency of $G = S_p$ with stabiliser $H = \mathrm{AGL}_1(p)$, we only need to count the number of $g \in G$ such that $H \cap H^g \neq 1$. Corollary 2.2 gives that it suffices to count the number of $g \in G \backslash H$ such that $\langle h_i \rangle \cap \langle h_j^g \rangle \neq 1$ for fixed $i, j \in \{1, \ldots, p\}$.

Lemma 2.3. *Let σ be an n-cycle in S_n. Then the number of n-cycle $\tau \in S_n$ such that $\langle \sigma \rangle \cap \langle \tau \rangle \neq 1$ is*

$$m := (n-1)! - \sum_{D \subseteq P} (-1)^{|D|} \left(\frac{n}{\pi_D} - 1 \right)! \cdot \pi_D^{\frac{n}{\pi_D} - 1} \prod_{q \in D} (q-1), \tag{1}$$

where P is the set of prime numbers that divides n, and $\pi_D = \prod_{q \in D} q$ is the product of elements in D.

Proof. Firstly if $\langle \sigma \rangle \cap \langle \tau \rangle \neq 1$ then $\sigma^{\frac{n}{d}} = \tau^{\frac{n}{d}}$ for some $1 \neq d \mid n$. $\sigma^{\frac{n}{d}}$ is a product of $\frac{n}{d}$ d-cycles. To find τ, we may divide the n-cycle into d parts and the adjacent numbers in $\tau^{\frac{n}{d}}$ should be placed in τ with $\frac{n}{d}$ apart. This gives

$$\frac{d^{\frac{n}{d}}(\frac{n}{d})!}{n} = d^{\frac{n}{d}-1}\left(\frac{n}{d}-1\right)!$$

such τ's with a fixed d.

Note that if $\gcd(d,k) = 1$ then $\tau^{\frac{n}{d}} \in \langle\sigma\rangle$ if and only if $\tau^{k\frac{n}{d}} \in \langle\sigma\rangle$. This gives $\phi(d)$ such number of τ's in the above equation.

We can therefore use the principle of inclusion-exclusion to calculate. Define

$$E_d = \{\tau : \sigma^{\frac{n}{d}} = \tau^{k\frac{n}{d}} \text{ for some } \gcd(d,k) = 1\}.$$

Then an easy observation gives that $E_{d_1} \cap E_{d_2} = E_{\mathrm{lcm}(d_1,d_2)}$ and so

$$|\{\tau : \langle\sigma\rangle \cap \langle\tau\rangle \neq 1\}| = \left|\bigcup_{d|n} E_d\right| = \left|\bigcup_{q\in P} E_q\right|,$$

where P is the set of prime divisors of n. This yields the number of τ's such that $\langle\sigma\rangle \cap \langle\tau\rangle = 1$ being

$$\sum_{d|n} \mu(d)d^{\frac{n}{d}-1}\left(\frac{n}{d}-1\right)!\phi(d) = \sum_{D\subseteq P}(-1)^{|D|}\left(\frac{n}{\pi_D}-1\right)!\cdot\pi_D^{\frac{n}{\pi_D}-1}\prod_{q\in D}(q-1),$$

where μ is the Möbius function, P is the set of primes that divide n and $\pi_D = \prod_{q\in D} q$. It follows the statement as there are $(n-1)!$ n-cycles in S_n. □

Proposition 2.4. *Let H be a subgroup of $G = S_p$ that is isomorphic to $\mathrm{AGL}_1(p)$. Then the valency of G with stabiliser H is*

$$(p-2)! - (m-1)p - 1,$$

where m is given in (1) with $n = p-1$.

Proof. For each $(i,j) \in \{1,\ldots,p\}^2$, the number of $g \in G$ such that $\langle h_i\rangle \cap \langle h_j^g\rangle \neq 1$ is $m|C_G(h_j)| = m(p-1)$. Some of these g's is contained in H, which forms a coset of a stabiliser and thus the number of which is $p-1$. Hence, the number of $g \in G\backslash H$ such that $\langle h_i\rangle \cap \langle h_j^g\rangle \neq 1$ is $m(p-1)-(p-1) = (m-1)(p-1)$. By Corollary 2.2, the total number of $g \in G\backslash H$ such that $H \cap H^g \neq 1$ is therefore $(m-1)(p-1)p^2$. It follows that there are

$$p! - (m-1)(p-1)p^2 - p(p-1)$$

$g \in G$ that $H \cap H^g = 1$. This gives the valency by dividing $p(p-1)$. □

2.1.2 $G = A_p$ and $H = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$

Now we consider the case when $G = A_p$ and $H = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$. H is indeed a subgroup of $\mathrm{AGL}_1(p)$ in S_p of index 2. This case is similar to the previous one: Corollary 2.2 also holds and the method to calculate the valency is very similar.

Lemma 2.5. *Let $\sigma \in A_n = A_{2k}$ be of cycle type $[k,k]$. Then the number of $\tau \in S_n$ with cycle type $[k,k]$ such that $\langle\sigma\rangle \cap \langle\tau\rangle \neq 1$ is*

$$m := \frac{2(n-1)!}{n} - \sum_{D \subseteq P} (-1)^{|D|} \cdot \frac{2\pi_D^{\frac{n}{\pi_D}-1}\left(\frac{n}{\pi_D}-1\right)!}{n} \cdot \prod_{q \in D}(q-1), \tag{2}$$

where P is the set of prime numbers that divides $k = \frac{n}{2}$ and $\pi_D = \prod_{q\in D} q$ is the product of elements in D.

Proof. This is similar to Lemma 2.3: the number of cycles with cycle type $[k,k]$ is $\frac{2(n-1)!}{n}$ and for a fixed $d \mid k$, the number of τ's such that $\langle\sigma\rangle \cap \langle\tau\rangle$ contains $\langle\sigma^{\frac{n}{d}}\rangle$ is

$$\binom{\frac{2k}{d}}{\frac{k}{d}} \cdot \frac{1}{2} \cdot \left(d^{\frac{k}{d}-1}\left(\frac{k}{d}-1\right)!\right)^2 = \frac{2d^{\frac{n}{d}-1}\left(\frac{n}{d}-1\right)!}{n}.$$

and so

$$|E_d| = \frac{2d^{\frac{n}{d}-1}\left(\frac{n}{d}-1\right)!}{n}\phi(d).$$

It follows the statement with the same method of inclusion-exclusion. □

Now the valency follows.

Proposition 2.6. *Let H be a maximal subgroup of $G = A_p$ that is isomorphic to $\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$. Then the valency of G with stabiliser H is*

$$(p-2)! - \left(\frac{(p-1)m}{2} - 1\right)p - 1,$$

where m is given in (2) with $n = p-1$.

Proof. The proof is very similar as the proof of Proposition 2.4: Corollary 2.2 also holds and this gives

$$\left(m|C_G(h_i)| - \frac{p-1}{2}\right)p^2 = \left(m(p-1)^2 - \frac{p-1}{2}\right)p^2$$

$g \in G\backslash H$ such that $H \cap H^g \neq 1$. The valency is hence

$$\frac{\frac{p!}{2} - \left(m(p-1)^2 - \frac{p-1}{2}\right)p^2 - \frac{p(p-1)}{2}}{\frac{p(p-1)}{2}} = (p-2)! - \left(\frac{(p-1)m}{2} - 1\right)p - 1$$

with m given in (2) for $n = p - 1$. □

With this in mind, we may go back to Theorem 1.16. We claim that $G = A_p$ and $H = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$ cannot happen in that case.

Theorem 2.7. *Let $G = A_p$ with stabiliser $H = \mathbb{Z}_p{:}\mathbb{Z}_{p-1}$ for $p \neq 7, 11, 17, 23$. Then* $\mathrm{val}(G, H)$ *is even.*

Proof. By Proposition 2.6, the valency is odd if and only if $\frac{(p-1)m}{2}$ is odd, if and only if both m and $\frac{p-1}{2}$ are odd. Note that in (2), each summand is even except when $D = \{2\}$. This gives $\frac{p-1}{2}$ even and so the valency is even. Therefore, this case in Theorem 1.16 cannot happen and so Theorem 1.17 holds. □

2.1.3 Conclusion

In conclusion, the valencies of the groups in Table 6 are all calculated.

Theorem 2.8. *Let G be an almost simple primitive group with socle A_n for $n \geqslant 5$ and soluble stabiliser H. Then $(G, H, \mathrm{val}(G))$ are listed in Table 7.*

Corollary 2.9. *If G is an almost simple primitive group with* $\mathrm{soc}(G) = A_n$, *then* $\mathrm{val}(G)$ *is even.*

Proof. All valencies in Table 7 are even, and all insoluble groups are of even orders. □

2.2 Prime-power Valencies

We will classify almost simple primitive groups G with $\mathrm{val}(G)$ being prime powers.

G	H	$\mathrm{val}(G,H)$
A_5	S_3, A_4	6, 0
S_5	D_{12}, S_4	0, 0
A_6	S_4, S_4, $3^2{:}4$	0, 0, 0
$A_6.2 \cong \mathrm{M}_{10}$	$\mathrm{AGL}_1(5)$, $8{:}2$, $\mathrm{PSU}_3(2)$	20, 32, 0
$A_6.2 \cong \mathrm{PGL}_2(9)$	D_{20}, D_{16}, $\mathrm{AGL}_1(9)$	0, 16, 0
S_6	$S_4 \times S_2$, $S_4 \times S_2$, $S_3 \wr S_2$	0, 0, 0
A_7	$3{:}S_4$	0
S_7	$S_3 \times S_4$	0
A_8	$A_4^2.2^2$	0
S_8	$(2 \wr S_4).2$, $A_4^2.D_8$	0, 0
A_9	$\mathrm{ASL}_2(3)$, $3^3{:}S_4$	432, 0
S_9	$\mathrm{AGL}_2(3)$, $3^3{:}2^2.D_{12}$	0, 0
A_{12}	$3^4{:}2^3{:}S_4$, $2^6{:}3^3{:}S_4$	0, 0
S_{12}	$3^4.2 \wr A_4.2$, $2^6.3^3.A_4.2^2$	0, 0
A_{16}	$2^8.3^4.2^3.S_4$	0
S_{16}	$2^8.3^4.2 \wr A_4.2$	0
A_p	$\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$, $p \geqslant 5$ is a prime, $p \neq 7, 11, 17, 23$	Proposition 2.6
S_p	$\mathrm{AGL}_1(p)$, $p \geqslant 5$ is a prime	Proposition 2.4

Table 7: Valencies of almost simple primitive group G with $\mathrm{soc}(G) = A_n$ for $n \geqslant 5$ and soluble stabiliser H up to conjugacy

2.2.1 Stabilisers of 2-power Orders

First, we consider the case when the valency is a power of 2. In this case, the stabiliser is a 2-group, and in particular, soluble. A quick check of the classification of almost simple primitive groups with soluble stabilisers in [11] gives the possible cases in Table 8.

G_0	H_0	Conditions and descriptions
$\mathrm{PSL}_2(q)$	$D_{2(q-1)/(2,q-1)}$	$q \neq 5, 7, 9, 11$
	$D_{2(q+1)/(2,q-1)}$	$q \neq 7, 9$
$\mathrm{PGL}_2(7)$	D_{16}	
$\mathrm{PGL}_2(9)$	D_{16}	
$\mathrm{PSL}_2(9).2 \cong \mathrm{M}_{10}$	8:2	
$\mathrm{PSL}_3(2).\langle\tau\rangle$	D_{16}	τ is the transpose-inverse action

Table 8: Possible cases of almost simple primitive group G with stabiliser H a 2-group given in [11], where $G_0 \lhd G$ is minimal such that $H_0 := H \cap G_0$ is maximal in G_0 and $H = H_0.(G/G_0)$

Consider the case when $G_0 = \mathrm{PSL}_2(q)$ and $H_0 = D_{2(q\pm1)/(2,q-1)}$. If we want $|H_0|$ be a 2-power, then q must be odd. Hence, $H_0 = D_{2(q\pm1)}$. Now we need $q \pm 1$ to be a 2-power and hence $q = 2^f \pm 1$, which is also a prime power. Theorem 1.18 gives that a prime power of the form $q = 2^f \pm 1$ is indeed a prime unless $q = 9$. Note that the outer automorphism group of $\mathrm{PSL}_2(p)$ is of order 2, which gives the full automorphism group $\mathrm{PGL}_2(p)$. We have a complete classification of such groups:

Lemma 2.10. *Let G be an almost simple primitive group such that the stabiliser H is a 2-group. Then (G, H) are listed in Table 9.*

We now check the cases listed in Table 9 one by one.

2.2.2 $\mathscr{C}_2$ Subgroups

Proposition 2.11. *Let $G = \mathrm{PSL}_2(q)$ with q odd and $q \neq 5, 7, 9, 11$, and $H \cong D_{q-1}$ a maximal subgroup of $\mathscr{C}_2$ type. Then the Saxl graph of G with stabiliser H is of valency $\frac{q^2+6q-7}{4}$. In particular, when $q = 2^f + 1$ ($q \neq 5$) is a Fermat prime, the valency is $2^f(2^{f-2} - 2)$.*

Proof. Consider the action of $\mathrm{SL}_2(q)$ on $Q_{2(q-1)}$, which is equivalent to the action of G on $[G : H]$ and the action of $\mathrm{SL}_2(q)$ on the set of direct sum decompositions of $\mathbb{F}_q^2$ into two 1-dimensional subspaces. Let $\langle v_1\rangle \oplus \langle v_2\rangle$ and $\langle w_1\rangle \oplus \langle w_2\rangle$ be two distinct such

G	H	Conditions and descriptions
$\mathrm{PSL}_2(p)$	D_{p-1}	$p \neq 5$ is a Fermat prime, subgroup of class $\mathscr{C}_2$
	D_{p+1}	$p \neq 7$ is a Mersenne prime, subgroup of class $\mathscr{C}_3$
$\mathrm{PGL}_2(p)$	$D_{2(p-1)}$	$p \neq 5$ is a Fermat prime, subgroup of class $\mathscr{C}_2$
	$D_{2(p+1)}$	$p \neq 7$ is a Mersenne prime, subgroup of class $\mathscr{C}_3$
$\mathrm{PGL}_2(7)$	D_{16}	
$\mathrm{PGL}_2(9)$	D_{16}	
$\mathrm{PSL}_2(9).2 \cong \mathrm{M}_{10}$	8:2	
$\mathrm{PSL}_3(2).\langle\tau\rangle$	D_{16}	τ is the transpose-inverse action

Table 9: Almost simple primitive group G with stabiliser H a 2-group

decompositions and $w_1 = a_1v_1 + a_2v_2$ and $w_2 = b_1v_1 + b_2v_2$. If $h \in \mathrm{SL}_2(q)$ stabilises both of two decompositions, then there are four cases.

Case 1: $v_1^h = \lambda_1 v_1$, $v_2^h = \lambda_2 v_2$, $w_1^h = \lambda w_1$ and $w_2^h = \mu w_2$. In this case we have

$$\begin{cases} a_1\lambda v_1 + a_2\lambda v_2 = \lambda w_1 = w_1^h = a_1v_1^h + a_2v_2^h = a_1\lambda_1 v_1 + a_2\lambda_2 v_2 \\ b_1\mu v_1 + b_2\mu v_2 = \mu w_2 = w_2^h = b_1v_1^h + b_2v_2^h = b_1\lambda_1 v_1 + b_2\lambda_2 v_2 \end{cases}$$

and thus

$$\begin{cases} a_1\lambda = a_1\lambda_1 \\ a_2\lambda = a_2\lambda_2 \end{cases} \quad \text{and} \quad \begin{cases} b_1\mu = b_1\lambda_1 \\ b_2\mu = b_2\lambda_2. \end{cases}$$

If $a_1 = 0$ then $a_2 \neq 0$, as h is non-degenerate, and so $\lambda_2 = \lambda$. Also $b_2 \neq 0$, otherwise the two decompositions are the same, which implies that $\lambda = \lambda_2 = \mu$. Thus, $h = \lambda I$ and so $h = \pm I$, which is in the kernel of this action.

Case 2: $v_1^h = \lambda_1 v_1$, $v_2^h = \lambda_2 v_2$, $w_1^h = \lambda w_2$ and $w_2^h = \mu w_1$. In this case we have

$$\begin{cases} b_1\lambda v_1 + b_2\lambda v_2 = \lambda w_2 = w_1^h = a_1v_1^h + a_2v_2^h = a_1\lambda_1 v_1 + a_2\lambda_2 v_2 \\ a_1\mu v_1 + a_2\mu v_2 = \mu w_1 = w_2^h = b_1v_1^h + b_2v_2^h = b_1\lambda_1 v_1 + b_2\lambda_2 v_2 \end{cases}$$

and thus

$$\begin{bmatrix} a_1 & & -b_1 & \\ & a_2 & -b_2 & \\ b_1 & & & -a_1 \\ & b_2 & & -a_2 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda \\ \mu \end{bmatrix} = 0. \tag{3}$$

If such h exists, then $(\lambda_1, \lambda_2, \lambda, \mu)$ has a non-zero solution. Thus, we may consider the case when

$$\begin{vmatrix} a_1 & & -b_1 & \\ & a_2 & -b_2 & \\ b_1 & & & -a_1 \\ & b_2 & & -a_2 \end{vmatrix} = (a_1b_2 - b_1a_2)(a_1b_2 + b_1a_2) = 0.$$

Note that w_1, w_2 is linearly independent, which gives $a_1b_2 - b_1a_2 \neq 0$. It suffices to consider the case when $a_1b_2 + b_1a_2 = 0$. If $a_1 = 0$ then either $b_1 = 0$ or $a_2 = 0$. In either case w_1, w_2 is not linearly independent. Thus, a_1, a_2, b_1, b_2 are all non-zero. Without loss of generality, we may assume $a_1 = b_1 = 1$ because a non-zero scalar product does not change the subspace. Then (3) becomes

$$\begin{bmatrix} 1 & & -1 & \\ & a_2 & -b_2 & \\ 1 & & & -1 \\ & b_2 & & -a_2 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda \\ \mu \end{bmatrix} = 0$$

and so $(\lambda_1, \lambda_2, \lambda, \mu) = (\mu, -\mu, \mu, \mu)$. Computing the determinant, we have $\lambda_1\lambda_2 = \lambda\mu = -\det h$ and thus $-\mu^2 = \mu^2 = -1$. Since q is odd, this is impossible. Therefore, there is no such h in this case.

Case 3: $v_1^h = \lambda_1 v_2$, $v_2^h = \lambda_2 v_1$, $w_1^h = \lambda w_1$ and $w_2^h = \mu w_2$. This is the same as Case 2.

Case 4: $v_1^h = \lambda_1 v_2$, $v_2^h = \lambda_2 v_1$, $w_1^h = \lambda w_2$ and $w_2^h = \mu w_1$. In this case we have

$$\begin{bmatrix} a_1 & & -b_2 & \\ & a_2 & -b_1 & \\ b_1 & & & -a_2 \\ & b_2 & & -a_1 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda \\ \mu \end{bmatrix} = 0. \tag{4}$$

Note that if $a_1 = 0$ then $\lambda = 0$, a contradiction to $h \in \mathrm{SL}_2(q)$. Thus, all of a_1, a_2, b_1

and b_2 are non-zero. Again, without loss of generality, we may assume $a_1 = b_1 = 1$ and then (4) becomes

$$\begin{bmatrix} 1 & & -b_2 & \\ & a_2 & -1 & \\ 1 & & & -a_2 \\ & b_2 & & -1 \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \lambda \\ \mu \end{bmatrix} = 0.$$

Solve the above system of linear equations we have $(\lambda_1, \lambda_2, \lambda, \mu) = (a_2\mu, b_2^{-1}\mu, a_2 b_2^{-1}\mu, \mu)$. Hence, (4) has a non-zero solution if and only if there exists μ such that $a_2 b_2^{-1}\mu^2 = -1$. The number of different choices of (a_2, b_2) so that (4) has a non-zero solution is therefore $\frac{(q-1)(q-3)}{2}$, which gives $\frac{(q-1)(q-3)}{4}$ decompositions $\langle w_1 \rangle \oplus \langle w_2 \rangle$. These decompositions, together with $\langle v_1 \rangle \oplus \langle v_2 \rangle$, have a non-trivial stabiliser given above.
Note that there are $\frac{q(q+1)}{2}$ decompositions in total, we have, therefore,

$$\frac{q(q+1)}{2} - \frac{(q-1)(q-3)}{4} - 1 = \frac{q^2 + 6q - 7}{4}$$

such $\langle w_1 \rangle \oplus \langle w_2 \rangle$ that its stabiliser intersects trivially (in $\mathrm{PSL}_2(q)$) with the stabiliser of $\langle v_1 \rangle \oplus \langle v_2 \rangle$. Therefore, the valency of the Saxl graph of G with stabiliser H is $\frac{q^2+6q-7}{4}$. □

However, if we remove the restriction of determinant, we have

Proposition 2.12. *Let $G = \mathrm{PGL}_2(q)$ with q odd and $q \neq 5, 7, 9, 11$, and $H \cong D_{2(q-1)}$ a maximal subgroup of $\mathscr{C}_2$ type. Then the Saxl graph of G with stabiliser H is of valency $2(q-1)$. In particular, when $q = 2^f + 1$ ($q \neq 5$) is a Fermat prime, the valency is 2^{f+1}.*

The proof is similar: the number of decompositions in Case 4 is $\frac{(q-1)^2}{4} + \frac{(q-1)(q-3)}{4}$ by discussing the parity of the determinant of h. Indeed, the Saxl graph is the Johnson graph $J(q+1, 2)$: two unordered pairs of 1-dimensional subspaces form a base if and only if they have exactly one 1-subspace in common, and the total number of decompositions is $q + 1$. Therefore, the $\mathscr{C}_2$ cases in Table 9 has been done.

2.2.3 $\mathscr{C}_3$ Subgroups

Now we consider the $\mathscr{C}_3$ cases in Table 9.

Proposition 2.13. *Let $G = \mathrm{PSL}_2(q)$ with $q \equiv 3 \pmod 4$ and $q \neq 7$, and $H \cong D_{q+1}$ a maximal subgroup of $\mathscr{C}_3$ type. Then the Saxl graph of G with stabiliser H is of valency $\frac{q^2-2q-3}{4}$. In particular, when $q = 2^f - 1$ ($q \neq 7$) is a Mersenne prime, the valency is $2^{2f-2} - 2^f$.*

Proof. Let $D = \{H^g \mid g \in G\}$ be the conjugacy class of H in G. We have

$$|D| = \frac{|G|}{|N_G(H)|} = \frac{|G|}{|H|} = \frac{q(q-1)}{2}$$

and we need to count the number of those subgroups in D that intersects trivially with H. If there exists $H^g \in D$ such that there exists $h \in H^g \cap H$ with $|h| > 2$, then $H = N_G(\langle h \rangle) = H^g$. Thus, $H \cap H^g \cong 1$, $\mathbb{Z}_2$ or $\mathbb{Z}_2^2$ if $H \neq H^g$.

There are $\frac{q+3}{2}$ involutions in H, each of which can be in another $H^g \in D$. Let Γ_1, Γ_2 be subsets of D consisting subgroups such that their intersection with H are $\mathbb{Z}_2$ and $\mathbb{Z}_2^2$ respectively. Denote $Z(H) = \langle z_H \rangle \cong \mathbb{Z}_2$, then $C_G(z_H) = H$. If $z_H \in H \cap H^g$ then $z_{H^g} = z_H^g \in H \cap H^g$ and so $H \cap H^g = \langle z_H, z_{H^g} \rangle \cong \mathbb{Z}_2^2$.

It follows that $|\Gamma_2| = \frac{q+1}{2}$. Consider the incidence relation of the set of involutions in H and $\Gamma_1 \cup \Gamma_2$, we have

$$|\Gamma_1| + 3|\Gamma_2| = \frac{q+3}{2} \cdot \left(\frac{q+3}{2} - 1 \right)$$

and so $|\Gamma_1| = \frac{q^2-2q-3}{4}$. This gives $|\Gamma_1 \cup \Gamma_2| = \frac{q^2-1}{4}$ and thus the valency is

$$\frac{q(q-1)}{2} - \frac{q^2-1}{4} - 1 = \frac{q^2-2q-3}{4}.$$

This completes the proof. ☐

Proposition 2.14. *Let $G = \mathrm{PGL}_2(q)$ with $q \equiv 3 \pmod 4$ and $q \neq 7$, and $H \cong D_{2(q+1)}$ a maximal subgroup of $\mathscr{C}_3$ type. Then the Saxl graph of G with stabiliser H is empty.*

Proof. This is given by [12], which gives the subdegrees of $\mathrm{PGL}_2(q)$ with stabiliser $D_{2(q+1)}$ are 1, $(q+1)/2$ and $(q+1)^{(q-3)/2}$. Hence, there is no regular orbit of the stabiliser. ☐

2.2.4 Conclusion

Therefore, we have

Proposition 2.15. *Let G be an almost simple primitive permutation group with socle T stabiliser H such that* $\mathrm{val}(G,H)$ *is a 2-power. Then (G,H) is one of the following:*

1. $G = \mathrm{PSL}_2(9).2 \cong \mathrm{M}_{10}$, $H \cong 8{:}2$ *with* $\mathrm{val}(G,H) = 32$.

2. $G = \mathrm{PGL}_2(q)$, $H \cong D_{2(q-1)}$ *is a maximal subgroup of G of class $\mathscr{C}_2$, where $q \geqslant 17$ is a Fermat prime or $q = 9$, with* $\mathrm{val}(G,H) = 2(q-1)$. *The Saxl graph is isomorphic to the Johnson graph $J(q+1,2)$.*

Now we focus on odd prime powers. In Theorem 1.16, a quick check follows that only the third case is possible. In this case, we need $\frac{q^n \pm 1}{q \pm 1} = n^k$ for some integer k, where $n \geqslant 3$ is a prime and q is a prime power. However, Corollary 1.20 and Corollary 1.22 implies that neither case is possible.

Therefore, we have the main theorem:

Theorem 2.16. *Let G be an almost simple primitive permutation group with stabiliser H such that* $\mathrm{val}(G)$ *is a prime power. Then (G,H) is one of the following:*

1. $G = \mathrm{PSL}_2(9).2 \cong \mathrm{M}_{10}$, $H \cong 8{:}2$ *with* $\mathrm{val}(G,H) = 32$.

2. $G = \mathrm{PGL}_2(q)$, $H \cong D_{2(q-1)}$ *is a maximal subgroup of G of class $\mathscr{C}_2$, where $q \geqslant 17$ is a Fermat prime or $q = 9$, with* $\mathrm{val}(G,H) = 2(q-1)$. *The Saxl graph is isomorphic to the Johnson graph $J(q+1,2)$.*

3 Problems

3.1 Odd Valencies and Normalisers of Field Automorphisms

Theorem 1.17 gives only two possible cases of an almost simple group which has odd valency. For the second case of linear groups, if $q = p$ is a prime then $G = \mathrm{PGL}_n(p)$ with $H = \mathbb{Z}_a{:}\mathbb{Z}_n$, where $a = \frac{p^n-1}{p-1}$. Use the same method as in the calculation of $\mathrm{val}(S_p, \mathrm{AGL}_1(p))$ we have

Proposition 3.1. *Suppose $G = \mathrm{PGL}_n(p)$ with both p and n primes ($n \geqslant 3$). Let $H = \mathbb{Z}_a{:}\mathbb{Z}_n = \langle x\rangle{:}\langle y\rangle$ a maximal subgroup of G of type $\mathscr{C}_3$ with $a = \frac{p^n-1}{p-1}$. Then*

$$\mathrm{val}(G,H) = \frac{|G| - (|N_G(\langle y\rangle)| - n)\, a^2 - an}{an} = \frac{|G|}{|H|} - \left(\frac{|N_G(\langle y\rangle)|}{n} - 1\right) a - 1.$$

Note that in this case $\mathrm{val}(G,H)$ is odd if and only if $|N_G(\langle y\rangle)|$ is odd. We shall show that the order of this normaliser must be even.

Proposition 3.2. *Let* $H = \Gamma\mathrm{L}_m(p^f) = \mathrm{GL}_m(p^f).\langle\sigma\rangle$ *be a* $\mathscr{C}_3$ *subgroup of* $G = \mathrm{GL}_{fm}(p)$, *where* σ *is a field automorphism of* $\mathrm{GL}_m(p^f)$, p *is a prime and* $fm > 2$, $f > 1$. *Then the image of* $N_G(\langle\sigma\rangle)$ *in* $\mathrm{PGL}_{fm}(p)$ *is of even order.*

Proof. Note that $N_H(\langle\sigma\rangle) \cong \mathrm{GL}_m(p).\langle\sigma\rangle$. If $m > 1$ then the image of $N_H(\langle\sigma\rangle)$ in $\mathrm{PGL}_{fm}(p)$ is clearly of even order. Therefore, it suffices to consider the case when $m = 1$ and $f > 2$ is odd. In this case a matrix of σ is the permutation matrix of an f-cycle. (In general, a matrix of σ can be written as a m-copies of block diagonal matrix with each block an f-cycle.) Now f is odd, and we have $(1,2,\ldots,f)^{(2,f)(3,f-1)\cdots([f/2]+1,[f/2]+2)} = (1,2,\ldots,f)^{-1}$. This gives an involution in $N_G(\langle\sigma\rangle)$, which is not in the centre. □

Corollary 3.3. *The valency given in Proposition 3.1 must be even.*

The full automorphism group of $\mathrm{PSL}_n(q)$ for $n > 2$ is $\mathrm{P\Gamma L}_n(q).2 = \mathrm{PGL}_n(q).(\mathbb{Z}_f \times \mathbb{Z}_2)$, which is much larger than $\mathrm{PGL}_n(q)$. This leads a further analysis on valencies of such groups.

Problem 1. *Completely classify almost simple primitive groups of odd valencies.*

Conjecture 2. *The only almost simple primitive group of odd valency is* M_{23} *with stabiliser* 23:11.

3.2 $p_1^a p_2^b$ Valencies

Let p_1, p_2 be distinct prime numbers. The aim is to extend the result of prime-power valencies to $p_1^a p_2^b$ valencies. Note that we have already classified those groups of prime-power valencies, we may only consider the case when $a, b > 0$.

We have already calculated valencies of almost simple primitive groups G with $\mathrm{soc}(G) = A_n$ and with soluble stabilisers. We first consider this case.

Let $G = S_p$ and H the subgroup of G that is isomorphic to $\mathrm{AGL}_1(p)$. Then if we need the valency of G with stabiliser H to be $p_1^a p_2^b$, then p must be a Fermat prime. Proposition 2.4 implies

Corollary 3.4. *Let $G = S_p$ and H a subgroup of G that is isomorphic to* $\mathrm{AGL}_1(p)$*, where $p = 2^f + 1$ is a Fermat prime. Then*

$$\mathrm{val}(G, H) = (2^f - 1)! - (2^{2^{f-1}-1}(2^{f-1} - 1)! - 1)(2^f + 1) - 1. \tag{5}$$

Proof. In this case, (1) gives

$$m = (n - 1)! - \left(\frac{n}{2} - 1\right)! \cdot 2^{\frac{n}{2}-1}$$

with $n = p - 1 = 2^f$, and the valency follows by Proposition 2.4. □

Similarly, if we need the valency of $G = A_p$ with stabiliser $H = \mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$ a prime power, then $p = 2r^f + 1$ for some prime r. Now Proposition 2.6 gives

Corollary 3.5. *Let $G = A_p$ and H a maximal subgroup of G that is isomorphic to $\mathbb{Z}_p{:}\mathbb{Z}_{(p-1)/2}$, where $p = 2^f + 1$ is a Fermat prime. Then*

$$\mathrm{val}(G, H) = \left(2^f - 1\right)! - \left(2^{2^{f-1}-1}\left(2^{f-1} - 1\right)! - 1\right)\left(2^f + 1\right) - 1. \tag{6}$$

Proof. In this case

$$m = 2^{2^{f-1}-f}(2^{f-1} - 1)!$$

in (2) with $n = p - 1 = 2^f$, and the valency follows by Proposition 2.6. □

For (5) and (6), by now we have no method to determine whether they can be $p_1^a p_2^b$ or not. At least we know that the valencies are all even by Theorem 2.7 and this implies p is a Fermat prime. However, by checking all known existing Fermat primes, we find no such p that makes the valency $p_1^a p_2^b$. This leads

Conjecture 3. *(5) and (6) cannot equal to $p_1^a p_2^b$ for any primes p_1, p_2.*

Conjecture 4. *Let G be an almost simple primitive group with* $\mathrm{soc}(G) = A_n$ *and stabiliser H. If* $\mathrm{val}(G, H)$ *equals $p_1^a p_2^b$ for some distinct primes p_1, p_2 and $a, b \geqslant 1$, then exactly one of the following holds:*

1. *$G = A_5$, $H = S_3$ and* $\mathrm{val}(G, H) = 6$.
2. *$G = \mathrm{M}_{10}$, $H = \mathrm{AGL}_1(5)$ and* $\mathrm{val}(G, H) = 20$.
3. *$G = A_9$, $H = \mathrm{ASL}_2(3)$ and* $\mathrm{val}(G, H) = 432$.

For general almost simple primitive groups, thing are far more complicated: a large fraction of those with soluble stabilisers are $\{p_1, p_2\}$-groups.

Problem 2. *Classify almost simple primitve groups with valency* $p_1^a p_2^b$ *(or first study the case when* $\{p_1, p_2\} \neq \{2, 3\}$*).*

3.3 Generalisation

In [11], the classification of almost simple primitive groups with soluble stabilisers has been done. We have already calculated the valencies of a small fraction of those with some restrictions.

Problem 3. *Determine the valencies of all almost simple (quasi-)primitive groups with soluble stabilisers.*

In all the above cases, the stabiliser is soluble. If we remove the restriction of almost simple primitive groups and consider the general primitive groups, then an easy application of O'Nan-Scott Theorem gives that the group must be one of types HA, AS or PA.

Problem 4. *Generalise all the above results to the general primitive groups (or in particular, of PA type).*

Acknowledgements

The author thanks Cai Heng Li and Timothy C. Burness for their fantastic results in references and wonderful guidance. The author also thanks Qing Xiang, Jiyong Chen, Huye Chen and Binzhou Xia for their detailed comments. The author especially thanks Cai Heng Li for all of his patient supervision during the author's undergraduate years.

References

[1] Bertram Huppert. Zweifach transitive, auflösbare Permutationsgruppen[J]. Mathematische Zeitschrift. 1957, **68**(1):126–150.

[2] Christoph Hering. Transitive linear groups and linear groups which contain irreducible subgroups of prime order, II[J]. Journal of algebra. 1985, **93**(1):151–164.

[3] Peter J. Cameron, et al. Permutation groups[M], vol. 45. Cambridge University Press, 1999.

[4] Timothy C. Burness, Michael Giudici. On the Saxl graph of a permutation group[C]. Mathematical Proceedings of the Cambridge Philosophical Society. Cambridge University Press, 2020, vol. 168, 219–248.

[5] Martin W. Liebeck, Cheryl E. Praeger, Jan Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups[J]. Journal of the Australian Mathematical Society. 1988, **44**(3):389–396.

[6] Cheryl E. Praeger. An O'Nan-Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs[J]. Journal of the London Mathematical Society. 1993, **2**(2):227–239.

[7] Michael Aschbacher. On the maximal subgroups of the finite classical groups[J]. Inventiones mathematicae. 1984, **76**(3):469–514.

[8] Martin W. Liebeck, Jan Saxl. On point stabilizers in primitive permutation groups[J]. Communications in Algebra. 1991, **19**(10):2777–2786.

[9] Preda Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture[J]. Journal Für Die Reine Und Angewandte Mathematik. 2004, **572**:167–195.

[10] Karl Zsigmondy. Zur theorie der potenzreste[J]. Monatshefte für Mathematik und Physik. 1892, **3**(1):265–284.

[11] C. H. Li, H. Zhang. The finite primitive groups with soluble stabilizers, and the edge-primitive s-arc transitive graphs[J]. Proceedings of the London Mathematical Society. 2011, **103**(3):441–472.

[12] FL. Tchuda. Combinatorial geometric characterizations of some primitive representations of the groups $\mathrm{PSL}(n, q)$ for $n = 2, 3$[J]. Ph D Thesis. 1986.

[13] William Burnside. On groups of order $p^\alpha q^\beta$[J]. Proceedings of the London Mathematical Society. 1904, **2**(1):388–392.

[14] Walter Feit, John G. Thompson. Solvability of groups of odd order[M]. Pacific Journal of Mathematics, 1963.

[15] Philip Hall. A note on soluble groups[J]. Journal of the London Mathematical Society. 1928, **1**(2):98–105.

[16] Chris Godsil, Gordon F. Royle. Algebraic graph theory[M], vol. 207. Springer Science & Business Media, 2013.

[17] John D. Dixon, Brian Mortimer. Permutation groups[M], vol. 163. Springer Science & Business Media, 1996.

[18] Michael Giudici. Maximal subgroups of almost simple groups with socle $\mathrm{PSL}(2,q)$[J]. arXiv preprint math/0703685. 2007.

[19] Timothy C. Burness, Michael Giudici. Classical groups, derangements and primes[M], vol. 25. Cambridge University Press, 2016.

[20] John N. Bray, Derek F. Holt, Colva M. Roney-Dougal. The maximal subgroups of the low-dimensional finite classical groups[M], vol. 407. Cambridge University Press, 2013.

[21] Peter B. Kleidman, Martin W. Liebeck, et al. The subgroup structure of the finite classical groups[M], vol. 129. Cambridge University Press, 1990.

[22] Robert Wilson. The finite simple groups[M], vol. 251. Springer Science & Business Media, 2009.

[23] Roger W. Carter. Simple groups of Lie type[M], vol. 22. John Wiley & Sons, 1989.

[24] Robert A. Wilson. Maximal subgroups of sporadic groups[J]. Finite Simple Groups: Thirty Years of the Atlas and Beyond, Contemp Math. 2017, **694**:57–72.

[25] John Horton Conway. Atlas of finite groups: maximal subgroups and ordinary characters for simple groups[M]. Oxford University Press, 1985.

[26] Moshe Roitman. On Zgismondy Primes[J]. Proceedings of the American Mathematical Society. 1997:1913–1919.