UNIVERSITÀ
DI PAVIA

CONSTRAINTS ON VERTEX-TRANSITIVE GROUPS OF AUTOMORPHISMS OF CONNECTED GRAPHS

Marco Barbieri

Supervised by Pablo Spiga

Joint PhD Program in Mathematics
Milano-Bicocca – Pavia – INdAM

December 2024

Contents

Introduction

Luego estos viajes
y el mío mar de nuevo:

– *Finale*, Pablo Neruda (1923)

THE PLAYERS. The driving motivation of all the work contained in this thesis is the following question.

Question A · *Let G be a group, and let Γ be a d-valent connected graph. What constraints must G obey to be a vertex-transitive group of automorphisms of Γ?*

Before discussing the philosophy behind Question A, let us recall what a vertex-transitive group of automorphisms is.

A *graph* Γ is a pair $(V\Gamma, E\Gamma)$ where $E\Gamma$ is an asymmetric binary relation on $V\Gamma$. (The set $V\Gamma$ is assumed to be finite throughout this thesis, unless explicitly stated otherwise.) A graph is *d-valent* if the neighbourhood of every vertex contains d elements, while a graph is *connected* if, for every pair of vertices, there exists a path joining them. An *automorphism of the graph* Γ is a permutation of the vertex-set $V\Gamma$ that preserves the relation $E\Gamma$. As usual, the composition of two automorphisms is an automorphism, and the inverse of an automorphism is an automorphism. Hence, the set of all automorphisms with the operation of composition forms a group, which we denote by $\mathrm{Aut}(\Gamma)$, and we call the *automorphism group of* Γ. A *group of automorphisms of* Γ is any subgroup of $\mathrm{Aut}(\Gamma)$. Our focus is on those groups of automorphisms whose action on $V\Gamma$ is transitive, and we call them *vertex-transitive*. Similarly, we define *edge-transitive* and *vertex-primitive*.

The way we defined our players suggests that our focus is studying the symmetries of a given discrete geometry, but that is not the case. The flavour of Question A is closer to that of questions in Geometric Group Theory: a geometry is associated to a group so that the geometric and combinatorial properties of the former shed light on the algebraic aspects of the latter. Indeed, we can also think of the opposite approach when introducing our d-valent connected graphs. Let G be a transitive group on a permutation domain Ω. We define an *orbital graph for G* as the graph whose vertex-set is Ω and whose edge-set is the G-orbit of an arbitrary 2-subset $\{\alpha,\beta\} \in \Omega^{\{2\}}$. If G is primitive, the graph described is connected, and its valency d is the length of some suborbit of G, that is,

$$d = |\beta^{G_\alpha}|.$$

In general, a connected graph with a transitive group of automorphisms G is obtained by taking appropriate unions of different orbital graphs for G. Therefore,

d gives a measure of how long the subdegrees of G are. Hence, Question A can be interpreted as asking *what do the subdegrees tell us about a transitive permutation group G?*

To make Question A more concrete, we can answer it in the 2-valent case. Every 2-valent connected graph is precisely a cycle of length r. Hence, G is a transitive subgroup of the dihedral group of order $2r$. In particular, G is solvable, and the order of G is at most $2r$. We point out that such a satisfactory answer becomes impossible as soon as the valency exceeds 3.

Number of automorphisms. The most interesting piece of information of the solution to Question A for valency 2 is that the order of G is linear in the number of vertices of Γ. A similar behaviour is described by the celebrated *Tutte's Theorem*: if G is an arc-transitive group of automorphisms of a connected 3-valent graph Γ, then the order of G divides $48|V\Gamma|$ (see Theorem 1.24). Here, *arc-transitive* means that the action of G on the ordered pairs of adjacent vertices is transitive.

This result does not generalise if we remove the hypothesis of arc-transitivity or if we increase the valency to 4. The counterexamples are the ubiquitous Praeger–Xu graphs for valency 4 and their split 3-valent counterpart for groups which are not transitive on the arcs. Indeed, these graphs have exponentially large groups of automorphisms with respect to the number of vertices, and this fact causes various complications with regard to many natural questions. They are the object of study in Sections 2.A to 2.D. For lack of a better place in this introduction, we give here some novel result on this family of graphs and the operations linking them.

Theorem C · *For any positive integer $r \geq 3$ and for any positive integer $s \leq r-1$, the Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph if, and only if, the polynomial t^r+1 has a divisor of degree $r-s$ in $\mathbb{Z}_2[t]$.*

Corollary D · *Let a be a non-negative integer, let b be an odd positive integer such that $r = 2^a b$, with $r \geq 3$, and let s be a positive integer with $s \leq r-1$. The Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph if, and only if, s can be written as*

$$s = \sum_{d|b} \alpha_d \omega(d), \quad \textit{for some integers} \quad \alpha_d \quad \textit{with} \quad 0 \leq \alpha_d \leq \frac{2^a \varphi(d)}{\omega(d)}.$$

The operations linking Praeger–Xu graphs and their splits are called *merging* and *splitting*, and they can be used more generally to translate problems about 4-valent arc-transitive (but not 2-arc-transitive) graphs in analogue problems about 3-valent vertex-transitive (but not arc-transitive) graphs, and vice versa. By [115, Theorem 12], outside of some known degenerate scenarios, the merging operator is the right-inverse of the splitting one. The following result shows that the merging operation is also its left-inverse.

Theorem E · *Let Δ be a 4-valent graph, let $\mathcal{C}$ be a partition of $E\Delta$ into cycles, and let G be an arc-transitive group of automorphisms of Δ such that $\mathcal{C}$ is G-invariant. Then the merging operation can be applied to the pair $(\mathrm{s}(\Delta,\mathcal{C}),G)$ and it gives as a result $(\Delta,\mathcal{C})$.*

On the other hand, it has been conjecture that Tutte's Theorem can be generalised under some mild local hypothesis. Let G be a vertex-transitive group of automorphisms of Γ, and let α be an arbitrary vertex. The *local group of the pair* (Γ, G) is the permutation group that the vertex-stabilzer G_α induces on the neighbourhood of α, that is,

$$G_\alpha^{\Gamma(\alpha)} \cong G_\alpha / G_\alpha^{[1]}.$$

The *Weiss Conjecture* states that there is a constant C_d such that, if the local group of G is primitive and the valency of the graph Γ is d, then $|G| \leq C_d |V\Gamma|$. We give a survey of this conjecture and the subsequent generalisations in Section 1.K.

The feasibility of many algorithmic routines is based on finding a function of the number of vertices of Γ which gives an upper bound on the order of G. In Chapter 1, we explore how this kind of considerations affects the Graph Isomorphism Problem and the compilation of censuses of vertex-transitive graphs of small valency.

Fixed point ratio. The *Graph Isomorphism Problem* asks what is the complexity of the algorithmic problem of establishes whether two graphs are isomorphic or not. Through the *Group Theory Method* (see Section 1.C), this problem has been reduced to the case in which the automorphism group of the graph analysed is vertex-primitive. In turn, nothing better that bounding the order of a primitive permutation group with a function of its degree is known to complete the algorithm. In Section 1.E, we focus on the solution that L. Babai has given to this problem for the class of strongly regular graphs using the notion of fixed point ratio (see [5, 6]). The *fixed point ratio* of a permutation group G of degree n is defined by

$$\mathrm{fpr}(G) = \max_{g \in G - \{1\}} \left(1 - \frac{|\mathrm{supp}(g)|}{n} \right),$$

that is, the maximum proportion of points that a nonindentity permutation fixes. L. Babai develops a general machinery that shows that, if the fixed point ratio of an infinite family of primitive groups is bounded away from 1, then the order of the group is a bounded by a quasipolynomial function of its degree. For his application, he proves that every connected strongly regular graph either is isomorphic to a Hamming graph or Johnson graph, or its fixed point ratio is at most 7/8, thus obtaining a quasipolynomail bound on the number of automorphisms.

Relying on a recent classification of T. Burness and R. M. Guralnick contained in [27], we extend this result by giving a classification of vertex-primitive graphs with fixed point ratio exceeding 1/3. Theorem K relies on a quite involved construction, which is explained in details in Section 3.C. Just to give a glimpse of the underlying idea, a *merged product action graph* is the equivalent for product action of what a wreath graph is for a wreath product in imprimitive action. The proof of this theorem spans Sections 3.D to 3.F.

Theorem K · *Let Γ be a finite vertex-primitive graph with at least one arc. Then*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma)) > \frac{1}{3}$$

if and only if one of the following occurs:

(i) Γ *is a generalised Hamming graph* $\mathbf{H}(r,m,\mathcal{J})$, *with* $m \geq 4$, *and, if* m *is optimal in the sense of Definition 3.20, then*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma)) = 1 - \frac{2}{m};$$

(ii) Γ *is a merged product action graph* $\mathcal{P}(r,\mathcal{G},\mathcal{J})$, *where* $r \geq 1$, *where* $\mathcal{J}$ *is a non-Hamming subset of* X^r *with* $X = \{0,1,\dots,|\mathcal{G}|-1\}$, *and where* $\mathcal{G}$ *is as in one of the following:*

(a) $\mathcal{G} = \{\mathbf{J}(m,k,i) \mid i \in \{0,1,\dots,k\}\}$ *is the family of distance-i Johnson graphs, where* k,m *are fixed integers such that* $k \geq 2$ *and* $m \geq 2k+2$ *(see Section 3.E.2 for details), and*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma)) = 1 - \frac{2k(m-k)}{m(m-1)};$$

(b) $\mathcal{G} = \{\mathbf{QJ}(2m,m,i) \mid i \in \{0,1,\dots,\lfloor m/2 \rfloor\}\}$ *is the family of squashed distance-i Johnson graphs, where* m *is a fixed integer with* $m \geq 4$ *(see Section 3.E.3 for details), and*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma)) = \frac{1}{2}\left(1 - \frac{1}{2m-1}\right);$$

(c) $\mathcal{G} = \{\mathbf{L}_m, \Gamma_1, \Gamma_2\}$, *where* Γ_1 *is a strongly regular graph listed in Section 3.E.4,* Γ_2 *is its complement, and*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma)) = \mathrm{fpr}(\mathrm{Aut}(\Gamma_1))$$

(the fixed point ratios are collected in Table 3.3).

We can attempt a more general attack based on fixed point ratios, although, with our current knowledge, they are not enough to bound the size of a group of automorphisms. The main idea is that having high fixed point ratio forces the group to grow bigger (see Section 1.D). Therefore, we aim to show that, aside of some well-understood exceptions, the fixed point ratio is arbitrarily close to zero.

This approach has been used, for instance, by F. Lehner, P. Potočnik and P. Spiga in [85]. Let d be a positive integer, and let ϵ and C be two positive constants. We can consider the family $\mathcal{F}$ of pairs pairs (Γ, G) where

(a) Γ is a connected d-valent graph,

(b) the local group of the pair (Γ, G) is quasiprimitive,

(c) $\mathrm{fpr}(G) \geq \epsilon$ and $|G_\alpha| \leq C$.

Then, [85, Theorem 3.1] states that $\mathcal{F}$ is finite, and its cardinality only depends on the parameters d, ϵ, C. We refer to Section 3.A for details.

Using the positive solution to the Sims Conjecture (see Section 1.J), we can change the local hypothesis for a global one.

Theorem I · *Let* ϵ *and* C *be two positive constants, and let* $\mathcal{F}$ *be a family of quasiprimitive permutation groups* G *on* Ω *satisfying* (*a*) $\mathrm{fpr}(G) \leq \epsilon$,

(*b*) $|G_\omega| \leq C$ *for every* $\omega \in \Omega$.

Then $\mathcal{F}$ *is a finite family.*

Corollary J · *Let* ϵ *be a positive constant, and let* d *be a positive integer. There are only finitely many vertex-primitive digraphs of valency at most* d *and fixed point ratio exceeding* ϵ.

Moreover, as a high fixed point ratio separate Hamming and Johnson graphs from the other connected strongly regular graphs, fixed point ratios can also be used to separate Praeger–Xu graphs and their splitting from other connected graphs of the same valency. To be precise, in [112], P. Potočnik and P. Spiga have proved that, apart from fourteen small exceptions, if the fixed point ratio of a 3-valent vertex-transitive or 4-valent vertex- and edge-transitive connected graph exceeds 1/3, then it is a split Praeger–Xu graph or a Praeger–Xu graph (depending on the valency). Their proof is explained in Section 2.E. If we shift our attention to the action on the edge, we can get rid of almost all exceptions – unfortunately the complete graph on 5 vertices survives. The proof of the following results is contained in Sections 2.F to 2.H.

Theorem F · *Let* Γ *be a finite connected* 4*-valent vertex- and edge-transitive graph admitting a nontrivial automorphism fixing more than* 1/3 *of the edges. Then one of the following holds:*

(*a*) Γ *is isomorphic to* $\mathbf{K}_5$, *the complete graph on* 5 *vertices;*

(*b*) Γ *is isomorphic to a Praeger–Xu graph* $\mathrm{C}(r,s)$, *for some* r *and* s *with* $3s < 2r-3$.

Theorem G · *Let* Γ *be a finite connected* 3*-valent vertex-transitive graph admitting a nontrivial automorphism fixing more than* 1/3 *of the edges. Then* Γ *is isomorphic to a split Praeger–Xu graph* $\mathrm{sC}(r,s)$, *for some* r *and* s *with* $3s < 2r-3$.

Derangements and semiregular elements. Until now, we have focused on permutations with fixed points, but these kind of elements are surprisingly rare. A *derangement* is a permutation whose support coincides with the domain. The *proportion of derangements* of a permutation group G is defined as the ratio

$$\delta(G) = \frac{\#\{g \in G \mid g \text{ is a derangement}\}}{|G|}.$$

To exemplify their abundance, we recall the well-known *Cameron–Cohen Bound* (see [32]). Let G be a transitive permutation group of degree n and permutation rank r (which coincides with the number of distinct suborbits of G). Then

$$\delta(G) \geq \frac{r-1}{n}.$$

In Section 3.I, by pushing their proof in a different direction, we obtain the following result.

Theorem P · *Let G be a finite transitive permutation group whose minimal nontrivial subdegree is d. Then*

$$\delta(G) \geq \frac{1}{2d} + \frac{n-2}{2|G|}.$$

Equality is attained if and only if G is a Frobenius group.

As an immediate consequence, every vertex-transitive group of automorphisms has its proportion of derangements bounded away from zero by a function of the valency alone.

Corollary Q · *Let Γ be a finite digraph, and let G be a group of automorphisms of Γ. If G is transitive, and Γ has valency d, then*

$$\delta(G) \geq \frac{1}{2d}.$$

A *semiregular element* is a derangement such that all its nontrivial powers are also derangements. For instance, every derangement of prime order is semiregular. A classical result of Jordan states that every transitive permutation group contains a derangement, while something more is believed to be true for automorphism groups of graphs. The *Polycirculant Conjecture* claims that any automorphism group of a graph contain a semiregular element. We focus on the 3-valent case. The conjecture is settled in this case, but what can we say about the semiregular element? In [35], it has been mistakenly conjectured that, as the number of vertices goes to infinity, the order of a semiregular element grows to infinity. This has been disproved in [144], by exhibiting an infinite family of 3-valent graphs such that all the semiregular elements of their automorphism groups have orders that does not exceed 6. In Sections 2.I and 2.J, we show that 6 is optimal in the following sense.

Theorem H · *We have that*

$$\liminf_{\substack{|V\Gamma|\to\infty \\ \Gamma \text{ 3-valent vertex-transitive}}} \max\{\mathbf{o}(g) \mid g \in \mathrm{Aut}(\Gamma),\, g \text{ semiregular}\} = 6.$$

Amalgams. We now switch to the second algorithmic problem explored in Chapter 1: *Can we list all the pairs (Γ, G), where Γ is a connected 3-valent graph with $|V\Gamma| \leq n$, and G is an arc-transitive group of automorphisms of Γ?* Amalgams are the main ingredient used in compiling censuses of arc-transitive.

An *amalgam* is a triplet of groups (L, B, R) such that B is subgroup of L and R. We say that (L, B, R) is *of index* $(d, 2)$ if $|L : B| = d$ and $|R : B| = 2$, that it is *faithful* if B is core-free in $\langle L, R\rangle$, and that it is *finite* if L and R are both finite. For every arc-transitive graph (Γ, G), there is a universal cover of the form $(\mathcal{T}_d, G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}})$, where α and β are two adjacent vertices of Γ, and $\mathcal{T}_d$ is the infinite d-valent tree. The triplet $(G_\alpha, G_{\alpha\beta}, G_{\{\alpha,\beta\}})$ can be isomorphic to any finite faithful amalgam of index $(d, 2)$. We explain this theory in Section 1.H.

As a consequence, to list all the 3-valent arc-transitive graphs up to n vertices, it is enough to classify all the finite faithful amalgam of index $(3, 2)$ and to take all the finite quotients of the universal cover, with the quotient graphs having at most n vertices. The first step has been performed by D. Ž. Djokovic and

G. L. Miller in [47], while the second one has been implemented by M. D. E. Conder and P. Dobcsányi in [39].

As soon as we increase the valency, it is not clear if the classification of the amalgams is a reasonable problem to tackle. For instance, rather than seven as in the 3-valent case, the number of finite faithful amalgam of index $(4,2)$ is infinite. On the other hand, all the known finite faithful amalgams of index $(d,2)$ have some desirable properties. Indeed, the minimal *number of generators* of the amalgamated product is seemingly bounded by a constant C_d, depending on the valency, and the same is true for the *exponent* of each one of the three groups composing the amalgam.

In Section 3.H, we prove that the first property does not hold in general. We denote by $\mathbf{d}(G)$ the minimal number of generators of the group G.

Theorem N · *There exists no function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ such that, for every pair (Γ, G), where Γ is a connected d-valent graph, and G is an arc-transitive group of automorphisms of Γ,*

$$\mathbf{d}(G) \leq \mathbf{f}(d).$$

To prove the previous result, we exhibit an infinite family of d-valent arc-transitive graphs such that $\mathbf{d}(G)$ is a linear function of the exponent of the group. This suggests that the exponent of G could be a relevant parameter to consider. Indeed, we note that the number of vertices of every vertex-transitive graph can be bounded by a function of both the valency and the exponent.

Theorem O · *There exists a function $\mathbf{B} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for every vertex-transitive graph (Γ, G) where the valency of Γ is d, and that the exponent of G is e,*

$$|V\Gamma| \leq \mathbf{B}(d,e) \quad \textit{and} \quad |G| \leq \mathbf{B}(d,e)!\,.$$

A similar investigation for the exponent of a vertex-stabilizer has not produced many fruits yet. In Section 3.G, we are able to prove that the exponent of a vertex-stabilizer is bounded under the assumption that the local group is *weakly p-subregular* (see Definition 3.27).

Theorem M · *Let p be a prime, and let L be a weakly p-subregular permutation group. Then, for every pair (Γ, G) where Γ is a connected graph, G is a vertex-transitive group of automorphisms, and the local group of (Γ, G) is isomorphic to L, and for every vertex $\alpha \in V\Gamma$,*

$$\exp(G_\alpha) \leq p^3 \exp(L).$$

Although this result is not trivial, these local groups are known to behave surprisingly well regardless of the fact that the order of a vertex-stabilizer is unbounded (see [157]). As a corollary, we obtain that the exponent of a vertex-stabilizer is bounded by $16d$ for the pairs (Γ, G), where Γ is connected d-valent, and the local group is dihedral.

Structure of the thesis. This thesis consists of three chapters.

Chapter 1 collects most of the tools and ideas we use in this work. The proofs contained in it are selected either for clarity of exposition or to make them more accessible. We also point out that, in contrast with the other results of Chapter 1, Theorem B is original. We state it here.

Theorem B · *Let G be a finite group, and let H and K be two maximal subgroups whose intersection is core-free in G. Suppose that*

$$h = |H : H \cap K| \quad \textit{and} \quad k = |K : H \cap K|.$$

Then, if we denote by $\mathbf{f}$ *the function that solves the Sims Conjecture,*

$$|H \cap K| \leq \mathbf{f}(hk)^2 .$$

Chapter 2's aim is to prove Theorems F to H. What sets these results apart is that they pertain to graphs of small valency. All faithful amalgams of index $(d, 2)$ have been classified for $d \leq 4$, hence we can extract precise information on their local group from there. Moreover, Chapter 2 massively uses the *normal quotient method*, which seems to stop being a useful tool for studying Question A as the valency of the graph grows.

Finally, Chapter 3 deals with results where the valency of the graph can be arbitrarily large. Most of the results presented there provide a bound on some group-theoretical parameter that depends on the valency of the underlying graph alone, in line with the philosophy of Question A. The techniques used throughout Chapter 3 are considerably more varied that those of Chapter 2, thus we cannot give a brief account of them here.

1 Number of automorphisms

Time for you and time for me,
And time yet for a hundred indecisions,
And for a hundred visions and revisions,
Before the taking of a toast and tea.

– *The Love Song of J. Alfred Prufrock*,
Thomas S. Eliot (1915)

In this chapter, we present the main ingredients of this work. To make this chapter more engaging, we are at the same time introducing two core problems in which the tool we develop can find an application: the *Graph Isomorphism Problem* and the compilation of *censuses of symmetric graphs*. Moreover, these topics can also be regarded as the leading motivations for the remaining chapters.

1.A Graph Isomorphism Problem

A *digraph* is a pair

$$\Gamma = (V\Gamma, A\Gamma)$$

where $A\Gamma$ is a binary relation on $V\Gamma$. The elements of $V\Gamma$ are called *vertices*, while the elements of $A\Gamma$ are called *arcs*. We assume that $V\Gamma$ is finite unless explicitly stated.

Furthermore, suppose that $A\Gamma$ is a symmetric relation, that is, for every arc $(\alpha, \beta) \in A\Gamma$, the *opposite arc* (β, α) is also an element of $A\Gamma$. The pairs $\{(\alpha, \beta), (\beta, \alpha)\}$ partition $A\Gamma$, thus we can consider the quotient relation $E\Gamma$ where opposite arcs are identified. A *graph* is a pair

$$\Gamma = (V\Gamma, E\Gamma).$$

We can also see a graph as the most barren incidence structure: from this point of view, two vertices α and β are *adjacent* if $\{\alpha, \beta\}$ is an element of $E\Gamma$. The elements of $E\Gamma$ are called *edges*.

We can describe as example two surprisingly simple graphs which will remain relevant for most of the work. For a positive integer m, let $\mathbf{L}_m$ and $\mathbf{K}_m$ denote the *loop graph* and the *complete graph* on a vertex-set V of cardinality m and with arc-sets $\{(v, v) \mid v \in V\}$ and $\{(u, v) \mid u, v \in V, u \neq v\}$, respectively.

Let Γ be a graph, and let $\alpha \in V\Gamma$ be an arbitrary vertex of Γ. We denote the *neighbourhood of α* by $\Gamma(\alpha)$, and we define the *valency of α* as the number of neighbours of α, that is,

$$\mathrm{val}(\alpha) = |\Gamma(\alpha)|.$$

If the valency is shared by all vertices, we call this number *valency of* Γ, and we denote it by $\mathrm{val}(\Gamma)$.

Let Γ and Δ be two graphs. A *morphism of graphs* is a map

$$g : V\Gamma \to V\Delta$$

such that adjacent vertices are mapped to adjacent vertices, that is,

$$g(E\Gamma) \subseteq E\Delta.$$

Our main interest lies in *isomorphisms*, which are invertible morphisms of graphs. Moreover, an *automorphism* is an isomorphism from a graph to itself. The set of automorphisms of a graph is a group with respect to composition, and we denote this group by $\mathrm{Aut}(\Gamma)$. Lastly, we say that G is a *group of automorphisms* of Γ if G is a subgroup of $\mathrm{Aut}(\Gamma)$.

The *Graph Isomorphism Problem* consists in giving an algorithm that establishes, in the least possible time, whether or not two arbitrary graphs are isomorphic. The naive algorithm – compare the number of vertices, and, if they are equal, check for all the bijection of the vertex-set of the first into the vertex-set of the second – has an exponential run time. What is usually tackled is the polynomially equivalent problem of assigning a canonical labelling for the vertices of the graphs. (The expression *polynomially equivalent* means that there exists an algorithm that runs in polynomial time that takes as input the solution of one problem and produces as output the solution of the other problem.) In fact, if a canonical labelling can be found in an efficient way, the Graph Isomorphism Problem is solved by applying this efficient algorithm to both graphs and then comparing their labellings. For different algorithmic problems that are polynomially equivalent to the Graph Isomorphism Problem, we refer to [101].

The Graph Isomorphism Problem has been first tackled with combinatorial heuristics. The spotlight in this sense has been taken by the *Weisfeiler–Leman algorithm*, introduced in [158]. Let Γ be the graph for which we want to produce a canonical labelling. Suppose that $|V\Gamma| = n$, and consider the complete graph with loops $\mathbf{K}_n \cup \mathbf{L}_n$. (By $\mathbf{K}_n$ we denote the *complete graph* on n vertices, while by $\mathbf{L}_n$ we denote the *loop graph* on n vertices. Given two graphs Γ and Δ, their *union* is the graph $\Gamma \cup \Delta$ whose vertex-set is $\Gamma \cup \Delta$ and whose edge-set is $\Gamma \cup \Delta$.) We assign to the edges of $\mathbf{K}_n \cup \mathbf{L}_n$ a colouring $\mathbf{c}_0$ whose fibres are $\mathbf{L}_n$, Γ and $\mathbf{K}_n - \Gamma$ respectively. The algorithm refines the colouring to $\mathbf{c}_1$ so that two edges share the same colours if the number of triangles with a given colour assignment in $\mathbf{c}_0$ containing the edge are the same. This process can be iterated by obtaining finer and finer colourings. A special vertex $\alpha \in V\Gamma$ is chosen, and its loop is coloured with a special colour. Applying the Weisfeiler–Leman algorithm spreads this irregularity, giving a loose classification of the vertices and thereby reducing the isomorphism search space. In [10], it is shown that this approach solves the Graph Isomorphism Problem in linear time for almost all graphs. Clever choices of the special vertex α give efficient algorithm for specific classes of graphs: an example is the polynomial solution for the planar case by J. E. Hopcroft and R. E. Tarjan in [70].

However, this combinatorial method alone cannot solve the general problem in less than exponential time: in [30], J.-Y. Cai, M. Fürer and N. Immerman have built an infinite family of graphs for which the runtime of the described algorithm has an exponential lower bound (see also [106]). To break this wall, a massive use of group theory entered the picture in [3], where L. Babai has introduced a *Las Vegas* algorithm that solves the Graph Isomorphism Problem in polynomial time, outside of a small probability of failure. His algorithm is based on a *tower of groups* that reveals, step by step, the automorphism group of a coloured graph Γ. Each group of the tower, roughly speaking, extends the previous group by the automorphisms of the connection set of two colours. To guarantee an efficient generation of each extension, we take some uniformly distributed elements of the quotient. The probabilistic nature of this generation is the cause of the chance of failure of the Las Vegas algorithm. The idea of taking advantage of the symmetries of the graph – the so-called *Group Theory Method* – has been later implemented by E. M. Luks in [94] to find an algorithm that solves the Graph Isomorphism Problem in polynomial time for graphs of bounded valency, and then refined by both authors in [11]. The results produced with this approach have stayed unbeaten until, on these (and more) ideas, L. Babai built his solution of the Graph Isomorphism Problem in quasipolynomial time (see, for instance, [7, 8, 67]).

1.B Permutation groups

The Group Theory Method relies on some basic notions of permutation groups. In Section 1.B, we are developing the basics of this theory.

Any subgroup of the symmetric group $\mathrm{Sym}(\Omega)$ on the set Ω is a *permutation group*. More generally, let G be an abstract group, and let $\rho : G \to \mathrm{Sym}(\Omega)$ be a group homomorphism. The map ρ defines an *action of G on Ω*, that is, any element of g can be identified with the bijection g^ρ of Ω. We denote by

$$G^\Omega = G/\ker(\rho)$$

the image of the action ρ, which is a permutation group on Ω. If $\ker(\rho)$ is trivial, we say that the action if *faithful*, and G itself is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$.

The set Ω on which the group G is acting is called *permutation domain*, and the elements of Ω are called *points*. Furthermore, we write our actions with the exponential notation, that is, the image of $\alpha \in \Omega$ under the permutation $g \in G$ is denoted by α^g.

Let G be a permutation group on Ω, and let $\alpha \in \Omega$ be a point. The *G-orbit of α* is defined as

$$\alpha^G = \{\alpha^g \mid g \in G\}.$$

The group G is *transitive on* Ω if it defines a single G-orbit. Observe that the property *two points belong to the same G-orbit* defines an equivalence relation on Ω, thus the action of G on Ω partitions the set in G-orbits.

Let $\Delta \subseteq \Omega$ be a G-orbit. We call the permutation group G^Δ a *transitive constituent of* G. The group G is a *sub-Cartesian product* of its transitive constituents, that is, G is a subgroup of the direct product of its transitive constituents, and the projection of G on each Cartesian component is surjective. In particular, if we ignore the loss of information caused by the fact that we do not know how the transitive constituents interact, the study of an arbitrary permutation group reduces to that of its transitive constituents, that is, of transitive groups.

Let H be a subgroup of G. We can define a transitive action of G on the right coset space G/H by, for any $x, g \in G$,

$$(Hx)^g = Hxg.$$

This action is transitive by the definition of right coset space.

Let G be transitive on Ω. The *stabilizer of* α is defined by

$$G_\alpha = \{g \in G \mid \alpha^g = \alpha\}.$$

It is immediate to verify that G_α is a subgroup of G, and that the map

$$\varphi : \Omega \to G/G_\alpha, \quad \beta \mapsto G_\alpha g_\beta,$$

where $g_\beta \in G$ is a permutation such that $\alpha^{g_\beta} = \beta$, is a well-defined bijection. Therefore, the study of transitive groups is equivalent to that of actions by right multiplication on right coset spaces.

We recall a surprisingly useful observation, which is now usually referred to as *Frattini's Argument*.

Theorem 1.1 ([45] Exercise 1.4.1) · *For any point $\alpha \in \Omega$, and for any subgroup H of G, then*

$$G = G_\alpha H = H G_\alpha \quad \textit{if, and only if,} \quad H \textit{ is transitive.}$$

In particular, the only transitive subgroup of G containing G_α is G itself.

Let G be a transitive group on Ω. A subset Δ of Ω is a *block of imprimitivity for G* if, for any permutation $g \in G$,

$$\text{either } \Delta = \Delta^g, \quad \text{or } \Delta \cap \Delta^g = \emptyset.$$

For instance, singletons and Ω are blocks for every action. Because of this, they are called *trivial blocks*. A transitive permutation group G is *primitive* if the only blocks of imprimitivity for G are trivial blocks. It is *imprimitive* otherwise.

An easy computation shows that, for a fixed point $\alpha \in \Omega$, there is a one-to-one inclusion preserving correspondence between the blocks of imprimitivity containing α and the subgroups of G containing G_α as a subgroup (see [45, Theorem 1.5A]). It follows that a transitive group is primitive if, and only if, each point stabilizer is a maximal subgroup.

Observe that the G-orbit of a block Δ defines a partition of Ω into blocks of imprimitivity. Such a partition is called a *system of imprimitivity for G*. Note that any G-invariant partition of Ω defines a system of imprimitivity. Thus, a primitive group G is a primitive group such that Ω admits no nontrivial G-invariant partitions.

We can reduce imprimitive actions to primitive action, mimicking what we did to pass from intransitive to transitive permutation groups. Let G be an imprimitive permutation group, let Σ be a system of imprimitivity for G, and let

$\Delta \in \Sigma$ be a block. Although we lose some information hidden in the kernels, the comprehension of G relies on how well we can control the induced actions G^{Σ} and G_{Δ}^{Δ}.

Let N be a normal subgroup of G, then the partition of Ω in N-orbits is G-invariant. Hence, any nontrivial normal subgroup of a primitive group is transitive. This fact leads to a natural generalisation of the concept of primitivity: we say that a transitive permutation group G is *quasiprimitive* if, for any nontrivial normal subgroup N of G, N is transitive. For instance, every simple group in imprimitive action is quasiprimitive and not primitive.

A permutation group G is called *semiregular* if, for every $\alpha \in \Omega$, the stabilizer of α is trivial, that is, $G_\alpha = 1$. It is called *regular* if it is both transitive and semiregular. Observe that, for every regular group G, the map φ previously defined is now a bijection that identifies Ω with G. This defines an action of G on itself by right multiplication, which we call the *right regular representation of* G.

Lemma 1.2 ([164] Proposition 4.3, and Exercise 4.5) · *Let G be a permutation group on Ω, and let C be the centralizer of G in* $\mathrm{Sym}(\Omega)$. *If G is transitive, then C is semiregular. If G is semiregular, then C is transitive. In particular, G is regular if, and only if, C is regular.*

Proof. Suppose that G is a transitive permutation group, and choose a point $\alpha \in \Omega$. Aiming for a contradiction, let $c \in C$ be a nontrivial element of the centralizer such that $\alpha^c = \alpha$. As G is transitive, for every $\beta \in \Omega$, we can find a permutation $g \in G$ such that $\beta = \alpha^g$. We compute

$$\beta^c = \alpha^{gc} = \alpha^{cg} = \alpha^g = \beta\,.$$

We obtain that c is contained in the kernel of the action of C on Ω. As $C \leq \mathrm{Sym}(\Omega)$, the action of C is faithful, thus $c = 1$, a contradiction. This proves that C is semiregular.

Assume, now, that G is semiregular. Let $\{\Omega_i \mid i \in I\}$ be a system of orbits for G. By the Axiom of Choice, we can choose a section

$$i \in I \mapsto \omega_i \in \Omega\,.$$

For every $\sigma \in \mathrm{Sym}(I)$, and for every $\tau \in G$, we can consider the map

$$c(\sigma,\tau) : \omega_i^g \mapsto \omega_{i\sigma}^{\tau^{-1}g}$$

Since G is semiregular, there is a one-to-one correspondence between the elements of the group and the elements of each orbit Ω_i. Hence, each $c(\sigma,\tau)$ is a well-defined permutation. Observe that, for every $h \in G$, and for every $\omega_i^g \in \Omega$,

$$\left(\omega_i^g\right)^{[c(\sigma,\tau),h]} = \left(\omega_{i\sigma^{-1}}^{\tau g h^{-1}}\right)^{c(\sigma,\tau)h} = \omega_{i\sigma^{-1}\sigma}^{\tau^{-1}\tau g h^{-1}h} = \omega_i\,.$$

Therefore,

$$\langle c(\sigma,\tau) \mid \sigma \in \mathrm{Sym}(I), \tau \in G\rangle \leq C\,.$$

Since the set of all $c(\sigma,1)$ is transitive on $\{\Omega_i \mid i \in I\}$, while the set of all $c(1,\tau)$ is transitive on each orbit Ω_i, this is enough to conclude that C is transitive. ∎

Suppose that G contains a normal subgroup N whose action on Ω is regular. We may identify the permutation domain Ω with N. In particular, we can choose a point $\alpha \in \Omega$ which we identify with 1, thus every other $n \in N$ is identified with α^n. The action of G_α on Ω is thus isomorphic to the action of G on N by conjugation. (See [164, Theorem 11.2] for details.)

We briefly recall that the finite primitive groups can be divided into eight families – this result is now known as the *O'Nan–Scott Theorem*. The original result, proved independently by M. E. O'Nan and L. Scott, was a classification of the maximal subgroup of the symmetric group. Using the Classification of Finite Simple Groups, their ideas extend to a classification of all primitive groups: this observation can be found, for instance, in [31, Secton 4]. The first self-contained proof was written by M. W. Liebeck, C. E. Praeger and J. Saxl in [89]. We are not going to explain the nature of the eight families: we will introduce the key properties of some families as they will become relevant for our discussion. Just to give a glimpse into this subdivision, recall that the socle of a finite primitive groups is a direct product of pairwise isomorphic simple groups. Different families are distinguished by the nature of the socle (*Is it abelian or not? Is it a single direct factor or multiple? Is acting regularly or not?*) and how it is embedded in the group.

Theorem 1.3 · *The set of all finite primitive permutation groups can be partitioned in eight families as follows:*

- HA *holomorphs of an abelian group;*
- HS *holomorphs of a simple group;*
- HC *holomorphs of a compound group;*
- TW *twisted wreath products of two groups;*
- AS *almost simple groups;*
- SD *groups in simple diagonal action;*
- CD *wreath products of groups in compound diagonal action;*
- PA *wreath products of groups in product action.*

We remark that Theorem 1.3 extends to quasiprimitive group with some slight modification, as showed by C. E. Praeger in [124]. Indeed, types HA, HS and HC stay the same, while the other types need some tweaking. For instance, for types AS and CD, the socle does not need to be primitive, but it can just be transitive.

Observe that, for any positive integer k, the action of G on Ω can be naturally extended to Ω^k, by putting, for every $g \in G$,

$$(\alpha_1, \alpha_2, \dots, \alpha_k)^g = \left(\alpha_1^g, \alpha_2^g, \dots, \alpha_k^g\right).$$

We say that a permutation group G is k-transitive if $\Omega^k - \mathrm{diag}(\Omega^k)$ is an orbit of this action. For instance, the symmetric group of degree n, $\mathrm{Sym}(n)$, is n-transitive, while the alternating group of degree n, $\mathrm{Alt}(n)$, is $(n-2)$-transitive.

Observe that any 2-transitive group is primitive. Let k, h be two positive integers such that $k \leq h$. If a group is h-transitive, then it is also k-transitive. Hence, 2-transitive groups have been the main object of study for this property.

It turns out that the possibilities for 2-transitive groups are quite limited. A classical result of W. Burnside states that the socle of a 2-transitive group is either an elementary abelian group or a simple group (see [29, Theorem XIII]). Building on this, many later works, and using the Classification of Finite Simple Groups, P. J. Cameron has completed the classification of 2-transitive groups in [31, Section 5]. We refer to [45, Section 7.7] for a description of the finite 2-transitive permutation group, and to [45, Chapter 7] for a description of the richer situation if one allows the groups to be infinite.

1.C Group Theory Method

The Group Theory Method takes advantage of the natural refinement that can be used to study permutation groups. Thus, the method consists in processing an intransitive permutation group orbit by orbit, and a transitive but imprimitive permutation group by the blocks of an invariant equivalence relation. The Weisfeiler–Leman algorithm produces colourings that witness these refinements in polynomial time. Further refinements in the hierarchy of permutation groups are possible, but, to this day, no efficient algorithms to move down this hierarchy are known. Hence, we run out of our *divide et impera* options when a primitive group is encountered: before L. Babai's breakthrough, nothing much better than complete enumeration of those primitive groups had been used in this case. Bounds on the order of a primitive permutation group, in turn, depend on the thickness of the group, which was introduced by L. Babai, P. J. Cameron and P. P. Pálfy in [9] for this precise purpose. The *thickness* of a finite group G is the maximum integer θ such that $\mathrm{Alt}(\theta)$ appears as a section of G. (The next result is not stated in its original form: the fact that the exponent can be chosen to be a linear function in θ can be easily obtained from [100, Corollary 1.4], and there are examples meeting this bound.)

Theorem 1.4 ([9] Theorem 1.1) · *Let G be a primitive permutation group of degree n and thickness θ. Then*

$$|G| \leq n^{O(\theta)}.$$

We can reconstruct E. M. Luks's bound in [94]. Let Γ be a k-valent graph, and let α be a vertex. By our previous discussion, we can suppose that $\mathrm{Aut}(\Gamma)$ is primitive. Let us denote by G the permutation group that $\mathrm{Aut}(\Gamma)_\alpha$ induces on the neighbourhood of α. We want to apply [45, Theorem 3.2C] to $\mathrm{Aut}(\Gamma)$ (see also Lemma 1.33). In our setting, this result states that all the simple sections of $\mathrm{Aut}(\Gamma)_\alpha$ appear as sections of G. Since the latter permutation group has degree k by assumption, its thickness is at most k. As a consequence, the thickness of $\mathrm{Aut}(\Gamma)_\alpha$ cannot exceed k. Therefore, by Theorem 1.4,

$$|\mathrm{Aut}(\Gamma)| = n|\mathrm{Aut}(\Gamma)_\alpha| \leq n^{O(k)}.$$

In particular, we can produce a canonical labelling of the graph in polynomial time, and this solves the Graph Isomorphism Problem for bounded valency.

On the other hand, without extra hypothesis, the thickness can be arbitrarily close to n, thus needing to consider all the primitive groups up to $n!$ elements. This step is computationally unfeasible, and thus it is the bottleneck of the approach.

A primitive permutation group G is a *Cameron group* if

$$\mathrm{Alt}(m)^r \le G \le \mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r),$$

where the direct factors of the base group are endowed with the action on the k-subsets of $\{1,2,\dots,m\}$, $\mathrm{Sym}(r)$ is endowed with the natural action on r points, and the wreath product is endowed with the product action. In [31], P. J. Cameron has pointed out that, among primitive groups of degree n, the order of Cameron groups is significantly larger than any other group. Qualitatively, A. Maróti has proved the following result.

Theorem 1.5 ([100] Corollary 1.2) · *Let G be a primitive permutation group of degree $n \ge 25$. Then either G is a Cameron group, or*

$$|G| < 2^n.$$

L. Babai has worked around this dichotomy with his theory of *local certificates* in [7]. An efficient test (that runs in polynomial time) can establish whether the (primitive) automorphism group is a Cameron group or not. In the former case, an *ad hoc* polynomial algorithm solves the Graph Isomorphism Problem. If the automorphism group is not a Cameron group, we can dive into an exhaustive search and Theorem 1.5 guarantees that the algorithm comes to completion in polylogarithmic time.

Fixed point ratios have been applied to the automorphism group of graphs as a rudimental approach before the theory of local certificates was developed. Section 1.D explores the permutation group theoretic concept in general, and Section 1.E dives into how this parameter has been applied to the Graph Isomorphism Problem.

1.D Fixed point ratios

To overcome the bottleneck for strongly regular graphs, in [5, 6], L. Babai has used the notion of fixed point ratio to bound the order of the automorphism group of some graphs. In Section 1.D, we explore the concept of fixed point ratio in the general context of permutation groups.

Let G be a permutation group of domain Ω, and let $g \in G - \{1\}$ be a nontrivial permutation. We define the *fixed point ratio of g* by

$$\mathrm{fpr}(g,\Omega) = 1 - \frac{|\mathrm{supp}(g)|}{n}.$$

Moreover, the *fixed point ratio of G* is the maximum among the fixed point ratios of the elements of G, that is,

$$\mathrm{fpr}(G,\Omega) = \max\{\mathrm{fpr}(g,\Omega) \mid g \in G - \{1\}\}.$$

If the permutation domain Ω is understood, we drop it from the notation.

A naive reader might believe that having a large fixed point ratio is correlated with having large stabilizers. And this is not far from the truth. The first evidence is given by this result.

Lemma 1.6 ([12] Lemma 3) · *Let $g \in \mathrm{Sym}(\Omega)$ be a permutation, and let $\epsilon > 0$ be a positive number such that $\mathbf{o}(g) = |\Omega|^{\epsilon}$. Then, there is a positive integer k such that*

$$1 - \frac{1}{\epsilon} \le \mathrm{fpr}\left(g^k, \Omega\right) < 1\,.$$

Proof. Let $|\Omega| = n$ be the degree of $\mathrm{Sym}(\Omega)$. We can write the order of g as

$$\mathbf{o}(g) = n^{\epsilon} = \prod_{i=1}^{r} q_i\,,$$

where $q_i = p_i^{\beta_i}$ are powers of distinct primes p_i. For each $\alpha \in \Omega$, let $P(\alpha)$ be the set of indices i for which q_i divides the length of the cycle of g through α.

Observe that, for each $\alpha \in \Omega$, as the longest cycle in $\mathrm{Sym}(\Omega)$ has length n,

$$\prod_{i \in P(\alpha)} q_i \le n\,.$$

Let $n(i)$ be the number of points $\omega \in \Omega$ such that $i \in P(\omega)$. We can bound the minimum of $n(i)$ with the following weighted sum

$$\min_i n(i) \le \frac{\sum_{i=1}^{r} n(i) \log q_i}{\sum_{i=1}^{r} \log q_i} = \sum_{i=1}^{r} \frac{n(i) \log q_i}{\epsilon \log n}\,.$$

Indeed, the minimum $n(i)$ is the term appearing with the lowest coefficient.

Moreover, we can split the last term using the definition of $n(i)$

$$\min_i n(i) \le \sum_{\omega \in \Omega} \sum_{i \in P(\omega)} \frac{\log q_i}{\epsilon \log n} \le \frac{n \log n}{\epsilon \log n} = \frac{n}{\epsilon}\,.$$

It follows that, for some $j \in \{1, 2, \dots, r\}$, $n(j) \le n/\epsilon$. Upon choosing $k = n^{\epsilon}/p_j$, we obtain that g^k is not the identity and it fixes all but $n(j)$ points. ∎

Lemma 1.6 shows that the assumption that a permutation has exponential order with respect to the degree implies that the fixed point ratio of the cyclic group it generates is close to 1. On the other hand, we can prove that if a permutation fixed multiple points, then the groups that contain it must have large stabilizers, which, in turn, forces the permutation group to be big.

We recall that a *base* for a permutation group G on the domain Ω is a subset of Ω whose pointwise stabilizer is trivial. For instance, the basis of a vector space coincides with a base for the action of the general linear group on it. We denote by $\mathbf{b}(G)$ the minimal size of a base for G. This quantity also arises in combinatorial settings: for any graph Γ, $\mathbf{b}(\mathrm{Aut}(\Gamma))$ is the *fixing number of* Γ (also known as the *determining number of* Γ, or as the *rigidity index of* Γ).

Lemma 1.7 ([45] Exercise 3.3.7) **·** *Let G be a permutation group. Then*

$$1 \le (1-\mathrm{fpr}(G))\mathbf{b}(G).$$

Proof. Let Σ be a basis for G, let $x \in G$ such that $\mathrm{fpr}(x) = \mathrm{fpr}(G)$, and let Δ be the support of x. The proof consists of a double counting technique on the set

$$X = \{(\alpha, g) \in \Delta \times G \mid \alpha^g \in \Sigma\}.$$

On one hand, by the Orbit Stabilizer Lemma,

$$|X| = \sum_{\alpha\in\Omega} |\Sigma||G_\alpha| = \sum_{\alpha\in\Omega} \frac{|\Sigma||G|}{n} = \frac{|\Delta||\Sigma||G|}{n} = (1-\mathrm{fpr}(G))\mathbf{b}(G)|G|.$$

On the other hand, we have that, for every $g \in G$, $|\cap \Delta| \ge 1$. Indeed, Σ^g is a minimal basis, and the support of any element has nontrivial intersection with every given basis. Hence,

$$|X| = \sum_{g\in G} |\Sigma^g \cap \Delta| \ge |G|$$

Therefore, we conclude because

$$(1-\mathrm{fpr}(G))\mathbf{b}(G)|G| \ge |G|.$$

■

This can be translated to a fairly general result about the order of G.

Lemma 1.8 ([42] Theorem 3.1) **·** *Let G be a transitive nonregular permutation group on Ω. Then*

$$|G| \ge n \cdot 2^{2^{-1}(1-\mathrm{fpr}(G))^{-1}}.$$

Proof. Let

$$\Sigma = \left\{\omega_1, \omega_2, \ldots, \omega_{\mathbf{b}(G)}\right\}$$

be a minimal basis for G. Consider the chain of subgroups

$$G_{\omega_1} \ge G_{\omega_2} \ge \ldots \ge G_{\omega_{\mathbf{b}(G)}} = 1.$$

Each index $|G_{\omega_i} : G_{\omega_{i+1}}|$ is at least 2. Hence, we find that

$$|G_{\omega_1}| \ge 2^{\mathbf{b}(G)-1},$$

and, by the Orbit Stabilizer Lemma,

$$|G| \ge n \cdot 2^{\mathbf{b}(G)-1}.$$

Finally, by using Lemma 1.7, we obtain the desired inequality. ■

We observe that equality in Lemma 1.8 is rarely satisfied, as a necessary condition is for the stabilizer to be a 2-group.

The success of the approaches using fixed point ratios is caused by their key role in the probabilistic approaches to permutation group theory. In particular, once a problem is reduced to the primitive action of almost simple groups, a thorough understanding of this parameter can help extract the desired solution. The best asymptotic bound for this application is the following.

Lemma 1.9 ([90] Theorem 1) · *Let G be a transitive almost simple group of Lie type over $\mathbb{F}_q$. Either $|G| \leq 51\,840$, or the socle of G is $\mathrm{PSL}_2(q)$, or*

$$\mathrm{fpr}(G) \leq \frac{4}{3q}.$$

Observe that the action of $\mathrm{PGL}_d(q)$ on 1-subspaces, $d \geq 3$, has fixed point ratio that is roughly $1/q$. Moreover, the groups with $\mathrm{fpr}(G) \geq 4/3q$ have been classified in [90]. Further results of this kind will be discussed in Section 3.B.

Lemma 1.9 is the main ingredient, together with Aschbacher's classification of maximal subgroups of linear groups, to prove the following fascinating probabilistic result.

Theorem 1.10 ([65] Theorem 1) · *Let G_n be a finite simple group of order n, let $x, y \in G_n$ be two elements chosen uniformly at random. Then*

$$\lim_n \mathbb{P}\left(G_n = \langle x, x^y \rangle\right) = 1.$$

In the following years, Lemma 1.9 has been refined for specific actions. It has been extensively used to bound the size of minimal bases of primitive permutation group. The following result is an example of these applications.

Theorem 1.11 ([91] Theorem 1.4) · *There is a linear function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ such that, if G is a primitive group of thickness θ, then*

$$\mathbf{b}(G) \leq \mathbf{f}(\theta).$$

These tools are still relevant today: for instance, we can cite the following result. We recall that a group G is $3/2$-*generated* if every nontrivial element belongs to a generating pair.

Theorem 1.12 ([28] Theorem 1) · *A finite group is $3/2$-generated if, and only if, all its proper quotients are cyclic.*

1.E Strongly regular graphs

In Section 1.E, we follow [5] to prove that the graph isomorphism problem can be solved in quasipolynomial time for strongly regular graphs.

A general bound on the thickness of the automorphism group of a regular graph can be computed. The proof is based on Lemma 1.6 and the celebrated *Expander Mixing Lemma*, first proved by N. Alon and F. R. K. Chung as [1, Lemma 2.3]. We recall that, for any digraph Γ, the *eigenvalues* of Γ are the complex eigenvalues of the adjacency matrix of Γ. We recall that, if Γ is a graph, then the adjacency matrix is symmetric, thus all its eigenvalues are real. Moreover, if Γ is k-valent, then k is the maximum eigenvalue of Γ, and its multiplicity counts the number of connected components of Γ.

Lemma 1.13 ([5] Theorem 4) · *Let Γ be a connected k-valent graph with n vertices, and let*

$$\xi = \max\{|\zeta| \mid \zeta \text{ is an eigenvalue of } \Gamma \text{ distinct from } k\}.$$

Suppose that every pair of distinct vertices has at most q common neighbours, and that $q+\xi \leq k$. Then,

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), V\Gamma) \leq \frac{q+\xi}{k}.$$

In particular, the thickness θ of $\mathrm{Aut}(\Gamma)$ can be bounded as

$$\theta \leq \frac{(\log n)^2}{2\log(\log n)} \cdot \left(1 - \frac{q+\xi}{k}\right)^2 \cdot (1+o(1)).$$

Proof. Let $g \in \mathrm{Aut}(\Gamma) - \{1\}$ be a nontrivial automorphism. For every vertex $\alpha \in V\Gamma$, we denote by $\Gamma[g](\alpha)$ the neighbours of α that are fixed by g. Suppose that g does not fix all vertices, and, without loss of generality, suppose that α^g is distinct from α. We have that

$$\Gamma[g](\alpha) = \Gamma[g](\alpha^g),$$

thus, by assumption on the number of shared neighbours,

$$|\Gamma[g](\alpha)| \leq q. \tag{1.1}$$

We claim that

$$|\Gamma[g](\alpha)| \geq k\left(1 - \frac{|\mathrm{supp}(g)|}{n}\right) - \xi. \tag{1.2}$$

Let us denote by $\mathbf{J}$ the all one matrix and by $\mathbf{A}$ the adjacency matrix of Γ. Further, we write S for $\mathrm{supp}(g)$, which we identify with the induced subgraph of Γ, and we write $\chi_S \in \mathbb{R}^n$ for the characteristic vector of S. We compute

$$|AS| = \chi_S^t \mathbf{A} \chi_S \quad \text{and} \quad |S|^2 = \chi_S^t \mathbf{J} \chi_S.$$

Hence, we get

$$\left| |AS| - \frac{k}{n}|S|^2 \right| = \left| \chi_S^t \left(\mathbf{A} - \frac{k}{n}\mathbf{J}\right) \chi_S \right|.$$

Observe that, if the eigenvalues of $\mathbf{A}$ (thus Γ) are $k, \zeta_2, \dots, \zeta_n$, then the eigenvalues of $\mathbf{A} - k\mathbf{J}/n$ are $0, \zeta_2, \dots, \zeta_n$. In particular, ξ is the spectral radius of $\mathbf{A} - k\mathbf{J}/n$. Now, by applying the Cauchy–Schwarz inequality and dividing by $|S|$,

$$\left| \frac{|AS|}{|S|} - \frac{k}{n}|S| \right| \leq \xi.$$

(This is our version of the aforementioned Expander Mixing Lemma.) We can interpret this inequality as saying that the average number of neighbours (in the subgraph induced by S) of a vertex in S cannot be too far off from $k|S|/n$. Therefore, by looking at the neighbours fixed by g, there exists a vertex $\alpha \in S$ that satisfies Equation (1.2), which completes the proof of the claim.

By combining Equations (1.1) and (1.2), we obtain

$$n - |S| \leq n\frac{q+\xi}{k},$$

which proves the first proportion of the statement.

Suppose that θ is the thickness of $\mathrm{Aut}(\Gamma)$. In particular, $\mathrm{Alt}(\theta)$ is a section of $\mathrm{Aut}(\Gamma)$, thus $\mathrm{Aut}(\Gamma)$ contains an element whose order is the maximum among the orders of elements of $\mathrm{Alt}(\theta)$. Let us denote this maximum by $z(\theta)$. A classical result by E. Landau [84] states that

$$z(\theta) = \exp\left(\sqrt{\theta \log \theta}(1 + o(1))\right).$$

Therefore, not to contradict Lemma 1.6, we have that

$$\exp\left(\frac{k}{k-q-\xi}\log n\right) \geq \exp\left(\sqrt{\theta \log \theta}(1 + o(1))\right).$$

The required asymptotic bound follows. ∎

The hypotheses of Lemma 1.13 are quite harsh in general, and the lack of control over the ratio $(q+\xi)/k$ makes the bound impractical. Surprisingly, specializing it for strongly regular graphs does the bulk of the work in proving the result we are pursuing.

We recall that a *strongly regular graph of parameters* (n, k, λ, μ) is a k-valent graph on n vertices such that any two vertices have exactly λ common neighbourhoods if they are adjacent, μ otherwise. Following [5, 6], a strongly regular graph Γ is *trivial* if Γ or its complement is the disjoint union of cliques of equal size, *graphic* if Γ or its complement is the line graph of a complete or a complete bipartite graph. For a thorough survey on strongly regular graphs, we refer to [24].

We start with a combinatorial result. Most of the ideas behind it are found in [4, Section 3].

Lemma 1.14 · *Let Γ be a nontrivial strongly regular k-valent graph with n vertices. Suppose that $k < n/2$. Then*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), V\Gamma) < 1 - \frac{k}{2n}.$$

Proof. Let $g \in \mathrm{Aut}(\Gamma) - \{1\}$ be a nontrivial automorphism, and let $\alpha \in \mathrm{supp}(g)$ be a vertex moved by g. Consider the pair α and α^g: either they are adjacent or not.

Suppose that α and α^g are adjacent. We note that, since they have λ neighbours in common, there are $2(k-\lambda)$ vertices that are not adjacent to neither α nor α^g. In particular,

$$|\mathrm{supp}(g)| \geq 2(k-\lambda).$$

Similarly, if α and α^g are not adjacent, we obtain that

$$|\mathrm{supp}(g)| \geq 2(k-\mu).$$

Now, we need to prove that, if $\nu = \max\{\lambda, \mu\}$,

$$\min\{2(k-\lambda), 2(k-\mu)\} \geq k - \nu.$$

Let β, γ, δ be three vertices of Γ. Suppose that β and γ are adjacent. Since Γ is nontrivial, we can choose δ which is not adjacent to neither β nor γ. Observe that

$$\Gamma(\beta) - \Gamma(\gamma) \subseteq (\Gamma(\beta) - \Gamma(\delta)) \cup (\Gamma(\delta) - \Gamma(\gamma)).$$

It follows that

$$k - \nu \le k - \lambda \le 2(k - \mu).$$

Similarly, if β and γ are not adjacent, we can choose δ adjacent to both. Hence, we obtain that

$$k - \nu \le k - \mu \le 2(k - \lambda),$$

and the claim is true.

Therefore, in all cases,

$$|\mathrm{supp}(g)| \ge k - \nu,$$

thus

$$\mathrm{fpr}(g, V\Gamma) \le 1 - \frac{k - \nu}{n}.$$

To complete the proof, we need to show that $k/2 > \nu$. To do so, we introduce an auxiliary graph Δ. The graph Δ is bipartite: one part contains all the vertices α of Γ, while the other contains all the neighbourhoods $\Gamma(\alpha)$. A generic vertex of $V\Gamma$ is connected to all the neighbourhoods in which it is contained. Let us fix a vertex of Δ of the form $\Gamma(\alpha)$. We count in two ways the number $\mathbf{s}$ of 2-arcs starting from $\Gamma(\alpha)$. On one hand, $\Gamma(\alpha)$ contains k vertices, and each vertex is contained in other $k-1$ neighbours, thus $\mathbf{s} = k(k-1)$. On the other hand, any two neighbourhoods in Γ intersect in at least ν vertices, hence $\mathbf{s} \ge \nu(n-1)$. Putting the two relation on $\mathbf{s}$ together, we have that

$$k(k-1) \ge \nu(n-1) > \nu(2k-1).$$

This concludes the proof by dividing each side by $2k$ and ignoring the small negative terms. ■

Strongly regular graphs shine when their eigenvalues are studied, but we do not dare to dive into this extensive theory. We just report a lemma tailored for our discussion. (For the reader's convenience, we recall that a strongly regular graph Γ is *nontrivial* if neither Γ nor its complement are the disjoint union of cliques of equal size, and *nongraphic* if neither Γ nor its complement are the line graph of a complete or a complete bipartite graph.)

Lemma 1.15 ([5] Theorem 5) · *Let Γ be a a nontrivial, nongraphic strongly regular k-valent graph with n vertices, and let*

$$\xi = \max\{|\zeta| \mid \zeta \text{ is an eigenvalue of } \Gamma \text{ distinct from } k\}.$$

Suppose that every pair of distinct vertex has at most q common neighbours, and that $k \le n/4$. Then

$$q + \xi < \frac{7}{8}k.$$

With the final pieces of the puzzle, we are ready to dive into the main result of Section 1.E.

Theorem 1.16 ([5] Theorem 2 and Theorem 20) · *Let Γ be a a nontrivial, nongraphic strongly regular k-valent graph with n vertices, and let θ be the thickness of* $\mathrm{Aut}(\Gamma)$. *Then,*

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), V\Gamma) < \frac{7}{8} \quad \text{and} \quad \theta \le O\left(\frac{(\log n)^2}{\log(\log n)}\right).$$

Proof. Observe that the complement of a strongly regular graph is itself strongly regular, and that the two graphs share the same automorphism group. Thus, without loss of generality, we can suppose $k < n/2$. We split the discussion in two: either $k \leq n/4$ or $n/4 < k < n/2$. The former case is taken care of by Lemmas 1.13 and 1.15. Hence, we suppose the latter holds. We can now apply Lemma 1.14, thus obtaining

$$\mathrm{fpr}\,(\mathrm{Aut}(\Gamma), V\Gamma) < 1 - \frac{k}{2n} < 1 - \frac{k}{8k} = \frac{7}{8}.$$

By repeating the reasoning which we used to complete the proof of Lemma 1.13, we obtain that

$$\theta \leq \frac{(\log n)^2}{2\log(\log n)} \cdot \left(\frac{1}{8} + o(1)\right).$$

Therefore, the proof is complete. ■

Let us go back to the Graph Isomorphism Problem for strongly regular graphs. As a first step, we apply an algorithm that recognizes if the graph is trivial or graphic, and, in case of affirmative answer, recognizes it. It is known that this problem can be solved in polynomial time. Otherwise, as the graph is neither trivial nor graphic, Theorem 1.16 implies that its automorphism group is small. It follows that we can identify the automorphism group of the graph in quasipolynomial time through an exhaustive search among all the primitive groups. Therefore, the implementation of the Group Theory Method runs in quasipolynomial time under the extra assumption that the last graph obtained through its reductions is strongly regular.

To conclude Section 1.E, we mention that generalisations of Theorem 1.16 beyond strongly regular graphs are desirable regardless of the Graph Isomorphism Problem. A full survey on the relevant topics would lead us too much astray. We must be content with knowing that this results goes in the direction of proving [8, Conjecture 1.12], which can be interpreted as a combinatorial relaxation of Theorem 1.5. Moreover, it would provide a new approach for studying the minimal degree of primitive permutation groups. (Some known group theoretical results are surveyed in Section 3.B).

The class of distance-transitive graphs is an important open problem for this sought-after generalisation. Recall that a *distance-transitive graph* has the property that, given four vertices $\alpha, \beta, \gamma, \delta$ such that $d_\Gamma(\alpha, \beta) = d_\Gamma(\gamma, \delta)$, there is an automorphism of the graph mapping (α, β) to (γ, δ). The first generalisation of this result is due to B. Kivva.

Theorem 1.17 ([80] Theorem 1.12) · *Let Γ be a distance-transitive graph on n vertices of diameter d. Suppose that the automorphism group of Γ is not a Cameron group. There is a function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ such that*

$$\mathrm{fpr}\,(\mathrm{Aut}(\Gamma), V\Gamma) \leq \left(1 - \frac{1}{\mathbf{f}(d)}\right) n.$$

The function $\mathbf{f}$ appearing in the previous result grows exponentially with the diameter. L. Pyber and S. V. Skresanov has brought the growth down to polynomial.

Theorem 1.18 ([132] Theorem 1.4) · *Let Γ be a distance-transitive graph on n vertices of diameter d. Suppose that the automorphism group of Γ is not a Cameron group. There is a postive constant C such that*

$$\mathrm{fpr}\,(\mathrm{Aut}(\Gamma), V\Gamma) \leq \left(1 - \frac{C}{d^2}\right) n.$$

Last, we observe that the machinery of Section 1.E actually holds for all graphs whose automorphism group is primitive on the vertices. Indeed, Sections 3.C to 3.F are devoted to classifying those vertex-primitive graphs whose fixed point ratio exceeds 1/3.

1.F Orbital graphs

The bottleneck of the Group Theory Method for solving the Graph Isomorphism Problem in efficient time consists in having automorphism groups of graphs whose order is an exponential function of the number of vertices. The same obstruction may arise while trying to compute all the symmetric graphs of a certain class up to a given number of vertices. (In our discussion, symmetric does not have a precise meaning, but it suggests that we impose some property on the automorphism group of the graph.)

Let us assume that we want to enumerate all the arc-transitive digraphs up to n vertices. Let G be a permutation group whose degree does not exceed n. Then, for any pair of points, α and β, we can build a graph Γ whose vertex-set is Ω, and whose arc-set is the G-orbit of (α, β). This graph Γ is called an *orbital digraph for G*. We remark that, for every pair (Γ, G), where Γ is a digraph and G is a transitive group of permutation for Γ whose action on the arcs is transitive, Γ is an orbital digraph for G. If we drop the assumption of arc-transitivity, and we replace it by vertex-transitivity, then Γ is a union of orbital digraphs for G.

To compile the census, we just need to build all the possible orbital digraphs. Let us be more explicit. First of all, we assume that a friend gives us a list of all the possible transitive groups G of degree n. This list is itself quite lengthy.

Theorem 1.19 ([129] Theorem 4.2, and [93] Theorem 2) · *Let M be the number of transitive groups of degree n. Then*

$$\exp\left(O\left(\frac{n^2}{\log(n)}\right)\right) \leq M \leq \exp\left(O\left(\frac{n^2}{\sqrt{\log(n)}}\right)\right).$$

Now, for every group G on the list, we need to compute the orbit of each pair (α, β), where α is fixed, and β can vary among all the elements of Ω. This step will take at least $O(n^2)$ operations for every transitive group of degree n. Upon building the orbital digraph corresponding to each orbit, we need to verify that it was not already included in the list. We ignore the time that this step takes. In total, the algorithm runs in at least

$$O\left(n^2 \cdot \exp\left(\frac{n^2}{\log(n)}\right)\right)$$

steps. This task is unfeasible. Hence, we should be less greedy, and focus on a smaller class of graphs.

Before attempting another census, let us spend some more ink discussing orbital digraphs. Let G be a permutation group with domain Ω, and let α be a point in Ω. (Observe that, if Ω is infinite, all the objects defined in the rest of Section 1.F might also be infinite. In particular, orbital digraph are infinite digraphs.) The orbits of the stabilizer G_α acting on Ω are called the *suborbits of G with respect to α*. Let

$$O_1, O_2, \dots, O_r$$

be the list of all suborbits of G. The integer r is called the *permutational rank of G*, while the cardinalities

$$|O_1| = d_1, \dots, |O_r| = d_r$$

are called the *subdegrees of G*. Without loss of generality, we can suppose that $O_1 = \{\alpha\}$: this is the *trivial suborbit*, and its cardinality $d_1 = 1$ is the *trivial subdegree*. The orbital digraphs and the suborbits of G are in one-to-one correspondence via the map

$$O_i = \{\beta, \dots\} \mapsto \Gamma_i = \left(\Omega, (\alpha, \beta)^G\right). \tag{1.3}$$

Note that the image of the suborbit O_i under this map is a regular digraph of valency d_i.

Observe that $d_1, \dots, d_r$ are not necessarily distinct. Indeed, G has more than one subdegree equal to 1 if, and only if, G_α fixes more than one point. For instance, all the automorphism of the skeleton of a cube Q_8 that are not derangements fix (at least) two antipodal points, hence $d_i = 1$, for some index i.

We define the *minimal nontrivial subdegree of G* by

$$\min\{d_2, d_3, \dots, d_r\}.$$

By the previous discussion, this is the least valency of a digraph (with at least one arc) on which G acts vertex-transitively. We remark that the minimal nontrivial subdegree is well-defined except when $r = 1$, that is, $\Omega = \{\alpha\}$.

An orbital digraph can be, *a priori*, disconnected: for instance, this is always true for the diagonal orbital graph. D. G. Higman has proved in [68] that the group G is primitive if, and only if, all its orbital digraphs are connected. In particular, the number of connected arc-transitive digraphs on which a primitive group acts is $r-1$, while for an imprimitive group this number is at most $r-2$.

Let O be an orbital for G. We can define the *paired orbital* by

$$O^* = \{(\beta, \alpha) \mid (\alpha, \beta) \in O\}.$$

If O and O^* coincide, we say that O is *self-paired*. We can now switch from orbital digraph to *orbital graphs* by taking two paired orbitals as edges of the graph. In particular, the correspondence between orbital digraphs and arc-transitive digraphs can be restated for the undirected case. Upon identifying all orbitals with their paired in the domain of the map of Equation (1.3), we find that there is a one-to-one correspondence between self-paired orbitals of G and graphs on which G acts arc-transitively, and between pairs of orbitals of G, one paired to the other, and graphs on which G acts vertex- and edge-transitively, but not arc-transitively. (If a group of automorphisms has the latter property, it is said to be *half-arc-transitive*.)

We refer to [45, Section 3.2] for a more exhaustive account on orbital graphs.

1.G Normal quotient graphs

The road ahead is dangerous, hence we must sharpen our tools before proceeding. In Section 1.G, we introduce the normal quotient method to set up inductive procedures for vertex-transitive graphs. Meanwhile, in Section 1.H, we discuss faithful amalgams and their relation to arc-transitive graphs.

Definition 1.20 · Let (Γ, G) be a vertex-transitive graph, and let N be a normal subgroup of G. We define the *normal quotient graph* Γ/N as the graph whose vertex-set is the set of N-orbits on $V\Gamma$ as vertices,

$$V\Gamma/N := \left\{\alpha^N \mid \alpha \in V\Gamma\right\},$$

and we declare α^N and β^N to be adjacent if there is an edge of Γ between α' and β', for some $\alpha' \in \alpha^N$ and $\beta' \in \beta^N$.

We remark that, if Γ is connected, then Γ/N is connected. Indeed, let α^N and β^N be two vertices in the quotient. Since Γ is connected, there is a path between α and β. Finally, this path projects to a (possibly trivial) paths of Γ/N connecting α^N and β^N. Hence, the connectedness of Γ/N is proved.

By vertex-transitivity, we can suppose that $\alpha = \alpha'$, and hence β' is a neighbour of α. As a consequence, we have that the valency of a normal quotient cannot increase, that is,

$$\mathrm{val}(\Gamma/N) \le \mathrm{val}(\Gamma).$$

Moreover, if G is also edge-transitive, we claim that either Γ/N is a collection of isolated points or

$$\mathrm{val}(\Gamma/N) \quad \text{divides} \quad \mathrm{val}(\Gamma).$$

Let us assume that we are not in the former scenario. If α^N has a single neighbour in Γ/N, then $\mathrm{val}(\Gamma/N) = 1$, which divides all positive integers. We can suppose that β and γ are two distinct neighbours of α defining distinct N-orbits. Let $g \in G$ such that

$$\{\alpha, \beta\}^g = \{\alpha, \gamma\}.$$

Then

$$\{\alpha, \beta\}^{N_\alpha} \to \{\alpha, \gamma\}^{N_\alpha}, \quad \{\alpha, \beta\}^n \mapsto \{\alpha, \gamma\}^{g^{-1}ng}$$

defines a bijection between the neighbours of α in β^N and those in γ^N. In particular, if $m = |\beta^N \cap \Gamma(\alpha)|$,

$$m \cdot \mathrm{val}(\Gamma/N) = \mathrm{val}(\Gamma),$$

as claimed.

We remark that Definition 1.20 is a special case of the usual graph quotient, where the vertex-set is chosen to be the equivalence classes of some equivalence relation on $V\Gamma$. What sets our definition apart is that it preserves more group theoretical information. Indeed, the group G/N acts (possibly unfaithfully) on Γ/N as a group of automorphisms. We denote by K the kernel of the action of G on the N-orbits. Observe that N is a subgroup of K, and that G/K acts faithfully on Γ/N as a group of automorphisms. Furthermore, if G is vertex-, edge- or arc-transitive on Γ, then so are G/N and G/K on Γ/N. Finally, we observe that, for any vertex $\alpha \in V\Gamma$,

$$(G/K)_{\alpha^N} = G_\alpha K/K \quad \text{is isomorphic to} \quad G_\alpha/K_\alpha\,.$$

Hence, the stabilizer (and the local group, which we will define in Section 1.K) of Γ and Γ/N are isomorphic if, and only if, K is semiregular. (In this case, N must also be semiregular.) This is always the case when the valency does not decrease, $\mathrm{val}(\Gamma/N) = \mathrm{val}(\Gamma)$.

As explained in the introduction of [104], normal quotients can break graph-theoretical problems into surprisingly manageable pieces. The standard approach faces an inevitable dichotomy.

(a) If all the minimal normal subgroup of G are transitive, then G is quasiprimitive. These groups have been classified by C. E. Praeger in [124], and they have a well-understood structure. In many applications, this knowledge is sufficient to deal completely with these situations.

(b) Suppose that there is an intransitive normal subgroup N of G. Typically $(\Gamma/N, G/N)$ lies in the family of vertex-transitive graphs under consideration and, since Γ/N has fewer vertices than Γ, it is natural to try to use an inductive approach. However, the most complicated and creative step is to recover information about the starting pair (Γ, G) from the quotient $(\Gamma/N, G/N)$.

To conclude Section 1.G, we give two impressive application of this method. In [60], M. Giudici and J. Xu have proved that all vertex-transitive and locally-quasiprimitive graphs have a semiregular automorphism, proving the Polycirculant Conjecture for those graphs. (We refer to Section 2.I for the statement of the Polycirculant Conjecture and the definition of semiregular automorphism.) Meanwhile, in [127], C. E. Praeger, P. Spiga and G. Verret have reduced the Weiss Conjecture to a more complicated condition on graphs with simple automorphism groups. (We introduce the Weiss Conjecture in Section 1.K).

1.H Amalgams

We define an *amalgam* as a triplet (L, B, R) of groups such that $B = L \cap R$, and the *index of* (L, B, R) is the couple of positive integers

$$(|L : B|, |R : B|)\,.$$

We say that a group G *realizes* (L,B,R) if G contains both L and R and these subgroups generate G. We observe that, by definition of amalgamated product, $L *_B R$ is the universal covering of any group realizing (L,B,R). Moreover, the amalgam (L,B,R) is *faithful* if no nontrivial subgroup of B is normal in $\langle L,R\rangle$. (By $\langle L,R\rangle$, we denote the group generated by L and R.)

Here is a connecting result that brings us back to symmetric graphs. (Observe that the graph appearing in Lemma 1.21 can have vertex-sets of infinite cardinalities.)

Lemma 1.21 ([110] Lemma 1) · *Let (L,B,R) be a faithful amalgam of index $(k,2)$. There is a one-to-one correspondence between groups G that realize (L,B,R) and connected arc-transitive k-valent graphs (Γ,G) such that L is isomorphic to the stabilizer of a vertex, B of an arc, and R of an edge.*

Proof. Let (Γ,G) be a connected arc-transitive k-valent graph, and let $(\alpha,\beta)\in A\Gamma$ be an arc. We claim that

$$\mathbf{A}(\Gamma,G)=\left(G_\alpha,G_{\alpha\beta},G_{\{\alpha,\beta\}}\right)$$

is a faithful amalgam of index $(k,2)$ which G realizes. Observe that the choice of the arc (α,β) is irrelevant due to arc-transitivity.

Let us first compute the index. Since G is arc-transitive, $G_{\{\alpha,\beta\}}$ swaps (α,β) and its inverse arc (β,α). Note that such an action is transitive on the two arcs, and its stabilizer is $G_{\alpha\beta}$. Hence

$$\left|G_{\{\alpha,\beta\}}:G_{\alpha\beta}\right|=2.$$

Similarly, the arc-transitivity of G implies that G_α acts transitively on $\Gamma(\alpha)$ with point stabiliser $G_{\alpha\beta}$. Thus

$$\left|G_\alpha:G_{\alpha\beta}\right|=\mathrm{val}(\Gamma)=k,$$

which proves that $\mathbf{A}(\Gamma,G)$ has index $(k,2)$.

The action of G on the arcs of Γ is faithful. It follows that $G_{\alpha\beta}$, as the stabilizer of an arc, is core-free. In particular, the unique subgroup of $G_{\alpha\beta}$ that is simultaneously normal in G_α and $G_{\{\alpha,\beta\}}$ is the trivial group. Therefore, $\mathbf{A}(\Gamma,G)$ is a faithful amalgam.

Lastly, G realizes $\mathbf{A}(\Gamma,G)$. Indeed, G contains both G_α and $G_{\{\alpha,\beta\}}$, G_α and $G_{\{\alpha,\beta\}}$ intersects in $G_{\alpha\beta}$, and, by a connectedness argument, G is generated by G_α and $G_{\{\alpha,\beta\}}$. This complete the claim.

We need to deal with the remaining implication. Let G be a group that realizes the amalgam (L,B,R). We define the graph $\Delta(G)$ whose vertex-set is G/L, whose edge-set is G/R, and such that Lg is an endpoint of Rh, for some $g,h\in G$ whenever $Lg\cap Rh$ is nonempty. (Alternatively, for who prefers a Bass–Serre theoretical approach, $\Delta(G)$ is the unique graph whose barycentric subdivision is the universal covering of the graph of groups whose two vertices are labelled by L and R and whose connecting edge is labelled by B. We refer to [136] for the missing notation.)

The right multiplication of G on G/L preserves G/R, hence it induces an automorphism of $\Delta(G)$. By faithfulness of the amalgam, this action of G on the arcs of $\Delta(G)$ is faithful, thus G is a group of automorphisms of $\Delta(G)$. Furthermore, since G realizes (L,B,R), G is generated by L and R, thus $\Delta(G)$ is connected.

Let $\alpha \in V\Delta(G)$ be the vertex corresponding to the right coset L. Observe that L is the vertex-stabilizer of α. Moreover, as R is an edge incident with α, we can identify $B = L \cap R$ with a neighbour of α. It follows that R is the stabilizer of the edge connecting α with this prescribed neighbour, and that the neighbourhoods of α can be identified with the elements of L/B. In particular,

$$\mathrm{val}(\Delta(G)) = |L : B| = k .$$

The proof is complete by pointing out that

$$\mathbf{A}\,(\Delta(G), G) = (L, B, R) . \qquad \blacksquare$$

Let us denote by $\mathcal{T}_k$ the infinite k-valent tree. Observe that, using the notation introduced in the previous proof, $\mathcal{T}_k$ is isomorphic to $\Delta(L *_B R)$, and $L *_B R$ is a group of automorphisms of $\mathcal{T}_k$. Recalling that $L *_B R$ is the universal covering of any group G that realizes the amalgam (L,B,R), Lemma 1.21 implies that $(\mathcal{T}_k, L *_B R)$ is the universal covering of any arc-transitive k-valent graph (Γ, G), where L is isomorphic to the stabilizer of a vertex, B of an arc, and R of an edge. Therefore, we have obtained a recipe for building all such pairs (Γ, G): every (Γ, G) is a normal quotient of the pair $(\mathcal{T}_k, L *_B R)$ via a normal subgroup N of $L *_B R$.

We are only interested in finite graphs. Under the hypothesis of the finiteness of Γ, we obtain that

$$|L *_B R : N| = |V\Gamma|$$

is finite. Thus, the pairs (Γ, G) that we are studying are in one-to-one correspondence with finite index normal subgroups of $L *_B R$.

Moreover, as the graph Γ is finite, L and R are also finite. We say that the amalgam (L,B,R) is *finite* if both L and R is finite. In this case, both L and R can be finitely presented, hence $L *_B R$ is also finitely presented. Our search for amalgams, thus, can be limited to finite faithful amalgams.

To conclude Section 1.H, we list the amalgams that we are going to use in the following. We need to introduce two preliminary definitions. An amalgam (L,B,R) is 2-*transitive* if the action of L on the right cosets of B by right multiplication is 2-transitive, while it is *dihedral* if the action of L on the right cosets of B by right multiplication is isomorphic to the natural action of the dihedral group of degree k.

- (a) A finite presentation for the groups appearing in a faithful dihedral amalgam of index $(4,2)$ has been given in [46].
- (b) The list of the 7 amalgams of the faithful amalgams of index $(3,2)$ has been compiled in [47].
- (c) The list of the 9 amalgams of the faithful 2-transitive amalgams of index $(4,2)$ has been compiled in [110].

We remark that, for these examples, faithful amalgams of index $(d, 2)$ seem to present a generally tame behaviour. For instance, both the number of generators of the amalgamated product $L *_B R$ and the exponent of the groups L and R are bounded by a constant. Does this property generalise for higher valencies?

Question 1.22 · Let (L, B, R) be a faithful amalgam of index $(d, 2)$. Is the minimal number of generators fo $L *_B R$ bounded by a function of d?

We are going to settle Question 1.22 in the negative in Section 3.H.

Question 1.23 · Let (L, B, R) be a faithful amalgam of index $(d, 2)$. Is the exponent of L bounded by a function of d?

Question 1.23 remains quite open. In Section 3.G, we are going to show that the answer is affirmative if we assume some extra properties on the action of L on the right coset space L/B.

1.I Arc-transitive 3-valent graphs

Back to compiling censuses. The first class of symmetric graphs to receive a census was the set of arc-transitive 3-valent graphs. We start by stating a celebrated result by W. T. Tutte. (Theorem 1.24 is an immediate corollary of the two results cited: this has been noted for the first time by C. C. Sims in [139].)

Theorem 1.24 ([154] Theorem XXII, and [155] Theorem) · *Let Γ be a 3-valent arc-transitive graph. Then the order of the stabilizer of a vertex in Γ divides* 48.

Therefore, by the Orbit Stabilizer Lemma, the order of the group of automorphisms of an arc-transitive 3-valent graph Γ is linear in the number of vertices n, that is,

$$|\mathrm{Aut}(\Gamma)| \leq 48n.$$

Theorem 1.24 has been extended by D. Ž. Djoković and G. L. Miller in [47], by diving the arc-transitive 3-valent graphs in 7 classes, depending on the s-regularity and on the existence of an automorphism flipping the arcs. (An *s-arc* is a sequence of $s+1$ adjacent and nonrepeating vertices of $V\Gamma$. A group G acting on Γ is *s-regular* if it is regular on the set of s-arcs.) These classes correspond to the 7 possible amalgams. To compile the census, we need an algorithm that produces all the normal subgroups of the amalgamated products up to a prescribed finite index.

The first algorithmic approach to solve this problem has been performed by M. D. E. Conder and P. Dobcsányi, and it is described in [39]. As we noted in Section 1.H, all the amalgamated products which are universal covers of the automorphism group of an 3-valent arc-transitive graphs are finitely presented. Computational Group Theory has many specialized algorithm for finitely presented groups. For instance, in [44], A. Dietze and M. Scahps have developed the *Low-Index Subgroups Algorithm*, building on the ideas of C. C. Sims (see

[140, Section 5.9]). This classical algorithm has been adapted for this case exploiting two new ideas: the normality of the subgroup forces additional relators in the group, and the original algorithm can be parallelized. The result of M. D. E. Conder and P. Dobcsányi's investigation is the census of all the arc-transitive 3-valent graphs up to 768 vertices, and it is collected in [38].

An estimate of the computation time involved has never been computed. The main reason lies in the fact that this adaptation has been superseded by a much better one, described by D. Firth in his PhD thesis [51]. This procedure, now known as *Low-Index Normal Subgroups Algorithm*, works by considering all the possibilities for composition series for the quotient G/N where G is the finitely-presented group and N is a normal subgroup of up to a given finite index n in G. (I kindly thank F. Rober, who has implemented this algorithm in GAP, for patiently explaining me how this routine works.) Using the package LINS of GAP, the census can theoretically be extended up to $48^{-1} \cdot 10^7$ vertices. The online version of the census, compiled by M. D. E. Conder in MAGMA, currently contains graphs up to $48^{-1} \cdot 10^5$ vertices.

Although the run time of the algorithm described could be quite long if large alternating section appears, this is not the case when applied to the amalgamated products involved in compiling a census of 3-valent arc-transitive graphs. An analysis of the efficiency of the algorithm has never been performed, thus it would make sense to consider the following question. (The hypothesis on the thickness is still obscure, but it is suggested by Lemma 1.33.)

Question 1.25 · Let L, B and R be three finite groups whose thickness is bounded from above by a constant d. Let t be the run time of the LINS algorithm applied to the group $L *_B R$ for finding all the subgroup of index up to n. Can we determine an upper bound on t depending on n and d? Or rather, can we choose this upper bound so that the dependence on n is subexponential?

Can we extend this procedure beyond arc-transitive 3-valent graphs? Unfortunately, there is no hope of generalising Theorem 1.24 to higher valencies in a naive way. Indeed, its proof can be divided in two steps. First, it is proved that the stabilizer G_α acts regularly on the set of s-arcs whose starting vertex is α. This implies that the order of the vertex-stabilizer is of the form $3 \cdot 2^{s-1}$. The second, and more involved, step consists in proving that $s \leq 5$.

In general, for every d-valent graph Γ, with $d \geq 3$, it is true that $\mathrm{Aut}(\Gamma)$ cannot act transitive on the set of all s-arcs for large integer s. The precise result by R. Weiss is as follows.

Theorem 1.26 ([162] Theorem) · *Let Γ be an arc-transitive d-valent graph, with $d \geq 3$, and let*

$$s := \max\{t \in \mathbb{N} \mid \mathrm{Aut}(\Gamma)_\alpha \textit{ is transitive on } s\textit{-arcs starting at } \alpha\}.$$

Then either $s \leq 5$, or $s = 7$ and Γ belongs to a well-understood family of graphs.

Hence, the second step of the proof of Theorem 1.24 can be generalised for every d-valent graph, with $d \geq 3$. On the other hand, the first step is highly reliant on the fact that every t-arc can be prolonged to a $(t+1)$-arc in just two ways, and there is a unique nontrivial permutation group on 2 points. Indeed, there is no hope for a generalisation already for 4-valent graphs. Even worse, the vertex-stabilizer of an arc-transitive 4-valent graph can be exponentially large with respect to the number of points. (We have to patient until Section 2.A for an example.)

Therefore, we find an intermediate question to produce censuses efficiently. Observe that, if the order of a vertex-stabilizer has a growth that is faster than polynomial, the algorithmic approach to compiling a census becomes quickly unpractical. We have a specialization of Question A in this setting.

Question 1.27 · Let G be a group, and let Γ be a d-valent connected graph. Under which extra assumption on (Γ, G) can we control the order of a vertex-stabilizer G_α?

1.J Sims Conjecture

The most significant family of permutation groups for which we know how to answer Question 1.27 is that of finite primitive groups. In this case, the order of the vertex-stabilizer is bounded above by a function of the valency d. More precisely, in [139], C. C. Sims conjectured that the stabilizer in a primitive group is bounded from above by a function of the minimal nontrivial subdegree. Settling this conjecture has been one of the first results relying on the Classification of Finite Groups. Indeed, P. J. Cameron, C. E. Praeger, J. Saxl and G. M. Seitz have proved the following result.

Theorem 1.28 ([34] Theorem 1) · *There is a function* $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ *such that, for every finite primitive permutation group G of minimal nontrivial subdegree d, and for every point α,*

$$|G_\alpha| \le \mathbf{f}(d).$$

Their proof relies on two reductions that greatly reduce the number of permutation groups that must be considered. The first reduction consists, using the O'Nan-Scott Theorem on the structure of primitive groups (see [31, 89]), in excluding all the cases where the group does not have a simple socle. The second reduction relies on the following result by J. G. Thompson.

Theorem 1.29 ([149] Equation (∗∗)) · *There is a function* $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ *such that, for every finite primitive permutation group G of minimal nontrivial subdegree d, and for every point α,*

$$|G_\alpha : \mathbf{O}_p(G_\alpha)| \le \mathbf{f}(d).$$

Since we want to bound $|G_\alpha|$, in view of Theorem 1.29, we must take $|\mathbf{O}_p(G_\alpha)|$ to be the largest possible. Hence, it can be assumed that G_α is the normalizer of a nontrivial p-group P. At this point, the p-local structure of finite simple groups gives a solution to the problem.

The concrete functions $\mathbf{f}$ appearing in Theorems 1.28 and 1.29 have growth

$$\mathbf{f}(d) = \exp\left(d^2 o(d)\right).$$

This follows from the original proof of J. G. Thompson. It is unknown whether this upper bound is optimal or not, and there has been no attempt to improve it. Heuristically, by considering the natural action of the symmetric group Sym($d+1$), we find that

$$|\mathrm{Sym}(d) : \mathbf{O}_p(\mathrm{Sym}(d))| = |\mathrm{Sym}(d)| \leq \exp\left(d \log(d) + o(d)\right),$$

and we cannot think of groups with a larger index. Hence, an interesting open problem is to obtain a sharp version of Theorem 1.28. We can phrase it as follows.

Question 1.30 · What is the growth of the optimal function that solves Sims's Conjecture?

Theorem 1.28 has an amazing combinatorial corollary dealing with distance-transitive graphs. Upon identifying *antipodal vertices* (that is, pair of points at maximal distance) and breaking the bipartiteness by imposing that vertices at distance 2 are adjacent, the automorphism group of a distance-transitive graph is primitive. (This result is due to D. H. Smith and can be found in [141]). All the locally finite distance-transitive graphs have been described by H. D. Macpherson in [95]. Therefore, using some model theoretical arguments, we can obtain the following result.

Corollary 1.31 ([34] Theorem 2) · *For every $d \geq 3$, the number of finite distance transitive d-valent graphs is finite.*

Therefore, it makes no sense to develop a theory of limits for distance-transitive graphs. This is probably the reason why such a theory has not been developed for vertex-primitive graphs. What is known about this topic is contained in [59, 150]. The structure of the limit graphs of converging sequences of vertex-primitive graphs are, to this day, completely mysterious.

We conclude this section with a bipartite version of Theorem 1.28. (The following result has been proved with the invaluable help of L. Sabatini.)

Theorem B · *Let G be a finite group, and let H and K be two maximal subgroups whose intersection is core-free in G. Suppose that*

$$h = |H : H \cap K| \quad \textit{and} \quad k = |K : H \cap K|.$$

Then

$$|H \cap K| \leq \mathbf{f}(hk)^2.$$

Proof. Observe that

$$\mathrm{core}(H \cap K) = \bigcap_{g \in G} (H \cap K)^g$$

is a normal subgroup of G contained in both H and K. This yields that

$$\mathrm{core}(H) \cap \mathrm{core}(K) \leq \mathrm{core}(H \cap K) = 1.$$

We compute

$$\begin{aligned} |H \cap K| &= |H \cap K : \mathrm{core}(H) \cap \mathrm{core}(K)| \\ &\leq |H \cap K : \mathrm{core}(H) \cap K| \cdot |K \cap H : H \cap \mathrm{core}(K)|. \end{aligned}$$

Moreover,

$$|H \cap K : \mathrm{core}(H) \cap K| \leq |H : \mathrm{core}(H)|,$$

and

$$|K \cap H : \mathrm{core}(K) \cap H| \leq |K : \mathrm{core}(K)|.$$

To conclude the proof, we consider four auxiliary graphs. We start with Δ: this graph is bipartite, one part consists of the right coset space G/H, while the other part consists of the right coset space G/K. Two cosets are adjacent if their intersection is nonempty. We now consider the distance 2 graph of Δ, that is, a graph Δ_2 with the same vertices of Δ, two of which are declared adjacent if their distance in Δ is 2. Since H and K are at distance 1 in Δ, H and K belongs to two distinct connected components of Δ_2. By maximality of H and K in G, [68] implies that its connected components are exactly two. We denote by $\Delta(H)$ the connected component of Δ_2 containing H, and by $\Delta(K)$ the one containing K. Note that the valencies of $\Delta(H)$ and of $\Delta(K)$ cannot exceed hk. Moreover, G acts primitively on the vertex-sets of $\Delta(H)$ and of $\Delta(K)$ with stabilizers isomorphic to H and to K respectively. Therefore, by Theorem 1.28, we obtain

$$|H : \mathrm{core}(H)| \leq \mathbf{f}(hk) \quad \text{and} \quad |K : \mathrm{core}(K)| \leq \mathbf{f}(hk).$$

Our chains of inequality leads us to

$$|H \cap K| \leq \mathbf{f}(hk)^2,$$

as desired. ■

With some patience, the proof can be adapted to allow any finite number of maximal subgroups whose intersection is core-free.

1.K Weiss Conjecture

The beautiful hypothesis of vertex-primitivity, together with bounded valency, implies that the stabilizer of a vertex has bounded order. But this solution has one problem: it requires global information, that is, the lack of a nontrivial system of imprimitivity for the automorphism group of the graph. What we wish is a *local to global* approach mimicking Theorem 1.24: the local hypothesis that a vertex-stabilizer acts transitively on the 3 neighbours of a point is enough to obtain the global result of having bounded order for the vertex-stabilizer.

A graph Γ, where $V\Gamma$ is allowed to be an infinite set, is said to be *locally finite* if the valency of any vertex is bounded from above by a constant and the size. If the automorphism group of $\mathrm{Aut}(\Gamma)$ is vertex-transitive, this condition is equivalent to the valency of Γ being finite. Moreover, for the remainder of the thesis, when we talk about a group of automorphisms of Γ, we only focus on those groups whose vertex-stabilizer is finite.

The base ingredient for local to global procedures is the local group. Let Γ be a locally finite graph, and let G be a group of automorphisms of Γ. Suppose that G is transitive on the vertex-set $V\Gamma$, and choose a vertex α. The local group of the pair (Γ, G) is the permutation group $G_\alpha^{\Gamma(\alpha)}$ that G_α induces on the neighbourhood $\Gamma(\alpha)$. In particular, if we denote by $G_\alpha^{[r]}$ the stabilizer of a ball of radius r, then

$$G_\alpha^{\Gamma(\alpha)} \cong G_\alpha/G_\alpha^{[1]}.$$

Many global properties can be obtained from the local pair of (Γ, G). The following lemma gives an astonishing example. (We recall that, for a group H, $\pi(H)$ is the set of primes dividing the order of H.)

Lemma 1.32 · *Let Γ be a connected graph, let G be a vertex-transitive group of automorphisms of Γ, and let $\alpha \in V\Gamma$ be a vertex. Then*

$$\pi\left(G_\alpha^{\Gamma(\alpha)}\right) = \pi(G_\alpha).$$

Proof. Aiming for a contradiction, suppose that p is a prime that divides the order of G_α but not of $G_\alpha^{\Gamma(\alpha)}$. This implies that there is an automorphism g of order p such that $g \in G_\alpha^{[1]}$. Choose β to be a vertex at minimal distance from α such that g does not fix β. By connectedness, there exists a path

$$\alpha = \gamma_0 \sim \gamma_1 \sim \ldots \sim \gamma_h \sim \gamma_{h+1} = \beta.$$

Note that g fixes γ_h. In particular, g belongs to the stabilizer of γ_h. Therefore, p divides the order of G_{γ_h}. Finally, by vertex-transitivity, p divides the order of G_α, a contradiction. ■

The proof of Lemma 1.32 showcases the use of the standard connectedness argument. A polemic reader could complain that we used the hypothesis that Γ is connected, that is not a local condition. Indeed, the local to global approach works only on the family of connected graphs. A counterexample to most desirable properties is usually obtained by taking a large number of isomorphic copies of an arbitrary graph. In this case, a large symmetric groups acts on the graph shuffling the components, and the local group cannot predict anything about this.

We give some other examples of global properties that can be tested locally. Let Γ be a d-valent graph, and let G be a vertex-transitive group of automorphisms of Γ. We denote by L the local group of the pair (Γ, G).

(a) The local group L is trivial if, and only if, the group of automorphisms G acts regularly on the vertices $V\Gamma$. This fact is a direct consequence of Lemma 1.32.

(b) The local group L is semiregular if, and only if, the group of automorphisms G acts semiregularly on the arcs. Indeed, if the local group is semiregular, the only automorphism that stabilizer two adjacent vertices is trivial.

(c) The local group L is transitive if, and only if, the group of automorphisms G acts transitively on the arcs. To map the arc (α, β) to the arc (γ, δ), it is enough to choose a map $g \in G$ such that $\alpha^g = \gamma$ (which exists by vertex-transitivity), and then we use the local assumption to move β^g to δ with an element of G_γ.

(d) The local group L is 2-transitive if, and only if, the group of automorphisms G acts 2-arc-transitively. The proof is quite similar to that of part (c). Suppose you want to map the 2-arc $(\alpha_0, \alpha_1, \alpha_2)$ in $(\beta_0, \beta_1, \beta_2)$. By vertex-transitivity, we can map α_1 to β_1 via some $g \in G$. Then, using the 2-transitivity of the local group, we can find a permutation h that stabilizes β_1 such that the $\alpha_0^{gh} = \beta_0$ and $\alpha_2^{gh} = \beta_2$.

We end this brief review with a result that has already been anticipated twice before.

Lemma 1.33 · *Let Γ be a connected graph, let $\alpha \in V\Gamma$ be a vertex, and let G be a vertex-transitive group of automorphisms of Γ. Suppose that X is the collection of all simple sections of the local group. Then every simple section of G_α appears in X. In particular,*

(a) *the local group is solvable if, and only if, the vertex-stabilizer is solvable,*

(b) *the local group and the vertex-stabilizer share the same thickness.*

Proof. Let L be the local group of the pair (Γ, G). As G is vertex-transitive, the action of G_α on the ball of radius 2 centred in α can be embedded in the wreath product $L \operatorname{wr} L$, where the top group corresponds to the action of G_α on $\Gamma(\alpha)$, while the base group contains isomorphic images of some stabilizers in $G_\alpha^{\Gamma(\alpha)}$ in which the neighbour corresponding to α is fixed. Although it becomes increasingly difficult to write down as the radius of the ball increases, the reader should be convinced that, for any positive integer r,

$$G_\alpha / G_\alpha^{[r]} \quad \text{can be embedded in} \quad ((L \operatorname{wr} L) \operatorname{wr} \ldots) \operatorname{wr} L,$$

where the wreath product is iterated r times. The result is now a consequence of the fact that, for every group A and B, the set of simple sections of a wreath product $A \operatorname{wr} B$ is the same as the set of simple sections of A and B.

The two consequences can be obtained recalling that both solvability and thickness are completely determined by the set of simple sections X of the group. The former corresponds to having only cyclic groups in X, while the latter only depends on how large are the nonabelian factors in X. ■

We are interested in those local groups whose appearance forces the order of a vertex-stabilizer to be bounded by a constant.

Definition 1.34 · Let L be a finite permutation group. We say that L is *graph-restrictive* if there is a constant $\mathbf{c}(L)$ such that, for every pair (Γ, G), with Γ a connected locally finite graph, G a vertex-transitive group of automorphism with finite vertex-stabilizer, and local group isomorphic to L,

$$|G_\alpha| \leq \mathbf{c}(L).$$

The Holy Grail of this local to global approach is the *Weiss Conjecture*.

Conjecture 1.35 ([159] Conjecture 3.12) · Every finite primitive group is graph-restrictive.

The conjecture has been settled for 2-arc-transitive graphs through a monumental work spanning [57, 151, 152, 161, 163].

Theorem 1.36 · *Every finite 2-transitive group is graph-restrictive. In particular, for every pair* (Γ, G)*, where* Γ *is a locally finite connected graph,* G *is a vertex-transitive group of automorphisms with finite vertex-stabilizer, and the local group of* (Γ, G) *is 2-transitive, the stabilizer of a ball of radius* 6 *is trivial.*

In the following years, further evidence has arisen and Conjecture 1.35 has been extended. First, in [125], C. E. Praeger has noticed that almost all the attempt depended on techniques relying on the local group being quasiprimitive. Then, in [113], P. Potočnik, P. Spiga and G. Verret have proved that any graph-restrictive group must be a semiprimitive permutation group. (A permutation group G is *semiprimitive* if all its normal subgroups are either transitive or semiregular. All quasiprimitive groups are also semiprimitive.) This has prompted the current version of the conjecture.

Conjecture 1.37 ([113] Conjecture 3) · A finite permutation group is graph-restrictive if, and only if, it it semiprimitive.

We devout the rest of Section 1.K to a short survey of what is know about the Weiss Conjecture. Two different philosophies has been followed to tackle the problem: using the O'Nan–Scott Theorem to tackle the families of primitive groups in turn, or finding a reduction to an easier setting.

A key ingredient in all the O'Nan–Scott based attacks has been a generalisation of Theorem 1.29, now known as the *Thompson–Wielandt Theorem*. The original version of this result is due to A. Gardiner, generalising previous results of H. Wielandt and A. W. Knapp (see [56, Theorem 2.1 and Corollary 2.3]). The result was extended to quasiprimitive local groups by J. van Bon in [156], and later to semiprimitive local groups by P. Spiga in [143]. (We remark that, in [143], Theorem 1.38 is proven in a slightly more general setting.) For every arc (α, β) of a graph Γ, we denote by $G_{\alpha\beta}^{[1]}$ the pointwise stabilizer of $B_\Gamma(\alpha, 1) \cup B_\Gamma(\beta, 1)$, that is,

$$G_{\alpha\beta}^{[1]} = G_\alpha^{[1]} \cap G_\beta^{[1]}.$$

Theorem 1.38 · *Let* Γ *be a connected graph, let* G *be a group of automorphisms for* Γ *with finite vertex-stabilizer, and let* $(\alpha, \beta) \in A\Gamma$ *be an arc. Suppose that the local group of the pair* (Γ, G) *is semiprimitive. Then* $G_{\alpha\beta}^{[1]}$ *is a* p*-group.*

Theorem 1.38 imposes tight restrictions on the structure of G_α. For instance, if Γ has valency d, then G_α contains a normal p-subgroup of index at most $d(d-1)!^2$. Tinkering with these restrictions, it is possible to prove that either the local group is regular or it contains a nonabelian normal subgroup whose action is regular. Indeed, this argument has been used by P. Spiga in [142] to deal with local groups of type TW, while V. I. Trofimov has done the same in [153] for types HS and HC.

The next case solved has been local groups with elementary abelian socle, that is, primitive groups of type HA. Indeed, in [160], R. Weiss has settled the conjecture for all characteristic but 2 and 3. The proof has been completed for all primes by P. Spiga in [145] using the *Local* $\mathcal{C}(G,T)$ *Theorem* (see [25]).

The most recent progress consists in proving the Weiss Conjecture for local groups of type SD and CD. To do so, V. I. Trofimov in [153] has relied on the theory of *offenders*: we refer the curious reader to [37, 103].

Therefore, the only cases left are primitive local groups of type AS and PA.

Theorem 1.39 · *Then there is a function* $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ *with the following property. Let* Γ *be a* d*-valent connected graph, and let* G *be a group of automorphisms of* Γ *with finite vertex-stabilizer. Suppose that the local group of the pair* (Γ, G) *is primitive of type HA, HS, HC, TW, SD or CD. Then*

$$|G_\alpha| \le \mathbf{f}(d) < (d^6)!.$$

We now switch to the reduction based approach. In [122], C. E. Praeger has proved that, for nonbipartite graphs, we can assume that the automorphism group of the graph is quasiprimitive. We underline that her result has pioneered the normal quotient method. Building on this result, in [41], M. D. Conder, C. H. Li and C. E. Praeger further reduced the problem for nonbipartite graphs to the case of graphs with almost simple automorphism group. The last extension to these ideas is due to C. E. Praeger, P. Spiga and G. Verret in [127]: through the normal quotient method, we can reduce the problem to automorphism groups which are either quasiprimitive or *biquasiprimitive* (that is, intransitive with two orbits, with quasiprimitive transitive constituents), and, to solve this version of the problem, it is enough to consider automorphism groups which are almost simple. This is a genuine reduction of the Weiss Conjecture to the case with nonabelian finite simple automorphism groups.

The concept of growth in groups has also been ingeniously applied to tackle this last scenario. The celebrated [133, Theorem 2] by L. Pyber and E. Szabó (see also [23]) states that, for every simple group T of Lie type of rank r, and for every generating set S of T, either $T = S^3$, or there are two positive constants, $c(r)$ and $\epsilon(r)$, depending only on the rank r such that

$$|S|^{1+\epsilon(r)} \le c(r)|S^3|. \tag{1.4}$$

Recall that the thickness of a group of Lie type is a linear function of its Lie rank. Hence, we can replace Lie rank by thickness in the previous statement.

Suppose now that Γ is a finite d-valent connected graph, and T is an arc-transitive group of automorphisms of Γ. Moreover, suppose that T is of Lie type and thickness θ. Let us choose a vertex $\alpha \in \Gamma$, so we can choose

$$S = \{g \in T \mid \alpha^g \in \Gamma(\alpha)\}.$$

By connectedness of Γ, we have that S is a generating set for T (see the proof of Theorem O). Since S is a union of d right coset of T_α,

$$|S| = d|T_\alpha|.$$

Furthermore, $|S^3|$ counts the number of paths of length 3 starting from α. Thus (skipping some intermediate computations)

$$|S^3| \le d^3|T_\alpha|.$$

Now, we split the discussion according to whether $S^3 = T$ or not. In the former case,

$$|V\Gamma| = |T : T_\alpha| = \frac{|S^3|}{|T_\alpha|} \leq d^3.$$

Therefore, T_α can be embedded into $\mathrm{Sym}(d^3-1)$. Hence

$$|T_\alpha| \leq (d^3-1)!\,.$$

Suppose now that S^3 does not coincide with T. By Equation (1.4), we have that

$$(k|T_\alpha|)^{1+\epsilon(\theta)} = |S|^{1+\epsilon(\theta)} \leq c(\theta)|S^3| \leq c(\theta)k^3|T_\alpha|^3\,.$$

Hence, a direct computation leads to

$$|T_\alpha| = c(\theta)^{1/(\epsilon(\theta)-2)}k \leq c(\theta)^{1/(\epsilon(\theta)-2)}d\,.$$

Since we are dealing with a function increasing with thickness, there is nothing to discuss about the alternating groups, and, since our goal is asymptotic in nature, the sporadic groups do not enter the picture. Therefore, we have obtained the following result by L. Pyber, C. E. Praeger, P. Spiga and E. Szabó.

Theorem 1.40 ([131] Theorem 2) · *There exists a function* $\mathbf{g} : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ *with the following property. Let* Γ *be a finite* d*-valent connected graph, and let* G *be a group of automorphisms of* Γ*. Suppose that the local group of the pair* (Γ, G) *is primitive, and that the thickness of* G *is* θ*. Then*

$$|G_\alpha| \leq \mathbf{g}(d,\theta)\,.$$

1.L Vertex-transitive 3-valent graphs

In Section 1.L, following [115], we ask ourselves if we can broaden our census to include all vertex-transitive 3-valent graphs. The local group partitions the family according to the number of orbits it defines. If the local group is transitive, then the graph is arc-transitive, thus it already appears in the census described in Section 1.I. The interesting cases are when the local group is intransitive. Two scenarios need to be analysed: either the local group is trivial, and hence it defines three orbits, or it is isomorphic to a cyclic group of order two, and so it has an orbit of length two and a fixed point.

We start by dealing with the hypothesis of trivial local group. Since we cannot use amalgams, we must fall back to the naive approach described in Section 1.F. Rather than considering all the orbital graphs, a first reduction can be obtained from the following observation of G. Sabidussi.

Theorem 1.41 ([135] Theorem 3) · *There is a one-to-one correspondence between Cayley graphs* $\mathrm{Cay}(G,S)$ *and pairs* (Γ, G)*, where* G *is a vertex-regular group of automorphism of* Γ*.*

Therefore, our task can be translated to compiling a census of 3-valent Cayley graphs. Observe that, rather than a list of all the transitive permutation groups up to given degree, we are satisfied with a friend that gives us the list of all the abstract groups up to a given order. Now, [130, Corollary] states that the number of groups of order n does not exceed

$$\exp\left(\left(\frac{2}{27}+o(1)\right)\log(n)^3\right).$$

Hence, the size of the list of all groups up to order n is quasipolynomial in the number of vertices n. Although this task is considerably faster than computing all the orbital digraphs, our algorithm is still not viable for implementation. This is caused by the abundance of p-groups, whose number asymptotically coincides with the upper bound. This is a consequence of the famous lower bound that G. Higman proved in [69] (see also [138]). Therefore, when n is a prime power, the number of abstract groups to consider grows too large for our computational capabilities.

Rather than building all the orbital graphs of the regular actions of the groups on themselves, we shall take advantage of Theorem 1.41, and focus on finding a suitable connection set S. The following two results go in this direction.

Lemma 1.42 ([115] Lemma 2) · *Let G be a finite group, and let $\mathrm{Cay}(G,S)$ be a connected Cayley graph of valency at most 3. Then, G/G' is isomorphic to either C_2^3 or to $C_2\times C_r$ or to C_r, for some positive integer r.*

Lemma 1.43 ([2] Lemma 3.1) · *Let G be a group, let φ be a group automorphism of G, and let S be a symmetric subset of G. Then $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G,S^\varphi)$ are isomorphic.*

Lemma 1.42 drastically reduces the number of group that need to be considered. For instance, there are 1 090 235 groups of order 768 (up to isomorphism), while only 4 810 of them satisfy this condition on the abelian quotient. Furthermore, Lemma 1.43 gives us a recipe to greatly reduce the number of connection sets S we must consider for each group G. Observe that the converse of Lemma 1.43 does not hold, thus, if we want a representative for each class of isomorphism of graphs, we still need to run an algorithm that checks for isomorphisms.

Combining these results, we find that, to build our census of 3-valent Cayley graphs, it is sufficient to determine the $\mathrm{Aut}(G)$-orbits of inverse-closed generating 3-subsets of G. Still, our last refinement of the algorithm has two critical aspects.

Computing $\mathrm{Aut}(G)$ can take a long time. The complexity of the algorithm devised by B. Eick, C. R. Leedham-Green and E. A. O'Brien in [49] depends heavily on the number of generators of G and on the rank of the elementary abelian sections of G. In our case, since the groups we deal with are 3-generated, the algorithm takes a reasonable amount of time.

The second critical point is related to 2-groups. The list of 2-groups of order 512 is already too large to handle, while there is no exhaustive list of groups of order 1 024. This case has been dealt with in [115] using cohomological methods, which we will not explore here.

We now turn to the case with local group isomorphic to C_2. The main tool to deal with this scenario is a one-to-one correspondence between 3-valent graphs whose local group is isomorphic to C_2 and 4-valent graphs whose local group is transitive and imprimitive: the so-called splitting and merging operations. To prove some results of Chapter 2, we need an extensive study of this correspondence. Hence, rather than give a partial explanation here, we will devote Sections 2.C and 2.D to develop this subject in details.

Through this reduction, to find all the 3-valent vertex-transitive graphs, we need to compile the census of 4-valent arc-transitive graphs whose local group is imprimitive up to half the number of vertices. We can follow the same set of ideas we used for the arc-transitive 3-valent case. We need to describe the amalgams that can appear, and then we need to apply the LINS routine to produce the normal subgroups by which to quotient the universal covering of the graph.

The are three possible local groups: $C_2 \times C_2$, C_4 or D_8. In the former two cases, the permutation group is regular, thus G is arc-regular. In particular, it is immediate to find that the only two amalgams (L,B,R) arising in these cases are of the form

$$(C_2 \times C_2, 1, C_2) \quad \text{and} \quad (C_4, 1, C_2)\,.$$

We now have to deal with the last scenario. The amalgams corresponding to the local group D_8 have been described by D. Ž. Djoković in [46]. Since the local group is not graph-restrictive, the vertex-stabilizer has order 2^s, where s is an unbounded positive integer, thus infinitely many amalgams indexed by s arise. A significant bound on s depending on the number of vertices is needed before venturing further.

Theorem 1.44 ([117] Theorem 1.2) · *Let Γ be a 4-valent graph, let α be a vertex of Γ, and let G be an arc-transitive group of automorphisms of Γ. Suppose that the local group of the pair (Γ, G) is D_8. Then either*

$$2|G_\alpha|\log_2\left(\frac{|G_\alpha|}{2}\right) \leq |V\Gamma|,$$

or the pair (Γ, G) is known.

Theorem 1.44 tells us that only finitely many amalgams have to be considered depending on the choice of the target number of vertices. Observe that, apart from the known exceptions, this result states that the order of a vertex-stabilizer grows linearly with the number of vertices. This, rather than the local group being graph-restrictive, is what we need to compile a census of arc-transitive graphs.

We conclude Section 1.L by pointing out that the ideas we have explored to deal with the local group D_8 have been used by P. Potočnik, P. Spiga and G. Verret in [118] to build a census of 4-valent edge-transitive but not arc-transitive graphs. The result that plays the role of Theorem 1.44 has been proved in [147].

1.M Unbounded vertex-stabilizers

Inspired by the second half of Section 1.L, we can propose a general strategy to compile the census of arc-transitive graphs of a given valency in two steps.

(*a*) Obtain all the faithful amalgams of index $(d,2)$.

(*b*) Prove that, outside of a family of well-understood graphs, the number of automorphisms of our graphs does not grow too fast with respect to the number of vertices.

We underline that both steps are highly nontrivial, and the second step might even be impossible in general. Still, this approach explains why bounding the size of a vertex-stabilizer by a function of the number of vertices might be an interesting question to consider.

Theorem 1.45 ([116] Section 6, and [71] Theorem 1.1) • *Let Γ be a locally finite connected d-valent graph with n vertices, let α be a vertex of Γ, and let G be an arc-transitive group of automorphisms of Γ with $|G_\alpha|$ finite. Suppose that d is at most 7, and that the local group of the pair (G,Γ) is isomorphic to L. Then one of the following happens:*

(*a*) *if L is either primitive or regular, then $|G_\alpha|$ is bounded by a constant;*

(*b*) *if L is isomorphic to the dihedral group of degree 6, then there exists a positive integer ϵ_1 such that*

$$|G_\alpha| \leq O(n^{\epsilon_1}),$$

and there is an infinite family of such pairs (Γ, G) such that, for a positive integer ϵ_2,

$$O(n^{\epsilon_2}) \leq |G_\alpha|;$$

(*c*) *if L does not appear in the previous points, then there exists a positive constant c such that*

$$\exp(cn + o(1)) \leq |G_\alpha| \leq d^{n-1}.$$

Many open questions remain. For instance, we have no significant result about transitive local groups of degree 8.

We need some extra notation to state the most fascinating problem. We say that a function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ is *subpolynomial* if

$$\mathbf{f}(n) \text{ is unbounded} \quad \text{and} \quad \lim_n \frac{\log(\mathbf{f}(n))}{\log(n)} = 0,$$

while we say that $\mathbf{f}$ is *subexponential* if

$$\frac{\log(\mathbf{f}(n))}{\log(n)} \text{ is unbounded} \quad \text{and} \quad \lim_n \frac{\log(\mathbf{f}(n))}{n} = 0.$$

Note that, according to this definition, the classes of subpolynomial and subexponential functions are disjoint from the classes of constant, polynomial and exponential functions.

Problem 1.46 ([116] Question 4) · Let Γ be a locally finite connected graph, let α be a vertex of Γ, and let G be an arc-transitive group of automorphisms of Γ with $|G_\alpha$ finite. Does there exist a permutation group L such that, if the local group of the pair (G,Γ) is isomorphic to L, then we can find two subpolynomial functions $\mathbf{f}_1,\mathbf{f}_2 : \mathbb{N} \to \mathbb{N}$ such that

$$\mathbf{f}_1(|V\Gamma|) \leq |G_\alpha| \leq \mathbf{f}_2(|V\Gamma|)?$$

Does the same hold for subexponential functions?

2 Small valency

Tout ceci parce que tu sais que j'étais voleuse autrefois

– *Séance tenante*, Joyce Mansour (1953)

We say that the valency of a graph is *small* if we have control of the local group: as a consequence, we can exploit powerful tools such as amalgams (see Section 1.H) and normal quotients (see Section 1.G).

The first proportion of Chapter 2 is devoted to sharpening our tools to deal with Praeger–Xu graphs and their splitting. The second part tackles two separate problems. In Sections 2.E and 2.F, we show that the Praeger–Xu graphs and their splitting can be characterized as being those 4-valent and 3-valent graphs whose fixed point ratio exceeds 1/3. In Section 2.I, we prove that, if the number of vertices is large enough, the vertex-transitive automorphism group of a 3-valent graph contains a semiregular element of order at least 6.

(We would also like to emphasize now that all the permutation groups and all the graphs in Chapter 2 are finite.)

2.A Praeger–Xu graphs

While dealing with small valencies, two infinite families of graphs will pose the most intricate challenge: the Praeger–Xu graphs and their splittings. That is due to the fact that they have exponentially large groups of automorphisms with respect to the number of vertices, and this fact causes various complications with regard to many natural questions.

Section 2.A is devoted to introducing the ubiquitous 4-valent Praeger–Xu graphs $\mathrm{C}(r,s)$ and their automorphism groups. This infinite family had been originally defined in [128] while studying graphs whose automorphism group contains a normal elementary abelian subgroup whose action is not semiregular. Praeger–Xu graphs have been studied in detail by A. D. Gardiner, C. E. Praeger and M. Xu in [58, 123, 128], and more recently in [14, 15, 73, 74]. Here, we introduce them through their directed counterparts defined in [123].

We need to recall the definition of wreath product of graphs.

Definition 2.1 · Let Γ and Δ be two digraphs. The *wreath product of* Γ *and* Δ, denoted by $\Gamma \operatorname{wr} \Delta$, is the graph of vertex-set $V\Gamma \times V\Delta$, where (δ_1,γ_1) and (δ_2,γ_2) are adjacent if either $\delta_1 = \delta_2$ and $(\gamma_1,\gamma_2) \in A\Gamma$, or $(\delta_1,\delta_2) \in A\Delta$.

This name is due to the fact that

$$\mathrm{Aut}(\Gamma)\,\mathrm{wr}\,\mathrm{Aut}(\Delta) \quad \text{is a subgroup of} \quad \mathrm{Aut}(\Gamma\,\mathrm{wr}\,\Delta).$$

For further information on wreath products of digraphs, we refer the curious reader to [48].

Moreover, we recall that the neighbours of a digraph Γ can be distinguished in two classes: for any vertex $\alpha \in V\Gamma$, the *out-neighbours of* α are the $\beta \in V\Gamma$ such that $(\alpha,\beta) \in A\Gamma$, while the *in-neighbours of* α are the $\gamma \in V\Gamma$ such that $(\gamma,\alpha) \in A\Gamma$. In such fashion, the valency of a digraph is the sum of its *out-valency* and its *in-valency*.

Let r be a positive integer with $r \geq 3$. We define $\vec{\mathrm{C}}(r,1)$ to be the wreath product of an edgeless graph on 2 vertices, $2\mathbf{K}_1$, by a directed cycle of length r. In other words,

$$V\vec{\mathrm{C}}(r,1) = \mathbb{Z}_r \times \mathbb{Z}_2$$

with the out-neighbours of the vertex (x,i) being $(x+1,0)$ and $(x+1,1)$. We will identify the $(s-1)$-arc

$$(x,\epsilon_0) \sim (x+1,\epsilon_1) \sim \ldots \sim (x+s-1,\epsilon_{s-1})$$

with the pair $(x;k)$ where $k = \epsilon_0\epsilon_1\ldots\epsilon_{s-1}$ is a string in $\mathbb{Z}_2$ of length s. Let s be a positive integer with $s \geq 2$. We let $V\vec{\mathrm{C}}(r,s)$ be the set of all $(s-1)$-arcs of $\vec{\mathrm{C}}(r,1)$. For every string h in $\mathbb{Z}_2$ of length $s-1$, and for any $\epsilon \in \mathbb{Z}_2$, we define the out-neighbours of $(x;\epsilon h) \in V\vec{\mathrm{C}}(r,s)$ to be $(x+1;h0)$ and $(x+1;h1)$. Hence, the *Praeger–Xu graph* $\mathrm{C}(r,s)$ is defined as the underlying graph of $\vec{\mathrm{C}}(r,s)$. Observe that $\mathrm{C}(r,s)$ is a connected 4-valent graph with $r2^s$ vertices (see [123, Theorem 2.8]).

Let us now discuss the automorphisms of the graphs $\mathrm{C}(r,s)$. Every automorphism of $\vec{\mathrm{C}}(r,1)$ (or $\mathrm{C}(r,1)$, respectively) acts naturally as an automorphism of $\vec{\mathrm{C}}(r,s)$ (or $\mathrm{C}(r,s)$, respectively) for every $s \geq 2$. For $i \in \mathbb{Z}_r$, let τ_i be the transposition on $V\vec{\mathrm{C}}(r,1)$ swapping the vertices $(i,0)$ and $(i,1)$ while fixing every other vertex. This is an automorphism of $\vec{\mathrm{C}}(r,1)$, and thus also of $\vec{\mathrm{C}}(r,s)$ for $s \geq 2$. We set

$$K := \langle \tau_i \mid i \in \mathbb{Z}_r \rangle,$$

and we observe that K is isomorphic to C_2^r. Furthermore, let ρ and σ be the permutations on $V\vec{\mathrm{C}}(r,1)$ defined by

$$(i,\epsilon)^\rho := (i+1,\epsilon) \quad \text{and} \quad (i,\epsilon)^\sigma := (-x,\epsilon).$$

Then ρ is an automorphism of $\vec{\mathrm{C}}(r,1)$ or order r, and σ is an involutory automorphism of $\mathrm{C}(r,1)$ (but not of $\vec{\mathrm{C}}(r,1)$). Observe that ρ cyclically permutes the generators of K, while σ is a permutation of such set of order 2. It follows that the group $\langle \rho,\sigma \rangle$ normalises K. We define

$$H := K \rtimes \langle \rho,\sigma \rangle \quad \text{and} \quad H^\dagger := K \rtimes \langle \rho \rangle.$$

Hence, for every $r \geq 3$ and $s \geq 1$,

$$C_2 \mathrm{wr} D_r \cong H \leq \mathrm{Aut}(\mathrm{C}(r,s)) \quad \text{and} \quad C_2 \mathrm{wr} C_r \cong H^\dagger \leq \mathrm{Aut}(\vec{\mathrm{C}}(r,s)).$$

Moreover, H (or $H^\dagger$, respectively) acts arc-transitively on $\mathrm{C}(r,s)$ (or $\vec{\mathrm{C}}(r,s)$, respectively) whenever $1 \leq s \leq r-1$. With three exceptions, the groups H and $H^\dagger$ are, in fact, the automorphism groups of $\mathrm{C}(r,s)$ and $\vec{\mathrm{C}}(r,s)$, respectively.

Lemma 2.2 ([58] Theorem 2.13, and [123] Theorem 2.8) · *The automorphism group of a directed Praeger–Xu graph is*

$$\mathrm{Aut}(\vec{\mathrm{C}}(r,s)) = H^\dagger .$$

If $r \neq 4$, the automorphism group of a Praeger–Xu graph is

$$\mathrm{Aut}(\mathrm{C}(r,s)) = H .$$

Moreover,

$$|\mathrm{Aut}(\mathrm{C}(4,1)) : H| = 9 ,$$
$$|\mathrm{Aut}(\mathrm{C}(4,2)) : H| = 3 ,$$
$$|\mathrm{Aut}(\mathrm{C}(4,3)) : H| = 2 .$$

We note that the peculiarity of $r = 4$ is given by the fact that $\mathrm{C}(4,1)$ is isomorphic to the complete bipartite graph on 8 vertices $\mathbf{K}_{4,4}$, while $\mathrm{C}(4,2)$ is the tesseract graph. We have not found $\mathrm{C}(4,3)$ elsewhere in the literature.

To conclude, we point out that the Praeger–Xu graphs also admit the following characterizations. We remark that Lemma 2.3 builds on the less general [123, Theorem 2.9] and [128, Theorem 1].

Lemma 2.3 ([112] Lemma 1.13) · *Let Γ be a finite connected 4-valent graph, and let G be a vertex- and edge-transitive group of automorphisms of Γ. Suppose that G has an abelian normal subgroup which is not semiregular on $V\Gamma$. Then Γ is isomorphic to a Praeger–Xu graph $\mathrm{C}(r,s)$, for some positive integers r and s.*

Lemma 2.4 ([112] Lemma 1.11) · *Let Γ be a finite connected 4-valent graph, let G be a vertex- and edge-transitive group of automorphisms of Γ, and let N be a minimal normal subgroup of G. If N is a 2-group and Γ/N is a cycle of length at least 3, then Γ is isomorphic to a Praeger–Xu graph $\mathrm{C}(r,s)$ for some positive integers $r \leq 3$ and $s \leq r-1$.*

2.B Cayleyness

In [74], R. Jajcay, P. Potočnik and S. Wilson gave a sufficient and necessary condition for a Praeger–Xu graph to be a Cayley graph. Explicitly, [74, Theorem 1.1] states that, for any positive integer $r \geq 3$, with $r \neq 4$, and for any positive integer $s \leq r-1$, the Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph if, and only if, one of the following holds

(*a*) the polynomial $t^r + 1$ has a divisor of degree $r-s$ in $\mathbb{Z}_2[t]$;

(*b*) r is even, and there exist polynomials $f_1, f_2, g_1, g_2, u, v \in \mathbb{Z}_2[t]$ such that u, v are palindromic of degree $r-s$, and

$$t^r + 1 = f_1(t^2)u(t) + tg_1(t^2)v(t) = f_2(t^2)v(t) + tg_2(t^2)u(t). \qquad (2.1)$$

Section 2.B strengthens this result. Following [14], our aim is to prove that (b) implies (a), thus obtaining the following refinement. We remark that it can be verified explicitly that $\mathrm{C}(4,1)$, $\mathrm{C}(4,2)$ and $\mathrm{C}(4,3)$ are Cayley graphs, hence we will ignore the case $r=4$ in the proof of Theorem C.

Theorem C · *For any positive integer $r \geq 3$ and for any positive integer $s \leq r-1$, the Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph if, and only if, the polynomial t^r+1 has a divisor of degree $r-s$ in $\mathbb{Z}_2[t]$.*

Proof. Suppose (b) holds. We aim to show that t^r+1 is divisible by a polynomial of degree $r-s$ in $\mathbb{Z}_2[t]$, implying (a). Working in characteristic 2, Equation (2.1) can be written as

$$t^r+1 = f_1^2(t)u(t)+tg_1^2(t)v(t) = f_2^2(t)v(t)+tg_2^2(t)u(t).$$

From here on, we drop the indeterminate t, and we write

$$t^r+1 = f_1^2u+tg_1^2v = f_2^2v+tg_2^2u. \tag{2.2}$$

If either g_1 or g_2 is the trivial polynomial, then the result follows from Equation (2.2) and the fact that u and v have degree $r-s$. Therefore, for the rest of the argument, we may suppose that g_1, g_2 are not trivial. Moreover, observe that neither f_1 nor f_2 is the trivial polynomials, because t does not divide t^r+1.

We introduce four polynomials $u_e, u_o, v_e, v_o \in \mathbb{Z}_2[t]$ such that

$$u := u_e^2+tu_o^2, \qquad v := v_e^2+tv_o^2.$$

Substituting these expansions for u and v in Equation (2.2), we get

$$\begin{aligned} t^r+1 &= f_1^2u_e^2+t^2g_1^2v_o^2+t(f_1^2u_o^2+g_1^2v_e^2),\\ t^r+1 &= f_2^2v_e^2+t^2g_2^2u_o^2+t(f_2^2v_o^2+g_2^2u_e^2). \end{aligned}$$

Recall that r is even. By splitting the equalities in even and odd degree terms, we obtain

$$\begin{aligned} t^r+1 &= f_1^2u_e^2+t^2g_1^2v_o^2, & 0 &= t(f_1^2u_o^2+g_1^2v_e^2),\\ t^r+1 &= f_2^2v_e^2+t^2g_2^2u_o^2, & 0 &= t(f_2^2v_o^2+g_2^2u_e^2). \end{aligned}$$

Set $m=r/2$. Since we are working in characteristic 2, we get

$$t^m+1 = f_1u_e+tg_1v_o, \qquad t^m+1 = f_2v_e+tg_2u_o, \tag{2.3}$$

$$f_1u_o = g_1v_e, \qquad f_2v_o = g_2u_e. \tag{2.4}$$

Since u and v are palindromic by assumption, we get $1 = u(0) = u_e(0)$ and $1 = v(0) = v_e(0)$. In particular both u_e and v_e are not zero. From Equation (2.3) and Equation (2.4), we obtain

$$\begin{aligned} f_1 &= \frac{t^m+1}{u_ev_e+tu_ov_o}v_e, & g_1 &= \frac{t^m+1}{u_ev_e+tu_ov_o}u_o,\\ f_2 &= \frac{t^m+1}{u_ev_e+tu_ov_o}u_e, & g_2 &= \frac{t^m+1}{u_ev_e+tu_ov_o}v_o. \end{aligned} \tag{2.5}$$

Our candidate for the required divisor of t^r+1 is $h = u_e v_e + t u_o v_o$. Let us show first that $\deg(h) = r - s$. Since $u_e v_e$ and $u_o v_o$ have even degree, we deduce

$$\deg(h) = \max\{\deg(u_e v_e), \deg(t u_o v_o)\}.$$

Recall $u = u_e^2 + t u_o^2$ and $v = v_e^2 + t v_o^2$. If $r-s$ is even, then

$$\deg(u_e) = \deg(v_e) = \frac{r-s}{2}, \quad \text{and} \quad \deg(u_o) = \deg(v_o) < \frac{r-s-1}{2}.$$

On the other hand, if $r-s$ is odd, then

$$\deg(u_e) = \deg(v_e) < \frac{r-s}{2}, \ \text{and} \ \deg(u_o) = \deg(v_o) = \frac{r-s-1}{2}.$$

Therefore, in both cases, $\deg(h) = r-s$.

It remains to prove that h divides t^r+1. Since f_1, g_1, f_2, g_2 are polynomials, by Equation (2.5), h divides

$$\gcd((t^m+1)v_e, (t^m+1)v_o, (t^m+1)u_e, (t^m+1)u_o) = (t^m+1)\gcd(v_e, v_o, u_e, u_o).$$

Observe that $\gcd(v_e, v_o, u_e, u_o)$ divides $f_1 u_e + t g_1 v_o$, hence, in view of the first equation in Equation (2.3), $\gcd(v_e, v_o, u_e, u_o)$ divides t^m+1. Therefore, h divides $(t^m+1)^2 = t^r+1$. ■

Using the factorization of t^r+1 in $\mathbb{Z}_2[t]$, we give a purely arithmetic condition for the Cayleyness of $\mathrm{C}(r,s)$. Let φ be the Euler's totient φ-function and, for every positive integer d, let

$$\omega(d) := \min\{c \in \mathbb{N} \mid d \text{ divides } 2^c - 1\}$$

be the multiplicative order of 2 modulo d.

Corollary D · *Let a be a non-negative integer, let b be an odd positive integer such that $r = 2^a b$, with $r \geq 3$, and let s be a positive integer with $s \leq r-1$. The Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph if, and only if, s can be written as*

$$s = \sum_{d \mid b} \alpha_d \omega(d), \quad \textit{for some integers} \quad \alpha_d \quad \textit{with} \quad 0 \leq \alpha_d \leq \frac{2^a \varphi(d)}{\omega(d)}. \tag{2.6}$$

Proof. By Theorem C, deciding if a Praeger–Xu graph $\mathrm{C}(r,s)$ is a Cayley graph is tantamount to deciding if t^r+1 admits a divisor of order s in $\mathbb{Z}_2[t]$. An immediate way to proceed is to study how t^r+1 can be factorized in irreducible polynomials.

Let $r = 2^a b$, with $\gcd(2,b) = 1$. Since we are in characteristic 2 we have

$$t^r + 1 = t^{2^a b} + 1 = \left(t^b + 1\right)^{2^a}.$$

Furthermore, if $\lambda_d(t) \in \mathbb{Z}[t]$ denotes the d-th cyclotomic polynomial, then

$$t^b + 1 = \prod_{d \mid b} \lambda_d(t)$$

is the factorization of t^b+1 in irreducible polynomials over $\mathbb{Q}[t]$, by Gauss's theorem. Since the Galois group of any field extension of $\mathbb{Z}_2$ is a cyclic group generated by the Frobenius automorphism, the degree of an irreducible factor of $\lambda_d(t)$ in $\mathbb{Z}_2[t]$ is the smallest c such that a d-th primitive root ζ elevated to 2^c is ζ, that is, $\omega(d)$. Hence $\lambda_d(t)$ in $\mathbb{Z}_2[t]$ factorizes into $\varphi(d)/\omega(d)$ irreducible polynomials, each having degree $\omega(d)$.

Therefore, $t^r+1\in\mathbb{Z}_2[t]$ has a divisor of degree s if, and only if, s can be written as the sum of some $\omega(d)$'s, each summand repeated at most $2^a\varphi(d)/\omega(d)$ times, which is exactly Equation (2.6). ■

2.C Splitting and merging

To introduce the split Praeger–Xu graphs and analyse their properties, we need first to focus on the splitting operation and its converse, the merging operation. Section 2.C is devoted to the study of these constructions.

The operation of *splitting* was introduced in [115, Construction 11]. Let Δ be a 4-valent graph, let $\mathcal{C}$ be a partition of $E\Delta$ into cycles. By applying the splitting operation to the pair $(\Delta,\mathcal{C})$, we obtain the graph, denoted by $\mathrm{s}(\Delta,\mathcal{C})$, whose vertices are

$$V\mathrm{s}(\Delta,\mathcal{C}) := \{(\alpha,C)\in V\Delta\times\mathcal{C} \mid \alpha\in VC\},$$

and such that two vertices (α,C) and (β,D) are declared adjacent if either $C\neq D$ and $\alpha=\beta$, or $C=D$ and α and β are adjacent in Δ. Morally, this operation separates with a new edge the two cycles of $\mathcal{C}$ passing through α, and this explains its name.

Observe that, since Δ is 4-valent, there are precisely 2 cycles in $\mathcal{C}$ passing through α, thus $\mathrm{s}(\Delta,\mathcal{C})$ is 3-valent and

$$|V\mathrm{s}(\Delta,\mathcal{C})| = 2|V\Delta|.$$

Note that, for every $G\leq\mathrm{Aut}(\Delta)$ such that G fixes the edge-partition $\mathcal{C}$ setwise,

$$G \quad \text{is a subgroup of} \quad \mathrm{Aut}(\mathrm{s}(\Delta,\mathcal{C})).$$

Moreover, if G is also arc-transitive on Δ, then G can swap the two cycles passing through each vertex, thus it is vertex-transitive on $\mathrm{s}(\Delta,\mathcal{C})$. Observe that, the fact that $\mathcal{C}$ is G-invariant forces the action of G_α on the neighbourhood of α to be either the Klein four group, or the cyclic group of order 4, or the dihedral group of order 8, because these are the only imprimitive permutation groups of degree 4. For any vertex $(\alpha,C)\in\mathrm{s}(\Delta,\mathcal{C})$,

$$G_{(\alpha,C)} = G_\alpha\cap G_{\{C\}},$$

where $G_{\{C\}}$ is the setwise stabilizer of the cycle C. In particular, whenever G is arc-transitive on Δ, as G_α switches the two cycles passing through α,

$$|G_\alpha : G_{(\alpha,C)}| = 2.$$

Now, we introduce the tentative inverse of the splitting operator: the operation of *merging* (see [115, Construction 7]). Before, we need to recall two graph-theoretical definitions. For a graph Γ, a *perfect matching* is a subgraph of Γ containing all the vertices of Γ such that any two edges of the perfect matching are disjoint, while a 2-*factor* is a subgraph of Γ containing all the vertices of Γ such that all its connected components are cycles.

Let Γ be a connected 3-valent graph, and let G be a vertex-transitive group of automorphisms such that the action of G_α on the neighbourhood of α is cyclic of order 2. In particular, G_α is a nontrivial 2-group. Hence, G_α fixes a unique neighbour of α, which we denote by α'. It follows that $(\alpha')' = \alpha$ and $G_\alpha = G_{\alpha'}$. Thus, the set

$$\mathcal{M} := \{\{\alpha, \alpha'\} \mid \alpha \in V\Gamma\}$$

is a perfect matching of Γ, while the edges outside $\mathcal{M}$ form a 2-factor, which we denote by $\mathcal{F}$. The group G in its action on $E\Gamma$ fixes setwise both $\mathcal{F}$ and $\mathcal{M}$, and acts transitively on the arcs of each of these two sets. Let Δ be the graph with vertex-set $\mathcal{M}$ and two vertices $e_1, e_2 \in \mathcal{M}$ are declared adjacent if they are (as edges of Γ) at distance 1 in Γ. We may also think of Δ as being obtained by contracting all the edges in $\mathcal{M}$. Let $\mathcal{C}$ be the decomposition of $E\Delta$ into cycles given by the connected components of the 2-factor $\mathcal{F}$. The merging operation applied to the pair (Γ, G) gives as a result the pair $(\Delta, \mathcal{C})$.

The merging operation generates 4-valent graphs outside some pathological cases. Indeed, only two infinite families of 3-valent graph have *degenerate* merged graphs. These are the circular and Möbius ladders. For any $n \geq 3$, a *circular ladder graph* is a graph isomorphic to the Cayley graph

$$\mathrm{Cay}(\mathbb{Z}_n \times \mathbb{Z}_2, \{(0,1), (1,0), (-1,0)\}),$$

and, for any $n \geq 2$, a *Möbius ladder graph* is a graph isomorphic to the Cayley graph

$$\mathrm{Cay}(\mathbb{Z}_{2n}, \{1, -1, n\}).$$

Observe that we consider the complete graph on 4 vertices to be a Möbius ladder graph.

Remark 2.5 · Let Γ be a connected 3-valent graph that is neither a circular nor a Möbius ladder, and let G be a vertex-transitive group of automorphisms of Γ such that the action of G_α on the neighbourhood of α is cyclic of order 2. Then [115, Lemma 9 and Theorem 10] imply that the merging operator applied to the pair (Γ, G) gives a pair $(\Delta, \mathcal{C})$ such that Δ is 4-valent, the action of G on Δ is faithful and arc-transitive, and $\mathcal{C}$ is G-invariant. This result motivates the use of the word *degenerate* when referring to the circular and Möbius ladders.

We state here an auxiliary lemma that we will need in the following to deal with the ladders.

Lemma 2.6 · *Unless Λ is isomorphic to the skeleton of the cube or the complete graph on 4 vertices, the automorphism group of a (circular or Möbius) ladder Λ contains $N \leq \mathrm{Aut}(\Lambda)$, a normal cyclic subgroup of order 2, such that the normal quotient Λ/N is a cycle.*

Proof. Suppose that Λ is a circular ladder, and its vertex-set is $\mathbb{Z}_n \times \mathbb{Z}_2$, where $n \geq 3$ is an integer. Note that the subgraphs induced by $\mathbb{Z}_n \times \{0\}$ and $\mathbb{Z}_n \times \{1\}$ are two cycles of length n, which form an $\mathrm{Aut}(\Lambda)$-invariant 2-factor. The map

$$g : \Lambda \to \Lambda, \quad (x, \epsilon) \mapsto (x, \epsilon + 1)$$

is a central involution in $\mathrm{Aut}(\Lambda)$ that swaps $\mathbb{Z}_n \times \{0\}$ and $\mathbb{Z}_n \times \{1\}$. Hence, $N = \langle g \rangle$ is the desired normal subgroup.

Suppose now that Λ is a Möbius ladder, thus its vertices are the elements of $\mathbb{Z}_2 n$, for some integer $n \geq 2$. Similarly, if $n \neq 2$,

$$g : \Lambda \to \Lambda, \quad x \mapsto x + n$$

is a central involution of $\mathrm{Aut}(\Lambda)$. In this case, $N = \langle g \rangle$ defines n orbits of the form $\{x, x+n\}$. Thus Λ/N is a cycle of length n, as requested. ■

In view of [115, Theorem 12], the merging operator is the right-inverse of the splitting one, or, more explicitly, unless Γ is a (circular or Möbius) ladder, splitting a pair $(\Delta, \mathcal{C})$ obtained via the merging operation on (Γ, G) results in the starting pair. For our purposes, we need to show that the merging operator is also the left-inverse of the splitting one.

Theorem E · *Let Δ be a 4-valent graph, let $\mathcal{C}$ be a partition of $E\Delta$ into cycles, and let G be an arc-transitive group of automorphisms of Δ such that $\mathcal{C}$ is G-invariant. Then the merging operation can be applied to the pair $(\mathrm{s}(\Delta, \mathcal{C}), G)$ and it gives as a result $(\Delta, \mathcal{C})$.*

Proof. Let (α, C) be a vertex of $\mathrm{s}(\Delta, \mathcal{C})$, let $D \in \mathcal{C}$ be the other cycle of the partition passing through α, and let $\beta, \gamma \in V\Delta$ be the neighbours of α in C. Then, using the arc-transitivity of G,

$$(\alpha, D)^{G_{(\alpha,C)}} = \{(\alpha, D)\} \quad \text{and} \quad (\beta, C)^{G_{(\alpha,C)}} = (\gamma, C)^{G_{(\alpha,C)}} = \{(\beta, C), (\gamma, C)\}.$$

Therefore, for any vertex $(\alpha, C) \in V\mathrm{s}(\Delta, \mathcal{C})$, $G_{(\alpha,C)}$ acts on the neighbourhood of (α, C) as a cyclic group of order 2. Hence, we can apply the merging operation to the pair $(\mathrm{s}(\Delta, \mathcal{C}), G)$. Furthermore, we deduce that

$$\mathcal{M} = \{\{(\alpha, C), (\alpha, D)\} \mid \alpha \in VC \cap VD\}$$

is a perfect matching for $(\mathrm{s}(\Delta, \mathcal{C}), G)$. Thus the connected components of the resulting 2-factor $\mathcal{F} = E\mathrm{s}(\Delta, \mathcal{C}) - \mathcal{M}$ can be identified with the cycles of $\mathcal{C}$. Now, consider the map defined as

$$\theta : \mathcal{M} \to V\Delta, \quad \{(\alpha, C), (\alpha, D)\} \mapsto \alpha.$$

Since a generic vertex $\alpha \in V\Delta$ belongs to precisely two distinct cycles, θ is bijective. Moreover, β is adjacent to α in Δ if, and only if, either $\{(\alpha, C), (\beta, C)\}$ or $\{(\alpha, D), (\beta, D)\}$ is an edge in $\mathrm{s}(\Delta, \mathcal{C})$. In particular, θ also induces the bijection

$$\widehat{\theta} : \mathcal{F} \to E\Delta, \quad \{(\alpha, C), (\beta, C)\} \mapsto \{\alpha, \beta\},$$

which sends the connected components of $\mathcal{F}$ into disjoint cycles of $\mathcal{C}$. This shows that θ is a graph isomorphism between Δ and the 4-valent graph obtained by merging the pair $(\mathrm{s}(\Delta, \mathcal{C}), G)$. ■

Corollary 2.7 · *Let Δ be a 4-valent graph, let $\mathcal{C}$ be a partition of $E\Delta$ into cycles, and let G be an arc-transitive group of automorphisms of Δ such that $\mathcal{C}$ is G-invariant, thus $G \leq \mathrm{Aut}(\mathrm{s}(\Delta,\mathcal{C}))$. Suppose that $G \leq A \leq \mathrm{Aut}(\mathrm{s}(\Delta,\mathcal{C}))$ is a vertex-transitive group such that, for any vertex $\alpha \in V\mathrm{s}(\Delta,\mathcal{C})$, the action of A_α on the neighbourhood of α is cyclic of order 2, then $A \leq \mathrm{Aut}(\Delta)$.*

Proof. Note that, as G is a subgroup of A, the actions of G and A on the neighbourhood of any vertex α coincide. In particular, applying the merging operation to the pair $(\mathrm{s}(\Delta,\mathcal{C}),A)$ yields the same result as doing it on the pair $(\mathrm{s}(\Delta,\mathcal{C}),G)$, that is, by Theorem E, in both cases we obtain $(\Delta,\mathcal{C})$. The result follows by Remark 2.5. ∎

2.D Split Praeger–Xu graphs

Finally, we have all the tools to define the infinite family of split Praeger–Xu graphs.

All the partitions of the edge set of a Praeger–Xu graph into disjoint cycles were classified in [73, Section 6]. Regardless of the choice of the parameters r and s, there exists a decomposition into disjoint cycles of length 4 of the form

$$(x;0h) \sim (x+1;h0) \sim (x;1h) \sim (x+1;h1)$$

for some $x \in \mathbb{Z}_r$, and for some string h in $\mathbb{Z}_2$ of length $s-1$. We denote this partition by $\mathcal{S}$.

Definition 2.8 · The *split Praeger–Xu graph* $\mathrm{sC}(r,s)$ is the 3-valent graph obtained from the pair $(\mathrm{C}(r,s),\mathcal{S})$ by applying the splitting operation.

Recall that, by Lemma 2.2, the automorphism group of $\mathrm{C}(r,s)$ is of the form (or contains as a subgroup if $r=4$) $H = K \rtimes D_{2r}$, where K is the elementary abelian 2-group generated by the automorphisms τ_x that swaps the vertices $(x;0h)$ and $(x;1h)$ while fixing all the others. Observe that the only two neighbours of $(x;0h)$ in the K-orbit containing $(x+1;h0)$ are $(x+1;h1)$ and $(x+1;h0)$ itself, and similarly the only two neighbours of $(x+1;h0)$ in the K-orbit containing $(x;0h)$ are $(x;1h)$ and $(x;0h)$ itself. Therefore, $\mathcal{S}$ is the unique decomposition such that each cycle intersects exactly two K-orbits.

Lemma 2.9 · *For every positive integers $r \geq 3$ and $s \leq r-1$, the automorphism group of the split Praeger–Xu graph is*

$$\mathrm{Aut}(\mathrm{sC}(r,s)) = H,$$

and it acts transitively on $V\mathrm{sC}(r,s)$.

Proof. Note that H acts on the set of K-orbits in $V\mathrm{C}(r,s)$, thus each automorphism of H maps any cycle of $\mathcal{S}$ to a cycle intersecting exactly two K-orbits, that is, to an element of $\mathcal{S}$. Thus, $\mathcal{S}$ is H-invariant, and

$$H \leq \mathrm{Aut}(\mathrm{sC}(r,s)).$$

We now show the opposite inclusion. Let $\alpha \in V\mathrm{sC}(r,s)$ be a vertex, aiming for a contradiction we suppose that $\mathrm{Aut}(\mathrm{sC}(r,s))_\alpha$ does not act on the neighbourhood of α as a cycle of order 2. Let α', β, γ be the neighbours of α where α' is fixed by the action of H_α, and let δ be the unique vertex at distance 1 from both β and γ. Since

$$H_\alpha \leq \mathrm{Aut}(\mathrm{sC}(r,s))_\alpha\,,$$

our hypothesis implies that

$$\text{there is an element} \quad g \in \mathrm{Aut}(\mathrm{sC}(r,s))_\alpha \quad \text{such that} \quad \beta^g = \alpha' \quad \text{and} \quad \gamma^g = \gamma\,.$$

This yields a contradiction because δ^g is ill-defined: in fact there is no vertex of $\mathrm{sC}(r,s)$ at distance 1 from both γ^g and δ^g. Recall that, from Lemma 2.2, if $r \neq 4$, then $H = \mathrm{Aut}(\mathrm{C}(r,s))$, and so, by Corollary 2.7,

$$\mathrm{Aut}(\mathrm{sC}(r,s)) \leq H\,.$$

On the other hand, if $r = 4$, observe that H is vertex-transitive on $\mathrm{sC}(r,s)$ and $\mathrm{Aut}(\mathrm{sC}(r,s))_\alpha = H_\alpha$, hence the equality holds by Frattini's argument. ■

To conclude Section 2.D, we show two results mimicking the characterization of Praeger–Xu graphs. The first is an adaptation of Lemma 2.4 for 3-valent graphs.

Lemma 2.10 · *Let Γ be a connected 3-valent vertex-transitive graph, let $G \leq \mathrm{Aut}(\Gamma)$ be a vertex-transitive group such that the action of G_α on the neighbourhood of α is cyclic of order 2, and let N be a minimal normal subgroup of G. If N is a 2-group and Γ/N is a cycle of length at least 3, then Γ is isomorphic either to a circular ladder, or to a Möbius ladder, or to $\mathrm{sC}(r,s)$, for some positive integers $r \geq 3$ and $s \leq r-1$.*

Proof. We already know by Lemma 2.6 that both ladders admit a cyclic quotient graph, thus we can suppose that Γ is not isomorphic to a circular ladder or to a Möbius ladder. By hypothesis, we can apply the merging operator to (Γ, G), obtaining the pair $(\Delta, \mathcal{C})$. Since we have excluded the possibility of Γ being a ladder, by Remark 2.5, Δ is 4-valent, and the action of G on Δ is faithful and arc-transitive, and it fixes $\mathcal{C}$ setwise. Since the action of N cannot map edges in $\mathcal{M}$ to edges in $\mathcal{F}$, the quotient graph Γ/N retains a partition into two disjoint sets of edges, namely $\mathcal{M}/N$ and $\mathcal{F}/N$. Moreover, since $\mathcal{M}$ is a perfect matching, each edge in $\mathcal{M}/N$ is adjacent to precisely two edges in $\mathcal{F}/N$, and vice versa. This implies that the edges of Δ/N coincide with the elements of $\mathcal{F}/N$, two of which are adjacent if they share the same neighbour in $\mathcal{M}/N$. If $r \geq 6$, then Δ/N is a cycle of length $r/2$. From Lemma 2.4, we deduce that Δ is isomorphic to $\mathrm{C}(r,s)$, for some positive integers $r \geq 3$ and $s \leq r-1$. Observe that, as $\mathcal{C}$ coincides with the connected components of $\mathcal{F}$, each cycle in $\mathcal{C}$ intersects precisely two K-orbits. This implies that $\mathcal{C} = \mathcal{S}$, and so [115, Theorem 12] yields that Γ is isomorphic to

$$\mathrm{s}(\Delta, \mathcal{C}) = \mathrm{s}(\mathrm{C}(r,s), \mathcal{S}) = \mathrm{sC}(r,s)\,.$$

Now, suppose that $r = 4$. In this case, we have that G is a 2-group, hence $|N| = 2$ and $|V\Gamma| = 8$, and so the only possibility is for Γ to be a (circular or Möbius) ladder, which we already excluded. ■

The second result is the analogue of [112, Lemma 1.13] for 3-valent graphs.

Lemma 2.11 · *Let Γ be a connected 3-valent graph, let α be a vertex of Γ, let G be a vertex-transitive subgroup of* $\mathrm{Aut}(\Gamma)$, *and let N be a semiregular normal subgroup of G. Suppose that the local group of the pair (Γ, G) is isomorphic to C_2, and that the normal quotient Γ/N is a cycle of length $r \geq 3$. Denote by K the kernel of the action of G on the N-orbits on $V\Gamma$. Then*

(*a*) *either G_α has order 2 and K_α is trivial;*

(*b*) *or r is even and $G_\alpha = K_\alpha$ is an elementary abelian 2-group of order at most $2^{r/2}$.*

Proof. Let

$$\Delta_0, \quad \Delta_1, \quad \ldots, \quad \Delta_{r-1}$$

be the orbits of N in its action on $V\Gamma$. Since Γ/N is a cycle, we may assume that Δ_i is adjacent to Δ_{i-1} and Δ_{i+1} with indices computed modulo r. Moreover, without loss of generality, we suppose that $\alpha \in \Delta_0$.

As the local group is a nontrivial 2-group, by Lemma 1.32, G_α is a 2-group. Furthermore, by assumption, G_α fixes a unique neighbour of α. As usual, for each $\beta \in V\Gamma$, let β' be the unique neighbour of β fixed by G_β.

Suppose that $\{\alpha, \alpha'\}$ is contained in an N-orbit. Since $\alpha \in \Delta_0$, we deduce $\alpha' \in \Delta_0$. Let β and γ be the other two neighbours of α. As Γ/N is a cycle of length $r \geq 3$, we have $\beta \in \Delta_1$ and $\gamma \in \Delta_{r-1}$. Since $\mathrm{Aut}(\Gamma/N)$ is a dihedral group of order $2r$ and since G_α contains an element swapping β and γ, we deduce that $|G_\alpha : K_\alpha| = 2$. Observe that K_α fixes by definition each N-orbit and hence it fixes setwise Δ_1 and Δ_{r-1}. Therefore, K_α fixes β and γ, because β is the unique neighbour of α in Δ_1 and γ is the unique neighbour of α in Δ_{r-1}. This shows that K_α fixes pointwise the neighbourhood of α. Thus, Lemma 1.32 implies that K_α is trival. In particular, Lemma 2.11 (*a*) is satisfied.

For the rest of the argument, we suppose that $\{\alpha, \alpha'\}$ is not contained in an N-orbit. This means that α has two neighbours in an N-orbit, say Δ_1, and only one neighbour in the other N-orbit, say Δ_{r-1}. (Thus $\alpha' \in \Delta_{r-1}$ and $\beta, \gamma \in \Delta_1$.) This implies that r is even and, for every $i \in \{0, \ldots, r/2-1\}$, each vertex in Δ_{2i} has two neighbours in Δ_{2i+1} and only one neighbour in Δ_{2i-1}. Therefore, G/K is a dihedral group of order r when $r \geq 8$ and G/K is elementary abelian of order 4 when $r = 4$. Moreover, G/K acts regularly on Γ/N and hence $G_\alpha = K_\alpha$.

It remains to show that K_α is an elementary abelian 2-group of order at most $2^{r/2}$. Since N is normal in G, the orbits of N on the edge-set $E\Gamma$ form a G-invariant partition of $E\Gamma$.

We claim that, no two edges incident to a fixed vertex of Γ belong to the same N-edge-orbit. We argue by contradiction, and we suppose that α has two distinct neighbours β and γ such that the edges $\{\alpha, \beta\}$ and $\{\alpha, \gamma\}$ are in the same N-edge-orbit. In particular, there exists $n \in N$ with $\{\alpha, \beta\}^n = \{\alpha, \gamma\}$. This gives $\alpha^n = \alpha$ and $\beta^n = \gamma$, or $\alpha^n = \gamma$ and $\beta^n = \alpha$. Since there are no edges inside an N-orbit, we cannot have $\alpha^n = \gamma$ and $\beta^n = \alpha$. Therefore, $\alpha^n = \alpha$ and $\beta^n = \gamma$. Since N acts semiregularly on $V\Gamma$, we have $n = 1$ and hence $\beta = \beta^n = \gamma$, which is a contradiction.

Since G is vertex-transitive, the edges between Δ_{2i} and Δ_{2i+1} are partitioned into precisely two N-edge-orbits (let us call these two orbits Θ_{2i} and Θ'_{2i}), whereas the edges between Δ_{2i} and Δ_{2i-1} form one N-edge-orbit (which we call Θ''_{2i}).

An element of K (fixing setwise the sets Δ_{2i} and Δ_{2i+1}) can map an edge in Θ_{2i} only to an edge in Θ_{2i} or to an edge in Θ'_{2i}. On the other hand, as G_α is not the identity group, for every vertex $\beta \in \Delta_{2i}$ there is an element $g \in G_\beta$ which maps an edge of Θ_{2i} incident to β to the edge of Θ'_{2i} incident to β. This element g is clearly an element of K, because G/K acts semiregularly on Γ/N. This shows that the orbits of K on $E\Gamma$ are precisely the sets $\Theta_{2i} \cup \Theta'_{2i}, \Theta''_{2i}$, $i \in \{0,\dots,r/2-1\}$. In other words, each orbit of the induced action of K on the set

$$E\Gamma/N = \{e^N \mid e \in E\Gamma\}$$

has length at most 2. Consequently, if X denotes the kernel of the action of K on $E\Gamma/N$, then K/X embeds into $\mathrm{Sym}(2)^{r/2}$ and is therefore an elementary abelian 2- group of order at most $2^{r/2}$.

Let us now show, via a connectedness argument, that $X = N$. By definition, N is a subgroup of X. Let $\delta \in \Delta_0$. Since N is transitive on Δ_0, it follows that $X = NX_\delta$. Suppose that X_δ is nontrivial and let g be a nontrivial element of X_δ. Further, let δ' be a vertex which is closest to δ among all the vertices not fixed by g, and let

$$\delta = \delta_0 \sim \delta_1 \sim \dots \sim \delta_m = \delta'$$

be a path of minimal length from δ to δ'. Then δ_{m-1} is fixed by g. Since g fixes each N-edge-orbit setwise and since every vertex of Γ is incident to at most one edge in each N-edge-orbit, it follows that g fixes all the neighbours of δ_{m-1}, thus also $\delta_m = \delta'$. This contradicts our assumptions and proves that X_δ is a trivial group, and hence that $X = N$. This proves that Lemma 2.11 (b) holds. ■

2.E Fixed point ratios

In Section 2.E, we review how P. Potočnik and P. Spiga in [112] have studied the fixed point ratio for graphs of small valencies. We postpone their results for now, and we instead focus on the ingredients needed to achieve them.

As usual in this setting, the main obstruction has arisen when the vertex-stabilizers were 2-groups. Hence, Praeger–Xu and split Praeger–Xu graphs come into play. We start with two preliminary group-theoretic results: the first one significantly shortens the proof, while the second one is the cornerstone of the inductive argument. We recall that $\mathbf{O}_2(G)$ denotes the maximal normal 2-subgroup of G.

Theorem 2.12 ([111] Theorem 1.1) · *Let G be a transitive permutation group on Ω such that $\mathbf{O}_2(G)$ is trivial, and let $\omega \in \Omega$ be a point with G_ω 2-group. Then*

$$|\{\alpha \in \Omega \mid \alpha^g = \alpha\}| \le \frac{|\Omega|}{3}, \quad \textit{for every} \quad g \in G - \{1\}.$$

Lemma 2.13 ([112] Lemma 1.17) · *Let G be a group acting transitively on Ω and let Σ be a system of blocks of imprimitivity. For $g \in G$, let g^{Σ} be the permutation of Σ induced by g. Then*

$$\mathrm{fpr}(g) \leq \mathrm{fpr}\left(g^{\Sigma}\right).$$

In particular, if N is a normal subgroup of G, then

$$\mathrm{fpr}(g) \leq \mathrm{fpr}(Ng).$$

Proof. Let us denote by $\mathrm{Fix}(g,\Omega)$ the set of points in Ω fixed by g, and by $\mathrm{Fix}(g^{\Sigma},\Sigma)$ the set of fixed blocks in Σ. We note that, if $\alpha \in \mathrm{Fix}(g,\Omega)$, and if we denote by A the block containg α, then, $A \in \mathrm{Fix}(g^{\Sigma},\Sigma)$, because $\alpha \in A \cap A^{g}$. Hence,

$$\mathrm{Fix}(g,\Omega) = \sum_{B \in \mathrm{Fix}(g^{\Sigma},\Sigma)} |B \cap \mathrm{Fix}(g,\Omega)| \leq b|\mathrm{Fix}(g^{\Sigma},\Sigma)|, \tag{2.7}$$

where b is the size of an arbitrary block of Σ. Observe that, by transitivity of G, $b|\Sigma| = |\Omega|$. Therefore, the first proportion of the statement is obtained by dividing both sides of Equation (2.7) by $|\Omega|$. The proof is complete by recalling that the orbits of a normal subgroup are a G-invariant partition of Ω. ■

Let Γ be a connected 4-valent graph, and let G be a vertex- and edge-transitive group of automorphisms of Γ with $\mathrm{fpr}(G) \geq 1/3$. Note that, by Lemma 2.13, if N is a semiregular normal subgroup of G, then $\mathrm{fpr}(G) \leq \mathrm{fpr}(G/N)$. This allows an inductive approach on the number of vertices by considering subsequent normal quotients.

Suppose that Γ is not 2-arc-transitive, that is, in view of Lemma 1.32, the stabilizer of a vertex is a 2-group. Aiming for a contradiction, suppose that Γ is not a Praeger–Xu graph, and, among the graphs with these properties, it is minimal with respect to the number of vertices. We have that $\mathbf{O}_2(G)$ is either trivial or not. In the former case, by Theorem 2.12, $\mathrm{fpr}(G) \leq 1/3$, which goes against our hypothesis. Hence, we must assume that there is a minimal normal subgroup N of G which is an elementary abelian 2-group. If N is not semiregular, by Lemma 2.3, Γ is isomorphic to a Praeger–Xu graph. Thus, we are left to deal with the case that N is semiregular. If N defines one orbit, then Γ is a Cayley graph of an elementary abelian 2-group with at most 4 generators, hence $|V\Gamma| \leq 2^4$. A similar argument work if N defines two orbits, and we find that $|V\Gamma| \leq 2^7$ (see [112, Lemma 1.15]). In both cases, a direct inspection of the census of 4-valent vertex- and edge-transitive graphs (see, for instance, [118]) shows that such a counterexample does not exist. Therefore, N defines at least three orbits. Since $\mathrm{fpr}(G) \leq \mathrm{fpr}(G/N)$, the minimality of Γ with respect to $|V\Gamma|$ implies that Γ/N is either a cycle or a Praeger–Xu graph. In the former scenario, Lemma 2.4 forces Γ to be a Praeger–Xu graph. In the latter scenario, some careful considerations on the nature of the elementary abelian covers of a Praeger–Xu graph show that Γ must be, once again, a Praeger–Xu graph. We refer the reader who is interested in abelian covers of graphs to [97]. To sum up, in all the possible scenarios, we can prove that Γ is a Praeger–Xu graph, a contradiction.

On the other hand, if Γ is 2-arc-transitive, then the local group is graph-restrictive by Theorem 1.36, thus the size of a vertex-stabilizer is bounded from above by a constant. The proof is then reduced to an examination of the scenarios where G is an almost simple group. In this case, 6 sporadic graphs with high fixed point ratio appear.

Ψ_1 The first graph is the complete graph on 5 vertices $\mathbf{K}_5$, whose automorphism group is $\mathrm{Sym}(5)$. A permutation $g \in \mathrm{Sym}(5)$ fixing 2 or 3 points gives rise to a nonidentity automorphism with $\mathrm{fpr}(g) \geq 2/5$.

Ψ_2 The second graph is the complete bipartite graph on 10 vertices minus a perfect matching, $\mathbf{K}_{5,5} - 5\mathbf{K}_2$, whose automorphism group is $\mathrm{Sym}(5) \times C_2$. A permutation of $\mathrm{Sym}(5)$ fixing 2 or 3 points gives rise to a nonidentity automorphism fixing 4 or 6 vertices, thus $\mathrm{fpr}(g) \geq 2/5$.

Ψ_3 The third graph is the *bipartite complement of the Heawood graph* $\mathfrak{H}$: its vertices are the 7 points and the 7 lines of the Fano plane $\mathrm{PG}_2(2)$, and a pair of vertices (p, L) are connected if p is a point, L is a line and $p \notin L$. The automorphism group of the bipartite complement of the Heawood graph is isomorphic to the automorphism group of the Fano plane, $\mathrm{Aut}(\mathrm{PGL}_3(2))$. An involution $g \in \mathrm{PGL}_3(2)$ gives rise to a nonidentity automorphism fixing 6 vertices, hence $\mathrm{fpr}(g) = 3/7$.

Ψ_4 The fourth graph also arises from an incidence structure. Its vertices are the 13 points and the 13 lines of $\mathrm{PG}_2(3)$, and a pair of vertices (p, L) are connected if p is a point, L is a line and $p \in L$. The automorphism group of this graph is isomorphic to $\mathrm{Aut}(\mathrm{PGL}_3(3))$. An involution $g \in \mathrm{Aut}(\mathrm{PGL}_3(3))$ gives rise to a nontrivial automorphism fixing 10, hence $\mathrm{fpr}(g) = 10/23$.

Ψ_5 The fifth graph is the Kneser graph of parameter $(7, 3)$. The vertices correspond to the 35 3-subsets of $\{1, 2, \ldots, 7\}$, two of which are declared adjacent if they have trivial intersection. Its automorphism group is isomorphic to $\mathrm{Sym}(7)$, and a transposition g fixes 15 vertices, hence $\mathrm{fpr}(g) = 3/7$.

Ψ_6 The last graph is the regular double cover of the graph in Ψ_5. Its automorphism group is isomorphic to $\mathrm{Sym}(7) \times C_2$, and a noncentral transposition g fixes 30 vertices, hence $\mathrm{fpr}(g) = 3/7$.

Once all ingredients are thoroughly mixed, we obtain the following result.

Theorem 2.14 ([112] Theorem 1.1) · *Let Γ be a connected vertex- and edge-transitive 4-valent graph admitting a nonidentity automorphism fixing more than 1/3 of the vertices. Then Γ is arc-transitive and one of the following holds:*

(*a*) $|V\Gamma| \leq 70$, *and Γ is one of the six exceptions in $\Psi_1, \ldots, \Psi_6$;*

(*b*) *Γ is isomorphic to a Praeger–Xu graph* $\mathrm{C}(r, s)$ *with* $1 \leq s < 2r/3$ *and* $r \geq 3$.

The proof of Theorem 2.14 can be translated to valency 3. Let Γ be a connected 3-valent graph, and let G be a vertex-transitive group of automorphisms of Γ with $\mathrm{fpr}(G) \geq 1/3$. Once again, we can argue by induction on the number of vertices by taking subsequent normal quotients.

Suppose that the local group of (Γ, G) is isomorphic to the cyclic group of order 2. By applying the splitting operation, we observe that

$$\mathrm{fpr}(g, V\Gamma) \geq \mathrm{fpr}(g, V\mathrm{s}\Gamma) > \frac{1}{3}.$$

Therefore, in view of Theorem 2.14 and Remark 2.5, Γ can either be a split Praeger–Xu graph, or a circular ladder, or a Möbius ladder. All these cases are easily dealt with by direct inspection.

In view of Theorem 1.24, the case with transitive local group can be treated in the same way as the 2-arc-transitive case for valency 3. Chance decided that also in this case 6 sporadic examples appear. We remark that Φ_1 and Φ_3 are a Möbius and circular ladder respectively, so they already appeared in the previous case.

- Φ_1 The first graph is the complete graph on 4 vertices $\mathbf{K}_4$, whose automorphism group is $\mathrm{Sym}(4)$. A transposition $g \in \mathrm{Sym}(4)$ gives rise to a nonidentity automorphism with $\mathrm{fpr}(g) = 1/2$.
- Φ_2 The second graph is the *utility graph* $\mathbf{K}_{3,3}$, whose automorphism group is $\mathrm{Sym}(3) \,\mathrm{wr}\, \mathrm{Sym}(2)$. A transposition g from the base group fixes 4 vertices, hence $\mathrm{fpr}(g) = 2/3$.
- Φ_3 The third graph is the 1-skeleton of the 3-cube $\mathbf{Q}_8$, whose automorphism group is $\mathrm{Sym}(2) \,\mathrm{wr}\, \mathrm{Sym}(3) = \mathrm{Sym}(4) \times \mathrm{Sym}(2)$. A transposition $g \in \mathrm{Sym}(4)$ gives rise to a nonidentity automorphism fixing 4 vertices, hence $\mathrm{fpr}(g) = 1/2$.
- Φ_4 The fourth graph is the *Petersen graph*, whose automorphism group is $\mathrm{Sym}(5)$. A transposition $g \in \mathrm{Sym}(5)$ fixes 4 vertices, hence $\mathrm{fpr}(g) = 2/5$.
- Φ_5 The fifth graph is the *Heawood graph*, whose automorphism group is isomorphic to $\mathrm{Aut}(\mathrm{PGL}_3(2))$. An involution $g \in \mathrm{PGL}_3(2)$ gives rise to a nonidentity automorphism fixing 6 vertices, hence $\mathrm{fpr}(g) = 3/7$.
- Φ_6 The last graph is the regular double cover of the Petersen graph. Its automorphism group is isomorphic to $\mathrm{Sym}(5) \times C_2$, and a noncentral transposition g fixes 8 vertices, hence $\mathrm{fpr}(g) = 4/15$.

Theorem 2.15 ([112] Theorem 1.2) · *Let Γ be a connected vertex-transitive 3-valent graph admitting a nonidentity automorphism fixing more than 1/3 of the vertices. Then Γ is arc-transitive and one of the following holds:*

(*a*) $|V\Gamma| \leq 20$, *and Γ is one of the six exceptions in $\Phi_1, \dots, \Phi_6$;*

(*b*) *Γ is isomorphic to a split Praeger–Xu graph $\mathrm{sC}(r,s)$ with $1 \leq s < 2r/3$ and $r \geq 3$.*

Theorem 2.14 has found a remarkable application due to P. Potočnik, M. Toledo and G. Verret in [120]. This paper shows that the order of an automorphism of a vertex-transitive 3-valent graph cannot exceed the number of vertices, and that, apart from the utility graph $\mathbf{K}_{3,3}$ and the split Praeger–Xu graphs, the proportion of automorphisms of such a graph that admit a regular orbit is at least 5/12.

We note that the bound of 1/3 in both Theorem 2.14 and Theorem 2.15 is sharp. We consider the graph DW_m with vertex-set $\mathbb{Z}_m \times \mathbb{Z}_3$ and edge-set

$$\{\{(x,i),(x+1,j)\} \mid x \in \mathbb{Z}_m,\ i,j \in \mathbb{Z}_3,\ i \neq j\}\,.$$

The graphs DW_m are 4-valent, connected and arc-transitive. Moreover, there exists an automorphism g of DW_m which fixes every vertex of the form $(x,0)$ while swapping the vertices in each pair $\{(x,1),(x,2)\}$, for some $x \in \mathbb{Z}_m$. Therefore, $\mathrm{fpr}(g) = 1/3$, and the infinite family DW_m meets the bound of Theorem 2.14. Applying the splitting operation, we obtain the infinite family sDW_m, consisting of 3-valent graphs achieving the bound of Theorem 2.15.

We conclude Section 2.E by reporting the following question, which has a partial solution in Section 3.A.

Problem 2.16 ([112] Problem 1.6) · Let d be a positive integer. Find a constant C_d and a *well-understood family of special graphs* $\mathcal{F}_d$ such that every finite connected d-valent vertex-transitive graph Γ admitting a nontrivial automorphism fixing more than $C_d|V\Gamma|$ vertices belongs to $\mathcal{F}_d$.

2.F Fixed edge ratios

Since the automorphism group of a graph naturally defines an action on the edge-set, a shift of focus can be performed considering the fixity for the edges rather that for the vertices. In this direction, P. Potočnik and P. Spiga proposed the following problem.

Problem 2.17 ([112] Problem 1.7) · Determine the connected 4-valent arc-transitive graphs and the connected 3-valent vertex-transitive graphs admitting an automorphism fixing more than 1/3 of the edges.

Sections 2.F to 2.H answer this question, following [15]. More precisely, we prove the following results.

Theorem F · *Let Γ be a finite connected 4-valent vertex- and edge-transitive graph admitting a nontrivial automorphism fixing more than 1/3 of the edges. Then one of the following holds:*

(*a*) *Γ is isomorphic to $\mathbf{K}_5$, the complete graph on 5 vertices;*

(*b*) *Γ is isomorphic to a Praeger–Xu graph $\mathrm{C}(r,s)$, for some r and s with $3s < 2r-3$.*

Theorem G · *Let Γ be a finite connected 3-valent vertex-transitive graph admitting a nontrivial automorphism fixing more than 1/3 of the edges. Then Γ is isomorphic to a split Praeger–Xu graph $\mathrm{sC}(r,s)$, for some r and s with $3s < 2r-3$.*

We remark that the graphs appearing as exceptions in Theorems F and G form a proper subset of the exceptions of Theorems 2.14 and 2.15.

The bound in Theorem G is sharp. For instance, each 3-valent graph admitting a nontrivial automorphism fixing setwise a perfect matching has the aforementioned property. For valency 4, we cannot prove sharpness. The proof of Theorem F shows that, if such an infinite family of graphs meeting the bound exists, those graphs cannot be 2-arc-transitive. In view of Theorem 2.19, we pose the following question.

Question 2.18 · Can the bound in Theorem F be strengthened to 1/4, by eventually including some extra small exceptional graphs in Theorem F (a)?

We remark that Theorems 2.14, 2.15, F and G show that, besides small exceptions or well-understood families of graphs, nontrivial automorphisms of 3-valent or 4-valent vertex-transitive graphs cannot fix *too many* vertices or edges, where *too many* in this context has to be considered as a linear function on the number of vertices (and, even then, with a small caveat for 4-valent graphs, because of the assumption of edge-transitivity). The difficulty in having a unifying theory of vertex-transitive graphs of small valency admitting nontrivial automorphisms fixing too many vertices or edges seems to arise from our lack of understanding possible generalisations of Praeger–Xu graphs (that is, vertex-transitive graphs of bounded valency playing the role of Praeger–Xu graphs). This is a recurrent problem in the theory of groups acting on finite graphs of bounded valency, and one of the reasons why we limit our definition of *small* to less than 5.

Before dealing with the proofs, we need some explicit computation for the fixed point ratios of the action of the automorphism group on edges for some recurring families of graphs.

2.F.1 Cayley graphs

While talking about fixed point ratio on vertices, Cayley graph have not entered into the picture due to Theorem 1.41.

In the case of edge-fixity, we can give a sharp bound that depends on the valency alone. We recall that we denote the set of all edges fixed by g with the symbol $\mathrm{Fix}(g, E\Gamma)$.

Theorem 2.19 · *Let G be a finite group, let S be an inverse closed nonempty subset of G, and let $\Gamma = \mathrm{Cay}(G, S)$ be the Cayley graph of G of connection set S. Suppose that $g \in G - \{1\}$ is a nontrivial element fixing at least one edge. Then g is an involution and*

$$\mathrm{fpr}(g, E\Gamma) = \frac{|g^G \cap S|}{|S||g^G|}.$$

In particular,

$$\mathrm{fpr}(g, E\Gamma) \leq 1/|S|,$$

and equality is attained if, and only if, the conjugacy class g^G is a subset of the connection set S.

Proof. For each $s \in S$, we define

$$X(s) = \{\{x, sx\} \mid x \in G\}.$$

Observe that, for any $s \in S$, $X(s)$ is either a perfect matching or a 2-factor of Γ, and that

$$\{X(s) \mid s \in S\}$$

is a partition of the edge-set $E\Gamma$.

Let $s \in S$ be your favourite generator, and suppose that $X(s)$ contains some edges fixed by g, say

$$\{y, sy\} \in X(s) \cap \mathrm{Fix}(g, E\Gamma).$$

It follows that

$$yg = sy \quad \text{and} \quad syg = y,$$

thus

$$g^2 = 1 \quad \text{and} \quad s = ygy^{-1}.$$

In other words, g has order 2, and S contains a conjugate of g.

For every other $\{x, sx\} \in X(s)$, with a similar computation, we obtain that $\{x, sx\} \in \mathrm{Fix}(g, E\Gamma)$ if, and only if, $s = xgx^{-1}$. Thus $ygy^{-1} = xgx^{-1}$ and $x \in y\mathbf{C}_G(g)$. In particular, $X(s)$ and $\mathrm{Fix}(g, E\Gamma)$ have nonempty intersection if, and only if, s lies in the conjugacy class g^G, and

$$X(s) \cap \mathrm{Fix}(g, E\Gamma) = \{\{yh, syh\} \mid h \in \mathbf{C}_G(x)\},$$

hence

$$|X(s) \cap \mathrm{Fix}(g, E\Gamma)| = \frac{|\mathbf{C}_G(g)|}{2}.$$

Therefore,

$$\begin{aligned}\mathrm{fpr}(g, E\Gamma) &= \frac{|g^G \cap S||\mathbf{C}_G(g)|}{2|E\Gamma|} \\ &= \frac{|g^G \cap S||\mathbf{C}_G(g)|}{|S||G|} \\ &= \frac{|g^G \cap S|}{|S||G : \mathbf{C}_G(g)|} \\ &= \frac{|g^G \cap S|}{|S||g^G|}.\end{aligned}$$

Since $|g^G \cap S| \leq |g^G|$, we have

$$\mathrm{fpr}(g, E\Gamma) \leq 1/|S|.$$

Finally, equality is attained if, and only if, $g^G \cap S = g^G$, that is, $g^G \subseteq S$. ■

2.F.2 Praeger–Xu graphs

We now turn our attention to the nature of fixed edges in a Praeger–Xu graph $\mathrm{C}(r, s)$.

Recall, from Section 2.A, that K is the group generated by the centres of all vertex-stabilizers, and that $H = K \rtimes \langle \rho, \sigma \rangle$ is the extension of K with a rotation ρ and an axial symmetry σ of the underlying cycle.

Lemma 2.20 · *Let $\Gamma = \mathrm{C}(r,s)$ be a Praeger–Xu graph, and let $g \in \mathrm{Aut}(\Gamma)$ be a nontrivial automorphism such that $\mathrm{fpr}(g, E\Gamma) > 1/3$. Then $3s < 2r-3$ and, either $g \in K$ or $(r,s) = (r,1)$. In particular, g fixes an edge if, and only if, g fixes both of its ends.*

Proof. We suppose that $r = 4$. The wreath product $\mathrm{C}(4,1)$ is isomorphic to $K_{4,4}$, which admits automorphisms h fixing 8 edges and hence

$$\mathrm{fpr}(h, E\Gamma) = \frac{8}{16} = \frac{1}{2} > \frac{1}{3}.$$

Observe that the nonidentity elements in $\mathrm{Aut}(\mathrm{C}(4,1))$ with $\mathrm{fpr}(h, E\Gamma) > 1/3$ are not necessarily in K, but they fix an edge if, and only if, they fix both of its ends. Similarly, it can be explicitly verified that, for every $h \in \mathrm{Aut}(\mathrm{C}(4,2)) - \{1\}$, we have

$$\mathrm{fpr}(h, E\Gamma) \leq \frac{8}{32} = \frac{1}{4} < \frac{1}{3}.$$

Furthermore, for every $h \in \mathrm{Aut}(\mathrm{C}(4,3)) - \{1\}$, we have

$$\mathrm{fpr}(h, E\Gamma) = \frac{8}{64} = \frac{1}{8} < \frac{1}{3}.$$

These computation exhaust the cases with $r = 4$.

We now suppose that $r \neq 4$. By Lemma 2.2, $\mathrm{Aut}(\Gamma) = H$, thus every automorphism of the graph can be written as

$$g = \tau\rho^i\sigma^\epsilon, \qquad \text{for some} \quad \tau \in K, i \in \mathbb{Z}_r, \epsilon \in \mathbb{Z}_2.$$

We define $A(x)$ as the union of the sets of $(s-1)$-arcs in $\vec{C}(r,1)$ starting at $(x,0)$ or at $(x,1)$. From the definition of the vertex set of $\mathrm{C}(r,s)$, we have that $A(x) \subseteq V\mathrm{C}(r,s)$, $|A(x)| = 2^s$ and

$$V\mathrm{C}(r,s) = \bigcup_{x \in \mathbb{Z}_r} A(x).$$

Moreover, by definition of K, $A(x)$ is a K-orbit, and the subgraph induced by Γ on $A(x) \cup A(x+1)$ is the disjoint union of cycles of length 4. Indeed, this is the property we have used in Section 2.D to define the standard cycle decomposition $\mathcal{S}$ (see also [73]). Observe that, for any $x \in \mathbb{Z}_r$,

$$A(x)^\rho = A(x+1), \quad \text{and} \quad A(x)^\sigma = A(-x-s+1). \tag{2.8}$$

We start by proving that $g \in K$. We split the discussion in two cases: either $\epsilon = 0$ or $\epsilon = 1$.

Suppose $\epsilon = 0$. Let $\{a,b\} \in \mathrm{Fix}(g, E\Gamma)$. Replacing a with b if necessary, we may suppose that $a \in A(x)$ and $b \in A(x+1)$, for some $x \in \mathbb{Z}_r$.

If $a^g = a$ and $b^g = b$, then $A(x)^g = A(x)$ and $A(x+1)^g = A(x+1)$. Now, Equation (2.8) yields $x + i = x$ and $(x+1)+i = x+1$, that is, $i = 0$. Therefore $g \in K$.

Similarly, if $a^g = b$ and $b^g = a$, we have $A(x)^g = A(x+1)$ and $A(x+1)^g = A(x)$. Now, Equation (2.8) yields $x+i = x+1$ and $(x+1)+i = x$, that is, $2 = 0$. However, this implies $r = 2$, which is a contradiction because $r \geq 3$.

Suppose $\epsilon = 1$. Since $\langle \rho, \sigma \rangle$ is a dihedral group of order $2r$, replacing g by a suitable conjugate if necessary, we may suppose that either r is odd and $i = 0$, or r is even and $i \in \{0,1\}$.

Assume $i = 0$. Let $\{a,b\} \in \mathrm{Fix}(g, E\Gamma)$. As above, replacing a with b if necessary, we may suppose that $a \in A(x)$ and $b \in A(x+1)$, for some $x \in \mathbb{Z}_r$.

If $a^g = a$ and $b^g = b$, we have $A(x)^g = A(x)$ and $A(x+1)^g = A(x+1)$. Now, Equation (2.8) yields $-x-s+1 = x$ and $-(x+1)-s+1 = x+1$, that is, $2 = 0$. However, this gives rise to the contradiction $r = 2$.

Similarly, if $a^g = b$ and $b^g = a$, we have $A(x)^g = A(x+1)$ and $A(x+1)^g = A(x)$. Now, Equation (2.8) yields $-x-s+1 = x+1$ and $-(x+1)-s+1 = x$, that is, $2x+s = 0$. When r is odd, the equation $2x+s = 0$ has only one solution in $\mathbb{Z}_r$ and, when r is even, the equation $2x+s = 0$ has either zero or two solutions in $\mathbb{Z}_r$ depending on whether s is odd or even. Recalling that the subgraph induced by Γ on $A(x) \cup A(x+1)$ is a disjoint union of cycles of length 4, we obtain that

$$|\mathrm{fpr}(g, E\Gamma)| \leq \begin{cases} \dfrac{|A(x)|}{|E\Gamma|} = \dfrac{1}{2r} & \text{if } r \text{ is odd}, \\ \dfrac{2|A(x)|}{|E\Gamma|} = \dfrac{1}{r} & \text{if } r \text{ is even}. \end{cases}$$

In both cases, we have $\mathrm{fpr}(g, E\Gamma) \leq 1/4$, which is a contradiction.

Assume $i = 1$. Observe that this implies that r is even. Here the analysis is entirely similar. Let $\{a,b\} \in \mathrm{Fix}(g, E\Gamma)$. As above, replacing a with b if necessary, we may suppose that $a \in A(x)$ and $b \in A(x+1)$, for some $x \in \mathbb{Z}_r$.

If $a^g = a$ and $b^g = b$, we have $A(x)^g = A(x)$ and $A(x+1)^g = A(x+1)$. Now, Equation (2.8) yields $-(x+1)-s+1 = x$ and $-(x+2)-s+1 = x$, that is, $2 = 0$. However, this gives rise to the usual contradiction $r = 2$.

Similarly, if $a^g = b$ and $b^g = a$, we have $A(x)^g = A(x+1)$ and $A(x+1)^g = A(x)$. Now, Equation (2.8) yields $-(x+1)-s+1 = x+1$ and $-(x+2)-s+1 = x$, that is, $2x+s+1 = 0$. As r is even, the equation $2x+s+1$ has either zero or two solutions in $\mathbb{Z}_r$ depending on whether s is even or odd. Recalling that the subgraph induced by Γ on $A(x) \cup A(x+1)$ is a disjoint union of cycles of length 4, we obtain that

$$|\mathrm{fpr}(g, E\Gamma)| \leq \frac{2|A(x)|}{|E\Gamma|} = \frac{1}{r}.$$

Thus, we have $\mathrm{fpr}(g, E\Gamma) \leq 1/4$, which is a contradiction.

Since $g \in K$, if g fixes the edge $\{a,b\} \in E\Gamma$, then g fixes both end-vertices a and b. It remains to show that $3s < 2r-3$. Notice that τ_i moves precisely those $(s-1)$-arcs of $\vec{C}(r,1)$ that pass through one of the vertices $(i,0)$ or $(i,1)$. Therefore, τ_i, as an automorphism of $\mathrm{C}(r,s)$, fixes all but $s2^s$ vertices, thus it fixes all but those $(s+1)2^{s+1}$ edges which are incident with such vertices. Recall that $\{\tau_i \mid i \in \mathbb{Z}_r\}$ is a set of generators for K whose elements all have disjoint supports. It follows that, among the elements of K, these generators have minimal support size. Hence

$$\frac{1}{3} < \mathrm{fpr}(E\Gamma, g) \leq \mathrm{fpr}(E\Gamma, \tau_i) = \frac{(r-(s+1))\,2^{s+1}}{r2^{s+1}} = \frac{r-s-1}{r}. \qquad \blacksquare$$

We conclude Section 2.F with two auxiliary lemmas.

Lemma 2.21 · *Let $\Gamma = \mathrm{C}(r,s)$ be a Praeger–Xu graph, let G be a vertex- and edge-transitive group of automorphism of Γ. Suppose that G contains a nontrivial element g fixing more that $1/3$ of the edges, and that G is not 2-arc-transitive. Then G is $\mathrm{Aut}(\Gamma)$-conjugate to a subgroup of H.*

Proof. By Lemma 2.20, $3s < 2r-3$. If $r \neq 4$, then, in view of Lemma 2.2, we have

$$G \leq \mathrm{Aut}(\Gamma) = H\,.$$

When $r = 4$, then inequality $3s < 2r-3$ implies $s = 1$. Now, the veracity of this lemma can be verified with an explicit computation in

$$\mathrm{Aut}(\mathrm{C}(4,1)) = \mathrm{Aut}(K_{4,4}) = S_4 \,\mathrm{wr}\, S_2\,.$$ ■

Lemma 2.22 ([112] Lemma 2.3) · *Let Γ be a connected 4-valent graph, let G be a vertex- and edge-transitive group of automorphism of Γ, and let g be a nontrivial element of G such that*

$$\mathrm{fpr}(g, V\Gamma) > \frac{1}{3}\,.$$

Suppose that G contains a minimal normal 2-subgroup N of such that Γ/N is isomorphic to $\mathrm{C}(r,s)$ for some r and s, and that G/N is a subgroup of $H^\dagger$. Then Γ is isomorphic to $\mathrm{C}(r',s')$, for some positive integers r' and s' with $s' \leq 2r'/3$.

2.G Rigid cells

Section 2.G deals with the proof of Theorems F and G in the cases with Γ 4-valent and 2-arc-transitive, or with Γ 3-valent and arc-transitive. The rich symmetric structure arising in these scenarios can be exploited for proving the result via mostly combinatorial means.

Definition 2.23 · Let Γ be a finite connected graph, and let g be an automorphism of Γ. The action of g partitions $E\Gamma$ in three sets:

(i) edges that are fixed as an arc, that is,

$$A[g] := \{\{a,b\} \in E\Gamma \mid a^g = a \text{ and } b^g = b\}\,;$$

(ii) edged that are fixed as an edge but not as an arc, that is,

$$F[g] := \mathrm{Fix}(g, E\Gamma) - A[g] = \{\{a,b\} \in E\Gamma \mid a^g = b \text{ and } b^g = a\}\,;$$

(iii) edges that are not fixed, that is,

$$N[g] := E\Gamma - \mathrm{Fix}(g, E\Gamma) = E\Gamma - (A[g] \cup F[g])\,.$$

The *rigid cell of g*, in symbols $\Gamma[g]$, is the subgraph of Γ on the vertices which are incident with edges in $A[g]$. For every positive integer i, we denote by $V_i\Gamma[g]$ the set of vertices of $\Gamma[g]$ having valency i.

Observe that, under the assumption that Γ has valency 3 or 4, since the valency of the vertices of a rigid cell $\Gamma[g]$ cannot be equal to $\mathrm{val}(\Gamma) - 1$, we obtain that their valencies divide the valency of Γ. In particular, in the 3-valent case $V\Gamma[g]$ is partitioned by $V_1[g]$ and $V_3[g]$, while in the 4-valent case by $V_1[g]$, $V_2[g]$ and $V_4[g]$.

Rigid cells have been introduced by K. Kutnar and D. Marušič in [83] to tackle the odd/even problem for 3-valent arc-transitive graphs. Broadly speaking, the *odd/even problem* consists in establishing, given a graph Γ with n vertices, whether $\mathrm{Aut}(\Gamma)$ embeds in $\mathrm{Alt}(n)$ (that is, all the automorphisms are even permutation) or not (that is, there is an automorphism which is an odd permutation). Their proof relies on the interplay between the possible local groups of a 3-valent arc-transitive graph and the corresponding rigid cells. To a lesser extent, the philosophy of our proof will be the same. A further investigation of rigid cells for 3-valent arc-transitive graphs can be found in [40].

The discussion of Section 2.G is divided in three cases:

(a) 4- and 3-valent graphs of girth at most 4 (see Section 2.G.1),

(b) 4-valent graphs of girth at least 5 (see Section 2.G.2),

(c) 3-valent graphs of girth at least 5 (see Section 2.G.3).

2.G.1 Small girth

We recall that the *girth* of a graph Γ, in symbols $\mathrm{girth}(\Gamma)$, is the minimal length of a cycle in Γ. We start by pointing out that symmetrical graphs cannot be too sparse or have too small of a girth.

Lemma 2.24 ([63] Lemma 4.1.3) · *Let Γ be a connected k-valent graph, with $k \geq 3$, and let G be an s-arc-transitive group of automorphisms of Γ. Then*

$$2s \leq \mathrm{girth}(\Gamma) + 2.$$

In particular, the girth of Γ is greater than s.

Lemma 2.25 ([63] Lemma 3.3.3) · *Let Γ be a finite connected vertex-transitive graph of valency k. Then Γ is* k-edge-connected, *that is, Γ remains connected upon eliminating any m edges, with $m \leq k - 1$.*

The 4-valent 2-arc-transitive graphs of small girth fly under the radar of the strategy we are going to use to prove Theorem F. The 4-valent vertex-transitive graphs have been studied by P. Potočnik and S. Wilson in [121]. We give a specialized version of [121, Theorem 3.3].

Lemma 2.26 · *Let Γ be a 4-valent vertex- and edge-transitive graph. Then one of the following holds*

(i) *each vertex in Γ is contained in exactly one 4-cycle;*

(ii) *there are two distinct vertices sharing the same neighbourhood, that is,*

$$\alpha, \beta \in V\Gamma \quad \textit{with} \quad \Gamma(\alpha) = \Gamma(\beta);$$

(*iii*) *Γ is isomorphic to either* $\mathbf{K}_{5,5}-5\mathbf{K}_2$*, or* $\mathbf{Q}_{16}$*, or* $\mathfrak{H}$.

Pivoting on this result, we obtain the following characterization.

Lemma 2.27 · *Let Γ be a finite connected 4-valent 2-arc-transitive graph of girth at most 4, that is,*

$$\mathrm{girth}(\Gamma)\in\{3,4\}.$$

Then one of the following holds:

(*a*) $\mathrm{girth}(\Gamma)=3$ *and Γ is isomorphic to the complete graph* $\mathbf{K}_5$*;*

(*b*) $\mathrm{girth}(\Gamma)=4$ *and Γ is isomorphic to either* $\mathbf{K}_{4,4}\cong \mathrm{C}(4,1)$*, or* $\mathbf{K}_{5,5}-5\mathbf{K}_2$*, or* $\mathbf{Q}_{16}$*, or* $\mathfrak{H}$.

Proof. Let α be your favourite vertex of Γ, let

$$\Gamma(\alpha)=\{\beta_1,\beta_2,\beta_3,\beta_4\}$$

be its neighbourhood, and let us write G for $\mathrm{Aut}(\Gamma)$.

First, assume $\mathrm{girth}(\Gamma)=3$. Without loss of generality, suppose β_1 and β_2 are adjacent. Since G is 2-arc-transitive, G_α is 2-transitive on $\Gamma(\alpha)$. Hence β_i is adjacent to β_j for any $i\neq j$. Thus $\Gamma\cong\mathbf{K}_5$, proving Lemma 2.27 (*a*).

Now, suppose $\mathrm{girth}(\Gamma)=4$. We consider the three possibilities of Lemma 2.26 in turn.

Consider Lemma 2.26 (*i*). Up to a permutation of the indices, there is a vertex $\gamma\in\Gamma(\beta_1)\cap\Gamma(\beta_2)$ such that

$$\alpha\sim\beta_1\sim\gamma\sim\beta_2\quad\text{is a 4-cycle}.$$

Since the local group is 2-transitive, there exists $g\in G_\alpha$ with $(\beta_1,\beta_2)^g=(\beta_3,\beta_4)$. Therefore, by applying g to the 4-cycle, we obtain

$$\alpha\sim\beta_3\sim\gamma^g\sim\beta_4,$$

which is a 4-cycle different from

$$\alpha\sim\beta_1\sim\gamma\sim\beta_2.$$

This gives a contradiction.

Suppose that Γ satisfies Lemma 2.26 (*ii*). Since Γ is arc-transitive, [121, Lemma 4.3] gives that Γ is isomorphic to $\mathrm{C}(r,1)$ for some positive integer r. From Lemma 2.2, $\mathrm{C}(r,1)$ is 2-arc-transitive if, and only if, $r=4$. Therefore, we obtain that Γ is taken into account in Lemma 2.27 (*b*).

Finally, suppose that Γ appears in Lemma 2.26 (*iii*), By a routine computation, one can check that $\mathrm{Aut}(\Gamma)$ is 2-arc-transitive in these cases. Hence, we obtain the remaining possibilities in Lemma 2.27 (*b*). ■

It is worth to spend some ink to compute the fixed point ratio of the action of the automorphism groups of the graphs arising in Lemma 2.27 for their action on the edges.

(*a*) The complete graph $\mathbf{K}_5$ is the only sporadic example arising in Theorem F: its automorphism group is Sym(5), and each transposition fixes 4 edges out of 10.

(*b*) The automorphism group of the graph $\mathbf{K}_{5,5} - 5\mathbf{K}_2$ is $\mathrm{Sym}(5)\times C_2$, and every nontrivial automorphism fixes at most 6 edges out of 20.

(*c*) Every nontrivial automorphism of the skeleton of the hypercube $\mathbf{Q}_{16}$ fixes at most 8 edges out of 32.

(*d*) The automorphism group of the bipartite complement of the Heawood graph $\mathfrak{H}$ is isomorphic to $\mathrm{SL}_3(2) \rtimes C_2$: a nontrivial automorphism of $\mathfrak{H}$ fixes at most 4 edges out of 28.

We remark that $\mathbf{K}_5$ is the only 4-valent 2-arc-transitive graph with

$$\mathrm{fpr}\,(\mathrm{Aut}(\Gamma), E\Gamma) \geq \frac{1}{3}.$$

We can obtain a similar characterization for 3-valent 2-arc-transitive graphs. (The girth is irrelevant in the arc-transitive case.)

Lemma 2.28 · *Let Γ be a finite connected 3-valent 2-arc-transitive graph of girth at most 4, that is,*

$$\mathrm{girth}(\Gamma) \in \{3, 4\}.$$

Then either $\mathrm{girth}(\Gamma) = 3$ *and Γ is isomorphic to the complete graph $\mathbf{K}_4$, or* $\mathrm{girth}(\Gamma) = 4$ *and Γ is isomorphic to $\mathbf{K}_{3,3}$ or to $\mathbf{K}_{4,4} - 4\mathbf{K}_2$.*

Proof. Suppose $\mathrm{girth}(\Gamma) = 3$. Let $\alpha \in V\Gamma$ be a vertex, and let

$$\Gamma(\alpha) = \{\beta_1, \beta_2, \beta_3\}$$

be its neighbourhood. Without loss of generality, suppose β_1 and β_2 are adjacent. Since $\mathrm{Aut}(\Gamma)$ is arc-transitive, both β_1 and β_2 are also adjacent to β_3. It follows that Γ is isomorphic to $\mathbf{K}_4$.

Suppose $\mathrm{girth}(\Gamma) = 4$. Since $\mathrm{Aut}(\Gamma)$ is s-arc-transitive, for some $s \geq 2$, [109, Theorem 1.1 and Table I] implies that Γ is isomorphic to either $K_{3,3}$ or $K_{4,4} - 4K_2$. This completes the proof. ∎

A direct computation shows that all the graphs appearing in Lemma 2.28 satisfy

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), E\Gamma) < 1/3.$$

2.G.2 Valency 4

We are now ready to tackle the proof of Theorem F for 2-arc-transitive graphs. For the reader's convenience, we extract some preliminary lemmas.

We start by giving a lower bound on the number of vertices depending on the combinatorial information of the rigid cell of g.

Lemma 2.29 · *Let* Γ *be a finite connected* 4*-valent arc-transitive graph with* $\mathrm{girth}(\Gamma) \geq 5$, *and let* g *be an automorphism of* Γ. *Then*

$$2|F[g]| + 4|V_1\Gamma[g]| + 3|V_2\Gamma[g]| + |V_4\Gamma[g]| \leq |V\Gamma|.$$

Proof. We define

$$\mathcal{F} := \{\alpha \in V\Gamma \mid \{\alpha, \beta\} \in F[g] \text{ for some } \beta \in V\Gamma\},$$
$$\mathcal{N} := \{\alpha \in V\Gamma - (V_1\Gamma[g] \cup V_2\Gamma[g]) \mid \{\alpha, \beta\} \in N[g] \text{ for some } \beta \in V\Gamma\}.$$

Observe that the sets

$$V_1\Gamma[g], \quad V_2\Gamma[g], \quad V_4\Gamma[g], \quad \mathcal{F}, \quad \mathcal{N}$$

are pairwise disjoint and partition the vertex-set of Γ. Hence, we obtain

$$|V\Gamma| = |V_1\Gamma[g]| + |V_2\Gamma[g]| + |V_4\Gamma[g]| + |\mathcal{F}| + |\mathcal{N}|.$$

Furthermore, we have that $|\mathcal{F}| = 2|F[g]|$. Hence, to prove the statement, it suffices to show that

$$|\mathcal{N}| \geq 3|V_1\Gamma[g]| + 2|V_2\Gamma[g]|. \tag{2.9}$$

We construct an auxiliary graph Δ. The vertex set of Δ is

$$V\Delta = V_1\Gamma[g] \cup V_2\Gamma[g] \cup \mathcal{N},$$

and we declare a vertex $\alpha \in V_1\Gamma[g] \cup V_2\Gamma[g]$ adjacent to a vertex $\beta \in \mathcal{N}$ if $\{\alpha, \beta\} \in E\Gamma$. By construction, Δ is bipartite with parts $V_1\Gamma[g] \cup V_2\Gamma[g]$ and $\mathcal{N}$.

Given $\alpha \in V_1\Gamma[g]$, the automorphism g acts as a 3-cycle on $\Gamma(\alpha)$. Let

$$\beta_1, \beta_2, \beta_3 \in \Gamma(v)$$

be the three neighbours permuted by g. By definition,

$$\{\alpha, \beta_1\}, \{\alpha, \beta_2\}, \{\alpha, \beta_3\} \in N[g].$$

Thus, $\beta_1, \beta_2, \beta_3 \in \mathcal{N}$. This shows that each vertex in $V_1\Gamma[g]$ has three neighbours in $\mathcal{N}$. Repeating the same reasoning, each vertex in $V_2\Gamma[g]$ has two neighbours in $\mathcal{N}$. As $\mathrm{girth}(\Gamma) \geq 5$, we have that $\mathrm{girth}(\Delta) \geq 5$. Suppose that, for two distinct $\alpha, \alpha' \in V_1\Gamma[g] \cup V_2\Gamma[g]$, we can find a vertex $\beta \in \Delta(\alpha) \cap \Delta(\alpha')$. It follows that

$$\alpha \sim \beta \sim \alpha' \sim \beta^g$$

is a 4-cycle in Δ, against the fact that girth is 5. It follows that, for any two distinct $\alpha, \alpha' \in V_1\Gamma[g] \cup V_2\Gamma[g]$, the intersection $\Delta(\alpha) \cap \Delta(\alpha')$ is empty. In particular, by the Handshake Lemma, Equation (2.9) is true, thus the proof is complete. ∎

Finite faithful 2-transitive amalgams of index $(4, 2)$ have been studied in detail by P. Potočnik in [110]. We highlight the information we are going to use in the sequel.

Consider the finite faithful amalgam (L,B,R). With our usual notation, we have that the stabilizer of a ball of radius 1 is isomorphic to

$$\bigcap_{g\in L} B^g .$$

We now explain how we can explicitly find a shunt s in G using the presentation given in [110]. Let α be a vertex of the infinite 4-valent tree, and identify L with the stabilizer of α. We can choose a generator in L that does not appear in B, and we call it f. Similarly, we can observe that the generator a only appears in R, hence it defines the nontrivial element in R/B. We call β the neighbour of α such that $\alpha^a = \beta$. Without loss of generality, we can also suppose that β is not a fixed point for the action of f. We claim that $f^{-1}a$ is a shunt. Indeed,

$$(\beta^f,\alpha)^{f^{-1}a} = (\alpha,\beta).$$

Therefore, as the graph is 2-arc-transitive, for any two vertices $\alpha,\gamma \in V\Gamma$ at distance at most 2,

$$G_\alpha^{[1]} \cap G_\gamma^{[1]} \quad \text{is isomorphic to} \quad \bigcap_{g\in L} B^g \cap \left(\bigcap_{g\in L} B^g\right)^{(f^{-1}a)^{d_\Gamma(\alpha,\gamma)}} .$$

Using a calculator, as all the groups are finitely presented, we can now perform a case-by-case computation on the finite faithful 2-transitive amalgams of index $(4,2)$ classified in [110], and we find out the following dichotomy. (This computation is possible because the amalgams involved are finite and in finite number.)

Remark 2.30 · For any two distinct vertices $\alpha,\gamma \in V\Gamma$ at distance at most 2,

(i) either $G_\alpha^{[1]} \cap G_\gamma^{[1]}$ is a (possibly trivial) 3-group;

(ii) or the pair (Γ,G) has the amalgam type

$$(\mathrm{Sym}(3)\times\mathrm{Sym}(4), \mathrm{Sym}(3)\times\mathrm{Sym}(3), (\mathrm{Sym}(3)\times\mathrm{Sym}(3)) \rtimes C_2) :$$

moreover, in this case, if $d_\Gamma(\alpha,\gamma) = 1$, then $G_\alpha^{[1]} \cap G_\gamma^{[1]} = 1$, while, if $d_\Gamma(\alpha,\gamma) = 2$, then $G_\alpha^{[1]} \cap G_\gamma^{[1]}$ is isomorphic to C_2.

To make this more concrete to the reader, we prove this for two amalgams by hand.

Example 2.31 · Consider the amalgam of type

$$(C_3 \rtimes \mathrm{Sym}(4), (C_3\times C_3)\rtimes C_2, (C_3\times C_3)\rtimes(C_2\times C_2)) .$$

We report the presentation of L and B as given in [110]:

$$\begin{aligned} L = \langle x,y,c,d,t \mid x^2 = y^2 = [x,y] = c^3 = d^3 = [c,d] = [c,x] = [c,y] = \\ = x^d y = y^d yx = t^2 = c^t c = d^t d = x^t y = 1\rangle, \\ B = \langle c,d,t \mid c^3 = d^3 = [c,d] = t^2 = c^t c = d^t d = 1\rangle, \\ R = \langle c,d,t,a \mid c^3 = d^3 = [c,d] = t^2 = c^t c = d^t d = a^2 = c^a d^{-1} = [a,t] = 1\rangle. \end{aligned}$$

As c, d, t are elements of B, we only need to compute B^x and B^y. As x and y centralize c but not d and t, we get

$$B^x = \langle c, d^x, t^x \rangle \quad \text{and} \quad B^y = \langle c, d^y, t^y \rangle.$$

We claim that

$$X = B \cap B^x \cap B^y = \langle c, td \rangle.$$

Observe that $\langle d, t \rangle$ is a subgroup of $\mathbf{N}_L(\langle c \rangle)$. This implies that, for every word $\mathbf{v}$ in three variables, there exists a word $\mathbf{w}$ in two variables such that, for an appropriate integer h,

$$\mathbf{v}(c, d, t) = c^h \mathbf{w}(d, t).$$

Since $\mathbf{C}_L(\langle c \rangle)$ contains the subgroup $\langle x, y \rangle$, the same holds (with the same $\mathbf{w}$) if we evaluate on d^x or d^y instead of d, and on t^x or t^y instead of t. Therefore, as c is an element in B, B^x and B^y, to prove the claim it is enough to show that

$$\langle d, t \rangle \cap \langle d^x, t^x \rangle \cap \langle d^y, t^y \rangle = \langle td \rangle.$$

Let $\mathbf{w}$ be a word in two variables. We observe that

$$\mathbf{w}(d^x, t^x) = x\mathbf{w}(d, t)x \quad \text{and} \quad \mathbf{w}(d^y, t^y) = y\mathbf{w}(d, t)y.$$

Without loss of generality, we may assume that $\mathbf{w}(d, t)$ is a reduced word. As the action of t by conjugation on $\langle d \rangle$ inverts the elements, we obtain that there exist two integers $h \in \{0, 1, 2\}$ and $k \in \{0, 1\}$ such that

$$\mathbf{w}(d, t) = t^h d^k.$$

$x\mathbf{w}(d,t)x$	$k = 0$	$k = 1$
$h = 0$	1	$xtx = txy$
$h = 1$	$xdx = dxy$	$xtdx = tydx = tdy$
$h = 2$	$xd^2x = d^2y$	$xtd^2x = tyd^2x = td$

Table 2.1: Reduced forms for $x\mathbf{w}(d,t)x$.

$y\mathbf{w}(d,t)y$	$k = 0$	$k = 1$
$h = 0$	1	$yty = txy$
$h = 1$	$ydy = dx$	$ytdy = txdy = td$
$h = 2$	$yd^2y = d^2xy$	$ytd^2y = txd^2y = td^2x$

Table 2.2: Reduced forms for $y\mathbf{w}(d,t)y$.

In Tables 2.1 and 2.2, we compute all the possibilities for $x\mathbf{w}(d,t)x$ and $y\mathbf{w}(d,t)y$. Since $\langle d, t \rangle$ and $\langle x, y \rangle$ intersect trivially, it follows that the only two words in the alphabet $\{d, t\}$ that can be written using the symbols $\{d^x, t^x\}$ or $\{d^y, t^y\}$ are the trivial word and td. The claim is thus proved.

Before proceeding, we need a shunt. By the discussion preceding Remark 2.30, every shunt is of the form $f^{-1}a$, where f is either x or y. Since $L *_B R$ acts transitively on the right coset space of L, it is irrelevant if we choose $f = x$ or $f = y$. To fix the notation, we make the first choice, thus xa is our shunt.

We start by computing

$$X^{xa} = \langle c, tdy \rangle^a = \langle d, tcy^a \rangle .$$

We observe that the X^{xa} is isomorphic to Sym(3), where $\mathbf{o}(d) = 3$ and $\mathbf{o}(tcy^a) = 2$. It follows that

$$\mathbf{O}_3(X) \cap \mathbf{O}_3(X^{xa}) = \langle c \rangle \cap \langle d \rangle \quad \text{is trivial.}$$

Furthermore, all the involutions of X^{xa} can be written as $d^h tcy^a$, for some $h \in \{0,1,2\}$. Hence, as X is a subgroup of $\langle c, d, t \rangle$, while $d^h tcy^a$ is an element of $\langle c, d, t \rangle y^a$, X and X^{xa} share no transposition. It follows that

$$X \cap x^{xa} \quad \text{is trivial.}$$

We can apply the second shunt. We obtain

$$X^{xaxa} = \langle dxy, tcyy^a x \rangle^a = \langle cx^a y^a, tcy^a yx^a \rangle .$$

This old dog has not learned any new tricks. Note that

$$\langle c, dt \rangle \leq \langle c, d, t \rangle, \quad cx^a y^a \in \langle c, d, t \rangle x^a y^a, \quad tcy^a yx^a \in \langle c, d, t \rangle y^a yx^a .$$

This implies that

$$X \cap X^{xaxa} \quad \text{is trivial.}$$

By the discussion preceding Remark 2.30, this proves that every pair (Γ, G), where Γ realized the amalgam

$$(C_3 \rtimes \mathrm{Sym}(4), (C_3 \times C_3) \rtimes C_2, (C_3 \times C_3) \rtimes (C_2 \times C_2)) ,$$

satisfies part (i) of Remark 2.30 (where the 3-groups are trivial).

Example 2.32 · Consider the amalgam of type

$$(\mathrm{Sym}(3) \times \mathrm{Sym}(4), \mathrm{Sym}(3) \times \mathrm{Sym}(3), (\mathrm{Sym}(3) \times \mathrm{Sym}(3)) \rtimes C_2) .$$

The presentations of L, B and R as given in [110] read

$$\begin{aligned} L = \langle x, y, c, d, r, s \mid x^2 = y^2 = [x,y] = c^3 = d^3 = [c,d] = [c,x] = [c,y] = \\ = x^d y = y^d yx = r^2 = s^2 = [r,s] = [x,r] = [y,r] = \\ = x^s y = c^r c = [c,s] = [d,r] = d^s d = 1 \rangle, \\ B = \langle c, d, r, s \mid c^3 = d^3 = [c,d] = r^2 = s^2 = [r,s] = c^r c = \\ = [c,s] = [d,r] = d^s d = 1 \rangle, \\ R = \langle c, d, r, s, a \mid c^3 = d^3 = [c,d] = r^2 = s^2 = [r,s] = c^r c = [c,s] = \\ = [d,r] = d^s d = a^2 = c^a d^{-1} = s^a r = 1 \rangle, \end{aligned}$$

Repeating the same discussion as in Example 2.31, we see that

$$X = B \cap B^x \cap B^y = \langle c, r \rangle \times \langle sd \rangle .$$

To obtain part (ii) of Remark 2.30, we need to compute the intersection of X with its conjugate by a shunt and by a square of a shunt. By the discussion preceding Remark 2.30, we know that a shunt can be written ad $f^{-1}a$, where f is either x or y. Without loss of generality, we choose $f = x$.

Let us compute

$$X^{xa} = \langle c, r\rangle^a \times \langle sdy\rangle^a = \langle d, s\rangle \times \langle rcy^a\rangle .$$

We know that $\langle c, r\rangle$ and $\langle d, s\rangle$ intersect in 1, and that rcy^a is an involution in the right coset Xy^a. Therefore,

$$X \cap X^{xa} \quad \text{is trivial},$$

as desired.

Shunting once more, we get

$$X^{xaxa} = \langle dyx, syx\rangle^a \times \langle rcxy^a x\rangle^a = \langle cy^a x^a, ry^a x^a\rangle \times \langle sdx^a yx^a\rangle .$$

We want to compute $X \cap X^{xaxa}$. We claim that the intersection is contained in $\langle c, r\rangle$. Indeed, $sdx^a yx^a$ is an involution in $Xx^a yx^a$, which is a proper right coset of X.

Observe that, by construction, $\mathbf{o}(cy^a x^a) = 3$ and $\mathbf{o}(ry^a x^a) = 2$. Moreover, the action of $ry^a x^a$ by conjugation inverts the elements of $\langle cy^a x^a\rangle$. Hence, any word in the alphabet $\{cy^a x^a, ry^a x^a\}$ can be reduced to the form

$$(cy^a x^a)^h (ry^a x^a)^k ,$$

where $h \in \{0, 1, 2\}$ and $k \in \{0, 1\}$.

We start by observing that, for $h = 0$ and $k = 0$, we find the identity element, which belongs to the intersection. Thus, we can suppose that one of these integers is nonzero. We want to find two integers n and m, not both zero, such that

$$c^n r^m = (cy^a x^a)^h (ry^a x^a)^k . \tag{2.10}$$

Let us assume that $h \neq 0$. Using the properties of $ry^a x^a$ and the analogues for r, by raising to the power of 2, we obtain

$$c^{2n(1-\delta(m,1))} = (cy^a x^a)^{2h(1-\delta(k,1))} , \tag{2.11}$$

where $\delta(x, y)$ denotes the Kronecker delta between x and y. We split the discussion according to $k = 1$ or $k = 0$.

Let us assume that $k = 1$. We obtain, from Equation (2.11),

$$c^{2n(1-\delta(m,1))} = 1 ,$$

which can hold only if $n = 0$ or $m = 1$. In the former scenario, Equation (2.10) becomes

$$r^m = (cy^a x^a)^h (ry^a x^a) = (cy^a x^a)^h (x^a y^a r) = (cy^a x^a)^{h-1} cr .$$

If $m = 0$,

$$cr = (cy^a x^a)^{h-1} ,$$

which is a contradiction because $\mathbf{o}(cr) = 2$ and $\mathbf{o}(cy^a x^a) = 3$. Similarly, if $h = 1$,

$$r^m = cr ,$$

which is not the case as $\langle c, r\rangle$ is isomorphic to $\mathrm{Sym}(3)$. Hence, $h-1 \neq 0$, and we can rearrange the equality as

$$c^{-1} = (cy^a x^a)^{h-1}.$$

If $h = 0$, we find

$$1 = x^a y^a,$$

but $\langle x^a, y^a\rangle$ is isomorphic to the Klein group $C_2 \times C_2$. Meanwhile, if $h = 2$,

$$c^{-2} = y^a x^a,$$

but a nontrivial 2-element and a nontrivial 3-element cannot coincide. Therefore, we have that $n \neq 0$ and $m = 1$. We can rewrite Equation (2.10) as

$$c^{n-1} = (cy^a x^a)^{h-1}.$$

We go through the possible choices of h. If $h = 0$, then

$$c^n = x^a y^a.$$

If $h = 1$, then

$$c^{n-1} = 1.$$

If $h = 2$, then

$$c^{n-2} = y^a x^a.$$

Unless $h = 1$ and $n = 1$, the left hand side and the right hand side have different orders. Otherwise, we find that

$$cr \in \langle c, r\rangle \cap \langle cy^a x^a, ry^a x^a\rangle. \tag{2.12}$$

This concludes the case $k = 1$.

Let us assume that $k = 0$. We now compute

$$(cy^a x^a)^2 = cy^a x^a cy^a x^a = cayxdyxa = caydyyxa = cadxyxa = cd^a y^a = c^2 y^a.$$

Substituting this in Equation (2.11), we get

$$c^{2n(1-\delta(m,1))} = (c^2 y)^h.$$

Recall that h cannot be zero, otherwise we find the identity of $\langle cy^a x^a, ry^a x^a\rangle$. Then either $h = 1$, or $h = 2$. In the former case, we have that

$$c^{-2n\delta(m,1)} = y,$$

which is impossible, as $\mathbf{o}(c) = 3$ while $\mathbf{o}(y) = 2$. In the latter case, we obtain

$$c^{2n(1-\delta(m,1))} = c^2 y c^2 y = c.$$

Therefore, as $2n(1-\delta(m,1)) \equiv 1 \pmod 3$, $m = 0$ and $n = 2$. Finally, Equation (2.10) reads

$$c^2 = (cy^a x^a)^2 = c^2 y,$$

but y is nontrivial. This is the final contradiction.

To sum up, if the reader can still remember Equation (2.12), we have proved that

$$\langle c, r\rangle \cap \langle cy^a x^a, ry^a x^a\rangle = \langle cr\rangle.$$

This is precisely what part (ii) of Remark 2.30 asks, and it concludes this example.

We can squeeze a last piece of information from the faithful amalgams of index $(4,2)$.

Lemma 2.33 · *Let Γ be a finite connected 4-valent graph, let G be an s-arc-transitive group of automorphisms of Γ with $s \geq 2$, and let $g \in G$ fixing pointwise the s-arc*

$$\alpha_0 \sim \ldots \sim \alpha_{s-1}.$$

Suppose that G is not $(s+1)$-arc-transitive, and that g fixes pointwise $\Gamma(\alpha_0) \cup \Gamma(\alpha_{s-1})$. Then $g = 1$ is trivial.

Proof. If G is s-arc-regular, then $g = 1$ is trivial, because g fixes an s-arc. Using [110], we see that there are 6 amalgams such that G is not s-arc-regular. For each of these remaining amalgams, via a computer-assisted calculation, we can show that

$$G_{\alpha_0}^{[1]} \cap G_{\alpha_{s-1}}^{[1]} \cong \bigcap_{g \in L} B^g \cap \left(\bigcap_{g \in L} B^g \right)^{(f^{-1}a)^s} = 1.$$

Therefore, the only automorphism leaving the neighbourhood of each end of a given s-arc fixed is the identity map, as claimed. ■

We have built all the machinary to conclude Section 2.G.2.

Proof of Theorem F for Γ 2-arc-transitive. Let Γ be a 4-valent 2-arc-transitive graph with

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), E\Gamma) > \frac{1}{3}.$$

If $\mathrm{girth}(\Gamma) \leq 4$, in view of Lemma 2.27 and the consideration at the end of Section 2.G.1, we have that Γ is isomorphic to $\mathbf{K}_5$, the complete graph on 5 vertices. This is Theorem F (*a*).

Hence, we can suppose for the rest of the proof that $\mathrm{girth}(\Gamma) \geq 5$. From here on, we fix a nontrivial automorphism $g \in \mathrm{Aut}(\Gamma)$. We can compute a general upper bound for $\mathrm{fpr}(E\Gamma, g)$ based on the combinatorics of the rigid cell of g. Since $4|V\Gamma| = 2|E\Gamma|$, using the inequality in Lemma 2.29, we obtain

$$\begin{aligned} \mathrm{fpr}(E\Gamma, g) &= \frac{|F[g]| + |A[g]|}{|E\Gamma|} \\ &= \frac{2|F[g]| + 2|A[g]|}{4|V\Gamma|} \\ &\leq \frac{2|F[g]| + |V_1\Gamma[g]| + 2|V_2\Gamma[g]| + 4|V_4\Gamma[g]|}{8|F[g]| + 16|V_1\Gamma[g]| + 12|V_2\Gamma[g]| + 4|V_4\Gamma[g]|}. \end{aligned} \tag{2.13}$$

Assume that the vertices in $V_4\Gamma[g]$ are at pairwise distance more than 2. Then any two such vertices share no common neighbour. In particular,

$$\bigcup_{\alpha \in V_4\Gamma[g]} \Gamma(\alpha)$$

has cardinality $4|V_4\Gamma[g]|$ and it is contained in $V_1\Gamma[g] \cup V_2\Gamma[g]$. Therefore,

$$4|V_4\Gamma[g]| \leq |V_1\Gamma[g]| + |V_2\Gamma[g]|.$$

By substituting this last inequality in Equation (2.13), we obtain

$$\mathrm{fpr}(E\Gamma,g)\le\frac{2\left(|F[g]|+|V_1\Gamma[g]|+\frac{3}{2}|V_2\Gamma[g]|\right)}{8\left(|F[g]|+|V_1\Gamma[g]|+\frac{3}{2}|V_2\Gamma[g]|\right)+8|V_1\Gamma[g]|+4|V_4\Gamma[g]|}<\frac{1}{4},$$

a contradiction.

Hence, we must suppose that there exist two distinct vertices α and β of $V_4\Gamma[g]$ having distance at most 2. We split our discussion according to Remark 2.30.

Suppose that Remark 2.30 (i) holds. In this case, g is a 3-element, because, via direct inspection of the possible amalgams, we find that

$$g\in G_\alpha^{[1]}\cap G_\beta^{[1]}\quad\text{is a 3-group}.$$

Observe that $V_2\Gamma[g]$ is empty: indeed, an element of order 3 cannot have an orbit of even length, so in a local group cannot fix exactly two elements.

We claim that $\Gamma[g]$ is a forest. Let $s\ge 2$ such that G is s-arc-transitive, but not $(s+1)$-arc-transitive. Aiming for a contradiction, suppose that $\Gamma[g]$ is not a forest. Then $\Gamma[g]$ contains an ℓ-cycle C. As $V_2\Gamma[g]$ is empty, the vertices of C are elements of $V_4\Gamma[g]$. From Lemma 2.24,

$$\mathrm{girth}(\Gamma[g])\ge\mathrm{girth}(\Gamma)\ge s+1\,.$$

Hence, from C, we can extract an s-arc whose ends lie in $V_4\Gamma[g]$. Lemma 2.33 is in contradiction with the fact that g is nontrivial. The claim is proved.

Let c be the number of connected components of $\Gamma[g]$. From Euler's Formula, we have

$$|V\Gamma[g]|-|E\Gamma[g]|=c\,.$$

Moreover, by the Handshake Lemma,

$$2|E\Gamma[g]|=|V_1\Gamma[g]|+4|V_4\Gamma[g]|.$$

It follows that, as $|V\Gamma[g]|=|V_1\Gamma[g]|+|V_4\Gamma[g]|$,

$$2|V_4\Gamma[g]|=|V_1\Gamma[g]|-2c<|V_1\Gamma[g]|.$$

This last inequality together with Equation (2.13) generates a contradiction. In fact, recalling that $|V_2\Gamma[g]|=0$,

$$\mathrm{fpr}(E\Gamma,g)\le\frac{2\left(|F[g]|++\frac{3}{2}|V_1\Gamma[g]|\right)}{8\left(|F[g]|++\frac{3}{2}|V_1\Gamma[g]|\right)+4|V_1\Gamma[g]|+4|V_4\Gamma[g]|}<\frac{1}{4}.$$

Suppose that Remark 2.30 (ii) holds. Recall that, if two distinct vertices α and β are at distance 1 and lie in $V_4\Gamma[g]$, then g is trivial, which is a contradiction.

Thus, we can suppose, without loss of generality, that α and β are two distinct vertices in $V_4\Gamma[g]$ with $d_\Gamma(\alpha,\beta)=2$. Since

$$g \in G_\alpha^{[1]} \cap G_\beta^{[1]} \quad \text{is isomorphic to} \quad C_2\,,$$

g has order 2. This implies that $V_1\Gamma[g]$ is empty, because an involution in a local group cannot fix only one element. The condition that any two elements of $V_4\Gamma[g]$ are never adjacent implies that the number of neighbours of the vertices in $V_4\Gamma[g]$ is at most the number of edges, that is,

$$4|V_4\Gamma[g]| \le |E\Gamma[g]|.$$

As before, from the Handshake Lemma, we also have

$$2|E\Gamma[g]| \le 2|V_2\Gamma[g]| + 4|V_4\Gamma[g]|.$$

Hence

$$2|V_4\Gamma[g]| \le |V_2\Gamma[g]|.$$

Using this inequality in (2.13), we obtain

$$\mathrm{fpr}(E\Gamma, g) \le \frac{2\left(|F[g]| + 2|V_2\Gamma[g]|\right)}{6\left(|F[g]| + 2|V_2\Gamma[g]|\right) + 2|F[g]| + 4|V_4\Gamma[g]|} < \frac{1}{3}.$$

This is the final contradiction: we have, thus, proved that the only 4-valent 2-arc-transitive graph with $\mathrm{fpr}(\mathrm{Aut}(\Gamma), E\Gamma)$ exceeding 1/3 is $\mathbf{K}_5$. ■

2.G.3 Valency 3

We now turn our attention to finite connected 3-valent arc-transitive graphs. In this case, the local group is transitive, and we can use the celebrated result of Tutte concerning the structure of a vertex-stabilizer (see Theorem 1.24). Since the tools employed are analogue, the proof mimics closely the one in Section 2.G.2.

Proof of Theorem G for Γ arc-transitive. Aiming for a contradiction, let Γ be a finite connected 3-valent arc-transitive graph with

$$\mathrm{fpr}(g, E\Gamma) > \frac{1}{3}.$$

We fix a nontrivial automorphism $g \in \mathrm{Aut}(\Gamma)$, and we claim that $\Gamma[g]$ is a forest. Let s be a positive integer such that G is s-arc-transitive but not $(s+1)$-arc-transitive. Suppose that the claim is false. Then $\Gamma[g]$ contains an ℓ-cycle C. In view of Lemma 2.24, we have

$$\mathrm{girth}(\Gamma[g]) \ge \mathrm{girth}(\Gamma) \ge s+1\,.$$

Thus, we can extract an s-arc

$$\alpha_0 \sim \alpha_1 \sim \ldots \sim \alpha_{s-1}$$

from C. As g fixes this s-arc, and as Theorem 1.24 implies that $\mathrm{Aut}(\Gamma)$ is s-arc-regular, we deduce that $g = 1$ is trivial. This is a contradiction, hence $\Gamma[g]$ is a forest.

Let us start by assuming that $s \geq 2$. Moreover, by Lemma 2.28, we can assume that $\mathrm{girth}(\Gamma) \geq 5$. We let

$$\mathcal{F} := \{\alpha \in V\Gamma \mid \{\alpha, \beta\} \in F[g] \text{ for some } \beta \in V\Gamma\},$$
$$\mathcal{N} := \{\alpha \in V\Gamma - V_1\Gamma[g] \mid \{\alpha, \beta\} \in N[g] \text{ for some } \beta \in V\Gamma\}.$$

We want to give a lower bound on the number of vertices of Γ that does not depend on $|\mathcal{N}|$.

We construct an auxiliary graph Δ whose vertex-set is $V_1\Gamma[g] \cup \mathcal{N}$. We declare a vertex $\alpha \in V_1\Gamma[g]$ adjacent to a vertex $\beta \in \mathcal{N}$ if $\{\alpha, \beta\} \in E\Gamma$. By construction, Δ is bipartite with parts $V_1\Gamma[g]$ and $\mathcal{N}$. For every vertex $\alpha \in V_1\Gamma[g]$, the automorphism g acts as a 2-cycle on $\Gamma(\alpha)$. Let $\beta_1, \beta_2 \in \Gamma(\alpha)$ be the two neighbours swapped by g. Thus

$$\{\alpha, \beta_1\}, \{\alpha, \beta_2\} \in N[g] \quad \text{and} \quad \beta_1, \beta_2 \in \mathcal{N}.$$

This shows that each vertex in $V_1\Gamma[g]$ has two neighbours in $\mathcal{N}$. As $\mathrm{girth}(\Gamma) \geq 5$, we also have that $\mathrm{girth}(\Delta) \geq 5$. Hence, for any pair of distinct vertices $\alpha, \alpha' \in V_1\Gamma[g]$, the intersection $\Delta(\alpha) \cap \Delta(\alpha')$ is empty. Therefore,

$$2|V_1\Gamma[g]| \leq |\mathcal{N}|.$$

Recalling that

$$V_1\Gamma[g], \quad V_3\Gamma[g], \quad \mathcal{F}, \quad \mathcal{N}$$

is a partition of $V\Gamma$, and that $|\mathcal{F}| = 2|F[g]|$, we obtained the sought after bound

$$2|F[g]| + 3|V_1\Gamma[g]| + |V_3\Gamma[g]| \leq |V\Gamma|. \tag{2.14}$$

Let us now assume that $s = 1$. Since $\mathrm{Aut}(\Gamma)$ acts regularly on the arcs and g is nontrivial, $A[g]$ is the empty set, and thus $V_1\Gamma[g]$ and $V_3\Gamma[g]$ are also empty. Moreover, since two edges of $F[g]$ cannot be incident, $|F[g]| \leq |E\Gamma|/3$. Combining the last two observations with the Handshake Lemma for Γ, we obtain

$$2|F[g]| + 3|V_1\Gamma[g]| + |V_3\Gamma[g]| = 2|F[g]| \leq \frac{2}{3}|E\Gamma| = |V\Gamma|.$$

In particular, Equation (2.14) holds also in this scenario.

With Equation (2.14) in our hands, and recalling that $2|E\Gamma| = 3|V\Gamma|$, we obtain the upper bound,

$$\begin{aligned} \mathrm{fpr}(E\Gamma, g) &= \frac{|F[g]| + |A[g]|}{|E\Gamma|} \\ &= \frac{2|F[g]| + 2|A[g]|}{3|V\Gamma|} \\ &\leq \frac{2|F[g]| + |V_1\Gamma[g]| + 3|V_3\Gamma[g]|}{6|F[g]| + 9|V_1\Gamma[g]| + 3|V_3\Gamma[g]|}. \end{aligned} \tag{2.15}$$

Let c be the number of connected components of $\Gamma[g]$. From Euler's Formula, we have

$$|V\Gamma[g]| - |E\Gamma[g]| = c\,.$$

and, from the Handshake Lemma for $\Gamma[g]$, we have

$$2|E\Gamma[g]| = |V_1\Gamma[g]| + 3|V_3\Gamma[g]|\,.$$

Combining them,

$$|V_3\Gamma[g]| = |V_1\Gamma[g]| - 2c < |V_1\Gamma[g]|\,.$$

Finally, using Equation (2.15) and this last inequality, we obtain

$$\mathrm{fpr}(E\Gamma, g) \leq \frac{2|F[g]| + 3|V_1\Gamma[g]| + |V_3\Gamma[g]|}{6|F[g]| + 9|V_1\Gamma[g]| + 3|V_3\Gamma[g]|} - \frac{2\,(|V_1\Gamma[g] - V_3\Gamma[g])}{6|F[g]| + 9|V_1\Gamma[g]| + 3|V_3\Gamma[g]|} \leq \frac{1}{3}\,.$$

This is our final contradiction. ■

2.H Quotienting

For the remaining cases, we can set up an inductive approach similar to [112]. In broad terms, we are quotienting until we obtain a cyclic graph, and then we are proving that the only lift with the desired property is either a Praeger–Xu or a split Praeger–Xu graph.

2.H.1 Valency 4

Proof of Theorem F for Γ not 2-arc-transitive. Let Γ be a finite connected 4-valent vertex- and edge-transitive but not 2-arc-transitive graph admitting a nontrivial automorphism g fixing more than 1/3 of the edges of Γ. If Γ is isomorphic to a Praeger–Xu graph, then Theorem F *(b)* holds. Therefore, for the rest of the argument, we suppose that Γ is not isomorphic to $\mathrm{C}(r,s)$, for any choice of r and s with $r \geq 3$ and $1 \leq s \leq r-1$. Moreover, aiming for a contradiction, we suppose that Γ is a counterexample of Theorem F minimal with respect to $|V\Gamma|$, the number of vertices of Γ.

The assumption on $\mathrm{Aut}(\Gamma)$ implies that the local group is either transitive but not 2-transitive, or it defines two orbits of cardinality 2. In both cases, by Lemma 1.32, we deduce that the local group is a 2-group. As Γ is connected, it follows that, for every $\alpha \in V\Gamma$, G_α is a 2-group.

If $\mathrm{Aut}(\Gamma)$ does not have any nontrivial normal 2-subgroups, Theorem 2.12 (applied to the faithful and transitive action of $\mathrm{Aut}(\Gamma)$ on $E\Gamma$) contradicts

$$\mathrm{fpr}(g, E\Gamma) > 1/3\,.$$

Thus, $\mathrm{Aut}(\Gamma)$ has a minimal normal 2-subgroup N.

Since Γ is not isomorphic to a Praeger–Xu graph, Lemma 2.3 yields that N acts semiregularly on $V\Gamma$. Consider the quotient graph Γ/N and observe that, as G is vertex- and edge-transitive, Γ/N has valency 0, 1, 2 or 4 (see Section 1.G for a general proof of this implication).

If Γ/N has valency 0, then N is transitive on $V\Gamma$. Thus N is vertex-regular on Γ. As Γ is connected of valency 4, N is generated by at most 4 elements and hence $|V\Gamma| = |N|$ divides 2^4.

If Γ/N has valency 1, then N has two orbits on $V\Gamma$. In particular, Γ is a bi-Cayley graph, that is, a bipartite graph such that N acts regularly on both parts. Our approach here can mimic what we did for Cayley graphs: indeed, [112, Lemma 1.15] implies that $|V\Gamma| = 2|N|$ divides 2^7.

In both cases, the statement can be checked computationally by inspecting the candidate graphs from the census of all 4-valent vertex- and edge-transitive graphs of small order (see Section 1.L and [115, 119]).

If Γ/N has valency 2, then we contradict Lemma 2.4. Therefore, for the rest of the proof, we may suppose that Γ/N has valency 4.

Let K be the kernel of the action of G on $V\Gamma/N$. Since the quotient graph is 4-valent, the local group that K_α induces on $\Gamma(\alpha)$ is trivial. Hence, Lemma 1.32 implies that K_α is trivial. By Frattini's Argument,

$$K = K_\alpha N = N\,.$$

In particular, $\mathrm{Aut}(\Gamma)/N$ acts faithfully as a group of automorphisms on Γ/N. Moreover, $\mathrm{Aut}(\Gamma)/N$ acts vertex- and edge-transitively on Γ/N, but not 2-arc-transitively.

We claim that g is not an element of N. Recall that N is a normal subgroup of the edge-transitive automorphisms group. It follows that, if $g \in N$, then, by conjugating by elements of $\mathrm{Aut}(\Gamma)$, g would fix all the edges of the graph. This is impossible, because the action of $\mathrm{Aut}(\Gamma)$ is faithful. Hence, the claim is true, and $g \notin N$.

Thus Ng is not the identity automorphism of Γ/N. By Lemma 2.13, we obtain that

$$\mathrm{fpr}(Ng, E\Gamma/N) > \frac{1}{3}\,.$$

By minimality of $|V\Gamma|$, we have that Γ/N is isomorphic to either $\mathbf{K}_5$ or to a Praeger–Xu graph $\mathrm{C}(r,s)$ with $3s < 2r - 3$.

Assume that Γ/N is isomorphic to $\mathbf{K}_5$. We have that Ng is an element of $\mathrm{Aut}(\mathbf{K}_5)$ whose fixed point ratio exceeds 1/3. The only possibility for Ng is a transposition of $\mathrm{Aut}(\mathbf{K}_5) = \mathrm{Sym}(5)$. We observe that the group $\mathrm{Sym}(5)$ contains a unique conjugacy class of subgroups which are vertex- and edge-transitive, but not 2-transitive (namely, the Frobenius groups of order 20). On the other hand, such subgroups contain no transpositions. This contradiction excludes this case.

Assume that Γ/N is isomorphic to $\mathrm{C}(r,s)$, for some r and s with $3s < 2r - 3$. From Lemma 2.21, $\mathrm{Aut}(\Gamma)/N$ is $\mathrm{Aut}(\Gamma/N)$-conjugate to a subgroup of H as defined in Section 2.A. Without loss of generality, we can identify $\mathrm{Aut}(\Gamma)/N$ with such a subgroup, so that $\mathrm{Aut}(\Gamma)/N$ is a subgroup of H.

We first deal with the exceptional case $(r,s) = (4,1)$. As $\mathrm{Aut}(\Gamma)/N$ is a 2-group and N is a minimal normal subgroup of G, we deduce that $|N| = 2$, and hence

$$|V\Gamma| = |V\Gamma/N||N| = 8 \cdot 2 = 16\,.$$

The proof follows inspecting the vertex- and edge-transitive graphs of order 16.

Therefore, for the rest of the argument, we suppose $(r,s) \neq (4,1)$. Lemma 2.20 implies that

$$Ng \in K \leq H^{+}.$$

We denote by X the group $\mathrm{Aut}(\Gamma)/N \cap H^{+}$. This group is a half-arc-transitive group of automorphisms of Γ/N. Since $|H : H^{+}| = 2$, we have

$$|\mathrm{Aut}(\Gamma)/N : X| \leq 2.$$

Denote by G the preimage of X with respect to the quotient projection

$$\mathrm{Aut}(\Gamma) \to \mathrm{Aut}(\Gamma)/N$$

so that G/N is isomorphic to X. We remark that G acts half-arc-transitively on Γ, and, from $Ng \in X$, we see that $g \in G$.

By Lemma 2.20, all the edges fixed in Γ/N by Ng are fixed as arcs. Therefore, all the edges fixed in Γ by g are fixed as arcs. Considering the subgraph of Γ induced by the fixed vertices, we deduce that

$$2|\mathrm{Fix}(g, E\Gamma)| \leq 4|\mathrm{Fix}(g, V\Gamma)|.$$

Observe that, if $\mathrm{fpr}(g, V\Gamma) \leq 1/3$, then

$$\frac{1}{3} < \mathrm{fpr}(g, E\Gamma) = \frac{|\mathrm{Fix}(g, E\Gamma)|}{|E\Gamma|} \leq \frac{2|\mathrm{Fix}(g, V\Gamma)|}{|E\Gamma|} \leq \frac{2|V\Gamma|}{3|E\Gamma|} = \frac{|E\Gamma|}{3|E\Gamma|} = \frac{1}{3},$$

which is a contradiction. Therefore, $\mathrm{fpr}(g, V\Gamma) > 1/3$. We can, thus, apply Lemma 2.22 to the group G. This implies that Γ is a Praeger–Xu graph, which is our final contradiction. ■

2.H.2 Valency 3

Our last effort consists in proving Theorem G for 3-valent graphs whose local group is not transitive.

When the local group is trivial, the connectivity of Γ implies that all vertex-stabilizers are trivial, hence G acts regularly on $V\Gamma$ (as usual, see Lemma 1.32). In this case, Theorem 1.41 yields that Γ is Cayley graph over G. Theorem 2.19 states that $\mathrm{fpr}(g, E\Gamma) \leq 1/3$. Therefore, Theorem G holds in this case.

When the local group is cyclic of order 2, the situation becomes more delicate, and we are exploiting the merging operation. This calls for an *ad hoc* treatment of our beloved ladders.

Lemma 2.34 · *Let Λ be a (circular or Möbius) ladder, and let $G \leq \mathrm{Aut}(\Lambda)$ be a vertex-transitive group. Then*

$$\mathrm{fpr}(G, E\Lambda) \leq \frac{1}{3}.$$

Proof. Suppose that Λ is a circular ladder which is not isomorphic to the skeleton of the cube $\mathbf{Q}_8$. The automorphism group of Λ is isomorphic to $D_n \times C_2$ (with $n = 4$ excluded). An automorphism with some fixed edges is either a noncentral involutions of the dihedral group D_n or the involution of the central factor C_2. Thus, for each nontrivial automorphism $g \in \mathrm{Aut}(\Lambda)$, we can compute

$$\mathrm{fpr}(g, E\Lambda) \le \frac{2 \cdot (2,n)}{3n} \le \frac{2}{9}.$$

The skeleton of the cube $\mathbf{Q}_8$ (which correspond to $n = 4$) is exceptional because the graph is 2-arc-transitive. The result follows from the cases already analysed of Theorem G.

Similarly, suppose that Λ is a Möbius ladder whose vertex-set contains at least 8 points. The automorphism group of Λ is isomorphic to D_{2n}, and its involutions are the only automorphisms with a fixed edge. It can be verified that, for each nontrivial $g \in \mathrm{Aut}(\Lambda) - \{1\}$,

$$\mathrm{fpr}(g, E\Lambda) \le \frac{2 \cdot (2,n)}{3n} \le \frac{1}{3}.$$

Once again, the cases with 4 and 6 vertices are exceptional, because both of them are 2-arc-transitive. Hence, since Theorem G has been established for arc-transitive graphs, these graphs are of no concern to us here. ■

At last, we can tackle the last proportion of the proof.

Proof of Theorem G for Γ not arc-transitive. We have already discussed how the case with trivial local group reduces to Theorem 2.19. Therefore, we suppose that Γ is a connected 3-valent graph with local group isomorphic to C_2 with

$$\mathrm{fpr}(\mathrm{Aut}(\Gamma), E\Gamma) > \frac{1}{3}.$$

Moreover, Lemma 2.34 guarantees that Γ is not isomorphic to a ladder.

By Remark 2.5, we can apply the merging operation to the pair $(\Gamma, \mathrm{Aut}(\Gamma))$, and the resulting graph Δ is 4-valent and arc-transitive (but not 2-arc-transitive). Recall that, if the local group has order 2, $\mathrm{Aut}(\Gamma)$ partitions $E\Gamma$ in a perfect matching and a 2-factor, and that the merging operator maps the former in $V\Delta$ and the latter in $E\Delta$. (We recall that all the details are contained in Section 2.C.) It follows that, for every nontrivial $g \in \mathrm{Aut}(\Gamma)$,

$$\begin{aligned}\mathrm{fpr}(g, E\Gamma) &= \frac{|\mathrm{Fix}(g, V\Delta)| + |\mathrm{Fix}(g, E\Delta)|}{|V\Delta| + |E\Delta|} \\ &= \frac{|\mathrm{Fix}(g, V\Delta)|}{3|V\Delta|} + \frac{2|\mathrm{Fix}(g, E\Delta)|}{3|E\Delta|} \\ &= \frac{1}{3}\mathrm{fpr}(g, V\Delta) + \frac{2}{3}\mathrm{fpr}(g, E\Delta).\end{aligned}$$

Observe that either $\mathrm{fpr}(g, V\Delta) > 1/3$ or $\mathrm{fpr}(g, E\Delta) > 1/3$, otherwise

$$\frac{1}{3} < \mathrm{fpr}(g, E\Gamma) \le \frac{1}{3} \cdot \frac{1}{3} + \frac{2}{3} \cdot \frac{1}{3} = \frac{1}{3}.$$

Using Theorem 2.14 when $\mathrm{fpr}(g, V\Delta) > 1/3$, and using Theorem F when $\mathrm{fpr}(g, E\Delta)$ exceeding 1/3, we find that either Δ is isomorphic to a Praeger–Xu graph $\mathrm{C}(r,s)$

with $3s < 2r$, or $|V\Delta| \leq 70$. The latter case yields $|V\Gamma| \leq 140$, and the veracity of Theorem G follows with an inspection on the connected 3-valent graphs having at most 140 vertices.

Therefore, we must suppose that Δ is isomorphic to $\mathrm{C}(r,s)$. Recall that, by [115, Theorem 12], the merging operator is the right-inverse of the splitting one. In particular, the graph Γ can be uniquely reconstructed from Δ and the decomposition $\mathcal{C}$ of $E\Delta$ arising from the initial 2-factor via the splitting operation. Therefore, recalling Definition 2.23, Γ is isomorphic to $\mathrm{sC}(r,s)$, for some positive integers r and s. Finally, we observe that

$$\frac{1}{3} < \mathrm{fpr}(g, E\Gamma) \leq \frac{1}{3}\mathrm{fpr}(\tau_i, V\Delta) + \frac{2}{3}\mathrm{fpr}(\tau_i, E\Delta) = \frac{r-s}{3r} + \frac{2(r-s-1)}{3r}.$$

(The τ_i's are defined in Section 2.A.) Hence, a direct computation leads to

$$3s < 2r - 2.$$

This concludes the proof of Theorem G. ■

2.I Semiregular elements of 3-valent graphs

A permutation on the set Ω is a *derangement* if it fixes no points in Ω. A permutation is *semiregular* if all of its cycles have the same length. For instance, any derangement of prime order is semiregular.

A fascinating old-standing question in the theory of group actions on graphs is the so-called *Polycirculant Conjecture*. We recall that a permutation group G is 2-*closed* if it is the automorphism group of some of its orbital digraphs.

Question 2.35 · Does every nontrivial 2-closed transitive permutation group contain nontrivial semiregular elements?

This formulation of the conjecture has been introduced by M. Klin in [81]. However, the original question in terms of graphs has been previously posed independently by D. Marušič in [99, Problem 2.4] and by D. Jordan in [78]

Question 2.36 · Does every vertex-transitive graph having more than one vertex admit nontrivial semiregular automorphisms?

Section 2.I focuses on 3-valent graphs. D. Marušič and R. Scappellato have given a positive answer to Question 2.36 for 3-valent vertex-transitive graphs.

Theorem 2.37 ([98] Theorem 3.3) · *Each 3-valent vertex-transitive graph admits a nontrivial semiregular automorphism*

Surprisingly, their proof is essentially based on Lemma 1.32. Indeed, by a connectedness argument, the vertex-stabilizer of a 3-valent graph Γ is a $\{2,3\}$-group. If $\mathrm{Aut}(\Gamma)$ does not contain any semiregular element, then $\mathrm{Aut}(\Gamma)$ is itself a $\{2,3\}$-group. Hence, by Burnside's $p^a q^b$ Theorem, $\mathrm{Aut}(\Gamma)$ is solvable. In particular, its minimal normal subgroups are elementary abelian. A bit of extra work produces the desired contradiction.

D. Marušič's and R. Scappellato's proof does not take into account the order of the semiregular elements. In this direction, P. J. Cameron, J. Sheehan and P. Spiga have proved the following by exploiting the power of the normal quotient method.

Theorem 2.38 ([35] Theorem 3) · *Let Γ be a 3-valent vertex-transitive graph. Then $\mathrm{Aut}(\Gamma)$ contains a semiregular automorphism of order at least 3.*

The challenging cases in their analysis actually turn out to be graphs containing semiregular elements whose order is equal to the exponent of $\mathrm{Aut}(\Gamma)$. Moreover, they have conjectured as [35, Conjecture 2] that, as the number of vertices of Γ tends to infinity, the maximal order of a semiregular automorphism tends to infinity.

The conjecture is true for 3-valent Cayley and arc-transitive graphs, as proved by P. Spiga in [144, Theorem 1.2]. The keystone of his proof is the positive solution of the *Burnside Restricted Problem*. (This problem was posed by W. Magnus in [96] as a restriction to the finite case of the 1902 *Burnside Problem*.)

Question 2.39 · Let (d,e) be a pair of positive integers. Is the number of finite groups G such that $\mathbf{d}(G) \le d$ and $\exp(G) \le e$ finite?

Observe that Question 2.39 can be solved by finding an upper bound on the order of G depending upon the pair (d,e). The problem was solved by E. I. Zel'manov in [165, 166] as follows.

Theorem 2.40 · *Let (d,e) be a pair of positive integers, and let G be a finite group such that $\mathbf{d}(G) \le d$ and $\exp(G) \le e$. Then, there is a constant $\mathbf{B}(d,e)$ such that the order of $|G| \le \mathbf{B}(d,e)$. In particular, Question 2.39 has an affirmative answer.*

On the other hand, in [144] it is also shown that the conjecture of P. J. Cameron, J. Sheehan and P. Spiga is false when the local group is cyclic of order 2.

Theorem 2.41 ([144] Theorem 1.1) · *There exists an infinite family of 3-valent vertex-transitive graphs Γ_m whose local group is cyclic of order 2 such that*

$$\max\{\mathbf{o}(g) \mid g \in \mathrm{Aut}(\Gamma_m),\ g \text{ semiregular}\} = 6\,.$$

In light of these results, it is unclear whether 6 is optimal in the sense of minimizing the maximal order of a semiregular element.

Theorem H · *We have that*

$$\liminf_{\substack{|V\Gamma|\to\infty \\ \Gamma \text{ 3-valent vertex-transitive}}} \max\{\mathbf{o}(g) \mid g \in \mathrm{Aut}(\Gamma),\ g \text{ semiregular}\} = 6\,.$$

Theorem H is a consequence of the following result and Theorem 2.41.

Theorem 2.42 · *Let Γ be a connected 3-valent graph, and let G be a vertex-transitive group of automorphisms of Γ. Then either G contains a semiregular automorphism of order at least 6 or the pair (Γ, G) appears in Table 2.3.*

Following [16], Section 2.J is devoted to prove Theorem 2.42, and hence Theorem H.

2.I.1 Exceptional pairs

In Section 2.I.1, we record the exceptional pairs appearing in Theorem 2.42. If the graph Γ has less than 1 280 vertices, the information in Table 2.3 is enough to uniquely identify the pair (Γ, G). For the few outliers, we are giving some extra comments.

Let us begin by explaining the entries of Table 2.3. In the first column, we report the number of vertices of the exceptional 3-valent vertex-transitive graph Γ. In the second column, we report the order of the transitive subgroups G of $\mathrm{Aut}(\Gamma)$ with G not containing semiregular elements of order at least 6: each subgroup is reported up to $\mathrm{Aut}(\Gamma)$-conjugacy class. In the third column, we report the cardinality of $\mathrm{Aut}(\Gamma)$. In the fourth column, when the number of vertices $|V\Gamma|$ does not exceed 1 280, we report the number of the graph in the database of small 3-valent vertex-transitive graphs in [119]. Finally, in the fifth column of Table 2.3, we write the symbol ✓ when the graph is arc-transitive, and the symbol † when the graph is a split Praeger–Xu graph.

The fourth column of Table 2.3 contains a hyphen when the number of vertices $|V\Gamma|$ exceeds 1 280. Here we report some comments to guide the understanding of these last graphs.

(*a*) The graph with 2 560 vertices is the canonical double cover of the graph with 1 280 vertices.

(*b*) The graphs with 6 250 vertices are two nonisomorphic covers of the graph with 1 250 vertices: these graphs are covers of the Petersen graphs (the graph with 10 vertices of database number 3), which is the source of almost all our exceptions.

(*c*) The graphs with 31 250 vertices are five nonisomorphic covers of the graphs with 6 250 vertices: these graphs are covers of the Petersen graph.

(*d*) The graph with 65 610 vertices is a cover of the graph with 810 vertices, and, due to computational limitation, we cannot establish how large its automorphism group is.

(*e*) The graphs with $2 \cdot 5^{\ell}$ vertices, with $7 \leq \ell \leq 34$, are covers of graphs with $2 \cdot 5^{\ell-1}$ vertices, the smaller one being a cover of a graph with 31 250 vertices: these graphs are covers of the Petersen graph, we can describe their automorphism groups, but we do not know which is the maximum ℓ that can appear (the upper bound we give is a theoretical bound obtained from the upper bound to the size of a 2-generated group of exponent 5, see [66]).

2.J Proof of Theorem H

As we have pointed out in Section 2.I, Theorem H is a corollary of Theorems 2.41 and 2.42. Therefore, our objective here is to prove Theorem 2.42.

First, we remark that we can use a calculator to deal with the small exceptions (see Section 1.L).

$\lvert V\Gamma\rvert$	$\lvert G\rvert$	$\lvert\mathrm{Aut}(\Gamma)\rvert$	DB	✓ / †	$\lvert V\Gamma\rvert$	$\lvert G\rvert$	$\lvert\mathrm{Aut}(\Gamma)\rvert$	DB	✓ / †
4	4, 4, 8, 12, 24	24	1	✓	24	24, 24	48	11	†
6	6	12	1		30	720	1 440	8	✓
	6, 36	24	2	✓		60, 120	120	9	
8	8	16	1			60	60	10	
	8, 8, 8, 8, 16, 24, 24, 48	48	2	✓	32	32	64	2	
10	10	20	1			32, 32, 64, 64	128	3	†
	10	20	2			32, 96	192	4	✓
	20, 60, 120	120	3	✓	36	36	72	9	
12	12, 24	24	2		40	160, 160	320	12	†
	24, 24	48	4	†	50	100	200	7	
16	16, 16, 32, 32, 64, 64	128	2	†		50, 150	300	8	✓
	16	32	3		54	108	216	11	
	16, 48	96	4	✓	60	60	360	2	✓
18	18, 108	216	4	✓		60, 120	120	3	
	36	72	5			60	60	4	
20	20	20	2			60	120	5	
	160, 160	320	3	†		60	120	6	
	60	120	6	✓		60, 120	120	7	
	120	240	7	✓		60	120	8	
24	24	144	2	✓		60	120	9	
	24	48	8			60	120	10	
	24	24	9		64	64, 192	384	2	✓
	24	48	10			64	256	4	

Table 2.3: Exceptional cases for Theorem 2.42

$\lvert V\Gamma\rvert$	$\lvert G\rvert$	$\lvert\mathrm{Aut}(\Gamma)\rvert$	DB	✓ / †	$\lvert V\Gamma\rvert$	$\lvert G\rvert$	$\lvert\mathrm{Aut}(\Gamma)\rvert$	DB	✓ / †
64	64, 64	128	11	†	360	360	181		
80	80, 160	160	29			360	720	182	
	160, 160	320	31	†		360	720	183	
90	720	1 440	20			360	720	184	
96	96	192	37			360	720	185	
100	100	200	19			720	1 440	268	
128	128	256	5			720	1 440	270	
160	160	160	89		512	512	1 024	734	
	160	160	90		810	1 620	1 620	198	
	160	320	91		1 024	1 024, 3 072	6 144	3 470	✓
	160	320	92		1 250	2 500	2 500	187	
	160	320	93	†	1 280	1 280	2 500	2 591	
	160	320	94		2 560	2 560	5 120	–	
180	720		77		6 250	12 500	25 000	–	
	360, 720		78			12 500	12 500	–	
250	500		31		31 250	62 500	125 000	–	
256	256, 768		30	✓		62 500	125 000	–	
360	360	720	176			62 500	125 000	–	
	360	720	177			62 500	62 500	–	
	360	720	178			62 500	62 500	–	
	360	360	179		65 610	131 220	?	–	
	360	720	180		$2\cdot 5^{\ell}$	$4\cdot 5^{\ell}$	$*7 \le \ell \le 34$	–	

Table 2.3: Exceptional cases for Theorem 2.42 (continued)

Remark 2.43 · The veracity of Theorem 2.42 for graphs with at most 1 280 vertices has been proven computationally using the database of small 3-valent vertex-transitive graphs in [119]. Therefore, in the course of the proof of Theorem 2.42 whenever we reduce to a graph having at most 1 280 vertices we simply refer to this computation.

We will ease into the proof with two preliminary results. Recall that a p-*element* is an element of a group whose order is a power of the prime p.

Lemma 2.44 · *Let G be a permutation group on Ω, and let p be a prime. If all the elements of G of order p are derangements, then all p-elements of G are semiregular.*

Proof. Let $g \in G$ be an element of order p^k, for some positive integer k. Aiming for a contradiction, assume that g is not semiregular, that is, there exists $\alpha \in \Omega$ such that

$$|\alpha^{\langle g\rangle}| \le p^{k-1}.$$

Hence $g^{p^{k-1}}$ fixes α, which implies $g^{p^{k-1}}$ is not a derangement, a contradiction. ∎

Lemma 2.45 · *Let G be a permutation group acting on Ω, and let p and q be two distinct primes. If G has a semiregular element g of order p and a semiregular element h of order q with $gh = hg$, then gh is a semiregular element of order pq.*

Proof. Since g and h commute, $\mathbf{o}(gh) = pq$, and hence it remains to prove that gh is semiregular. Note that $(gh)^p = h^p$ is semiregular, and also $(gh)^q = g^q$ is semiregular. Therefore, each orbit of $\langle gh\rangle$ has size pq, proving that gh is semiregular. ∎

We can now tackle the proof of Theorem 2.42.

Proof of Theorem 2.42. We argue by contradiction, thus assuming the following.

Hypothesis 2.46 · Let (Γ, G) be a connected 3-valent vertex-transitive graph which is a minimal counterexample to Theorem 2.42, first with respect to the cardinality of $V\Gamma$, and then to the order of G. From Remark 2.43, we have $|V\Gamma| > 1\,280$. Moreover, let α be an arbitrary vertex of Γ, and let N be a minimal normal subgroup of G.

Since Γ is connected, by Lemma 1.32, the stabilizer G_α is a $\{2,3\}$-group. Moreover, G must be a $\{2,3,5\}$-group, otherwise we can find derangements of prime order at least 7, hence semiregular elements.

Since N is a minimal normal subgroup of G, N is a direct product of simple groups, any two of which are isomorphic. By our previous discussion, N is a $\{2,3,5\}$-group, and N_α is a $\{2,3\}$-group. Thus N is a direct product S^ℓ, for some positive integer ℓ and for some simple $\{2,3,5\}$-group S. Using the Classification of Finite Simple Groups, we see that the collection of simple $\{2,3,5\}$-groups consists of

$$C_2,\quad C_3,\quad C_5,\quad \mathrm{Alt}(5),\quad \mathrm{Alt}(6),\quad \mathrm{PSp}(4,3).$$

(We refer, for instance, to [87].)

Lemma 2.47 · *Under Hypothesis 2.46, if N_α is a 2-group (eventually trivial), then N is an elementary abelian p-group, for some prime $p \in \{2,3,5\}$.*

Proof. If N is abelian, then there is nothing to prove. Thus, suppose that $N = S^\ell$, where

$$S \in \{\mathrm{Alt}(5), \mathrm{Alt}(6), \mathrm{PSp}(4,3)\} \quad \text{and} \quad \ell \geq 1\,.$$

Assume $\ell \geq 2$. Let S and T be two distinct direct factors of N. Then S_α and T_α are 2-groups, because so is N_α. Thus, by Lemma 2.44, all the 3- and 5-elements of S and T are semiregular. Applying Lemma 2.45, we obtain that $S \times T$, contains a semiregular element of order 15. Thus G contains a semiregular element of order exceeding 6, contradicting Hypothesis 2.46.

Assume $\ell = 1$. If $N = \mathrm{PSp}(4,3)$, then Lemma 2.44 implies that the 3-elements in N are semiregular. As $\mathrm{PSp}(4,3)$ contains elements of order 9, G contains a semiregular element of order 9, contradicting Hypothesis 2.46. Thus, N is either $\mathrm{Alt}(5)$ or $\mathrm{Alt}(6)$.

We claim that G is almost simple, that is, N is the unique minimal normal subgroup of G. Aiming for a contradiction, let M be a minimal normal subgroup of G distinct from N. If Γ/M is a 3-valent graph, then $M_\alpha = 1$, and hence each element of M is semiregular. Since $[N,M] = 1$, by Lemma 2.45, G contains a semiregular element of order at least 10, against Hypothesis 2.46.

On the other hand, suppose that Γ/M is not 3-valent. Regardless of the valency of Γ/M, the group that G induces in its action on the vertices of Γ/M is a subgroup of a dihedral group, hence such a permutation group is soluble. It follows that, as N is a nonabelian simple group, N acts trivially on the vertices of Γ/M. This means that N fixes setwise each M-orbit. Recall that, by Lemma 1.2, if $X \leq \mathrm{Sym}(\Omega)$ is an abelian group and X acts regularly on Ω, then X coincides with its centralizer in $\mathrm{Sym}(\Omega)$, that is, $X = \mathbf{C}_{\mathrm{Sym}(\Omega)}(X)$. If M is abelian, then M acts regularly on each of its orbits. However, as N commutes with M and fixes each M-orbit, this contradicts the fact that N is not abelian.

Therefore, M is not abelian. In particular, there is a prime $p \geq 5$ that divides the order of M, and the elements of M of order p are semiregular. As before, applying Lemma 2.45, we get that NM contains a semiregular element of order $3p$, a contradiction. We conclude that N is the unique minimal normal subgroup of G.

Therefore, we are left with few possibilities: either $\mathrm{Alt}(5) \leq G \leq \mathrm{Sym}(5)$, or $\mathrm{Alt}(6) \leq G \leq \mathrm{Aut}(\mathrm{Alt}(6))$. An explicit calculator-assisted computation in each of these cases shows that, if $G \leq \mathrm{Aut}(\Gamma)$ has no semiregular elements of order at least 6, then

$$|V\Gamma| \in \{30, 60, 90, 180, 360\}\,,$$

which contradicts Hypothesis 2.46. ■

From here on, we divide the proof in the following cases:

(*a*) G_α is trivial (see Section 2.J.1);

(*b*) G_α is not trivial, and Γ/N contains either 1 or 2 vertices (see Section 2.J.2);

(*c*) G_α is not trivial, and Γ/N is a cycle of length at least 3 (see Section 2.J.3);

(*d*) G_α is not trivial, and Γ/N is a 3-valent graph (see Section 2.J.4).

2.J.1 Cayley graphs

Some obstructions in the following cases of the proof can be avoided if we pre-emptively deal with case with trivial vertex-stabilizer. This problem is essentially group-theoretic, as we need to analyse all the groups which admit a 3-valent connected Cayley graph and whose elements have orders bounded from above by 5.

Suppose that G_α is trivial, and hence, by Theorem 1.41, Γ is a Cayley graph over G. Let S be an inverse-closed subset of G such that Γ is isomorphic to $\mathrm{Cay}(G,S)$. Since Γ has valency 3, we have $|S| = 3$. Moreover, since Γ is connected, we have that G is generated by S. In particular, G is generated by at most 3 elements. More precisely, either S consists of three involutions, or S consists of an involution and an element of order greater than 2 together with its inverse.

Property $\mathcal{P}$ · We say that a finite group X satisfies Property $\mathcal{P}$ if X is generated by either three involutions, or by an involution and by an element of order greater than 2.

In particular, G satisfies Property $\mathcal{P}$.

As every element of G is semiregular, and as G has no semiregular elements of order at least 6, we deduce that each element of G has order at most 5. As customary, we let

$$\omega(G) := \{\mathbf{o}(g) \mid g \in G\}$$

be the *spectrum of* G. Observe that

$$\{1,2\} \subseteq \omega(G) \subseteq \{1,2,3,4,5\}.$$

Since G is generated by at most 3 elements, we deduce from Theorem 2.40, Zel'manov's solution of the restricted Burnside problem, that $|G|$ is bounded above by an absolute constant. We divide the proof depending on $\omega(G)$.

Assume $\omega(G) = \{1,2\}$. In this case, G is elementary abelian. Since G is generated by at most 3 elements, we deduce $|G| \le 8$, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,3\}$. The groups having spectrum $\{1,2,3\}$ are classified in [107]. If we only consider groups with Property $\mathcal{P}$, the list in [107, Theorem] boils down to two possibilities: G is isomorphic either to $(C_2 \times C_2) \rtimes C_3$ (where the elements of order 3 cyclically permutes the elements of order 2 in $C_2 \times C_2$), or to $\mathrm{Sym}(3)$. Hence, we obtain that $|G| \le 12$, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,4\}$. We need to consider two cases: either G is generated by an element of order 2 and an element of order 4, or G is generated by three involutions. We resolve both cases with the aid of a computer.

Suppose first that G is generated by an involution and by an element of order 4. We consider the free group $F := \langle x,y \rangle$. We can construct the set W of words in x,y of length at most 6, and then we can construct the finitely presented group

$$\bar{F} := \langle F \mid x^2 = y^4 = w^4 = 1, \forall w \in W \rangle.$$

We use the *bar notation* for the projection of F onto $\bar{F}$. Now, $\bar{x}$ has order 2 and $\bar{y}$ has order 4. Furthermore, each element of $\bar{F}$ that can be written as a word in $\bar{x}$

and $\bar{y}$ of length at most 6 has order at most 4. The number 6 is a magic number: for our purposes, it needs to be large enough to guarantee that $\bar{F}$ has a bounded cardinality, but not too large to exceed the memory limit of our computer. (Further tests have showed that any number from 3 to 6 are such that $\bar{F}$ is a finite group, and its order is always 64, while $\bar{F}$ is infinite if we only force words of length 1 and 2 to have order 4.) With the aid of a calculator, we can see that $\bar{F}$ has order 64 and exponent 4. This proves that the largest group of exponent 4 and generated by an involution and by an element of order 4 has order 64. Now, G is a quotient of $\bar{F}$, and hence $|G| \le |\bar{F}| \le 64$. This contradicts Hypothesis 2.46.

Now, suppose that G is generated by three involutions. The argument here is very similar. We consider the free group $F = \langle x, y, z \rangle$, and we can build the set W of words in x, y, z of length at most 6. Once again, the magic number 6 works for bounding the order of $\bar{F}$. (Further computation showed that if we change 5 for 6 we obtain the same result, while any number lesser or equal to 4 exceeds the memory of our computer). Indeed, we can verify that

$$\bar{F} := \langle F \mid x^2 = y^2 = z^2 = w^4 = 1, \forall w \in W \rangle$$

has order 1 024 and exponent 4. This shows that $|G| \le |\bar{F}| \le 1\,024$, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,5\}$. The groups having spectrum $\{1,2,5\}$ are classified in [108]. As G satisfies Property $\mathcal{P}$, we have that G can be written as $V \rtimes P$, where V is an elementary abelian p-group, with $p \in \{2,5\}$, and P is a cyclic group of order q, with $q \in \{2,5\} - \{p\}$, whose action on V is irreducible. In particular, we have that $|G| \le 80$, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,3,4\}$. The groups having spectrum $\{1,2,3,4\}$ are classified in [21]. The list of groups in [21, Theorem] consists of

(i) $G = N \rtimes C_3$, where N has exponent 4 and nilpotency class at most 2,

(ii) $G = (C_2 \times C_2)^\ell \rtimes \mathrm{Sym}(3)$, with $\ell \in \mathbb{N}$,

(iii) $G = (C_3 \times C_3)^\ell \rtimes C_4$, with $\ell \in \mathbb{N}$.

As above, since G satisfies Property $\mathcal{P}$, the list shortens significantly.

To deal with part (i), we can use the same approach as the one we have used for $\omega(G) = \{1,2,4\}$. We take the free group $F = \langle x, y, z, t \rangle$, and we consider the set W of all the words in the alphabet $\{x, y, z\}$ of length 9. (We have not performed any test to verify that this choice is optimal.) We define the quotient

$$\bar{F} := \langle F \mid x^2 = y^2 = z^2 = w_i^4 = [[w_1, w_2], w_3] = t^3 = x^t y = y^t z = z^t x = 1, \forall w_i \in W \rangle.$$

We can verify that $|\bar{F}| = 96$. Hence, every G arising in part (i) does not satisfy Hypothesis 2.46.

We now consider part (ii) and (iii). Here, G is a *crown-based product* (we refer to [92] for the definition and a review of related topics). A rich theory has been developed to compute the number of generators of a crown-based product (see [92, Theorem 3]). Our application is limited enough that we can deal with these cases with a calculator. Indeed, observe that every group $V^\ell \rtimes K$ projects onto

$V^{\ell-1} \rtimes K$. It follows that the number of generators for the former is at least the number of generators of the latter. Hence, we can compute the minimal integer ℓ_0 such that the number of generator exceeds what Property $\mathcal{P}$ prescribes. For part (ii) we find $\ell_0 = 3$, while for part (iii) $\ell_0 = 2$. Therefore, we have only 3 possibilities for G. In particular, $|G| \leq 96$,, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,4,5\}$. The groups having spectrum $\{1,2,4,5\}$ are classified in [105]. This case is sligthly more involved, and hence we need to give more details. The three cases to consider are the following.

(i) $G = T \rtimes D_{10}$ where T is a nontrivial elementary abelian normal 2-subgroup and D_{10} is the dihedral group of degree 5,

(ii) $G = F \rtimes T$ where F is an elementary abelian normal 5-subgroup and T is isomorphic to a subgroup of the quaternion group Q_8,

(iii) G contains a normal 2-subgroup T which is nilpotent of class at most 6 such that G/T is a 5-group.

Suppose Item (i) holds. Here, T is a module for D_{10} over the field $\mathbb{F}_2$. The dihedral group D_{10} has two irreducible modules over $\mathbb{F}_2$ up to equivalence: the trivial module and a 4-dimensional module W. Since G has no elements of order 10, we deduce that T is isomorphic to W^ℓ, for some $\ell \geq 1$. Once again, this is a crown-based product. We can verify with a calculator-aided computation that $W^3 \rtimes D_{10}$ does not satisfy Property $\mathcal{P}$, and hence G is isomorphic to $W^\ell \rtimes D_{10}$ with $\ell \leq 2$. In particular,

$$|G| = |V\Gamma| \in \{10 \cdot 16, 10 \cdot 16^2\} = \{160, 2\,560\}.$$

From Hypothesis 2.46, we have that $|V\Gamma| > 1\,280$, and hence G is isomorphic to $W^2 \rtimes D$. By constructing all connected 3-valent Cayley graphs over $W^2 \rtimes D$, we find that there is a single one up to isomorphism. Therefore, we obtain the graph in Table 2.3 having 2 560 vertices.

Suppose Item (ii) holds. Since G satisfies Property $\mathcal{P}$, while the quaternion group of order 8 does not, we deduce that T is cyclic of order 4. Thus $G = F \rtimes \langle x \rangle$, for some x having order 4. As G satisfies Property $\mathcal{P}$, this means that $G = \langle x, y \rangle$, for some involution y. Note that $y = fx^2$ for some $f \in F$. As

$$G = \langle x, y \rangle = \langle x, fx^2 \rangle = \langle x, f \rangle,$$

we have that

$$F = \langle f, f^x, f^{x^2}, f^{x^3} \rangle.$$

Since $y = fx^2$ has order 2 and x has order 4, we deduce that

$$1 = y^2 = fx^2fx^2 = ff^{x^2},$$

that is, $f^{x^2} = f^{-1}$. Now,

$$F = \langle f, f^x, f^{x^2}, f^{x^3} \rangle = \langle f, f^x, f^{-1}, (f^x)^{-1} \rangle = \langle f, f^x \rangle.$$

Thus, as F is elementary abelian, $|F| \leq 25$. Therefore, $|G| \leq 100$, which contradicts Hypothesis 2.46.

Suppose Item *(iii)* holds. Since G satisfies Property $\mathcal{P}$, we deduce that G/T is cyclic of order 5. Thus $G = T \rtimes \langle x \rangle$, for some x having order 5. This means that $G = \langle x, y \rangle$ for some involution y. By assumption, $y \in T$. Let N be a minimal normal subgroup of G. We have $N \leq T$ and N is an irreducible $\mathbb{F}_2\langle x \rangle$-module. The cyclic group of order 5 has two irreducible modules over $\mathbb{F}_2$ up to equivalence: the trivial module and a 4-dimensional module. Since G has no elements of order 10, x does not centralize N, and hence N is the irreducible 4-dimensional module for the cyclic group of order 5. In particular, $|N| = 2^4$.

Consider $\bar{G} := G/N$. Observe that

$$\{1,2,5\} \subseteq \omega(\bar{G}) \subseteq \omega(G) = \{1,2,4,5\}.$$

Assume $\omega(\bar{G}) = \{1,2,5\}$. From the discussion above regarding the finite groups having spectrum $\{1,2,5\}$ and satisfying Property $\mathcal{P}$, we have $|\bar{G}| \leq 80$ and hence $|G| = |G : N||N| \leq 80 \cdot 16 = 1\,280$. Recall that, from Hypothesis 2.46, we have $|G| = |V\Gamma| > 1\,280$. Thus, we have found a contradiction.

Therefore, $\omega(\bar{G}) = \{1,2,4,5\}$. Since (Γ, G) was chosen minimal in Hypothesis 2.46, we have $|\bar{G}| \leq 1\,280$. Therefore the quotient graph $(\Gamma/N, \bar{G})$ appears in Table 2.3. A direct inspection on the groups appearing in this table shows that there is only one group having spectrum $\{1,2,4,5\}$, and it is the group of order $1\,280$. Thus we know precisely $\bar{G}$. Now, the group G is an extension of $\bar{G}$ by N. With the aid of a computer-assisted calculation, we can compute all the extensions E of $\bar{G}$ via N. Then, we can verify that none of the extensions E has the property that $\omega(E) = \{1,2,4,5\}$ while satisfying Property $\mathcal{P}$. This concludes this scenario.

Assume $\omega(G) = \{1,2,3,5\}$. The main result of [102] states that, if G is a group sharing the same spectrum as $\mathrm{PSL}_2(2^f)$, with $f \geq 2$, then G and $\mathrm{PSL}_2(2^f)$ are isomorphic. Therefore, it follows that the unique group having spectrum $\{1,2,3,5\}$ is $\mathrm{Alt}(5) \cong \mathrm{PSL}_2(4)$. In particular, $|G| = 60$, which contradicts Hypothesis 2.46.

Assume $\omega(G) = \{1,2,3,4,5\}$. The groups having spectrum $\{1,2,3,4,5\}$ are classified in [21]. We deduce from [21, Theorem] that G is isomorphic to either $\mathrm{Alt}(6)$ or to $V^\ell \rtimes \mathrm{Alt}(5)$ where V is a 4-dimensional natural module over the finite field of size 2 for $\mathrm{Alt}(5) \cong \mathrm{PSL}_2(4)$ and $\ell \geq 1$. The group $V^2 \rtimes \mathrm{Alt}(5)$ does not satisfy Property $\mathcal{P}$ (this can be verified with a computer). Therefore, G is either $\mathrm{Alt}(6)$ or $G \cong V \rtimes \mathrm{Alt}(5)$. Thus $|G| = |V\Gamma| \leq 960$, which contradicts Hypothesis 2.46.

2.J.2 Small quotients

We need to tackle the case where the quotient Γ/N contains either a single vertex or a single edge. In all cases, our approach consists in showing that the graph Γ is small enough, and we can find the orders of its semiregular elements with the aid of a computer

Suppose that Γ/N is a single vertex. It follows that N is transitive on $V\Gamma$. By Hypothesis 2.46, (Γ, G) is a minimal counterexample. This minimality and the fact that N is transitive on $V\Gamma$ imply that $G = N$. As N is a minimal normal subgroup of G, we have that G is simple. Thus

$$G \in \{\mathrm{Alt}(5), \mathrm{Alt}(6), \mathrm{PSp}(4,3)\}.$$

A calculator-assisted computation in each of these cases shows that, if $G \le \mathrm{Aut}(\Gamma)$ has no semiregular elements of order at least 6, then

$$|V\Gamma| \in \{10, 20, 30, 60, 90, 180, 360\},$$

which contradicts Hypothesis 2.46.

Suppose that Γ/N is an edge. We have that N defines two orbits on $V\Gamma$. We need to further divide our discussion according to N being abelian or not.

Assume that N is abelian. By [112, Lemma 1.15], either Γ is complete bipartite, or Γ is a bi-Cayley graph over N and the minimal number of generators of N is at most 4. Once again, what is really relevant is the fact that, by [112, Lemma 1.15], N is generated by at most 4 elements. Recalling that N is a $\{2,3,5\}$-group, it follows that

$$|V\Gamma| = 2|N| \le 2 \cdot 5^4 = 1\,250,$$

and the equality is realized for $N = C_5^4$. In particular, this contradicts Hypothesis 2.46.

Assume that N is not abelian. By Lemma 2.47, 3 divides the order of N_α. *A fortiori*, 3 divides the order of G_α, hence G acts arc-transitively on Γ. We can extract information on the local group of G by consulting the amalgams in [47, Section 4]. In particular, with a direct inspection (on a case-by-case basis) on these amalgams, it can be verified that, for any edge $\{\alpha,\beta\}$ of Γ, G contains an element y that swaps α and β and its order is either 2 or 4. As α and β belong to distinct N-orbits, y maps α^N to β^N. Moreover, as N has two orbits on $V\Gamma$, the subgroup $N\langle y\rangle$ is vertex-transitive on Γ. Therefore, by minimality of G, we have $G = N\langle y\rangle$. We split the discussion according to the order of y.

Suppose that $\mathbf{o}(y) = 2$. Thus $|G : N| = 2$. As $N = S^\ell$ is a minimal normal subgroup of G, $\ell \in \{1,2\}$. If $\ell = 1$, then G is an almost simple group whose socle is either $\mathrm{Alt}(5)$, $\mathrm{Alt}(6)$ or $\mathrm{PSp}(4,3)$. by the same computation we did for the simple case, (Γ, G) satisfies Theorem 2.42, a contradiction. If $\ell = 2$, then $\langle y\rangle$ permutes transitively the two simple direct factors of N. Let $s \in N$ be a 5-element in a simple direct factor of N, and notice that $t := s^y$ is a 5-element in the other simple direct factor of N. Thus $[s,t] = 1$. We claim that ys is a semiregular element of order 10. We get

$$(ys)^2 = ysys = ts \in N,$$
$$(ys)^5 = ysysysysys = ys(ts)^2 \in yN.$$

We have that $(ys)^2$ is a 5-element in N, thus semiregular, and that $(ys)^5$ has order 2 and, being an element of $yN = Ny$, it has no fixed points, hence it is semiregular. Therefore ys is a semiregular element of order 10, contradicting Hypothesis 2.46.

Suppose that $\mathbf{o}(y) = 4$. As $|G : N| = 4$ and $N = S^\ell$ is a minimal normal subgroup of G, $\ell \in \{1,2,4\}$. Observe that, since Γ is 3-valent and G is arc-transitive, we can apply Theorem 1.24. It follows that a Sylow 3-subgroup of G_α has order 3. Let $x \in G_\alpha$ be an element of order 3. As $|G : N| = 4$, we have that

$$x \in N \cap G_\alpha = N_\alpha \le S^\ell .$$

In particular, we may write $x = (s_1, \dots, s_\ell)$, for some $s_i \in S$. Let κ be the number of coordinates of x different from 1, we call κ the *type of* x. Since $\langle x \rangle$ is a Sylow 3-subgroup of G_α, from Sylow's Theorem, we deduce that each element of order 3 in G fixing some vertex of Γ has type κ. Let $s \in S$ be an element of order 3 and let $t \in S$ be an element of order 5. We consider some easy to deal with cases. Suppose that $\ell = 4$. If $\kappa \ne 1$, then $g = (s, t, 1, 1)$ has order 15 and it is semiregular, because $g^5 = (s^5, 1, 1, 1)$ has order 3 but it is not of type κ. Similarly, if $\ell = 4$ and $\kappa = 1$, then $g = (s, s, t, 1)$ has order 15 and it is semiregular. Analogously, when $\ell = 2$, if $\kappa \ne 1$, then $g = (s, t)$ has order 15 and is semiregular. When $\ell = 2$, $\kappa = 1$ and $S = \mathrm{PSp}(4, 3)$, the group S contains an element r having order 9, and hence $g = (r, r)$ is a semiregular element having order 9.

Summing up, from these reductions, we may suppose that either $\ell = 1$, or $\ell = 2$ and $S \in \{\mathrm{Alt}(5), \mathrm{Alt}(6)\}$. These cases can also be dealt with a computer. Hence, the invaluable help of a calculator shows that no counterexample to Theorem 2.42 arises.

2.J.3 Cyclic quotients

In this section, we deal with the cases where Γ/N is a cycle. This scenario contains the most involved proportion of the proof.

Suppose that Γ/N is a cycle of length $r \ge 3$. The automorphism group of Γ/N is the dihedral group of order $2r$. Let K be the kernel of the action of G on the N-orbits. The quotient G/K acts faithfully on Γ/N, that is, it is a transitive subgroup of the dihedral group of order $2r$.

We claim that

$$G/K \quad \text{is regular in its action on the vertices of} \quad \Gamma/N . \tag{2.16}$$

Assume G/K acts on the vertices of Γ/N transitively but not regularly. In particular, G/K is isomorphic to the dihedral group of order $2r$. Thus, by the Correspondence Theorem, G has an index 2 subgroup M such that M is vertex-transitive and M/K is isomorphic to the cyclic group of order r. By minimality of G, we have $G = M$, which goes against the choice of M. Hence G/K is regular. In particular, either G/K is isomorphic to the cyclic group of order r, or r is even and G is isomorphic to the dihedral group of order r. (Later in this proof we resolve this ambiguity and we prove that r is even and G/K is dihedral of order r, see Equation (2.20).)

As G/K acts regularly on the vertices of Γ/N, we have

$$1_{G/K} = (G/K)_{\alpha^N} = G_\alpha K/K .$$

Therefore

$$K_\alpha = K \cap G_\alpha = G_\alpha . \tag{2.17}$$

Aiming for a contradiction, assume G is arc-transitive. Let β be a neighbour of α. We claim that $G = \langle G_\alpha, G_{\{\alpha,\beta\}}\rangle$. We note that, by arc-transitivity, $G_{\{\alpha,\beta\}}$ contains an *edge-flip*, that is, a permutation $g \in G$ such that $(\alpha,\beta)^g = (\beta,\alpha)$. It follows that $\langle G_\alpha, G_{\{\alpha,\beta\}}\rangle$ contains G_β. Hence, Lemma 3.2 implies $\langle G_\alpha, G_{\{\alpha,\beta\}}\rangle$ defines either one or two orbit on the vertices. Moreover, if it defines two orbits, then the orbits of α and β would be disjoint, which goes against the existence of an edge-flip. Therefore, $\langle G_\alpha, G_{\{\alpha,\beta\}}\rangle$ is transitive, and, since it contains a vertex-stabilizer, by Frattini's Argument, $G = \langle G_\alpha, G_{\{\alpha,\beta\}}\rangle$.

We can thus consider the following chain of inclusions

$$G = \langle G_\alpha, G_{\{\alpha,\beta\}}\rangle = \langle K_\alpha, G_{\{\alpha,\beta\}}\rangle \le \langle K, G_{\{\alpha,\beta\}}\rangle = KG_{\{\alpha,\beta\}}\,.$$

Hence, as both K and $G_{\{\alpha,\beta\}}$ are subgroups of G, $G = KG_{\{\alpha,\beta\}}$. Observe that α^N and β^N are distinct N-orbits. Recalling that K fixes all the N-orbits,

$$|G:K| = |KG_{\{\alpha,\beta\}} : K| = |G_{\{\alpha,\beta\}} : K_{\{\alpha,\beta\}}| = |G_{\{\alpha,\beta\}} : G_{\alpha\beta}| = 2\,.$$

Thus G/K is the cyclic group of order 2 and $r = 2$, which is a contradiction.

Therefore, G is not arc-transitive. This implies that G_α does not act transitively on the neighbourhood of α. Thus, by Lemma 1.32, G_α is a 2-group. By Equation (2.17), we deduce that $G_\alpha = K_\alpha$ is a 2-group. Actually, Lemma 2.11 shows that

$$G_\alpha = K_\alpha \quad \text{is an elementary abelian 2-group}\,. \tag{2.18}$$

If N is an elementary abelian 2-group, then, by Lemma 2.10, Γ is either a circular ladder, or a Möbius ladder, or a split Praeger–Xu graph $\mathrm{sC}(r/2,s)$. We can explicitly compute the order of the semiregular elements in both scenarios.

Lemma 2.48 · *Let Λ be a (circular or Möbius) ladder, and let $G \le \mathrm{Aut}(\Lambda)$ be a vertex-transitive group. Then either $|V\Lambda| \le 16$ or G contains a semiregular element of order at least* 6.

Proof. Recalling the definition of the ladders, under the assumption that $|V\Lambda| \ge 10$, we have that $\mathrm{Aut}(\Lambda)$ contains a unique abelian regular subgroup of index 2. We call such subgroup H, and we note that H contains a semiregular element of order $|V\Lambda|/2$. Moreover, for every vertex-transitive subgroup $G \le \mathrm{Aut}(\Lambda)$, we have that $G \cap H$ has index at most 2 in H. It follows that G must contain the square of a semiregular element of order $|V\Lambda|/2$ in H. Therefore, if $|V\Lambda| \ge 24$, we can find in G an element with the desired property. To close the gap between 10 and 24, we can just invoke Remark 2.43. ■

Lemma 2.49 · *Let G be a vertex-transitive subgroup of $\mathrm{Aut}(\mathrm{sC}(r,s))$. Then either G contains a semiregular element of order at least* 6, *or* $(\mathrm{sC}(r,s), G)$ *is one of the examples in Table 2.3 marked with the symbol* †.

Proof. We use the notation for the automorphism group of $\mathrm{Aut}(\mathrm{sC}(r,s))$ developed in Section 2.A. From Lemma 2.9, we have that G is a subgroup of $H = K \rtimes \langle \rho, \sigma\rangle$. Observe that

$$G/G\cap K \quad \text{is isomorphic} \quad \langle \rho,\sigma\rangle,$$

otherwise G is not transitive on the vertices of the split graph $\mathrm{sC}(r,s)$. From this, it follows that

$$G = V \rtimes \langle \rho f, \sigma g \rangle,$$

for some $f,g \in K$, where $V = G \cap K$. Since ρ has order r, we get that

$$\begin{aligned}(\rho f)^r &= \rho f \rho \dots (\rho f \rho) f \\ &= \rho f \rho \dots (\rho^2 \rho^{-1} f \rho) f \\ &= \rho f \rho \dots \rho^2 f^{\rho} f \\ &= \rho f \rho^{r-1} \dots f^{\rho} f \\ &= f^{\rho^{r-1}} \dots f^{\rho} f\end{aligned}$$

is an element of V. Since V is an elementary abelian 2-group, the element ρf has order either r or $2r$. Recalling that V is a subgroup of K,

$$(\rho f)^r = \prod_{i=0}^{r-1} \tau_i^{a_i}$$

with $a_i \in \{0,1\}$. Furthermore,

$$\begin{aligned}(\rho f)^r \rho &= \rho (f \rho \dots \rho f \rho f \rho) \\ &= \rho (f f^{\rho} \dots f^{\rho^{r-2}} f^{\rho^{r-1}}) \\ &= \rho (f^{\rho^{r-1}} \dots f^{\rho} f) \\ &= \rho (\rho f)^r,\end{aligned}$$

thus ρ centralizes $(\rho f)^r$. From this, and from the fact that $\langle \rho \rangle$ acts transitively on $\{\tau_0, \dots, \tau_{r-1}\}$, we deduce that

$$(\rho f)^r = \prod_{i=0}^{r-1} \tau_i^{a} = \left(\prod_{i=0}^{r-1} \tau_i \right)^a,$$

where a is either 0 or 1. If $a = 0$, then ρf is a semiregular element of order r. In particular, either $r \geq 6$, or the number of vertices of $\mathrm{sC}(r,s)$ is $r2^s$, which is bounded by $5 \cdot 2^5 = 160$, and we finish by using Remark 2.43. On the other hand, if $a = 1$, ρf has order $2r$, and it corresponds to the so-called *super flip* of the Praeger–Xu graph $\mathrm{C}(r,s)$. Since $(\rho f)^r$ does not fix any vertex in $\mathrm{C}(r,s)$, and since the vertex-stabilizer for a split graph has index 2 in the vertex-stabilizer of the starting graph, for any vertex $\alpha \in V\mathrm{sC}(r,s)$, we obtain that $(\rho f)^r \notin G_\alpha$. Hence ρf is semiregular of order $2r \geq 6$. ■

Therefore, if Γ is a ladder, the proof follows from Lemma 2.48, while, if Γ is a split Praeger–Xu graph, we conclude by Lemma 2.49. In particular, for the rest of the proof we may suppose that N is not an elementary abelian 2-group.

For any minimal normal subgroup M of G, $M_\alpha = M \cap G_\alpha$ is also a 2-group. Thus, in view of Lemma 2.47, M is an elementary abelian p-group, for some $p \in \{2,3,5\}$. This is true, in particular, for N. Let M be a minimal normal subgroup distinct from N. Since $[N,M]=1$, Lemma 2.45 gives a contradiction unless N and M are both p-groups for the same prime p. Thus,

$$\text{the socle of } G \text{ is an elementary abelian } p\text{-group, for some } p\in\{3,5\}. \tag{2.19}$$

Before going any further, we need some extra information on the local group of G on Γ. Since G_α is a nontrivial 2-group, there exists a unique vertex $\alpha'\in V\Gamma$ adjacent to α that is fixed by the action of G_α (see Section 2.C). It follows that $\{\alpha,\alpha'\}$ is a block of imprimitivity for the action of G on the vertices. Hence,

$$G_\alpha \le G_{\{\alpha,\alpha'\}} \quad \text{and} \quad |G_{\{\alpha,\alpha'\}}:G_\alpha|=2.$$

We obtain that, for any vertex $\beta\in V\Gamma$ which is a neighbour of α distinct from α',

$$|G_{\{\alpha,\alpha'\}}:G_{\alpha\beta}|=4 \quad \text{and} \quad |G_{\{\alpha,\beta\}}:G_{\alpha\beta}|=2.$$

Let $\{\alpha',\beta,\gamma\}$ be the neighbourhood of α.

Assume G/K is cyclic of order r. As Γ/N is a cycle of length r, this means that G/K acts transitively on the vertices and on the edges of Γ/N. Now, β and γ are in the same K-orbit because $K_\alpha=G_\alpha$ and G_α acts transitively on $\{\beta,\gamma\}$. In particular, each element in α^N has two neighbours in β^N. As G/K is transitive on edges, we reach a contradiction, because each element in α^N would have two neighbours in $(\alpha')^N$, contradicting the fact that α has valency 3. Thus

$$r \text{ is even and } G/K \text{ is dihedral of order } r. \tag{2.20}$$

Recall that N is an elementary abelian p-group with $p\in\{3,5\}$. Thus N is semiregular. We consider $\mathbf{C}_K(N)$. Since N is a subgroup of $\mathbf{C}_K(N)$ and since, by Frattini's Argument, $K=K_\alpha N$, we deduce that there is a subgroup Q of K_α such that $\mathbf{C}_K(N)=N\times Q$. As K_α is a 2-group, so is Q. Therefore, Q coincides with $\mathbf{O}_2(\mathbf{C}_K(N))$, which is characteristic in $\mathbf{C}_K(N)$. It follows that Q is normal in K. Since K_α is a core-free subgroup of K, we get that Q is trivial. Thus, $\mathbf{C}_K(N)=N$.

Since N is a minimal normal abelian subgroup of G, we have that G acts irreducibly by conjugation on it, that is, N is an irreducible $\mathbb{F}_pG$-module. As K is normal in G, by Clifford's Theorem (see, for instance, [134, Theorem 8.1.3]), N is a completely reducible $\mathbb{F}_pK$-module. By Frattini's Argument, $K=NG_\alpha$, which implies that N is a completely reducible $\mathbb{F}_pG_\alpha$-module. As G_α is abelian, by Schur's Lemma (see, for instance, [134, Theorem 8.1.6]), G_α induces on each irreducible $\mathbb{F}_pG_\alpha$-submodule a cyclic group action. Now, recall that Lemma 2.45 gives us that the exponent of G_α is 2. We deduce that each irreducible $\mathbb{F}_pG_\alpha$-submodule has dimension 1 and G_α induces on each irreducible $\mathbb{F}_pG_\alpha$-submodule the scalars ±1. Therefore, G_α acts on N by conjugation as a group of diagonal matrices having eigenvalues in $\{\pm1\}$. In other words, there exists a basis $(n_1,\ldots,n_e)$ of N as a vector space over $\mathbb{F}_p$ such that,

$$\text{for each } g\in G_\alpha \text{ and for each } n_i, \text{ we have } n_i^g\in\{n_i,n_i^{-1}\}. \tag{2.21}$$

Furthermore, the action of G by conjugation on N preserves the direct product decomposition $N=\langle n_1\rangle\times\cdots\times\langle n_e\rangle$.

We claim that

$$\mathbf{C}_{G_{\{\alpha,\beta\}}}(N) = 1\,, \quad \text{and} \quad \mathbf{C}_{G_{\{\alpha,\alpha'\}}}(N) = 1\,. \tag{2.22}$$

In other words, $G_{\{\alpha,\beta\}}$ and $G_{\{\alpha,\alpha'\}}$ both act faithfully by conjugation on N. Let $\delta \in \{\alpha',\beta\}$ and suppose, arguing by contradiction, that $\mathbf{C}_{G_{\{\alpha,\delta\}}}(N)$ is not trivial. Recall that $\mathbf{C}_K(N)$ is trivial, and, by applying the Orbit Stabilizer Lemma, we obtain that

$$|G_{\{\alpha,\delta\}} : K \cap G_{\{\alpha,\delta\}}| = 2\,.$$

We deduce that $\mathbf{C}_{G_{\{\alpha,\delta\}}}(N) = \langle x\rangle$, where x is an involution. Since x is not an element of K, and since the length of Γ/N is even by Equation (2.20), the fact that Nx swaps α^N and δ^N implies that Nx acts semiregularly on Γ/N. Hence, x acts semiregularly on Γ. Furthermore, from the fact that x centralizes N, we deduce that G contains some semiregular elements of order $2p \geq 6$. This contradicts Hypothesis 2.46, thus Equation (2.22) is proven.

Observe that Equation (2.22) implies that an element of $G_{\{\alpha,\alpha'\}}$ or of $G_{\{\alpha,\beta\}}$ is the identity if, and only if, its action on N by conjugation is trivial. We show that

$$G_{\{\alpha,\beta\}} - G_{\alpha\beta} \quad \text{contains an involution}\,. \tag{2.23}$$

Before proceeding in the proof, we need a little detour to prove that

$$G = \langle G_{\{\alpha,\alpha'\}}, G_{\{\alpha,\beta\}}\rangle\,. \tag{2.24}$$

Recall that the local group of the pair (Γ, G) is C_2. We can apply the merging operation, thus obtaining a 4-valent graph Δ such that G is an arc-transitive group of automorphisms of Δ. Moreover, the stabilizer of vertices in Δ is isomorphic to $G_{\{\alpha,\alpha'\}}$, while the stabilizer of edges in Δ is isomorphic to $G_{\{\alpha,\beta\}}$ (see Section 2.C). Therefore, applying to the pair (Δ, G) the argument that combines Lemma 3.2 and the existence of an edge-flip we have explained a few lines before in this proof, we obtain the desired Equation (2.24).

Let H be the permutation group induced by $G_{\{\alpha,\alpha'\}}$ in its action on the four right cosets of $G_{\alpha\beta}$ in $G_{\{\alpha,\alpha'\}}$. Since H is a 2-group, H is isomorphic to either the cyclic group C_4, or the Klein Group $C_2 \times C_2$, or to the dihedral group of degree 4 D_8. In the first two cases, $G_{\alpha\beta}$ is a normal subgroup of both $G_{\{\alpha,\alpha'\}}$ and $G_{\{\alpha,\beta\}}$. In view of Equation (2.24) and of the fact that $G_{\alpha\beta}$ is core-free in G, we have that $G_{\alpha\beta} = 1$ is trivial. In particular, $G_{\{\alpha,\beta\}}$ is cyclic of order 2, hence it contains an involution. Therefore, Equation (2.23) follows in this case.

In the latter case, we have that the triple

$$\left(G_{\{\alpha,\alpha'\}}, G_{\alpha\beta}, G_{\{\alpha\,\beta\}}\right)$$

is a locally dihedral faithful group amalgam of index $(4,2)$ and G is one of its realizations (see Section 1.H). Indeed, from the classification in [46], we see that either $G_{\{\alpha,\alpha'\}} - G_\alpha$ or $G_{\{\alpha,\beta\}} - G_{\alpha\beta}$ contains an involution. If $G_{\{\alpha,\beta\}} - G_{\alpha\beta}$ contains an involution, then Equation (2.23) holds true also in this case. Therefore, we suppose that $\tau_1 \in G_{\{\alpha,\alpha'\}} - G_\alpha$ is an involution. We investigate the action by conjugation of τ_1 on N. By Equation (2.16), τ_1 is a semiregular automorphism of Γ/K, because τ_1 lies outside the kernel K. Therefore, τ_1 is a semiregular automorphism of Γ. Note that no semiregular involution can commute with a nontrivial element of N, otherwise, by Lemma 2.45, we find a semiregular element of order $2p \geq 6$. Hence, τ_1 acts by conjugation on N without fixed points. In particular, for any $n \in N$,

$$n^{\tau_1} = n^{-1}.$$

It follows from Equation (2.21) that τ_1 commutes with G_α. Hence,

$$G_{\{\alpha,\alpha'\}} = \langle G_\alpha, \tau_1 \rangle$$

is an elementary abelian 2-group. Now, as $G_{\alpha\beta}$ is normal in both $G_{\{\alpha,\alpha'\}}$ and $G_{\{\alpha,\beta\}}$, we can conclude, as before, that $G_{\{\alpha,\beta\}}$ is cyclic of order 2. Hence, it contains an involution $G_{\{\alpha,\beta\}}$, and, in any case, Equation (2.23) holds true.

Let e be the positive integer such that $N = C_p^e$. We aim to show that

$$e \in \{1,2\}. \tag{2.25}$$

Let $\tau_2 \in G_{\{\alpha,\beta\}} - G_{\alpha\beta}$ be an involution: the existence of τ_2 is guaranteed by Equation (2.23). Now, we look at the action by conjugation of τ_2 on N. Observe that τ_2 does not lie in K, thus, as $K_\alpha = G_\alpha$, τ_2 is a semiregular automorphism of Γ. Therefore, arguing as in the previous paragraph (with the involution τ_1 replaced by τ_2), we deduce that

$$n^{\tau_2} = n^{-1} \quad \text{for every } n \in N.$$

Let us define

$$L := \langle \tau_2^g \mid g \in G \rangle.$$

Since G/K is a dihedral group and τ_2 is a noncentral involution, we deduce that

$$|G/K : LK/K| \leq 2, \quad \text{that is,} \quad |G : LK| \leq 2.$$

Observe now that, for any $n \in N$,

$$n^{\tau_2^g} = n^{-1}.$$

Therefore, the group induced by the action by conjugation of L on N has order 2. This together with Equation (2.21) shows that the subgroup LK of G preserves the direct sum decomposition

$$N = \langle n_1 \rangle \times \cdots \times \langle n_e \rangle.$$

However, since G acts irreducibly on N and since $|G : LK| \leq 2$, we finally obtain $e \leq 2$, as claimed in Equation (2.25). Observe that from this it follows that

$$|N| = p^e \in \{3, 9, 5, 25\}.$$

Observe that G_α contains an element x with $n^x = n^{-1}$ for every $n \in N$. This is immediate from Equation (2.21) when $e = 1$, or when $e = 2$ and $|G_\alpha| = 4$. When $e = 2$ and $|G_\alpha| < 4$, we have $|G_\alpha| = 2$, and hence, recalling that $\mathbf{C}_{G_\alpha}(N)$ is trivial, the nontrivial element of G_α acts by conjugation on N inverting each of its elements. Now, x and τ_2 both induce the same action by conjugation on N. It follows that the kernel of the action of G_α on N is not trivial, contradicting Equation (2.22). This final contradiction concludes the analysis of this case.

2.J.4 Nondegenerate quotients

The last scenario we have to deal with is the case in which the quotient is 3-valent. Here, a possible counterexample can only spread as a covering of an already known case. Thus, we manage to handle most cases with a computer algorithm.

Suppose that Γ/N is a 3-valent graph. Under this assumption, any two distinct neighbours of α are in distinct N-orbits, thus $N_\alpha = 1$. In particular, Lemma 2.47 gives that N is elementary abelian. Since $|V\Gamma/N| < |V\Gamma|$, by Hypothesis 2.46, the pair $(\Gamma/N, G/N)$ is not a counterexample to Theorem 2.42. Hence, $(\Gamma/N, G/N)$ is one of the pairs appearing in Table 2.3. Moreover, since the vertex-stabilizer G_α is not trivial, we have the additional information that a vertex-stabilizer

$$(G/N)_{\alpha^N} = G_\alpha N/G \cong G_\alpha/N_\alpha = G_\alpha$$

is not the identity.

We now outline the algorithm we used to resolve this case.

(1) Take as input a pair $(\Gamma/N, G/N)$ appering in Table 2.3.

(2) For each prime $p \in \{2,3,5\}$, construct all the irreducible modules of G/N over the field $\mathbb{F}_p$.

We denote by V these irreducible modules. Such modules V correspond to our putative minimal normal subgroup N of G.

(3) For all the irreducible modules V, construct all the distinct extensions of G/N via V.

We denote by E one of these group extensions. Such extension E corresponds to our putative abstract group G. Let $\pi : E \to G/N$ be the natural projection with $\ker(\pi) = V$.

(4) Compute all the subgroups H of E with the property that $\pi_{|H}$ is an isomorphism between H and $(G/N)_{\alpha/N}$.

This subgroup H is our putative vertex-stabilizer G_α.

(5) Construct the permutation representation E_ρ of E acting on the right cosets of H in E.

This permutation group E_ρ is our putative permutation group G.

(6) Check if the semiregular elements of E_ρ have order at most 5. If not, discard E_ρ from further consideration.

(7) For each permutation group E_ρ, build all the orbital graphs for E_ρ, and store the connected 3-valent graphs Γ.

This is our putative graph Γ. This last step is by far the most expensive step in the computation.

(8) Give as output the set of all the constructed pairs (Γ, E_ρ).

This whole process had to be applied repeatedly, starting with the pairs arising from the census of connected 3-valent graphs having at most 1 280 vertices, and adding to Table 2.3 each novel graph having more than 1 280 vertices.

For instance, the graphs having 65 610 vertices were found by applying this procedure starting with the graph having 810 vertices and its transitive group of automorphisms having 1 620 elements: here the elementary abelian cover N has cardinality $81 = 3^4$. Incidentally, we have found only one pair up to isomorphism. Next, by applying this procedure to this pair, we found no new examples.

The procedure comes to termination as in the previous example for all starting pairs but for an exceptional family. Consider the unique graph Δ in Table 2.3 having $1\,250 = 2\cdot 5^4$ vertices and with its corresponding vertex-transitive group H having order $2\,500 = 2^2\cdot 5^4$. When we applied this procedure, we have obtained graphs having $2\cdot 5^5 = 6\,250$ vertices and admitting a group of automorphisms having $2^2\cdot 5^5 = 12\,500$ elements, and we have found that this pair is unique up to isomorphism. We have repeated this procedure two more times, obtaining graphs having $2\cdot 5^6 = 31\,250$ and $2\cdot 5^7 = 156\,250$ vertices. We were not able to push this computation further. Therefore, to complete the proof of Theorem 2.42, we need to show that any new pair (Γ, G) has the property that $|V\Gamma| = 2\cdot 5^\ell$ and $|G| = 4\cdot 5^\ell$, with $\ell \le 34$.

From the discussion above, we may suppose that

$$|V\Gamma/N| = 2\cdot 5^\ell \quad \text{and} \quad |G/N| = 4\cdot 5^\ell \quad \text{with} \quad \ell \le 34.$$

Moreover, Γ/N is a regular cover of the graph Δ having 1 250 vertices, and G/N is an extension of H, the vertex-transitive group of automorphisms of Δ with $|H| = 2500$. We can observe that H has a cyclic Sylow 2-subgroup, and that the Sylow 5-subgroup is normal. Since H is a quotient of G/N via a normal 5-subgroup, G/N inherits the same properties. Let P_0 be a Sylow 5-subgroup of G/N. Observe that every nontrivial element of P_0 has order 5, because every semiregular element of G/N has order at most 6. Let P be the subgroup of G such that $P/N = P_0$. Assume N is not an elementary abelian 5-group. Then, by Lemma 2.47, N is an elementary abelian p-group for some $p \in \{2,3\}$. Let Q be a Sylow 5-subgroup of P. We obtain that $P = N \rtimes Q$. The elements in P are semiregular: indeed, all the 5-elements are semiregular by Lemma 1.32, while all the p-elements, with $p \in \{2,3\}$, are semiregular because $N_\alpha = 1$. Hence, each element of P has order at most 6. This implies that the elements of P have order 1, 5 or p. It follows that the action by conjugation of Q on N is fixed-point-free. Thus, P is a Frobenius group with Frobenius kernel N and Frobenius complement Q. The structure theorem of Frobenius complements gives that Q is cyclic and hence $|Q| = 5$, which is a contradiction. This contradiction has shown that N is an elementary abelian 5-group and hence P is a Sylow 5-subgroup of G. Moreover, $G = P \rtimes \langle x\rangle$, where $\langle x\rangle$ is a cyclic group of order 4. We have shown that $|V\Gamma| = 2\cdot 5^{\ell'}$ and $|G| = 2^2\cdot 5^{\ell'}$. Therefore, it remains to show that $\ell' \le 34$.

Since $|G_\alpha| = 2$, G_α fixes a unique neighbour of α. Let us call α' this neighbour. Note that $G_{\{\alpha,\alpha'\}}$ has order 4, because $\{\alpha,\alpha'\}$ is a block of imprimitivity for the action of G on $V\Gamma$. Therefore, by Sylow's Theorem, we may suppose that

$$G_{\{\alpha,\alpha'\}} = \langle x\rangle.$$

In particular, by the Orbit Stabilizer Lemma,

$$G_\alpha = \langle x^2 \rangle.$$

Let β and γ be the neighbours of α that distinct from α'. As β and γ are swapped by x^2, $|G_{\{\alpha,\beta\}}| = 2$. Hence, by Sylow's Theorem,

$$G_{\{\alpha,\beta\}} = \langle (x^2)^y \rangle, \quad \text{for some } y \in P.$$

Since Γ is connected (see Equation (2.24)), we have

$$G = \langle G_{\{\alpha,\alpha'\}}, G_{\{\alpha,\beta\}} \rangle = \langle x, (x^2)^y \rangle = \langle x, y^{-1} y^{x^2} \rangle.$$

As P is normal in G and $\mathbf{o}(x) = 4$, we deduce that

$$P = \langle y^{-1} y^{x^2}, (y^{-1} y^{x^2})^x, (y^{-1} y^{x^2})^{x^2}, (y^{-1} y^{x^2})^{x^3} \rangle.$$

We can compute

$$(y^{-1} y^{x^2})^{x^2} = (y^{x^2})^{-1} y^{x^4} = (y^{x^2})^{-1} y = (y^{-1} y^{x^2})^{-1}.$$

Therefore,

$$P = \langle y^{-1} y^{x^2}, (y^{-1} y^{x^2})^x \rangle$$

is a 2-generated group of exponent 5. In view of Theorem 2.40, the order of P is limited by a function $\mathbf{B}(2,5)$. Moreover, in [66], it is shown that

$$\mathbf{B}(2,5) \le 5^{34}.$$

Therefore, $\ell' \le 34$, and the proof of Theorem 2.42 is complete. ■

3 Unbounded valency

I look at my watch. Sunday at 10.
You stand and smile
and almost glide out of the door.
What could I tell you?–
that in 1943 I was thirty,
a member of the Reich,
that Paris was mine
and I didn't want it.

– *The psychiatrist*, Ai Ogawa (1980)

This chapter collects result which holds for vertex-transitive graphs of unbounded valency. We start by studying how the valency affects the fixed point ratio of automorphism groups of graphs. Then we study some properties that negatively affect the possibility of efficiently enumerating the amalgams.

(Some preliminary comments about the finiteness hypothesis in Chapter 3. In Sections 3.A to 3.C, 3.E, 3.F and 3.I, all graphs and all permutation groups are finite. In Sections 3.G and 3.H, all graphs are locally finite and, most of the time, the vertex-stabilizer of the groups of automorphism is supposed to be finite. Last, in Section 3.D, we build graphs that may not be locally finite.)

3.A Bounding the fixed point ratio

How is the fixed point ratio affected by the minimal subdegree of a permutation group? Or, rather, what can we say about the fixed point ratio of a group G acting on a connected d-valent graph?

The answer to this problem cannot be too thrilling in general. Indeed, the fixed point ratio of a split Praeger–Xu $\mathrm{C}(r,s)$ is

$$\mathrm{fpr}\,(\mathrm{Aut}(\mathrm{C}(r,s))) = \frac{r-s}{r}$$

(see [112, Lemma 1.10] and Section 2.A). For every $\epsilon > 0$, by choosing $r \geq \epsilon^{-1}s$,

$$\mathrm{fpr}\,(\mathrm{Aut}(\mathrm{C}(r,s))) = 1-\epsilon\,.$$

Hence, their fixed point ratio is arbitrarily close to 1.

On the other hand, if the local group is graph-restrictive, as Lemma 1.8 suggests, the fixed point ratio of the group of automorphism could tend to zero as the number of vertices grows. This has been proved by F. Lehner, P. Potočnik and P. Spiga in [85] under the extra assumption that the local group is quasiprimitive.

Theorem 3.1 ([85] Theorem 3.1) · *There exists a function* $\mathbf{f}: \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ *such that, for every pair* (Γ, G)*, where* Γ *is a* d*-valent connected graph,* G *is an arc-transitive group of automorphism, and the local group of the pair is quasiprimitive and graph-restrictive, and for every positive constant* ϵ*,*

$$\textit{if } |V\Gamma| > \mathbf{f}(d,\epsilon), \quad \textit{then } \operatorname{fpr}(G) < \epsilon.$$

Althought a complete proof of Theorem 3.1 would lead us too much astray, we want to give a sketch of it to highlight where the hypothesis of quasiprimitive and graph-restrictive local group are used. Let (Γ, G) be a pair as described, and let ϵ be a positive constant. Suppose that $\operatorname{fpr}(G) \geq \epsilon$. Further, in view of the asymptotic nature of the claimed result, we can assume that

$$|V\Gamma| \geq \max\left\{\frac{1}{\epsilon}, 2d+1\right\}.$$

This assumption on the number of vertices has two consequences: the graph Γ is not isomorphic to a complete bipartite graph, and, for all elements $g \in G$ such that $\operatorname{fpr}(g) \geq \epsilon$, g fixes at least one vertex. Let us choose such an automorphism g, and let us pick a vertex α such that $\alpha^g = \alpha$. We define H as the subgroup of G generated by the G-conjugates of g, that is,

$$H = \langle g^G \rangle.$$

Observe that H is a normal subgroup of G, thus, for every vertex $\alpha \in V\Gamma$, H_α is a normal subgroup of G_α. Moreover, it also follows that

$$H_\alpha^{\Gamma(\alpha)} \quad \text{is a normal subgroup of } G_\alpha^{\Gamma(\alpha)}.$$

(Note that, since H is not transitive, we cannot talk about the local group of the pair (Γ, H), as the permutation group that H_α induces on the neighbourhood of α might depend on α.) Since we assume that the local group is quasiprimitive, this implies that

$$H_\alpha^{\Gamma(\alpha)} \quad \text{is transitive on } \Gamma(\alpha).$$

We can thus apply the following result.

Lemma 3.2 · *Let* Γ *be a connected graph, and let* H *be a group of automorphisms. Suppose that,*

$$\textit{for every vertex } \alpha \in V\Gamma, \quad H_\alpha^{\Gamma(\alpha)} \textit{ is transitive}.$$

Then H *defines either one or two orbits on the vertices of* Γ*.*

Proof. Let us choose two adjacent vertices, say α, β. We claim that $H^+ = \langle H_\alpha, H_\beta \rangle$ has at most two orbits on $V\Gamma$. Since H^+ contains the stabilizers of α and of β, and since the actions that H^+ induces on $\Gamma(\alpha)$ and $\Gamma(\beta)$ are transitive, we obtain that $\alpha^{H^+} \cup \beta^{H^+}$ contains the union of the neighbourhoods of α and β. In particular, for any $\gamma \in \Gamma(\alpha) \cup \Gamma(\beta)$, there exists an automorphism $h \in H^+$ such that either $\alpha^h = \gamma$

or $\beta^h = \gamma$. By conjugating either H_α or H_β by h, we get that H_γ is a subgroup of H^+. By repeating the same consideration with all the $\gamma \in \Gamma(\alpha) \cup \Gamma(\beta)$, we see that $\alpha^{H^+} \cup \beta^{H^+}$ contains all the elements at distance at most 2 from α or from β. By iterating the process as many times as the diameter, it follows that $\alpha^{H^+} \cup \beta^{H^+}$ contains the connected component of Γ containing the edge $\{\alpha, \beta\}$. But, as Γ is connected, we just proved that all the vertices of the graphs are contained in the two H^+-orbits of α and of β. Moreover, H^+ is a subgroup of H, thus the proof is complete. ■

Therefore, H defines at most two orbits on $V\Gamma$. Recall that the local group is graph-restrictive, thus there exists a constant C_d (depending on the valency d) such that $|G_\alpha| \leq C_d$. We compute

$$|G:H| = \frac{|V\Gamma||G_\alpha|}{|\alpha^H||H_\alpha|} \leq 2|G_\alpha : H_\alpha| \leq |G_\alpha| \leq C_d\,.$$

We now need to invoke another result, but we will not give a proof, as it uses tools we have not developed in this work. We stress that the hypothesis of quasiprimitivity of the local group is needed to use Lemma 3.2.

Lemma 3.3 ([85] Corollary 2.5 and Lemma 2.7) · *There exists a strictly decreasing function*

$$\mathbf{g} : \mathbb{N} \to \mathbb{R} \quad \textit{with} \quad \lim_n \mathbf{g}(n) = 0$$

such that, for every pair (Γ, G), where Γ is a d-valent connected graph, G is an arc-transitive group of automorphism, and the local group of the pair is quasiprimitive, then, for every $g \in G$,

$$\mathrm{fpr}(g) \leq |\langle g^G \rangle_\alpha| \cdot |G : \langle g^G \rangle| \cdot \mathbf{g}\left(|\langle g^G \rangle|\right).$$

Specializing Lemma 3.3 to our setting,

$$\epsilon \leq \mathrm{fpr}(g) \leq |H_\alpha| \cdot |G:H| \cdot \mathbf{g}(|H|) \leq |G_\alpha| \cdot |G:H| \cdot \mathbf{g}(|H|) \leq C_d^2 \mathbf{g}(|H|)\,.$$

Upon diving both sides by C_d^2 and taking the inverse of $\mathbf{g}$,

$$|H| \leq \mathbf{g}^{-1}\left(\frac{\epsilon}{C_d^2}\right).$$

(Recall that, as $\mathbf{g}^{-1}$ is strictly decreasing, by applying it we reverse the inequality.) We conclude, using the Orbit Stabilizer Lemma,

$$|V\Gamma| \leq 2|H : H_\alpha| \leq |H| \leq \mathbf{g}^{-1}\left(\frac{\epsilon}{C_d^2}\right).$$

Although the proof of Theorem 3.1 heavily relies on the assumption of quasiprimitivity, we have no reason to think that, with a different set of ideas, graph-restrictiveness is not enough. Assuming the veracity of Conjecture 1.37, checking if the result can be extended to semiprimitive local groups is enough.

Question 3.4 · Consider all the pairs (Γ, G), where Γ is a d-valent connected graph, G is an arc-transitive group of automorphism, such that the local group of the pair is graph-restrictive. Is there a function $\mathbf{f} : \mathbb{N} \times (0,1) \to \mathbb{N}$ such that, for every such pair (Γ, G), and for every positive constant ϵ,

$$\text{if } |V\Gamma| > \mathbf{f}(d,\epsilon), \quad \text{then } \operatorname{fpr}(G) < \epsilon\,?$$

Since this problem appears to be related to graph-restrictiveness, it makes sense to ask if a similar result can be proven with the global hypothesis of vertex-primitivity. We conclude Section 3.A with the analogue of Theorem 3.1 for vertex-primitive permutation group, as proved in [17].

Lemma 3.5 ([45] Exercise 1.7.6) · *Let G be a transitive permutation group on Ω, let $x \in G$ be a permutation, and let $\omega \in \Omega$ be a point. Then*

$$\operatorname{fpr}(x) = \frac{|x^G \cap G_\omega|}{|x^G|}.$$

Proof. Our proof proceeds by double counting the set

$$X = \left\{(\alpha, g) \in \Omega \times x^G \mid \alpha^g = \alpha\right\}.$$

On one hand, by the transitivity of G,

$$|X| = \sum_{\alpha \in \Omega} |x^G \cap G_\alpha| = |\Omega| \cdot |x^G \cap G_\omega|.$$

On the other hand, as the number of fixed point is constant con conjugacy classes,

$$|X| = \sum_{g \in x^G} |\Omega - \operatorname{supp}(g)| = |x^G| \cdot |\Omega - \operatorname{supp}(x)|.$$

Therefore, we obtain

$$\operatorname{fpr}(x) = \frac{|\Omega - \operatorname{supp}(x)|}{|\Omega|} = \frac{|x^G \cap G_\omega|}{|x^G|},$$

as desired ■

Theorem I · *Let ϵ and C be two positive constants, and let $\mathcal{F}$ be a family of quasiprimitive permutation groups G on Ω satisfying*

(*a*) $\operatorname{fpr}(G) \geq \epsilon$,

(*b*) $|G_\omega| \leq C$ *for every* $\omega \in \Omega$.

Then $\mathcal{F}$ is a finite family.

Proof of Theorem I. Let G be a quasiprimitive permutation group on a set Ω, and let $x \in G$ be a nontrivial element achieving $|\operatorname{supp}(x)| \leq (1-\epsilon)|\Omega|$. For any point $\omega \in \Omega$, we obtain

$$\epsilon \leq \frac{|x^G \cap G_\omega|}{|x^G|} \leq \frac{|G_\omega|}{|x^G|} \leq \frac{C}{|x^G|}.$$

It follows that $|x^G| \le \epsilon^{-1}C$. Now, let us consider the normal subgroup of G defined by

$$N := \bigcap_{g\in G} \mathbf{C}_G(x^g).$$

Recall that $|G : \mathbf{C}_G(x)| = |x^G|$. Observe that G acts by conjugation on the set

$$\{\mathbf{C}_G(x^g) \mid g \in G\},$$

it defines a single orbit of size at most $|x^G|$, and N is the kernel of this action. Therefore

$$|G : N| \le |\{\mathbf{C}_G(x^g) \mid g \in G\}|! \le |x^G|! \le \left\lceil \frac{C}{\epsilon} \right\rceil!,$$

that is, N is a bounded index subgroup of G. Since G is quasiprimitive, either N is trivial or N is transitive.

Aiming for a contradiction, we suppose that N is transitive. We note that $|\mathrm{supp}(x)| < |\Omega|$. In particular, x fixes at least one point, and we choose $\omega \in \Omega$ to be a point that is fixed by x. Since $[N, x] = 1$, for any $n \in N$,

$$\omega^{nx} = \omega^{xn} = \omega^n.$$

The transitivity of N implies that $x = 1$, against our choice of x.

Therefore, N is trivial. It follows that

$$|G| = |G : N| \le \left\lceil \frac{C}{\epsilon} \right\rceil!.$$

Since there are finitely many abstract groups of bounded size (see, for instance, [130]), the proof is complete. ■

We observe that the affirmative solution to the Sims Conjecture (see Theorem 1.28) implies that the hypothesis of vertex-primitivity is enough to conclude.

Corollary J · *Let ϵ be a positive constant, and let d be a positive integer. There are only finitely many vertex-primitive digraphs of valency at most d and fixed point ratio exceeding ϵ.*

Proof. Let Γ be a vertex-primitive digraphs of valency at most d and relative fixity exceeding α, and let $G = \mathrm{Aut}(\Gamma)$. The hypothesis on the out-valency implies that, for any $\omega \in V\Gamma$, $|G_\omega| \le \mathbf{f}(d)$, where $\mathbf{f}(d)$ is the function appearing in Theorem 1.28. The result thus follows by choosing $C = \mathbf{f}(d)$ in Theorem I. ■

We observe that the fixed point ratio can be arbitrarily close to 1. Indeed, in Lemma 3.21, we will prove that, if $\mathbf{H}(r, m)$ is the Hamming graph of rank r on a set of cardinality m, then

$$\mathrm{fpr}\,(\mathrm{Aut}(\mathbf{H}(r, m))) \ge 1 - \frac{2}{m}.$$

In particular, for any positive constant $0 < \epsilon < 1$, upon choosing $m \le 2\epsilon^{-1}$, we get

$$\mathrm{fpr}\,(\mathrm{Aut}(\mathbf{H}(r, m))) \ge 1 - \epsilon,$$

which is arbitrarily close to 1.

We conclude Section 3.A by observing that the proofs developed to study fixed point ratio for small valency and for unbounded valency are widely different. Out of curiosity, one might pose the following problem.

Question 3.6 · Can the normal quotient method be applied to study the fixed point ratio of vertex-transitive group automorphisms of graphs even though the valency of the underlying graphs is unbounded?

3.B Minimal degree for primitive groups

Let G be a finite permutation group on Ω. We define the *minimal degree* (or *motion*) by

$$\mu(G) = \min_{g\in G-\{1\}} |\mathrm{supp}(g)|.$$

The study of minimal degree can be traced back to the classical result by C. Jordan in [36] stating that, for any positive integer $C \geq 2$, the number of primitive groups such that $\mu(G) \leq C$ is finite. As a well known consequence, $\mathrm{Sym}(\Omega)$ and $\mathrm{Alt}(\Omega)$ (in their natural action) are the only primitive groups of minimal degree 2 and 3 respectively.

Observe that, for every permutation group G of degree n,

$$\mathrm{fpr}(G) = 1 - \frac{\mu(G)}{n}.$$

Therefore, the wide range of application has been already explored in Section 1.D. As a consequence, classifications of primitive group of bounded minimal degree are desirable. In [90], M. W. Liebeck and J. Saxl proved that any primitive group G such that $\mu(G) \leq |\Omega|/3$ is of type AS or PA and of socle type $\mathrm{Alt}(m)$ in its action on k-subsets. (If G is a primitive permutation group, all direct factors of its socle are isomorphic. We refer to the isomorphism class of these subgroups as the *socle type of* G. For a detailed discussion of this result, see [45, Section 4.3].) The primitive groups G with $\mu(G) \leq |\Omega|/2$ were determined by R. M. Guralnick and K. Magaard in [64], adding the possibility of socle types $\mathrm{SO}^+_{2m}(2)$ and $\mathrm{SO}^-_{2m}(2)$ and the possibility that the whole group is of type HA. Finally, the most recent list was compiled by T. C. Burness and R. M. Guralnick in [27], and it accomplishes the task of describing those primitive groups G such that $\mu(G) < 2|\Omega|/3$.

Since we are also exploiting this last classification in the proof of Theorem K, we report it here. We observe that, also in this refined classification, we have that G is either or type AS, PA or HA. Moreover, we explicitly write the permutational rank of the almost simple groups of Lie type. This information can be easily obtained combining the complete list of 2-transitive finite permutation groups, first described by P. J. Cameron in [31, Section 5], and the complete list of classical finite permutation groups of permutational rank 3, compiled by W. M. Kantor and R. A. Liebler in [79, Theorem 1.1].

Theorem 3.7 ([27] Theorem 4) · *Let G be a finite permutation group of degree n with*

$$\mu(G) < \frac{2n}{3}.$$

Then one of the following holds:

(*a*) $\mathrm{Alt}(m) \le G \le \mathrm{Sym}(m)$, *for some* $m \ge 3$, *in its action on k-subsets, for some* $k < m/2$;

(*b*) $G = \mathrm{Sym}(2m)$, *for some* $m \ge 2$, *in its primitive action with stabilizer* $G_\alpha = \mathrm{Sym}(m) \,\mathrm{wr}\, C_2$;

(*c*) $G = M_{22} : 2$ *in its primitive action of degree* 22 *with stabilizer* $G_\alpha = \mathrm{L}_3(4).2_2$;

(*d*) *G is an almost simple group of permutational rank 2 and socle described in Table 3.1;*

(*e*) *G is an almost simple group of permutational rank 3 and socle described in Table 3.2;*

(*f*) $G \le K \,\mathrm{wr}\, \mathrm{Sym}(r)$ *is a primitive group of type* PA, *where K is a permutation group appearing in points (a) – (e), the wreath product is endowed with the product action, and* $r \ge 2$;

(*g*) *G is an affine group with a regular normal socle N, which is an elementary abelian 2-subgroup.*

	Socle	Action	Comments
(i)	$\mathrm{L}_m(2)$	Natural module	$m \ge 3$
(ii)	$\mathrm{L}_m(3)$	Natural module	$m \ge 3$, and G contains an element of the form $(-I_{n-1}, I_1)$
(iii)	$\mathrm{Sp}_{2m}(2)$	Singular points	$m \ge 3$
(iv)	$\mathrm{Sp}_{2m}(2)$	Right coset space of $\mathrm{SO}^-_{2m}(2)$	$m \ge 3$
(v)	$\mathrm{Sp}_{2m}(2)$	Right coset space of $\mathrm{SO}^+_{2m}(2)$	$m \ge 3$

Table 3.1: Description of the groups in Theorem 3.7 (d).

3.C Vertex-primitive digraphs

It is now time for us to state the classification of vertex-primitive digraphs with large fixed point ratio. The notation is quite heavy, thus we use Section 3.C to introduce and explain it.

Recall that the *direct product of the family of digraphs* $\Gamma_1, \dots, \Gamma_r$ (sometimes also called the *tensor product* or the *categorical product*) is the digraph $\Gamma_1 \times \ldots \times \Gamma_r$ whose vertex-set is the Cartesian product $V\Gamma_1 \times \ldots \times V\Gamma_r$ and whose arc-set is

$$A(\Gamma_1 \times \ldots \times \Gamma_r) = \{((u_1, \dots, u_r), (v_1, \dots, v_r)) \,|\, (u_i, v_i) \in A\Gamma_i \text{ for all } i \in \{1, \dots, r\}\}.$$

	Socle	Action	Comments
(i)	$U_4(q)$	Totally singular 2-dimensional subspaces	$q \in \{2,3\}$, and G contains the graph automorphism τ
(ii)	$\Omega_{2m+1}(3)$	Singular points	$m \geq 3$, and G contains an element of the form $(-I_{2m}, I_1)$ with a "+"-type (-1)-eigenspace
(iii)	$\Omega_{2m+1}(3)$	Nonsingular points whose orthogonal complement is an orthogonal space of "−"-type	$m \geq 3$, and G contains an element of the form $(-I_{2m}, I_1)$ with a "−"-type (-1)-eigenspace
(iv)	$\mathrm{P}\Omega^{\epsilon}_{2m}(2)$	Singular points	$\epsilon \in \{+,-\}$, and $G = \mathrm{SO}^{\epsilon}_{2m}(2)$
(v)	$\mathrm{P}\Omega^{\epsilon}_{2m}(2)$	Nonsingular points	$\epsilon \in \{+,-\}$, and $G = \mathrm{SO}^{\epsilon}_{2m}(2)$
(vi)	$\mathrm{P}\Omega^{+}_{2m}(3)$	Nonsingular points	G contains an element of the form $(-I_{2m-1}, I_1)$ such that the discriminant of the 1-dimensional 1-eigenspace is a nonsquare
(vii)	$\mathrm{P}\Omega^{-}_{2m}(3)$	Singular points	G contains an element of the form $(-I_{2m-1}, I_1)$
$(viii)$	$\mathrm{P}\Omega^{-}_{2m}(3)$	Nonsingular points	G contains an element of the form $(-I_{2m-1}, I_1)$ such that the discriminant of the 1-dimensional 1-eigenspace is a square

Table 3.2: Description of the groups in Theorem 3.7 (e).

Recall also that a *union of digraphs* Γ_1 and Γ_2 is the digraph whose vertex-set and arc-set are the sets $V\Gamma_1 \cup V\Gamma_2$ and $A\Gamma_1 \cup A\Gamma_2$, respectively. Note that when Γ_1 and Γ_2 share the same vertex-set, their union is then obtained simply by taking the union of their arc-sets.

We now have all the ingredients needed to present a construction yielding the digraph appearing in our main result.

Construction 3.8 · Let $\mathcal{G} = \{\Gamma_0, \Gamma_1, \dots, \Gamma_k\}$ be a list of $k+1$ pairwise distinct digraphs sharing the same vertex-set Δ. Further, let r be a positive integer, and let $\mathcal{J}$ be a subset of the r-fold Cartesian power X^r, where $X = \{0, 1, \dots, k\}$. Given this input, we construct the digraph

$$\mathcal{P}(r, \mathcal{G}, \mathcal{J}) = \bigcup_{(j_1, j_2, \dots, j_r) \in \mathcal{J}} \Gamma_{j_1} \times \Gamma_{j_2} \times \dots \times \Gamma_{j_r}$$

and we call it the *merged product action digraph*.

Our interest lies in applying Construction 3.8 with $\mathcal{G}$ being the set of all orbital digraphs for a primitive permutation group. In this case, we may assume that Γ_0 is the diagonal orbital digraph, that is, that Γ_0 is the loop graph $\mathbf{L}_m$ where

$m = |\Delta|$. Meanwhile the union of the remaining digraphs in $\mathcal{G}$ is the complete graph, that is,

$$\mathbf{K}_m = \bigcup_{i=1}^{k} \Gamma_i .$$

For the sake of a simpler and more compact presentation, we assume that, from here onwards, this property holds for all the families $\mathcal{G}$.

Remark 3.9 · We give some example to give a flavour of what can be obtained using Construction 3.8.

If $r = 1$, then $\mathcal{P}(1,\mathcal{G},\mathcal{J})$ is simply the union of some digraphs from the set $\mathcal{G}$.

If $r = 2$ and $\mathcal{J} = \{(1,0),(0,1)\}$, then $\mathcal{P}(2,\mathcal{G},\mathcal{J}) = \mathbf{L}_m \times \Gamma_1 \cup \Gamma_1 \times \mathbf{L}_m$, which is, in fact, the *Cartesian product* $\Gamma_1 \Box \Gamma_1$. (This product is sometimes called the *box product*, and we refer to [72] for its general definition and further details.)

More generally, if $\mathcal{J} = \{e_i \mid i \in \{1,\dots,r\}\}$, where $e_i = (0,\dots,0,1,0,\dots,0)$ is the r-tuple with 1 in the i-th component and zeroes elsewhere, then $\mathcal{P}(r,\mathcal{G},\mathcal{J}) = (\Gamma_1)^{\Box r}$, the r-th Cartesian power of the graph $\Gamma_1 \in \mathcal{G}$. More specifically, if $\Gamma_1 = \mathbf{K}_m$ and $\mathcal{J}$ is as above, then $\mathcal{P}(r,\mathcal{G},\mathcal{J})$ is the *Hamming graph* $\mathbf{H}(r,m) = \mathbf{K}_m^{\Box r}$.

While $\mathcal{J}$ can be an arbitrary set of r-tuples in X^r, we will be mostly interested in the case where $\mathcal{J} \subseteq X^r$ is invariant under the induced action of some permutation group $H \leq \mathrm{Sym}(r)$ on the set X^r given by the rule

$$(j_1, j_2, \dots, j_r)^h = (j_{1h^{-1}}, j_{2h^{-1}}, \dots, j_{rh^{-1}}).$$

(We choose to write ih^{-1} instead of $i^{h^{-1}}$ for improved legibility.) We shall say that $\mathcal{J}$ is an *H-invariant subset of X^r* in this case. A subset $\mathcal{J} \subseteq X^r$ which is H-invariant for some *transitive* subgroup of $\mathrm{Sym}(r)$ will be called *homogeneous*.

The last example of Remark 3.9 justifies the introduction of the following new family of graphs.

Definition 3.10 · Let r, m be two positive integers, and let $\mathcal{J} \subseteq \{0,1\}^r$ be a homogeneous set. The graph $\mathcal{P}(r,\{\mathbf{L}_m,\mathbf{K}_m\},\mathcal{J})$ is called *generalised Hamming graph* and is denoted by $\mathbf{H}(r,m,\mathcal{J})$.

Remark 3.11 · The generalised Hamming graphs $\mathbf{H}(r,m,\mathcal{J})$, where $\mathcal{J}$ is H-invariant, are precisely the unions of orbital digraphs for the group $\mathrm{Sym}(m) \,\mathrm{wr}\, H$ endowed with the product action (see Lemma 3.19 for further details).

Since the union of all nondiagonal orbital digraphs is $\mathbf{K}_{m^r}$, all the complete graphs are generalised Hamming graphs. Furthermore, $\mathbf{K}_{m^r}$ can be explicitly build from Definition 3.10 upon choosing $\mathcal{J}$ containing only the vectors with all entries equal to 1.

A homogeneous set $\mathcal{J}$ is said to be *Hamming* if,

$$\mathcal{J} = \bigcup_{h \in H} \left((X - \{0\})^a \times X^b \times \{0\}^{r-a-b} \right)^h ,$$

for some nonnegative integers a, b such that $a + b \leq r$ and a transitive group $H \leq \mathrm{Sym}(r)$. It is said to be *non-Hamming* otherwise.

Remark 3.12 · Let $\mathcal{P}(r,\mathcal{G},\mathcal{J})$ be a merged product action digraph where $\mathcal{J}$ is a Hamming set. Since the union of all the digraphs that are not labelled by 0 is $\mathbf{K}_m$ by assumption, upon switching the order of the unions and of the direct products in Construction 3.8, we obtain that every factor of $\mathcal{P}(r,\mathcal{G},\mathcal{J})$ (which we can now think of as a direct product of digraphs) is isomorphic either to $\mathbf{L}_m$, to $\mathbf{K}_m$ or to $\mathbf{L}_m \cup \mathbf{K}_m$. We can be more precise with this observation. Build $\mathcal{J}' \subseteq \{0,1\}^r$ from $\mathcal{J}$ by substituting any nonzero entry of a sequence in $\mathcal{J}$ with 1. Then

$$\mathcal{P}(r,\mathcal{G},\mathcal{J}) = \mathcal{P}(r,\{\mathbf{L}_m,\mathbf{K}_m\},\mathcal{J}')\,.$$

In particular, a generalised Hamming graph arises from Construction 3.8 if and only if $\mathcal{J}$ is a Hamming set.

Remark 3.13 · The ordering of the Cartesian components in the definition of a Hamming set does not matter: indeed, a permutation of the components corresponds to a conjugation of the group H in $\mathrm{Sym}(r)$, thus defining isomorphic digraphs in Construction 3.8.

One last piece of notation: when computing the fixed point ratio of the automorphism group of a graph Γ, rather than writing $\mathrm{fpr}(\mathrm{Aut}(\Gamma))$, from here on we will use $\mathrm{fpr}(\Gamma)$. We are ready to state our main characterization.

Theorem K · *Let Γ be a finite vertex-primitive digraph with at least one arc. Then*

$$\mathrm{fpr}(\Gamma) > \frac{1}{3}$$

if and only if one of the following occurs:

(*i*) *Γ is a generalised Hamming graph $\mathbf{H}(r,m,\mathcal{J})$, with $m \geq 4$, and, if m is optimal in the sense of Definition 3.20, then*

$$\mathrm{fpr}(\Gamma) = 1 - \frac{2}{m}\,;$$

(*ii*) *Γ is a merged product action graph $\mathcal{P}(r,\mathcal{G},\mathcal{J})$, where $r \geq 1$, where $\mathcal{J}$ is a non-Hamming subset of X^r with $X = \{0,1,\dots,|\mathcal{G}|-1\}$, and where $\mathcal{G}$ is as in one of the following:*

(*a*) *$\mathcal{G} = \{\mathbf{J}(m,k,i) \mid i \in \{0,1,\dots,k\}\}$ is the family of distance-i Johnson graphs, where k,m are fixed integers such that $k \geq 2$ and $m \geq 2k+2$ (see Section 3.E.2 for details), and*

$$\mathrm{fpr}(\Gamma) = 1 - \frac{2k(m-k)}{m(m-1)}\,;$$

(*b*) *$\mathcal{G} = \{\mathbf{QJ}(2m,m,i) \mid i \in \{0,1,\dots,\lfloor m/2 \rfloor\}\}$ is the family of squashed distance-i Johnson graphs, where m is a fixed integer with $m \geq 4$ (see Section 3.E.3 for details), and*

$$\mathrm{fpr}(\Gamma) = \frac{1}{2}\left(1 - \frac{1}{2m-1}\right);$$

(*c*) $\mathcal{G} = \{\mathbf{L}_m, \Gamma_1, \Gamma_2\}$, *where* Γ_1 *is a strongly regular graph listed in Section 3.E.4,* Γ_2 *is its complement, and*

$$\mathrm{fpr}(\Gamma) = \mathrm{fpr}(\Gamma_1)$$

(the fixed point ratios are collected in Table 3.3).

Remark 3.14 · Although we do not assume that a vertex-primitive digraph Γ in Theorem K is a graph, the assumption of large fixed point ratio forces it to be such. In other words, every vertex-primitive digraph of relative fixity larger than $\frac{1}{3}$ is a graph.

By analysing the vertex-primitive graphs of fixed point ratio exceeding 1/3, one can notice that the valency of these graphs must grow as the number of vertices grows. More explicitly, a careful inspection of the families in Theorem K leads to the following result.

Corollary L · *There exists a constant C such that every finite connected vertex-primitive digraph* Γ *with*

$$\mathrm{fpr}(\Gamma) > \frac{1}{3}$$

satisfies

$$\mathrm{val}(\Gamma) \geq C \log(|V\Gamma|)\,.$$

Observe that, for the Hamming graphs $\mathbf{H}(r,m)$ with $m \geq 4$, we have that

$$\mathrm{val}(\mathbf{H}(r,m)) = r(m-1) \geq r\log(m) = \log(|V\mathbf{H}(r,m)|)\,.$$

In particular, as both expressions are linear in r, a logarithmic bound in Corollary L is the best that can be achieved. Moreover, as the function $\mathbf{f}(d)$ appearing in Theorem 1.28 grows exponentially with d, Corollary L gives a significantly better growth than what we have found in Corollary J (although the latter also holds in a considerably larger class of digraphs).

3.D Orbital digraphs for product actions

In Section 3.D, we are interested in reconstructing the orbital digraphs for a wreath product $K \operatorname{wr} H$ endowed with product action once the orbital digraphs for K are known. Since the concept of wreath product and its product action will be key in what follows, we start by recalling their definition and basic concepts. We refer to [45, Section 2.6 and 2.7] for the details we will miss.

Let H be a permutation group on a finite set Ω of degree r. Without loss of generality, we can identify Ω with the set $\{1,2,\ldots,r\}$. For an arbitrary set X, we may define a *permutation action of H of rank r over X* as the action of H on the set X^r given by the rule

$$(x_1,x_2,\ldots,x_r)^h = (x_{1h^{-1}}, x_{2h^{-1}}, \ldots, x_{rh^{-1}})\,.$$

Let K be a permutation group on a set Δ. (Note that we will not put any assumption of finiteness on Δ.) We can consider the permutation action of H of rank r over K by letting

$$(k_1, k_2, \dots, k_r)^h = (k_{1h^{-1}}, k_{2h^{-1}}, \dots, k_{rh^{-1}}) \quad \text{for all } (k_1, k_2, \dots, k_r) \in K^r, h \in H.$$

If we denote by ϑ the homomorphism $H \to \mathrm{Aut}(K^r)$ corresponding to this action, then the *wreath product of K by H*, in symbols $K \operatorname{wr} H$, is the semidirect product $K^r \rtimes_\vartheta H$. We call K^r the *base group*, and H the *top group* of this wreath product.

Note that the base and the top group are both embedded into $K \operatorname{wr} H$ via the monomorphisms

$$(k_1, k_2, \dots, k_r) \mapsto ((k_1, k_2, \dots, k_r), 1_H)$$

and

$$h \mapsto ((1_K, 1_K, \dots, 1_K), h).$$

In this way, we may view the base and the top group as subgroups of the wreath product and identify an element $((k_1, k_2, \dots, k_r), h) \in K \operatorname{wr} H$ with the product $(k_1, k_2, \dots, k_r)h$ of $(k_1, k_2, \dots, k_r) \in K^r$ and $h \in H$ (both viewed as elements of the group $K \operatorname{wr} H$).

The wreath product $K \operatorname{wr} H$ can be endowed with an action on Δ^r by letting

$$(\delta_1, \delta_2, \dots, \delta_r)^{(k_1, k_2, \dots, k_r)h} = \left(\delta_1^{k_1}, \delta_2^{k_2}, \dots, \delta_r^{k_r}\right)^h = \left(\delta_{1h^{-1}}^{k_{1h^{-1}}}, \delta_{2h^{-1}}^{k_{2h^{-1}}}, \dots, \delta_{rh^{-1}}^{k_{rh^{-1}}}\right),$$

for all $(\delta_1, \delta_2, \dots, \delta_r) \in \Delta^r, (k_1, k_2, \dots, k_r) \in K^r$, and $h \in H$. We call this action the *product action of the wreath product $K \operatorname{wr} H$ on Δ^r*.

We recall the condition for a wreath product endowed with product action to be primitive.

Lemma 3.15 ([45] Lemma 2.7A) · *Let K be a permutation group on Δ and let H be a permutation group on Ω, with $|\Omega| = r$. The wreath product $K \operatorname{wr} H$ endowed with the product action on Δ^r is primitive if and only if H is transitive on Ω and K is primitive but not regular on Δ.*

We now introduce some notation to deal with a generic subgroup G of the wreath product $\mathrm{Sym}(\Delta) \operatorname{wr} \mathrm{Sym}(\Omega)$ endowed with product action on Δ^r.

By abuse of notation, we identify the set Δ with

$$\left\{\{\delta\} \times \Delta^{r-1} \,\middle|\, \delta \in \Delta\right\}$$

via the mapping $\delta \mapsto \{\delta\} \times \Delta^{r-1}$. We denote by G_Δ^Δ the permutation group that G_Δ induces on Δ, that is,

$$G_\Delta^\Delta \cong G_\Delta / G_{(\Delta)}.$$

Moreover, recalling that every element of G can be written uniquely as gh, for some $g \in \mathrm{Sym}(\Delta)^r$ and some $h \in \mathrm{Sym}(\Omega)$, we can define the group homomorphism

$$\psi : G \to \mathrm{Sym}(\Omega), \quad gh \mapsto h.$$

This map defines a permutational representation of G acting on Ω. We denote by G^{Ω} the permutation group corresponding to the faithful action that G defines on Ω, that is,

$$G^{\Omega} \cong G/\ker(\psi).$$

A detailed description of primitive wreath product in product action has been given by L. G. Kovács in [82]. Building on his work, C. E. Praeger and C. Schneider have given a strong embedding property, which we will implicitly use quite often.

Theorem 3.16 ([126] Theorem 1.1 (b)) · *Let $G \le K \,\mathrm{wr}\, H$ be a permutation group embedded in a wreath product in product action. Then G is permutationally isomorphic to a subgroup of $G_{\Delta}^{\Delta} \,\mathrm{wr}\, G^{\Omega}$. Therefore, up to a conjugation in* $\mathrm{Sym}(\Delta^r)$*, the group K can always be chosen as G_{Δ}^{Δ}, and H as G^{Ω}.*

Lemma 3.17 · *Let $K \,\mathrm{wr}\, H$ be a wreath product endowed with the product action on Δ^r, and let*

$$\mathcal{G} = \{\Gamma_0, \Gamma_1, \ldots, \Gamma_k\}$$

be the complete list of the orbital digraphs for K. Then any orbital digraph for $K \,\mathrm{wr}\, H$ is a merged product action digraph of the form

$$\mathcal{P}\left(r, \mathcal{G}, (j_1, j_2, \ldots, j_r)^H\right),$$

for a sequence of indices $(j_1, j_2, \ldots, j_r) \in X^r$, where $X = \{0, 1, \ldots, k\}$.

Proof. Let Γ be an orbital digraph for $K \,\mathrm{wr}\, H$. Suppose that $(u, v) \in A\Gamma$, where $u = (u_1, u_2, \ldots, u_r)$ and $v = (v_1, v_2, \ldots, v_r)$. We aim to compute the $K \,\mathrm{wr}\, H$-orbit of (u, v), and, in doing so, proving that there is a sequence of indices $(j_1, j_2, \ldots, j_r) \in X^r$ such that

$$A\Gamma = A\mathcal{P}\left(r, \mathcal{G}, (j_1, j_2, \ldots, j_r)^H\right).$$

We start by computing the K^r-orbit of (u, v) (where by K^r we refer to the base group of $K \,\mathrm{wr}\, H$). Since this action is componentwise, we obtain that

$$\begin{aligned}
(u, v)^{K^r} &= \left\{\left((u_1^{k_1}, u_2^{k_2}, \ldots, u_r^{k_r}), (v_1^{k_1}, v_2^{k_2}, \ldots, v_r^{k_r})\right) \,\middle|\, (k_1, k_2, \ldots, k_r) \in K^r\right\} \\
&= \left\{((u'_1, \ldots, u'_r), (v'_1, \ldots, v'_r)) \,\middle|\, (u'_i, v'_i) \in (u_i, v_i)^K \text{ for all } i \in \{1, \ldots, r\}\right\} \\
&= A\left(\Gamma_{j_1} \times \Gamma_{j_2} \times \ldots \times \Gamma_{j_r}\right)
\end{aligned}$$

where the last equality follows from the fact that there is a unique index $j_i \in X$ such that (u_i, v_i) is an arc of Γ_{j_i}. (Recall that orbital graphs partition the arc-set of the complete digraph on Δ, see Section 1.F.)

The top group H acts by permuting the components, so that

$$(u, v)^{K \,\mathrm{wr}\, H} = \bigcup_{(j'_1, j'_2, \ldots, j'_r) \in (j_1, j_2, \ldots, j_r)^H} A\left(\Gamma_{j'_1} \times \Gamma_{j'_2} \times \ldots \times \Gamma_{j'_r}\right)$$

Therefore, the arc-sets of Γ and $\mathcal{P}\left(r, \mathcal{G}, (j_1, j_2, \ldots, j_r)^H\right)$ coincide.

As their vertex-sets are both Δ^r, the proof is complete. ■

According to the O'Nan–Scott classification (see Theorem 1.3), a primitive permutation group G is said to be *of type PA* if there exists a transitive group $H \leq \mathrm{Sym}(\Omega)$ and a primitive almost simple group $K \leq \mathrm{Sym}(\Delta)$ with socle T such that, for some integer $r \geq 2$,

$$T^r \leq G \leq K \,\mathrm{wr}\, H,$$

where T^r is the socle of G, thus contained in the base group K^r. (Be careful! Type PA in the literature can also refer to primitive group of type CD.) For our application, we need to build the orbital digraphs for primitive groups of type PA.

Theorem 3.18 · *Let $G \leq \mathrm{Sym}(\Delta) \,\mathrm{wr}\, \mathrm{Sym}(\Omega)$ be a primitive group of type PA, and let T be the socle of G_Δ^Δ. Suppose that T and G_Δ^Δ share the same orbital digraphs. Then the orbital digraphs for G coincide with the orbital digraphs for $G_\Delta^\Delta \,\mathrm{wr}\, G^\Omega$, or, equivalently, for $T \,\mathrm{wr}\, G^\Omega$.*

Proof. Since G is a primitive group of product action type, we can suppose that G is a subgroup of $G_\Delta^\Delta \,\mathrm{wr}\, G^\Omega$ with socle T^r, where $r = |\Omega|$. Further, we set $K = G_\Delta^\Delta$, $H = G^\Omega$.

As $G \leq K \,\mathrm{wr}\, H$, the partition of $\Delta^r \times \Delta^r$ in arc-sets of orbital digraphs for $K \,\mathrm{wr}\, H$ is coarser than the one for G. Hence, our aim is to show that a generic orbital digraph for $K \,\mathrm{wr}\, H$ is also an orbital digraph for G.

Let

$$\mathcal{G} = \{\Gamma_0, \Gamma_1, \dots, \Gamma_k\}$$

be the complete list of orbital digraphs for T acting on Δ, and let $X = \{0, 1, \dots, k\}$. Observe that the set of orbital digraphs for T^r can be identified with the Cartesian product of r copies of $\mathcal{G}$: indeed, we can bijectively map the generic orbital digraph for T^r, say $\Gamma_{j_1} \times \Gamma_{j_2} \times \dots \times \Gamma_{j_r}$, for some $(j_1, j_2, \dots, j_r) \in X^r$, to the generic r-tuple of the Cartesian product $\mathcal{G}^r$ of the form $(\Gamma_{j_1}, \Gamma_{j_2}, \dots, \Gamma_{j_r})$. This point of view explains why H can act on the set of orbital digraphs for T^r with its action of rank r.

Observe that the set of orbital digraphs for T^r is equal to the set of orbital digraphs for K^r. Moreover, T^r is a subgroup of G, and K^r is a subgroup of $K \,\mathrm{wr}\, H$. Thus the orbital digraphs for G and for $K \,\mathrm{wr}\, H$ are obtained as a suitable unions of the elements of $\mathcal{G}^r$.

By Lemma 3.17, the orbital digraphs for $K \,\mathrm{wr}\, H$ are of the form

$$\bigcup_{(j_1', j_2', \dots, j_r') \in (j_1, j_2, \dots, j_r)^H} \Gamma_{j_1'} \times \Gamma_{j_2'} \times \dots \times \Gamma_{j_r'},$$

for some $(j_1, j_2, \dots, j_r) \in X^r$. Aiming for a contradiction, suppose that

$$\Gamma_{j_1} \times \Gamma_{j_2} \times \dots \times \Gamma_{j_r} \quad \text{and} \quad \Gamma_{i_1} \times \Gamma_{i_2} \times \dots \times \Gamma_{i_r}$$

are two distinct orbital digraphs for T^r that are merged under the action of the top group H, but they are not under the action of G. The first proportion of the assumption yields that there is an element $h \in H$ such that

$$\left(\Gamma_{j_1} \times \Gamma_{j_2} \times \dots \times \Gamma_{j_r}\right)^h = \Gamma_{i_1} \times \Gamma_{i_2} \times \dots \times \Gamma_{i_r}.$$

By definition of $H = G^{\Omega}$, there is an element in G of the form

$$(g_1, g_2, \ldots, g_r)h \in G.$$

Recalling that, for any $i = 1, 2, \ldots, r$, $g_i \in K$, we get

$$\left(\Gamma_{j_1} \times \Gamma_{j_2} \times \ldots \times \Gamma_{j_r}\right)^{(g_1,g_2,\ldots,g_r)h} = \Gamma_{i_1} \times \Gamma_{i_2} \times \ldots \times \Gamma_{i_r}.$$

Therefore, the merging among these orbital graphs is also realised under the action of G, a contradiction.

By the initial remark, the proof is complete. ■

3.E Daily specials

The aim of Section 3.E is to give a descriptions of the digraphs appearing in Theorem K. We also compute the fixed point ratio for their automorphism groups.

3.E.1 Generalised Hamming graphs

We start by clarifying Remark 3.11.

Lemma 3.19 · *Let $H \leq \mathrm{Sym}(r)$ be a transitive permutation group, let $G = \mathrm{Alt}(\Delta) \,\mathrm{wr}\, H$ endowed with the product action on Δ^r, and let Γ be a digraph with vertex-set $V\Gamma = \Delta^r$. Then $G \leq \mathrm{Aut}(\Gamma)$ if and only if Γ is a generalised Hamming graph $\mathbf{H}(r, m, \mathcal{J})$, where $|\Delta| = m$ and $\mathcal{J} \subseteq \{0,1\}^r$ is H-invariant.*

Proof. By applying Lemma 3.17 to the group G, we obtain, in view of Definition 3.10, that Γ is a generalised Hamming graph $\mathbf{H}(r, m, \mathcal{J})$, with the prescribed properties that $|\Delta| = m$ and $\mathcal{J} \subseteq \{0,1\}^r$ is H-invariant. This completes the proof of the left-to-right direction of the equivalence.

Let us now deal with the converse implication. Let $\Gamma = \mathbf{H}(r, m, \mathcal{J})$, where $|\Delta| = m$ and $\mathcal{J} \subseteq \{0,1\}^r$ is H-invariant. Remark 3.13 gives us the opportunity of writing a normal form for the Hamming graph $\mathbf{H}(r, m, \mathcal{J})$. Indeed, consider the rearrangement of the entries of the vectors in $\mathcal{J}$ such that the representative of each orbit is a vector whose first entries are all 1, while the last ones are all 0. More explicitly, up to reordering of the Cartesian components, there are two nonnegative integers a, b with $a + b \leq r$ such that

$$\mathcal{J} = \left\{ \sum_{i=a}^{a+j} e_i \,\middle|\, j \in \{0, \ldots, b\} \right\}^H,$$

where e_i denotes the r-tuple whose only nonzero entry is in the i-th position. Substituting this $\mathcal{J}$ in Construction 3.8 and Definition 3.10, we obtain

$$\mathbf{H}(r, m, \mathcal{J}) = \bigcup_{h \in H} \left(\bigcup_{i=0}^{b} \mathbf{K}_m^{a+i} \times \mathbf{L}_m^{r-a-i} \right)^h.$$

Observe that the automorphism group of a Cartesian product of digraphs contains the Cartesian product of the automorphism group of the factors. Since the automorphism groups of $\mathbf{K}_m, \mathbf{L}_m$ or $\mathbf{K}_m \cup \mathbf{L}_m$ are isomorphic to $\mathrm{Sym}(m)$, the previous observation implies

$$\mathrm{Alt}(m)^r \leq \mathrm{Aut}\left(\bigcup_{i=0}^{b} \mathbf{K}_m^{a+i} \times \mathbf{L}_m^{r-a-i}\right).$$

Moreover, as $\mathcal{J}$ is H-invariant, the action of rank r that H induces on Δ^r preserves the arc-set of $\mathbf{H}(r, m, \mathcal{J})$. As G is generated by $\mathrm{Alt}(m)^r$ and H in their actions on Δ^r, this implies that $G \leq \mathrm{Aut}(\Gamma)$, as claimed. ■

For the sake of clarity, we would like to stress the fact that, in Lemma 3.19, the parameters m and r are not unique and they do not depend on Γ alone, but rather they depend on the Cartesian product Δ^r which G preserves. It follows that multiple groups with such property for distinct Cartesian products can be found in $\mathrm{Aut}(\Gamma)$. For instance, we can consider $\mathbf{H}(2,4)$, whose automorphism group is isomorphic to $\mathrm{Sym}(2) \,\mathrm{wr}\, \mathrm{Sym}(4)$. Let P be the Sylow 2-subgroup of $\mathrm{Sym}(4)$ (which is isomorphic to the dihedral group of degree 4), and let $G = \mathrm{Sym}(2) \,\mathrm{wr}\, P$. Since P defines two blocks of imprimitivity of size 2, we find that G fixes both the usual Cartesian product, and a Cartesian decomposition on two parts.

On the other hand, note that, for every generalised Hamming graph Γ, as $|V\Gamma|$ is finite, the integer

$$\mathbf{m}(\Gamma) := \max\{m \in \mathbb{N} \,|\, \Gamma \text{ is isomorphic to } \mathbf{H}(m, r, \mathcal{J})\}$$

is well-defined. We would like to always choose m in such a way, as this guarantees that

$$\mathrm{Alt}(m)^r \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r).$$

Definition 3.20 · We say that the parameter m of a generalised Hamming graph $\mathbf{H}(m, r, \mathcal{J})$ is *optimal* whenever

$$m = \mathbf{m}(\mathbf{H}(m, r, \mathcal{J})).$$

Instead of directly computing the relative fixity of $\mathbf{H}(r, m, \mathcal{J})$, we prove the following, slightly stronger, result.

Lemma 3.21 · *Let $K \,\mathrm{wr}\, H$ be a wreath product endowed with the product action on Δ^r, and let Γ be a digraph with vertex set Δ^r. Suppose that*

$$K \,\mathrm{wr}\, H \leq \mathrm{Aut}(\Gamma) \leq \mathrm{Sym}(\Delta) \,\mathrm{wr}\, \mathrm{Sym}(r).$$

Then

$$\mathrm{fpr}(\Gamma) = 1 - \frac{\mu(\mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(\Delta)^r)}{|V\Gamma|}.$$

In particular, whenever the parameter m is optimal in the sense of Definition 3.20, the fixed point ratio of a generalised Hamming graph is

$$\mathrm{fpr}(\mathbf{H}(r, m, \mathcal{J})) = 1 - \frac{2}{m}.$$

Proof. For simplicity's sake, let us write $|\Delta| = m$. We claim that the automorphism that realizes the minimal support size must be contained in $\mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(m)^r$ (where $\mathrm{Sym}(m)^r$ is the base group of $\mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$). Indeed, upon choosing an element of minimal support size in $K \times \{id\} \times \ldots \{id\}$ and a transposition from the top group in $\mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$, we obtain the inequalities

$$\begin{aligned}\mu(\mathrm{Aut}(\Gamma) \cap \mathrm{Sym}(m)^r) &\leq \mu(K) m^{r-1} \\ &\leq (m-1) m^{r-1} \\ &\leq \min\{|\mathrm{supp}(g)| \mid g \in \mathrm{Aut}(\Gamma) - \mathrm{Sym}(m)^r\}\end{aligned}$$

This is enough to prove the first proportion of the statement.

Since $\mathbf{H}(r, m, \mathcal{J})$ could be realized by multiple choices of the parameters m and r, we choose m to be optimal in the sense of Definition 3.20. This assumption guarantees that the automorphism group of the graph embeds into $\mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$. In particular, it is enough to look at the action of $\mathrm{Sym}(m)$ on a single component. Thus, upon choosing a transposition in $\mathrm{Sym}(m) \times \{id\} \times \ldots \{id\}$, we obtain

$$\mathrm{fpr}(\mathbf{H}(r, m, \mathcal{J})) = 1 - \frac{2m^{r-1}}{m^r} = 1 - \frac{2}{m}. \qquad \blacksquare$$

3.E.2 Distance-i Johnson graphs

The nomenclature dealing with possible generalisations of the Johnson graph is surprisingly lush. Here, we are adopting the one from [76].

Let m, k, i be integers such that $m \geq 1$, $1 \leq k \leq m$ and $0 \leq i \leq k$. A *distance-i Johnson graph*, denoted by $\mathbf{J}(m, k, i)$ is a graph whose vertex-set is the family of k-subsets of $\{1, 2, \ldots, m\}$, and such that two k-subsets, say X and Y, are adjacent whenever $|X \cap Y| = k - i$. The usual Johnson graph is then $\mathbf{J}(m, k, 1)$, and two k-subsets X and Y of $\{1, 2, \ldots, m\}$ are adjacent in $\mathbf{J}(m, k, i)$ if and only if they are at distance i in $\mathbf{J}(m, k, 1)$.

Lemma 3.22 · *Let m, k be two positive integers such that $m \geq 2k + 2$. The orbital digraphs of $\mathrm{Alt}(m)$ and of $\mathrm{Sym}(m)$ in their action on k-subsets are the distance-i Johnson graphs $\mathbf{J}(m, k, i)$, one for each choice of $i \in \{0, 1, \ldots, k\}$.*

Proof. Suppose that two k-subsets X and Y of $\{1, 2, \ldots, n\}$ are such that (X, Y) is an arc of the considered orbital digraph and $|X \cap Y| = k - i$, for a nonnegative integer $i \leq k$. Since $\mathrm{Alt}(m)$ is $(m-2)$-transitive and $2k \leq m - 2$, the $\mathrm{Alt}(m)$-orbit of the arc (X, Y) contains all the pairs (Z, W), where Z and W are k-subsets with $|Z \cap W| = k - i$. Therefore, the statement is true for the alternating group. The same proof can be repeated *verbatim* for $\mathrm{Sym}(m)$. ■

Lemma 3.23 · *Let m, k, i be three positive integers such that $m \geq 2k + 2$ and $i < k$. Then the fixed point ratio of the distance-i Johnson graphs $\mathbf{J}(m, k, i)$ is*

$$\mathrm{fpr}(\mathbf{J}(m, k, i)) = 1 - \frac{2k(m-k)}{m(m-1)}.$$

Proof. Under our assumption, by [75, Theorem 2 (a)], the automorphism group of $\mathbf{J}(m, k, i)$ is $\mathrm{Sym}(m)$ in its action on k subsets. Its minimal degree is achieved by any transposition (see [64, Section 1]), where

$$\mu(\mathrm{Sym}(m)) = 2\binom{m-2}{k-1}.$$

Hence, we find that

$$\mathrm{fpr}(\mathbf{J}(m,k,i)) = 1 - \frac{2k(m-k)}{m(m-1)}.$$ ■

3.E.3 Squashed distance-i Johnson graphs

As we have seen in Section 1.J, a routine construction in the realm of distance transitive graphs consists in obtaining smaller example starting from a distance transitive graph and identifying antipodal vertices. We need to apply this idea to a family of generalised Johnson graphs.

Consider the distance-i Johnson graph $\mathbf{J}(2m,m,i)$, for some integers m and i, with m positive and $0 \le i \le m$. We say that two vertices of $\mathbf{J}(2m,m,i)$ are *disjoint* if they have empty intersection as m-subset. Observe that being disjoint is an equivalence relation, and our definition coincides with the usual notion of antipodal for $\mathbf{J}(2m,m,1)$ seen as a metric space. We can build a new graph $\mathbf{QJ}(2m,m,i)$ whose vertex-set is the set of equivalence classes of the disjoint relation, and such that, if $[X]$ and $[Y]$ are two vertices, then $([X],[Y])$ is an arc in $\mathbf{QJ}(2m,m,i)$ whenever there is a pair of representatives, say $X' \in [X]$ and $Y' \in [Y]$, such that (X',Y') is an arc in $\mathbf{J}(2m,m,i)$. We call $\mathbf{QJ}(2m,m,i)$ a *squashed distance-i Johnson graph*.

Observe that $\mathbf{J}(2m,m,i)$ is a regular double cover of $\mathbf{QJ}(2m,m,i)$. Furthermore, $\mathbf{QJ}(2m,m,i)$ and $\mathbf{QJ}(2m,m,m-i)$ are isomorphic graphs, thus we can restrict the range of i to $\{0,1,\dots,\lfloor m/2\rfloor\}$.

Lemma 3.24 · *Let $m \ge 3$ be an integer. The orbital digraphs of* $\mathrm{Alt}(2m)$ *and of* $\mathrm{Sym}(2m)$ *in their primitive actions with stabilizer* $(\mathrm{Sym}(m)\,\mathrm{wr}\,C_2)\cap\mathrm{Alt}(2m)$ *and* $\mathrm{Sym}(m)\,\mathrm{wr}\,C_2$ *respectively are the squashed distance-i Johnson graphs* $\mathbf{QJ}(m,k,i)$, *one for each choice of $i \in \{0,1,\dots,\lfloor m/2\rfloor\}$.*

Proof. To start, we note that the set Ω on which the groups are acting can be identified with the set of partitions of the set $\{1,2,\dots,2m\}$ with two parts of equal size m. Suppose that $\{X_1,X_2\}$ and $\{Y_1,Y_2\}$ are two such partitions and that $(\{X_1,X_2\},\{Y_1,Y_2\})$ is an arc of the orbital digraph we are building, with

$$\min\{|X_1 \cap Y_1|, |X_1 \cap Y_2|\} = m-i,$$

for a nonnegative integer $i \le \lfloor m/2\rfloor$. To determine the image of $(\{X_1,X_2\},\{Y_1,Y_2\})$ under the group action, it is enough to know the images of X_1 and Y_2, that is, of at most $2m-\lceil m/2\rceil \le 2m-2$ distinct points. By the $(2m-2)$-transitivity of $\mathrm{Alt}(2m)$, the $\mathrm{Alt}(2m)$-orbit of $(\{X_1,X_2\},\{Y_1,Y_2\})$ contains all the arc of the form $(\{Z_1,Z_2\},\{W_1,W_2\})$, where $\{Z_1,Z_2\},\{W_1,W_2\} \in \Omega$ and

$$\min\{|Z_1 \cap W_1|, |Z_1 \cap W_2|\} = m-i.$$

To conclude, observe that Ω is the set of m-subsets of $\{1,2,\dots,2m\}$ in which two elements are identified if they are disjoint, and that

$$\min\{|X_1 \cap Y_1|, |X_1 \cap Y_2|\} = m - i\,,$$

is the adjacency condition in an squashed distance-i Johnson graph. As in the proof of Lemma 3.22, the same reasoning can be exteneded to $\mathrm{Sym}(2m)$. Therefore, the orbital digraphs of $\mathrm{Alt}(2m)$ and of $\mathrm{Sym}(2m)$ in these primitive actions are the squashed distance-i Johnson graphs $\mathbf{QJ}(2m,m,i)$, for some index $i \in \{0,1,\dots,\lfloor m/2\rfloor\}$. ■

Lemma 3.25 · *Let m,i be two positive integers such that $m \ge 3$ and $i < \lfloor m/2\rfloor$. Then the fixed point ratio of the distance-i Johnson graphs $\mathbf{QJ}(2m,m,i)$ is*

$$\mathrm{fpr}(\mathbf{QJ}(2m,m,i)) = 1 - \frac{2k(m-k)}{m(m-1)}\,.$$

Proof. Consider $\mathbf{J}(2m,m,i)$, the regular double covering of $\mathbf{QJ}(2m,m,i)$. In view of [75, Theorem 2 (e)], the automorphism group of $\mathbf{J}(2m,m,i)$ is $\mathrm{Sym}(2m) \times \mathrm{Sym}(2)$, where the central involution swaps pairs disjoint vertices. It follows that the automorphism group of $\mathbf{QJ}(2m,m,i)$ is $\mathrm{Sym}(2m)$. Now, we can immediately verify that the stabilizer of the vertex $\{\{1,2,\dots,m\},\{m+1,m+2,\dots,2m\}\}$ is $\mathrm{Sym}(m)\,\mathrm{wr}\,C_2$. The minimal degree of the primitive action of $\mathrm{Sym}(2m)$ with stabilizer $\mathrm{Sym}(m)\,\mathrm{wr}\,C_2$ is

$$\mu(\mathrm{Sym}(2m)) = \frac{1}{4}\left(1 + \frac{1}{2m-1}\right)\frac{(2m)!}{m!^2}$$

(see [27, Theorem 4]). Thus, we find that

$$\mathrm{fpr}(\mathbf{QJ}(2m,m,i)) = \frac{1}{2}\left(1 - \frac{1}{2m-1}\right).$$ ■

3.E.4 Strongly regular graphs

We list all the strongly regular graphs appearing as Γ_1 in Theorem K (c). We divide them according to the socle L of the almost simple group that acts on them. (We point out that this list keeps the same enumeration as the one of the corresponding socles in Theorem 3.7 (e).)

(i) $L = U_4(q)$, $q \in \{2,3\}$, acting on totally singular 2-dimensional subspaces of the natural module, two vertices of Γ are adjacent if there is a third 2-dimensional subspace that intersect both vertices in a 1-dimensional subspace (see [24, Section 2.2.12]);

(ii) $L = \Omega_{2m+1}(3), m \ge 2$, acting on the singular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Theorem 2.2.12]);

(iii) $L = \Omega_{2m+1}(3), m \ge 2$, acting on the nonsingular points of the natural module, two vertices of Γ are adjacent if the line that connects them is tangent to the quadric where the quadratic form vanishes (see [24, Section 3.1.4]);

(*iv*) $L = \mathrm{P}\Omega^{\epsilon}_{2m}(2), \epsilon \in \{+,-\}, m \geq 3$, acting on the singular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Theorem 2.2.12]);

(*v*) $L = \mathrm{P}\Omega^{\epsilon}_{2m}(2), \epsilon \in \{+,-\}, m \geq 2$, acting on the nonsingular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Section 3.1.2]);

(*vi*) $L = \mathrm{P}\Omega^{+}_{2m}(3), m \geq 2$ acting on the nonsingular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Section 3.1.3]);

(*vii*) $L = \mathrm{P}\Omega^{-}_{2m}(3), m \geq 3$ acting on the singular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Theorem 2.2.12]);

(*viii*) $L = \mathrm{P}\Omega^{-}_{2m}(3), m \geq 2$ acting on the nonsingular points of the natural module, two vertices of Γ are adjacent if they are orthogonal (see [24, Section 3.1.3]).

All the permutation groups described have rank 2. We recall that all the groups of rank 3 define two strongly regular graphs as their nondiagonal orbital graph. Hence, we do not need to waste any ink to show that these graphs are actually strongly regular.

Table 3.3 collects the usual parameters of a strongly regular graph, (v, d, λ, μ), and their relative fixity. Recall that v is the number of vertices, d is the valency of the graph, λ is the number of common neighbours between two adjacent vertices, and μ is the number of common neighbours between two nonadjacent vertices. As $\mu(G)$ can be found in [27, Theorem 4], the fixed point ratio is computed as

$$\mathrm{fpr}(\Gamma) = 1 - \frac{\mu(G)}{v}.$$

3.F Proofs of Theorem K and Corollary L

All our tools are sharp enough to prove Theorem K. This proof takes most of Section 3.F.

Proof of Theorem K. The proof is split in two independent chunks. First, we prove that every vertex-primitive digraph whose fixed point ratio exceeds $\frac{1}{3}$ belongs to one of the families appearing in Theorem K. Then, we tackle the problem of computing the relative fixities of the graphs appearing in Theorem K, thus showing that they indeed all have fixed point ratios larger than $\frac{1}{3}$.

Assume that Γ is a digraph on n vertices with at least one arc and with $\mathrm{fpr}(\Gamma) > \frac{1}{3}$ such that $G = \mathrm{Aut}(\Gamma)$ is primitive. If Γ is disconnected, then the primitivity of G implies that Γ is isomorphic to the loop graph $\mathbf{L}_n$. Hence, we may assume that Γ is connected. Moreover, $\mathrm{fpr}(\Gamma) > \frac{1}{3}$ implies that $\mu(G) < \frac{2n}{3}$. Hence G is one of the groups determined in [27] and described in Theorem 3.7.

	Socle	v	d	λ	μ	fpr	Comments
(i)	$U_4(2)$	27	10	1	5	$\frac{7}{27}$	
	$U_4(3)$	112	30	2	10	$\frac{11}{56}$	
(ii)	$\Omega_{2m+1}(3)$	$\frac{1}{2}(9a-1)$	$\frac{3}{2}(a^2-1)$	$\frac{1}{2}(a^2-9)+2$	$\frac{1}{2}(a^2-1)$	$\frac{a+1}{3a+1}$	$a=3^{m-1}$
(iii)	$\Omega_{2m+1}(3)$	$\frac{3a}{2}(3a-1)$	$(a-1)(3a+1)$	$2(a^2-a-1)$	$2a(a-1)$	$\frac{3a^2+a+1}{3a(3a-1)}$	
(iv)	$\mathrm{P}\Omega^+_{2m}(2)$	$(4b-1)(2b-1)$	$2(2b-1)(b+1)$	$(2b-2)(b-2)+1$	$(2b-1)(b+1)$	$\frac{b-1}{2b-1}$	$b=2^{m-2}$
	$\mathrm{P}\Omega^-_{2m}(2)$	$4b^2-1$	$2(b^2-1)$	b^2-3	b^2-1	$\frac{2b+1}{4b+1}$	
(v)	$\mathrm{P}\Omega^\epsilon_{2m}(2)$	$2b(4b-\epsilon)$	$4b^2-1$	$2(b^2-1)$	$b(2b+\epsilon)$	$\frac{2b}{4b-\epsilon}$	$\epsilon=\pm 1$
(vi)	$\mathrm{P}\Omega^+_{2m}(3)$	$\frac{3c}{2}(9c-1)$	$\frac{3c}{2}(3c-1)$	$\frac{c}{2}(3c-1)$	$\frac{3c}{2}(c-1)$	$\frac{3(c+1)}{9c-1}$	$c=3^{m-2}$
(vii)	$\mathrm{P}\Omega^-_{2m}(3)$	$\frac{1}{2}(9c^2-1)$	$\frac{3}{2}(c^2-1)$	$\frac{1}{2}(c^2-9)+2$	$\frac{1}{2}(c^2-1)$	$\frac{3c+1}{9c+1}$	
$(viii)$	$\mathrm{P}\Omega^-_{2m}(3)$	$\frac{3c}{2}(9c+1)$	$\frac{3c}{2}(3c+1)$	$\frac{c}{2}(3c-1)$	$\frac{3c}{2}(c+1)$	$\frac{9c^2+3c-2}{3c(9c+1)}$	

Table 3.3: Parameters of strongly regular graphs with large fixity.

Suppose that G is an almost simple group. Then G is one of the groups appearing in parts (a) – (e) of Theorem 3.7. Since any G-vertex-primitive graph is a union of orbital digraphs for G, the digraphs arising from these cases will be merged product action digraphs $\mathcal{P}(1,\mathcal{G},\mathcal{J})$ (see Remark 3.9). Hence, our goal is to consider these almost simple groups in turn and compile their list of orbitals digraphs $\mathcal{G}$.

Let G be a group as described in Theorem 3.7 (a). Lemma 3.22 states the orbital digraphs for G are the distance-i Johnson graph $\mathbf{J}(m,k,i)$.

Assume that $k=1$, that is, consider the natural action of either $\mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$ of degree m. Since this action is 2-transitive, their set of orbital digraphs is $\mathcal{G}=\{\mathbf{L}_m,\mathbf{K}_m\}$. In particular, $\mathcal{P}(1,\mathcal{G},\mathcal{J})=\mathbf{H}(1,m,\mathcal{J})$. This case exhausts the generalised Hamming graphs with $r=1$, which appear in Theorem K (i). Therefore, in view of Remark 3.12, for as long as we suppose $r=1$, we can also assume that $\mathcal{J}$ is a non-Hamming homogeneous set. Observe $m\geq 4$, otherwise, we go against our assumption on the fixed point ratio.

Going back to distance-i Johnson graphs, we have to take $k\geq 2$ to guarantee that $\mathcal{J}$ is non-Hamming. Thus,

$$\mathcal{G}=\{\mathbf{J}(m,k,i)\mid i\in\{0,1,\dots,k\}\}\,,$$

which corresponds to Theorem K $(ii)(a)$.

Let $G=\mathrm{Sym}(2m)$ be a permutation group from Theorem 3.7 (b). If $m=2$, the degree of G is 3, and the relative fixity of any action of degree 3 can either be 0 or $\frac{1}{3}$. Hence, we must suppose that $m\geq 3$: by Lemma 3.24, the orbital digraphs for G are the squashed distance-i Johnson graph $\mathbf{QJ}(2m,m,i)$. We obtain that

$$\mathcal{G}=\{\mathbf{QJ}(2m,m,i)\mid i\in\{0,1,\dots,\lfloor m/2\rfloor\}\}\,,$$

as described in Theorem K $(ii)(b)$.

Let $G=M_{22}:2$ in the action described in Theorem 3.7 (c). Consulting the list of all the primitive groups of degree 22 in Magma [20] (which is based on the list compiled in [43]), we realize that they are all 2-transitive. Hence, the set of orbital digraphs is $\mathcal{G}=\{\mathbf{K}_{22},\mathbf{L}_{22}\}$. In particular, all the graphs are generalised Hamming graphs.

Let G be an almost simple of Lie type appearing in Theorem 3.7 (d). Since all these groups are 2-transitive with a 2-transitive socle L, their orbital digraphs are either $\mathbf{K}_m$ or $\mathbf{L}_m$, where $m\geq 7$ is the degree of G. Once again, we obtain only generalise Hamming graphs.

Let G be an almost simple of Lie type described in Theorem 3.7 (e). Any group of permutational rank 3 defines two nondiagonal orbital digraphs, and, as such digraphs are arc-transitive and one the complement of the other, they are strongly regular digraphs (see, for instance, [24, Section 1.1.5]). The set of orbital digraphs is of the form $\mathcal{G}=\{\mathbf{L}_m,\Gamma_1,\Gamma_2\}$, where we listed the possible Γ_1 in Section 3.E.4, and where $m=|V\Gamma_1|$. The graphs described in this paragraph appear in Theorem K $(ii)(c)$.

We have exhausted the almost simple groups from Theorem 3.7.

Suppose that $G\leq K\,\mathrm{wr}\,\mathrm{Sym}(r)$ is a primitive group of type PA. Recall that G appears in Theorem 3.7 (f). We want to apply Theorem 3.18 to G. The only hypothesis we miss is that T and G_Δ^Δ share the same set of orbital digraphs.

We claim that T and K induces the same set of orbital digraphs. If K is either alternating or symmetric, the claim follows from Lemmas 3.22 and 3.24. If K is 2-transitive, then we can observe that its socle L is also 2-transitive: the socle of $M_{22}:2$ is $T = M_{22}$ in its natural 3-transitive action, while the socle T of the almost simple groups of Lie type of rank 2 is 2-transitive by [31, Section 5]. In particular, K and T both have $\mathcal{G} = \{\mathbf{L}_m, \mathbf{K}_m\}$ as their set of orbital graphs. Finally, suppose that K is an almost simple group of permutational rank 3. We have that its socle T is also of permutational rank 3 by [79, Theorem 1.1]. Observe that, since any orbital digraph for T is a subgraph of an orbital digraph for K, the fact that K and T both have permutational rank 3 implies that they share the same set of orbital digraphs. Therefore, the claim is true.

By our claim together with the double inclusion

$$T \leq G_\Delta^\Delta \leq K,$$

we obtain that T, G_Δ^Δ and K all induce the same set of orbital digraphs. Therefore, we can apply Theorem 3.18 to G: we obtain that G shares its orbital graphs with $T \operatorname{wr} G^\Omega$.

Therefore, all the G-vertex-primitive digraphs are union of orbital digraphs for $T \operatorname{wr} H$, with T the socle type of G and H a transitive permutation group isomorphic to G^Ω. In other words, we found all the graphs $\mathcal{P}(r, \mathcal{G}, \mathcal{J})$ with $r \geq 2$ described in Theorem K. (Recall that, by Definition 3.10, among the graphs $\mathcal{P}(r, \mathcal{G}, \mathcal{J})$, we find all the generalised Hamming graphs.)

Suppose that G is an affine group. Then the regular socle N is an elementary abelian 2-subgroup. We have that G can be written as the split extension $N \rtimes H$, where H is a group of matrices that acts irreducibly on N. It follows that G is 2-transitive on N, hence, as $|N| \geq 4$, the graphs arising in this scenario are $\mathbf{L}_{|N|}, \mathbf{K}_{|N|}$ and $\mathbf{L}_{|N|} \cup \mathbf{K}_{|N|}$, which are generalised Hamming graphs.

We have completed the first part of the proof, showing that the list of vertex-primitive digraphs appearing in Theorem K is exhaustive. As all the orbital digraphs in $\mathcal{G}$ are actually graphs, the same property is true for the graphs in the list, as we have underlined in Remark 3.14.

We can now pass to the second part of the proof, that is, we can now tackle the computation of fixed point ratios. We already took care of the generalised Hamming graphs in Lemma 3.21. Thus, we can suppose that Γ is a merged product action graph $\mathcal{P}(r, \mathcal{G}, \mathcal{J})$ appearing in Theorem K (ii).

Suppose that $r = 1$, that is, Γ is a union of graphs for some primitive almost simple group K. (We are tacitly assuming that K is maximal among the groups appearing in a given part of Theorem 3.7.) In view of [88, Theorem], we have that K is a maximal subgroup of either $\operatorname{Alt}(|V\Gamma|)$ or $\operatorname{Sym}(|V\Gamma|)$. Therefore, there are just two options for $\operatorname{Aut}(\Gamma)$: either it is isomorphic to K or it contains $\operatorname{Alt}(|V\Gamma|)$. In the latter scenario, as $\operatorname{Alt}(|V\Gamma|)$ is 2-transitive on the vertices, we obtain that $\Gamma \in \{\mathbf{L}_m, \mathbf{K}_m, \mathbf{L}_m \cup \mathbf{K}_m\}$. All those graphs are generalised Hamming graphs, against our assumption on Γ. Therefore, we have $K = \operatorname{Aut}(\Gamma)$. In particular, the relative fixity for Γ are computed in Lemma 3.23, Lemma 3.25 or Table 3.3 given that $\mathcal{G}$ is described in Theorem K $(ii)(a)$, $(ii)(b)$ or $(ii)(c)$ respectively.

Suppose now that $r \geq 2$. The automorphism group of Γ either embeds into $\mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$, where $m = |V\Gamma_i|$ for any $\Gamma_i \in \mathcal{G}$, or, by maximality of the wreath product $\mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$, $\mathrm{Aut}(\Gamma) = \mathrm{Sym}(m^r)$. In the latter scenario, $\Gamma \in \{\mathbf{L}_m, \mathbf{K}_m, \mathbf{L}_m \cup \mathbf{K}_m\}$. All these graphs can be written as a merged product graph where $r = 1$ and $\mathcal{J}$ is a Hamming set. This goes against our assumption on Γ, thus we must suppose $\mathrm{Aut}(\Gamma) \neq \mathrm{Sym}(m^r)$.

As a consequence, we obtain that, for some almost simple group K listed in Theorem 3.7 (a)–(e), and for some transitive group $H \leq \mathrm{Sym}(r)$, $K \,\mathrm{wr}\, H \leq \mathrm{Aut}(\Gamma)$. Note that, as $K \leq \mathrm{Aut}(\Gamma)_\Delta^\Delta$, by [88, Theorem], $\mathrm{Aut}(\Gamma)_\Delta^\Delta$ is either K or it contains $\mathrm{Alt}(m)$. If the latter case occurs, then $\mathrm{Alt}(m)^r \,\mathrm{wr}\, H \leq \mathrm{Aut}(\Gamma)$. By Lemma 3.19, Γ is a generalised Hamming graph, which contradicts our choice of Γ. Therefore, $\mathrm{Aut}(\Gamma) \leq K \,\mathrm{wr}\, \mathrm{Sym}(r)$.

Observe that we can apply Lemma 3.21. We obtain that

$$\mathrm{fpr}(\Gamma) = 1 - \frac{\mu(K) m^{r-1}}{m^r} = 1 - \frac{\mu(K)}{m} = \mathrm{fpr}\left(\mathcal{P}(1, \mathcal{G}, \mathcal{J}')\right),$$

for some non-Hamming homogeneous set $\mathcal{J}'$. In particular, the fixed point ratios for $r \geq 2$ coincides with those we have already computed for $r = 1$. This complete the proof. ■

We conclude Section 3.F with the proof of Corollary L.

Proof of Corollary L. Note that, upon taking union of digraphs, the valency can only increase. Thus, to give a lower bound to the valency, we can assume, without loss of generality, that Γ is an orbital graph (that is, we chose $\mathcal{J}$ in Theorem K to be a single orbit). We split the discussion between the cases $r = 1$ and $r \geq 2$.

Assume that $r = 1$. If Γ is a generalised Hamming graph as in Theorem K (i), then Γ is either $\mathbf{K}_m$ or $\mathbf{L}_m \cup \mathbf{K}_m$, for some $m \geq 4$. In particular,

$$|V\Gamma| = m - 1 \geq \log(m) = \log\left(|V\Gamma|\right).$$

Suppose that $\Gamma = \mathcal{P}(1, \mathcal{G}, \mathcal{J})$ is a merged product action graph. If $\mathcal{G}$ is as in Theorem K $(ii)(a)$, then Γ is isomorphic to a distance-i Johnson graph. Among them, the minimal valency is achieved by the proper Johnson graph, that is, $i = 1$, whose valency is $k(m-k)$. Hence, we obtain

$$\mathrm{val}(\Gamma) \geq k(m-k) \geq k\frac{m}{2} \geq k\log(m) \geq \log\left(\binom{m}{k}\right) = \log\left(|V\Gamma|\right).$$

Suppose that $\mathcal{G}$ is described in Theorem K $(ii)(b)$, that is, if Γ is a squashed distance-i Johnson graph. As the Johnson distance-i graph with $k = m/2$ is a regular double cover of Γ, and the previous inequalities holds also if $k = m/2$, we conclude in the same way.

To conclude the case $r = 1$, we have to choose $\mathcal{G}$ as in Theorem K $(ii)(c)$. A direct inspection of Table 3.3 reveals that $|V\Gamma| \geq 6$ and

$$\mathrm{val}(\Gamma) \geq \frac{|V\Gamma|}{3} \geq \log\left(|V\Gamma|\right).$$

Observe that, in all the cases, we showed that the constant C is greater than 1.

Assume that $r \geq 2$. Suppose that Γ is either a generalised Hamming graph $\mathbf{H}(r,m,\mathcal{J})$ or a merged product action graph $\mathcal{P}(r,\mathcal{G},\mathcal{J})$, where $\mathcal{J} = \mathbf{j}^H$ for some transitive $H \leq \mathrm{Sym}(r)$ and some $\mathbf{j} = (j_1, j_2, \dots, j_r) \in X^r$. Recall that we have suppose that $\Gamma_0 = \mathbf{L}_m$, thus $\mathrm{val}(\Gamma_0) = 1$. Observe that, by applying the Orbit Stabilizer Lemma on the rank r action,

$$\mathrm{val}(\Gamma) = \left|\mathbf{j}^H\right| \cdot \mathrm{val}\left(\Gamma_{j_1}\right)\mathrm{val}\left(\Gamma_{j_2}\right)\dots\mathrm{val}\left(\Gamma_{j_r}\right).$$

For any $\mathbf{x} = (x_1, x_2, \dots, x_r) \in X^r$, we define

$$w(\mathbf{x}) = \sum_{i=1}^{r} 1 - \delta(0, x_i).$$

(By $\delta(a,b)$ we are denoting the Kronecker delta between a and b.) To guarantee connectedness, at least one of the indices j_i must be nonzero, which implies that $w(\mathbf{j}) \geq 1$. Moreover, since H is transitive, we can compute

$$|\mathbf{j}^H| w(\mathbf{j}) = \sum_{\mathbf{x}\in\mathbf{j}^H} w(\mathbf{x}) \geq r.$$

Hence,

$$|\mathbf{j}^H| \geq \frac{r}{w(\mathbf{j})}.$$

Therefore, upon setting $w = w(\mathbf{j})$ and $d = \min\{\mathrm{val}(\Gamma_i) \mid \Gamma_i \in \mathcal{G}, i \neq 0\}$, we obtain

$$\mathrm{val}(\Gamma) \geq \min\left\{ d^w \frac{r}{w} \,\middle|\, 1 \leq w \leq r \right\}.$$

Recall that, by Construction 3.8, $|V\Gamma| = |V\Gamma_{j_1}|^r$. By the case with $r = 1$, we have $d \geq C\log(|V\Gamma_{j_1}|)$, for a universal constant $C \geq 1$. Also, for any $m \geq 4$ and for any $w \geq 1$, a direct computation shows that

$$\frac{\log(m)^{w-1}}{w} \geq \frac{e\log\left(\log(4)\right)}{\log(4)} \geq 0.64.$$

We conclude

$$\begin{aligned}
\mathrm{val}(\Gamma) &\geq \min\left\{ d^w \frac{r}{w} \,\middle|\, 1 \leq w \leq r \right\} \\
&\geq \min\left\{ C^w \log(|V\Gamma_{j_1}|)^w \frac{r}{w} \,\middle|\, 1 \leq w \leq r \right\} \\
&= \min\left\{ C^w \frac{\log(|V\Gamma_{j_1}|)^{w-1}}{w} \,\middle|\, 1 \leq w \leq r \right\} \log(|V\Gamma|) \\
&\geq \min\left\{ \frac{\log(|V\Gamma_{j_1}|)^{w-1}}{w} \,\middle|\, 1 \leq w \leq r \right\} \log(|V\Gamma|) \\
&\geq 0.64 \cdot \log\left(|V\Gamma|\right)
\end{aligned}$$

This concludes the proof with the universal constant $C = 0.64$. ■

3.G Bounding the exponent

Let G be a finite group. The *exponent of* G is the minimal positive integer e such that, for every $g \in G$, $g^e = 1$, and we denote it by $\exp(G)$.

Let G be a group of automorphisms of a connected d-valent graph with finite vertex-stabilizer. (In this section, we need not to require the graph to be finite: indeed, all the results mentioned holds for locally finite graphs.) The exponent of G is loosely related to the diameter of the graph. In particular, no information about $\exp(G)$ can be gathered from local information on G.

On the other hand, the situation seems different if we consider the exponent of a vertex-stabilizer. For instance, let α be a vertex, and suppose that the local group of the pair (Γ, G) is graph-restrictive. Then, if $\mathbf{f}(d)$ is a function such that $|G_\alpha| \le \mathbf{f}(d)$, then, as the exponent divides the order of the group,

$$\exp(G_\alpha) \le |G_\alpha| \le \mathbf{f}(d).$$

Moreover, a direct inspection of the amalgams described in Section 1.H shows that there is a universal constant C that bounds from above the order of G_α for all graphs of order 3 and 4.

As for Definition 1.34, we introduce a name for the local groups showing this behaviour.

Definition 3.26 · Let L be a permutation group. We say that L is *exponent-restrictive* if there is a constant $\mathbf{e}(L)$ such that, for every pair (Γ, G) with Γ a locally finite connected graph, G a vertex-transitive group of automorphism with finite vertex-stabilizer, and local group L,

$$|G_\alpha| \le \mathbf{e}(L).$$

We are aware of one class of local group that are not graph-restrictive but are exponent-restrictive. The following notion, introduced in [157], is quite involved, so we number it for future reference.

Definition 3.27 · Let p be a prime and let L be a transitive permutation group acting on a set Ω. Then L is *weakly p-subregular* provided that there exist points $x, y \in \Omega$ such that $|L_x| = |L_y| = p$ and $x^M \cup y^M = \Omega$, where $M = \langle L_x, L_y \rangle$.

For instance, any dihedral group in its natural action is weakly 2-subregular. Indeed, choose any two points, say x and y, and, if the degree is even, impose that y does not belong to the orbit of x under the cyclic subgroup whose degree is half of the original. We have that $L_x = C_2$, and that M is, if the degree is odd, the whole dihedral group or, when the degree is even, the dihedral subgroup of index 2 while x and y belong to the two distinct orbits.

Theorem M · *Let p be a prime, and let L be a weakly p-subregular permutation group. Then L is exponent-restricitive of constant*

$$\mathbf{e}(L) = p^3 \exp(L).$$

In particular, every dihedral group is exponent-restrictive.

3.G.1 Proof of Theorem M

This proof of Theorem M is taken from an unpublished note of P. Potočnik and P. Spiga. It heavily relies on two theorems of G. Glauberman (see Theorem 3.28 below). We start by introducing the notation needed to state them.

Let G be a group, and let i be a positive integer. We denote by $\gamma_i(G)$ the *i-th term of the lower central series*, which is defined inductively by putting $\gamma_1(G) = G$, and for every $i \geq 2$, $\gamma_i(G) = [\gamma_{i-1}(G), G]$. Furthermore, suppose that G is a p-group. We define

$$\Omega_i(G) = \langle g \mid g \in G, g^{p^i} = 1\rangle$$

and

$$\mho^i(G) = \langle g^{p^i} \mid g \in G\rangle.$$

Finally, the *Thompson subgroup of G*, denoted by $\mathbf{J}(G)$, is the subgroup generated by all abelian subgroups of maximal order.

Theorem 3.28 ([61] Theorem 1, and [62] Theorem 1) · *Let p be a prime, let P be a finite p-group, let Q and R be subgroups of P of index p, let $\varphi : Q \to R$ be a group isomorphism, and let N be the group generated by all subgroups T of P such that $T^\varphi = T$. Then N is normal in P. Let c be the nilpotency class of P/N. Then P satisfies at least one of the following conditions:*

(i) $\Omega_1(\mathbf{Z}(P)) = \Omega_1(\mathbf{Z}(Q)) = \Omega_1(\mathbf{Z}(R))$;

(ii) $\mathbf{J}(P) = \mathbf{J}(Q) = \mathbf{J}(R)$;

(iii) P/N *is abelian;*

(iv) one of the following holds:

(a) $p = 2, c \leq 2$ *and*

$$\gamma_{c+2}(P)\mho^{c+1}(P) = \gamma_{c+2}(Q)\mho^{c+1}(Q) = \gamma_{c+2}(R)\mho^{c+1}(R);$$

(b) $p = 3, c \leq 3$, *and*

$$\gamma_{c+2}(P)\mho^{2}(P) = \gamma_{c+2}(Q)\mho^{2}(Q) = \gamma_{c+2}(R)\mho^{2}(R);$$

(c) $p \geq 5, c \leq 3$, *and*

$$\gamma_{c+2}(P)\mho^{1}(P) = \gamma_{c+2}(Q)\mho^{1}(Q) = \gamma_{c+2}(R)\mho^{1}(R).$$

The normality of N in P is essentially due to Sims (see [139]), and the proof can be found in [61, Proposition 2.1].

What we will be using is actually the following consequence of Theorem 3.28.

Corollary 3.29 · *Let G be a group, let P be a p-subgroup of G, and let Q be a subgroup of P of index p. Further, let $g \in G$ and let N be the group generated by all the subgroups of Q normalised by g. Then N is normal in P. Furthermore, one of the following holds:*

(*i*) *there exists a nontrivial subgroup of Q which is characteristic in P and Q and is normalised by g;*

(*ii*) *the exponent of P is at most* p^3 *(more precisely, it is at most* p^2 *if* $p = 3$ *and is* p *if* $p \geq 5$*);*

(*iii*) P/N *is abelian.*

Proof. We are considering each of the cases of Theorem 3.28 in turn.

Suppose Theorem 3.28 (*i*) occurs. Note that $\Omega_1(\mathbf{Z}(P))$ is characteristic in both P and Q. Compute

$$\Omega_1(\mathbf{Z}(P))^g = \Omega_1(\mathbf{Z}(Q))^g = \Omega_1(\mathbf{Z}(Q^g)) = \Omega_1(\mathbf{Z}(Q)) = \Omega_1(\mathbf{Z}(P)).$$

The previous equality implies that $\Omega_1(\mathbf{Z}(P))$ is normalized by g (thus it is also characteristic in P^g). Moreover, as P is a p-group, $\Omega_1(\mathbf{Z}(P))$ is the non-trivial subgroup of Q described in Corollary 3.29 (*i*).

Suppose Theorem 3.28 (*ii*) occurs. By applying the same reasoning, we get that $\mathbf{J}(P)$ is the non-trivial subgroup of Q described in Corollary 3.29 (*i*).

Suppose Theorem 3.28 (*iii*) occurs. This is the same as asking that Corollary 3.29 (*iii*) holds.

Suppose Theorem 3.28 (*iv*) occurs. Since the prime p is already understood, let us write $\gamma(P)$ and $\mho(P)$ without their appropriate indices. We have two possibilities: either $\gamma(P)\mho(P)$ is trivial, or it is not. In the former case, as $\gamma(P)\mho(P)$ is trivial, *a fortiori* $\mho(P)$ is trivial, hence Corollary 3.29 (*ii*) holds. In the latter case, if $\gamma(P)\mho(P)$ is a nontrivial characteristic subgroup of Q and of P. Hence, we can replicate the reasoning we used for the first and second item, thus obtaining that Corollary 3.29 (*i*) holds. ∎

We can now dive in the proof of Theorem M.

Proof of Theorem M. Let Γ be a connected graph, and let G be an arc-transitive group of automorphisms. We can choose a vertex α whose associated local group is weakly p-subregular for some prime p. Recall that by $G_\alpha^{[1]}$ we denote the kernel of the action of G_α on the neighbourhood $\Gamma(\alpha)$. By Definition 3.27, there exist two neighbours of α, say β and γ, such that

$$|G_{\alpha\beta}^{\Gamma(\alpha)}| = |G_{\alpha\gamma}^{\Gamma(\alpha)}| = p,$$

and such that $\beta^M \cup \gamma^M = \Gamma(\alpha)$, where

$$M = \langle G_{\alpha\beta}^{\Gamma(\alpha)}, G_{\alpha\gamma}^{\Gamma(\alpha)} \rangle.$$

To simplify the notation (and to foreshadow how we will apply Corollary 3.29), we let

$$P = G_{\alpha\beta} \quad \text{and} \quad Q = G_\alpha^{[1]}.$$

Note that, since the point-stabilizer of the local group has order p, by the Orbit Stabilizer Lemma, the index of Q in P is p. Moreover, by adapting the proof of Lemma 1.32, we can show that P is a p-group. Indeed, aiming for a contradiction, let $t \in P$ be a nontrivial element of P whose order is coprime with p. Observe that, as $|P : Q| = p$, t fixes the neighbourhood of α. Let δ be a vertex at minimal distance from α such that δ^t and δ are distinct. By connectedness of Γ, there is a path $(\delta'', \delta', \delta)$ such that (δ'', δ') is an edge fixed by t. In particular,

$$t \in G_{\delta''\delta'}^{\Gamma(\delta')}.$$

As p does not divide the order of t, this contradicts the fact that the order of the group underlying the local group is p. Hence, the claim is proved.

Now, let g be an element of G mapping the arc (β, α) to the arc (α, γ). We define

$$H = \langle P, g \rangle.$$

We observe that $G_{\alpha\gamma} = P^g$ is a subgroup of H.

Let us show that H acts transitively on the edge-set of Γ. By the way of contradiction, suppose that this is not the case. Suppose that $\{\mu, \nu\}$ is an edge of Γ such that, among those edges outside of $\{\alpha, \beta\}^H$, μ is an endpoint at minimal distance from α. Note that, as Γ is connected, our choice of μ yields that there is a vertex ω such that $\{\omega, \mu\} \in \{\alpha, \beta\}^H$.

We let

$$E_\alpha = \{\{\alpha, \delta\} \mid \delta \in \Gamma(\alpha)\}$$

be set of edges incident with α. We observe that, since Definition 3.27 requires $\langle P, P^g \rangle$ to be transitive on the neighbourhood of α, E_α is contained in the H-orbit of $\{\alpha, \beta\}$.

By the choice of μ, there exists an automorphism $h \in H$ such that

$$\{\omega, \mu\}^h = \{\alpha, \beta\}.$$

If $\mu^h = \beta$, we put $t = hg^{-1}$, and if $\mu^h = \beta$, we put $t = h$. In either case, we see that $t \in H$ and $\mu^t = \alpha$. Moreover t maps $\{\mu, \nu\}$ in E_α. Thus

$$\{\mu, \nu\} \in \{\alpha, \beta\}^H,$$

contradicting our assumptions. This proves our claim that H acts transitively on the edges of Γ.

We can now consider the cases of Corollary 3.29 in turn.

Suppose Corollary 3.29 (i) occurs. Then there exists a non-trivial characteristic subgroup K of P contained in Q such that $K^g = K$. In particular, K is normal in H, and hence fixes every arc of Γ, contradicting the assumption that G acts faithfully on the vertices of Γ. This contradiction shows that the case (i) of Lemma 3.29 cannot occur.

Suppose Corollary 3.29 (ii) occurs. Then the exponent of P, and hence of Q, is at most p^3. Recalling that Q is the kernel of the action of G_α on the neighbourhood of α, we obtain that

$$\exp(G_\alpha) \le p^3 \exp\left(G_\alpha^{\Gamma(\alpha)}\right).$$

Suppose Corollary 3.29 (iii) occurs. The normal group N appearing in the statement of Corollary 3.29, in this case, is generated by all the subgroups of Q normalised by g. Since N is normalised by both P and g by construction, N is normal in the edge-transitive group $H = \langle P, g\rangle$. On the other hand, N is a subgroup of Q, and thus fixes the edge $\{\alpha, \beta\}$. As a normal subgroup in an edge-transitive group, every element of N fixes every edge of Γ, implying that N is trivial.

By our assumption, it follows that $G_{\alpha\beta}$ is abelian. By the arc-transitivy of G, this is true for all the arc-stabilizers. In particular, $G_{\alpha\gamma}$ is also abelian. We split our discussion in two cases.

Assume that

$$\Omega_1(G_{\alpha\beta}) = \Omega_1\left(G_\alpha^{[1]}\right) = \Omega_1(G_{\alpha\gamma}). \tag{3.1}$$

By computing

$$\Omega_1\left(G_\alpha^{[1]}\right)^g = \Omega_1(G_{\alpha\beta})^g = \Omega_1(G_{\alpha\gamma}) = \Omega_1\left(G_\alpha^{[1]}\right),$$

we obtain that

$$\Omega_1\left(G_\alpha^{[1]}\right) \quad \text{is a normal subgroup} \quad H.$$

By the edge-transitivity of H, we have that such a group is trivial. Thus, by Equation (3.1), $\Omega_1(G_{\alpha\beta})$ is trivial. It follows that the local group is semiregular. but a semiregular permutation group cannot satisfy any condition of Definition 3.27. This contradiction implies that Equation (3.1) is false.

Hence, we must assume (after swapping β and γ, if necessary) that

$$\Omega_1(G_{\alpha\beta}) \neq \Omega_1\left(G_\alpha^{[1]}\right).$$

Since $G_{\alpha\beta}$ is abelian and $G_\alpha^{[1]}$ is of index p in $G_{\alpha\beta}$, we have that $G_{\alpha\beta}$ contains an element of prime order p not contained in $G_\alpha^{[1]}$, that is,

$$G_{\alpha\beta} \quad \text{is isomorphic} \quad C_p \times G_\alpha^{[1]}.$$

Therefore, we have that

$$\mho^1(G_{\alpha\beta}) = \mho^1\left(G_\alpha^{[1]}\right).$$

Further more, since conjugation by g maps isomorphically $G_{\alpha\beta}$ in $G_{\alpha\gamma}$, the same argument yields also

$$\mho^1(G_{\alpha\beta}) = \mho^1\left(G_\alpha^{[1]}\right).$$

We can compute

$$\mho_1\left(G_\alpha^{[1]}\right)^g = \mho_1(G_{\alpha\beta})^g = \mho_1(G_{\alpha\gamma}) = \mho_1\left(G_\alpha^{[1]}\right).$$

It follows that

$$\mho^1\left(G_\alpha^{[1]}\right) \quad \text{is normalised by} \quad g,$$

and hence by H. As above, since H is transitive on the edges of Γ,

$$\mho^1\left(G_\alpha^{[1]}\right) \quad \text{is trivial}.$$

Hence, as G_α is an extension of $G_\alpha^{[1]}$ by the local group,

$$\exp(G_\alpha) \le p\exp\left(G_\alpha^{\Gamma(\alpha)}\right).$$

■

3.H Bounding the number of generators

Let Γ be a locally finite d-valent connected graph, let G be an arc-transitive group of automorphisms with finite vertex-stabilizer. Our initial goal is to bound the number of generators of G (which we denote by the symbol $\mathbf{d}(G)$) with a function that depends on the valency of Γ alone. This can be done, for instance, if the local group is graph-restrictive. (The results contained in Section 3.H have been published in [19].)

Lemma 3.30 · *There exists a function* $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ *such that, for every pair* (Γ, G), *where* Γ *is a locally finite connected* d*-valent graph,* G *is an arc-transitive group of automorphisms of* Γ*, and the local group of the pair* (Γ, G) *is graph-restrictive,*

$$\mathbf{d}(G) \le \mathbf{f}(d).$$

Proof. Let us choose a vertex α. For any of its neighbours β, we consider an automorphism $g_\beta \in G$ such that

$$\alpha^{g_\beta} = \beta.$$

Recall that these elements exist by the transitivity of G on $V\Gamma$. We can define the subgroup of G

$$H := \langle g_\beta \mid \beta \text{ is a neighbour of } \alpha \rangle.$$

We now prove, via a connectedness argument, that H is transitive on the vertex-set of Γ. Aiming for a contradiction, suppose that H is not transitive on $V\Gamma$. We can choose a vertex γ at minimal distance from α which is not contained in the H-orbit of α. As Γ is connected, we can choose a vertex δ adjacent to γ such that

$$d_\Gamma(\alpha, \delta) + 1 = d_\Gamma(\alpha, \gamma).$$

By our choice of γ, there is an element $h \in H$ such that $\alpha^h = \delta$. Observe that

$$X := \left\{h^{-1} g_\beta h \mid \beta \text{ is a neighbour of } \alpha\right\}$$

is a subset of H with the property that

$$\delta^X = \Gamma(\delta).$$

In particular, the set hX contains an automorphism of H mapping α to γ. Thus, γ belongs to the H-orbit of α, a contradiction.

By Frattini's Argument, $G = G_\alpha H$. In particular, $|G_\alpha| + d$ elements are sufficient to generate G. Since the local group is graph-restrictive, we can find a positive constant C_d (depending on the valency d alone) such that $|G_\alpha| \le C_d$. To conclude,

$$\mathbf{d}(G) \le C_d + d\,. \qquad \blacksquare$$

The function $\mathbf{f}$ arising in the proof of Lemma 3.30 is far from being optimal. For instance, by observing that the local group is transitive, we can see that one generator of H, rather than the d we take, are enough.

More surprisingly, for valency at most 4, $\mathbf{d}(G)$ is bounded by a constant for every transitive local groups. If $d = 1$, Γ is isomorphic to a segment, thus the automorphism group is a subgroup of the cyclic group of order 2. If $d = 2$, Γ is isomorphic to a cycle, thus G is either a dihedral group or a cyclic group. In both cases, $\mathbf{d}(G) \le 2$. For $d \in \{3, 4\}$, we need to use amalgams (see Section 1.H). Indeed, for every amalgamated product arising, we can directly check the number of generators in the presentation, which in turn is an upper bound for $\mathbf{d}(G)$. This direct inspection proves that $\mathbf{d}(G) \le 10$. With a bit of extra hustle, we can prove a sharp bound.

Lemma 3.31 · *Let Γ be a d-valent graph, with $d \in \{3, 4\}$, and let G be an arc-transitive group of automorphisms of Γ. Then*

$$\mathbf{d}(G) \le 3\,,$$

and this bound is sharp.

The bulk of the proof of Lemma 3.31 relies on the following observation.

Lemma 3.32 · *Let Γ be a locally finite graph, let G be an arc-transitive group of automorphisms of Γ, and let $\alpha \in V\Gamma$ be a vertex. Then*

$$\mathbf{d}(G) \le \mathbf{d}(G_\alpha) + 1\,.$$

Proof. Let $\{\alpha, \beta\}$ be an edge of Γ and let $x \in G_{\{\alpha,\beta\}} - G_{\alpha\beta}$ be an *edge-flip*, that is, an automorphism satisfying $\alpha^x = \beta$ and $\beta^x = \alpha$. (Examples of such elements are the generators y in the presentations of [47] and the generators a in [110]). We define two subgroups of G as

$$H := \langle G_\alpha, x\rangle \quad \text{and} \quad K := \langle G_\alpha, G_\beta\rangle\,.$$

Repeating the proof of Lemma 3.2, we can show that K defines either one or two orbits on $V\Gamma$, and, if they are distinct, α and β lie in distinct K-orbits. As x swaps α and β, we have that $K \le H$, and that H is transitive on $V\Gamma$. Since $G_\alpha \le H$, by Frattini's Argument, $G = H$. In particular, by construction of H,

$$\mathbf{d}(G) = \mathbf{d}(H) \le \mathbf{d}(G_\alpha) + 1\,. \qquad \blacksquare$$

Proof of Lemma 3.31. Let us assume that Γ is 3-valent. The five possible amalgam types for this case have been collected in [47]. We observe that the possibility for a vertex-stabilizer are

$$G_\alpha \in \{1, C_3, \mathrm{Sym}(3), D_6, \mathrm{Sym}(4), \mathrm{Sym}(4) \times C_2\}\,.$$

It is easy to check that all these groups are 2-generated. Hence, Lemma 3.32 concludes the proof in this case.

We turn to the scenario where the valency of Γ is 4. We need to consider three cases.

First, we suppose that the local group is dihedral. There are infinitely many amalgams whose local group is isomorphic to D_4, and these amalgams are classified in [46]. Using the notation from [46], we deduce that $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$ admits a generating set of the form $\{x, a_0, a_1, \dots, a_{n-1}, y\}$, with $n \geq 2$. (Note that $\{x, a_0, a_1, \dots, a_{\lceil (n-1)/2 \rceil}\}$ is a minimal generating set for G_α, thus we cannot apply Lemma 3.32.) We also recall, from [46], that

$$a_i^x = a_{n-1-i} \quad \text{for every } 0 \leq i \leq n-1\,,$$
$$a_i^y = a_{n-i} \quad \text{for every } 1 \leq i \leq n-1\,.$$

We compute, for every $0 \leq i \leq n-2$,

$$a_i^{xy} = a_{n-1-i}^y = a_{n-n+i+1} = a_{i+1}\,.$$

It follows that $\{x, a_0, y\}$ is a generating set for $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$, and hence $\mathbf{d}(G) \leq 3$.

Now, we assume that the local group is not dihedral and that G is s-arc-transitive, for some $s \geq 1$. Without loss of generality, replacing s if necessary, we may also assume that G is not $(s+1)$-arc-transitive. If $s = 1$, then every vertex-stabilizer is isomorphic either to C_4 or to $C_2 \times C_2$. If $s \geq 2$, then the amalgams have been classified in [110]. If $s = 1$, or if $s \geq 2$ and

$$G_\alpha \in \{\mathrm{Alt}(4), \mathrm{Sym}(4), C_3 \times \mathrm{Alt}(4), \mathrm{Sym}(3) \times \mathrm{Sym}(4)\}\,,$$

then G_α is 2-generated. In all cases under consideration, by Lemma 3.32, $\mathbf{d}(G)$ is at most 3, as desired.

To conclude, there are precisely four amalgams of index $(4,2)$ left. To complete the proof for the upper bound, it is enough to manipulate their explicit presentations in [110] to identify a generating set of cardinality 3. There are two amalgams with G_α isomorphic to $C_3 \rtimes \mathrm{Sym}(3)$. In the first case, $\{x, t, ac\}$ is a generating set for $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$ in view of

$$a = acdcd^{-1}c = acacacac^{-1}ac = (ac)^3(ac)^t(ac)\,,$$
$$c = a(ac)\,, \quad y = x^t\,, \quad d = c^a\,.$$

In the second case, we find that $\{x, c, a\}$ generates $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$ as

$$t = a^2\,, \quad y = x^t\,, \quad d = c^a\,.$$

For the 4-arc-transitive case, we find that $\{t, c, a\}$ is a generating set for $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$ in view of

$$d = (c^t)^{-1}\,, \quad e = d^a\,,$$
$$x = (et)^{-4}\,, \quad y = x^a\,.$$

Meanwhile, for the 7-arc-transitive amalgams, $G_\alpha *_{G_{\alpha\beta}} G_{\{\alpha,\beta\}}$ can be generated by $\{h,p,a\}$, because

$$k = h^{-2}, \quad v = k^a k^{-1}, \quad q = (p^a)^{-1},$$
$$r = qq^h, \quad s = (r^a)^{-1},$$
$$t = (s^h)^{-1} pq^{-1} r^{-1} s^{-1}, \quad u = (t^a)^{-1}.$$

We have thus proved that a minimal generating set for G contains at most 3 elements. To prove that this bound is sharp it is sufficient to inspect the census of arc-transitive graphs of valency 3 and 4 (see [39, 115] or Sections 1.I and 1.L). In doing so, we discover that most graphs have 3-generated automorphism groups. This completes the proof of Lemma 3.31. ■

One could dare to conjecture that there exists a function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ that takes the valency of the graph Γ as input, and returns an upper bound for $\mathbf{d}(G)$. In Section 3.H.1, we prove that such a function cannot exist.

Theorem N · *There exists no function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ such that, for every pair (Γ, G), where Γ is a connected d-valent graph, and G is an arc-transitive group of automorphisms of Γ,*

$$\mathbf{d}(G) \leq \mathbf{f}(d).$$

Remark 3.33 · To prove the veracity of Theorem N, we will exhibit an infinite family $\mathcal{F}$ of pairs (Γ_h, G_h) such that the valency of the graphs is a constant (at least 8), while $\mathbf{d}(G_h)$ grows linearly with the exponent of the group. We would like to remark that, although the philosophies of the constructions are profoundly different, the graphs Γ_h carry an oustanding similiarity with those built in [71, 114, 116] to prove that, for some imprimitive local groups of degree 6, the order of the vertex-stabilizers grows exponentially with the number of vertices of the graph.

We also observe that, in our construction, G is not the automorphism group of Γ. This prompts the following question.

Problem 3.34 · Is there a function $\mathbf{f} : \mathbb{N} \to \mathbb{N}$ such that, if Γ is a connected arc-transitive graph of valency d, then

$$\mathbf{d}(\mathrm{Aut}(\Gamma)) \leq \mathbf{f}(d)?$$

Moreover, for our current and limited knowledge, having $\mathbf{d}(G)$ bounded appears to be quite common. Therefore, we ask the following.

Problem 3.35 · Which assumptions on the pair (Γ, G) are needed to bound $\mathbf{d}(G)$ with a function of the valency (or of the local group)?

Apart from the case we have already discussed, M. Lekše has showed in [86, Corollary 7.5.] that the number of generators of G is bounded by d if the local group is weakly p-subregular (see Definition 3.27).

Observe that the infinite family we build is characterized by the fact of having unlimited exponent. If we decide to bound the exponent of G *a priori*, we get a bound on the number of vertices of Γ, and hence on the order of G.

Theorem O · *There exists a function $\mathbf{B} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that, for every pair (Γ, G). where Γ is a connected d-valent graph, and G is an automorphism group of Γ of exponent e,*

$$|V\Gamma| \le \mathbf{B}(d,e) \quad \textit{and} \quad |G| \le \mathbf{B}(d,e)!.$$

Two comment before the proof. The function $\mathbf{B}$ appearing in Theorem O is the solution of the Burnside Restricted Problem, that is, $\mathbf{B}(d,e)$ is the order of the largest group G with $\mathbf{d}(G) = d$ and $\exp(G) = e$. We recall that the existence of this function was proved by E. Zel'manov in [165, 166]. (We refer to Section 2.I for further details on the Burnside Restricted Problem.)

We also remark that the bound on the number of vertices is sharp. Indeed, let G be the largest finite group with $\mathbf{d}(G) = d$ and $\exp(G) = e$, and let S be a generating set of cardinality d. Then $\mathrm{Cay}(G,S)$ has precisely $\mathbf{B}(d,e)$ vertices.

Proof of Theorem O. Let α be a vertex of Γ, and, for every neighbour $\beta \in \Gamma(\alpha)$, denote by g_β the automorphism mapping α to β. As we have seen in the proof of Lemma 3.30,

$$H := \langle g_\beta \mid \beta \text{ is a neighbour of } \alpha \rangle$$

is a vertex-transitive subgroup of G.

Observe that, as H is a subgroup of G, and as the exponent of G is e, the exponent of H divides e. Therefore, we find that the order of H is bounded from above by $\mathbf{B}(d,e)$. Moreover, since H is transitive on the vertex-set of Γ,

$$|V\Gamma| \le |H| \le \mathbf{B}(d,e).$$

This proves the first part of Theorem O.

To complete the proof, it is enough to observe that G can be embedded into $\mathrm{Sym}(V\Gamma)$, which in turn embeds into $\mathrm{Sym}(\mathbf{B}(d,e))$. Therefore,

$$|G| \le \mathbf{B}(d,e)!,$$

as desired. ■

3.H.1 Proof of Theorem N

Proof of Theorem N. Let h be a positive integer, and let p be a prime. The proof is divided in three steps. First, we build an abstract p-group whose number of generators is linear in the exponent. Second, we build a graph Γ_h whose automorphism group contains the previously constructed group. Last, we consider a group extension of the previous group, say G_h, and we prove that G_h is an arc-transitive group of automorphisms for Γ_h whose number of generator is, again, a linear function of its exponent.

Let us build a p-group whose number of generators is linear in the exponent. We set

$$H := C_{p^h} \times C_{p^h} = \langle a, b \mid a^{p^h} = b^{p^h} = [a,b] = 1 \rangle.$$

Let us consider the group algebra $\mathbb{F}_p[H]$ over the finite field with p elements. We define recursively the following chain of $\mathbb{F}_p[H]$-modules:

$$\gamma_0 := \mathbb{F}_p[H], \quad \text{and,} \quad \text{for any } i \ge 1,$$

$$\gamma_i := [\gamma_{i-1}, H] = \langle v - vh \mid v \in \gamma_{i-1}, h \in H\rangle_{\mathbb{F}_p}.$$

Recall that the natural basis for the group algebra $\mathbb{F}_p[H]$ is

$$\left(a^i b^j \mid i,j \in \left\{0,1,\ldots,p^h-1\right\}\right).$$

For all $x, y \in \left\{0,1,\ldots,p^h-1\right\}$, we write $e_{xy} = (a-1)^x(b-1)^y \in \mathbb{F}_p[H]$. We claim that

$$\mathcal{B} = \left(e_{xy} \mid x,y \in \left\{0,1,\ldots,p^h-1\right\}\right)$$

is also a basis. As $\mathcal{B}$ and the natural basis have the same cardinality, to prove the claim we show that every element of the natural basis can be written as a linear combinations of the elements of $\mathcal{B}$. First we prove, by induction on i, that

$$a^i = \sum_{x=0}^{i} \lambda_x e_{x0}. \tag{3.2}$$

Observe that $1 = e_{00} = a^0$ is an element of the natural basis and of $\mathcal{B}$. We can write

$$a^i = (a-1)\mathbf{p}_i(a) + 1,$$

where $\mathbf{p}_i$ is a polynomial in one variable with coefficients in $\mathbb{F}_p$ and degree $i-1$. By inductive hypothesis, for some suitable coefficients,

$$\mathbf{p}_i(a) = \sum_{x=0}^{i-1} \mu_x e_{x0}.$$

Hence,

$$a^i = (a-1)\mathbf{p}_i(a) + 1 = \sum_{x=0}^{i-1} \mu_x e_{(x+1)0} + e_{00},$$

which proves Equation (3.2). Repeating the same argument for b^j, we can show that

$$b^j = \sum_{y=0}^{j} \lambda_y e_{0y}.$$

Therefore, for some suitable coefficients,

$$a^i b^j = \left(\sum_{x=0}^{i} \lambda_x e_{x0}\right)\left(\sum_{y=0}^{j} \lambda_y e_{0y}\right) = \sum_{x=0}^{i-1}\sum_{y=0}^{j-1} \lambda_x \lambda_y e_{xy},$$

which completes the proof of the claim.

For convenience, we set $e_{xp^h} = e_{p^h y} = 0$, for every $x, y \in \left\{0,1,\ldots,p^h-1\right\}$. Observe that

$$\begin{aligned} e_{xy} \cdot a &= (a-1)^x(b-1)^y \cdot a \\ &= (a-1)^x(1+a-1)(b-1)^y \\ &= (a-1)^x(b-1)^y + (a-1)^{x+1}(b-1)^y \\ &= e_{xy} + e_{(x+1)y}, \end{aligned}$$

and

$$\begin{aligned} e_{xy} \cdot b &= (a-1)^x (b-1)^y \cdot b \\ &= (a-1)^x (b-1)^y (1+b-1) \\ &= (a-1)^x (b-1)^y + (a-1)^x (b-1)^{y+1} \\ &= e_{xy} + e_{x(y+1)} . \end{aligned}$$

By a direct computation, we get that

$$\gamma_i = \langle e_{xy} \mid x+y \geq i \rangle_{\mathbb{F}_p}, \quad \text{and}$$

$$\gamma_i/\gamma_{i+1} = \langle e_{xy} + \gamma_{i+1} \mid x+y = i \rangle_{\mathbb{F}_p} .$$

Indeed, the formula holds for $\gamma_0 = \mathbb{F}_p[H]$, and by induction on i

$$\begin{aligned} \gamma_i &= \langle e_{xy} \cdot a - e_{xy}, e_{xy} \cdot b - e_{xy} \mid x+y \geq i-1 \rangle_{\mathbb{F}_p} \\ &= \langle e_{(x+1)y}, e_{x(y+1)} \mid x+y+1 \geq i \rangle_{\mathbb{F}_p} . \end{aligned}$$

Recall that, for any $\mathbb{F}_p[H]$-module V, we denote by $\mathbf{d}_H(V)$ the minimal number of generators of V as an $\mathbb{F}_p[H]$-module. Since, by construction, γ_i/γ_{i+1} is a trivial section of $\mathbb{F}_p[H]$, we have that

$$\mathbf{d}_H(\gamma_i/\gamma_{i+1}) = \dim_{\mathbb{F}_p}(\gamma_i/\gamma_{i+1}) = \begin{cases} i+1 & \text{if } 0 \leq i \leq p^h - 1 \\ 2p^h - i - 1 & \text{if } p^h \leq i \leq 2(p^h-1) \\ 0 & \text{if } 2p^h - 1 \leq i . \end{cases} \tag{3.3}$$

We use this to compute the number of generators of $\gamma_{p^h} \rtimes H$. Indeed, we claim that

$$\mathbf{d}\left(\gamma_{p^h-1} \rtimes H\right) = p^h + 2 . \tag{3.4}$$

First, we recall that, as $\gamma_{p^h-1} \rtimes H$ is a p-group,

$$\mathbf{d}\left(\gamma_{p^h-1} \rtimes H\right) = \dim_{\mathbb{F}_p}\left(\frac{\gamma_{p^h-1} \rtimes H}{\Phi(\gamma_{p^h-1} \rtimes H)}\right),$$

where $\Phi(\gamma_{p^h-1} \rtimes H)$ is the Frattini subgroup of $\gamma_{p^h-1} \rtimes H$. Second, we note that

$$\Phi(\gamma_{p^h-1} \rtimes H) = [\gamma_{p^h-1} \rtimes H, \gamma_{p^h-1} \rtimes H](\gamma_{p^h-1} \rtimes H)^p .$$

Since H is abelian, using standard commutator computations, we have

$$[\gamma_{p^h-1} \rtimes H, \gamma_{p^h-1} \rtimes H] = \gamma_{p^h} .$$

Moreover,

$$(\gamma_{p^h-1} \rtimes H)^p \geq H^p .$$

This shows that

$$\Phi(\gamma_{p^h-1} \rtimes H) \geq \gamma_{p^h} \rtimes H^p .$$

It is now time to recall that H acts trivially on the section $\gamma_{p^h-1}/\gamma_{p^h}$: this fact implies that the quotient

$$\frac{\gamma_{p^h-1} \rtimes H}{\gamma_{p^h} \rtimes H^p}$$

is abelian of exponent p. Therefore,

$$\Phi(\gamma_{p^h-1} \rtimes H) = \gamma_{p^h} \rtimes H^p\,,$$

and Equation (3.4) immediately follows from Equation (3.3).

Let us build a graph Γ_h whose automorphism group contains $\gamma_{p^h-1} \rtimes H$. By Theorem 1.41, the group H acts regularly on the vertex-set of the Cayley graph defined by

$$\Delta := \mathrm{Cay}(H, \{a, a^{-1}, b, b^{-1}\}).$$

Recall that, for any two graphs Γ, Δ, the *wreath product of* Γ *by* Δ, denoted by $\Gamma \,\mathrm{wr}\, \Delta$, is the graph having vertex-set $V\Gamma \times V\Delta$, where (γ_1, δ_1) and (γ_2, δ_2) are adjacent if either $\delta_1 = \delta_2$ and $\{\gamma_1, \gamma_2\}$ is an edge of Γ, or $\{\delta_1, \delta_2\}$ is an edge of Δ. We define Γ_h as the wreath product of the empty graph on p vertices, $p\mathbf{K}_1$, by the Cayley graph Δ, that is,

$$\Gamma_h := p\mathbf{K}_1 \,\mathrm{wr}\, \Delta\,.$$

Note that, unless $p = 2$ and $h = 1$, Δ has valency 4, hence Γ_h has valency $4p$.

Observe that, as abstract groups, $C_p \mathrm{wr} H$ and $\mathbb{F}_p[H] \rtimes H$ are isomorphic. It follows that $\gamma_{p^h-1} \rtimes H$ is identified with a subgroup of $C_p \mathrm{wr} H$, which in turn is a subgroup of $\mathrm{Aut}(\Gamma_h)$. Moreover, $V\Gamma_h$ can be partitioned as

$$X := \{V(p\mathbf{K}_1) \times \{\delta\} \mid \delta \in V\Delta\}\,.$$

Note that X is γ_{p^h-1}-invariant, because the latter embeds in the base group of $C_p \mathrm{wr} H$. As γ_{p^h-1} is a nontrivial p-group, it must induce a transitive action on at least one part of X, while H permutes regularly the elements of X. It follows that $\gamma_{p^h-1} \rtimes H$ is transitive on the vertices of Γ_h, thus $\gamma_{p^h-1} \rtimes H$ is a vertex-transitive group of automorphisms of Γ_h. On the other hand, since $\gamma_{p^h-1} \rtimes H$ preserves the lifting of the labels $\{a, a^{-1}, b, b^{-1}\}$ from the Cayley graph Δ, this action is not arc-transitive. In particular, the local group of the pair $(\Gamma_h, \gamma_{p^h-1} \rtimes H)$ is intransitive with four distinct orbits.

Let us extend $\gamma_{p^h-1} \rtimes H$ to an arc-transitive group of automorphisms. To achieve the desired arc-transitivity, we extend the group H with some outer automorphisms. We consider the automorphisms φ and ψ of H defined on the generators by

$$\varphi : a \mapsto b, b \mapsto a, \quad \text{and} \quad \psi : a \mapsto a^{-1}, b \mapsto b^{-1}.$$

Observe that φ and ψ are commuting involutions, thus $\langle \varphi, \psi \rangle$ is isomorphic to the Klein group. We extend the multiplication on $\mathbb{F}_p[H]$ by putting, for every $\varepsilon, \delta \in \mathbb{Z}_2$,

$$\left(\sum_{h \in H} \lambda_h h\right) \cdot \left(\varphi^\varepsilon \psi^\delta\right) = \sum_{h \in H} \lambda_h h^{\varphi^\varepsilon \psi^\delta}\,.$$

With this operation, $\mathbb{F}_p[H]$ is an $\mathbb{F}_p[H \rtimes \langle \varphi, \psi \rangle]$-module. Our putative subgroup of $\mathrm{Aut}(\Gamma_h)$ is

$$G_h := \gamma_{p^h-1} \rtimes (H \rtimes \langle \varphi, \psi \rangle)\,.$$

Note that

$$\mathbb{F}_p[H] \rtimes H \geq \mathbb{F}_p[H] = \gamma_0 \geq \gamma_1 \geq \ldots \geq \gamma_{2(p^h-1)} \geq \gamma_{2p^h-1} = 1$$

is the central lower series of $\mathbb{F}_p[H]\rtimes H$, and hence, for all indices i, γ_i is a characteristic subgroup of $\mathbb{F}_p[H]\rtimes H$. It follows that γ_i is an $\mathbb{F}_p[H \rtimes \langle \varphi, \psi \rangle]$-submodule, and hence G_h is well-defined.

First, we give a lower bound on $\mathbf{d}(G_h)$, then we prove that G_h is an arc-transitive group of automorphisms of Γ_h.

Let S be a generating set for G_h. The set $S \cup \{\varphi, \psi\}$ also generates G_h. By multiplying each element of S by a (possibly trivial) element of $\langle \varphi, \psi \rangle$, we can produce a new generating set for G_h of the form $T \cup \{\varphi, \psi\}$ where T is a subset of $\gamma_{p^h-1} \rtimes H$. We claim that

$$U := T^{\langle \varphi, \psi \rangle} \subseteq \gamma_{p^h-1} \rtimes H$$

is a generating set for $\gamma_{p^h-1} \rtimes H$. For every $g \in \gamma_{p^h-1} \rtimes H$, g can be written as a word in $T \cup \{\varphi, \psi\}$. Whenever φ appears in this word, we can move it to the right end of the word by conjugating by φ all the generators from its initial position to the end of the string. The same procedure can be applied to ψ. Once we have completed these operations, we find that g can be expressed as the product of two words: one in U and the other in $\{\varphi, \psi\}$. As $g \in \gamma_{p^h-1} \rtimes H$, the latter word must be trivial. This proves that we can express g as a word in U, and hence U generates $\gamma_{p^h-1} \rtimes H$. By construction, since $|\langle \varphi, \psi \rangle| = 4$,

$$|U| \leq 4|T| = 4|S|.$$

Hence, by choosing $|S|$ to be minimal,

$$\frac{1}{4}\mathbf{d}(\gamma_{p^h-1} \rtimes H) \leq \frac{1}{4}|U| \leq \mathbf{d}(G_h).$$

Therefore, using Equation (3.4),

$$\mathbf{d}(G_h) \geq \frac{p^h}{4}.$$

Let us go back to the Cayley graph Δ. Observe that $\langle \varphi, \psi \rangle$ is transitive on the connection set $\{a, a^{-1}, b, b^{-1}\}$ of Δ. This implies that $H \rtimes \langle \varphi, \psi \rangle$ is an arc-transitive subgroup of $\mathrm{Aut}(\Delta)$. Therefore,

$$G_h \leq C_p \,\mathrm{wr}(H \rtimes \langle \varphi, \psi \rangle) \leq \mathrm{Aut}(\Gamma_h).$$

Moreover, the local group of (Γ_h, G_h) transitively permutes the four orbits defined by the local group of $(\Gamma_h, \gamma_{p^h-1} \rtimes H)$. Hence, the pair G_h is an arc-transitive group of automorphisms of Γ_h.

To wrap up, for a fixed prime p, the family

$$\mathcal{F}_p := \{(\Gamma_h, G_h) \mid h \geq 2\}$$

contains pairs such that every Γ_h is a $(4p)$-valent graph, meanwhile

$$\lim_{h\to+\infty} \mathbf{d}(G_h) \geq \lim_{h\to+\infty} \frac{p^h}{4} = +\infty.$$

This family is a counterexample to the existence of function $\mathbf{f}$ that, for every pair (Γ, G), where Γ is a connected d-valent graph, and G is an arc-transitive group of automorphisms of Γ, $\mathbf{d}(G)$ can be bounded in terms of d alone. Hence, the proof of Theorem N is complete. ■

3.I Bounding the number of derangements

In the *10th PhD Summer School in Discrete Mathematics* in Rogla, I has been asked by G. Korchmáros whether or not, for every graph Γ of valency d and transitive automorphism group $\mathrm{Aut}(\Gamma)$, the proproportion of derangements in $\mathrm{Aut}(\Gamma)$ is bounded away from zero by a function of d alone. I would like to thank him for inspiring me with this fascinating problem. The results of Section 3.I have been proven in [18].

Before presenting our solution, we need to recall some notation. Let G be a finite transitive permutation group with domain Ω. We recall that a *derangement of* G is a permutation g without any fixed points, that is, for any $\alpha \in \Omega$ we have that α and α^g are distinct points of Ω. We let $\delta(G)$ be the *proportion of derangements of* G, that is, the ratio between the number of derangements and the size of G. Our notation is a bit sloppy: observe that $\delta(G)$ depends on the action of G, thus it is not a parameter of the abstract group G, but rather of a permutational representation of it.

The interest in derangements predates the existence of groups themselves. In 1708, P. de Montmort's published his highly influential book on probability, *Essay d'analyse sur les jeux de hazard*. There, he presents a systematic combinatorial analysis of games of chance that were popular at the time, and through studying the card game *treize*, he calculates the proproportion of derangements in the symmetric group $\mathrm{Sym}(13)$ in its natural action on 13 points. A few years later, N. Bernoulli, by means of the inclusion-exclusion principle, generalised the formula to any symmetric group of degree n obtaining

$$\delta(\mathrm{Sym}(n)) = \sum_{i=2}^{n} \frac{(-1)^i}{i!}.$$

Jumping forward 150 years, C. Jordan has first noticed in [77] that every nontrivial finite transitive permutation group G contains a derangement, that is,

$$\delta(G) > 0.$$

This observation has far reaching consequences ranging from number theory to topology (see, for instance, [50, 137]). For further information, we refer to the extensive review in [26, Chapter 1].

An outstanding property of derangements in transitive groups is their abundance. We can give two impressive examples of lower bounds for $\delta(G)$. In [33],

P. J. Cameron, L. G. Kovács, M. F. Newman and C. E. Praeger have proven that, if G is a p-group, then

$$\delta(G) > \frac{p-1}{p+1}.$$

On the other end of the spectrum, there exists an absolute constant $\epsilon > 0$ such that, for every simple group T endowed with a transitive action, $\delta(T) \geq \epsilon$. This result has been obtained by J. E. Fulman and R. M. Guralnick by an extensive study of primitive actions of finite simple groups [52, 53, 54, 55].

The last result cannot even be extended to almost simple groups. In fact, there are infinite families of almost simple groups of Lie type containing a field automorphism whose proportion of derangements tends to zero as the size of the group grows. To give a concrete example, let $G_p = \mathrm{P\Gamma L}_2(2^p)$, for some odd prime p, and let G_p act on the right cosets of the subgroup $C_{2^p+1} \rtimes C_{2p}$. We have that the set of derangement is a normal subset: indeed, the number of fixed points is an invariant on conjugacy classes. Hence, all the derangements are trapped in $\mathrm{PGL}_2(2^p)$. Therefore,

$$\lim_p \delta(G_p) \leq \lim_p \frac{1}{p} = 0.$$

We refer to [13] for other examples and further details.

On the other hand, introducing the permutational rank in the equation, all transitive groups can be captured at once. This has been shown in [32], where P. J. Cameron and A. M. Cohen prove that, for every transitive groups G with permutational rank r,

$$\delta(G) \geq \frac{r-1}{|\Omega|}.$$

Furthermore, this bound is sharp: indeed, equality is achieved if and only if G is a *Frobenius group*. (For our purposes, a Frobenious group is a permutation group such that every nontrivial element either fixes one point or is a derangement. See [45, Section 3.4] for more details.) The first steps of the proof of Theorem P take enormous inspiration from this result (see Section 3.I.1). Because of this, we devote Section 3.I.2 to compare our bound with the *Cameron–Cohen bound*.

Indeed, we prove the following.

Theorem P · *Let G be a finite transitive permutation group whose minimal nontrivial subdegree is d_G. Then*

$$\delta(G) \geq \frac{1}{2d_G} + \frac{n-2}{2|G|}.$$

Equality is attained if and only if G is a Frobenius group.

In view of the one-to-one correspondence explored in Section 1.F, Theorem P gives at once an affirmative answer to G. Korchmáros's question.

Corollary Q · *Let Γ be a finite digraph, and let G be a group of automorphisms of Γ. If G is transitive, and Γ has valency d, then*

$$\delta(G) \geq \frac{1}{2d}.$$

3.1.1 Proof of Theorem P

We start by establishing some notation for the proof. Let G be a nonidentity finite transitive group of degree n and of minimal nontrivial subdegree d, and let α be a point of its domain Ω. Given $g \in G$, we let

$$\mathrm{Fix}(g) = \{\omega \in \Omega \mid \omega^g = \omega\},$$

and, given $i \in \{0, \ldots, n\}$, we let

$$F_i(G) = \{g \in G \mid |\mathrm{Fix}(g)| = i\}.$$

In particular, $F_0(G)$ is the set of all derangements of G.

Proof of Theorem P. Our aim to show that

$$\delta(G) = \frac{|F_0(G)|}{|G|} \geq \frac{1}{2d} + \frac{n-2}{2|G|},$$

and that the equality is attained if and only if G is a Frobenius group.

Since the sets $F_i(G)$ partition G, we get

$$|G| = \sum_{i=0}^{n} |F_i(G)|. \tag{3.5}$$

Moreover, from the Orbit Counting Lemma, we have

$$|G| = \sum_{i=0}^{n} i|F_i(G)|. \tag{3.6}$$

Observe that $F_n(G)$ contains a single element, which is the identity of G. By subtracting Equation (3.5) from Equation (3.6), we deduce

$$\begin{aligned} |F_0(G)| &= \sum_{i=1}^{n} (i-1)|F_i(G)| \\ &= \sum_{i=1}^{n-1} (i-1)|F_i(G)| + n - 1 \\ &\geq \sum_{i=2}^{n-1} |F_i(G)| + n - 1 \\ &= \sum_{i=2}^{n} |F_i(G)| + n - 2 \\ &= |G| - |F_0(G)| - |F_1(G)| + n - 2. \end{aligned}$$

Therefore,

$$|F_0(G)| \geq \frac{|G|}{2} - \frac{|F_1(G)|}{2} + \frac{n-2}{2}. \tag{3.7}$$

Observe that the sets $F_1(G_\omega)$, as ω runs through the elements of Ω, are pairwise disjoint and cover the whole of $F_1(G)$. This means that

$$\{F_1(G_\omega) \mid \omega \in \Omega\}$$

is a partition of $F_1(G)$ and hence, for every fixed $\alpha \in \Omega$,

$$|F_1(G)| = \sum_{\omega\in\Omega} |F_1(G_\omega)| = |\Omega||F_1(G_\alpha)| = \frac{|G|}{|G_\alpha|}|F_1(G_\alpha)|. \tag{3.8}$$

Now, we can choose $\beta \in \Omega - \{\alpha\}$ such that $|\beta^{G_\alpha}| = d$. Since $G_{\alpha\beta}$ and $F_1(G_\alpha)$ have empty intersection, we get

$$F_1(G_\alpha) \subseteq G_\alpha - G_{\alpha\beta}.$$

Therefore, using the Orbit Stabilizer Lemma on the action of G_α on β^{G_α}, we get

$$|F_1(G_\alpha)| \le |G_\alpha| - |G_{\alpha,\beta}| = |G_\alpha|\left(1 - \frac{|G_{\alpha\beta}|}{|G_\alpha|}\right) = |G_\alpha|\left(1 - \frac{1}{d}\right). \tag{3.9}$$

Finally, combining Equations (3.7), (3.8) and (3.9), we get

$$\delta(G) = \frac{|F_0(G)|}{|G|} \ge \frac{1}{2} - \frac{1}{2}\left(1 - \frac{1}{d_G}\right) + \frac{n-2}{|G|} = \frac{1}{2d} + \frac{n-2}{2|G|},$$

which is the desired inequality.

Moreover, if the equality is attained, then Equation (3.7) holds with an equal sign, thus we deduce that

$$G = F_0(G) \cup F_1(G) \cup F_n(G),$$

that is, G is a Frobenius group. Conversely, if G is a Frobenius group, all the estimates we have done in the proof are actually equalities. This completes the proof. ■

3.1.2 Comparison

In this section, we compare the bound obtained in Theorem P with the Cameron–Cohen bound from [32].

For every $\alpha \in \Omega$, we note that

$$\begin{aligned}
(|G_\alpha| + d_G)n &= (|G_\alpha| + d)\sum_{i=1}^{r} d_i \\
&= |G_\alpha| + d + |G_\alpha|\left(\sum_{i=2}^{r}(d_i - d) + d(r-1)\right) \\
&\quad + d\left(\sum_{i=2}^{r}(d_i - |G_\alpha|) + |G_\alpha|(r-1)\right) \\
&= |G_\alpha| + d + 2d|G_\alpha|(r-1) \\
&\quad + d|G_\alpha|\sum_{i=2}^{r}\left(\frac{d_i}{d} + \frac{d_i}{|G_\alpha|} - 2\right).
\end{aligned}$$

By substituting this equality in the difference of the two bounds, we obtain

$$\begin{aligned}\frac{1}{2d}+\frac{n-2}{2|G_\alpha|n}-\frac{r-1}{n} &= \frac{|G_\alpha|n+d(n-2)}{2d|G_\alpha|n}-\frac{r-1}{n}\\ &= \frac{(|G_\alpha|+d)n-2d}{2d|G_\alpha|n}-\frac{r-1}{n}\\ &= \frac{1}{2n}\left(\frac{1}{d}-\frac{1}{|G_\alpha|}+\sum_{i=2}^{r}\left(\frac{d_i}{d}+\frac{d_i}{|G_\alpha|}-2\right)\right).\end{aligned}$$

Therefore, the sign of

$$\frac{1}{d_G}-\frac{1}{|G_\alpha|}+\sum_{i=2}^{r}\left(\frac{d_i}{d_G}+\frac{d_i}{|G_\alpha|}-2\right) \tag{3.10}$$

determines which bound gives the best estimate for $\delta(G)$. In particular, the Cameron–Cohen bound is better when Equation (3.10) is negative, while our bound is stronger otherwise. We remark that the sign of Equation (3.10) depends on the distribution of the nontrivial subdegrees of G: a predominance of subdegrees proximate to $|G_\alpha|$ results in a positive expression, whereas a prevalence of subdegrees closer to the minimal nontrivial subdegree leads to a negative sign.

We conclude this section by giving two examples of infinite families of transitive permutation groups: two in which the bound in Theorem P is stronger, and one in which the Cameron–Cohen bound is better.

Let us work out in details the first example.

Example 3.36 · Let $G = \mathrm{PSL}_2(p)$ be the projective special linear group of dimension 2 over the field with p elements, p prime, and suppose that $p \equiv 43 \pmod{120}$. This condition guarantees that the alternating group $\mathrm{Alt}(4)$ is a maximal subgroup of $\mathrm{PSL}_2(p)$ (see, for instance, [22, Section 3.1]) and simplifies some computations. Observe that, as the subdegrees are the lengths of $\mathrm{Alt}(4)$-orbits, the possible subdegrees of this action are $1,2,3,4,6,12$. Let us denote by μ_i the number of suborbits having cardinality i.

Since G is primitive, all the orbital digraph but the diagonal one are connected. Hence, $\mu_1 = 1$.

From here on, we fix a point α in the permutation domain. We claim that $\mu_2 = \mu_3 = 0$. Observe that, if there is a point β so that it lies in a G_α-orbit of length 2 or 3, then, by the Orbit Stabilizer Lemma, we can choose a subgroup S of G_α whose index is either 2 or 3. Furthermore, as S is the stabilizer of β in the action of G_α, S is also a subgroup of G_β, and, from immediate arithmetic considerations, $|G_\beta : S| = |G_\alpha : S|$. If $|G_\alpha : S| = 2$, then S is normal in both G_α and G_β. If $|G_\alpha : S| = 3$, then, recalling that $G_\alpha = \mathrm{Alt}(4)$,

$$S = \mathbf{O}_2(G_\alpha) = \mathbf{O}_2(G_\beta),$$

and hence S is normal in both G_α and G_β. In both cases, S is a normal subgroup of the group generated by G_α and G_β, which, by primitivity, is G itself. We conclude that, although it is core-free, G_α contains a nontrivial normal subgroup, a contradiction. Thus β does not exist, and $\mu_2 = \mu_3 = 0$.

Our aim now is to compute μ_4. Let S be a Sylow 3-subgroup in G_α. Observe that S, in its action by right multiplication on $\mathrm{Alt}(4)/S-\{S\}$, is transitive. Hence, once we fix S, there is a single β in each suborbit of length 4 such that $S=G_{\alpha\beta}$. Since G is transitive, we can choose a $g\in G$ that maps α to β. As a consequence, S^g is a Sylow 3-subgroup of G_β. By Sylow's Theorem, we can choose $n\in G_\beta$ such that $S^{gn}=S$. Hence, we have that $gn\in \mathbf{N}_G(G_{\alpha\beta})$, and that $g\in \mathbf{N}_G(G_{\alpha\beta})n^{-1}$. Note that $p\equiv 43 \pmod{120}$ implies that $p\equiv 1 \pmod 3$. Thus, from [148, Lemma 6.23], $\mathbf{N}_G(G_{\alpha\beta})$ is isomorphic to a dihedral group of order $p-1$. Last, observe that, as $S^g=G_{\beta\beta^g}$, rather than n, we may also choose $G_\beta n$. Everything is in place to perform our counting argument. The number of possible g with the properties described is

$$|\mathbf{N}_G(G_{\alpha\beta})G_\beta|-|G_\alpha|,$$

hence the number of possible β is

$$\frac{|\mathbf{N}_G(G_{\alpha\beta})G_\beta|-|G_\alpha|}{|G_\beta|}=\frac{|\mathbf{N}_G(G_{\alpha\beta})||G_\beta|}{|\mathbf{N}_{G_\beta}(G_{\alpha\beta})||G_\beta|}-1=\frac{p-1}{3}-1=\frac{p-4}{3}.$$

Therefore, recalling that there is a one-to-one correspondence between the possible points β and the suborbits of length 4, we have proved that

$$\mu_4=\frac{p-4}{3}.$$

We can perform a similar counting argument for μ_6. Let S be a cyclic subgroup of order 2 in G_α. Observe that S, in its action by right multiplication on $\mathrm{Alt}(4)/S$, fixes two right cosets (namely, S itself and the other coset containing only involutions). Hence, once we fix S, there are two points β in each suborbit of length 6 such that $S=G_{\alpha\beta}$. By transitivity of G, let $g\in G$ be a permutation that sends α to β, so that S^g is a cyclic subgroup of G_β of order 2. Since the action of $\mathrm{Alt}(4)$ by conjugation on the set of its cyclic subgroups of order 2 is transitive, we can choose $n\in G_\beta$ such that $S^{gn}=S$. Hence, as before, $gn\in\mathbf{N}_G(G_{\alpha\beta})$, and thus $g\in \mathbf{N}_G(G_{\alpha\beta})n^{-1}$. Further, $p\equiv 43 \pmod{120}$ implies that $p\equiv -1 \pmod 4$. [148, Lemma 6.23] states that $\mathbf{N}_G(G_{\alpha\beta})$ is isomorphic to a dihedral group of order $p+1$. Finally, as $S^g=G_{\beta\beta^g}$, rather than n, we may also choose $G_\beta n$. Therefore, the number of possible g with the properties described is

$$|\mathbf{N}_G(G_{\alpha\beta})G_\beta|-|G_\alpha|,$$

hence the number of possible β is

$$\frac{|\mathbf{N}_G(G_{\alpha\beta})G_\beta|-|G_\alpha|}{|G_\beta|}=\frac{|\mathbf{N}_G(G_{\alpha\beta})||G_\beta|}{|\mathbf{N}_{G_\beta}(G_{\alpha\beta})||G_\beta|}-1=\frac{p+1}{4}-1=\frac{p-3}{4}.$$

As we have noticed at the beginning of this paragraph, the number of points β is twice the number of suborbits of length 6. Thus,

$$\mu_6=\frac{p-3}{8}.$$

Finally, as 12 is the last possible subdegree, if n denotes the degree of the permutation group, we get

$$\mu_{12} = \frac{1}{12}(n-1-4\mu_4-6\mu_6) \simeq \frac{p^3}{24\cdot 12}.$$

To sum up, the subdegrees of the primitive action of $\mathrm{PSL}_2(p)$ with stabilizer $\mathrm{Alt}(4)$ are

$$\begin{aligned}\mu_1 &= 1\,,\\ \mu_4 &= \frac{p-4}{3}\,,\\ \mu_6 &= \frac{p-3}{8}\,,\\ \mu_{12} &\simeq \frac{p^3}{24\cdot 12}\,.\end{aligned}$$

Moreover, if r denotes the permutation rank,

$$r = 1+\mu_4+\mu_6+\mu_{12} \quad \text{and} \quad n = 1+4\mu_4+6\mu_6+12\mu_{12}\,.$$

Therefore,

$$\lim_{p\to\infty}\frac{r-1}{n} = \frac{1}{12} < \frac{1}{8} = \frac{1}{2d}.$$

Since most subdegrees are equal to the cardinality of a point stabilizer, as expected, our bound is stronger, for sufficiently large primes p.

The remaining examples cover two infinite families.

Example 3.37 · P. Spiga in [146] gives remarkable examples of transitive permutation groups where most points lie in a suborbit of cardinality 2: examples of this type are relevant for the enumeration of vertex-transitive graphs of given valency. In these examples, $|G_\alpha| = 4$, and hence the subdegrees of G are 1, 2 or 4. Let μ_i be the number of subdegrees of G having cardinality i. From [146], we deduce that $\mu_1 = n/6$, $\mu_2 = n/3$ and $\mu_4 = n/24$, and hence

$$r = \mu_1+\mu_2+\mu_4 = \frac{13n}{24}.$$

Therefore,

$$\frac{1}{2d}+\frac{n-2}{2|G|} = \frac{1}{2}+\frac{n-2}{8n} \quad \text{and} \quad \frac{r-1}{n} = \frac{13n-24}{24n}.$$

In particular, the bound in Theorem P is stronger than the Cameron–Cohen bound.

Example 3.38 · Let G be a non-Frobenius 2-transitive permutation group of degree n. The Cameron–Cohen bound is $1/n$, while the bound in Theorem P is

$$\frac{1}{2d_G}+\frac{n-2}{2|G|} < \frac{1}{2(n-1)}+\frac{n-2}{2n(n-1)} = \frac{1}{n}.$$

Hence, for this family of groups, the Cameron–Cohen bound is stronger than ours.

We conclude Section 3.I with a question.

Problem 3.39 · Is there a function $f : \mathbb{N} \to \mathbb{N}$ such that, for every permutation group G of degree n, minimal nontrivial subdegree d and rank r, if $n \geq f(d)$, then

$$\frac{r-1}{n} \leq \frac{1}{2d} + \frac{n-2}{2|G|}?$$

In essence, Problem 3.39 revolves around determining whether our bound exhibits asymptotic superiority over the Cameron–Cohen bounds when d remains fixed.

Bibliography

[1] N. Alon and F. R. K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72(1):15–19, 1988.

[2] L. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Mathematica Academiae Scientiarum Hungaricae*, 29:329–336, 1977.

[3] L. Babai. Monte Carlo algorithms in graph isomorphism testing. *Université de Montréal Technical Report*, DMS 79-10:42, 1979.

[4] L. Babai. On the complexity of canonical labeling of strongly regular graphs. *SIAM Journal on Computing*, 9(1):212–216, 1980.

[5] L. Babai. On the automorphism groups of strongly regular graphs I. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 359–368, New York, NY, USA, 2014. Association for Computing Machinery.

[6] L. Babai. On the automorphism groups of strongly regular graphs II. *Journal of Algebra*, 421:560–578, 2015. Special issue in memory of Ákos Seress.

[7] L. Babai. Graph isomorphism in quasipolynomial time. 2016. `arXiv:1512.03547v2`.

[8] L. Babai. Groups, graphs, algorithms: The Graph Isomorphism Problem. In *Proceedings of the International Congress of Mathematicians (ICM 2018)*, volume 3, pages 3319–3336, Rio de Janeiro, BRA, 2019.

[9] L. Babai, P. J. Cameron, and P. P. Pálfy. On the orders of primitive groups with restricted nonabelian composition factors. *Journal of Algebra*, 79(1):161–168, 1982.

[10] L. Babai, P. Erdős, and S. M. Selkow. Random graph isomorphism. *SIAM Journal on Computng*, 9:628–635, 1980.

[11] L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proceedings of the fifteenth annual ACM symposium on Theory of computing*, pages 171–183, New York, USA, 1983.

[12] L. Babai and Á. Seress. On the degree of transitivity of permutation groups: A short proof. *Journal of Combinatorial Theory, Series A*, 45(2):310–315, 1987.

[13] R. A. Bailey, P. J. Cameron, M. Giudici, and G. F. Royle. Groups generated by derangements. *Journal of Algebra*, 572:245–262, 2021.

[14] M. Barbieri, V. Grazian, and P. Spiga. On the Cayleyness of Praeger–Xu graphs. *Bulletin of the Australian Mathematical Society*, 106(3):353–356, 2022.

[15] M. Barbieri, V. Grazian, and P. Spiga. On the number of fixed edges of automorphisms of vertex-transitive graphs of small valency. *Journal of Algebraic Combinatorics*, 57:329–348, 2023.

[16] M. Barbieri, V. Grazian, and P. Spiga. On the order of semiregular automorphisms of cubic vertex-transitive graphs. 2023. `arXiv:2302.00034`, accepted for publication in *European Journal of Combinatorics*.

[17] M. Barbieri and P. Potočnik. Vertex-primitive digraphs with large fixity. *Annali di Matematica Pura ed Applicata*, 203(6), 2024.

[18] M. Barbieri and P. Spiga. On derangements and suborbits in finite transitive groups. *Discrete Mathematics*, 347(7):114032, 2024.

[19] M. Barbieri and P. Spiga. On the number of generators of groups acting arc-transitively on graphs. *Aistralasian Journal of Combinatorics*, 90(2):187 – 198, 2024.

[20] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[21] R. Brandl and W. Shi. Finite groups whose element orders are consecutive integers. *Journal of Algebra*, 143(2):388–400, 1991.

[22] J. N. Bray, D. F. Holt, and C. M. Roney-Dougal. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, UK, 2013.

[23] E. Breuillard, B. Green, and T. Tao. Approximate subgroups of linear groups. *Geometric and Functional Analysis*, 21:774–819, 2011.

[24] A. E. Brouwer and H. Van Maldeghem. *Strongly regular graphs*, volume 182 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, UK, 2022.

[25] D. Bundy, N. Hebbinghaus, and B. Stellmacher. The Local $\mathcal{C}(G,T)$ Theorem. *Journal of Algebra*, 300(2):741–789, 2006. Special issue celebrating the 70th birthday of Bernd Fischer.

[26] T. C. Burness and M. Giudici. *Classical Groups, Derangements and Primes*. Australian Mathematical Society Lecture Series. Cambridge University Press, Cambridge, UK, 2016.

[27] T. C. Burness and R. M. Guralnick. Fixed point ratios for finite primitive groups and applications. *Advances in Mathematics*, 411:108778, 2022.

[28] T. C. Burness, R. M. Guralnick, and S. Harper. The spread of a finite group. *Annals of Mathemathics*, 193:619–687, 2021.

[29] W. Burnside. *Theory of groups of finite order*. Cambridge University Press, Cambridge, UK, 1911.

[30] J.-Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. In *30th Annual Symposium on Foundations of Computer Science*, pages 612–617, Washington DC, USA, 1989.

[31] P. J. Cameron. Finite permutation groups and finite simple groups. *Bulletin of the London Mathematical Society*, 13(1):1–22, 1981.

[32] P. J. Cameron and A. M. Cohen. On the number of fixed point free elements in a permutation group. *Discrete Mathematics*, 106-107:135–138, 1992.

[33] P. J. Cameron, L. G. Kovács, M. F. Newman, and C. E. Praeger. Fixed-point-free permutations in transitive permutation groups of prime-power order. *The Quarterly Journal of Mathematics*, 36(3):273–278, 09 1985.

[34] P. J. Cameron, C. E. Praeger, J. Saxl, and G. M. Seitz. On the Sims Conjecture and distance transitive graphs. *Bulletin of the London Mathematical Society*, 15(5):499–506, 1983.

[35] P. J. Cameron, J. Sheehan, and P. Spiga. Semiregular automorphisms of vertex-transitive cubic graphs. *European Journal of Combinatorics*, 27(6):924–930, 2006.

[36] J. Camille. Théorèmes sur les groupes primitifs. *Journal de Mathématiques Pures et Appliquées*, pages 383–408, 1871.

[37] A. Chermak. Quadratic action and the $\mathcal{P}(G,V)$ Theorem in arbitrary characteristic. *Journal of Group Theory*, 2(1):1–13, 1999.

[38] M. D. E. Conder and P. Dobcsányi. Applications and adaptations of the low index subgroups procedure. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 40:41–63, 2002.

[39] M. D. E. Conder and P. Dobcsányi. Applications and adaptations of the low index subgroups procedure. *Mathematics of Computation*, 74(249):485–497, 2005.

[40] M. D. E. Conder, A. Hujdurović, K. Kutnar, and D. Marušič. Symmetric cubic graphs via rigid cells. *Journal of Algebraic Combinatorics*, 53:170–192, 2021.

[41] M. D. E. Conder, C. H. Li, and C. E. Praeger. On the Weiss conjecture for finite locally primitive graphs. *Proceedings of the Edinburgh Mathematical Society*, 43(1):129–138, 2000.

[42] M. D. E. Conder and T. Tucker. Motion and distinguishing number two. *Ars Mathematica Contemporanea*, 4(1):63–72, 2011.

[43] H. J. Coutts, M. Quick, and C. M. Roney-Dougal. The primitive permutation groups of degree less than 4096. *Communications in Algebra*, 39(10):3526–3546, 2011.

[44] A. Dietze and M. Scahps. Determining subgroups of a given finite index in a finitely presented group. *Canadian Journal of Mathematics*, 26(4):769–782, 1974.

[45] J. D. Dixon and B. Mortimer. *Permutation Groups*, volume 163 of *Graduate Texts in Mathematics*. Springer, New York, USA, 1996.

[46] D. Ž. Djoković. A class of finite group-amalgams. *Proceedings of the American Mathematical Society*, 80:22–26, 1980.

[47] D. Ž. Djoković and G. L. Miller. Regular groups of automorphisms of cubic graphs. *Journal of Combinatorial Theory, Series B*, 29(2):195–230, 1980.

[48] E. Dobson and J. Morris. Automorphism groups of wreath product digraphs. *The Electronic Journal of Combinatorics*, 6(1):R17, 2009.

[49] B. Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Communications in Algebra*, 30(5):2271–2295, 2002.

[50] B. I. Fein, W. M. Kantor, and M. M. Schacher. Relative Brauer groups II. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1981:39–57, 1981.

[51] D. Firth. An algorithm to find normal subgroups of a finitely presented group up the a given index, 2005. PhD thesis at University of Warwick.

[52] J. E. Fulman and R. M. Guralnick. Derangements in simple and primitive groups. In *Groups, Combinatorics and Geometry*, pages 99–121, Durham, UK, 2003.

[53] J. E. Fulman and R. M. Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Transactions of the American Mathematical Society*, 364(6):3023–3070, 2012.

[54] J. E. Fulman and R. M. Guralnick. Derangements in subspace actions of finite classical groups. *Transactions of the American Mathematical Society*, 369:2521–2572, 2017.

[55] J. E. Fulman and R. M. Guralnick. Derangements in finite classical groups for actions related to extension field and imprimitive subgroups and the solution of the Boston–Shalev conjecture. *Transactions of the American Mathematical Society*, 370:4601–4622, 2018.

[56] A. Gardiner. Arc transitivity in graphs. *The Quarterly Journal of Mathematics*, 24(1):399–407, 1973.

[57] A. Gardiner. Arc transitivity in graphs, II. *The Quarterly Journal of Mathematics*, 25(1):163–167, 1974.

[58] A. D. Gardiner and C. E. Praeger. A characterization of certain families of 4-valent symmetric graphs. *European Journal of Combinatorics*, 15:383–397, 1994.

[59] M. Giudici, C. H. Li, C. E. Praeger, Á. Seress, and V. I. Trofimov. On limit graphs of finite vertex-primitive graphs. *Journal of Combinatorial Theory, Series A*, 114(1):110–134, 2007.

[60] M. Giudici and J. Xu. All vertex-transitive locally-quasiprimitive graphs have a semiregular automorphism. *Journal of Algebraic Combinatorics*, 25:217–232, 2007.

[61] G. Glauberman. Isomorphic subgroups of finite p-groups, I. *Canadian Journal of Mathematics*, 23(6):983–1022, 1971.

[62] G. Glauberman. Isomorphic subgroups of finite p-groups, II. *Canadian Journal of Mathematics*, 23(6):1023–1039, 1971.

[63] C. Godsil and G. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics. Springer, New York, USA, 2001.

[64] R. Guralnick and K. Magaard. On the minimal degree of a primitive permutation group. *Journal of Algebra*, 207(1):127–145, 1998.

[65] R. M. Guralnick, M. W. Liebeck, J. Saxl, and A. Shalev. Random generation of finite simple groups. *Journal of Algebra*, 219:345–355, 1999.

[66] G. Havas, G. E. Wall, and J. W. Wamsley. The two generator restricted Burnside group of exponent five. *Bulletin of the Australian Mathematical Society*, 10(3):459—470, 1974.

[67] H. A. Helfgott, J. Bajpai, and D. Dona. Graph isomorphism in quasipolynomial time. 2017. `arXiv:1710.04574`.

[68] D. G. Higman. Intersection matrices for finite permutation groups. *Journal of Algebra*, 6:22–42, 1967.

[69] G. Higman. Enumerating p-groups. I: Inequalities. *Proceedings of the London Mathematical Society*, s3-10(1):24–30, 1960.

[70] J. E. Hopcroft and R. E. Tarjan. A $|v|^2$ algorithm for determining isomorphism of planar graphs. *Information Processing Letters*, 1:32–34, 1971.

[71] A. Hujdurović, P. Potočnik, and G. Verret. Three local actions in 6-valent arc-transitive graphs. *Journal of Graph Theory*, 99(2):207–216, 2022.

[72] W. Imrich and S. Klavžar. *Product Graphs: Structure and Recognition*. Wiley-Interscience series in discrete mathematics and optimization. Wiley, New York, USA, 2000.

[73] R. Jajcay, P. Potočnik, and S. Wilson. The Praeger–Xu graphs: cycle structures, maps and semitransitive orientations. *Acta Mathemthica Universitatis Comanianae*, 88:22–26, 2019.

[74] R. Jajcay, P. Potočnik, and S. Wilson. On the Cayleyness of Praeger–Xu graphs. *Journal of Combinatorial Theorey, Series B*, 152:55–79, 2022.

[75] G. A. Jones. Automorphisms and regular embeddings of merged johnson graphs. *European Journal of Combinatorics*, 26(3):417–435, 2005. Topological Graph Theory and Graph Minors, second issue.

[76] G. A. Jones and R. Jajcay. Cayley properties of merged Johnson graphs. *Journal of Algebraic Combinatorics*, 44:1047–1067, 2016.

[77] C. Jordan. Recherches sur les substitutions. *Journal de Mathématiques Pures et Appliquées*, 17:351–367, 1872.

[78] D. Jordan. Eine Symmetrieeigenschaft von Graphen, Graphentheorie und ihre Anwendungen. In *Dresdner Reihe Forsch*, volume 9, pages 17–20, Stadt Wehlen, DE, 1988.

[79] W. M. Kantor and R. A. Liebler. The rank 3 permutation representation of the finite classical groups. *Transactions of the American Mathematical Society*, 271(1):1–71, 1982.

[80] B. Kivva. A characterization of Johnson and Hamming graphs and proof of Babai's conjecture. *Journal of Combinatorial Theory, Series B*, 151:339–374, 2021.

[81] M. Klin. On transitive permutation groups without semiregular subgroups. In *Proceedings of the International Congress of Mathematicians (ICM 1998)*, volume "Abstracts of short communications and poster sessions", page 279, Berlin, DE, 1998.

[82] L. G. Kovács. Wreath decompositions of finite permutation groups. *Bulletin of the Australian Mathematical Society*, 40(2):255–279, 1989.

[83] K. Kutnar and D. Marušič. Odd extensions of transitive groups via symmetric graphs – The cubic case. *Journal of Combinatorial Theory, Series B*, 136:170–192, 2019.

[84] E. Landau. Über die Maximalordnung der Permutationen gegebenen Grades. *Archiv der Mathematik und Physik*, 5:92–103, 1903.

[85] F. Lehner, P. Potočnik, and P. Spiga. On fixity of arc-transitive graphs. *Science China Mathematics*, 64:2603–2610, 2021.

[86] M. Lekše. Stabilizers of consistent walks. 2024. `arXiv:2405.16691`.

[87] J. S. Leon and D. B. Wales. Simple groups of order $2^a 3^b p^c$ with cyclic Sylow p-groups. *Journal of Algebra*, 29:246–254, 1974.

[88] M. W. Liebeck, C. E. Praeger, and J. Saxl. A classification of the maximal subgroups of the finite alternating and symmetric groups. *Journal of Algebra*, 111(2):365–383, 1987.

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

[90] M. W. Liebeck and J. Saxl. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of riemann surfaces. *Proceedings of the London Mathematical Society*, s3-63(2):266–314, 1991.

[91] M. W. Liebeck and A. Shalev. Simple groups, permutation groups and probability. *Journal of the American Mathematical Society*, 12(2):497–520, 1999.

[92] A. Lucchini. Prefrattini subgroups and crowns. *Archiv der Mathematik*, 121:469–483, 2023.

[93] A. Lucchini, F. Menegazzo, and M. Morigi. Asymptotic results for transitive permutation groups. *Bulletin of the London Mathematical Society*, 32(2):191–195, 2000.

[94] E. M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25(1):42–65, 1982.

[95] H. D. Macpherson. Infinite distance transitive graphs of finite valency. *Combinatorica*, 2:63–69, 1982.

[96] W. Magnus. A connection between the Baker–Hausdorff formula and a problem of Burnside. *Annals of Mathemathics*, 52:11–26, 1950.

[97] A. Malnič, D. Marušič, and P. Potočnik. Elementary Abelian covers of graphs. *Journal of Algebraic Combinatorics*, 20:71–97, 2004.

[98] D. Marušič and R. Scapellato. Permutation groups, vertex-transitive digraphs and semiregular automorphisms. *European Journal of Combinatorics*, 19(6):707–712, 1998.

[99] D. Marušič. On vertex symmetric digraphs. *Discrete Mathematics*, 36(1):69–81, 1981.

[100] A. Maróti. On the orders of primitive groups. *Journal of Algebra*, 258(2):631–640, 2002.

[101] R. Mathon. A note on the graph isomorphism counting problem. *Information Processing Letters*, 8(3):131–136, 1979.

[102] V. D. Mazurov and A. Kh. Zhurtov. On recognition of the finite simple groups $L_2(2^m)$ in the class of all groups. *Siberian Mathematical Journal*, 40(1):62–64, 1999.

[103] U. Meierfrankenfeld and B. Stellmacher. The general FF-module theorem. *Journal of Algebra*, 351(1):1–63, 2012.

[104] J. Morris, P. Spiga, and G. Verret. Semiregular automorphisms of cubic vertex-transitive graphs and the abelian normal quotient method. *The Electronic Journal of Combinatorics*, 22(3):P3.32, 2015.

[105] Gupta N. D and V. D. Mazurov. On groups with small orders of elements. *Bulletin of the Australian Mathematical Society*, 60(2):197–205, 1999.

[106] D. Neuen and P. Schweitzer. An exponential lower bound for individualization-refinement algorithms for graph isomorphism. *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, pages 138 – 150, 2017.

[107] B. H. Neumann. Groups whose elements have bounded orders. *The Journal of the London Mathematical Society*, 12(3):195–198, 1937.

[108] M. F. Newman. Groups of exponent dividing seventy. *The Mathematical Scientist*, 4(2):149–157, 1979.

[109] M. A. Perles, H. Martini, and Y. S. Kupitz. Locally symmetric graphs of girth 4. *Journal of Graph Theory*, 73(1):44–65, 2013.

[110] P. Potočnik. A list of 4-valent 2-arc-transitive graphs and finite faithful amalgams of index $(4,2)$. *European Journal of Combinatorics*, 30(5):1323–1336, 2009.

[111] P. Potočnik and P. Spiga. On the minimal degree of a transitive permutation group with stabilizer a 2-group. *Journal of Group Theory*, 24(3):619–634, 2021.

[112] P. Potočnik and P. Spiga. On the number of fixed points of automorphisms of vertex-transitive graphs. *Combinatorica*, 41:703–747, 2021.

[113] P. Potočnik, P. Spiga, and G. Verret. On graph-restrictive permutation groups. *Journal of Combinatorial Theory, Series B*, 102(3):820–831, 2012.

[114] P. Potočnik, P. Spiga, and G. Verret. On the nullspace of arc-transitive graphs over finite fields. *Journal of Algebraic Combinatorics*, 36:389–401, 2012.

[115] P. Potočnik, P. Spiga, and G. Verret. Cubic vertex-transitive graphs on up to 1 280 vertices. *Journal of Symbolic Computation*, 50:465–477, 2013.

[116] P. Potočnik, P. Spiga, and G. Verret. On the order of arc-stabilizers in arc-transitive graphs with prescribed local group. *Transactions of the American Mathematical Society*, 366(7):3729–3745, 2014.

[117] P. Potočnik, P. Spiga, and G. Verret. Bounding the order of the vertex-stabiliser in 3-valent vertex-transitive and 4-valent arc-transitive graphs. *Journal of Combinatorial Theory, Series B*, 111:148–180, 2015.

[118] P. Potočnik, P. Spiga, and G. Verret. A census of 4-valent half-arc-transitive graphs and arc-transitive digraphs of valence 2. *Ars Mathematica Contemporanea*, 8(1):133–148, 2015.

[119] P. Potočnik, P. Spiga, and G. Verret. A census of 4-valent half-arc-transitive graphs and arc-transitive digraphs of valence two. *Ars Matematica Contemporanea*, 8(1):133–148, 2015.

[120] P. Potočnik, M. Toledo, and G. Verret. On orders of automorphisms of vertex-transitive graphs. *Journal of Combinatorial Theory, Series B*, 166:123–153, 2024.

[121] P. Potočnik and S. Wilson. Tetravalent edge-transitive graphs of girth at most 4. *Journal of Combinatorial Theory, Series B*, 97(2):217–236, 2007.

[122] C. E. Praeger. Imprimitive symmetric graphs. *Ars Combinatorica*, 19(A):149–163, 1985.

[123] C. E. Praeger. Highly arc transitive digraphs. *European Journal of Combinatorics*, 10(3):281–292, 1989.

[124] C. E. Praeger. An O'Nan–Scott Theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs. *Journal of the London Mathematical Society*, s2-47(2):227–239, 1993.

[125] C. E. Praeger. Finite quasiprimitive group actions on graphs and designs. In *Groups – Korea'98*, pages 319–331, Pusan, 2000.

[126] C. E. Praeger and C. Schneider. Embedding permutation groups into wreath products in product action. *Journal of the Australian Mathematical Society*, 92(1):127–136, 2012.

[127] C. E. Praeger, P. Spiga, and G. Verret. Bounding the size of a vertex-stabiliser in a finite vertex-transitive graph. *Journal of Combinatorial Theory, Series B*, 102(3):797–819, 2012.

[128] C. E. Praeger and M. Xu. A characterization of a class of symmetric graphs of twice prime valency. *European Journal of Combinatorics*, 10:91–102, 1989.

[129] L. Pyber. Asymptotic results for permutation groups. In *Groups And Computation*, pages 197–219, New Brunswick, CA, 1991.

[130] L. Pyber. Enumerating finite groups of given order. *Annals of Mathematics*, 137(1):203–220, 1993.

[131] L. Pyber, C. E. Praeger, P. Spiga, and E. Szabó. Graphs with automorphism groups admitting composition factors of bounded rank. *Procedings of the American Mathemathical Society*, 140(7):2307–2318, 2012.

[132] L. Pyber and S. V. Skresanov. On the automorphism group of a distance-regular graph. 2023. arXiv:2312.00383.

[133] L. Pyber and E. Szabó. Growth in finite simple groups of Lie type. *Journal of the American Mathemathical Society*, 29:95–146, 2016.

[134] D. J. S. Robinson. *A Course in the Theory of Groups*. Spinger, New York, USA, 1996.

[135] G. Sabidussi. On a class of fixed-point-free graphs. *Proceedings of the American Mathematical Society*, 9:800–804, 1958.

[136] J.-P. Serre. *Trees*. Spinger, Heidelberg, DE, 2002.

[137] J.-P. Serre. On a theorem of Jordan. *Bulletin of the American Mathematical Society*, 40:429–440, 2003.

[138] C. C. Sims. Enumerating p-groups. *Proceedings of the London Mathematical Society*, s3-15(1):151–166, 1965.

[139] C. C. Sims. Graphs and finite permutation groups. *Mathematische Zeitschrift*, 95:76–86, 1967.

[140] C. C. Sims. *Computation with Finitely Presented Groups*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambrdidge, UK, 1994.

[141] D. H. Smith. Primitive and imprimitive graphs. *The Quarterly Journal of Mathematics*, 22(4):551–557, 1971.

[142] P. Spiga. On G-locally primitive graphs of locally twisted wreath type and a conjecture of Weiss. *Journal of Combinatorial Theory, Series A*, 118(8):2257–2260, 2011.

[143] P. Spiga. Two local conditions on the vertex stabiliser of arc-transitive graphs and their effect on the Sylow subgroups. *Journal of Group Theory*, 15(1):23–35, 2012.

[144] P. Spiga. Semiregular elements in cubic vertex-transitive graphs and the restricted Burnside problem. *Mathematical Proceedings of the Cambridge Philosophical Society*, 157(1):45–61, 2014.

[145] P. Spiga. An application of the Local $\mathcal{C}(G,T)$ Theorem to a conjecture of Weiss. *Bulletin of the London Mathematical Society*, 48(1):12–18, 2016.

[146] P. Spiga. Finite transitive groups having many suborbits of cardinality at most 2 and an application to the enumeration of Cayley graphs. *Canadian Journal of Mathematics*, 76(1):345–366, 2024.

[147] P. Spiga and G. Verret. On the order of vertex-stabilisers in vertex-transitive graphs with local group $C_p \times C_p$ or $C_p \,\mathrm{wr}\, C_2$. *Journal of Algebra*, 448:174–209, 2016.

[148] M. Suzuki. *Group Theory I*. Grundlehren der mathematischen Wissenschaften. Springer, Heidelberg, DE, 1982.

[149] J. G. Thompson. Bounds for orders of maximal subgroups. *Journal of Algebra*, 14(2):135–138, 1970.

[150] V. I. Trofimov. On the action of primitive groups. *Algebra Logika*, 28(3):337–363, 1989.

[151] V. I. Trofimov. Stabilizers of the vertices of graphs with projective suborbits. *Soviet Mathematics, Doklady*, 42:825–828, 1991.

[152] V. I. Trofimov. Graphs with projective suborbits. *Mathematics of the USSR - Izvestiya*, 39(1):869–893, 1992.

[153] V. I. Trofimov. On the weiss conjecture, I. *Mathematical Proceedings of the Cambridge Philosophical Society*, 319(supplement 1):S281–S290, 2022.

[154] W. T. Tutte. On a family of cubical graphs. *Mathematical Proceedings of the Cambridge Philosophical Society*, 43(3):459–474, 1947.

[155] W. T. Tutte. On the symmetry of cubic graphs. *Canadian Journal of Mathematics*, 11:621–624, 1959.

[156] J. J. van Bon. Thompson–Wielandt-like theorems revisited. *Bulletin of the London Mathematical Society*, 35(1):30–36, 2003.

[157] G. Verret. On the order of arc-stabilizers in arc-transitive graphs, II. *Bulletin of the Australian Mathematical Society*, 87(3):441–547, 2013.

[158] B. Yu. Weisfeiler and A. A. Leman. A reduction of a graph to a canonical form and an algebra arising during this reduction. *Nauchno Technicheskaya Informatsia*, 2(9):12–16, 1968.

[159] R. Weiss. s-transitive graphs. *Colloquia Mathematica Societatis János Bolyai*, 25:827–847, 1978.

[160] R. Weiss. An application of p-factorization methods to symmetric graphs. *Mathematical Proceedings of the Cambridge Philosophical Society*, 85(1):43–48, 1979.

[161] R. Weiss. Groups with a (B,N)-pair and locally transitive graphs. *Nagoya Mathematical Journal*, 74:1–21, 1979.

[162] R. Weiss. The nonexistence of 8-transitive graphs. *Combinatorica*, 1:309–311, 1981.

[163] R. Weiss. Graphs which are locally Grassmann. *Mathematische Annalen*, 297:325–334, 1993.

[164] H. Wielandt. *Finite permutation groups*. Academic Press, London, UK, 1964.

[165] E. I. Zel'manov. Solution of the restricted Burnside problem for groups of odd exponent. *Mathematics of the USSR – Izvestiya*, 36:41–60, 1991.

[166] E. I. Zel'manov. A solution of the restricted Burnside problem for 2-groups. *Mathematics of the USSR – Sbornik*, 72(2):543–565, 1992.