

ASYMPTOTIC ENUMERATION OF HAAR GRAPHICAL REPRESENTATIONS

YUNSONG GAN, PABLO SPIGA, AND BINZHOU XIA

ABSTRACT. This paper represents a significant leap forward in the problem of enumerating vertex-transitive graphs. Recent breakthroughs on symmetry of Cayley (di)graphs show that almost all finite Cayley (di)graphs have the smallest possible automorphism group. Extending the scope of these results, we enumerate (di)graphs admitting a fixed semiregular group of automorphisms with m orbits. Moreover, we consider the more intricate inquiry of prohibiting arcs within each orbit, where the special case $m = 2$ is known as the problem of finding Haar graphical representations (HGRs). We significantly advance the understanding of HGRs by proving that the proportion of HGRs among Haar graphs of a finite nonabelian group approaches 1 as the group order grows. As a corollary, we obtain an improved bound on the proportion of DRRs among Cayley digraphs in the solution of Morris and the second author to the Babai-Godsil conjecture.

Key words: Haar graph; Cayley graph; automorphism groups; asymptotic enumeration
MSC2020: 20B25, 05E18, 05C30

1. INTRODUCTION

A *Haar graph* of a group G is a bipartite graph whose automorphism group has a subgroup isomorphic to G that is semiregular on the vertex set with orbits giving a bipartition. For such a graph, we may identify the vertex set with $G \times \{1, 2\}$ such that the parts of the bipartition are $G \times \{1\}$ and $G \times \{2\}$. Therefore, every Haar graph of G can be determined uniquely by a subset S of G such that $(g, 1)$ and $(h, 2)$ are adjacent if and only if $hg^{-1} \in S$. We denote this Haar graph by $H(G, S)$. Introduced initially in [20], Haar graphs have been studied extensively by several authors from different viewpoints [5, 7, 11, 13, 14, 15, 24].

A Haar graph of G is called a *Haar graphical representation* (HGR), if its automorphism group is isomorphic to G . When G is abelian, an easy observation (see Definition 2.3) shows that, for each Haar graph of G , there exists an automorphism ι of order two such that the group $G \rtimes \langle \iota \rangle$ acts regularly on the vertex set, transforming each Haar graph into a Cayley graph. Hence no Haar graph of an abelian group is an HGR. It is then natural to ask: Which groups permit HGRs? In fact, this problem has been posed for finite groups in relevant research, for example [11, 14]. Recently, Morris and the second author [37] have classified finite groups admitting an HGR. They proved that, except for abelian groups and 22 small groups, every finite group admits an HGR. This leads to the following problem.

Problem 1.1. *For a finite nonabelian group G , count the HGRs of G .*

The first result of this paper addresses Problem 1.1 by giving an upper bound on the number of subsets S of a nonabelian group G such that $H(G, S)$ is not an HGR. For completeness, we also establish a similar result for abelian groups G such that the automorphism group of $H(G, S)$ is not isomorphic to $G \rtimes \langle \iota \rangle$.

Theorem 1.2. *Let $\varepsilon \in (0, 0.1]$, and let n_ε be a positive integer such that for all $n \geq n_\varepsilon$,*

$$(6 + 2 \log_2 n)(n^{0.5-\varepsilon} + \log_2 n)^2 + (1 - \log_2 n)(n^{0.5-\varepsilon} + \log_2 n) + \log_2^2 n + 2 \log_2 n < n^{1-\varepsilon}. \quad (1)$$

Let G be a finite group of order n , and let $f_\varepsilon(n) = \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} - \frac{3 \log_2^2 n}{4} - 15$.

- (a) If G is nonabelian, then the number of subsets S of G such that $H(G, S)$ is not an HGR is less than $2^{n-f_\varepsilon(n)}$.
- (b) If G is abelian, then the number of subsets S of G such that the automorphism group of $H(G, S)$ is not isomorphic to $G \rtimes \langle \iota \rangle$ is less than $2^{n-f_\varepsilon(n)-1}$.

Fix some $\varepsilon \in (0, 0.1]$. Note that the left-hand side of (1) is approximately $2 \log_2 n \cdot n^{1-2\varepsilon}$, which is smaller than $n^{1-\varepsilon}$ for sufficiently large n . Hence there exists an integer n_ε such that (1) holds for all $n \geq n_\varepsilon$. Since a group of order n has exactly 2^n subsets, Theorem 1.2(a) yields that, for a nonabelian group G of order n satisfying (1), the proportion of subsets S of G such that $H(G, S)$ is an HGR is larger than

$$1 - 2^{-\frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15}. \quad (2)$$

Since (2) approaches 1 as n tends to infinity, this reveals that almost all Haar graphs of a finite nonabelian group are HGRs. Similarly, Theorem 1.2(b) implies that almost all Haar graphs of a finite abelian group have automorphism group isomorphic to $G \rtimes \langle \iota \rangle$.

We remark that the graphs in Theorem 1.2 are labelled. For comparison, we offer an unlabelled version as follows.

Theorem 1.3. *Let $\varepsilon \in (0, 0.1]$, and let n_ε be a positive integer such that (1) holds for all $n \geq n_\varepsilon$.*

Let G be a finite group of order n , and let $h_\varepsilon(n) = \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} - \log_2^2(2n) - \frac{3 \log_2^2 n}{4} - 2 \log_2 n - 15$.

- (a) *If G is nonabelian, then the proportion of HGRs of G among Haar graphs of G , up to isomorphism, is greater than $1 - 2^{-h_\varepsilon(n)}$.*
- (b) *If G is abelian, then the proportion of Haar graphs of G whose automorphism group is isomorphic to $G \rtimes \langle \iota \rangle$, among Haar graphs of G , up to isomorphism, is greater than $1 - 2^{-h_\varepsilon(n)}$.*

We now discuss the roots of Theorem 1.2 and present other results. The study of groups represented as the automorphism groups of (di)graphs of the same order commences with classical problems known as DRR and GRR problems. Let G be a finite group and S a subset of G . A *Cayley digraph* $\text{Cay}(G, S)$ of G with *connection set* $S \subseteq G$ is a digraph with vertex set G such that (g, h) is an arc if and only if $hg^{-1} \in S$. A Cayley digraph $\text{Cay}(G, S)$ is a graph if and only if S is inverse-closed. We call a Cayley (di)graph of G a *(di)graphical regular representation*, or GRR (DRR) for short, if its automorphism group is isomorphic to G .

A natural problem is to determine which finite groups admit a DRR or GRR. In 1980, Babai [2] proved that C_2^2 , C_3^3 , C_2^4 , C_3^2 and Q_8 are the only groups without DRRs. Based on a series of partial results (see [21, 39], for example), the problem for GRRs was eventually solved by Godsil [18] in 1981: Apart from abelian groups of exponent greater than 2, generalized dicyclic groups (see Section 7.2 for definition), and 13 small solvable groups, every finite group admits a GRR. Following this, Babai and Godsil [3, 18] conjectured in early 1980s that almost all finite Cayley digraphs are DRRs. This conjecture was confirmed by Morris and the second author by showing the following theorem in [36].

Theorem 1.4 (Morris-Spiga). *Let G be a finite group of order n . When n is sufficiently large, the proportion of subsets S of G such that $\text{Cay}(G, S)$ is not a DRR is at most $2^{-\frac{bn^{0.499}}{41 \log_2^3 n} + 2}$, where b is an absolute constant.*

We illustrate a connection between Theorem 1.4 and Theorem 1.2. Let Γ be a digraph with vertex set V . The *standard double cover* $D(\Gamma)$ of Γ is the graph with vertex set $V \times \{1, 2\}$ and edge set $\{(g, 1), (h, 2)\} \mid (g, h) \text{ is an arc of } \Gamma\}$. Observe that the automorphism group of Γ also acts as a group of automorphisms of $D(\Gamma)$ that stabilizes both of $V \times \{1\}$ and $V \times \{2\}$ (see [17, Section 3.1]), and that the Haar graph $H(G, S)$ is precisely the standard double cover

$D(\text{Cay}(G, S))$. This implies that, if all the automorphisms of $H(G, S)$ that stabilizes both of the biparts constitute solely the group G , then $\text{Cay}(G, S)$ is a DRR. Therefore, Theorem 1.2 leads to the following stronger assertion than Theorem 1.4 regarding the Babai-Godsil conjecture.

Corollary 1.5. *For each $\varepsilon \in (0, 0.1]$, there exists $n_\varepsilon > 0$ such that for a finite group G of order $n \geq n_\varepsilon$, the proportion of subsets S of G with $\text{Cay}(G, S)$ not a DRR is less than $2^{-n^{0.5-\varepsilon}}$.*

For the proportion of GRRs among Cayley graphs, Babai, Godsil, Imrich and Lovász conjectured that, except for the groups G that are abelian of exponent greater than 2 or generalised dicyclic, almost all finite Cayley graphs of G are GRRs [3, Conjecture 2.1]. This was recently confirmed by the third author and Zheng [46], following the framework developed in [35, 44].

Theorem 1.6 (Xia-Zheng). *Let G be a finite group of order n such that G is neither abelian of exponent greater than 2 nor generalized dicyclic. When n is sufficiently large, the proportion of inverse-closed subsets S of G such that $\text{Cay}(G, S)$ is not a GRR is at most $2^{-\frac{n^{0.499}}{8 \log_2^3 n} + \log_2^2 n + 3}$.*

It is evident that a digraph constitutes a Cayley digraph of G if and only if its automorphism group contains a regular subgroup isomorphic to G . Thus, the essence of Theorems 1.4 and 1.6 lies in the observation that, except for two special families outlined in Theorem 1.6, nearly all (di)graphs possessing a regular group of automorphisms exhibit automorphism groups that are “as small as possible”. This leads us to the following question: What about (di)graphs endowed with a semiregular group of automorphisms?

Let G be a finite group. A digraph is termed an m -Cayley digraph of G if it admits a group G of automorphisms acting semiregularly on the vertex set, featuring precisely m orbits. Similarly, for each m -Cayley digraph of G , we can identify the m orbits of G with m copies of G and employ a set-matrix \mathcal{S} of G to delineate the arcs between them. Consequently, an m -Cayley digraph of G can be conceptualized in terms of G along with a set-matrix \mathcal{S} of G (see Section 2.1), denoted by $\text{Cay}(G, \mathcal{S})$. A digraph $\text{Cay}(G, \mathcal{S})$ is a graph if and only if \mathcal{S} is inverse-closed, as defined in Definition 2.1.

An m -Cayley (di)graph of a finite group G is called a *(di)graphical m -semiregular representation*, abbreviated as $GmSR$ ($DmSR$), if its automorphism group is isomorphic to G . In their work [10], Du, Feng, and the second author demonstrated that every group of order greater than 8 possesses a $GmSR$ and $DmSR$ for each $m \geq 2$. This naturally leads to the question: For a finite group G of sufficiently large order, are almost all m -Cayley (di)graphs of G $GmSR$ s ($DmSR$ s)? We provide an affirmative answer to this question by proving the following theorem.

Theorem 1.7. *Fix an integer $m \geq 2$, and let G be a finite group of order n . When n is sufficiently large, the proportion of (inverse-closed) set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is a $DmSR$ ($GmSR$) is greater than $1 - m^2/\sqrt{n}$.*

To provide further background of Theorem 1.7, it is worth remarking the relationship between Cayley (di)graphs, vertex-transitive (di)graphs, and m -Cayley (di)graphs. Let \mathcal{V} and \mathcal{C}_m be the set of vertex-transitive (di)graphs and m -Cayley (di)graphs, respectively. It is clear that $\mathcal{C}_1 \subseteq \mathcal{V}$. However, determining $\mathcal{V} \setminus \mathcal{C}_1$ is difficult, and the famous McKay-Praeger conjecture [34] states that $|\mathcal{C}_1|/|\mathcal{V}|$ approaches 1 as the (di)graph order grows. Another related fascinating long-standing problem is the so-called *Polycirculant conjecture* [33], which asserts that

$$\mathcal{C}_1 \subseteq \mathcal{V} \subseteq \bigcup_{m \geq 1} \mathcal{C}_m. \quad (3)$$

We refer the reader to [1] for a survey of this conjecture. Given that the McKay-Praeger conjecture predicts the first inclusion in (3) to be asymptotically tight, one might be interested in whether the second inclusion is tight. In this sense, Theorem 1.7 gives negative evidence by indicating that $\mathcal{V} \cap \mathcal{C}_m$ is extremely small relative to \mathcal{C}_m for each $m \geq 2$.

The validity of Theorem 1.7 relies significantly on the presence of arcs within each G -orbit in most m -Cayley (di)graphs of G . Indeed, a crucial step in establishing Theorem 1.7 is to utilize Theorem 1.6 (Theorem 1.4) to assert that the induced sub(di)graph of a G -orbit typically conforms to a GRR (DRR) structure. Establishing an analog of Theorem 1.7 becomes notably more challenging if arcs within each G -orbit are prohibited. Even for $m = 2$, corresponding to the examination of HGRs, Theorem 1.2 stands as the inaugural result enumerating them. The last main result of this paper is to provide an asymptotic result for the general case.

An m -Cayley graph $\text{Cay}(G, \mathcal{S})$ is m -partite with G -orbits as the m parts if and only if the diagonal entries of \mathcal{S} are empty sets. Such a set-matrix \mathcal{S} is said to be *skew* (see Definition 2.1). An m -Cayley graph $\text{Cay}(G, \mathcal{S})$ with skew \mathcal{S} is called an *m -partite graphical semiregular representation* (m -PGSR) of G , if its automorphism group is isomorphic to G . Notably, 2-PGSRs are equivalent to HGRs. Similar to the asymptotic result in Theorem 1.2 for HGRs, the following theorem demonstrates that the majority of skew set-matrices \mathcal{S} make $\text{Cay}(G, \mathcal{S})$ an m -PGSR.

Theorem 1.8. *Fix an integer $m \geq 3$, and let G be a finite group of order n . When n is sufficiently large, the proportion of skew set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is an m -PGSR is greater than $1 - m^2/\sqrt{n}$.*

The subsequent sections of this paper unfold as follows. In the next section, we introduce some notations and preliminary results. Following that, Section 3 outlines the strategy employed to prove Theorem 1.2 and streamlines the proof to the enumeration of primitive groups harboring a “large” regular subgroup. This enumeration is carried out in Section 4, facilitating the culmination of the proof for Theorems 1.2 and 1.3 in Section 5. The proof of Theorem 1.7, divided into the cases of digraphs and graphs, is presented towards the conclusion of Sections 6 and 7, respectively. We establish Theorem 1.8 in Section 8.

2. PRELIMINARIES

For a graph Γ , we use $V(\Gamma)$ to denote its vertex set, and for a vertex u of Γ , we use $N_\Gamma(u)$ to denote the neighbourhood of u in Γ . For a finite group X , denote by $P(X)$ the minimal index of proper subgroups of X , and by $\text{Soc}(X)$ the socle (product of the minimal normal subgroups) of X . For a permutation α of a set Ω , denote by $\text{Fix}(\alpha)$ the set of elements in Ω fixed by α .

2.1. m -Cayley (di)graphs. Let m be a positive integer. In Introduction, an m -Cayley digraph of a group G is defined as a digraph whose automorphism group has a subgroup isomorphic to G that is semiregular on the vertex set with exactly m orbits. Now we give an equivalent definition of m -Cayley (di)graphs. Let

$$\mathcal{S} = (S_{i,j})_{m \times m} = \begin{pmatrix} S_{1,1} & S_{1,2} & \cdots & S_{1,m} \\ S_{2,1} & S_{2,2} & \cdots & S_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ S_{m,1} & S_{m,2} & \cdots & S_{m,m} \end{pmatrix}$$

be a *set-matrix* of G , namely, a matrix whose entries are subsets of G . The *m -Cayley digraph* $\text{Cay}(G, \mathcal{S})$ of G with respect to \mathcal{S} is the digraph with vertex set $G \times \{1, \dots, m\}$ and arc set

$$\bigcup_{i,j \in \{1, \dots, m\}} \{((g, i), (sg, j)) \mid s \in S_{i,j}, g \in G\}.$$

Definition 2.1. We call a set-matrix \mathcal{S} *inverse-closed* if $S_{j,i} = S_{i,j}^{-1}$ for all $i, j \in \{1, \dots, m\}$. For such \mathcal{S} , we call the digraph $\text{Cay}(G, \mathcal{S})$ an *m -Cayley graph* as it is undirected. If a set-matrix \mathcal{S} is inverse-closed and satisfies $S_{i,i} = \emptyset$ for each $i \in \{1, \dots, m\}$, then \mathcal{S} is said to be *skew*.

It is clear that each element x of G induces an automorphism $R(x)$ of m -Cayley digraphs of G by mapping (g, i) to (gx, i) for each $g \in G$ and $i \in \{1, \dots, m\}$. In this way, $R(G)$ is a

semiregular subgroup of $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ with orbits $G \times \{1\}, \dots, G \times \{m\}$. For simplicity of notation, we identify $R(G)$ with G and $R(x)$ with x for each $x \in G$ when there is no confusion.

If a (di)graph has a group G of automorphisms acting semiregularly on the vertex set with exactly m orbits, then it is isomorphic to some m -Cayley (di)graph of G . Hence the two definitions of m -Cayley (di)graphs from Introduction and this section are equivalent.

2.2. Haar graphs and odd-quotient graphs. For convenient, we adopt the following notations about Haar graphs in the rest of this paper.

Notation 2.2. Let G be a finite group. Then each Haar graph Γ of G has vertex set $G \times \{1, 2\}$. For each $g \in G$, denote $g_+ = (g, 1)$ and $g_- = (g, 2)$. For $S \subseteq G$ and $\epsilon \in \{+, -\}$, denote $S_\epsilon = \{s_\epsilon \mid s \in S\}$. In particular, $G_+ = G \times \{1\}$ and $G_- = G \times \{2\}$. Let $\text{Aut}^+(\Gamma)$ be the subgroup of $\text{Aut}(\Gamma)$ fixing setwise G_+ and G_- .

The next definition reveals that each Haar graph of an abelian group has an automorphism that exchanges the parts G_+ and G_- .

Definition 2.3. Let G be an abelian group, and let ι be the permutation on $G_+ \cup G_-$ which maps g_ϵ to $(g^{-1})_{-\epsilon}$ for each $g \in G$ and $\epsilon \in \{+, -\}$. It is easy to check that, ι is a graph automorphism of each Haar graph of G and normalizes the semiregular group $R(G)$ (via the right multiplication action on $G_+ \cup G_-$). Hence each Haar graph of G has a group of automorphisms isomorphic to $G \rtimes \langle \iota \rangle$. In particular, each Haar graph of an abelian group is a Cayley graph.

The following concept, as defined in [36, Definition 6.1], is used in the proof of Theorem 1.2.

Definition 2.4. Let Γ be a graph, and let \mathcal{B} be a partition of $V(\Gamma)$ such that for any fixed $B, C \in \mathcal{B}$, all vertices in B have the same number of neighbours, denoted by $e(B, C)$, in C . The *odd-quotient digraph* $\Gamma_{\mathcal{B}}^{\text{odd}}$ of Γ with respect to \mathcal{B} is the digraph with vertex set \mathcal{B} such that B is adjacent to C if and only if $e(B, C)$ is odd. If \mathcal{B} is the orbit partition of some group $H \leq \text{Aut}(\Gamma)$, we write $\Gamma_{\mathcal{B}}^{\text{odd}}$ as Γ_H^{odd} .

In the above definition, if $|B| = |C|$, then a double-counting of the edges between B and C shows that $e(B, C) = e(C, B)$. This leads to the following remark.

Remark 2.5. In Definition 2.4, if all the sets in \mathcal{B} have the same size, then $\Gamma_{\mathcal{B}}^{\text{odd}}$ is undirected.

2.3. Simple arithmetic results. For a subset S of a group, let $\mathcal{I}(S)$ be the set of elements in S of order at most 2, and let

$$c(S) = \frac{|S| + |\mathcal{I}(S)|}{2}.$$

The proof of the following lemma is straightforward (see [43, Lemma 2.2], for example).

Lemma 2.6. *Let S be an inverse-closed subset of a finite group. Then the number of inverse-closed subsets of S is $2^{c(S)}$.*

We also require the following two useful lemmas, where the proof of the first is elementary and hence omitted.

Lemma 2.7. *For a non-empty set, the number of subsets of odd size equals the number of subsets of even size.*

Lemma 2.8. *For a set of size n , the number of its subsets with a given size is at most $2^n / \sqrt{n}$.*

Proof. Clearly, the lemma holds true for $n = 1$, and so we assume $n \geq 2$. According to Stirling's formula (see [42]), for any positive integer x , the factorial $x!$ satisfies

$$\sqrt{2\pi x} \left(\frac{x}{e}\right)^x < x! < \sqrt{2\pi x} \left(\frac{x}{e}\right)^x e^{\frac{1}{12x}}.$$

Hence,

$$\binom{2x}{x} = \frac{(2x)!}{x! \cdot x!} < e^{\frac{1}{24x}} \frac{\sqrt{4\pi x} \cdot (2x)^{2x}}{(\sqrt{2\pi x} \cdot x^x)^2} = \frac{e^{\frac{1}{24x}}}{\sqrt{\pi}} \cdot \frac{2^{2x}}{\sqrt{x}} < \frac{2^{2x}}{\sqrt{2x}}.$$

Note that the maximum binomial coefficient in $\binom{n}{0}, \dots, \binom{n}{n}$ is $\binom{n}{\lfloor n/2 \rfloor}$. If n is even, the conclusion immediately follows from the above inequality by taking $2x$ as n . If n is odd, we also obtain

$$\binom{n}{\lfloor n/2 \rfloor} = \frac{n}{(n+1)/2} \binom{n-1}{(n-1)/2} < \frac{2n}{n+1} \cdot \frac{2^{n-1}}{\sqrt{n-1}} < \frac{2^n}{\sqrt{n}},$$

as the lemma asserts. \square

2.4. Counting and group structure. For a positive $d \in \mathbb{R}$, a group X is said to be d -generated if it has a generating set of size at most d (note that $\lfloor d \rfloor$ is not necessarily the minimum size of a generating set of X). Since a chain of subgroups in G has length at most $\log_2 |X|$, it turns out that X is always $(\log_2 |X|)$ -generated.

Lemma 2.9. *Let X be a finite group. The following statements hold.*

- (a) *For a fixed positive number m , there are at most $|X|^{\log_2 m}$ subgroups of order m in X .*
- (b) *$|\text{Aut}(X)| \leq |X|^{\log_2 |X|} = 2^{\log_2^2 |X|}$.*
- (c) *X has less than $2^{(\log_2^2 n)/4+3}$ subgroups.*

Proof. Parts (a) and (b) follow from the previous paragraph, and part (c) is proved in [16]. \square

The following deep result due to Lubotzky [31, Page 198, (1)] estimates the number of finite groups of given order and given number of generators.

Theorem 2.10 (Lubotzky). *The number of isomorphism classes of d -generated groups of order n is at most $2^{2(d+1)\log_2^2 n}$.*

The next well-known result (see [25] and [12, Theorem 4.1], for example), along with its application Lemma 2.12, plays a crucial role in the proof of Theorem 1.2.

Lemma 2.11. *There is no finite nonabelian group with an automorphism inverting more than $3/4$ of its elements. Moreover, a finite group in which more than $3/4$ of the elements are involutions is an elementary abelian 2-group.*

Lemma 2.12. *Let X be a finite group, and let G be a nonabelian subgroup of index 2 in X . Then $|\mathcal{I}(X \setminus G)| \leq 3|G|/4$.*

Proof. Assume without loss of generality $\mathcal{I}(X \setminus G) \neq \emptyset$. Fix $x \in \mathcal{I}(X \setminus G)$, so that $X = G \rtimes \langle x \rangle$. For each $g \in G$, we have $(gx)^2 = 1$ if and only if $x^{-1}gx = xgx = g^{-1}$, that is, $gx \in \mathcal{I}(X \setminus G)$ if and only if x inverts g . As G is nonabelian, we derive from Lemma 2.11 that there is no automorphism of G inverting more than $3/4$ of its elements. Thus $|\mathcal{I}(X \setminus G)| \leq 3|G|/4$. \square

As usual, the symbol \sqcup denotes disjoint union of sets, and $H \setminus G/K$ denotes the set of double cosets of H and K in G , for subgroups H and K of a group G .

Lemma 2.13. *Let G be a group with subgroups H and K of finite indices. Then either $|H \setminus G/K| \leq \frac{3}{4} \max\{|G:H|, |G:K|\}$, or $H = K$ is normal in G .*

Proof. Without loss of generality, assume that $|H| \leq |K|$. Let Hg_1K, \dots, Hg_sK be the double cosets of size $|H|$. If $s \leq |G:H|/2$, then

$$|H \setminus G/K| \leq s + \frac{|G:H| - s}{2} = \frac{|G:H| + s}{2} \leq \frac{3}{4}|G:H| = \frac{3}{4} \max\{|G:H|, |G:K|\},$$

satisfying the conclusion of the lemma. Assume for the rest of the proof that $s > |G:H|/2$.

For each $i \in \{1, \dots, s\}$, it follows from $Hg_iK = Hg_i$ that $K \subseteq g_i^{-1}Hg_i$, which together with $|H| \leq |K|$ implies $g_i^{-1}Hg_i = K$. In particular, $g_1^{-1}Hg_1 = \dots = g_s^{-1}Hg_s$. Hence every element of $Hg_1g_1^{-1} \sqcup \dots \sqcup Hg_s g_s^{-1}$ normalizes H . This yields $|\mathbf{N}_G(H)| \geq |H|s > |H||G:H|/2 = |G|/2$, which forces $\mathbf{N}_G(H) = G$, that is, H is normal in G . Then we deduce from $g_1^{-1}Hg_1 = K$ that $H = K$, proving the conclusion of the lemma. \square

The following result follows from [9, Lemma 2.3] and Lemma 2.13.

Lemma 2.14. *Let M be an intransitive permutation group with exactly two orbits U and W , and let κ be the number of double cosets of the stabilizers M_w and M_u in M , where $u \in U$ and $w \in W$. Then there are exactly 2^κ bipartite graphs Γ with bipartition $\{U, W\}$ such that $M \leq \text{Aut}(\Gamma)$. Moreover, if $|U| = |W|$ and M is not semiregular, then $\kappa \leq \frac{3}{4}|U|$.*

The final lemma is an immediate consequence of the Classification of Finite Simple Groups, and a detailed verification can be found in [45].

Lemma 2.15. *For every finite nonabelian simple group T we have $|\text{Out}(T)| \leq \log_2 |T|$.*

3. STRATEGY TO PROVE THEOREM 1.2

We first establish two reduction results for Theorem 1.2, which will be presented in Sections 3.1 and 3.2, respectively. Building upon these results, the key to proving Theorem 1.2 lies in estimating the number of subsets S of G for which there exists a “large” subgroup M of $\text{Aut}^+(\mathbf{H}(G, S))$ such that G is maximal and core-free in M . We present this enumeration in Section 3.3 and dedicate Section 4 to its proof. This proof, of independent interest, analyzes primitive groups with a “large” regular subgroup. In essence, the analytical framework mirrors that of [36, Section 5]. Summarizing these results we arrive at an upper bound on the number of subsets S of G such that $\text{Aut}^+(\mathbf{H}(G, S)) > G$ (see Proposition 5.2). Armed with this bound, we conclude the proof of Theorem 1.2 in Section 5, requiring only minimal additional effort.

Let us start with the following definition, which will also be used in Sections 4 and 5.

Definition 3.1. Let G be a group. For a subset S of G and a subgroup X of $\text{Aut}^+(\mathbf{H}(G, S))$ such that $G < X$, we call (S, X) an *exceptional pair* of G (with respect to S). If, in addition, G is maximal in X , then we call (S, X) a *minimally exceptional pair*.

3.1. Babai-Godsil-like reduction. Let X be a permutation group on Ω . If a subset Δ of Ω is invariant under X , we denote by $X|_\Delta$ the group induced by X on Δ . Moreover, if Δ is $\langle g \rangle$ -invariant, where $g \in X$, then we write $g|_\Delta$ to denote the permutation induced by g on Δ .

Lemma 3.2. *Let G be a group of order n . For each positive integer t , the number of subsets S of G such that there exists a pair (H, f) satisfying the following conditions (a) and (b) is less than $2^{n - \frac{n}{3t} \log_2(\frac{4}{3}) + \frac{\log_2^2 n}{4} + \log_2 n + 2 \log_2 t + 1}$.*

- (a) H is a nontrivial proper normal subgroup of G with $|H| \leq t$;
- (b) $f \in \text{Aut}^+(\mathbf{H}(G, S))$ stabilizes every H -orbit on $V(\mathbf{H}(G, S))$ and fixes 1_+ , and the induced permutation $f|_{(G \setminus H)_+}$ of f on $(G \setminus H)_+$ is nontrivial.

Proof. Let \mathcal{H} be the set of nontrivial normal subgroups of G with order at most t , and let

$$\mathcal{S} = \{S \subseteq G \mid \text{there exists a pair } (H, f) \text{ satisfying both (a) and (b)}\}.$$

For $H \in \mathcal{H}$, let

$$\mathcal{S}(H) = \{S \subseteq G \mid \text{there exists } f \in \text{Aut}^+(\mathbf{H}(G, S)) \text{ satisfying (b)}\}.$$

Since Lemma 2.9(c) implies that $|\mathcal{H}| \leq 2^{(\log_2^2 n)/4 + 3}$, we only need to prove

$$|\mathcal{S}(H)| < 2^{n - \frac{n}{3t} \log_2(\frac{4}{3}) + \log_2 n + 2 \log_2 t - 2}, \quad (4)$$

for each $H \in \mathcal{H}$.

Fix some $H \in \mathcal{H}$ for the rest of the proof. Let $a = |H| \leq t$, $b = n/a$, and H_1, \dots, H_b be the right cosets of H in G , where $H_1 = H$. For each $i \in \{2, \dots, b\}$, let

$$\mathcal{S}_i = \{S \subseteq G \mid \text{there exists } f \text{ satisfying (b) with } f|_{(N_i)_+} \neq 1\}.$$

As $b \leq n/2 = 2^{\log_2 n - 1}$, to prove (4), it suffices to show

$$|\mathcal{S}_i| < 2^{n - \frac{n}{3t} \log_2(\frac{4}{3}) + 2 \log_2 t - 1} \quad (5)$$

for each $i \in \{2, \dots, b\}$.

From now on, fix some $i \in \{2, \dots, b\}$. The right multiplication of any element in H_i induces a permutation on $\{H_1, \dots, H_b\}$ and hence on $\{1, \dots, b\}$. Denote by σ this induced permutation on $\{1, \dots, b\}$, which does not depend on the choice of elements in H_i . Since H is normal in G and $H_i \neq H$, we have $j \neq j^\sigma$ for $j \in \{1, \dots, b\}$. Choose a subset $J \subseteq \{1, \dots, b\}$ of maximal size satisfying $\{j, j^\sigma\} \cap \{k, k^\sigma\} = \emptyset$ for all distinct $j, k \in J$. Then $j^\sigma \notin J$ for $j \in J$, that is, $J \cap J^\sigma = \emptyset$. If $|J| < b/3$, then

$$\left| \bigcup_{j \in J} \{j, j^\sigma, j^{\sigma^{-1}}\} \right| \leq 3|J| < b,$$

and so there exists $\ell \in \{1, \dots, b\} \setminus \bigcup_{j \in J} \{j, j^\sigma, j^{\sigma^{-1}}\}$. However, it follows that $\{j, j^\sigma\} \cap \{\ell, \ell^\sigma\} = \emptyset$ for each $j \in J$, which implies that the set $J \cup \{\ell\}$ satisfies $\{j, j^\sigma\} \cap \{k, k^\sigma\} = \emptyset$ for all distinct $j, k \in J \cup \{\ell\}$, contradicting the maximality of J . Therefore, $|J| \geq b/3$.

For each $S \subseteq G$, $x \in H_i$ and $j \in \{1, \dots, b\}$, let $C(S, x, j)$ denote the set of common neighbours of 1_+ and x_+ in $(H_{j^\sigma})_-$ within the graph $\mathbb{H}(G, S)$. If $S \in \mathcal{S}_i$, then there exists $f \in \text{Aut}^+(\mathbb{H}(G, S))$ and distinct $x, y \in H_i$ such that $(1_+)^f = 1_+$ and $(x_+)^f = y_+$. Since f fixes every H -orbit on $V(\mathbb{H}(G, S))$, we obtain

$$|C(S, x, j)| = |C(S, x, j)^f| = |C(S, y, j)|,$$

for each $j \in \{1, \dots, b\}$. In particular, if $S \in \mathcal{S}_i$, then there exists a 2-subset $\{x, y\}$ of H_i such that $|C(S, x, j)| = |C(S, y, j)|$ for each $j \in J$. Denote

$$\mathcal{S}_i(\{x, y\}, j) = \{S \in \mathcal{S}_i \mid |C(S, x, j)| \equiv |C(S, y, j)| \pmod{2}\}, \quad (6)$$

for each $\{x, y\} \in \binom{H_i}{2}$ and $j \in J$. Then

$$\mathcal{S}_i \subseteq \bigcup_{\{x, y\} \in \binom{H_i}{2}} \left(\bigcap_{j \in J} \mathcal{S}_i(\{x, y\}, j) \right).$$

Since $|\binom{H_i}{2}| = \binom{a}{2} \leq \binom{t}{2} \leq 2^{2 \log_2 t - 1}$, to prove (5), it remains to show that

$$\left| \bigcap_{j \in J} \mathcal{S}_i(\{x, y\}, j) \right| \leq 2^{n - \frac{n}{3t} \log_2(\frac{4}{3})}. \quad (7)$$

Fix some 2-subset $\{x, y\}$ of H_i . For $g \in G$,

$$\begin{aligned} g_- \in C(S, x, j) &\Leftrightarrow (g \in S) \wedge (g \in Sx) \wedge (g \in H_{j^\sigma}) \\ &\Leftrightarrow (g \in Sx \cap H_{j^\sigma}) \wedge (g \in S \cap H_{j^\sigma}) \\ &\Leftrightarrow (g \in (S \cap H_j)x) \wedge (g \in S \cap H_{j^\sigma}). \end{aligned}$$

For each $S \subseteq G$, denote $S_j = S \cap H_j$. Then the above means

$$C(S, x, j) = ((S_j)x \cap S_{j^\sigma})_-. \quad (8)$$

Let μ_j be the number of pairs $(S_j, S_{j\sigma})$ such that

$$|(S_j)x \cap S_{j\sigma}| \equiv |(S_j)y \cap S_{j\sigma}| \pmod{2}. \quad (9)$$

We claim $\mu_j \leq 3 \cdot 2^{2a-2}$. To this end, let c_j be the number of subset S_j of H_j with $(S_j)x = (S_j)y$. Such an S_j is a union of $\langle xy^{-1} \rangle$ -orbits on H_j . The condition $x \neq y$ implies that $\langle xy^{-1} \rangle = \langle yx^{-1} \rangle$ is a nontrivial subgroup of H and hence fixes setwise H_j . The semiregularity of H implies

$$c_j \leq 2^{a/2}.$$

Therefore, the number of pairs $(S_j, S_{j\sigma})$ with $(S_j)x = (S_j)y$ is at most $c_j \cdot 2^a$. Next we enumerate the pairs $(S_j, S_{j\sigma})$ with $(S_j)x \neq (S_j)y$. For such a pair, both $(S_j)x \setminus (S_j)y$ and $(S_j)y \setminus (S_j)x$ are non-empty subset of $N_{j\sigma}$. It follows from (9) that $|((S_j)x \setminus (S_j)y) \cap S_{j\sigma}|$ must have the same parity as $|((S_j)y \setminus (S_j)x) \cap S_{j\sigma}|$. By Lemma 2.7, this gives 2^{a-1} choices for $S_{j\sigma}$ for each fixed S_j . Therefore,

$$\mu_j \leq c_j \cdot 2^a + (2^a - c_j) \cdot 2^{a-1} = c_j \cdot 2^{a-1} + 2^{2a-1} \leq 2^{3a/2-1} + 2^{2a-1} \leq 3 \cdot 2^{2a-2},$$

as $a = |N| \geq 2$.

Since $J \cap J^\sigma = \emptyset$, we then conclude from (6) and (8) that

$$\left| \bigcap_{j \in J} \mathcal{S}_i(\{x, y\}, j) \right| \leq \left(\prod_{j \in J} \mu_j \right) \cdot 2^{a(b-2|J|)} \leq (3 \cdot 2^{2a-2})^{|J|} \cdot 2^{n-2a|J|} = 2^n \left(\frac{3}{4} \right)^{|J|} \leq 2^n \left(\frac{3}{4} \right)^{b/3},$$

which leads to (7), as desired. \square

We also need the following lemma for the first reduction.

Lemma 3.3. *Let G be a group of order n . The number of subsets S of G such that there exists a pair (H, f) satisfying the following conditions (a)–(c) is less than $2^{\frac{3}{4}n + \frac{\log_2^2 n}{4} + 2 \log_2 n + 4}$.*

- (a) H is a nontrivial proper subgroup of G ;
- (b) $f \in \text{Aut}^+(\text{H}(G, S))$ stabilizes every H -orbit on $V(\text{H}(G, S))$;
- (c) f induces a nontrivial permutation on G_+ fixing $(G \setminus H)_+$ pointwise.

Proof. Since Lemma 2.9(c) asserts that there are less than $2^{(\log_2^2 n)/4+3}$ subgroups of G , we only need to show that, for a fixed nontrivial $H < G$, the size of the following set is at most $2^{\frac{3}{4}n + 2 \log_2 n + 1}$.

$$\mathcal{S} = \{S \subseteq G \mid \text{there exists } f \in \text{Aut}^+(\text{H}(G, S)) \text{ satisfying (b) and (c)}\}.$$

We first estimate the size of

$$\mathcal{T} := \{S \subseteq G \mid \text{there exists } f \in \text{Aut}^+(\text{H}(G, S)) \text{ satisfying (b) and (c) such that } f|_{G_-} = 1\}.$$

Let $S \in \mathcal{T}$ with a witness $f \in \text{Aut}^+(\text{H}(G, S))$. Since $f|_{H_+} \neq 1$, there exist distinct $x, y \in H$ such that $(x_+)^f = y_+$. Write $\Gamma = \text{H}(G, S)$. Then since $(x_+)^{fy^{-1}} = (y_+)^{y^{-1}} = 1_+$, we derive from $f|_{G_-} = 1$ that

$$S_- = N_\Gamma(1_+) = N_\Gamma((x_+)^{fy^{-1}}) = (N_\Gamma(x_+))^{fy^{-1}} = ((Sx)_-)^{fy^{-1}} = ((Sx)_-)^{y^{-1}} = (Sxy^{-1})_-.$$

Hence $S = Sxy^{-1}$, which means that S is a union of some left cosets of $\langle xy^{-1} \rangle$. Since $xy^{-1} \neq 1$, it follows that, for a fixed non-identity element xy^{-1} , there are at most $2^{n/2}$ possibilities for S . Considering the choices for $xy^{-1} \in H$, we conclude that

$$|\mathcal{T}| \leq (|H| - 1) \cdot 2^{\frac{n}{2}} < 2^{\log_2 |H|} \cdot 2^{\frac{n}{2}} < 2^{\frac{n}{2} + \log_2 n}. \quad (10)$$

Now assume $S \in \mathcal{S} \setminus \mathcal{T}$. Then there exists $f \in \text{Aut}^+(\text{H}(G, S))$ satisfying (a) and (b) such that $f|_{G_-} \neq 1$. In particular, there exist distinct elements $x, y \in G$ such that $(x_-)^f = y_-$ and so $(1_-)^{xfy^{-1}} = (x_-)^{fy^{-1}} = (y_-)^{y^{-1}} = 1_-$. Since $(S^{-1})_+$ is the neighbourhood of 1_- in

$\mathbb{H}(G, S)$, it follows that xfy^{-1} stabilizes $(S^{-1})_+$. Write $D = G \setminus H$. We claim that xfy^{-1} also stabilizes $(Dx^{-1})_+$. In fact, since (b) implies that x_- and y_- are in the same H -orbits, we have $(1_-)^{xH} = (x_-)^H = (y_-)^H = (1_-)^{yH}$. This together with the semiregularity of G implies that $xH = yH$ and so $Hx^{-1} = Hy^{-1}$. Hence $Dx^{-1} = Dy^{-1}$, which leads to

$$((Dx^{-1})_+)^{xfy^{-1}} = (D_+)^{fy^{-1}} = (D_+)^{y^{-1}} = (Dy^{-1})_+ = (Dx^{-1})_+,$$

as claimed. It follows that

$$\begin{aligned} (S^{-1} \cap Dx^{-1})_+ &= ((S^{-1} \cap Dx^{-1})_+)^{xfy^{-1}} \\ &= ((S^{-1}x \cap D)_+)^{fy^{-1}} = ((S^{-1}x \cap D)_+)^{y^{-1}} = ((S^{-1} \cap Dx^{-1})xy^{-1})_+. \end{aligned}$$

Consequently, $S^{-1} \cap Dx^{-1} = (S^{-1} \cap Dx^{-1})xy^{-1}$, which means that $S^{-1} \cap Dx^{-1}$ is a union of left cosets of $\langle xy^{-1} \rangle$. Since $xy^{-1} \neq 1$, the condition $Dx^{-1} = Dy^{-1}$ indicates that Dx^{-1} is a union of at most $|D|/2$ left cosets of $\langle xy^{-1} \rangle$. Therefore, for a fixed pair (x, y) of elements in G such that $xy^{-1} \in D$, there are at most $2^{|D|/2}$ choices for $S^{-1} \cap Dx^{-1}$ and hence at most

$$2^{|H|} \cdot 2^{\frac{|D|}{2}} = 2^{|H|} \cdot 2^{\frac{n-|H|}{2}} = 2^{\frac{n+|H|}{2}}$$

choices for S . Noting that $|H| \leq n/2$, we obtain

$$|\mathcal{S} \setminus \mathcal{T}| \leq n^2 \cdot 2^{\frac{n+|H|}{2}} \leq 2^{\frac{3}{4}n+2\log_2 n}.$$

Combining this with (10), we conclude that

$$|\mathcal{S}| \leq |\mathcal{T}| + |\mathcal{S} \setminus \mathcal{T}| < 2^{\frac{n}{2}+\log_2 n} + 2^{\frac{3}{4}n+2\log_2 n} < 2^{\frac{3}{4}n+2\log_2 n+1},$$

completing the proof. \square

We are now ready to state the first reduction result.

Proposition 3.4. *Let G be a group of order n . For each positive integer t , the number of subsets S of G such that there exists a pair (H, f) satisfying the following conditions (a) and (b) is less than $2^{n-\frac{n}{3t}\log_2(\frac{4}{3})+\frac{\log_2^2 n}{4}+\log_2 n+2\log_2 t+5}$.*

- (a) H is a nontrivial proper normal subgroup of G with $|H| \leq t$;
- (b) $f \in \text{Aut}^+(\mathbb{H}(G, S)) \setminus G$ stabilizes every H -orbit on $V(\mathbb{H}(G, S))$.

Proof. Let $\mathcal{S} = \{S \subseteq G \mid \text{there exists a pair } (H, f) \text{ satisfying (a) and (b)}\}$. For each $S \in \mathcal{S}$ and a witness pair (H, f) , the condition (b) implies that there exist unique elements $\alpha(S, H, f)$ and $\beta(S, H, f)$ in the right coset Hf of H in $\text{Aut}^+(\mathbb{H}(G, S))$ with $(1_+)^{\alpha(S, H, f)} = 1_+$ and $(1_-)^{\beta(S, H, f)} = 1_-$.

We first estimate the size of

$$\mathcal{S}_1 := \{S \in \mathcal{S} \mid \text{there exists } (H, f) \text{ satisfying (a) and (b) such that } \alpha(S, H, f)|_{G_+} \neq 1\}. \quad (11)$$

Let $S \in \mathcal{S}_1$ and (H, f) be a witness pair as in (11). Write $\alpha = \alpha(S, H, f)$ and $\beta = \beta(S, H, f)$. Then α stabilizes every H -orbit on $V(\mathbb{H}(G, S))$ and $(1_+)^{\alpha} = 1_+$. Applying Lemmas 3.2 and 3.3 to the pair (H, α) , we estimate the number of $S \in \mathcal{S}_1$ such that $\alpha|_{(G \setminus H)_+} \neq 1$ or $\alpha|_{(G \setminus H)_+} = 1$, respectively, and obtain

$$|\mathcal{S}_1| < 2^{n-\frac{n}{3t}\log_2(\frac{4}{3})+\frac{\log_2^2 n}{4}+\log_2 n+2\log_2 t+1} + 2^{\frac{3}{4}n+\frac{\log_2^2 n}{4}+2\log_2 n+4}. \quad (12)$$

With a similar argument we obtain the same upper bound as in (12) for

$$\mathcal{S}_2 := \{S \in \mathcal{S} \mid \text{there exists } (H, f) \text{ satisfying (a) and (b) such that } \beta(S, H, f)|_{G_-} \neq 1\}.$$

Now assume $S \in \mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2)$. Then we may take a pair (H, f) satisfying (a) and (b) such that $\alpha|_{G_+} = 1$ and $\beta|_{G_-} = 1$, where $\alpha = \alpha(S, H, f)$ and $\beta = \beta(S, H, f)$. In particular, $\alpha \neq \beta^{-1}$

(the condition $\alpha \in Hf$ indicates $\alpha \neq 1$). Since $\alpha\beta^{-1} \in H$, there exists a non-identity element $\gamma \in H$ such that $(g_-)^{\alpha\beta^{-1}} = (g\gamma)_-$ for each $g \in G$. Thus we deduce that

$$(S_-)^\alpha = (S_-)^{\alpha\beta^{-1}} = (S\gamma)_-$$

As S_- is the neighbourhood of 1_+ in $H(G, S)$ while $\alpha \in \text{Aut}^+(H(G, S))$ fixes 1_+ , it follows that $S_- = (S_-)^\alpha = (S\gamma)_-$. Hence S is a union of some left cosets of $\langle \gamma \rangle$. Therefore,

$$|\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2)| \leq (|H| - 1) \cdot 2^{\frac{n}{2}} < 2^{\frac{n}{2} + \log_2 t}.$$

Combining this with (12), we conclude that

$$\begin{aligned} |\mathcal{S}| &\leq |\mathcal{S}_1| + |\mathcal{S}_2| + |\mathcal{S} \setminus (\mathcal{S}_1 \cup \mathcal{S}_2)| \\ &< 2^{n - \frac{n}{3t} \log_2(\frac{4}{3}) + \frac{\log_2^2 n}{4} + \log_2 n + 2 \log_2 t + 2} + 2^{\frac{3}{4}n + \frac{\log_2^2 n}{4} + 2 \log_2 n + 5} + 2^{\frac{n}{2} + \log_2 t} \\ &< 2^{n - \frac{n}{3t} \log_2(\frac{4}{3}) + \frac{\log_2^2 n}{4} + \log_2 n + 2 \log_2 t + 5}, \end{aligned}$$

where the last inequality follows with a computation. \square

3.2. Morris-Spiga-like reduction. In this section, we give two reduction results, namely, Propositions 3.6 and 3.7, based on the following lemma.

Lemma 3.5. *Let $\varepsilon \in (0, 0.5)$, and let n_ε be a positive integer such that (1) holds for all $n \geq n_\varepsilon$. Then for each semiregular subgroup G of $\text{Sym}(2n)$ with order $n \geq n_\varepsilon$, the number of subgroups M of $\text{Sym}(2n)$ satisfying the following conditions (a) and (b) is less than $2^{n^{1-\varepsilon}}$.*

- (a) $G < M$ and M has exactly two orbits;
- (b) $|M| \leq 2^{n^{0.5-\varepsilon} + \log_2 n}$ and M is $(1 + \log_2 n)$ -generated.

Proof. Fix a semiregular subgroup G of $\text{Sym}(2n)$ with order $n \geq n_\varepsilon$. Then G has exactly two orbits, acting regularly on each of them. Hence $G \leq \text{Sym}(n) \times \text{Sym}(n)$ and $\mathbf{C}_{\text{Sym}(n) \times \text{Sym}(n)}(G) = G \times G$. Since $|\text{Aut}(G)| \leq 2^{\log_2^2 n}$ as Lemma 2.9(b) asserts, it then follows that

$$|\mathbf{N}_{\text{Sym}(n) \times \text{Sym}(n)}(G)| \leq |\mathbf{C}_{\text{Sym}(n) \times \text{Sym}(n)}(G)| |\text{Aut}(G)| \leq n^2 2^{\log_2^2 n} = 2^{\log_2^2 n + 2 \log_2 n}. \quad (13)$$

Let $\mathcal{X} = \{[M] \mid M \text{ satisfies (b)}\}$, where $[M]$ denotes the equivalence class of groups isomorphic to M . Write $d(n) = n^{0.5-\varepsilon} + \log_2 n$. We conclude by Theorem 2.10 that

$$|\mathcal{X}| \leq 2^{d(n)} \cdot 2^{2((1+\log_2 n)+1)d^2(n)} = 2^{(4+2\log_2 n)d^2(n)+d(n)}.$$

Given a group X with a pair (H, K) of subgroups and a group Y with a pair (P, Q) of subgroups, define $(X, H, K) \approx (Y, P, Q)$ if there is a group isomorphism $\varphi: X \rightarrow Y$ such that $\varphi(H) = P$ and $\varphi(K) = Q$. Clearly, \approx is an equivalence relation. Let

$$\mathcal{T} = \{(X, H, K) \mid [X] \in \mathcal{X}, |X:H| = |X:K| = n, \text{Core}_X(H) \cap \text{Core}_X(K) = 1\}$$

and let \mathcal{T}/\approx denote the \approx -equivalence classes in \mathcal{T} . For each group X with $[X] \in \mathcal{X}$, we derive from Lemma 2.9(a) that there are at most

$$|X|^{2 \log_2(|X|/n)} = 2^{2(\log_2 |X|)(\log_2 |X| - \log_2 n)} \leq 2^{2d(n)(d(n) - \log_2 n)}$$

choices for a pair (H, K) of subgroups of index n in X . Hence

$$\begin{aligned} |\mathcal{T}/\approx| &\leq |\mathcal{X}| \cdot 2^{2d(n)(d(n) - \log_2 n)} \leq 2^{(4+2\log_2 n)d^2(n)+d(n)} \cdot 2^{2d(n)(d(n) - \log_2 n)} \\ &= 2^{(6+2\log_2 n)d^2(n)+(1-2\log_2 n)d(n)}. \end{aligned}$$

Let \sim be the equivalence relation of conjugation of subgroups in $\text{Sym}(n) \times \text{Sym}(n)$. Note that each triple $(X, H, K) \in \mathcal{T}$ gives rise to a subgroup $T(X, H, K)$ of $\text{Sym}(n) \times \text{Sym}(n)$ via the right multiplication action of X on $[X:H]$ and $[X:K]$, and that triples in the same \approx -equivalence class give subgroups of $\text{Sym}(n) \times \text{Sym}(n)$ in the same \sim -equivalence class.

Let

$$\mathcal{M} = \{M \leq \text{Sym}(2n) \mid M \text{ satisfies (a) and (b)}\}.$$

Since each $M \in \mathcal{M}$ lies in the same \sim -equivalence class with $T(X, H, K)$ for some $(X, H, K) \in \mathcal{T}$, we conclude that

$$|\mathcal{M}/\sim| \leq |\mathcal{T}/\approx| \leq 2^{(6+2\log_2 n)d^2(n)+(1-2\log_2 n)d(n)}.$$

Suppose for a contradiction that $|\mathcal{M}| \geq 2^{n^{1-\varepsilon}}$. Then by Pigeonhole Principal, there are pairwise distinct $M_1, \dots, M_t \in \mathcal{M}$ in the same \sim -equivalence class with

$$t \geq \frac{2^{n^{1-\varepsilon}}}{2^{(6+2\log_2 n)d^2(n)+(1-2\log_2 n)d(n)}} > 2^{(\log_2 n)d(n)+\log_2^2 n+2\log_2 n}, \quad (14)$$

where the $>$ sign in (14) follows from (1). We deduce that for each $i \in \{1, \dots, t\}$ we have $M_1 = x_i^{-1}M_i x_i$ for some $x_i \in \text{Sym}(n) \times \text{Sym}(n)$ (note that $x_i \neq x_j$ if $i \neq j$, as M_1, \dots, M_t are pairwise distinct). In particular, $x_1^{-1}Gx_1, \dots, x_t^{-1}Gx_t$ are all subgroups of order n in M_1 , as $G < M_i$ for all $i \in \{1, \dots, t\}$. However, by Lemma 2.9(a), M_1 has at most

$$|M_1|^{\log_2 n} \leq 2^{(\log_2 n)d(n)}$$

subgroups of order n . Then again by Pigeonhole Principal, we deduce from (14) that there exists $\{i_1, \dots, i_s\} \subseteq \{1, \dots, t\}$ with $s > 2^{\log_2^2 n+2\log_2 n}$ and $x_{i_1}^{-1}Gx_{i_1} = \dots = x_{i_s}^{-1}Gx_{i_s}$. This shows the existence of s distinct elements $x_{i_1}x_{i_1}^{-1}, \dots, x_{i_s}x_{i_s}^{-1}$ in $\text{Sym}(n) \times \text{Sym}(n)$ normalizing G , contradicting (13). Thus the proof is complete. \square

Recall Definition 3.1, noting that for each exceptional pair (S, X) there exists a minimally exceptional pair (S, M) such that $M \leq X$.

Proposition 3.6. *Let $\varepsilon \in (0, 0.5)$, and let n_ε be a positive integer such that (1) holds for all $n \geq n_\varepsilon$. Then for each group G of order $n \geq n_\varepsilon$, the number of subsets S of G such that there exists an exceptional pair (S, X) with $|X| \leq 2^{n^{0.5-\varepsilon}+\log_2 n}$ is less than $2^{\frac{3}{4}n+n^{1-\varepsilon}}$.*

Proof. Fix a group G with order $n \geq n_\varepsilon$. Suppose, for a contradiction, that there are t subsets S_1, \dots, S_t of G , where $t > 2^{\frac{3}{4}n+n^{1-\varepsilon}}$, such that there exists an exceptional pair (S_i, X_i) with $|X_i| \leq 2^{n^{0.5-\varepsilon}+\log_2 n}$ for each $i \in \{1, \dots, t\}$. Let V be the (same) vertex set of

$$\text{H}(G, S_1), \dots, \text{H}(G, S_t),$$

and let U and W be the two orbits of G on V .

The definition of exceptional pair implies that $X_i \leq \text{Aut}^+(\text{H}(G, S_i))$ and X_i has exactly two orbits U and W on V . For each $i \in \{1, \dots, t\}$, let M_i be a subgroup of X_i such that (S_i, M_i) is a minimally exceptional pair. Since G is $(\log_2 n)$ -generated and is a maximal subgroup of M_i , it follows that M_i is $(1 + \log_2 n)$ -generated. Hence each M_i satisfies both (a) and (b) of Lemma 3.5, and so there are at most $2^{n^{1-\varepsilon}}$ distinct ones among M_1, \dots, M_t . By Pigeonhole Principle, there exists $\{i_1, \dots, i_s\} \subseteq \{1, \dots, t\}$ with $s \geq t/2^{n^{1-\varepsilon}} > 2^{3n/4}$ such that

$$M_{i_1} = \dots = M_{i_s}.$$

Since M_{i_1} is not semiregular on V , Lemma 2.14 shows that there are at most $2^{3n/4}$ bipartite graphs with bipartition $\{U, W\}$ whose automorphism group contains M_{i_1} . This contradicts the condition that $M_{i_1} = M_{i_j} \leq \text{Aut}^+(\text{H}(G, S_{i_j}))$ for each $j \in \{i_1, \dots, i_s\}$. \square

Proposition 3.7. *Let $\varepsilon \in (0, 0.5)$, and let n_ε be a positive integer such that for all $n \geq n_\varepsilon$,*

$$\log_2^2 n < n^{0.5-\varepsilon}. \quad (15)$$

Then for each group G of order $n \geq n_\varepsilon$, the number of subsets S of G such that there exists a minimally exceptional pair (S, M) satisfying the following conditions (a) and (b) is less than $2^{n - \frac{n}{4 \log_2 n} \log_2 \left(\frac{e}{2}\right) + \frac{\log_2^2 n}{4} + \frac{1}{2} \log_2 \left(\frac{n}{4 \log_2 n}\right) + \log_2(24)}$.

- (a) $|M| > 2^{n^{0.5-\varepsilon} + \log_2 n}$;
- (b) $|\text{Core}_M(G)| > 8 \log_2 n$.

Proof. Fix a group G of order $n \geq n_\varepsilon$. Let $\{U, W\}$ be the bipartition for the Haar graphs of G . Let

$$\mathcal{M} = \{M \leq \text{Sym}(U) \times \text{Sym}(W) \mid M \text{ satisfies (a) and (b), } G \text{ is maximal in } M\}.$$

The proposition is an estimation on the number of $S \subseteq G$ such that there exists $M \in \mathcal{M}$ with $M \leq \text{Aut}^+(\text{H}(G, S))$. By Lemma 2.14, we only need to prove

$$|\mathcal{M}| < 2^{\frac{n}{4} - \frac{n}{4 \log_2 n} \log_2 \left(\frac{e}{2}\right) + \frac{\log_2^2 n}{4} + \frac{1}{2} \log_2 \left(\frac{n}{\log_2 n}\right) + \log_2(24)}. \quad (16)$$

Let $M \in \mathcal{M}$, and fix some $u \in U$. Then, by condition (a) and (15), the stabilizer M_u satisfies

$$|M_u| = \frac{|M|}{n} > \frac{2^{n^{0.5-\varepsilon} + \log_2 n}}{n} = 2^{n^{0.5-\varepsilon}} > 2^{\log_2^2 n}.$$

Let $C = \text{Core}_M(G)$. Since C is a subgroup of the semiregular group G , we have

$$\mathbf{C}_{\text{Sym}(2n)}(C) \cong C \wr \text{Sym}(2n/|C|).$$

By the inequality $x! < 3\sqrt{x}(x/e)^x$ (Stirling's formula), we obtain

$$\begin{aligned} |\mathbf{C}_{\text{Sym}(2n)}(C)| &= |C|^{\frac{2n}{|C|}} \cdot \left(\frac{2n}{|C|}\right)! < |C|^{\frac{2n}{|C|}} \cdot 3 \left(\frac{2n}{|C|}\right)^{\frac{1}{2}} \left(\frac{2n}{e|C|}\right)^{\frac{2n}{|C|}} \\ &= 3 \left(\frac{2n}{|C|}\right)^{\frac{1}{2}} \left(\frac{2n}{e}\right)^{\frac{2n}{|C|}} < 3 \left(\frac{n}{4 \log_2 n}\right)^{\frac{1}{2}} \left(\frac{2n}{e}\right)^{\frac{n}{4 \log_2 n}}, \end{aligned} \quad (17)$$

where in the last inequality we have used condition (b).

Since M normalizes C , the group M_u acts by conjugation as a group of automorphisms on C . Moreover, by Lemma 2.9(b),

$$\text{Aut}(C) \leq 2^{\log_2^2 |C|} \leq 2^{\log_2^2 n} < |M_u|.$$

Hence the conjugation action of M_u on C is not faithful, and so there exists $g \in \mathbf{C}_{M_u}(C)$ with $g \neq 1$. In particular, $g \notin G$, as $G \cap M_u = 1$. Then it follows from the maximality of G in M that $M = \langle G, g \rangle$. Accordingly, M is determined by a non-identity element of $\mathbf{C}_{\text{Sym}(2n)}(C)$. Considering the choices for the subgroup C of G , we conclude by Lemma 2.9(c) and (17) that

$$|\mathcal{M}| < 2^{\frac{\log_2^2 n}{4} + 3} \cdot 3 \left(\frac{n}{4 \log_2 n}\right)^{\frac{1}{2}} \left(\frac{2n}{e}\right)^{\frac{n}{4 \log_2 n}},$$

This is equivalent to

$$\begin{aligned} \log_2 |\mathcal{M}| &< \frac{\log_2^2 n}{4} + 3 + \log_2 3 + \frac{1}{2} \log_2 \left(\frac{n}{4 \log_2 n}\right) + \frac{n}{4 \log_2 n} \log_2 \left(\frac{2n}{e}\right) \\ &= \frac{n}{4} - \frac{n}{4 \log_2 n} \log_2 \left(\frac{e}{2}\right) + \frac{\log_2^2 n}{4} + \frac{1}{2} \log_2 \left(\frac{n}{4 \log_2 n}\right) + \log_2(24), \end{aligned}$$

proving (16), as required. \square

3.3. Critical pairs. Recall Definition 3.1. For each subset S of a finite group G such that $\text{Aut}(\text{H}(G, S)) > G$, there exists a minimally exceptional pair with respect to S . As stated at the beginning of Section 3, to prove Theorem 1.2, the primary task is to estimate the number of subsets S of G such that there exists a “large” subgroup M of $\text{Aut}^+(\text{H}(G, S))$ with G maximal and core-free in M . We make this precise in the following definition.

Definition 3.8. Let G be a finite group of order n , and let $\varepsilon \in (0, 0.1]$. A minimally exceptional pair (S, M) of G is said to be ε -critical if it satisfies

- (C1) $|M| > 2^{n^{0.5-\varepsilon} + \log_2 n}$, or equivalently, $|M_{1+}| = |M_{1-}| > 2^{n^{0.5-\varepsilon}}$;
- (C2) $\text{Core}_M(G) = 1$.

Clearly, an ε -critical pair is also an ε' -critical pair for each $\varepsilon' \geq \varepsilon$. We omit the label ε when $\varepsilon = 0.1$. Denote $\mathcal{Z}(G, \varepsilon) = \{S \subseteq G \mid \text{there exists an } \varepsilon\text{-critical pair } (S, M) \text{ of } G\}$.

The following is the desired estimation on the size of $\mathcal{Z}(G, \varepsilon)$.

Proposition 3.9. *Let G be a group of order $n \geq 2^{57}$. Then for each $\varepsilon \in (0, 0.1]$,*

$$|\mathcal{Z}(G, \varepsilon)| < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 9}.$$

Before proving Proposition 3.9 in Section 4, here we briefly outline the main idea underlying its technical proof. For an ε -critical pair (S, M) , since G is maximal in M and $\text{Core}_M(G) = 1$, the group M acts faithfully and primitively by right multiplication on the set $[M : G]$ of right cosets of G in M . Moreover, as $M = M_{1+}G = M_{1-}G$ and $M_{1+} \cap G = M_{1-} \cap G = 1$, the actions of M_{1+} and M_{1-} on $[M : G]$ are regular. Consequently, we obtain a primitive permutation group M on $[M : G]$ with regular subgroups M_{1+} and M_{1-} satisfying

$$|M_{1+}| = |M_{1-}| > 2^{|G|^{0.5-\varepsilon}}. \quad (18)$$

We follow the division in [41] of primitive groups into eight types, namely, HS, HC, AS, PA, CD, HA, SD and TW. For each type \mathcal{T} , let $\mathcal{Z}_{\mathcal{T}}(G, \varepsilon)$ be the set of $S \in \mathcal{Z}(G, \varepsilon)$ such that there exists an ε -critical pair (S, M) with the action of M on $[M : G]$ primitive of \mathcal{T} type. We write $\mathcal{Z}_{\mathcal{T}}(G, 0.1)$ as $\mathcal{Z}_{\mathcal{T}}(G)$ for simplicity. Since $\mathcal{Z}_{\mathcal{T}}(G, \varepsilon) \subseteq \mathcal{Z}_{\mathcal{T}}(G)$ for each $\varepsilon \in (0, 0.1]$, we have

$$\mathcal{Z}(G, \varepsilon) \subseteq \mathcal{Z}_{\text{HS}}(G) \cup \mathcal{Z}_{\text{HC}}(G) \cup \mathcal{Z}_{\text{AS}}(G) \cup \mathcal{Z}_{\text{PA}}(G) \cup \mathcal{Z}_{\text{CD}}(G) \cup \mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon).$$

In Section 4, we estimate $|\mathcal{Z}_{\mathcal{T}}(G)|$ for HS, HC, AS, PA, CD types and estimate $|\mathcal{Z}_{\mathcal{T}}(G, \varepsilon)|$ for HA, SD and TW types. More precisely, we establish Propositions 4.2, 4.4, 4.8, 4.10 and 4.13, which respectively imply the following upper bounds under the assumption $|G| = n \geq 2^{57}$:

$$\begin{aligned} \mathcal{Z}_{\text{HS}}(G) \cup \mathcal{Z}_{\text{HC}}(G) \cup \mathcal{Z}_{\text{PA}}(G) &= \emptyset, \\ |\mathcal{Z}_{\text{AS}}(G)| &< 2^{3(\log_2 n) + 75}, \end{aligned} \quad (19)$$

$$|\mathcal{Z}_{\text{CD}}(G)| < 2^{\frac{3}{4}n + 2 \log_2^4 n + \log_2^3 n + 1702 \log_2^2 n + 2 \log_2 n}, \quad (20)$$

$$|\mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon)| < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 7}. \quad (21)$$

Since the right-hand sides of (19) and (20) are both less than the right-hand side of (21) for each $\varepsilon \in (0, 0.1]$, we then derive

$$\begin{aligned} |\mathcal{Z}(G)| &\leq |\mathcal{Z}_{\text{AS}}(G)| + |\mathcal{Z}_{\text{CD}}(G)| + |\mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon)| \\ &< 3|\mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon)| < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 9}, \end{aligned}$$

as Proposition 3.9 asserts.

4. PRIMITIVE PERMUTATION GROUPS WITH A LARGE REGULAR SUBGROUP

In this section, we estimate $|\mathcal{Z}_{\mathcal{T}}(G, \varepsilon)|$ for various primitive types \mathcal{T} . The analysis depends on the structure of primitive groups with a “large” regular subgroup.

4.1. Estimate $|\mathcal{Z}_{\text{HS}}(G) \cup \mathcal{Z}_{\text{HC}}(G)|$.

Lemma 4.1. *Let M be a primitive group of HS or HC type with stabilizer G such that $|G| > 132$. Then M has no regular subgroup with order greater than $2^{|G|^{0.4}}$.*

Proof. In both of these cases, the socle of M has the form $H \times K$, where H and K are normal regular subgroups of M with $H \cong K \cong T^\ell$ for some nonabelian simple group T and some integer $\ell \geq 1$. Then the stabilizer $G \gtrsim \text{Inn}(H) \cong H$. Suppose on the contrary that M has a regular subgroup L with $|L| > 2^{|G|^{0.4}}$. Then

$$|G| \geq |\text{Inn}(H)| = |H| = |L| > 2^{|G|^{0.4}},$$

which is impossible as $|G| > 132$. \square

The following proposition follows immediately from Lemma 4.1 and (18).

Proposition 4.2. *Let G be finite group of order $n > 132$. Then $\mathcal{Z}_{\text{HS}}(G) \cup \mathcal{Z}_{\text{HC}}(G) = \emptyset$.*

4.2. Estimate $|\mathcal{Z}_{\text{AS}}(G)|$.

Lemma 4.3. *Let M be a primitive permutation group of AS type with socle N and the stabilizer G with $|G| \geq 2^{11}$. Suppose that M has a regular subgroup L with $|L| > 2^{|G|^{0.4}}$. Then one of the following occurs for some odd prime p .*

- (a) $N = \text{Alt}(p)$, $N \cap G = p \cdot \frac{p-1}{2}$, and $L = \text{Sym}(p-2)$ or $\text{Alt}(p-2) \times C_2$;
- (b) $N = \text{Alt}(p+1)$, $N \cap G = \text{PSL}_2(p)$, and $L = \text{Sym}(p-2)$ or $\text{Alt}(p-2) \times C_2$;
- (c) $N = \text{Alt}(p^2+1)$ with $p \equiv 3 \pmod{4}$, $N \cap G = \text{PSL}_2(p^2).2$, and $L = \text{Alt}(p^2-2)$.

Proof. The almost simple primitive groups with a regular subgroup are classified in [30]. By a computation for each case in [30, Table 16.1–16.3], we obtain that when $|G| \geq 2^{11}$, the inequality $|L| > 2^{|G|^{0.4}} \geq 2^{|N \cap G|^{0.4}}$ holds only in one of the three cases stated in the lemma. \square

Proposition 4.4. *Let G be finite group of order $n \geq 2^{11}$. Then $|\mathcal{Z}_{\text{AS}}(G)| < 2^{3(\log_2 n) + 75}$.*

Proof. Let $S \in \mathcal{Z}_{\text{AS}}(G)$. Then there is a critical pair (S, M) such that the action of M on $[M : G]$ is primitive of AS type. Let N be the socle of M , and let $L = M_{1_\epsilon}$, where $\epsilon \in \{+, -\}$. Since $|L| > 2^{n^{0.4}}$, the triple (G, N, L) is described in Lemma 4.3. In particular, $N = \text{Alt}(m)$ with $m \in \{p, p+1, p^2+1\}$ for some odd prime p , and

$$\text{Alt}(\{1, \dots, m\} \setminus \Delta) \leq L \leq \text{Sym}(\Delta) \times \text{Sym}(\{1, \dots, m\} \setminus \Delta), \quad (22)$$

for some subset Δ of $\{1, \dots, m\}$ of size 2 or 3. As $n \geq 2^{11}$ by hypothesis, we get $|L| > 2^{n^{0.4}} \geq 2^{2^{4.4}}$. This implies $m > 7$. Considering the choices for subsets Δ and for the groups L satisfying (22), we obtain that the number of the choices for L is at most

$$\max \left\{ \binom{m}{2} \cdot 5, \binom{m}{3} \cdot 16 \right\} = \binom{m}{3} \cdot 16 = \frac{8m(m-1)(m-2)}{3}.$$

This implies that, for each $\epsilon \in \{+, -\}$, there are less than $8m(m-1)(m-2)/3$ choices M_ϵ . As $M \in \{\text{Alt}(m), \text{Sym}(m)\}$, it follows that there are at most $2(8m(m-1)(m-2)/3)^2$ choices for the triple (M, M_+, M_-) . Since $\text{Alt}(m)$ acts 6-transitively on $\{1, \dots, m\}$, the group $\text{Alt}(\{4, \dots, m\})$ has exactly

$$\binom{3}{0} + \binom{3}{1} \cdot 3 + \binom{3}{2} \cdot 3 \cdot 2 + 3 \cdot 2 \cdot 1 = 34$$

orbits on the set of triples of pairwise distinct elements in $\{1, \dots, m\}$. Since $\text{Alt}(\{1, \dots, m\}) \leq M \leq \text{Sym}(\{1, \dots, m\})$ and $L \geq \text{Alt}(\{1, \dots, m\} \setminus \Delta) \gtrsim \text{Alt}(\{4, \dots, m\})$, there are at most 68 double cosets of M_{1+} and M_{1-} in M . Therefore, in view of Lemma 2.14, there are less than

$$2(8m(m-1)(m-2)/3)^2 \cdot 2^{68} < 2^{72}(m(m-1)(m-2))^2$$

choices for $S \in \mathcal{Z}^{\text{AS}}(G)$. Note that, for each case arising in Lemma 4.3, we have

$$n = \frac{|M|}{|M_{1+}|} \geq \frac{|\text{Alt}(m)|}{|\text{Sym}(m-2)|} = \frac{m(m-1)}{2}.$$

We conclude that

$$|\mathcal{Z}^{\text{AS}}(G)| < 2^{72}(m(m-1)(m-2))^2 < 2^{72}(m(m-1))^3 \leq 2^{3(\log_2 n)+75},$$

as the proposition asserts. \square

4.3. Estimate $|\mathcal{Z}_{\text{PA}}(\mathbf{G})|$. Let M be a primitive permutation group of PA type with socle N and point stabilizer G . Then we have $M \leq H \wr \text{Sym}(\kappa)$ endowed with its natural wreath product action on Δ^κ , where H is a primitive group of AS type on Δ and $\kappa \geq 2$. Let T be the socle of H , and let $\delta \in \Delta$. Then $N = T^\kappa$ and $T_\delta \neq 1$. Recall that $P(X)$ denotes the minimal index of proper subgroups of a finite group X .

Lemma 4.5. *Let H be a finite almost simple group with socle T , and let B be a core-free subgroup of H such that $H = KB$ for some core-free subgroup K of H . Then either $|\text{Out}(T)| \leq |T \cap B|$ or $T \in \{\text{PSL}_2(9), \text{PSL}_3(4)\}$. Moreover, if B is maximal in H , then $|\text{Out}(T)| \leq |T \cap B|$.*

Proof. Suppose that $|\text{Out}(T)| > |T \cap B|$. Then we derive from $H = KB$ that

$$|\text{Out}(T)|^2 > |\text{Out}(T)||T \cap B| \geq \frac{|H||T \cap B|}{|T|} = \frac{|H||B|}{|TB|} \geq |B| \geq \frac{|H|}{|K|} \geq \frac{|T|}{|T \cap K|} \geq |P(T)|.$$

By [19, Table 4], this implies $T \cong \text{PSL}_2(9)$, $\text{PSL}_2(27)$, $\text{PSL}_3(4)$ or $\text{PSL}_3(16)$. A computation in MAGMA [4] for these candidates of T shows that there is no core-free subgroup K of H with $H = KB$ and $|\text{Out}(T)| > |T \cap B|$ for $T \in \{\text{PSL}_2(27), \text{PSL}_3(16)\}$, and that $|\text{Out}(T)| \leq |T \cap B|$ if B is maximal. \square

Before proceeding we need an elementary fact as follows.

Lemma 4.6. *Let $\text{Alt}(m) \leq X \leq \text{Sym}(m)$ for some $m \geq 7$, and let Y be a maximal subgroup of X . Then $|Y \cap \text{Alt}(m)| \geq 3m$.*

Proof. If Y is intransitive on $\{1, \dots, m\}$, then $Y \cap \text{Alt}(m) \cong (\text{Sym}(s) \times \text{Sym}(m-s)) \cap \text{Alt}(m)$, for some $s \in \{1, \dots, m-1\}$, and $|Y \cap \text{Alt}(m)| = s!(m-s)!/2 \geq 3m$.

If Y is transitive and imprimitive on $\{1, \dots, m\}$, then $Y \cap \text{Alt}(m) \cong (\text{Sym}(s) \wr \text{Sym}(m/s)) \cap \text{Alt}(m)$, for some divisor s of m with $1 < s < m$, and $|Y \cap \text{Alt}(m)| = s^{m/s}(m/s)!/2 \geq 3m$.

Now assume Y is primitive on $\{1, \dots, m\}$. If the stabilizer Y_1 of the point 1 is nonabelian, then $|Y_1| \geq 6$ and hence $|Y \cap \text{Alt}(m)| \geq 3m$. If Y_1 is abelian, then the primitivity of Y implies that Y is solvable (see [6, Exercise 3.4.7]). Therefore, $Y \cap \text{Alt}(m) = \text{AGL}_s(p)$ for some integer s and prime p such that $m = p^s$, and so $|Y \cap \text{Alt}(m)| \geq m(m-1)/2 \geq 3m$. \square

A subgroup Y of a group X is said to be \max^+ if Y is maximal and core-free in X , and is said to be \max^- if Y is maximal among core-free subgroups of X . Clearly, \max^+ subgroups of X are necessarily \max^- in X , but the converse is not true.

Lemma 4.7. *Let M be a primitive permutation group of PA type with the notation at the beginning of Section 4.3. Suppose that M has a regular subgroup L of order $|L| > 2^{|G|^{0.4}}$. Then $|T : T_\delta|^\kappa > 2^{(\kappa|T_\delta|^\kappa)^{0.4}}$, and there exists a \max^- subgroup K of H acting transitively on Δ with $|K| > 2^{\frac{1}{\kappa}(\kappa|T_\delta|^\kappa)^{0.4}}$.*

Proof. Since GN/N is a transitive subgroup of $\text{Sym}(\kappa)$, we have $|GN/N| \geq \kappa$, and so $|G| = |GN/N||G \cap N| \geq \kappa|T_\delta|^\kappa$. It follows from $|L| > 2^{|G|^{0.4}}$ that

$$|T : T_\delta|^\kappa = |L| > 2^{|G|^{0.4}} \geq 2^{(\kappa|T_\delta|^\kappa)^{0.4}}.$$

Since $T_\delta \neq 1$, the group L contains no simple direct factor of N . Consider the set \mathcal{K} of core-free subgroups of H that are transitive on Δ . By [29, Theorem 1(i)], $\mathcal{K} \neq \emptyset$. Take a maximal one K in \mathcal{K} . Then K is \max^- in H . Moreover, we derive that

$$|K| \geq |\Delta| = |T : T_\delta| > 2^{\frac{1}{\kappa}(\kappa|T_\delta|^\kappa)^{0.4}},$$

completing the proof. \square

Based on Lemmas 4.5–4.7, we now establish the main result of this section.

Proposition 4.8. *Let G be a finite group with $|G| \geq 2^{57}$. Then $\mathcal{Z}_{\text{PA}}(G) = \emptyset$.*

Proof. Suppose for contradiction that $\mathcal{Z}_{\text{PA}}(G) \neq \emptyset$. Then there exists a critical pair (S, M) of G such that M is primitive of PA type on $[M : G]$ with a regular subgroup L of order $|L| > 2^{|G|^{0.4}}$ (recall (18)). Adopt the notation at the beginning of Section 4.3. By Lemma 4.7, there exists a \max^- subgroup K of H acting transitively on Δ such that

$$|K| > 2^{\frac{1}{\kappa}(\kappa|T_\delta|^\kappa)^{0.4}}. \quad (23)$$

Since K is a transitive subgroup of the primitive group H on Δ , we obtain $H = KH_\delta = TH_\delta$. Observe that as H is primitive, H_δ is \max^+ in H . Let

$$X = KT \cap H_\delta T = KT \cap H = KT.$$

Then $K = K \cap X$, $X_\delta = H_\delta \cap X$, and $X = KX_\delta$. By [28, Theorem], either both K and X_δ are \max^+ in X , or $(T, K \cap T, T_\delta)$ lies in [28, Table 1]. With a case-by-case analysis on the triples $(T, K \cap T, T_\delta)$ in [28, Table 1], we see that $|T : T_\delta|^\kappa < 2^{(\kappa|T_\delta|^\kappa)^{0.4}}$, contradicting Lemma 4.7. Thus both K and X_δ are \max^+ subgroups of X , and so X acts faithfully and primitively by right multiplication on $[X : K]$. Consider this primitive action and let $d = |X : K|$. It follows from [32, Theorem 1.1] that one of the following holds

- (i) $|X| < d^{\lceil \log_2 d \rceil + 1}$;
- (ii) X is M_{11} , M_{12} , M_{23} or M_{24} in their 4-transitive actions;
- (iii) $(\text{Alt}(m))^x \wr X \leq \text{Sym}(m) \wr \text{Sym}(x)$, where $m \geq 5$, $x \geq 1$, and the action of $\text{Sym}(m)$ is on the set of s -subsets of $\{1, \dots, m\}$ for some $1 \leq s \leq m/2$.

We start with case (i). Since X has socle T and $X = KX_\delta$ with X_δ maximal in H , Lemma 4.5 implies that $|\text{Out}(T)| \leq |T_\delta|$, and so

$$|H_\delta| = |T_\delta||H_\delta : T_\delta| \leq |T_\delta||\text{Out}(T)| \leq |T_\delta|^2.$$

Therefore, $|G| \leq |H_\delta| \wr \text{Sym}(\kappa) \leq |T_\delta|^{2\kappa} \cdot \kappa!$ and $d = |X : K| \leq |X_\delta| \leq |H_\delta| \leq |T_\delta|^2$. Combining this with (23) and (i), we deduce that

$$2^{\frac{1}{\kappa}(\kappa|T_\delta|^\kappa)^{0.4}} < |K| = |X|/d < d^{\lceil \log_2 d \rceil} \leq |T_\delta|^{4 \lceil \log_2 |T_\delta| \rceil}. \quad (24)$$

However, as $|T_\delta|^{2\kappa} \cdot \kappa! \geq |G| \geq 2^{57}$, there is no solution for $(\kappa, |T_\delta|)$ in (24), a contradiction.

For each X in case (ii), we have $X = T$, and the pair $(K, T_\delta) = (K, X_\delta)$ can be read off from the classification of factorizations $X = KX_\delta$ with \max^+ subgroups K and X_δ (see [27, Table 6]). However, there is no such pair satisfying (23) as $\kappa \geq 2$, a contradiction.

For the rest of the proof we consider case (iii). Since X is almost simple, we have $\text{Alt}(m) \leq X \leq \text{Sym}(m)$ for some $m \geq 5$, and K is the stabilizer of an s -subset of $\{1, \dots, m\}$ with $1 \leq s \leq m/2$. In particular, $|K| \leq s!(m-s)!$. If $m \leq 9$, then $|K| \leq 8!$ and there is no solution for $(\kappa, |T_\delta|)$ in (23) such that $|T_\delta|^{2\kappa} \cdot \kappa! \geq |G| \geq 2^{57}$, a contradiction. Hence we assume $m \geq 10$. Since K stabilizes an s -subset, we derive from $X = KX_\delta$ that X_δ is s -homogeneous on

$\{1, \dots, m\}$. Suppose that $s \geq 2$. Then, from the maximality of X_δ in X and the classification of s -homogeneous groups [22], we have $|T_\delta| \geq \binom{m}{s}$. Combining this with (23), we obtain that

$$\frac{1}{\kappa} \left(\kappa \binom{m}{s} \right)^{0.4} \leq \frac{1}{\kappa} (\kappa |T_\delta|^\kappa)^{0.4} < \log_2 |K| \leq \log_2 (s! \cdot (m-s)!).$$

However, this holds only if $\kappa = 2$, $s = 2$, $m < 60$ and $|T_\delta| < 2^{11}$. It follows that

$$|G| \leq |H_\delta \wr \text{Sym}(2)| \leq 2(2|T_\delta|)^2 < 2^{25},$$

a contradiction. Therefore, $s = 1$ and we have $\log_2 |K| \leq \log_2((m-1)!) < (m-1) \log_2(m-1)$. Since Lemma 4.6 implies $|T_\delta| \geq 3m$, the inequality (23) yields

$$\frac{1}{\kappa} (\kappa(3m)^\kappa)^{0.4} \leq \frac{1}{\kappa} (\kappa |T_\delta|^\kappa)^{0.4} < \log_2 |K| < (m-1) \log_2(m-1).$$

For $\kappa \geq 3$, this holds only if $\kappa = 3$ and $|T_\delta| < 2^{17}$, which is impossible as $6(2|T_\delta|)^3 \geq |G| \geq 2^{57}$. Consequently, $\kappa = 2$.

So far we have shown that $m \geq 10$, $s = 1$ and $\kappa = 2$. Then $K = X \cap \text{Sym}(m-1)$ and

$$\text{Alt}(m) \wr \text{Sym}(2) \leq M \leq \text{Sym}(m) \wr \text{Sym}(2).$$

For $i \in \{1, 2\}$, let $\pi_i: N \cap L \rightarrow \text{Alt}(m)$ be the projection of $N \cap L$ to the i th factor of the direct product $N = \text{Alt}(m) \times \text{Alt}(m)$, and let $C_i = \pi_i(N \cap L)$.

Suppose that one of π_1 or π_2 , say, π_1 , is surjective. Then as $\text{Ker}(\pi_2) \trianglelefteq C_1 = \text{Alt}(m)$, we obtain $\text{Ker}(\pi_2) = \text{Alt}(m)$ or 1. The former contradicts $L \cap G = 1$. Thus $\text{Ker}(\pi_2) = 1$, that is, π_2 is injective. Moreover, since π_1 is surjective, we derive that $N \cap L$ is a diagonal subgroup of $\text{Alt}(m) \times \text{Alt}(m)$. It follows that $N \cap L$ has point stabilizer isomorphic to $\text{Alt}(m-1)$, contradicting the regularity of L .

Thus neither π_1 nor π_2 is surjective. Note that $|M| \leq 2(m!)^2$ and $|M| = |L||G| > 2^{|G|^{0.4}} \cdot |G|$. If $|G| \geq \binom{m}{2}^2$, then

$$2(m!)^2 > 2^{|G|^{0.4}} \cdot |G| \geq 2^{\binom{m}{2}^{0.8}} \cdot \binom{m}{2}^2,$$

which holds only if $m \leq 146$ and $|G| < 2^{28}$, a contradiction. Hence

$$|G| < \binom{m}{2}^2.$$

In view of $N \cap L \leq C_1 \times C_2$, we obtain

$$\frac{|\text{Alt}(m)|}{|C_1|} \cdot \frac{|\text{Alt}(m)|}{|C_2|} = \frac{|N|}{|C_1 \times C_2|} \leq \frac{|N|}{|N \cap L|} \leq \frac{|M|}{|L|} = |G| < \binom{m}{2}^2.$$

As a consequence, $|\text{Alt}(m) : C_i| < \binom{m}{2}$ for some $i \in \{1, 2\}$, say, $i = 1$. Since π_1 is not surjective, C_1 is a proper subgroup of $\text{Alt}(m)$. Recall $m \geq 10$. According to [6, Theorem 5.2A], the only proper subgroup of $\text{Alt}(m)$ with index less than $\binom{m}{2}$ is $\text{Alt}(m-1)$. Thus

$$C_1 = \text{Alt}(m-1).$$

Since $\text{Ker}(\pi_2) \trianglelefteq C_1$, it follows that $\text{Ker}(\pi_2) = \text{Alt}(m-1)$ or 1. The latter implies $N \cap L \cong C_2$ and then

$$|\text{Alt}(m)| = \frac{|N|}{|\text{Alt}(m)|} \leq \frac{|N|}{|C_2|} = \frac{|N|}{|N \cap L|} \leq \frac{|M|}{|L|} = |G| < \binom{m}{2}^2,$$

which is impossible. Therefore, $\text{Ker}(\pi_2) = \text{Alt}(m-1) = C_1$ and hence

$$C_2/\text{Ker}(\pi_1) \cong C_1/\text{Ker}(\pi_2) = 1.$$

Since $\text{Ker}(\pi_2) \times \text{Ker}(\pi_1) \leq N \cap L \leq C_1 \times C_2$, we conclude that $N \cap L = C_1 \times C_2$. Consequently,

$$1 = G \cap N \cap L = (G \cap N) \cap (N \cap L) = (T_\delta \times T_\delta) \cap (\text{Alt}(m-1) \times C_2),$$

and so $T_\delta \cap \text{Alt}(m-1) = 1$. This means that T_δ acts regularly on $\{1, \dots, m\}$. In particular, T_δ is not maximal in $\text{Alt}(m)$. Since X_δ is maximal in X , we deduce that $X \neq T$, and so $X = \text{Sym}(m)$. Moreover, since $T_\delta \trianglelefteq X_\delta$, the maximality of X_δ in X implies that $X_\delta = \mathbf{N}_X(T_\delta) = T_\delta \rtimes \text{Aut}(T_\delta)$. As $|X_\delta| = 2|T_\delta|$, this yields $|\text{Aut}(T_\delta)| = 2$, and so $|T_\delta| \leq 6$. However, this leads to $|G| \leq 2(2|T_\delta|)^2 \leq 2(2 \cdot 6)^2$, contradicting $|G| \geq 2^{57}$. This completes the proof. \square

4.4. Estimate $|\mathcal{Z}_{\text{CD}}(G)|$. The following result can be extracted from [40, Theorem I], where the constant c in [40, Theorem I] can be chosen to be 1700.

Lemma 4.9 (Pyber-Shalev). *The number of conjugacy classes of primitive subgroups of the symmetric group $\text{Sym}(\ell)$ is at most $2^{1700 \log_2^2 \ell}$.*

Let $S \in \mathcal{Z}_{\text{CD}}(G)$, and let (S, M) be a critical pair such that the action of M on $[M : G]$ is primitive of CD type. Then M is contained in $H \wr \text{Sym}(\kappa)$ endowed with its natural product action on Δ^κ , where $\kappa \geq 2$ and H is a primitive group of SD type on Δ . Thus there is a positive integer ℓ and a nonabelian simple group T such that $|\Delta| = |T|^{\ell-1}$ and

$$T^\ell \leq H \leq T^\ell \cdot (\text{Out}(T) \times \text{Sym}(\ell)).$$

Let Q be the projection of H to $\text{Sym}(\ell)$. Then from the structure of primitive groups of CD type, we derive that

$$n = |G| \geq \kappa |Q| |T|^\kappa \geq \kappa \ell |T|^\kappa.$$

Since $\ell, \kappa \geq 2$ and $|T| \geq 60$, this implies

$$|T| \leq \frac{\sqrt{n}}{2}, \quad \ell \leq \frac{n}{7200}, \quad \kappa \leq \log_{60} \frac{n}{4}. \quad (25)$$

From (18), M_{1+} is regular on $[M : G]$ with $|M_{1+}| > 2^{n^{0.4}}$. We conclude that

$$|T|^{(\ell-1)\kappa} = |\Delta|^\kappa = |M_{1+}| > 2^{n^{0.4}} \geq 2^{(\kappa|Q||T|^\kappa)^{0.4}},$$

which yields

$$\frac{\ell-1}{|Q|^{0.4}} \geq \frac{|T|^{0.4\kappa}}{\kappa^{0.6} \log_2 |T|} > 1,$$

and so $|Q| < \ell^{2.5}$. It is now not hard to prove the next proposition.

Proposition 4.10. *Let G be a finite group of order n . Then*

$$|\mathcal{Z}_{\text{CD}}(G)| < 2^{\frac{3}{4}n + 2 \log_2^4 n + \log_2^3 n + 1702 \log_2^2 n + 2 \log_2 n}.$$

Proof. We adopt the notation established after Lemma 4.9, and let (S, M) be a critical pair with M primitive on $[M : G]$ of CD type. Then there exist T, ℓ, κ satisfying (25) and a primitive group $Q \leq \text{Sym}(\ell)$ with $|Q| < \ell^{2.5}$ such that

$$T^{\ell\kappa} = \text{Soc}(M) =: N \trianglelefteq M \leq W := (T^\ell \cdot (\text{Out}(T) \times Q)) \wr \text{Sym}(\kappa).$$

We first estimate the number of choices for the tuple (T, ℓ, κ, W, M) . Note that at most two nonabelian simple groups, up to isomorphism, have the same order (see [31]). Considering the choices for T, ℓ, κ and Q , we derive from (25) and Lemma 4.9 that there are at most

$$2 \cdot \frac{\sqrt{n}}{2} \cdot \frac{n}{7200} \cdot \left(\log_{60} \frac{n}{4} \right) \cdot 2^{1700 \log_2^2 \ell} < n^2 \cdot 2^{1700 \log_2^2 n} = 2^{1700 \log_2^2 n + 2 \log_2 n} \quad (26)$$

possibilities for the tuple (T, ℓ, κ, W) . Moreover, in view of (25) and Lemma 2.15, we have

$$\begin{aligned} |W : N| &= (|\text{Out}(T)||Q|)^\kappa \cdot \kappa! \leq \left((\log_2 |T|) \cdot \ell^{2.5} \right)^\kappa \cdot \kappa^\kappa \\ &= 2^{\kappa(\log_2(\log_2 |T|) + 2.5 \log_2 \ell + \log_2 \kappa)} < 2^{5\kappa \log_2 n} < 2^{\log_2^2 n}, \end{aligned}$$

where the last two inequalities follow from (rather crude) estimates using (25). For a given pair (N, W) , recall that $M = GN$. Therefore, since G has at most $\log_2 n$ generators, the number of choices for $M = NG$ with $N \leq M \leq W$ is at most $|W/N|^{\log_2 n} \leq 2^{\log_2^3 n}$. Combining this with (26) and recalling that $N = T^{\ell\kappa}$, we conclude that the number of possible tuples (T, ℓ, κ, W, M) is at most $2^{\log_2^3 n + 1700 \log_2^2 n + 2 \log_2 n}$.

Next we fix (T, ℓ, κ, W, M) to estimate the number of choices for M_{1+} . Consider the right multiplication of N on $[N : N_{1+}]$. Let $C = \text{Core}_N(N_{1+})$ so that $N/C \cong T^s$ for some $s \leq \ell\kappa$. Since $|N : N_{1+}| \leq |M : M_{1+}| = n$, the group N/C has a faithful transitive permutation representation on $[N : N_{1+}]$ of degree at most n . By [23, Proposition 5.2.7(ii)], the minimal degree of a faithful transitive permutation representation of T^s is greater than $(\min\{|T|^{1/2}, P(T)\})^s$, where $P(T)$ is the minimal degree of a nontrivial permutation representation of T . Clearly, $\min\{|T|^{1/2}, P(T)\} \geq 5$. Thus $n \geq (\min\{|T|^{1/2}, P(T)\})^s \geq 5^s$ and so $s \leq \log_2 n / \log_2 5$. Note that, for a fixed $s \leq \ell\kappa$, there are at most $\binom{\ell\kappa}{s} < (\ell\kappa)^s$ possibilities for C . Therefore, it follows from (25) that the number of choices for C is at most

$$\frac{\log_2 n}{\log_2 5} \cdot (\ell\kappa)^{\frac{\log_2 n}{\log_2 5}} < \frac{\log_2 n}{2} \cdot 2^{(\log_2 n) \frac{\log_2(\ell\kappa)}{2}} < 2^{(\log_2 n) \left(\frac{\log_2(\ell\kappa)}{2} + 1 \right)} < 2^{\log_2^2 n}. \quad (27)$$

Now fix some $C \trianglelefteq N$ such that $|N/C| = |T|^s$ for some $s \leq \log_2 n / \log_2 5$. Then

$$|M : C| = \frac{|G||M_{1+}|}{|C|} = \frac{n|T|^{(\ell-1)\kappa}}{|T|^{\ell\kappa-s}} < n|T|^s \leq n \left(\frac{\sqrt{n}}{2} \right)^{\frac{\log_2 n}{\log_2 5}} < 2^{\log_2^2 n}.$$

Since $C \leq M_{1+} \leq M$, this together with (27) implies that the number of choices for M_{1+} is less than

$$2^{\log_2^2 n} \cdot |M : C|^{\log_2 |M : C|} < 2^{\log_2^4 n + \log_2^2 n}.$$

Similarly, the number of choices for M_{1-} for a fixed (T, ℓ, κ, W, M) is less than $2^{\log_2^4 n + \log_2^2 n}$. Consequently, the number of possible triples (M, M_{1+}, M_{1-}) is less than

$$2^{\log_2^3 n + 1700 \log_2^2 n + 2 \log_2 n} \cdot 2^{2 \log_2^4 n + 2 \log_2^2 n} = 2^{2 \log_2^4 n + \log_2^3 n + 1702 \log_2^2 n + 2 \log_2 n}.$$

Then the proposition follows immediately from Lemma 2.14. \square

4.5. Estimate $|\mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon)|$. Before exhibiting the main result of this section, we prove two technical lemmas.

Lemma 4.11. *Let (S, M) be an ε -critical pair of a group G of order n , let N be the socle of M , and let $\tau \in \{+, -\}$.*

- (a) *If the primitive type of M on $[M : G]$ is HA, then $|(1_\tau)^N| < n^{0.5+\varepsilon} \log_2 n$.*
- (b) *If the primitive type of M on $[M : G]$ is SD or TW, then $|(1_\tau)^N| < n^{0.5+\varepsilon} \log_2^2 n$.*

Proof. We only prove the result for $\tau = +$, as the argument for $\tau = -$ is the same. Write $u = 1_+$. Then we have

$$|u^N| = |N : N_u| = |N : N \cap M_u| = |NM_u : M_u|. \quad (28)$$

In the following, we discuss the cases $S \in \mathcal{Z}_{\text{HA}}(G)$, $S \in \mathcal{Z}_{\text{YSD}}(G)$ and $S \in \mathcal{Z}_{\text{TW}}(G)$ one by one. Note that in each case we have $|M_u| > 2^{n^{0.5-\varepsilon}}$ from the definition of \mathcal{Z} .

CASE 1: $S \in \mathcal{Z}_{\text{HA}}(G)$.

In this case, $M = N \rtimes G$ with $N = C_p^\ell$ for some prime p and positive integer ℓ , and so $|M_u| = |M : G| = |N| = p^\ell$. Let $H = NM_u \cap G$. Then H is a p -group, and

$$NM_u = NM_u \cap M = NM_u \cap NG = N(NM_u \cap G) = NH = N \rtimes H. \quad (29)$$

Hence (28) turns out to be

$$|u^N| = |NM_u : M_u| = |NH : M_u| = |NH : N| = |H|. \quad (30)$$

If $M_u = N$, then $|u^N| = |u^{M_u}| = |\{u\}| = 1 < n^{0.5+\varepsilon} \log_2 n$. Now suppose that $M_u \neq N$. Then (29) shows that $H \neq 1$, which implies $n = |G| \geq |H| \geq p$. Since H is a p -subgroup of G , there exists a non-identity $x \in N \setminus \{1\}$ fixed by H . Therefore, $H \leq \mathbf{C}_G(x)$. Since G acts irreducibly on N , the set x^G spans N . So we obtain $\ell \leq |x^G| = |G : \mathbf{C}_G(x)| \leq |G : H|$, which means $|H| \leq n/\ell$. Moreover, it follows from $p^\ell = |N| = |M_u| \geq 2^{n^{0.5-\varepsilon}}$ that

$$\ell > \log_p 2^{n^{0.5-\varepsilon}} = \frac{n^{0.5-\varepsilon}}{\log_2 p} \geq \frac{n^{0.5-\varepsilon}}{\log_2 n}.$$

Combining this with (30) and $|H| \leq n/\ell$, we conclude that

$$|u^N| = |H| \leq \frac{n}{\ell} < \frac{n \log_2 n}{n^{0.5-\varepsilon}} = n^{0.5+\varepsilon} \log_2 n.$$

CASE 2: $S \in \mathcal{Z}_{\text{SD}}(G)$.

In this case, $N = T^\ell$ for some nonabelian simple group T and integer $\ell \geq 2$ such that $N \cap G \cong T$ and GN/N is a transitive subgroup of $\text{Sym}(\ell)$. Then $n = |G| \geq \ell|T|$, and

$$|M_u| = |M : G| = |N : N \cap G| = |T|^{\ell-1}.$$

Since [36, Proposition 5.5] implies that $|M_u N| \leq |T|^\ell |\text{Out}(T)|$, we infer from (28) and Lemma 2.15 that

$$|u^N| = |NM_u : M_u| \leq |T| |\text{Out}(T)| \leq |T| \log_2 |T|. \quad (31)$$

As $|T|^\ell > |T|^{\ell-1} = |M_u| \geq 2^{n^{0.5-\varepsilon}}$, we have $\ell > n^{0.5-\varepsilon}/\log_2 |T|$. This combined with (31) and $|T| \leq n/\ell$ leads to

$$|u^N| \leq |T| \log_2 |T| \leq \frac{n}{\ell} \log_2 |T| < \frac{n \log_2^2 |T|}{n^{0.5-\varepsilon}} < n^{0.5+\varepsilon} \log_2^2 n.$$

CASE 3: $S \in \mathcal{Z}_{\text{TW}}(G)$.

In this case, $N = T^\ell$ for some nonabelian simple group T and integer $\ell \geq 6$ such that $|N| = |M : G|$ and GN/N is a transitive subgroup of $\text{Sym}(\ell)$. By [36, Proposition 5.6] we have $|M_u : N \cap M_u| \leq |\text{Aut}(T)|$. Hence (28) and Lemma 2.15 yields that

$$|u^N| = |N : N \cap M_u| = |M_u : N \cap M_u| \leq |\text{Aut}(T)| = |T| |\text{Out}(T)| \leq |T| \log_2 |T|.$$

Note that the induced permutation group P of G on the ℓ direct factors in T^ℓ is a transitive subgroup of $\text{Sym}(\ell)$ with stabilizer $P_1 \cong T$ (see [26]). Thus, we obtain $|G| \geq \ell|T|$ and so $|T| \leq n/\ell$. Then the same argument as in Case 2 leads to $|u^N| < n^{0.5+\varepsilon} \log_2^2 n$, as required. \square

Lemma 4.12. *Let G be a group of order n . For each positive integer t , the number of subsets S of G such that there exist subgroups H and K of G satisfying the following conditions (a)–(c) is at most $2^{n - \frac{n}{4t} + \frac{\log_2^2 n}{2} + 6}$.*

- (a) $\min\{|H|, |K|\} \leq t$;
- (b) either $H \neq K$, or H is not normal in G ;
- (c) $\{(Hg)_+ \mid g \in G\} \cup \{(Kg)_- \mid g \in G\}$ is the set of orbits of some $X \leq \text{Aut}(H(G, S))$.

Proof. Let H and K be subgroups of G satisfying (a)–(c), and write $\Gamma = \mathbf{H}(G, S)$. Let $g \in G$ and $h \in H$. As $(1_+)^H = (1_+)^X$, there exists $x \in X$ such that $(1_+)^h = (1_+)^x$, that is, hx^{-1} fixes 1_+ . Then it follows from (c) that

$$\begin{aligned} |N_\Gamma(1_+) \cap (Kg)_-| &= |(N_\Gamma(1_+) \cap (Kg)_-)^{hx^{-1}}| \\ &= |N_\Gamma((1_+)^{hx^{-1}}) \cap ((Kg)_-)^{hx^{-1}}| = |N_\Gamma(1_+) \cap (Kgh)_-|. \end{aligned}$$

(Observe here that $(Kg)_-^{hx^{-1}} = (Kgh)_-^{x^{-1}}$; moreover, as $x \in X$, we see that x fixes setwise the K -orbit $(Kgh)_-$.) Thus we obtain $|S \cap Kg| = |S \cap Kgh|$ for each $g \in G$ and $h \in H$. Consequently, the intersections between S and the right cosets Kgh of K with $h \in H$ have the same size, and in particular, the same parity. In other words, the intersections between S and different right cosets of K in KgH have the same parity of size. Let $\Delta_1, \dots, \Delta_\kappa$ be the double cosets of K and H in G , and fix a right coset Θ_i of K in Δ_i for each $i \in \{1, \dots, \kappa\}$. Then the intersection of S with each right coset of K in G other than $\Theta_1, \dots, \Theta_\kappa$ must have fixed parity of size. Hence the number of choices for S is at most

$$2^{\kappa|K|} \cdot 2^{(|G:K|-\kappa)(|K|-1)} = 2^{|G|+\kappa-|G:K|}. \quad (32)$$

Similarly, as $(1_-)^K = (1_-)^X$, the intersections between S and different right cosets of H in HgK have the same parity of size, which implies that the number of choices for S is at most $2^{|G|+\kappa-|G:H|}$. Combining this with (32), we deduce that, for fixed H and K , the number of choices for S is at most

$$2^{|G|+\kappa-m},$$

where $m = \max\{|G:H|, |G:K|\}$. Since H and K satisfy (a), we have $m \geq |G|/t$. Moreover, since H and K satisfy (b), by Lemma 2.13, we have $\kappa \leq 3m/4$. Therefore,

$$2^{|G|+\kappa-m} \leq 2^{|G|-\frac{m}{4}} \leq 2^{n-\frac{n}{4t}}.$$

Thus the conclusion of the lemma immediately follows, as there are at most $2^{\frac{\log_2^2 n}{2}+6}$ choices for the pair (H, K) of subgroups of G by Lemma 2.9(c). \square

We are now ready to give the main result of this section.

Proposition 4.13. *Let G be a finite group of order $n \geq 2^{23}$, and let $\varepsilon \in (0, 0.1]$. Then*

$$|\mathcal{Z}_{\text{HA}}(G, \varepsilon) \cup \mathcal{Z}_{\text{SD}}(G, \varepsilon) \cup \mathcal{Z}_{\text{TW}}(G, \varepsilon)| < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 7}.$$

Proof. Let (S, M) be an ε -critical pair of G such that the primitive type of M on $[M:G]$ is HA, SD or TW, and let N be the socle of M . Then M preserves the partition into N -orbits of $G_+ \cup G_-$. Let H and K be the stabilizers in G of $(1_+)^N$ and $(1_-)^N$, respectively. It follows from the semiregularity of G that $|H| = |(1_+)^N|$ and $|K| = |(1_-)^N|$. Thus Lemma 4.11 gives

$$\max\{|H|, |K|\} \leq n^{0.5+\varepsilon} \log_2^2 n. \quad (33)$$

We estimate the number of S in the following two categories:

- (i) S is such that $H = K$ is normal in G ;
- (ii) S is such that either $H \neq K$ or H is not normal in G .

First assume that (i) holds. Then it follows from the definition of H and K that H has the same orbits on $V(\mathbf{H}(G, S))$ as N . In particular, $H \neq 1$. As the inequality $n^{0.5+\varepsilon} \log_2^2 n < n$ holds for $n \geq 2^{23}$, we see from (33) that $H \neq G$. Moreover, since $N \not\leq G$, there is $f \in N \setminus G$ stabilizing each H -orbit on $V(\mathbf{H}(G, S))$. Applying Proposition 3.4 with $t = n^{0.5+\varepsilon} \log_2^2 n$ to the pair (H, f) , we conclude from (33) that the number of S in (i) is at most

$$2^{n - \frac{n}{3n^{0.5+\varepsilon} \log_2^2 n} \log_2\left(\frac{4}{3}\right) + \frac{\log_2^2 n}{4} + \log_2 n + 2 \log_2(n^{0.5+\varepsilon} \log_2^2 n) + 5} < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 6}. \quad (34)$$

Next assume that (ii) holds. Since $(1_+)^H = (1_+)^N$ and $(1_-)^H = (1_-)^N$, it follows that

$$\begin{aligned} \{(Hg)_+ \mid g \in G\} \cup \{(Kg)_- \mid g \in G\} &= \{(1_+)^{Hg} \mid g \in G\} \cup \{(1_-)^{Kg} \mid g \in G\} \\ &= \{(1_+)^{Ng} \mid g \in G\} \cup \{(1_-)^{Ng} \mid g \in G\} \end{aligned}$$

is the set of orbits of N . Then Lemma 4.12 and (33) imply that the number of S in (ii) is at most

$$2^{n - \frac{n}{4n^{0.5+\varepsilon} \log_2^2 n} + \frac{\log_2^2 n}{2} + 6} < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 6}.$$

This together with (34) proves the proposition. \square

5. PROOF OF THEOREMS 1.2 AND 1.3

In this section, we first prove Theorem 1.2 by using the results in Sections 3. Then we apply Theorem 1.2 to show Theorem 1.3, which gives an asymptotic enumeration for HGRs up to isomorphism.

5.1. Proof of Theorem 1.2. First recall Definition 2.4 and Remark 2.5 on odd-quotient digraphs.

Lemma 5.1. *Let G be a finite group, and let C be a normal subgroup of G . Then there are exactly $2^{|G|-|G|/|C|}$ subsets S of G corresponding to the same $\mathsf{H}(G, S)_C^{\text{odd}}$.*

Proof. Let $\mathcal{B} = \{(Cg)_+ \mid g \in G\} \cup \{(Cg)_- \mid g \in G\}$. Then \mathcal{B} is the set of C -orbits on the vertex set of $\mathsf{H}(G, S)$ for every $S \subseteq G$. Note that C_+ is adjacent to $(Cg)_-$ if and only if $|S \cap Cg|$ is odd. By Lemma 2.7, for a fixed $\mathsf{H}(G, S)_C^{\text{odd}}$, there are exactly $(2^{|C|-1})^{|G:C|} = 2^{|G|-|G|/|C|}$ choices for S , as the lemma asserts. \square

Recall also the concept of exceptional pairs and minimally exceptional pairs in Definition 3.1. The following result is crucial in the proof of Theorem 1.2.

Proposition 5.2. *Let $\varepsilon \in (0, 0.1]$, and let n_ε be a positive integer such that (1) holds for all $n \geq n_\varepsilon$. Let G be a finite group of order n . Then the number of subsets S of G such that $\text{Aut}^+(\mathsf{H}(G, S)) > G$ is less than $2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15}$.*

Proof. Since (1) holds, a direct computation shows that $n \geq n_\varepsilon \geq n_{0.1} > 2^{67}$. Let $\mathcal{X}(G) = \{S \subseteq G \mid \text{Aut}^+(\mathsf{H}(G, S)) > G\}$. Then for each $S \in \mathcal{X}(G)$, there exists a minimally exceptional pair (S, M) . Consider the following conditions:

- (C1) $|M| > 2^{n^{0.5-\varepsilon} + \log_2 n}$;
- (C2) $\text{Core}_M(G) = 1$;
- (C3) $|\text{Core}_M(G)| \leq 8 \log_2 n$;
- (C4) no f in $M_{1_+} \setminus G$ stabilizes every $\text{Core}_M(G)$ -orbit on $G_+ \cup G_-$.

For $i \in \{1, 2, 3, 4\}$, we say that (S, M) satisfies condition (Ci) if (Ci) holds, and that (S, M) satisfies condition (\overline{Ci}) if (Ci) does not hold.

Let $\mathcal{Y}(G) = \{S \subseteq G \mid \text{there is a minimally exceptional pair } (S, M) \text{ satisfying } (\overline{C1}) \text{ or } (\overline{C3})\}$. Note that (15) holds as $n > 2^{67}$ and $\varepsilon \in (0, 0.1]$. Applying Propositions 3.6 and 3.7, we obtain

$$|\mathcal{Y}(G)| < 2^{\frac{3}{4}n + n^{1-\varepsilon}} + 2^{n - \frac{n}{4 \log_2 n} \log_2\left(\frac{\varepsilon}{2}\right) + \frac{\log_2^2 n}{4} + \frac{1}{2} \log_2\left(\frac{n}{4 \log_2 n}\right) + \log_2(24)}. \quad (35)$$

Recall from Definition 3.8 that $\mathcal{Z}(G, \varepsilon)$ is the set of $S \subseteq G$ such that there exists a minimally exceptional pair (S, M) satisfying (C1) and (C2). By Proposition 3.9,

$$|\mathcal{Z}(G, \varepsilon)| < 2^{n - \frac{n^{0.5-\varepsilon}}{8 \log_2^2 n} + \frac{\log_2^2 n}{2} + 9}. \quad (36)$$

Hence we only need to estimate the size of $\mathcal{X}(G) \setminus (\mathcal{Y}(G) \cup \mathcal{Z}(G, \varepsilon))$, that is, the number of $S \subseteq G$ such that there exists a minimally exceptional pair (S, M) satisfying (C1), $(\overline{C2})$ and (C3).

Let $S \in \mathcal{X}(G) \setminus (\mathcal{Y}(G) \cup \mathcal{Z}(G, \varepsilon))$, and let (S, M) be a minimally exceptional pair satisfying (C1), $(\overline{C2})$ and (C3). We first estimate the number of S under the assumption that (S, M) satisfies $(\overline{C4})$. Let f be an element of $M_{1+} \setminus G$ stabilizing every $\text{Core}_M(G)$ -orbit on $G_+ \cup G_-$. Then applying Proposition 3.4 with the normal subgroup $\text{Core}_M(G)$ of G and the automorphism f , we derive from (C3) that the number of such subsets S is at most

$$2^{n - \frac{n}{24 \log_2 n} \log_2 \left(\frac{4}{3}\right) + \frac{\log_2^2 n}{4} + \log_2 n + 2 \log_2(8 \log_2 n) + 5}. \quad (37)$$

Now assume that (S, M) satisfies (C4). Write $\Gamma = H(G, S)$ and $C = \text{Core}_M(G)$. Then it is clear from the semiregularity of G on $V(\Gamma)$ that Γ_C^{odd} is a Haar graph of G/C . Thus $\Gamma_C^{\text{odd}} = H(G/C, T)$ for some $T \subseteq G/C$. Since the kernel N of the induced action of M on $V(\Gamma_C^{\text{odd}})$ is contained in $M_{1+}C$ while $M_{1+} \cap G = 1$, it follows from (C4) that $N = C$, and so M/C acts on $V(\Gamma_C^{\text{odd}})$ faithfully. Since every automorphism of Γ induces an automorphism of Γ_C^{odd} , we may regard M/C as a subgroup of $\text{Aut}(\Gamma_C^{\text{odd}})$. Then $(T, M/C)$ is a minimally exceptional pair of G/C , as G is maximal in M . The condition (C1) implies that

$$|M/C| \geq \frac{2^{n^{0.5-\varepsilon} + \log_2 n}}{|C|} = |G:C| \cdot 2^{n^{0.5-\varepsilon}} \geq |G:C| \cdot 2^{|G:C|^{0.5-\varepsilon}}.$$

Moreover, it follows from $C = \text{Core}_M(G)$ that $\text{Core}_{M/C}(G/C) = 1$. Hence $(T, M/C)$ is an ε -critical pair of G/C (recall Definition 3.8), and so $T \in \mathcal{Z}(G/C, \varepsilon)$. Since $n > 2^{67}$ and (C3) gives $|C| \leq 8 \log_2 n$, we have $|G/C| \geq n/(8 \log_2 n) > 2^{57}$. Counting the number of choices for subgroups C of G and the number of $T \in \mathcal{Z}(G/C, \varepsilon)$, we derive from Lemma 2.9(c), Proposition 3.9 and Lemma 5.1 that the number of choices for S is at most

$$\begin{aligned} 2^{\frac{\log_2^2 n}{4} + 3} \cdot |\mathcal{Z}(G/C, \varepsilon)| \cdot 2^{n - \frac{n}{|C|}} &< 2^{\frac{\log_2^2 n}{4} + 3} \cdot 2^{\frac{n}{|C|} - \frac{(n/|C|)^{0.5-\varepsilon}}{8 \log_2^2(n/|C|)} + \frac{\log_2^2(n/|C|)}{2} + 9} \cdot 2^{n - \frac{n}{|C|}} \\ &< 2^{n - \frac{(n/|C|)^{0.5-\varepsilon}}{8 \log_2^2(n/|C|)} + \frac{3 \log_2^2 n}{4} + 12} < 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 12}. \end{aligned}$$

Note that the above upper bound is greater than (37). Accordingly,

$$|\mathcal{X}(G) \setminus (\mathcal{Y}(G) \cup \mathcal{Z}(G, \varepsilon))| < 2 \cdot 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 12} = 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 13}. \quad (38)$$

Since $n > 2^{67}$, the right-hand sides of (35) and (36) are both less than the right-hand side of (38). We conclude that

$$\begin{aligned} |\mathcal{X}(G)| &\leq |\mathcal{Y}(G)| + |\mathcal{Z}(G)| + |\mathcal{X}(G) \setminus (\mathcal{Y}(G) \cup \mathcal{Z}(G, \varepsilon))| \\ &< 3|\mathcal{X}(G) \setminus (\mathcal{Y}(G) \cup \mathcal{Z}(G, \varepsilon))| < 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15}. \end{aligned}$$

This completes the proof. \square

For a subset S of a group, recall that $\mathcal{I}(S)$ is the set of elements in S of order at most 2, and $c(S) = (|S| + |\mathcal{I}(S)|)/2$.

Lemma 5.3. *Let G be a nonabelian permutation group acting semiregularly on $2n$ points with exactly two orbits U and W . Then for each regular group $X > G$, there are at most $2^{7n/8}$ bipartite graphs Γ with bipartition $\{U, W\}$ such that $X \leq \text{Aut}(\Gamma)$.*

Proof. Each bipartite graph Γ with bipartition $\{U, W\}$ such that $X \leq \text{Aut}(\Gamma)$ is a Cayley graph $\text{Cay}(X, S)$ for some inverse-closed subset S of $X \setminus G$. By Lemma 2.12,

$$c(X \setminus G) = \frac{|X \setminus G| + |\mathcal{I}(X \setminus G)|}{2} \leq \frac{1}{2} \left(n + \frac{3n}{4} \right) \leq \frac{7n}{8}.$$

Thus Lemma 2.6 implies that there are at most $2^{c(X \setminus G)} \leq 2^{7n/8}$ choices for the inverse-closed subsets S of $X \setminus G$ and hence for bipartite graphs Γ . \square

We are now in a position to prove Theorem 1.2.

Proof of Theorem 1.2. Recall Definition 2.3 and note that, when G is abelian and $S \subseteq G$, $\text{Aut}(\text{H}(G, S)) = G \rtimes \langle \iota \rangle$ if and only if $\text{Aut}^+(\text{H}(G, S)) = G$. Hence Theorem 1.2(b) immediately follows from Proposition 5.2. Next let G be nonabelian, and let $\mathcal{X}(G) = \{S \subseteq G \mid \text{Aut}(\text{H}(G, S)) > G\}$. Proposition 5.2 gives an upper bound for the size of the subset $\mathcal{Y}(G) := \{S \subseteq G \mid \text{Aut}^+(\text{H}(G, S)) > G\}$ of $\mathcal{X}(G)$. Hence we just need to estimate $|\mathcal{X}(G) \setminus \mathcal{Y}(G)|$. Let $S \in \mathcal{X}(G) \setminus \mathcal{Y}(G)$. Then $\text{Aut}(\text{H}(G, S)) = X$ for some $X > G$ with $|X : G| = 2$ such that X is regular on $V(\text{H}(G, S))$. Since G is normal and maximal in X , the group X can be determined by an element of $\mathbf{N}_{\text{Sym}(2n)}(G)$. Observe that since G is semiregular with 2 orbits, we have $|\mathbf{C}_{\text{Sym}(n)}(C)| = 2|G|^2 = 2n^2$. Now Lemma 2.9(b) implies that

$$\begin{aligned} |\mathbf{N}_{\text{Sym}(2n)}(G)| &= |\mathbf{C}_{\text{Sym}(2n)}(G)| \cdot |\text{Aut}(G)| \\ &= 2n^2 \cdot |\text{Aut}(G)| \leq 2n^2 \cdot 2^{\log_2^2 n} \leq 2^{\log_2^2 n + 2 \log_2 n + 1}. \end{aligned}$$

Hence there are at most $2^{\log_2^2 n + 2 \log_2 n + 1}$ choices for $X > G$ with $|X : G| = 2$. Combining this with Lemma 5.3, we deduce that

$$|\mathcal{X}(G) \setminus \mathcal{Y}(G)| \leq 2^{\frac{7n}{8} + \log_2^2 n + 2 \log_2 n + 1}.$$

Together with Proposition 5.2, we conclude that

$$\begin{aligned} |\mathcal{X}(G)| &= |\mathcal{Y}(G)| + |\mathcal{X}(G) \setminus \mathcal{Y}(G)| \leq 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15} + 2^{\frac{7n}{8} + \log_2^2 n + 2 \log_2 n + 1} \\ &< 2^{n - \frac{n^{0.5-\varepsilon}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 16}, \end{aligned}$$

proving Theorem 1.2(a). \square

5.2. Unlabeled Haar graphs. For a group G , let $\mathcal{H}(G)$ be the set of Haar graphs of G up to isomorphism. Elements of $\mathcal{H}(G)$ are called *unlabelled* Haar graphs of G , and in contrast, we call a Haar graph $\text{H}(G, S)$ *labeled* to indicate that it is not counted up to isomorphism. In this section, we prove Theorem 1.3, which indicates that, up to isomorphism, almost all Haar graphs of a finite group have the smallest possible automorphism group. We first give the following lemma.

Lemma 5.4. *Let G be a finite group of order n .*

- (a) *If G is nonabelian, then there are at most $2^{\log_2^2 n + 2 \log_2 n + 1}$ labeled HGRs of G isomorphic to each other.*
- (b) *If G is abelian, then there are at most $2^{\log_2^2(2n) + 2 \log_2 n + 1}$ labeled Haar graphs of G isomorphic to each other such that they have automorphism group $G \rtimes \langle \iota \rangle$.*

Proof. When $n = 1$, the result is clear. Thus we suppose $n > 1$.

First assume that G is nonabelian. Fix a subset S of G such that $\text{H}(G, S)$ is an HGR. To prove (a), we show that there are at most $2^{\log_2^2 n + 2 \log_2 n + 2}$ subsets T of G such that $\text{H}(G, T)$ is isomorphic to $\text{H}(G, S)$. Let T be such a subset, and write $\Gamma = \text{H}(G, S)$ and $\Sigma = \text{H}(G, T)$. Then there exists a graph isomorphism φ from Γ to Σ , and the mapping $\psi: g \mapsto \varphi^{-1}g\varphi$, for each $g \in G$, is a group isomorphism from $\text{Aut}(\Gamma)$ to $\text{Aut}(\Sigma)$. Since $N_\Gamma(1_+) = S_-$, we have

$$N_\Sigma((1_+)^\varphi) = (S_-)^\varphi. \quad (39)$$

Let $(1_+)^{\varphi} = x_{\epsilon}$ and $(1_-)^{\varphi} = y_{\mu}$ for some $x, y \in G$ and $\epsilon, \mu \in \{+, -\}$. Since $\text{Aut}^+(\Gamma) = \text{Aut}^+(\Sigma) = G$ and $|G| = n > 1$, both the bipartite graphs Γ and Σ are connected, and so the partition $\{G_+, G_-\}$ is preserved by φ . This implies that $\mu = -\epsilon$. Then (39) yields that

$$N_{\Sigma}(x_{\epsilon}) = N_{\Sigma}((1_+)^{\varphi}) = (S_-)^{\varphi} = (1_-)^{S\varphi} = (1_-)^{\varphi\varphi^{-1}S\varphi} = (y_{-\epsilon})^{\varphi^{-1}S\varphi} = (y_{-\epsilon})^{S^{\psi}},$$

where $S^{\psi} = \{s^{\psi} \mid s \in S\}$. Thus $(T^{\epsilon 1}x)_{-\epsilon} = N_{\Sigma}(x_{\epsilon}) = (y_{-\epsilon})^{S^{\psi}}$, and so T is uniquely determined by (ϵ, x, y, ψ) . Considering the choices for (ϵ, x, y, ψ) , we conclude from $\text{Aut}(\Gamma) = \text{Aut}(\Sigma) = G$ and Lemma 2.9(b) that the number of choices for T is at most

$$2 \cdot n^2 \cdot 2^{\log_2^2 n} = 2^{\log_2^2 n + 2 \log_2 n + 1},$$

proving (a).

Next assume that G is abelian. Fix a subset S of G such that $\text{Aut}(\text{H}(G, S)) = G \rtimes \langle \iota \rangle$. We enumerate the subsets T of G such that $\text{H}(G, T)$ is isomorphic to $\text{H}(G, S)$. By the notation and similar argument as above (note that $|\text{Aut}(\Gamma)| = 2n$ in this case), there are at most

$$2 \cdot n^2 \cdot 2^{\log_2^2(2n)} = 2^{\log_2^2(2n) + 2 \log_2 n + 1}$$

choices for T , which proves (b). \square

We conclude this section by proving Theorem 1.3.

Proof of Theorem 1.3. Use the notation established at the beginning of Section 5.2, and let $\mathcal{HGR}(G)$ be the set of HGRs of G up to isomorphism. First assume that G is nonabelian. To prove Theorem 1.3(a), we need to estimate the ratio $|\mathcal{HGR}(G)|/|\mathcal{H}(G)|$. Let

$$a_{\epsilon}(n) = \frac{n^{0.5-\epsilon}}{24(\log_2 n)^{2.5}} - \frac{3 \log_2^2 n}{4} - 15 \quad \text{and} \quad b(n) = \log_2^2 n + 2 \log_2 n + 1.$$

Then Theorem 1.2(a) and Lemma 5.4(a) imply that

$$|\mathcal{H}(G) \setminus \mathcal{HGR}(G)| < 2^{n-a_{\epsilon}(n)} \quad \text{and} \quad |\mathcal{HGR}(G)| > \frac{2^n - 2^{n-a_{\epsilon}(n)}}{2^{b(n)}}.$$

Hence we deduce from $|\mathcal{H}(G)| = |\mathcal{H}(G) \setminus \mathcal{HGR}(G)| + |\mathcal{HGR}(G)|$ that

$$\frac{|\mathcal{H}(G)|}{|\mathcal{HGR}(G)|} = 1 + \frac{|\mathcal{H}(G) \setminus \mathcal{HGR}(G)|}{|\mathcal{HGR}(G)|} < 1 + \frac{2^{n+b(n)-a_{\epsilon}(n)}}{2^n - 2^{n-a_{\epsilon}(n)}} = 1 + \frac{2^{b(n)-a_{\epsilon}(n)}}{1 - 2^{-a_{\epsilon}(n)}},$$

which yields

$$\begin{aligned} \frac{|\mathcal{HGR}(G)|}{|\mathcal{H}(G)|} &= \left(\frac{|\mathcal{H}(G)|}{|\mathcal{HGR}(G)|} \right)^{-1} > \frac{1 - 2^{-a_{\epsilon}(n)}}{1 - 2^{-a_{\epsilon}(n)} + 2^{b(n)-a_{\epsilon}(n)}} \\ &= 1 - \frac{2^{b(n)-a_{\epsilon}(n)}}{1 + 2^{b(n)-a_{\epsilon}(n)} - 2^{-a_{\epsilon}(n)}} > 1 - 2^{b(n)-a_{\epsilon}(n)}. \end{aligned}$$

Since $b(n) - a_{\epsilon}(n) = -\frac{n^{0.5-\epsilon}}{24(\log_2 n)^{2.5}} + \frac{7 \log_2^2 n}{4} + 2 \log_2 n + 16 < -h_{\epsilon}(n)$, Theorem 1.3(a) follows.

Next assume that G is abelian. Let $\mathcal{A}(G)$ be the set of Haar graphs of G up to isomorphism that have automorphism group $G \rtimes \langle \iota \rangle$. By an argument similar to the one above and applying Theorem 1.2(b) and Lemma 5.4(b), we obtain that

$$\frac{|\mathcal{A}(G)|}{|\mathcal{H}(G)|} > 1 - 2^{(\log_2^2(2n) + 2 \log_2 n + 1) - \left(\frac{n^{0.5-\epsilon}}{24(\log_2 n)^{2.5}} - \frac{3 \log_2^2 n}{4} - 14 \right)} = 1 - 2^{-h_{\epsilon}(n)},$$

as Theorem 1.3(b) asserts. \square

6. ASYMPTOTIC ENUMERATION OF m -CAYLEY DIGRAPHS

For an m -Cayley digraph $\text{Cay}(G, \mathcal{S})$ of a group G , set $G_i = \{(g, i) \mid g \in G\}$ for $i \in \{1, \dots, m\}$. Since G acts transitively on each G_i , each vertex in G_i has the same out-valency and the same in-valency, denoted as $d_i^+(\mathcal{S})$ and $d_i^-(\mathcal{S})$, respectively. In this section, we prove the conclusion of Theorem 1.7 for digraphs, which shows that almost all m -Cayley digraphs of a finite group G are DmSRs.

Proposition 6.1. *Fix an integer $m \geq 2$, and let G be a finite group of order n . When n is sufficiently large, the number of set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a DmSR is less than $m^2 \cdot 2^{m^2 n} / \sqrt{n}$.*

Proof. Let \mathcal{Z} be the set of set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a DmSR. We first estimate the size of

$$\mathcal{Z}_1 := \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

Note that, if a vertex of G_i is mapped by some automorphism of $\text{Cay}(G, \mathcal{S})$ into G_j , then $d_i^+(\mathcal{S}) = d_j^+(\mathcal{S})$ and $d_i^-(\mathcal{S}) = d_j^-(\mathcal{S})$. This means that, for any $\mathcal{S} \in \mathcal{Z}_1$, there exists a pair (i, j) with $i < j$ such that

$$d_i^+(\mathcal{S}) + d_i^-(\mathcal{S}) = d_j^+(\mathcal{S}) + d_j^-(\mathcal{S}). \quad (40)$$

Now, fix (i, j) with $i < j$ satisfying (40). Clearly,

$$\begin{aligned} d_i^+(\mathcal{S}) &= |S_{i,i}| + |S_{i,j}| + \sum_{k \neq i,j} |S_{i,k}|, & d_i^-(\mathcal{S}) &= |S_{i,i}| + |S_{j,i}| + \sum_{k \neq i,j} |S_{k,i}|, \\ d_j^+(\mathcal{S}) &= |S_{j,j}| + |S_{j,i}| + \sum_{k \neq i,j} |S_{j,k}|, & d_i^-(\mathcal{S}) &= |S_{j,j}| + |S_{i,j}| + \sum_{k \neq i,j} |S_{k,j}|. \end{aligned}$$

Substituting these into (40), we obtain

$$2|S_{i,i}| + \sum_{k \neq i,j} (|S_{i,k}| + |S_{k,i}|) = 2|S_{j,j}| + \sum_{k \neq i,j} (|S_{j,k}| + |S_{k,j}|).$$

This indicates that the size of $S_{i,i}$ is determined by $S_{k,\ell}$ with $(k, \ell) \neq (i, i)$. Hence, we derive from Lemma 2.8 that the number of \mathcal{S} satisfying (40) is at most

$$2^{(m^2-1)n} \cdot \frac{2^n}{\sqrt{n}} = \frac{2^{m^2 n}}{\sqrt{n}}.$$

Since there are $\binom{m}{2}$ choices for (i, j) with $i < j$, we conclude that

$$|\mathcal{Z}_1| \leq \binom{m}{2} \frac{2^{m^2 n}}{\sqrt{n}}. \quad (41)$$

By the definition of \mathcal{Z}_1 , every $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1$ is such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each G_i and hence induces a subgroup A_i of $\text{Aut}(\text{Cay}(G, S_{i,i}))$ on G_i . Let

$$\mathcal{Z}_2 = \{\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1 \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } A_i \not\cong G\}.$$

Then we derive from Theorem 1.4 that

$$|\mathcal{Z}_2| \leq m \cdot 2^{(m^2-1)n} \cdot 2^{n - \frac{bn^{0.499}}{4 \log_2^3 n} + 2} = m \cdot 2^{m^2 n - \frac{bn^{0.499}}{4 \log_2^3 n} + 2}, \quad (42)$$

where b is an absolute constant.

Now consider $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$. It follows from $\mathcal{S} \notin \mathcal{Z}_1 \cup \mathcal{Z}_2$ and $\text{Aut}(\text{Cay}(G, \mathcal{S})) > G$ that the action of $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ on each G_i has kernel $K_i > 1$. Take an arbitrary i . Then there exists j distinct from i such that K_i acts nontrivially on G_j . This implies that $S_{i,j}$ is a union of some K_i -orbits on G_j . Since $A_j \cong G$ acts regularly on G_j , the action of K_i on

G_j is semiregular, and so there are at most $n/2$ orbits of K_i on G_j . Hence we derive from Lemma 2.9(c) that the choices of $S_{i,j}$ is at most $2^{\log_2^2 n} \cdot 2^{n/2}$. Consequently,

$$|\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| \leq 2^{(m^2-m)n} \cdot \left((m-1) \cdot 2^{\log_2^2 n + \frac{n}{2}} \right)^m = (m-1)^m \cdot 2^{m^2 n - \frac{mn}{2} + m \log_2^2 n}. \quad (43)$$

Noting $m \geq 2$ and combining (41)–(43), we obtain for sufficiently large n that

$$|\mathcal{Z}| = |\mathcal{Z}_1| + |\mathcal{Z}_2| + |\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| < m^2 \frac{2^{m^2 n}}{\sqrt{n}},$$

which completes the proof. \square

Proof of Theorem 1.7 for digraphs. Since G has order n , there are exactly $2^{m^2 n}$ set-matrices of G . Thus, by Proposition 6.1, the proportion of set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is a $DmSR$ is greater than

$$1 - \frac{m^2 \cdot 2^{m^2 n} / \sqrt{n}}{2^{m^2 n}} = 1 - m^2 / \sqrt{n}. \quad \square$$

7. ASYMPTOTIC ENUMERATION OF m -CAYLEY GRAPHS

In this section, we prove Theorem 1.7 for graphs, which implies that almost all m -Cayley graphs of a finite group G are $GmSRs$. We divide the proof into three cases in the following three subsections, respectively, which will be summarized at the end of the section to complete the proof. Recall the notations $c(\mathcal{S})$ and $\mathcal{I}(\mathcal{S})$ in Section 2.3.

Recall that a digraph $\text{Cay}(G, \mathcal{S})$ is undirected if and only if \mathcal{S} is inverse-closed (see Definition 2.1). Such a set-matrix $\mathcal{S} = (S_{i,j})_{m \times m}$ is uniquely determined by the subsets $S_{i,j}$ for $1 \leq i < j \leq m$ and the inverse-closed subsets $S_{i,i}$ for $i \in \{1, \dots, m\}$. So the number of inverse-closed set-matrices \mathcal{S} of G is 2^d , where

$$d = \binom{m}{2} |G| + mc(G).$$

For an m -Cayley graph $\text{Cay}(G, \mathcal{S})$, set $G_i = \{(g, i) \mid g \in G\}$ for $i \in \{1, \dots, m\}$. Since G acts transitively on each G_i , every vertex of G_i has the same valency, denoted as $d_i(\mathcal{S})$.

Lemma 7.1. *Fix an integer $m \geq 2$. Let G be a group of order n . Then the number of inverse-closed set-matrices \mathcal{S} of G such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ does not stabilize G_i for some $i \in \{1, \dots, m\}$ is at most $m(m-1)2^d / \sqrt{n}$, where $d = \binom{m}{2}n + mc(G)$.*

Proof. Let \mathcal{Z} be the set of inverse-closed set-matrices \mathcal{S} of G such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ does not stabilize G_i for some $i \in \{1, \dots, m\}$. Note that, if a vertex of G_i is mapped by some automorphism of $\text{Cay}(G, \mathcal{S})$ into G_j , then $d_i(\mathcal{S}) = d_j(\mathcal{S})$. This means that, for any $\mathcal{S} \in \mathcal{Z}_1$, there exists a pair (i, j) with $i < j$ such that $d_i(\mathcal{S}) = d_j(\mathcal{S})$. Now, fix (i, j) with $i < j$ that satisfies $d_i(\mathcal{S}) = d_j(\mathcal{S})$. Then

$$|S_{i,i}| + |S_{i,j}| + \sum_{k \neq i,j} |S_{i,k}| = d_i(\mathcal{S}) = d_j(\mathcal{S}) = |S_{j,j}| + |S_{j,i}| + \sum_{k \neq i,j} |S_{j,k}|.$$

For a subset X of G , denote $\mathcal{N}(X) = X \setminus \mathcal{I}(X)$. Since $S_{i,j} = S_{j,i}^{-1}$, the equation above becomes

$$|\mathcal{I}(S_{i,i})| + |\mathcal{N}(S_{i,i})| + \sum_{k \neq i,j} |S_{i,k}| = |S_{j,j}| + \sum_{k \neq i,j} |S_{j,k}|. \quad (44)$$

When G is not an elementary abelian 2-group, the equation (44) indicates that the size of $\mathcal{N}(S_{i,i})$ is determined by $\mathcal{I}(S_{i,i})$ and $S_{k,\ell}$ with $(k, \ell) \neq (i, i)$. In this case, we derive from

Lemmas 2.8 and 2.11 that the number of \mathcal{S} satisfying (44) is at most

$$\frac{2^d}{2^{c(G)}} \cdot 2^{|\mathcal{I}(G)|} \cdot \frac{2^{|\mathcal{N}(G)|}}{\sqrt{|\mathcal{N}(G)|}} = \frac{2^d}{\sqrt{|\mathcal{N}(G)|}} \leq \frac{2^d}{\sqrt{n/4}} = \frac{2^{d+1}}{\sqrt{n}}.$$

When G is an elementary abelian 2-group, we have $\mathcal{I}(S_{i,i}) = S_{i,i}$ and $\mathcal{N}(S_{i,i}) = \emptyset$, and so (44) implies that the size of $S_{i,i}$ is determined by the sets $S_{k,\ell}$ with $(k,\ell) \neq (i,i)$. In this case, the number of \mathcal{S} satisfying (44) is at most

$$\frac{2^d}{2^{c(G)}} \cdot \frac{2^{c(G)}}{\sqrt{c(G)}} = \frac{2^d}{\sqrt{c(G)}} = \frac{2^d}{\sqrt{n}} < \frac{2^{d+1}}{\sqrt{n}}.$$

Since there are $\binom{m}{2}$ choices for (i,j) with $i < j$, summing up the two cases, we conclude that

$$|\mathcal{Z}| \leq \binom{m}{2} \frac{2^{d+1}}{\sqrt{n}} = m(m-1) \frac{2^d}{\sqrt{n}},$$

as the lemma asserts. \square

7.1. m -Cayley graphs on abelian groups. In this section, we concentrate on the case when the group is abelian with exponent greater than 2. We first present a useful result and give a technical lemma as follows.

Theorem 7.2. ([8, Theorem 1.7]) *Let G be an abelian group of order n , and let ι be the automorphism of G defined by $\iota: g \mapsto g^{-1}$ for every $g \in G$. Then the number of inverse-closed subsets S such that $\text{Aut}(\text{Cay}(G, S)) \neq G \rtimes \langle \iota \rangle$ is at most $2^{c(G)-n/24+2 \log_2^2 n+2}$.*

Lemma 7.3. *Let G be an abelian group of exponent greater than 2, and let ι be the automorphism of G defined by $\iota: g \mapsto g^{-1}$ for every $g \in G$. Then for each non-identity $b \in G \rtimes \langle \iota \rangle$, the number of orbits of $\langle b \rangle$ on G is at most $5|G|/6$.*

Proof. Since G is abelian and of exponent greater than 2, we may assume $G = C_k \times H$ for some $k > 2$ and subgroup H . Note that, if $x \in G$ is fixed by $g\iota$, then

$$x = x^{g\iota} = (xg)^\iota = g^{-1}x^{-1},$$

which implies $x \in \{y \mid y^2 = g^{-1}\}$. Moreover, we consider the homomorphism $\psi: G \rightarrow \{g^2 \mid g \in G\}$, which maps g to g^2 . As $k > 2$, the image $\psi(G)$ has size at least $k/2$. So, we obtain

$$|\text{Ker}(\psi)| = \frac{|G|}{|\psi(G)|} \leq \frac{2|G|}{k} \leq \frac{2}{3}|G|.$$

This implies that $|\text{Fix}(g\iota)| \leq \frac{2}{3}|G|$. Hence the number of orbits of $\langle g\iota \rangle$ on G is at most

$$|\text{Fix}(g\iota)| + \frac{|G| - |\text{Fix}(g\iota)|}{2} = \frac{|G| + |\text{Fix}(g\iota)|}{2} \leq \frac{5}{6}|G|,$$

as the lemma asserts. \square

We conclude this section with the following proposition.

Proposition 7.4. *Fix an integer $m \geq 2$, and let G be an abelian group with exponent greater than 2 and order n . When n is sufficiently large, the number of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a Gm SR is less than $m^2 2^d / \sqrt{n}$, where $d = \binom{m}{2}n + mc(G)$.*

Proof. Let \mathcal{Z} be the set of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a Gm SR. By Lemma 7.1, the size of the set

$$\mathcal{Z}_1 := \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

is at most $m(m-1)2^d/\sqrt{n}$. By the definition of \mathcal{Z}_1 , every $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1$ is such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each G_i and hence induces a subgroup A_i of $\text{Aut}(\text{Cay}(G, S_{i,i}))$ on G_i . Let

$$\mathcal{Z}_2 = \{\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1 \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } A_i \neq G \times \langle \iota \rangle\}.$$

Then we derive from Theorem 7.2 that

$$|\mathcal{Z}_2| \leq m \cdot \frac{2^d}{2^{c(G)}} \cdot 2^{c(G) - \frac{n}{24} + 2 \log_2^2 n + 2} = m \cdot 2^{d - \frac{n}{24} + 2 \log_2^2 n + 2}. \quad (45)$$

Now consider

$$\mathcal{Z}_3 = \{\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2) \mid \text{Aut}(\text{Cay}(G, \mathcal{S})) \neq G \times \langle \iota \rangle\}.$$

Take $\mathcal{S} \in \mathcal{Z}_3$. It follows from $\mathcal{S} \notin \mathcal{Z}_1 \cup \mathcal{Z}_2$ and $\text{Aut}(\text{Cay}(G, \mathcal{S})) \neq G \times \langle \iota \rangle$ that the action of $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ on each G_i has kernel $K_i > 1$. In particular, there exists $j \in \{2, \dots, m\}$ such that some element of K_1 induces a nontrivial action $\alpha_{1j} \in G \times \langle \iota \rangle$ on G_j . It follows that $S_{1,j}$ is a union of some $\langle \alpha_{1j} \rangle$ -orbits on G_j . Moreover, according to Lemma 7.3, there are at most $5n/6$ orbits of $\langle \alpha_{1j} \rangle$ on G_j . Hence we deduce that the number of choices for $S_{1,j}$ is at most $2n \cdot 2^{5n/6}$. Consequently,

$$|\mathcal{Z}_3| \leq (m-1) \frac{2^d}{2^n} \cdot 2n \cdot 2^{\frac{5}{6}n} \leq (m-1) 2^{d - \frac{n}{6} + \log_2 n + 1}. \quad (46)$$

Finally, we estimate the cardinality of $\mathcal{Z}_4 := \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \mathcal{Z}_3)$. Let $\mathcal{S} \in \mathcal{Z}_4$. Then $\text{Aut}(\text{Cay}(G, \mathcal{S})) = G \times \langle \iota \rangle$. Clearly, the automorphism ι keeps each 1_i invariant for each $i \in \{1, \dots, m\}$. Thus, for any pair (i, j) with $i < j$, the subset $S_{i,j}$ is a union of $\langle \iota \rangle$ -orbits on G_j . Since $\langle \iota \rangle$ has $c(G)$ orbits on G , and Lemma 2.11 implies $c(G) = (|G| + |\mathcal{I}(G)|)/2 \leq 7n/8$, we derive that that

$$|\mathcal{Z}_4| = 2^{mc(G)} \cdot \left(2^{c(G)}\right)^{\frac{m(m-1)}{2}} = 2^d \cdot (2^{c(G)-n})^{\frac{m(m-1)}{2}} \leq 2^d \cdot \left(2^{-\frac{n}{8}}\right)^{\frac{m(m-1)}{2}} = 2^{d - \frac{m(m-1)}{16}n}. \quad (47)$$

Combining $|\mathcal{Z}_1| \leq m(m-1)2^d/\sqrt{n}$ and (45)–(47), we obtain for sufficiently large n that

$$|\mathcal{Z}| = |\mathcal{Z}_1| + |\mathcal{Z}_2| + |\mathcal{Z}_3| + |\mathcal{Z}_4| < m^2 \frac{2^d}{\sqrt{n}},$$

which completes the proof. \square

7.2. m -Cayley graphs on generalised dicyclic groups. Let A be an abelian group of even order and of exponent greater than 2, and let y be an involution of A . The *generalised dicyclic group* $\text{Dic}(A, y, x)$ is the group $\langle A, x \mid x^2 = y, a^x = a^{-1}, \forall a \in A \rangle$. In this section, we establish asymptotic results for m -Cayley graphs of $\text{Dic}(A, y, x)$. The conclusions are divided into Propositions 7.8 and 7.12, addressing two cases based on $\text{Dic}(A, y, x) \cong Q_8 \times C_2^\ell$ or not, where C_2^ℓ is an elementary abelian 2-group. Let us start with the case $\text{Dic}(A, y, x) \cong Q_8 \times C_2^\ell$.

Notation 7.5. Let $G = Q_8 \times E$ with $E = C_2^\ell$ for some $\ell \geq 0$, and we label the element of Q_8 with $\{1, -1, \mathbf{i}, -\mathbf{i}, \mathbf{j}, -\mathbf{j}, \mathbf{k}, -\mathbf{k}\}$ in the usual way. Define the following permutations of G : for $\mathbf{u} \in \{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, $\alpha_{\mathbf{u}}$ is the involution which swaps $\mathbf{u}e$ and $-\mathbf{u}e$ for every $e \in E$ while fixes every other element of G . Let $M(G) = \langle G, \iota_{\mathbf{i}}, \iota_{\mathbf{j}}, \iota_{\mathbf{k}} \rangle$, viewed as a permutation group on G with G acting regularly on itself by right multiplication.

We need the following asymptotic result and technical lemma.

Theorem 7.6. [38, Theorems 1.6] *Let $G, M(G)$ as in Notation 7.5 and $|G| = n$. Then the number of inverse-closed subsets S of G such that $\text{Aut}(\text{Cay}(G, S)) \neq M(G)$ is at most $2^{c(G) - n/512 + 2 \log_2^2 n + 2}$.*

Lemma 7.7. *Let $G = Q_8 \times E$ and $M(G)$ as in Notation 7.5. Then for any non-identity element $s \in M(G)$, the number of orbits of $\langle s \rangle$ on G is at most $7|G|/8$.*

Proof. Let $\alpha = \iota_{\mathbf{i}}$, $\beta = \iota_{\mathbf{j}}$ and $\gamma = \iota_{\mathbf{k}}$. Since $|M(G):G| = 8$ (see [38, Lemma 4.3]), and α, β, γ commute pairwise, the group $M(G)$ has the coset decomposition

$$M(G) = \bigcup_{i,j,k \in \{0,1\}} G\alpha^i\beta^j\gamma^k.$$

It is straightforward to verify that

$$\begin{aligned} \text{Fix}(qe\alpha^i\beta^j\gamma^k) &= \emptyset \text{ for each } q \in Q_8 \text{ and non-identity } e \in E, \\ \text{Fix}(q\alpha^i\beta^j\gamma^k) \cap ((Q_8 \setminus \{\pm 1\}) \times E) &= \emptyset \text{ for each non-identity } q \in Q_8, \\ \text{Fix}(\alpha\beta^j\gamma^k) \cap (\{\pm\alpha\} \times E) &= \emptyset, \\ \text{Fix}(\alpha^i\beta\gamma^k) \cap (\{\pm\beta\} \times E) &= \emptyset, \\ \text{Fix}(\alpha^i\beta^j\gamma) \cap (\{\pm\gamma\} \times E) &= \emptyset. \end{aligned}$$

This implies that for any $s \in M(G)$ with $s \neq 1$, the fixed point ratio $|\text{Fix}(s)|/|G|$ on G is at most $3/4$. Thus, the number of orbits of $\langle s \rangle$ on G is at most $7|G|/8$, as the lemma asserts. \square

We are now ready to prove the asymptotic result for m -Cayley graphs of $Q_8 \times C_2^\ell$.

Proposition 7.8. *Fix an integer $m \geq 2$, and let $G = Q_8 \times C_2^\ell$ with order n . When n is sufficiently large, the number of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a GmSR is less than $m^2 2^d / \sqrt{n}$, where $d = \binom{m}{2}n + mc(G)$.*

Proof. We use Notation 7.5. Let \mathcal{Z} be the set of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a GmSR, and let

$$\mathcal{Z}_1 = \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

By Lemma 7.1, the cardinality of \mathcal{Z}_1 satisfies

$$|\mathcal{Z}_1| \leq m(m-1)2^d / \sqrt{n}. \quad (48)$$

By the definition of \mathcal{Z}_1 , every $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1$ is such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each G_i and hence induces a subgroup A_i of $\text{Aut}(\text{Cay}(G, S_{i,i}))$ on G_i . Let

$$\mathcal{Z}_2 = \{\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1 \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } A_i \not\cong M(G)\}.$$

Then we derive from Theorem 7.6 that

$$|\mathcal{Z}_2| \leq m \cdot \frac{2^d}{2^{c(G)}} \cdot 2^{c(G) - \frac{n}{512} + 2 \log_2^2 n + 2} = m \cdot 2^{d - \frac{n}{512} + 2 \log_2^2 n + 2}. \quad (49)$$

Now consider $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$. As $\text{Aut}(\text{Cay}(G, \mathcal{S})) > G$, we have $\text{Aut}(\text{Cay}(G, \mathcal{S}))_x > 1$ for any $x \in G_1$. Moreover, since $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$, there exists $j \in \{2, \dots, m\}$ such that some element of $\text{Aut}(\text{Cay}(G, \mathcal{S}))_x$ induces a nontrivial permutation $\alpha_j \in M(G)$ on G_j . Hence $S_{1,j}$ is a union of some $\langle \alpha_j \rangle$ -orbits on G_j . On the other hand, according to Lemma 7.7, there are at most $7n/8$ orbits of $\langle \alpha_j \rangle$ on G_j . Hence we deduce that the number of choices of $S_{1,j}$ is at most $2n \cdot 2^{7n/8}$. Consequently,

$$|\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| \leq (m-1) \frac{2^d}{2^n} \cdot 2n \cdot 2^{7n/8} \leq (m-1) 2^{d - \frac{n}{8} + \log_2 n + 1}. \quad (50)$$

Combining (48)–(50), we obtain for sufficiently large n that

$$|\mathcal{Z}| = |\mathcal{Z}_1| + |\mathcal{Z}_2| + |\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| < m^2 \frac{2^d}{\sqrt{n}},$$

which completes the proof. \square

In the rest of this section, we handle the case $\text{Dic}(A, y, x) \not\cong Q_8 \times C_2^\ell$.

Notation 7.9. Let $G = \text{Dic}(A, y, x)$ be a generalised dicyclic group such that $G \not\cong Q_8 \times C_2^\ell$, where Q_8 is the quaternion group. Let ι be the automorphism of G fixing A pointwise and mapping every element of $G \setminus A$ to its inverse, and let $M(G) = G \rtimes \langle \iota \rangle$.

Similarly, we need the following asymptotic result and technical lemma.

Theorem 7.10. ([38, Theorems 1.5]) *Let $G = \text{Dic}(A, y, x)$ be a generalised dicyclic group of order n such that $G \not\cong Q_8 \times C_2^\ell$ for any $\ell \geq 0$. Then the number of inverse-closed subsets S of G with $\text{Aut}(\text{Cay}(G, S)) \neq M(G)$ is at most $2^{c(G)-n/48+2\log_2^2 n+5}$.*

Lemma 7.11. *Let $G = \text{Dic}(A, y, x)$ be a generalised dicyclic group such that $G \not\cong Q_8 \times C_2^\ell$. Then for each non-identity $s \in M(G)$, the number of orbits of $\langle s \rangle$ on G is at most $3|G|/4$.*

Proof. Note that $M(G) = G \cup G\iota$ and $G = A \cup Ax$. It is straightforward to verify that

$$\begin{aligned} \text{Fix}(g) &= \emptyset \text{ for each } g \in G, \\ \text{Fix}(ax\iota) \cap Ax &= \emptyset \text{ for each } a \in A, \\ \text{Fix}(a\iota) \cap A &= \emptyset \text{ for each non-identity } a \in A, \\ \text{Fix}(\iota) \cap Ax &= \emptyset. \end{aligned}$$

This implies that for each $s \in M(G)$, we have $|\text{Fix}(s)| \leq |G|/2$. Hence the number of orbits of $\langle s \rangle$ on G is at most

$$|\text{Fix}(s)| + \frac{|G| - |\text{Fix}(s)|}{2} = \frac{|G| + |\text{Fix}(s)|}{2} \leq \frac{3}{4}|G|,$$

as the lemma asserts. \square

We close this section with the following proposition.

Proposition 7.12. *Fix an integer $m \geq 2$. Let G be a generalised dicyclic group of order n such that $G \not\cong Q_8 \times C_2^\ell$ for each $\ell \geq 0$. When n is sufficiently large, the number of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a $GmSR$ is less than $m^2 2^d / \sqrt{n}$, where $d = \binom{m}{2}n + mc(G)$.*

Proof. Let $\mathcal{Z} = \{\mathcal{S} \mid \mathcal{S} \text{ is inverse-closed, } \text{Aut}(\text{Cay}(G, \mathcal{S})) > G\}$ and let

$$\mathcal{Z}_1 = \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

By Lemma 7.1, the cardinality of \mathcal{Z}_1 satisfies

$$|\mathcal{Z}_1| \leq m(m-1)2^d / \sqrt{n}. \quad (51)$$

By the definition of \mathcal{Z}_1 , every $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1$ is such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each G_i and hence induces a subgroup A_i of $\text{Aut}(\text{Cay}(G, S_{i,i}))$ on G_i . Let

$$\mathcal{Z}_2 = \{\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1 \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } A_i \not\cong M(G)\}.$$

Then we derive from Theorem 7.10 that

$$|\mathcal{Z}_2| \leq m \cdot \frac{2^d}{2^{c(G)}} \cdot 2^{c(G) - \frac{n}{48} + 2\log_2^2 n + 5} = m \cdot 2^{d - \frac{n}{48} + 2\log_2^2 n + 5}. \quad (52)$$

Now consider $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$. As $\text{Aut}(\text{Cay}(G, \mathcal{S})) \neq G$, it holds $\text{Aut}(\text{Cay}(G, \mathcal{S}))_v > 1$ for any $v \in G_1$. Moreover, since $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$, there exists $j \in \{2, \dots, m\}$ such that some element of $\text{Aut}(\text{Cay}(G, \mathcal{S}))_v$ induces a nontrivial permutation $\alpha_j \in M(G)$ on G_j . Hence $S_{1,j}$ is a union of some $\langle \alpha_j \rangle$ -orbits on G_j . According to Lemma 7.11, there are at most $3n/4$ orbits of $\langle \alpha_j \rangle$ on G_j . Hence we derive that the choices of $S_{1,j}$ is at most $|M(G)| \cdot 2^{3n/4} = 2n \cdot 2^{3n/4}$. Consequently,

$$|\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| \leq (m-1) \frac{2^d}{2^n} \cdot 2n \cdot 2^{\frac{3}{4}n} \leq (m-1) 2^{d - \frac{n}{4} + \log_2 n + 1}. \quad (53)$$

Combining (51)–(53), we obtain for sufficiently large n that

$$|\mathcal{Z}| = |\mathcal{Z}_1| + |\mathcal{Z}_2| + |\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| < m^2 \frac{2^d}{\sqrt{n}},$$

which completes the proof. \square

7.3. m -Cayley graphs on other groups. In view of Sections 7.1 and 7.2, we are left to deal with the case that G is neither abelian with exponent greater than 2 nor generalised dicyclic.

Proposition 7.13. *Fix an integer $m \geq 2$. Let G be a group of order n such that G is neither abelian of exponent greater than 2 nor generalised dicyclic. When n is sufficiently large, the number of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a $GmSR$ is less than $m^2 2^d / \sqrt{n}$, where $d = \binom{m}{2}n + mc(G)$.*

Proof. Let $\mathcal{Z} = \{\mathcal{S} \mid \mathcal{S} \text{ is inverse-closed, } \text{Aut}(\text{Cay}(G, \mathcal{S})) > G\}$. We first estimate the size of

$$\mathcal{Z}_1 := \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

Since there are $\binom{m}{2}$ choices for (i, j) with $i < j$, we derive from Lemma 7.1 that

$$|\mathcal{Z}_1| \leq m(m-1)2^d / \sqrt{n}. \quad (54)$$

By the definition of \mathcal{Z}_1 , every $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1$ is such that $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each G_i and hence induces a subgroup A_i of $\text{Aut}(\text{Cay}(G, S_{i,i}))$ on G_i . Let

$$\mathcal{Z}_2 = \{\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Z}_1 \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } A_i \not\cong G\}.$$

Then we derive from Theorem 1.6 and Lemma 2.6 that

$$|\mathcal{Z}_2| \leq m \cdot \frac{2^d}{2^{c(G)}} \cdot 2^{c(G) - \frac{n^{0.499}}{8 \log_2^3 n} + \log_2^2 n + 3} = m \cdot 2^{d - \frac{n^{0.499}}{8 \log_2^3 n} + \log_2^2 n + 3}. \quad (55)$$

Now consider $\mathcal{S} \in \mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)$. It follows from $\mathcal{S} \notin \mathcal{Z}_1 \cup \mathcal{Z}_2$ and $\text{Aut}(\text{Cay}(G, \mathcal{S})) > G$ that the action of $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ on each G_i has kernel $K_i > 1$. In particular, there exists $j \in \{2, \dots, m\}$ such that K_1 acts nontrivially on G_j . It follows that $S_{1,j}$ is a union of some K_1 -orbits on G_j . Since $A_j \cong G$ acts regularly on G_j , the action of K_1 on G_j is semiregular, and so there are at most $n/2$ orbits of K_1 on G_j . Hence we derive from Lemma 2.9(c) that the choices of $S_{1,j}$ is at most $2^{\log_2^2 n} \cdot 2^{n/2}$. Consequently,

$$|\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| \leq (m-1) \frac{2^d}{2^n} \cdot 2^{\log_2^2 n + \frac{n}{2}} \leq (m-1) 2^{d - \frac{n}{2} + \log_2^2 n}. \quad (56)$$

Combining (54)–(56), we obtain for sufficiently large n that

$$|\mathcal{Z}| = |\mathcal{Z}_1| + |\mathcal{Z}_2| + |\mathcal{Z} \setminus (\mathcal{Z}_1 \cup \mathcal{Z}_2)| < m^2 \frac{2^d}{\sqrt{n}},$$

which completes the proof. \square

Proof of Theorem 1.7 for graphs. As stated at the beginning of this section, there are exactly 2^d inverse-closed set-matrices of G , where $d = \binom{m}{2}n + mc(G)$. Combining this with Propositions 7.4, 7.8, 7.12 and 7.13, we conclude that the proportion of inverse-closed set-matrices \mathcal{S} of G such that $\text{Cay}(G, \mathcal{S})$ is not a $GmSR$ is less than

$$\frac{m^2 2^d / \sqrt{n}}{2^d} = m^2 / \sqrt{n}. \quad \square$$

8. m -PARTITE GRAPHICAL SEMIREGULAR REPRESENTATIONS

Recall from Definition 2.1 that a set-matrix $\mathcal{S} = (S_{i,j})_{m \times m}$ is skew if it is inverse-closed and $S_{i,i} = \emptyset$ for each $i \in \{1, \dots, m\}$. Such a set-matrix $\mathcal{S} = (S_{i,j})_{m \times m}$ is uniquely determined by the subsets $S_{i,j}$ for $1 \leq i < j \leq m$, and so there are exactly 2^d skew set-matrices of G , where $d = \binom{m}{2}n$.

Proof of Theorem 1.8. Write $d = \binom{m}{2}n$, and let \mathcal{Z} be the set of skew set-matrices \mathcal{S} of G such that $\text{Aut}(\text{Cay}(G, \mathcal{S})) > G$. Let

$$\mathcal{Y} := \{\mathcal{S} \in \mathcal{Z} \mid \text{there exists } i \in \{1, \dots, m\} \text{ such that } \text{Aut}(\text{Cay}(G, \mathcal{S})) \text{ does not stabilize } G_i\}.$$

Observe that if a vertex of G_i is mapped by some automorphism of $\text{Cay}(G, \mathcal{S})$ into G_j , then $d_i(\mathcal{S}) = d_j(\mathcal{S})$. This means that, for each $\mathcal{S} \in \mathcal{Y}$, there exists a pair (i, j) with $i < j$ such that $d_i(\mathcal{S}) = d_j(\mathcal{S})$. Fix some (i, j) with $i < j$ that satisfies $d_i(\mathcal{S}) = d_j(\mathcal{S})$. Then

$$|S_{i,j}| + \sum_{k \neq i,j} |S_{i,k}| = d_i(\mathcal{S}) = d_j(\mathcal{S}) = |S_{j,i}| + \sum_{k \neq i,j} |S_{j,k}|. \quad (57)$$

Take $x \in \{1, \dots, m\} \setminus \{i, j\}$. Then (57) indicates that the size of $S_{i,x}$ is determined by the sets $S_{k,\ell}$ with $(k, \ell) \neq (i, x)$. We derive from Lemma 2.8 that the number of \mathcal{S} satisfying (57) is at most $2^{d-n} \cdot 2^n / \sqrt{n} = 2^d / \sqrt{n}$. Since there are $\binom{m}{2}$ choices for (i, j) with $i < j$, we deduce that

$$|\mathcal{Y}| \leq \binom{m}{2} \frac{2^d}{\sqrt{n}}. \quad (58)$$

Now consider $\mathcal{S} \in \mathcal{Z} \setminus \mathcal{Y}$. Note that for each pair (i, j) , the parts G_i and G_j induce the Haar graph $H(G, S_{i,j})$. Since $\text{Aut}(\text{Cay}(G, \mathcal{S}))$ stabilizes each part and $\text{Aut}(\text{Cay}(G, \mathcal{S})) > G$, there exists a pair (i, j) with $i < j$ such that $\text{Aut}^+(H(G, S_{i,j})) > G$. Applying Proposition 5.2 with $\varepsilon = 0.1$, we obtain that, when n is sufficiently large, there are at most

$$2^{n - \frac{n^{0.4}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15}$$

choices for $S_{i,j}$. Counting the choices for (i, j) with $i < j$, we conclude that

$$|\mathcal{Z} \setminus \mathcal{Y}| \leq \binom{m}{2} 2^{d-n} \cdot 2^{n - \frac{n^{0.4}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15} = \binom{m}{2} 2^{d - \frac{n^{0.4}}{24(\log_2 n)^{2.5}} + \frac{3 \log_2^2 n}{4} + 15}.$$

This together with (58) yields that, for sufficiently large n ,

$$|\mathcal{Z}| = |\mathcal{Y}| + |\mathcal{Z} \setminus \mathcal{Y}| < m^2 \frac{2^d}{\sqrt{n}}.$$

Since there are exactly 2^d skew set-matrices of G , the theorem follows. \square

ACKNOWLEDGMENTS

The first author was supported by the China Scholarship Council (202306370173). The work was done during a visit of the first author to The University of Melbourne.

REFERENCES

- [1] M. Arezoomand, A. Abdollahi and P. Spiga, On problems concerning fixed-point-free permutations and on the polycirculant conjecture—a survey, *Trans. Comb.* 8 (2019), no. 1, 15–40.
- [2] L. Babai, Finite digraphs with given regular automorphism groups, *Period. Math. Hung.* 11 (1980), 257–270.
- [3] L. Babai and C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* 3 (1982), 9–15.
- [4] W. Bosma, J. Cannon and C. Playoust, The magma algebra system I: The user language, *J. Symbolic Comput.* 24 (1997), 235–265.

- [5] M. Conder, I. Estélyi and T. Pisanski, Vertex-transitive Haar graphs that are not Cayley graphs, *Discrete geometry and symmetry*, 61–70, *Springer Proc. Math. Stat.*, 234, Springer, Cham, 2018.
- [6] J. D. Dixon and B. Mortimer, *Permutation groups*, Springer-Verlag, New York, (1996).
- [7] T. Dobson, On automorphisms of Haar graphs of abelian groups, *Art Discrete Appl. Math.* 5 (2022), no. 3, Paper No. 3.06, 22 pp.
- [8] E. Dobson, P. Spiga and G. Verret, Cayley graphs on abelian groups, *Combinatorica* 36 (2016), 371–393.
- [9] S. F. Du and M. Y. Xu, A classification of semisymmetric graphs of order $2pq$, *Comm. Algebra* 28 (2000), 2685–2715.
- [10] J.-L. Du, Y.-Q. Feng and P. Spiga, A classification of the graphical m -semiregular representation of finite groups, *J. Combin. Theory, Ser. A* 171 (2020).
- [11] J.-L. Du, Y.-Q. Feng and P. Spiga, On Haar digraphical representations of groups, *Discrete Math.* 343 (2020), 6 pp.
- [12] A. L. Edmonds and Z. B. Norwood, Finite groups with many involutions, <https://arxiv.org/abs/0911.1154v1>.
- [13] I. Estélyi and T. Pisanski, Which Haar graphs are Cayley graphs?, *Electron. J. Combin.*, 23 (2016), no. 3, Paper 3.10, 13 pp.
- [14] Y.-Q. Feng, I. Kovács, J. Wang and D.-W. Yang, Existence of non-Cayley Haar graphs, *European J. Combin.* 89 (2020), 12 pp.
- [15] Y.-Q. Feng, I. Kovács and D.-W. Yang, On groups all of whose Haar graphs are Cayley graphs, *J. Algebraic Combin.*, 52 (2020), no. 1, 59–76.
- [16] M. Fusari and P. Spiga, On the maximum number of subgroups of a finite group, *J. Algebra*, 635 (2023), 486–526.
- [17] M. Giudici, C. H. Li and C. E. Praeger, Analysing finite locally s -arc transitive graphs, *Trans. Amer. Math. Soc.* 356 (2004), no. 1, 291–317.
- [18] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* 1 (1981), 243–256.
- [19] S. Guest, J. Morris, C. E. Praeger and P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* 367 (2015), 7665–7694.
- [20] M. Hladnik, D. Marušič and T. Pisanski, Cyclic Haar graphs, *Discrete Math.* 244 (2002), no. 1-3, 137–152.
- [21] W. Imrich, Graphical regular representations of groups of odd order, in: *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976) Vol. II, Colloq. Math. Soc. János Bolayi*, 18 (1978), 611–621.
- [22] W. M. Kantor, k -homogenous groups, *Math. Z.* 124 (1972), 261–265.
- [23] P. B. Kleidman and M. W. Liebeck, *The subgroup structure of the finite classical groups*, Cambridge University Press, Cambridge, 1990.
- [24] H. Koike and I. Kovács, Isomorphic tetravalent cyclic Haar graphs, *Ars Math. Contemp.* 7 (2014), no. 1, 215–235.
- [25] H. Liebeck and D. MacHale, Groups with automorphisms inverting most elements, *Math. Z.* 124 (1972), 51–63.
- [26] M. W. Liebeck, C. E. Praeger and J. Saxl, On the O’Nan–Scott theorem for finite primitive permutation groups, *J. Austral. Math. Soc.* 44 (1988), 389–396.
- [27] M. W. Liebeck, C. E. Praeger and J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Mem. Amer. Math. Soc.* 86 (1990).
- [28] M. W. Liebeck, C. E. Praeger and J. Saxl, On factorizations of almost simple groups, *J. Algebra* 185 (1996), 409–416.
- [29] M. W. Liebeck, C. E. Praeger and J. Saxl, Transitive subgroups of primitive permutation groups, *J. Algebra* 234 (2000), 291–361.
- [30] M. W. Liebeck, C. E. Praeger and J. Saxl, Regular subgroups of primitive permutation groups, *Mem. Amer. Math. Soc.* 203 (2010).
- [31] A. Lubotzky, Enumerating boundedly Generated Finite Groups, *J. Algebra* 238 (2001), 194–199.
- [32] A. Maróti, On the orders of primitive groups, *J. Algebra* 258 (2002), 631–640.
- [33] D. Marušič, On vertex symmetric digraphs, *Discrete Math.* 36 (1981), 69–81.
- [34] B.D. McKay and C.E. Praeger, Vertex-transitive graphs which are not Cayley graphs, I, *J. Austral. Math. Soc. Ser. A* 56 (1994), no. 1, 53–63.
- [35] J. Morris, M. Moscatiello and P. Spiga, On the asymptotic enumeration of Cayley graphs, *Ann. Mat. Pura Appl.* 201 (2022), 1417–1461.
- [36] J. Morris and P. Spiga, Asymptotic enumeration of Cayley digraphs, *Israel J. Math.* 242 (2021), 401–459.
- [37] J. Morris and P. Spiga, Haar graphical representations of finite groups and an application to poset representations, <https://arxiv.org/abs/2404.12658>.
- [38] J. Morris, P. Spiga and G. Verret, Automorphisms of Cayley graphs on generalised dicyclic groups, *European J. Combin.* 43 (2015), 68–81.

- [39] L. A. Nowitz and M. E. Watkins, Graphical regular representations of non-abelian groups. I, II, *Canadian J. Math.*, 24 (1972), 993–1018.
- [40] L. Pyber and A. Shalev, Asymptotic results for primitive permutation groups, *J. Algebra* 188 (1997), 103–124.
- [41] C. E. Praeger, Finite quasiprimitive graphs, *Surveys in Combinatorics*, 1997 (London), Cambridge Univ. Press, (1997), 65–85.
- [42] H. Robbins, A remark on Stirling’s formula, *Amer. Math. Monthly* 62 (1955), 26–29.
- [43] 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), no. 1, 1–10.
- [44] P. Spiga, Finite transitive groups having many suborbits of cardinality at most 2 and an application to the enumeration of Cayley graphs, *Canad. J. Math.* 76 (2024), no. 1, 345–366.
- [45] K. Stefan, A bound on the order of the outer automorphism group of finite simple group of given order, <https://stefan-kohl.github.io/preprints/outbound.pdf>.
- [46] B. Xia and S. Zheng, Asymptotic enumeration of graphical regular representations, *Proc. London Math. Soc.*(3) 127 (2023), 1424–1450.

(GAN) SCHOOL OF MATHEMATICS AND STATISTICS, CENTRAL SOUTH UNIVERSITY, CHANGSHA, HUNAN, 410083, P.R. CHINA

Email address: `songsirr@126.com`

(SPIGA) DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, UNIVERSITY OF MILANO-BICOCCA, VIA COZZI 55, 20125 MILANO, ITALY

Email address: `pablo.spiga@unimib.it`

(XIA) SCHOOL OF MATHEMATICS AND STATISTICS, THE UNIVERSITY OF MELBOURNE, PARKVILLE, VIC 3010, AUSTRALIA

Email address: `binzhoux@unimelb.edu.au`