Canad. J. Math. Vol. 76 (1), 2024 pp. 345–366
http://dx.doi.org/10.4153/S0008414X23000093

Finite transitive groups having many suborbits of cardinality at most 2 and an application to the enumeration of Cayley graphs

Pablo Spiga

Abstract. Let G be a finite transitive group on a set Ω, let $\alpha \in \Omega$, and let G_α be the stabilizer of the point α in G. In this paper, we are interested in the proportion

$$\frac{|\{\omega \in \Omega \mid \omega \text{ lies in a } G_\alpha\text{-orbit of cardinality at most } 2\}|}{|\Omega|},$$

that is, the proportion of elements of Ω lying in a suborbit of cardinality at most 2. We show that, if this proportion is greater than 5/6, then each element of Ω lies in a suborbit of cardinality at most 2, and hence G is classified by a result of Bergman and Lenstra. We also classify the permutation groups attaining the bound 5/6.

We use these results to answer a question concerning the enumeration of Cayley graphs. Given a transitive group G containing a regular subgroup R, we determine an upper bound on the number of Cayley graphs on R containing G in their automorphism groups.

1 Introduction

This paper is part of a series [17–19, 24] aiming to obtain an asymptotic enumeration of finite Cayley graphs. However, the main players in this paper are not finite Cayley graphs, but finite transitive groups. Our results on finite transitive groups can then be used to make a considerable step toward the enumeration problem of Cayley graphs and thus getting closer to solving an outstanding question of Babai and Godsil (see [2] or [8, Conjecture 3.13]).

Let G be a finite transitive group on Ω, let $\alpha \in \Omega$, and let G_α be the stabilizer in G of the point α. The orbits of G_α on Ω are said to be the *suborbits* of G and their cardinalities are said to be the *subdegrees* of G. In this paper, we are concerned in finite transitive groups having many subdegrees equal to 1 or 2. In particular, we are interested in the ratio

$$\mathbf{I}_\Omega(G) := \frac{|\{\omega \in \Omega \mid \omega \text{ lies in a } G_\alpha\text{-orbit of cardinality at most } 2\}|}{|\Omega|}.$$

Received by the editors September 27, 2021; revised June 16, 2022; accepted July 10, 2022.
Published online on Cambridge Core January 30, 2023.
AMS subject classification: **05C25**, 05C30, 20B25, 20B15.
Keywords: Suborbits, Cayley graph, automorphism group, asymptotic enumeration, graphical regular representation.

As G is transitive on Ω, the value of $\mathbf{I}_\Omega(G)$ does not depend on α. Clearly, $0 < \mathbf{I}_\Omega(G) \leq 1$.

Theorem 1.1 *Let G be a finite transitive group on Ω, let $\alpha \in \Omega$, and let G_α be the stabilizer in G of the point α. If $\mathbf{I}_\Omega(G) > \frac{5}{6}$, then $\mathbf{I}_G(G_\alpha) = 1$, that is, each suborbit of G has cardinality at most 2.*

It turns out that finite transitive groups G with $\mathbf{I}_\Omega(G) = 1$ are classified by a classical result of Bergman and Lenstra [3]. The result of Bergman and Lenstra is rather general and applies to arbitrary (i.e., not necessarily finite) groups. The proof of [3, Theorem 1] is very beautiful and it is based on certain equivalence relations; also the strengthening of Isaacs [14] of the theorem of Bergman and Lenstra has a remarkably ingenious proof.

From [3, Theorem 1], finite transitive groups with $\mathbf{I}_\Omega(G) = 1$ can be partitioned in three families:

(a) finite transitive groups G where the stabilizer G_α has order 1,
(b) finite transitive groups G where the stabilizer G_α has order 2,
(c) finite transitive groups G admitting an elementary abelian normal 2-subgroup N with $|N : G_\alpha| = 2$.

In the first family, each suborbit of G has cardinality 1, that is, G acts regularly on Ω. In the second family, since G_α has cardinality 2, each orbit of G_α has cardinality at most 2. In the third family, since $N \trianglelefteq G$, the orbits of N on Ω form a system of imprimitivity for the action of G; as $|N : G_\alpha| = 2$, the blocks of this system of imprimitivity have cardinality 2 and hence all orbits of G_α have cardinality at most 2.

Theorem 1.1 shows that, with respect to the operator $\mathbf{I}_\Omega(G)$, there is a gap between 5/6 and 1. The value 5/6 is special: there exist finite transitive groups attaining the value 5/6.

Theorem 1.2 *Let G be a finite transitive group on Ω, let $\alpha \in \Omega$, and let G_α be the stabilizer in G of the point α. If $\mathbf{I}_\Omega(G) = \frac{5}{6}$, then there exists an elementary abelian normal 2-subgroup V of G with $|V : G_\alpha| = |G_\alpha| = 4$.*

Moreover, let e_1, e_2, e_3, e_4 be a basis of V, regarded as a four-dimensional vector space over the field with two elements, with $G_\alpha = \langle e_1, e_2 \rangle$, let $H := G/\mathbf{C}_G(V)$ where $\mathbf{C}_G(V)$ is the centralizer of V in G, and let K be the stabilizer of the subspace G_α in $\mathrm{GL}(V)$. Then, H is K-conjugate to one of the following two groups:

$$\left\langle \begin{pmatrix} 0&0&0&1\\1&1&0&0\\0&0&1&0\\1&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 0&0&0&1\\1&1&0&0\\0&0&1&0\\1&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&1\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&1&0&0\\1&1&0&1\\1&1&1&0 \end{pmatrix} \right\rangle.$$

The first group has order 12 and is isomorphic to the alternating group of degree 4 and the second group has order 24 and is isomorphic to the symmetric group of degree 4.

Conversely, if G is a finite group containing an elementary abelian normal 2-subgroup $V := \langle e_1, e_2, e_3, e_4 \rangle$ of order 16 and $H := G/\mathbf{C}_G(V)$ is as above, then the action of G on the set Ω of the right cosets of $\langle e_1, e_2 \rangle$ gives rise to a finite permutation group of degree $4|G : V|$ with $\mathbf{I}_\Omega(G) = 5/6$.

Theorem 1.2 classifies the finite transitive groups attaining the bound 5/6.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Before discussing our motivation for proving Theorems 1.1 and 1.2, we make some speculations. A computer search among the transitive groups G of degree at most 48 with the computer algebra system `magma` [5] reveals that, if $\mathbf{I}_\Omega(G) > 1/2$, then $\mathbf{I}_\Omega(G) = (q+1)/2q$, for some $q \in \mathbb{Q}$ with $2q \in \mathbb{N}$. We pose this as a conjecture.

Conjecture 1.3 *Let G be a finite transitive group on Ω. If $\mathbf{I}_\Omega(G) > 1/2$, then $\mathbf{I}_\Omega(G) = (q+1)/2q$, for some $q \in \mathbb{Q}$ with $2q \in \mathbb{N}$.*

If true, Conjecture 1.3 establishes a permutation analog with a classical problem in finite group theory. Let G be a finite group, and let

$$\mathbf{I}(G) := \{x \in G \mid x \text{ has order at most } 2\}.$$

Miller [16] in 1905 has shown that, if $\mathbf{I}(G) > 3/4$, then each element of G has order at most 2 and hence G is an elementary abelian 2-group. In this regard, Theorem 1.1 can be seen as a permutation analog of the theorem of Miller, with the only difference that the ratio 3/4 in the context of abstract groups has to bump up to 5/6 in the context of permutation groups. Miller has also classified the finite groups G with $\mathbf{I}(G) = 3/4$. Therefore, Theorem 1.2 can be seen as a permutation analog of the classification of Miller. The theorem of Miller has stimulated a lot of research; for instance, Wall [26] has classified all finite groups G with $\mathbf{I}(G) > 1/2$. In his proof, Wall uses the Frobenius–Schur formula for counting involutions. An application of this classification shows that, if $\mathbf{I}(G) > 1/2$, then $\mathbf{I}(G) = (q+1)/2q$, for some positive integer q. Therefore, in Conjecture 1.3, we believe that the same type of result holds for the permutation analog $\mathbf{I}_\Omega(G)$, but allowing q to be an element of $\{x/2 \mid x \in \mathbb{N}\}$. As a wishful thinking, we also pose the following problem.

Problem 1.4 Classify the finite transitive groups G acting on Ω with $\mathbf{I}_\Omega(G) > 1/2$.

Liebeck and MacHale [15] have generalized the results of Miller and Wall in yet another direction. Indeed, Liebeck and MacHale have classified the finite groups G admitting an automorphism inverting more than half of the elements of G. (The classical results of Miller and Wall can be recovered by considering the identity automorphism.) Then, this classification has been pushed even further by Fitzpatrick [7] and Hegarty and MacHale [10], by classifying the finite groups G admitting an automorphism inverting exactly half of the elements of G. An application of this classification shows that, if α is an automorphism of G inverting more than half of the elements of G, then the proportion of elements inverted by α is $(q+1)/2q$, for some positive integer q. Yet again, another analog with Theorems 1.1 and 1.2, with Conjecture 1.3 and with Problem 1.4. We observe that a partial generalization of this type of results in the context of association schemes is in [20].

We now discuss our original motivation for proving Theorems 1.1 and 1.2. A *digraph* Γ is an ordered pair (V, E), where V a finite nonempty set of vertices, and E is a subset of $V \times V$, representing the arcs. A *graph* Γ is a digraph (V, E), where the binary relation E is symmetric. An automorphism of a (di)graph is a permutation on V that preserves the set E.

Definition 1.5 Let R be a group, and let S be a subset of R. The *Cayley digraph* $\Gamma(R, S)$ is the digraph with $V = R$ and $(r, t) \in E$ if and only if $tr^{-1} \in S$.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

The Cayley digraph is a graph if and only if $S = S^{-1}$, that is, S is an inverse-closed subset of R.

The problem of finding graphical regular representations (GRRs) for groups has a long history. Mathematicians have studied graphs with specified automorphism groups at least as far back as the 1930s, and in the 1970s there were many papers devoted to the topic of finding GRRs (see, for example, [1, 11–13, 21–23, 27]), although the "GRR" terminology was coined somewhat later.

Definition 1.6 A *digraphical regular representation* (DRR) for a group R is a digraph whose full automorphism group is the group R acting regularly on the vertices of the digraph.

Similarly, a GRR for a group R is a graph whose full automorphism group is the group R acting regularly on the vertices of the graph.

It is an easy observation that when $\Gamma(R, S)$ is a Cayley digraph (graph), the group R acts regularly on the vertices as a group of graph automorphisms. A DRR (or GRR) for R is therefore a Cayley digraph (graph) on R that admits no other automorphisms.

The main thrust of much of the work through the 1970s was to determine which groups admit GRRs. This question was ultimately answered by Godsil in [9]. The corresponding result for DRRs was proved by a much simpler argument by Babai [1].

Babai and Godsil made the following conjecture. (Given a finite group R, $2^{\mathbf{c}(R)}$ denotes the number of inverse-closed subsets of R. See Definition 1.10 for the definition of generalized dicyclic group.)

Conjecture 1.7 ([2]; Conjecture 3.13 [8]) *If R is not generalized dicyclic or abelian of exponent greater than 2, then for almost all inverse-closed subsets S of R, $\Gamma(R, S)$ is a GRR. In other words,*

$$\lim_{|R|\to\infty} \min\left\{ \frac{\left|\{S \subseteq R : S = S^{-1},\ \mathrm{Aut}(\Gamma(R,S)) = R\}\right|}{2^{\mathbf{c}(R)}} : R \text{ admits a GRR} \right\} = 1.$$

From Godsil's theorem [9], as $|R| \to \infty$, the condition "R admits a GRR" is equivalent to "R is neither a generalized dicyclic group, nor abelian of exponent greater than 2."

The corresponding conjecture for Cayley digraphs (which does not require any families of groups to be excluded) was proved by Morris and the author in [18]. Our current strategy for proving the conjecture of Babai and Godsil is to use the proof of the corresponding conjecture for Cayley digraphs as a template and extend the work in [18] in the context of undirected Cayley graphs. This strategy so far has been rather successful and in [17, 24] the authors have already adapted some of the arguments in [18] for undirected graphs.

One key tool in [18] is an elementary observation of Babai.

Lemma 1.8 *Let G be a finite transitive group acting on a set Ω and properly containing a regular subgroup R. Then there are at most $2^{\frac{3|\Omega|}{4}} = 2^{\frac{3|R|}{4}}$ Cayley digraphs Γ on R with $G \leq \mathrm{Aut}(\Gamma)$.*

The proof of this fact is elementary (see, for instance, [18, Lemma 3.1]). Observe that the number of Cayley digraphs on R is the number of subsets of R, that is, $2^{|R|}$.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Therefore, Lemma 1.8 says that, given G properly containing R, only at most $2^{|R|-\frac{|R|}{4}}$ of these Cayley digraphs admit G as a group of automorphisms. This gain of $|R|/4$ is one of the tools in [18] for proving the Babai–Godsil conjecture on Cayley digraphs.

To continue our project of proving the Babai–Godsil conjecture for Cayley graphs, we need an analog of Lemma 1.8 for Cayley graphs. Observe that the number of Cayley graphs on R is the number of inverse-closed subsets of R. We denote this number with $2^{\mathbf{c}(R)}$. It is not hard to prove (see, for instance, [17, Lemma 1.12]) that

$$\mathbf{c}(R) = \frac{|R| + |\mathbf{I}(R)|}{2},$$

where $\mathbf{I}(R) = \{x \in R \mid x^2 = 1\}$. To obtain this analog, one needs to investigate finite transitive groups having many suborbits of cardinality at most 2. Therefore, our investigation leads to the following result.

Theorem 1.9 *Let G be a finite transitive group properly containing a regular subgroup R. Then one of the following holds:*

(a) *The number of Cayley graphs Γ on R with $G \leq \mathrm{Aut}(\Gamma)$ is at most $2^{\mathbf{c}(R)-\frac{|R|}{96}}$.*
(b) *R is abelian of exponent greater than 2.*
(c) *R is generalized dicyclic (see Definition 1.10).*

1.1 Notation

In this section, we establish some notation that we use throughout the rest of the paper.

Given a subset X of permutations from Ω, we use an exponential notation for the action on Ω and hence, in particular, given $\omega \in \Omega$, we let

$$\omega^X := \{\omega^x \mid x \in X\},$$

where ω^x is the image of ω under the permutation x. Similarly, we let

$$\mathrm{Fix}_\Omega(X) := \{\omega \in \Omega \mid \omega^x = \omega,\ \forall x \in X\}.$$

Let G be a transitive permutation group on Ω. Recall that a nonempty subset Δ of Ω is said to be a block of imprimitivity if, for every $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \varnothing$. Observe that, when Δ is a block of imprimitivity, $\{\Delta^g \mid g \in G\}$ is a partition of the set Ω and hence $|\Delta|$ divides $|\Omega|$.

For each positive integer i and for each $\omega \in \Omega$, we let

$$\Omega_{\omega,i} := \{\delta \in \Omega \mid |\delta^{G_\omega}| = i\}. \tag{1}$$

Observe that, $\delta \in \Omega_{\omega,i}$ if and only if $i = |\delta^{G_\omega}| = |G_\omega : G_\omega \cap G_\delta|$. In particular, since G is transitive on Ω, we have $|G_\omega| = |G_\delta|$ and hence $|\delta^{G_\omega}| = |G_\omega : G_\omega \cap G_\delta| = |G_\delta : G_\omega \cap G_\delta| = |\omega^{G_\delta}|$. Therefore,

$$\delta \in \Omega_{\omega,i} \text{ if and only if } \omega \in \Omega_{\delta,i}. \tag{2}$$

We use often (2) in what follows.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Clearly,

$$\Omega = \Omega_{\omega,1} \cup \Omega_{\omega,2} \cup \Omega_{\omega,3} \cup \cdots \tag{3}$$

and the nonempty sets in this union form a partition of Ω.

When $i := 1$, we have

$$\Omega_{\omega,1} = \{\delta \in \Omega \mid G_\omega \text{ fixes } \delta\},$$

that is, $\Omega_{\omega,1}$ is the set of fixed points of G_ω on Ω. It is well known that $\Omega_{\omega,1}$ is a block of imprimitivity for the action of G on Ω (see, for instance, [6, 1.6.5]). Since this fact will play a role in what follows, we prove it here; this will also be helpful for setting up some additional notation. Let $\mathbf{N}_G(G_\omega)$ be the normalizer of G_ω in G. As $\mathbf{N}_G(G_\omega)$ contains G_ω, the $\mathbf{N}_G(G_\omega)$-orbit containing ω is a block of imprimitivity for the action of G on Ω. Therefore, it suffices to prove that $\Omega_{\omega,1}$ is the $\mathbf{N}_G(G_\omega)$-orbit containing ω, that is, $\Omega_{\omega,1} = \omega^{\mathbf{N}_G(G_\omega)} = \{\omega^g \mid g \in \mathbf{N}_G(G_\omega)\}$. If $g \in \mathbf{N}_G(G_\omega)$, then $G_\omega = G_\omega^g = G_{\omega g}$ and hence G_ω fixes ω^g, that is, $\omega^g \in \Omega_{\omega,1}$. Conversely, let $\alpha \in \Omega_{\omega,1}$. As G is transitive on Ω, there exists $g \in G$ with $\alpha = \omega^g$. Thus $\omega^g \in \Omega_{\omega,1}$ and G_ω fixes ω^g. This yields $G_\omega = G_{\omega g} = G_\omega^g$ and $g \in \mathbf{N}_G(G_\omega)$. Therefore, $\alpha = \omega^g$ lies in the $\mathbf{N}_G(G_\omega)$-orbit containing ω.

We let

$$d := |\Omega_{\omega,1}|.$$

As G is transitive on Ω, d does not depend on ω. We claim that, if $g \in G$ and $\Omega_{\omega,1}^g \cap \Omega_{\omega,i} \neq \varnothing$, then $\Omega_{\omega,1}^g \subseteq \Omega_{\omega,i}$. To this end, let $\alpha \in \Omega_{\omega,1}^g \cap \Omega_{\omega,i}$. As $\alpha \in \Omega_{\omega,1}^g = \Omega_{\omega g,1}$, we deduce that $G_{\omega g}$ fixes α and hence $G_{\omega g} \leq G_\alpha$. Since G is transitive on Ω, the subgroups $G_{\omega g}$ and G_α have the same cardinality and hence $G_{\omega g} = G_\alpha$. From this, it follows that $\Omega_{\omega g,1} = \Omega_{\alpha,1}$ and hence we need to show that $\Omega_{\alpha,1} \subseteq \Omega_{\omega,i}$. Let $\beta \in \Omega_{\alpha,1}$; in particular, $\Omega_{\alpha,i} = \Omega_{\beta,i}$ because $G_\alpha = G_\beta$. As $\alpha \in \Omega_{\omega,i}$, from (2), we deduce $\omega \in \Omega_{\alpha,i} = \Omega_{\beta,i}$. Another application of (2) gives $\beta \in \Omega_{\omega,i}$. Since β is an arbitrary element of $\Omega_{\alpha,1}$, we deduce $\Omega_{\alpha,1} \subseteq \Omega_{\omega,i}$.

Since $\Omega_{\omega,1}$ is a block of imprimitivity for the action of G on Ω, $\{\Omega_{\omega,1}^g \mid g \in G\}$ is a partition of Ω into subsets of cardinality $|\Omega_{\omega,1}| = d$. In particular, from the previous claim, we deduce that d divides $|\Omega_{\omega,i}|$, for each positive integer i. We define

$$x_i := \frac{|\Omega_{\omega,i}|}{|\Omega_{\omega,1}|} = \frac{|\Omega_{\omega,i}|}{d} \in \mathbb{N}. \tag{4}$$

In particular, $x_1 := 1$ and, from (3) and (4), we have

$$|\Omega| = d \sum_i x_i.$$

Observe that, as G is transitive on Ω, $|\Omega_{\omega,i}|$ does not depend on the choice of $\omega \in \Omega$. Thus x_i does not depend on the choice of $\omega \in \Omega$.

Definition 1.10 Let A be an abelian group of even order and of exponent greater than 2, and let y be an involution of A. The generalized dicyclic group $\mathrm{Dic}(A, y, x)$ is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A\rangle$. A group is called *generalized dicyclic* if it is isomorphic to some $\mathrm{Dic}(A, y, x)$. When A is cyclic, $\mathrm{Dic}(A, y, x)$ is called a dicyclic or generalized quaternion group.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

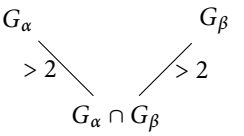

Figure 1: Auxiliary picture for the proof of Lemma 2.1.

2 Lemmata

In this section, we use the notation established in Section 1.1.

Lemma 2.1 *Let G be a finite transitive permutation group on a set Ω, and let $\alpha \in \Omega$. If*

$$\frac{|\Omega|}{2} < |\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| < |\Omega|,$$

then:

(a) $\Omega = \Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$ (*in particular, $\Omega_{\alpha,i} = \varnothing$, for every positive integer i with $i \notin \{1, 2, 4\}$*).
(b) *For every $\beta \in \Omega_{\alpha,4}$, $\Omega_{\alpha,2} \cap \Omega_{\beta,2} \neq \varnothing$.*
(c) *For every $\beta \in \Omega_{\alpha,4}$ and for every $\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}$, we have $G_\omega = (G_\alpha \cap G_\omega)(G_\beta \cap G_\omega)$.*

Proof As $|\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| < |\Omega|$, by (3), we get that $\Omega_{\alpha,1} \cup \Omega_{\alpha,2}$ is strictly contained in Ω. Therefore, let $\beta \in \Omega \setminus (\Omega_{\alpha,1} \cup \Omega_{\alpha,2})$.

Since $\beta \notin \Omega_{\alpha,1} \cup \Omega_{\alpha,2}$ and since the action of G on Ω is transitive, we have

$$|G_\alpha : G_\alpha \cap G_\beta| = |G_\beta : G_\alpha \cap G_\beta| > 2. \tag{5}$$

See Figure 1.

From this, we deduce

$$\Omega_{\alpha,1} \cap \Omega_{\beta,1} = \Omega_{\alpha,2} \cap \Omega_{\beta,1} = \Omega_{\alpha,1} \cap \Omega_{\beta,2} = \varnothing. \tag{6}$$

Indeed, if, for instance, $\omega \in \Omega_{\alpha,1} \cap \Omega_{\beta,2}$, then $|\omega^{G_\alpha}| = 1$ and $|\omega^{G_\beta}| = 2$. Therefore, $|G_\alpha : G_\alpha \cap G_\omega| = 1$ and $|G_\beta : G_\beta \cap G_\omega| = 2$. As $|G_\alpha : G_\alpha \cap G_\omega| = 1$, we get $G_\alpha = G_\omega$. Now, as $|G_\beta : G_\beta \cap G_\omega| = 2$ and $G_\alpha = G_\omega$, we get $2 = |G_\beta : G_\beta \cap G_\omega| = |G_\beta : G_\beta \cap G_\alpha|$, which contradicts (5). Therefore, $\Omega_{\alpha,1} \cap \Omega_{\beta,2} = \varnothing$. The proof for all other equalities in (6) is similar.

From (6), we obtain

$$(\Omega_{\alpha,1} \cup \Omega_{\alpha,2}) \cap (\Omega_{\beta,1} \cup \Omega_{\beta,2}) = \Omega_{\alpha,2} \cap \Omega_{\beta,2}. \tag{7}$$

Recall that, by hypothesis, $|\Omega_{\alpha,1} \cup \Omega_{\alpha,2}| > |\Omega|/2$. Using this together with (7), we get

$$\begin{aligned} |\Omega_{\alpha,2} \cap \Omega_{\beta,2}| &= |(\Omega_{\alpha,1} \cup \Omega_{\alpha,2}) \cap (\Omega_{\beta,1} \cup \Omega_{\beta,2})| \\ &= |\Omega_{\alpha,1} \cup \Omega_{\alpha,2}| + |\Omega_{\beta,1} \cup \Omega_{\beta,2}| - |(\Omega_{\alpha,1} \cup \Omega_{\alpha,2}) \cup (\Omega_{\beta,1} \cup \Omega_{\beta,2})| \\ &\geq |\Omega_{\alpha,1} \cup \Omega_{\alpha,2}| + |\Omega_{\beta,1} \cup \Omega_{\beta,2}| - |\Omega| \\ &> \frac{|\Omega|}{2} + \frac{|\Omega|}{2} - |\Omega| = 0. \end{aligned} \tag{8}$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

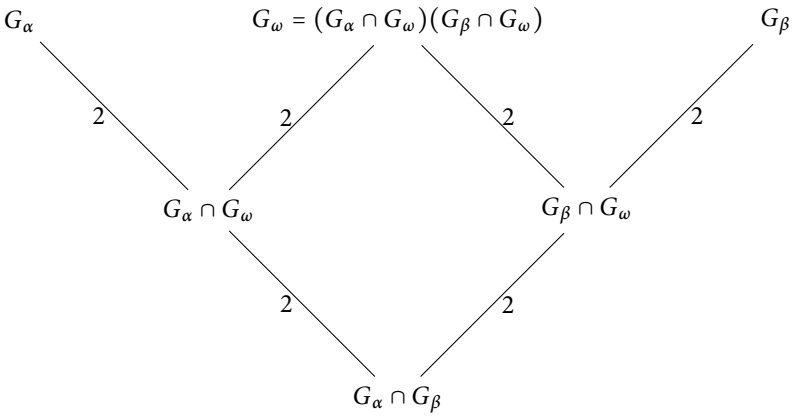

Figure 2: Auxiliary picture for the proof of Lemma 2.1.

From (8), we deduce $\Omega_{\alpha,2} \cap \Omega_{\beta,2} \neq \varnothing$. Let $\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}$. In particular, $|\omega^{G_\alpha}| = |\omega^{G_\beta}| = 2$. This means that $|G_\alpha : G_\alpha \cap G_\omega| = |G_\beta : G_\beta \cap G_\omega| = 2$. Since $|G_\alpha| = |G_\beta| = |G_\omega|$, we get that $G_\alpha \cap G_\omega$ and $G_\beta \cap G_\omega$ have both index 2 in G_ω. Suppose $G_\alpha \cap G_\omega = G_\beta \cap G_\omega$. Then

$$G_\alpha \cap G_\omega = G_\beta \cap G_\omega = G_\alpha \cap G_\beta \cap G_\omega \leq G_\alpha \cap G_\beta,$$

and hence

$$|G_\alpha : G_\alpha \cap G_\beta| \leq |G_\alpha : G_\alpha \cap G_\omega| = 2.$$

However, this contradicts (5). Therefore, $G_\alpha \cap G_\omega$ and $G_\beta \cap G_\omega$ are two distinct subgroups of G_ω having index 2. This yields

$$G_\omega = (G_\alpha \cap G_\omega)(G_\beta \cap G_\omega), \tag{9}$$

for each $\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}$.

From (9) and from the fact that $|G_\omega : G_\alpha \cap G_\omega| = |G_\omega : G_\beta \cap G_\omega| = 2$, we see that $(G_\alpha \cap G_\omega) \cap (G_\beta \cap G_\omega) = G_\alpha \cap G_\beta \cap G_\omega$ has index 4 in G_ω. Since $|G_\omega| = |G_\alpha| = |G_\beta|$, we get that $G_\alpha \cap G_\beta \cap G_\omega$ has also index 4 in G_α and in G_β. Since $G_\alpha \cap G_\beta \cap G_\omega \leq G_\alpha \cap G_\beta$, we get that $|G_\alpha : G_\alpha \cap G_\beta| = |G_\beta : G_\alpha \cap G_\beta|$ divides $|G_\alpha : G_\alpha \cap G_\beta \cap G_\omega| = 4$. As $|G_\alpha : G_\alpha \cap G_\beta| = |G_\beta : G_\alpha \cap G_\beta| > 2$, we get $G_\alpha \cap G_\beta \cap G_\omega = G_\alpha \cap G_\beta$ and

$$|G_\alpha : G_\alpha \cap G_\beta| = |G_\beta : G_\alpha \cap G_\beta| = 4.$$

We have summarized this paragraph in Figure 2. In other words, $\beta \in \Omega_{\alpha,4}$.

Since β is an arbitrary element in $\Omega \backslash (\Omega_{\alpha,1} \cup \Omega_{\alpha,2})$, we have proven part (a). Now, as $\Omega_{\alpha,4} = \Omega \backslash (\Omega_{\alpha,1} \cup \Omega_{\alpha,2})$, part (b) follows from (8) and part (c) follows from (9). ■

Lemma 2.2 *Let G be a finite transitive permutation group on a set Ω, and let $\alpha \in \Omega$. If $\Omega = \Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$ and $|\Omega_{\alpha,1}| = |\Omega_{\alpha,4}|$, then $\Omega_{\alpha,1} \cup \Omega_{\alpha,4}$ is a block of imprimitivity for G. Moreover, for every $\beta \in \Omega_{\alpha,4}$, we have $\mathbf{N}_G(G_\alpha) = \mathbf{N}_G(G_\beta)$.*

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Proof Let $\beta \in \Omega_{\alpha,4}$. As $\Omega_{\beta,1} \subseteq \Omega_{\alpha,4}$ and as $\Omega_{\beta,1}$ and $\Omega_{\alpha,4}$ have the same cardinality, we deduce $\Omega_{\alpha,4} = \Omega_{\beta,1}$. Analogously, $\Omega_{\beta,4} = \Omega_{\alpha,1}$.

Let $g \in G$ with $\beta = \alpha^g$. Now, we have

$$(\Omega_{\alpha,4})^g = \Omega_{\alpha^g,4} = \Omega_{\beta,4} = \Omega_{\alpha,1}.$$

Analogously, $\Omega_{\alpha,1}^g = \Omega_{\alpha,4}$. So,

$$\Omega_{\alpha,1}^g = \Omega_{\alpha,4} \text{ and } \Omega_{\alpha,4}^g = \Omega_{\alpha,1}.$$

Therefore, $(\Omega_{\alpha,1} \cup \Omega_{\alpha,4})^g = \Omega_{\alpha,1} \cup \Omega_{\alpha,4}$ and g^2 fixes setwise $\Omega_{\alpha,1}$ and $\Omega_{\alpha,4}$.

Since $\Omega_{\alpha,1}$ is a block of imprimitivity for G with setwise stabilizer $\mathbf{N}_G(G_\alpha)$, we deduce $g^2 \in \mathbf{N}_G(G_\alpha)$. Set $T := \langle \mathbf{N}_G(G_\alpha), g \rangle$.

Since G_α fixes setwise $\Omega_{\alpha,1} \cup \Omega_{\alpha,4}$, we deduce that G_α fixes setwise also $\Omega_{\alpha,4} = \Omega_{\beta,1}$. Now, for every $x \in \mathbf{N}_G(G_\alpha)$, we have

$$\Omega_{\alpha,1}^{g^{-1}\alpha g} = (\Omega_{\alpha,1}^{g^{-1}})^{xg} = \Omega_{\beta,1}^{xg} = (\Omega_{\beta,1}^{x})^g = \Omega_{\beta,1}^g = \Omega_{\alpha,1}.$$

Thus, $g^{-1}xg$ fixes setwise $\Omega_{\alpha,1}$ and hence $g^{-1}xg \in \mathbf{N}_G(G_\alpha)$. This yields

$$\mathbf{N}_G(G_\beta) = \mathbf{N}_G(G_{\alpha^g}) = (\mathbf{N}_G(G_\alpha))^g = \mathbf{N}_G(G_\alpha).$$

As g normalizes $\mathbf{N}_G(G_\alpha)$, we have $T = \mathbf{N}_G(G_\alpha)\langle g \rangle$ and

$$\alpha^T = (\alpha^{\mathbf{N}_G(G_\alpha)})^{\langle g \rangle} = \Omega_{\alpha,1}^{\langle g \rangle} = \Omega_{\alpha,1} \cup \Omega_{\alpha,4}.$$

Now, since T is an overgroup of G_α and since $\Omega_{\alpha,1} \cup \Omega_{\alpha,4}$ is the T-orbit containing α, we deduce that $\Omega_{\alpha,1} \cup \Omega_{\alpha,4}$ is a block of imprimitivity for G. ∎

We now need two rather technical lemmas, at first they seem out of context, but their relevance is pivotal in the proof of Lemma 2.5. We could phrase Lemma 2.3 in a purely group theoretic terminology, but it is easier to state in our opinion using some terminology from graph theory.

Lemma 2.3 *Let G be a group, let X be an elementary abelian 2-subgroup of G, and let Y be a G-conjugate of X with $Z := X \cap Y$ having index 4 in X and in Y. Let $\Lambda_X := \{X_1, X_2, X_3\}$ and $\Lambda_Y := \{Y_1, Y_2, Y_3\}$ be the collection of the proper subgroups of X and Y, respectively, properly containing Z.*

Let Γ be the bipartite graph having vertex set $\Lambda_X \cup \Lambda_Y$, where a pair $\{X_i, Y_j\}$ is declared to be adjacent if X_iY_j is a subgroup of G conjugate to X via an element of G. If Γ has at least six edges, then X commutes with Y.

Proof Suppose that

(*) there exist two distinct vertices of Γ having valency at least 2.

By symmetry, without loss of generality, we suppose that these two vertices are in Λ_X. Thus, suppose that $X_i, X_j \in \Lambda_X$ have valency at least 2 in Γ.

Let Y_{i_1} and Y_{i_2} be two neighbors of X_i in Γ. Then, by definition, $X_iY_{i_1}$ and $X_iY_{i_2}$ are both subgroups of G conjugate to X. Therefore, $X_iY_{i_1}$ and $X_iY_{i_2}$ are elementary abelian 2-groups and hence X_i commutes with both Y_{i_1} and Y_{i_2}. Since $\langle Y_{i_1}, Y_{i_2} \rangle = Y$, we deduce that X_i commutes with Y.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Arguing as in the paragraph above with X_i replaced by X_j, we deduce that X_j commutes with Y. Therefore, $X = \langle X_i, X_j \rangle$ commutes with Y.

Now, it is elementary to see that every bipartite graph on six vertices, with parts having cardinality 3 and having at least six edges has the property $(*)$. ∎

Recall that a graph Γ is said to be vertex-transitive if its automorphism group acts transitively on the vertices of Γ. Given a vertex ω of Γ, we denote by $\Gamma(\omega)$ the neighborhood of ω in Γ.

Lemma 2.4 *Let Γ be a finite vertex-transitive graph with all vertices of valency 2, let V be the set of vertices of Γ, let ω_1, ω_2 be two adjacent vertices of Γ, and let W be a subset of V containing ω_1 and ω_2 and with the property that, for any two distinct vertices δ_1, δ_2 in W, $V \setminus (\Gamma(\delta_1) \cup \Gamma(\delta_2)) \subseteq W$. Then either $W = V$ or $|V| \leq 6$.*

Proof Since Γ is vertex-transitive of valency 2, Γ is a disjoint union of s cycles of the same length ℓ. If $\ell \geq 7$ or if Γ is disconnected, that is, $s \geq 2$, it can be easily checked that $W = V$. ∎

Lemma 2.5 *Let G be a finite transitive permutation group on a set Ω, and let $\alpha \in \Omega$. If*

$$\frac{|\Omega|}{2} < |\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| < |\Omega|,$$

then one of the following holds:

(a) $|\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| < 5|\Omega|/6$, *or*
(b) (i) $|\Omega_{\alpha,4}| \leq 2|\Omega_{\alpha,1}|$,
(ii) G_α *is an elementary abelian 2-group,*
(iii) G_α *commutes with G_β, for every $\beta \in \Omega_{\alpha,4}$, and*
(iv) $\langle G_\alpha, G_\beta \rangle = G_\alpha \times G_\beta$ *is an elementary abelian normal 2-subgroup of G of order 16, for every $\beta \in \Omega_{\alpha,4}$.*

Proof From Lemma 2.1, $\Omega = \Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$. Moreover, for each $\beta \in \Omega_{\alpha,4}$, we have shown that G_α contains a proper subgroup (namely, $G_\alpha \cap G_\omega$, for each $\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}$) strictly containing $G_\alpha \cap G_\beta$. This implies that the permutation group, P say, induced by G_α in its action on the suborbit β^{G_α} is a 2-group. (Indeed, if G_α induces the alternating group $\mathrm{Alt}(4)$ or the symmetric group $\mathrm{Sym}(4)$ on β^{G_α}, then G_α acts primitively on β^{G_α} and hence $G_\alpha \cap G_\beta$ is maximal in G_α.) Clearly, this 2-group P must be either cyclic of order 4, or elementary abelian of order 4, or dihedral of order 8.

We have drawn in Figure 3, the lattice of subgroups of the cyclic group of order 4, the elementary abelian group of order 4 and the dihedral group of order 8: the dark colored nodes indicate the lattice of subgroups between the whole group and the stabilizer of a point.

Figure 3 shows that, given G_α and $G_\alpha \cap G_\beta$, we only have one choice for $G_\alpha \cap G_\omega$ when P is cyclic of order 4 or dihedral of order 8, whereas, we have at most three choices for $G_\alpha \cap G_\omega$ when P is elementary abelian of order 4.

Given $\beta \in \Omega_{\alpha,4}$, let

$$\mathcal{S}_{\alpha,\beta} := \{G_\omega \mid \omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}\}.$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

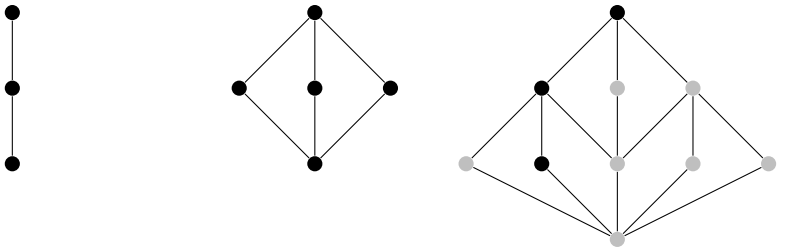

Figure 3: Auxiliary picture for the proof of Lemma 2.5.

Observe that in the set $\mathcal{S}_{\alpha,\beta}$, we are collecting point stabilizers and not elements of Ω and hence different elements ω_1, ω_2 of Ω can give rise to the same element of $\mathcal{S}_{\alpha,\beta}$ when $G_{\omega_1} = G_{\omega_2}$.

We claim that

(10)
$$|\mathcal{S}_{\alpha,\beta}| \leq \begin{cases} 3, & \text{when the permutation group induced by } G_\alpha \text{ on } \beta^{G_\alpha} \text{ or by } G_\beta \text{ on } \alpha^{G_\beta} \\ & \text{is not an elementary abelian 2-group of order 4,} \\ 9, & \text{otherwise.} \end{cases}$$

This claim follows from the paragraphs above and from Figure 3. Indeed, from Lemma 2.1 part (c), for each $X \in \mathcal{S}_{\alpha,\beta}$, there exist a proper subgroup A of G_α and a proper subgroup B of G_β with $G_\alpha \cap G_\beta < A$, $G_\alpha \cap G_\beta < B$ and $X = AB$. Observe that we have at most three choices for A and at most three choices for B and hence at most nine choices for X. Moreover, as long as the permutation group induced on the corresponding orbit is not elementary abelian, we actually have only one choice for either A or B yielding at most three choices for X.

For each $X \in \mathcal{S}_{\alpha,\beta}$, let $\mathcal{S}_X := \{\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2} \mid G_\omega = X\}$. From Section 1.1 and from the notation therein, we have $|\mathcal{S}_X| = |\Omega_{\omega,1}| = d$. From this and from the definition of $\mathcal{S}_{\alpha,\beta}$, we obtain

$$|\Omega_{\alpha,2} \cap \Omega_{\beta,2}| = \left| \bigcup_{X \in \mathcal{S}_{\alpha,\beta}} \mathcal{S}_X \right| = \sum_{X \in \mathcal{S}_{\alpha,\beta}} |\mathcal{S}_X| = |\mathcal{S}_{\alpha,\beta}| d. \tag{11}$$

From part (a) of Lemma 2.1, we have $\Omega = \Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$. From this, we immediately get $\Omega_{\beta,2} \subseteq \Omega \setminus \Omega_{\alpha,1} = \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$ and hence $\Omega_{\alpha,2} \cup \Omega_{\beta,2} \subseteq \Omega_{\alpha,2} \cup \Omega_{\alpha,4}$. Therefore,

$$\begin{aligned} |\Omega_{\alpha,2} \cap \Omega_{\beta,2}| &= |\Omega_{\alpha,2}| + |\Omega_{\beta,2}| - |\Omega_{\alpha,2} \cup \Omega_{\beta,2}| \\ &\geq |\Omega_{\alpha,2}| + |\Omega_{\beta,2}| - |\Omega_{\alpha,2} \cup \Omega_{\alpha,4}| \\ &= |\Omega_{\alpha,2}| + |\Omega_{\beta,2}| - |\Omega_{\alpha,2}| - |\Omega_{\alpha,4}| \\ &= |\Omega_{\alpha,2}| - |\Omega_{\alpha,4}|. \end{aligned} \tag{12}$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Now, dividing both sides of (11) and (12) by $|\Omega_{\alpha,1}| = d$, by recalling (4) and by rearranging the terms, we obtain

$$x_2 \leq |\mathcal{S}_{\alpha,\beta}| + x_4. \tag{13}$$

We now suppose that part (a) does not hold and we show that part (bi), (bii), (biii), and (biv) are satisfied. In particular, we work under the assumption that

$$|\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| \geq \frac{5|\Omega|}{6}.$$

As $|\Omega| = d(x_1 + x_2 + x_4)$, $|\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| = d(x_1 + x_2)$ and $x_1 = 1$, the inequality $|\Omega_{\alpha,1}| + |\Omega_{\alpha,2}| \geq 5|\Omega|/6$ gives

$$5x_4 \leq 1 + x_2.$$

Now, (13) yields $5x_4 \leq 1 + x_2 \leq 1 + |\mathcal{S}_{\alpha,\beta}| + x_4$, that is, $4x_4 \leq 1 + |\mathcal{S}_{\alpha,\beta}|$. From (10), we deduce that $x_4 \leq 2$. This already shows part (bi).

When $x_4 = 2$, we deduce $|\mathcal{S}_{\alpha,\beta}| \geq 7$ and hence (10) yields that the permutation groups induced by G_α on β^{G_α} and by G_β on α^{G_β} are both elementary abelian 2-groups of order 4. Since this argument does not depend upon $\beta \in \Omega_{\alpha,4}$, we have shown that G_α acts as an elementary abelian group on each of its orbits of cardinality 4. Since all other orbits of G_α have cardinality 1 or 2, we deduce that G_α acts as an elementary abelian 2-group on each of its orbits and hence G_α is an elementary abelian 2-group. This shows part (bii), under the additional assumption that $x_4 = 2$. Moreover, as $|\mathcal{S}_{\alpha,\beta}| \geq 7$, Lemma 2.3 applied with $X := G_\alpha$ and $Y := G_\beta$ gives that G_α and G_β commute with each other. This shows that part (biii) is satisfied. To prove part (biv), we use Lemma 2.4. Let Γ be the graph having vertex set V, the set of conjugates of G_α in G, that is,

$$V := \{G_\omega \mid \omega \in \Omega\}.$$

Then $|V| = 1 + x_2 + x_4$. We declare two vertices G_{ω_1} and G_{ω_2} of Γ adjacent if $G_{\omega_1} \cap G_{\omega_2}$ has index 4 in G_{ω_1} (and hence also in G_{ω_2}). Clearly, the action of G by conjugation gives rise to a vertex-transitive action of G on Γ. As $x_4 = 2$, Γ has valency 2. Let W be the collection of all vertices G_ω of Γ with $G_\alpha \cap G_\beta \leq G_\omega$. Clearly, $G_\alpha, G_\beta \in W$ and, from Lemma 2.1 part (c), for any two distinct vertices G_{δ_1} and G_{δ_2} of Γ contained in W, we have that

$$\Omega_{\delta_1,2} \cap \Omega_{\delta_2,2} = V \setminus (\Gamma(G_{\delta_1}) \cup \Gamma(G_{\delta_2})) \subseteq W.$$

From this, Lemma 2.4 gives that either $W = V$ or $|V| \leq 6$. The second alternative gives $x_2 = |V| - 1 - x_4 \leq 3$, which contradicts the fact that $5x_4 \leq 1 + x_2$. Therefore, $W = V$ and hence $G_\alpha \cap G_\beta \leq G_\omega$, for every $\omega \in \Omega$. Thus $G_\alpha \cap G_\beta = 1$ and hence $G_\alpha G_\beta = G_\alpha \times G_\beta$ is an elementary abelian 2-group of order 16. To prove that $G_\alpha \times G_\beta \trianglelefteq G$ it suffices to apply again this argument to the collection W of all vertices G_ω of Γ with $G_\omega \leq G_\alpha \times G_\beta$.

In particular, in the rest of the proof we work under the assumption $x_4 = 1$.

When $x_4 = 1$, we may refine some of the inequalities above. Indeed, when $x_4 = 1$, we have $\Omega_{\alpha,4} = \Omega_{\beta,1}$, because both sets have the same cardinality and $\Omega_{\beta,1} \subseteq \Omega_{\alpha,4}$. From this it follows $\Omega_{\alpha,2} = \Omega_{\beta,2}$. Therefore, from (11), we get

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

$$dx_2 = |\Omega_{\alpha,2}| = |\Omega_{\alpha,2} \cap \Omega_{\beta,2}| = d|\mathcal{S}_{\alpha,\beta}|.$$

Now, the inequality $5 = 5x_4 \leq 1 + x_2$ implies $|\mathcal{S}_{\alpha,\beta}| = x_2 \geq 4$. Again, we may use (10) to deduce that the permutation groups induced by G_α on β^{G_α} and by G_β on α^{G_β} are both elementary abelian 2-groups of order 4. This, as above, yields that G_α is an elementary abelian 2-group, that is, part (bii) holds.

From Lemma 2.1 part (c), $G_\alpha \cap G_\beta \leq G_\omega$, for every $\omega \in \Omega_{\alpha,2} \cap \Omega_{\beta,2}$. In particular, $G_\alpha \cap G_\beta$ fixes pointwise $\Omega_{\alpha,2} \cap \Omega_{\beta,2}$. As $\Omega_{\alpha,2} \cap \Omega_{\beta,2} = \Omega_{\alpha,2}$, we deduce that $G_\alpha \cap G_\beta$ fixes pointwise $\Omega_{\alpha,2}$. Since $G_\alpha \cap G_\beta$ fixes pointwise also $\Omega_{\alpha,1}$ and $\Omega_{\beta,1} = \Omega_{\alpha,4}$, we obtain that $G_\alpha \cap G_\beta$ fixes pointwise $\Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4} = \Omega$. Thus $G_\alpha \cap G_\beta = 1$ and $|G_\alpha| = 4$. Observe also that when $x_4 = 1$, the hypothesis of Lemma 2.2 is satisfied and hence $\mathbf{N}_G(G_\alpha) = \mathbf{N}_G(G_\beta)$. Therefore, G_β normalizes G_α. This gives that the commutator subgroup $[G_\alpha, G_\beta]$ lies in $G_\alpha \cap G_\beta = 1$, that is, G_α commutes with G_β. This shows that part (biii) is satisfied. Now, as $\Omega_{\alpha,2} = \Omega_{\beta,2}$, Lemma 2.1 part (c) yields $G_\omega \leq G_\alpha \times G_\beta$, for every $\omega \in \Omega_{\alpha,2}$. Therefore, $G_\alpha \times G_\beta$ contains G_ω, for every $\omega \in \Omega$. Thus,

$$G_\alpha \times G_\beta = \langle G_\omega \mid \omega \in \Omega \rangle \trianglelefteq G,$$

and $G_\alpha \times G_\beta$ has order 16. Thus, part (biv) is satisfied. ∎

We need one final preliminary lemma, with a somehow different flavor. We denote by C_2 and C_4 the cyclic groups of order 2 and 4, respectively, we denote by Q_8 the quaternion group of order 8 and we denote by D_8 the dihedral group of order 4.

Lemma 2.6 *Let R be a finite group, let U be a proper subgroup of R, and let $1 \neq r \in U$ be a central involution of R. Let $\tau : R \to R$ be the permutation defined by*

$$x \mapsto x^\tau := \begin{cases} x, & \text{when } x \in U, \\ xr, & \text{when } x \in R \backslash U. \end{cases}$$

Then one of the following holds:

(a) *The number of inverse-closed subsets S of R with $S^\tau = S$ is at most $2^{\mathbf{c}(R) - \frac{|R|}{48}}$.*
(b) *R is generalized dicyclic.*
(c) *$R \cong C_4 \times C_2^\ell$, for some nonnegative integer ℓ.*

Proof Let $\iota : R \to R$ be the permutation defined by $x^\iota = x^{-1}$, for every $x \in R$, and let

$$T := \langle \iota, \tau \rangle.$$

Observe that $\iota\tau = \tau\iota$ and $\iota^2 = \tau^2 = 1$. Therefore, T is an elementary abelian 2-group of order at most 4.

Now, a subset S of R is inverse-closed and τ-invariant if and only if S is T-invariant. In particular, the number of inverse-closed subsets S of R with $S^\tau = S$ is 2^κ, where κ is the number of orbits of T on R. To compute κ, we use the orbit-counting lemma, which says that

$$\kappa = \frac{1}{|T|} \sum_{t \in T} |\mathrm{Fix}_R(t)|. \tag{14}$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Observe that

$$\begin{aligned}\mathrm{Fix}_R(1) &:= R,\\ \mathrm{Fix}_R(\iota) &:= \mathbf{I}(R),\\ \mathrm{Fix}_R(\tau) &:= U,\\ \mathrm{Fix}_R(\iota\tau) &:= \mathbf{I}(U) \cup \{x \in R\backslash U \mid x^2 = r\}.\end{aligned} \tag{15}$$

Observe that $\tau \neq 1$ because U is a proper subgroup of R and $r \neq 1$. If $\iota = 1$, then R is an elementary abelian 2-group and $T = \langle \tau \rangle$. Thus, (14) and (15) yield

$$\begin{aligned}\kappa &= \frac{1}{2}\left(|R| + |U|\right) \leq \frac{|R|}{2} + \frac{|R|}{4} = \frac{3|R|}{4}\\ &= |R| - \frac{|R|}{4} = \mathbf{c}(R) - \frac{|R|}{4}.\end{aligned}$$

Therefore, part (a) holds and the proof follows in this case. Suppose now $\iota = \tau$. This means that U is an elementary abelian 2-subgroup of R and $x^{-1} = xr$, for every $x \in R\backslash U$. In other words, all elements in U square to 1 and all elements in $R\backslash U$ square to r. Let $\bar{R} := R/\langle r \rangle$ and let us use the "bar" notation for the subgroups and for the elements of $\bar{R}$. Consider the function

$$(\cdot,\cdot) : \bar{R} \times \bar{R} \to \langle r \rangle$$

defined by $(x\langle r \rangle, y\langle r \rangle) = x^{-1}y^{-1}xy$, for every $x, y \in R$. Similarly, consider the function

$$q : \bar{R} \to \langle r \rangle$$

defined by $q(x\langle r \rangle) = x^2$. It is not hard to see that, regarding $\bar{R}$ as a vector space over the field with two elements, $(\cdot,\cdot)$ is a bilinear form and q is a quadratic form polarizing to $(\cdot,\cdot)$, that is,

$$q(\bar{x}\bar{y})q(\bar{x})q(\bar{y}) = (\bar{x},\bar{y}),$$

for every $\bar{x}, \bar{y} \in \bar{R}$. Using this terminology, we have that each element of $\bar{U}$ is totally singular and each element of $\bar{R}\backslash\bar{U}$ is nondegenerate. From the classification of the quadratic forms over finite fields, we have $|\bar{R} : \bar{U}| \in \{2, 4\}$. When $|\bar{R} : \bar{U}| = 2$, we deduce that R is an abelian group isomorphic to the direct product $C_4 \times C_2^\ell$, for some $\ell \geq 0$. In particular, part (c) holds. When $|\bar{R} : \bar{U}| = 4$, we deduce that $R \cong Q_8 \times C_2^\ell$, for some $\ell \geq 0$. In particular, R is generalized dicyclic and part (b) holds. For the rest of our argument, we may suppose that $\tau \neq \iota \neq 1$.

Set $\mathcal{S} := \{x \in R\backslash U \mid x^2 = r\}$. In the present situation, $T = \langle \iota, \tau \rangle$ has order 4 and hence, from (15), (14) becomes

$$\begin{aligned}\kappa &= \frac{1}{4}\left(|\mathrm{Fix}_R(1)| + |\mathrm{Fix}_R(\iota)| + |\mathrm{Fix}_R(\tau)| + |\mathrm{Fix}_R(\tau\iota)|\right)\\ &= \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + |U| + |\mathbf{I}(U)| + |\{x \in R\backslash U \mid x^2 = r\}|\right)\\ &\leq \frac{1}{4}\left(|R| + |\mathbf{I}(R)| + |U| + |\mathbf{I}(R)| + |\mathcal{S}|\right)\\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \left(\frac{|R|}{4} - \frac{|U|}{4} - \frac{|\mathcal{S}|}{4}\right) = \mathbf{c}(R) - \left(\frac{|R|}{4} - \frac{|U|}{4} - \frac{|\mathcal{S}|}{4}\right).\end{aligned} \tag{16}$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

If $\mathcal{S} = \varnothing$, then the proof follows immediately from (16), indeed, part (a) holds true. Therefore, for the rest of the proof, we suppose

$$\mathcal{S} \neq \varnothing.$$

To conclude, we divide the proof in various cases.

Suppose that $|R : U| = 2$. Let $x \in \mathcal{S}$ and observe that $R = U \cup Ux$. Now, a computation yields

$$\mathcal{S} = \{ux \mid u \in U, u^x = u^{-1}\}.$$

When $\mathcal{S} = Ux$, the action of x on U by conjugation is an automorphism of U inverting each element of U. Therefore, U is abelian and R is generalized dicyclic. Hence part (b) holds. When $\mathcal{S} \subsetneq Ux$, the result of Liebeck and MacHale [15] shows that the automorphism x can invert at most $3/4$ of the elements of U and hence $|\mathcal{S}| \leq 3|U|/4 = 3|R|/8$. Now, (16) gives $\kappa \leq \mathbf{c}(R) - |R|/32$; hence, part (a) holds and the proof in this case follows. ∎

Therefore, for the rest of the proof, we may suppose

$$|R : U| \geq 3. \tag{17}$$

Suppose that $|\mathcal{S}| \leq 3|R|/4 - |U|/2$. From (16) and (17), we deduce

$$\begin{aligned}\kappa &\leq \mathbf{c}(R) - \left(\frac{|R|}{4} - \frac{|U|}{4} - \frac{3|R|}{16} + \frac{|U|}{8}\right)\\ &= \mathbf{c}(R) - \left(\frac{|R|}{16} - \frac{|U|}{8}\right)\\ &\leq \mathbf{c}(R) - \left(\frac{|R|}{16} - \frac{|R|}{24}\right) = \mathbf{c}(R) - \frac{|R|}{48}\end{aligned}$$

and the proof in this case follows. ∎

Therefore, for the rest of the proof, we suppose

$$|\mathcal{S}| > 3|R|/4 - |U|/2.$$

To introduce the next case, we first need to make some general observations.

Let u be an arbitrary element of U. Then $u\mathcal{S} \subseteq R \backslash U$ and hence $\mathcal{S} \cup u\mathcal{S} \subseteq R \backslash U$. Therefore,

$$\begin{aligned}|\mathcal{S} \cap u\mathcal{S}| &= |\mathcal{S}| + |u\mathcal{S}| - |\mathcal{S} \cup u\mathcal{S}| = 2|\mathcal{S}| - |\mathcal{S} \cup u\mathcal{S}|\\ &\geq 2|\mathcal{S}| - (|R| - |U|) > \frac{3|R|}{2} - |U| - (|R| - |U|) = \frac{|R|}{2}.\end{aligned} \tag{18}$$

Now, let $ux \in \mathcal{S} \cap u\mathcal{S}$. Then $x \in \mathcal{S}$, and hence

$$r = (ux)^2 = uxux = uu^x x^2 = uu^x r.$$

Therefore, $u^x = u^{-1}$. Now, repeating the argument above with $y \in \mathcal{S} \cap u\mathcal{S}$, we deduce $u^y = u^{-1}$ and hence $xy^{-1} \in \mathbf{C}_R(u)$. Since we have $|\mathcal{S} \cap u\mathcal{S}|$ choices for y, (18) implies $|\mathbf{C}_R(u)| > |R|/2$ and hence $R = \mathbf{C}_R(u)$. Since u is an arbitrary element of U, we deduce that U is a central subgroup of R.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

Since $u^x = u^{-1}$, for every $u \in U$ and for every $ux \in \mathcal{S} \cap u\mathcal{S}$, and since U is contained in the center of R, we deduce that U has exponent 2. Since U is a central subgroup of R of exponent 2, we now have an easier description for $\mathcal{S}$, that is,

$$\mathcal{S} = \{x \in R \mid x^2 = r\}.$$

Now that we know that U has exponent 2, we consider the quotient group $\bar{R} := R/\langle r \rangle$. Observe that each element of $\bar{U}$ is an involution.

Suppose that $\bar{R}$ is not an elementary abelian 2 -group. The theorem of Miller [16] yields $|\mathbf{I}(\bar{R})| \leq 3|\bar{R}|/4$. In particular, the number of involutions in $\bar{R}\backslash\bar{U}$ is at most $3|\bar{R}|/4 - |\bar{U}|$. Since each element in $\bar{\mathcal{S}}$ is an involution and since $\bar{\mathcal{S}} \subseteq \bar{R}\backslash\bar{U}$, we deduce $|\mathcal{S}| \leq 3|R|/4 - |U|$. Using this inequality in (16), we get

$$\kappa \leq \mathbf{c}(R) - \frac{|R|}{16},$$

part (a) holds and the proof follows in this case. It remains to consider the case that $\bar{R}$ is an elementary abelian 2-group.

Suppose that $\bar{R}$ is an elementary abelian 2 -group. Recall that the Frattini subgroup $\Phi(X)$ of a finite group X is the intersection of all the maximal subgroups of X. Recall also that, if X is a p-group for some prime p, then $\Phi(X) = X^p[X, X]$, where $[X, X]$ is the commutator subgroup of X and $X^p := \langle x^p \mid x \in X \rangle$. When $p = 2$, $[X, X] \leq X^2$ because X/X^2 is abelian. Therefore, $\Phi(X) = X^2$.

Since the Frattini subgroup $\Phi(\bar{R})$ of $\bar{R}$ is the identity and since $r \in \Phi(R)$, we deduce $\Phi(R) = \langle r \rangle$. Now, if R is abelian, then from the structure theorem of finitely generated abelian groups, we deduce that R is isomorphic to

(i) $C_4 \times C_2^\ell$ for some $\ell \geq 0$.

If R is non-abelian, then $1 \neq [R, R] \leq \langle r \rangle$ and hence $[R, R] = \Phi(R) = \langle r \rangle$. Now, from [4, Lemmas 4.2 and 4.3 and Remark 1, p. 74], we obtain that $R = E \times A$, where E is an extraspecial 2-group and A is an elementary abelian 2-group. Now, from the structure theorem of extraspecial 2-groups [25, Theorem 4.18(ii)], we deduce that R is isomorphic to one of the following groups:

(ii) $\underbrace{D_8 \circ D_8 \circ \cdots \circ D_8}_{t \text{ times}} \times C_2^\ell$, for some $\ell \geq 0$ and $t \geq 1$.

(iii) $Q_8 \circ \underbrace{D_8 \circ D_8 \circ \cdots \circ D_8}_{(t-1) \text{ times}} \times C_2^\ell$, for some $\ell \geq 0$ and some $t \geq 1$.

(iv) $C_4 \circ \underbrace{D_8 \circ D_8 \circ \cdots \circ D_8}_{t \text{ times}} \times C_2^\ell$, for some $\ell \geq 0$ and some $t \geq 1$.

Therefore, the case that $\bar{R}$ is elementary abelian splits naturally into four cases. To conclude the proof of this lemma, we look at each case in detail.

In Case (i), an explicit computation gives $|\mathcal{S}| = |R|/2$. Hence, (16) gives

$$\begin{aligned}\kappa &\leq \mathbf{c}(R) - \left(\frac{|R|}{4} - \frac{|U|}{4} - \frac{|R|}{8}\right) = \mathbf{c}(R) - \left(\frac{|R|}{8} - \frac{|U|}{4}\right) \\ &\leq \mathbf{c}(R) - \left(\frac{|R|}{8} - \frac{|R|}{16}\right) = \mathbf{c}(R) - \frac{|R|}{16}\end{aligned}$$

and part (a) holds.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

In Case (ii), an explicit computation gives $|\mathcal{S}| = (2^t - 1)|R|/2^{t+1} \leq |R|/2$. Therefore, we may argue as in the previous case and we obtain that part (a) holds.

In Case (iii), an explicit computation gives $|\mathcal{S}| = (2^t + 1)|R|/2^{t+1}$. When $t = 1$, $R \cong Q_8 \times C_2^\ell$ is generalized dicyclic and hence part (b) hods. When $t \geq 2$, we have $|\mathcal{S}| \leq 5|R|/8$ and hence (16) gives

$$\kappa \leq \mathbf{c}(R) - \left(\frac{|R|}{4} - \frac{|U|}{4} - \frac{5|R|}{32}\right) = \mathbf{c}(R) - \left(\frac{3|R|}{32} - \frac{|U|}{4}\right)$$
$$\leq \mathbf{c}(R) - \left(\frac{3|R|}{32} - \frac{|R|}{16}\right) = \mathbf{c}(R) - \frac{|R|}{32}.$$

Thus, we obtain that part (a) holds.

In Case (iv), an explicit computation gives $|\mathcal{S}| = |R|/2$. Therefore, we may argue as in the first case and we obtain that part (a) holds. ∎

3 Proof of Theorems 1.1 and 1.2

In this section, using Section 2, we prove both Theorems 1.1 and 1.2. Thus, let G be a finite transitive permutation group on Ω with

$$\mathbf{I}_\Omega(G) \geq \frac{5}{6}.$$

If $\mathbf{I}_\Omega(G) = 1$, then there is nothing to prove and hence we may suppose that $\mathbf{I}_\Omega(G) < 1$. Let $\alpha \in \Omega$. From Lemma 2.1, we have

$$\Omega = \Omega_{\alpha,1} \cup \Omega_{\alpha,2} \cup \Omega_{\alpha,4}.$$

Since $\mathbf{I}_\Omega(G) < 1$, $\Omega_{\alpha,4} \neq \varnothing$. Let $\beta \in \Omega_{\alpha,4}$. From Lemma 2.5,

$$V := G_\alpha \times G_\beta$$

is an elementary abelian normal 2-subgroup of G of order 16. Let e_1, e_2, e_3, e_4 be a basis of V, regarded as a vector space over the field with two elements, and with $G_\alpha = \langle e_1, e_2\rangle$. Let $H := G/\mathbf{C}_G(V)$ and $W := G_\alpha$. Clearly, $H \leq \mathrm{GL}(V) \cong \mathrm{GL}_4(2)$. Now, consider the action of H on the two-dimensional subspaces of V and consider $O := \{W^h \mid h \in H\}$, the H-orbit containing W. Clearly,

$$\frac{|\Omega_{\alpha,1} \cup \Omega_{\alpha,2}|}{|\Omega|} = \frac{|\{U \in O \mid |W : W \cap U| \leq 2\}|}{|O|}.$$

Observe that the right-hand side of this equality can be easily computed with the help of a computer. With the computer algebra system `magma` [5], we have computed all the subgroups of $\mathrm{GL}_4(2)$. Then, we have selected only the subgroups H with the property that

$$V = \langle W^h \mid h \in H\rangle \text{ and } \bigcap_{h\in H} W^h = 0.$$

(This selection is due to the fact that $V = \langle G_\alpha^g \mid g \in G\rangle$ and that G_α is core-free in G.) Then, for each such subgroup H, we have computed the orbit $O = W^H$ and we have computed the ratio $\frac{|\{U\in O||W:W\cap U|\leq 2\}|}{|O|}$. We have checked that in all cases, this ratio is

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

at most 5/6. In particular, Theorem 1.1 is proved. Moreover, we have checked that this ratio is 5/6 if and only if H is given in the statement of Theorem 1.2. (We are including in the Appendix, the code required to perform this computation with the computer algebra system `magma`.) Since this construction can be reversed, we also obtain the converse implication for Theorem 1.2.

4 Proof of Theorem 1.9

Let G be a finite transitive group properly containing a regular subgroup R. Since R acts regularly, we may identify the domain of G with R. Now, the number of Cayley graphs $\Gamma(R,S)$ on R with $G \leq \mathrm{Aut}(\Gamma(R,S))$ is the number of inverse-closed subsets S of R left invariant by G_1, where G_1 is the stabilizer of the point $1 \in R$ in G. In particular, to prove Theorem 1.9, we need to estimate the number of inverse-closed subsets of R that are union of G_1-orbits.

Suppose first that

$$\mathbf{I}_R(G) = 1.$$

Since R is properly contained in G, from the theorem of Bergman and Lenstra mentioned in Section 1, we have two cases to consider:

- $|G_1| = 2$.
- G contains an elementary abelian normal 2-subgroup N with $|N : G_1| = 2$.

Assume first that $|G_1| = 2$. Let $\varphi \in G_1 \backslash \{1\}$. From the Frattini argument, $G = RG_1$ and hence $|G : R| = 2$. This gives $R \trianglelefteq G$ and hence φ acts by conjugation on R as a group automorphism. Now, from [24, Lemma 2.7] or [17, Theorem 1.13], we have that:

(a) The number of φ-invariant inverse-closed subsets of R is at most $2^{\mathfrak{c}(R)-\frac{|R|}{96}}$, or
(b) R is abelian of exponent greater than 2 and φ is the automorphism of R mapping each element to its inverse, or
(c) R is generalized dicyclic and φ is an automorphism of R with $x^\varphi \in \{x, x^{-1}\}$, for every $x \in R$.

In particular, the proof of Theorem 1.9 follows in this case.

Assume next that G contains an elementary abelian normal 2-subgroup N with $|N : G_1| = 2$. Since R acts transitively, $G = RN$. Moreover, since R acts regularly, $G = RG_1$ and $R \cap G_1 = 1$. Thus $|R \cap N| = |N|/|G_1| = 2$. Let r be a generator of $R \cap N$. Since $\langle r \rangle = R \cap N \trianglelefteq R$, r is a central involution of R. Let $U := \mathbf{N}_R(G_1)$. Since $\mathbf{N}_R(G_1)$ is a block of imprimitivity for G, $U = \mathbf{N}_R(G_1)$ is also a block of imprimitivity for the regular action of R and hence U is a subgroup of R. As $G_1 \neq 1$ because R is properly contained in G, we deduce that U is a proper subgroup of R. Now, G_1 fixes pointwise U and, for every $x \in R \backslash U$, we have

$$x^{G_1} = \{x, xr\}.$$

Let $\tau : R \to R$ be the permutation defined by

$$x \mapsto x^\tau := \begin{cases} x, & \text{when } x \in U, \\ xr, & \text{when } x \in R \backslash U. \end{cases}$$

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

We have shown that $S \subseteq R$ is G_1-invariant if and only if S is $\langle \tau \rangle$-invariant. Therefore, the proof of this case follows from Lemma 2.6.

To conclude the proof of Theorem 1.9, it remains to consider the case that

$$\mathbf{I}_R(G) \neq 1.$$

From Theorem 1.1, we have $\mathbf{I}_R(G) \leq 5/6$. Recall that $\mathbf{I}(R) = \{x \in R \mid x^2 = 1\}$. We define

$$\begin{aligned} a &:= |\Omega_{R,1} \cap \mathbf{I}(R)|, & b &:= |\Omega_{R,1} \cap (R \backslash \mathbf{I}(R))|, \\ c &:= |\Omega_{R,2} \cap \mathbf{I}(R)|, & d &:= |\Omega_{R,2} \cap (R \backslash \mathbf{I}(R))|, \\ e &:= |(R \backslash (\Omega_{R,1} \cup \Omega_{R,2})) \cap \mathbf{I}(R)|, & f &:= |(R \backslash (\Omega_{R,1} \cup \Omega_{R,2})) \cap (R \backslash \mathbf{I}(R))|. \end{aligned}$$

As $\mathbf{I}_R(G) \leq 5/6$, we deduce

$$\frac{|R|}{6} \leq |R \backslash (\Omega_{R,1} \cup \Omega_{R,2})| = e + f. \tag{19}$$

Let $\iota : R \to R$ be the permutation defined by $x^\iota := x^{-1}$, for every $x \in R$, and let $T := \langle \iota, G_1 \rangle$. Now, the number of G_1-invariant inverse-closed subsets of R is exactly the number of T-invariant subsets of R. Moreover, the number of T-invariant subsets of R is 2^κ, where κ is the number of orbits of T on R.

The group T has:

- Orbits of cardinality 1 on $\Omega_{R,1} \cap \mathbf{I}(R)$.
- Orbits of cardinality 2 on $\Omega_{R,1} \cap (R \backslash \mathbf{I}(R))$.
- Orbits of cardinality 2 on $\Omega_{R,2} \cap \mathbf{I}(R)$.
- Orbits of cardinality at least 2 on $\Omega_{R,2} \cap (R \backslash \mathbf{I}(R))$.
- Orbits of cardinality at least 3 on $(R \backslash (\Omega_{R,1} \cup \Omega_{R,2})) \cap \mathbf{I}(R)$.
- Orbits of cardinality at least 4 on $(R \backslash (\Omega_{R,1} \cup \Omega_{R,2})) \cap (R \backslash \mathbf{I}(R))$.

All of these assertions are trivial except, possibly, the last one. Indeed, if $x \in (R \backslash (\Omega_{R,1} \cup \Omega_{R,2})) \cap (R \backslash \mathbf{I}(R))$, then x is not an involution and the G_1-orbit x^{G_1} has cardinality at least 3. As

$$(x^{G_1})^{-1} = (x^{-1})^{G_1},$$

we deduce that $|x^T|$ has even cardinality and hence $|x^T|$ is at least 4.

Summing up, we have

$$\begin{aligned} \kappa &\leq a + \frac{b}{2} + \frac{c}{2} + \frac{d}{2} + \frac{e}{3} + \frac{f}{4} = a + c + e + \frac{b}{2} + \frac{d}{2} + \frac{f}{2} - \left(\frac{c}{2} + \frac{2e}{3} + \frac{f}{4} \right) \\ &= \frac{|R| + |\mathbf{I}(R)|}{2} - \left(\frac{c}{2} + \frac{2e}{3} + \frac{f}{4} \right) = \mathbf{c}(R) - \left(\frac{c}{2} + \frac{2e}{3} + \frac{f}{4} \right) \\ &\leq \mathbf{c}(R) - \left(\frac{2e}{3} + \frac{f}{4} \right) \leq \mathbf{c}(R) - \left(\frac{e}{4} + \frac{f}{4} \right) \\ &\leq \mathbf{c}(R) - \frac{|R|}{24}, \end{aligned}$$

where in the last inequality we have used (19). This concludes the proof of Theorem 1.9.

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

A Appendix

We report here the code used in the last paragraph of the proof of Theorem 1.2. We have performed the computations in the computer algebra system magma, and hence we present the code in this language. The code runs just under 4 minutes in the author's personal laptop.

```
G:=GL(4,2); /*we construct  the group GL(4,2)*/
Sub:=Subgroups(G); /*We construct the subgroups of G*/
V:=VectorSpace(GF(2),4); /*We construct the natural
                           G-module*/
W:=sub<V|V.1,V.2>; /*W is the subspace of V spanned by
                           the first two basis vectors*/
K:=Stabilizer(G,W); /*K is the stabilizer of W in G*/
/*we save in Subb, the elements H of Sub with
V=<W^h\mid h\in H>  and 0=\cap_{h\in H}W^h*/
Subb:={};
for h in Sub do
 H0:=h`subgroup;
 for g in Transversal(G,Normalizer(G,H0)) do
   H:=H0^g;
   if V eq sub<V|[W^h:h in H]> and
        #(&meet[W^h:h in H]) eq 1 then
     Include(~Subb,H);
   end if;
 end for;
end for;


/*for each H in Subb, we compute the orbit O:=W^H; then,
we compute and save in Subbb the ratio
|\{U\in O\mid |W:W\cap U|\le 2\}|/|O| and we save in
SubbbSpecial the groups H where this ratio is 5/6*/
Subbb:={};
SubbbSpecial:={};
for H in Subb do
  O:={W^h:h in H};
  sz:=#{U:U in O|(#W div #(W meet U)) le 2}/#O;
  Include(~Subbb,sz);
  if sz eq 5/6 then Include(~SubbbSpecial,H);end if;
end for;

Maximum(Subbb); /*the output is 5/6*/

/*H1 and H2 are the groups introduced in the statement
of Theorem 1.2*/
H1:=sub<G|G![0,0,0,1,1,1,0,0,0,0,1,0,1,0,0,1],
          G![1,1,1,1,0,0,1,0,0,1,0,0,0,0,0,1]>;
H2:=sub<G|G![0,0,0,1,1,1,0,0,0,0,1,0,1,0,0,1],
          G![1,1,1,1,0,0,1,0,0,1,0,0,0,0,0,1],
          G![1,0,0,0,0,1,0,0,1,1,0,1,1,1,1,0]>;
```

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press

```
/*we check that elements in SubbbSpecial are K-conjugate
to H1 or H2. The output is yes*/

SubbbSpecial eq ({H1^k:k in K} join {H2^k:k in K});
```

References

[1] L. Babai, *Finite digraphs with given regular automorphism groups*. Period. Math. Hungar. **11**(1980), 257–270.
[2] L. Babai and C. D. Godsil, *On the automorphism groups of almost all Cayley graphs*. European J. Combin. **3**(1982), 9–15.
[3] G. M. Bergman and H. W. Lenstra Jr, *Subgroups close to normal subgroups*. J. Algebra **127**(1989), 80–97.
[4] Y. Berkovich, *Groups of prime power order*. *Vol. I*, de Gruyter Expositions in Mathematics, 46, de Gruyter, Berlin, 2008.
[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*. J. Symb. Comput. **24**(1997), nos. 3–4, 235–265.
[6] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.
[7] P. Fitzpatrick, *Groups in which an automorphism inverts precisely half the elements*. Math. Proc. R. Ir. Acad. **86**(1986), 81–89.
[8] C. D. Godsil, *On the full automorphism group of a graph*. Combinatorica **1**(1981), 243–256.
[9] C. D. Godsil, *GRRs for nonsolvable groups*. In: Algebraic methods in graph theory (Szeged, 1978), Colloquia Mathematica Societatis János Bolyai, 25, North-Holland, Amsterdam–New York, 1981, pp. 221–239.
[10] P. Hegarty and D. MacHale, *Two-groups in which an automorphism inverts precisely half the elements*. Bull. Lond. Math. Soc. **30**(1998), 129–135.
[11] D. Hetzel, *Über reguläre graphische Darstellung von auflösbaren Gruppen*, Technische Universität, Berlin, 1976.
[12] W. Imrich, *Graphen mit transitiver Automorphismengruppen*. Monatsh. Math. **73**(1969), 341–347.
[13] W. Imrich, *On graphs with regular groups*. J. Combin. Theory Ser. B **19**(1975), 174–180.
[14] I. M. Isaacs, *Subgroups close to all of their conjugates*. Arch. Math. **55**(1990), 1–4.
[15] H. Liebeck and D. MacHale, *Groups with automorphisms inverting most elements*. Math. Z. **124**(1972), 51–63.
[16] G. A. Miller, *Groups containing the largest possible number of operators of order two*. Amer. Math. Monthly **12**(1905), 149–151.
[17] J. Morris, M. Moscatiello, and P. Spiga, *Asymptotic enumeration of Cayley graphs*. Ann. Mat. Pura Appl. **201**(2022), 1417–1461.
[18] J. Morris and P. Spiga, *Asymptotic enumeration of Cayley digraphs*. Israel J. Math. **242**(2021), 401–459.
[19] J. Morris, P. Spiga, and G. Verret, *Automorphisms of Cayley graphs on generalised dicyclic groups*. European J. Combin. **43**(2015), 68–81.
[20] M. Muzychuk and P. H. Zieschang, *On association schemes all elements of which have valency* 1 *or* 2. Discrete Math. **308**(2008), 3097–3103.
[21] L. A. Notwitz and M. Watkins, *Graphical regular representations of non-abelian groups, I*. Canad. J. Math. **24**(1972), 993–1008.
[22] L. A. Nowitz and M. Watkins, *Graphical regular representations of direct product of groups*. Monatsh. Math. **76**(1972), 168–171.
[23] L. A. Nowitz and M. Watkins, *Graphical regular representations of non-abelian groups, II*. Canad. J. Math. **24**(1972), 1009–1018.
[24] P. Spiga, *On the equivalence between a conjecture of Babai–Godsil and a conjecture of Xu concerning the enumeration of Cayley graphs*. Art Discrete Appl. Math. **4**(2021). https://doi.org/10.26493/2590-9770.1338.0b2s
[25] M. Suzuki, *Group theory II*, Springer, New York, 1986.

[26] C. T. C. Wall, *On groups consisting mostly of involutions*. Math. Proc. Cambridge Philos. Soc. **67**(1970), 251–262.
[27] M. E. Watkins, *On the action of non-abelian groups on graphs*. J. Combin. Theory Ser. B **11**(1971), 95–104.

Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca, Via Cozzi 55, 20162 Milan, Italy
e-mail: pablo.spiga@unimib.it

https://doi.org/10.4153/S0008414X23000093 Published online by Cambridge University Press