ASYMPTOTIC ENUMERATION OF CAYLEY DIGRAPHS

JOY MORRIS AND PABLO SPIGA

Abstract. In this paper we show that almost all Cayley digraphs have automorphism group as small as possible; that is, they are digraphical regular representations (DRRs). More precisely, we show that as r tends to infinity, for every finite group R of order r, out of all possible Cayley digraphs on R the proportion whose automorphism group is as small as possible tends to 1. This proves a natural conjecture first proposed in 1982 by Babai and Godsil.

1. Introduction

1.1. **Background and significance.** All digraphs and groups considered in this paper are finite. By a *digraph* Γ, we mean an ordered pair (V, A) where the *vertex-set* V is a finite non-empty set and the *arc-set* $A \subseteq V \times V$ is a binary relation on V. The elements of V and A are called *vertices* and *arcs* of Γ, respectively. An *automorphism* of Γ is a permutation σ of V that preserves the relation A, that is, $(x^\sigma, y^\sigma) \in A$ for every $(x, y) \in A$.

Let R be a group and let S be a subset of R. The *Cayley digraph* on R with connection set S, denoted $\Gamma(R, S)$, is the digraph with vertex-set R and with (g, h) being an arc if and only if $hg^{-1} \in S$. Note that we do not require our Cayley digraphs to be connected and that they may have loops. It is an easy observation that R acts regularly as a group of automorphisms of $\Gamma(R, S)$ by right multiplication and hence $R \leq \mathrm{Aut}(\Gamma(R, S))$.

Although we have just seen that the definition of a Cayley digraph forces the automorphism group of such a digraph to contain a group acting regularly, there is nothing in the definition that tells us whether or not such a digraph has any other automorphisms. When considering questions of structure and isomorphism, determining the full automorphism group of a digraph is a very important question. In the case of a Cayley digraph on a group R, a major first step in finding the answer to this question is to determine whether R is in fact the full automorphism group of this digraph. When it is, $\Gamma(R, S)$ is called a *DRR* (for digraphical regular representation).

In addition to the value of determining the full automorphism group of Cayley digraphs, DRRs are of considerable interest in that such a digraph provides a visual representation of the group on which it was defined. In this way, for example, the cyclic group of order n can be introduced as the group of symmetries of a directed n-gon.

Babai and Godsil made the following conjecture.

Conjecture 1.1 ([14], Conjecture 3.13; [4]). *Let R be a group of order r. The proportion of subsets S of R such that $\Gamma(R, S)$ is a* DRR *goes to* 1 *as $r \to \infty$.*

In other words, almost all Cayley digraphs are DRRs, in the sense that

$$\lim_{|R| \to \infty} \frac{|\{S \subseteq R \mid \mathrm{Aut}(\Gamma(R, S)) = R\}|}{2^{|R|}} = 1.$$

Godsil showed that Conjecture 1.1 holds if G is a p-group with no homomorphism onto the wreath product $\mathrm{C}_p \,\mathrm{wr}\, \mathrm{C}_p$ [14], and Babai and Godsil extended this to verify the conjecture in the case that G is nilpotent of odd order [4, Theorem 2.2]. This paper gives a proof of the full Conjecture 1.1 of Babai and Godsil.

Theorem 1.2. *Let R be a group of order r. The proportion of subsets S of R such that $\Gamma(R, S)$ is a* DRR *goes to* 1 *as $r \to \infty$.*

Actually, we prove a quantified version of this result, which might have some independent interest and might be useful in some applications.

Theorem 1.3. *Let R be a group of order r, where r is sufficiently large. The number of subsets S of R such that $\Gamma(R, S)$ is not a* DRR *is at most $2^{r - br^{0.499}/(4(\log_2(r))^3)+2}$, where b is an absolute constant that does not depend on R.*

This quantified version makes it clear that our results also resolve the directed version of Xu's conjecture about normal Cayley graphs. (A normal Cayley (di)graph $\Gamma(R, S)$ is a Cayley (di)graph having the property that $R \trianglelefteq \mathrm{Aut}(\Gamma(R, S))$, so every DRR is a normal Cayley digraph.)

2010 *Mathematics Subject Classification.* 05C25, 05C30, 20B25, 20B15.

Key words and phrases. regular representation, Cayley graph, automorphism group, asymptotic enumeration, graphical regular representation, DRR, GRR.

Supported in part by the National Science and Engineering Research Council of Canada. Address correspondence to P. Spiga, E-mail: pablo.spiga@unimib.it.

Theorem 1.4 (Conjecture 1, [46])**.** *The minimum over all groups R of order r of the proportion of subsets S of R such that $\Gamma(R,S)$ is a normal Cayley digraph tends to 1 as $r\to\infty$.*

It is well-known that almost all graphs (and almost all digraphs) are asymmetric. The graph version of this result (which is more difficult than the digraph version) follows from Pólya enumeration (or Burnside's counting lemma), as is mentioned in [13] without proof. A full proof along these lines is given in [17]; such a proof can also be found in [15, Section 2.3]. An alternative proof derives from work by Erdös and Rényi [12], who obtained formulas for the number of graphs of order n admitting a given permutation of degree n as an automorphism (the formulas depend on the number of fixed points of the permutation); combining these formulas over all possible permutations implies that almost all graphs of order n are asymmetric.

This makes the Babai-Godsil conjecture (and hence our theorem) very natural: nature seems to be typically meagre and rarely gives more than is truly necessary. Thus, even though the digraph $\Gamma(R,S)$ is constructed in such a way as to force it to contain R in its automorphism group, only exceptionally does $\Gamma(R,S)$ admit any extra automorphisms (beyond those that have been forced by the construction).

Let $\mathrm{CD}(R)$ denote the set of Cayley digraphs over R up to isomorphism and let $\mathrm{DRR}(R)$ denote the set of DRRs over R up to isomorphism. We also provide a proof of the following unlabelled version of Theorem 1.2. Formally, $\mathrm{CD}(R)$ is a set of representatives for the equivalent relation on $\{\Gamma(R,S)\mid S\subset R\}$ given by being isomorphic, and $\mathrm{DRR}(R)$ consists of the elements of $\mathrm{CD}(R)$ which are DRRs.

Theorem 1.5. *Let R be a group of order r. Then $|\mathrm{DRR}(R)|/|\mathrm{CD}(R)|$ tends to 1 as $r\to\infty$.*

1.2. Notation, and outline of the proof of Theorem 1.2.

Given a group G and $g\in G$, we write $o(g)$ for the order of g.

Throughout this paper, we denote by $\mathrm{Sym}(r)$ and by $\mathrm{Sym}(\Omega)$ the symmetric group of degree r and the symmetric group on the set Ω. We will use the first notation when the underlying point set is irrelevant for our investigation, and we will use the second notation otherwise. Moreover, we let R denote a group of order r. We identify R with its image in $\mathrm{Sym}(r)$ via the right regular representation. In particular, $R\le\mathrm{Sym}(r)$.

In Section 2 we present important reductions from the work of Babai and Godsil [4, Section 4] that are also needed in our proof. Since our needs are slightly different from theirs, our statements also differ, so we present full proofs of our statements.

In Section 3, Lemma 3.1 shows that the problem of enumerating the subsets S of R with $\mathrm{Aut}(\Gamma(R,S))=R$ reduces to obtaining an upper bound for the number of subgroups G of $\mathrm{Sym}(r)$ with $R<G$ and with R maximal in G. Under this reduction, G is filling the role of a possible subgroup of the full automorphism group for some Cayley digraph on R. We use this correspondence in several of our results, to pass from counting such groups G, to counting subsets S of R such that $\mathrm{Aut}(\Gamma(R,S))$ contains some subgroup G with R maximal in G and other specified attributes.

In the first significant result of this type, we use a rather deep result of Lubotzky [25] to show that the number of subsets S such that $\mathrm{Aut}(\Gamma(R,S))$ admits such a G where $|G|$ is "small" (that is, $|G:R|$ is at most $2^{r^{0.499}}$, say) is $2^{f(r)}$ for some function $f(r)$ such that $f(r)-r\to-\infty$ as $r\to\infty$, so that $2^{f(r)}$ is a vanishingly small proportion of all possible connection sets. This leaves us the problem of considering groups G with $|G:R|$ rather large.

Given G with $R<G\le\mathrm{Sym}(r)$, we denote by G_R the core of R in G, that is, $G_R=\bigcap_{g\in G}R^g$. Now, since R is maximal in G, we can view G/G_R as a primitive permutation group with stabiliser R/G_R. We are able to show that the number of subsets S of a given group R such that $\mathrm{Aut}(\Gamma(R,S))$ admits such a G where $|G|$ is "large" ($|G:R|$ is greater than $2^{r^{0.499}}$, say) and the order of the core G_R is "large" (greater than $4\log_2(|R|)$) is also a vanishingly small proportion of all possible connection sets. Again (to be more precise) we show that this number is $2^{f(r)}$ for some function $f(r)$ such that $f(r)-r\to-\infty$ as $r\to\infty$.

This leaves us needing to deal with counting the connection sets S such that every such $|G|$ is "large" but in all cases, the core G_R is "small". This is the heart of this paper, and comprises a majority of the content. In order to deal with this situation, we divide these connection sets up according to two main cases. We establish these cases and provide some groundwork in Section 4. In Section 5 we deal with the case where there is a G with $G_R=1$ so that G is acting faithfully and primitively on the set of right cosets of R in G. Our analysis involves case-by-case study of the various types of primitive permutation groups according to the O'Nan-Scott classification. Then in Section 6 we deal with the case where there is a G with $G_R>1$. In such a case we can define a particular type of quotient graph that allows us to establish a bound based on the previously discussed cases. The fact that the previous situations produced vanishingly small proportions of non-DRRs implies that the new case also produces a vanishingly small proportion of non-DRRs.

1.3. Some key ideas, and outline of the end of the paper.

In what follows we use repeatedly the following facts.

Remark 1.6.

(1) Let X be a finite group. Since a chain of subgroups of X has length at most $\log_2(|X|)$, X has a generating set of cardinality at most $\lfloor\log_2(|X|)\rfloor\le\log_2(|X|)$.

(2) Any automorphism of X is uniquely determined by its action on the elements of a generating set for X. Therefore $|\mathrm{Aut}(X)|\le|X|^{\lfloor\log_2(|X|)\rfloor}\le 2^{(\log_2(|X|))^2}$.

(3) Let g be a permutation of the finite set Ω and take $\Delta := \{\omega \in \Omega \mid \omega^g = \omega\}$. Then g fixes each point of Δ and the cycles of g on $\Omega \setminus \Delta$ have length at least 2. Therefore g fixes setwise at most $2^{|\Delta|+\frac{|\Omega\setminus\Delta|}{2}}$ subsets of Ω. In particular, if $|\Delta| \le |\Omega|/2$, then g fixes setwise at most $2^{\frac{3}{4}|\Omega|}$ subsets of Ω.

After the proof of Theorem 1.2 is completed at the end of Section 6.2, we turn to the case of unlabelled digraphs and explain in Section 7 how Theorem 1.2 implies the corresponding result Theorem 1.5 for unlabelled digraphs.

We conclude the paper with additional remarks about our proof strategy and other possible generalisations; these form Section 8.

2. Babai–Godsil estimates: first reduction

The argument in this section is completely inspired by, and in part taken from [4, Section 4]. For most of the arguments in this section we could simply refer to [4, Section 4], however the hypotheses there are slightly stronger than our current needs. Therefore, rather than pointing out which parts in [4, Section 4] need to be refined (and how to refine them), for the sake of completeness we make this section self-contained and repeat some parts of the results of [4, Section 4].

Henceforth, let R be a regular permutation group acting on $\{1,\dots,r\}$. Let N denote a non-identity proper normal subgroup of R. Let $n := |N|$ and $b := |R : N| = r/n$. We let $\gamma_1,\dots,\gamma_b$ be coset representatives of N in R. Moreover, we choose $\gamma_1 := 1$ to be the identity in R. Observe that R/N defines a group structure on $\{1,\dots,b\}$ by setting $ij = k$ for every $i,j,k \in \{1,\dots,b\}$ with $\gamma_i N \gamma_j N = \gamma_k N$.

Write $v_0 := 1$ where v_0 has to be understood as a point in the set $\{1,\dots,r\}$. For each $i \in \{1,\dots,b\}$, set $\mathcal{O}_i := {v_0}^{\gamma_i N}$. Observe that the $\mathcal{O}_i$s are the orbits of N on $\{1,\dots,r\}$, the group N acts regularly on $\mathcal{O}_i$ and $|\mathcal{O}_i| = |N| = n$.

For a subset S of R, we let $\Gamma := \Gamma(R,S)$ be the Cayley digraph of R with connection set S, and we denote by F_S the largest subgroup of $\mathrm{Aut}(\Gamma)$ under which each orbit of N is invariant. In symbols we have

$$F_S := \{g \in \mathrm{Aut}(\Gamma) \mid \mathcal{O}_i^g = \mathcal{O}_i, \text{ for each } i \in \{1,\dots,b\}\}.$$

(The subscript S in F_S will make some of the later notation cumbersome to use, but it constantly emphasises that the definition of "F" depends on S.)

For a subgroup H of $\mathrm{Sym}(r)$ and an H-invariant subset X of $\{1,\dots,r\}$, we write $H|_X$ for the restriction of H to X, that is, the image of the natural homomorphism $H \to \mathrm{Sym}(X)$ restricting a permutation of H to X. For $1 \le i \le b$, set $S_i := S \cap \mathcal{O}_i$ and let $F_S^i := (F_S)_{v_0}|_{\mathcal{O}_i}$ denote the restriction to $\mathcal{O}_i$ of the stabiliser $(F_S)_{v_0}$ in F_S of the point $v_0 \in \mathcal{O}_1$.

Lemma 2.1. (See [4, Lemma 4.1].) *If none of the S_i, $i \in \{2,\dots,b\}$, is invariant under any non-identity element of the group F_S^i, then $F_S = N$.*

Proof. Clearly, $N \le F_S$ and, from the Frattini argument, $F_S = (F_S)_{v_0}N$. Fix $i \in \{2,\dots,b\}$. Let $f \in (F_S)_{v_0}$. Since $f \in \mathrm{Aut}(\Gamma)$, we have $S^f = S$ and, since f fixes every N-orbit setwise, we have $S_i^f = S_i$. Therefore, by hypothesis, the permutation f restricted to $\mathcal{O}_i$ is the identity. Since this holds for each $i \in \{2,\dots,b\}$, f fixes $\{1,\dots,r\} \setminus \mathcal{O}_1$ pointwise. Since this holds for every element $f \in (F_S)_{v_0}$, $(F_S)_{v_0}$ fixes $\{1,\dots,r\} \setminus \mathcal{O}_1$ pointwise. In particular, $(F_S)_{v_0} \le (F_S)_{v_0^{\gamma_2}}$ and, as $(F_S)_{v_0}$ and $(F_S)_{v_0^{\gamma_2}}$ have the same order, $(F_S)_{v_0} = (F_S)_{v_0^{\gamma_2}}$.

Finally, as $(F_S)_{v_0}$ fixes $\{1,\dots,r\} \setminus \mathcal{O}_1$ pointwise, $((F_S)_{v_0})^{\gamma_2} = (F_S)_{v_0^{\gamma_2}}$ fixes $(\{1,\dots,r\} \setminus \mathcal{O}_1)^{\gamma_2} = \{1,\dots,r\} \setminus \mathcal{O}_2$ pointwise. Thus $(F_S)_{v_0}$ fixes $(\{1,\dots,r\} \setminus \mathcal{O}_1) \cup (\{1,\dots,r\} \setminus \mathcal{O}_2) = \{1,\dots,r\}$ pointwise, so $(F_S)_{v_0} = 1$. Therefore $F_S = (F_S)_{v_0}N = N$. □

In the following lemma we slightly generalise the previously-known result, and we make the estimates in the statement of [4, Lemma 4.2] more explicit.

Lemma 2.2. (See [4, Lemma 4.2].) *For each $i \in \{2,\dots,b\}$,*

$$|\{S \subseteq R \mid \textit{there exists } f \in F_S \cap \mathbf{N}_{\mathrm{Aut}(\Gamma)}(N) \textit{ with } v_0^f = v_0, \textit{ and } f|_{\mathcal{O}_i} \neq 1\}| \le 2^{r-\frac{n}{4}+(\log_2(n))^2+\log_2(n)}.$$

Proof. Fix $i \in \{2,\dots,r\}$ and denote by Φ_i the set

$$\Phi_i := \{S \subseteq R \mid \text{there exists } f \in F_S \cap \mathbf{N}_{\mathrm{Aut}(\Gamma)}(N) \text{ with } v_0^f = v_0 \text{ and } f|_{\mathcal{O}_i} \neq 1\}.$$

We follow the proof in [4, Lemma 4.2] (without assuming that R is nilpotent of odd order).

Let L^i denote the normaliser in $\mathrm{Sym}(\mathcal{O}_i)$ of $N^i := N|_{\mathcal{O}_i}$. The group N^i acts regularly on $\mathcal{O}_i$ and is contained in L^i, therefore, by the Frattini argument, $L^i = N^i(L^i)_v$, where $v \in \mathcal{O}_i$. The action of N^i on $\mathcal{O}_i$ is permutation isomorphic to the action of N^i on itself by right multiplication and, as $N^i \trianglelefteq L^i$, the action of $(L^i)_v$ on $\mathcal{O}_i$ is permutation isomorphic to the action of $(L^i)_v$ on N^i by conjugation. Therefore L^i is isomorphic to the holomorph $N \rtimes \mathrm{Aut}(N)$ of N and

$$|L^i| = |N||\mathrm{Aut}(N)| < n \cdot n^{\log_2(n)}.$$

We claim that if $\ell \in L^i$ fixes $v \in \mathcal{O}_i$, then the set $\{m \in N \mid v^{m\ell} = v^m\}$ is a subgroup of N. Clearly, $1 \in N$ and $v^{1\cdot\ell} = v^\ell = v$. Now, let $m_1, m_2 \in N$ with $v^{m_1\ell} = v^{m_1}$ and $v^{m_2\ell} = v^{m_2}$. Since ℓ normalises N^i we have $(m_2|_{\mathcal{O}_i})^\ell \in N^i$ and hence there exists $m_3 \in N$ with $m_3|_{\mathcal{O}_i} = (m_2|_{\mathcal{O}_i})^\ell$. The image of the point $v \in \mathcal{O}_i$ under $(m_2|_{\mathcal{O}_i})^\ell$ is $v^{\ell^{-1}m_2\ell} = v^{m_2\ell} = v^{m_2}$. Hence $v^{m_3} = v^{m_2}$ and, since N acts regularly on $\mathcal{O}_i$, we get $m_3 = m_2$. Therefore $m_2|_{\mathcal{O}_i} = (m_2|_{\mathcal{O}_i})^\ell$ and hence

$$v^{m_1m_2\ell} = v^{m_1\ell(m_2)^\ell} = (v^{m_1\ell})^{m_2^\ell} = (v^{m_1})^{m_2} = v^{m_1m_2}.$$

The previous paragraph shows that, if $\ell \in L^i \setminus \{1\}$ fixes $v \in \mathcal{O}_i$, then $\{m \in N \mid v^{m\ell} = v^n\}$ is a proper subgroup of N and hence $|\{w \in \mathcal{O}_i \mid w^\ell = w\}| = |\{v^m \mid m \in N, v^{m\ell} = v^m\}| = |\{m \in N \mid v^{m\ell} = v^m\}| \leq |N|/2$. Thus ℓ fixes at most $n/2$ elements of $\mathcal{O}_i$. Therefore the number of subsets S_i of $\mathcal{O}_i$ invariant under $\ell \in L^i \setminus \{1\}$ is at most $2^{3n/4}$.

For $S \in \Phi_i$, observe that S_j is an arbitrary subset of $\mathcal{O}_j$ when $j \neq i$; moreover, $(F_S)\,|_{\mathcal{O}_i} \leq L^i$. This shows that maps f that satisfy the conditions described in the definition of Φ_i lie in L^i, and since they are also in $F_S \leq \mathrm{Aut}(\Gamma)$, they must fix S_i setwise but not pointwise. So we can bound the number of choices for S_i by the number of choices for such an f times the number of subsets of $\mathcal{O}_i$ that are fixed by that f. This gives us at most $|L^i|2^{3n/4}$ choices for S_i. Therefore we get

$$|\Phi_i| \leq |L^i| 2^{3n/4}(2^n)^{b-1} \leq n^{\log_2(n)+1}2^{r-n/4},$$

and the lemma follows. $\square$

Lemma 2.3. (See [4, Lemma 4.2].) *For each $i \in \{2, \dots, b\}$,*

$$|\{S \subseteq R \mid \textit{there exists } f \in F_S \textit{ with } v_0^f = v_0, \textit{ and } f|_{\mathcal{O}_i} \neq 1\}| \leq 2^r \binom{n}{2} \left(\frac{3}{4}\right)^{\frac{r/n-2}{3}}.$$

Proof. Fix $i \in \{2, \dots, r\}$ and denote by Φ_i the set

$$\Phi_i := \{S \subseteq R \mid \text{there exists } f \in (F_S)_{v_0} \text{ with } f|_{\mathcal{O}_i} \neq 1\}.$$

Let S be a subset of R. For a vertex u of $\Gamma(R,S)$ in $\mathcal{O}_i$, let $\sigma(S,u,j)$ denote the outneighbours of v_0 and u lying in $\mathcal{O}_j$. Given $g_u \in R$ with $v_0^{g_u} = u$, it is clear that

$$\sigma(S,u,j) = S \cap S^{g_u} \cap \mathcal{O}_j = S_j \cap S^{g_u}.$$

Let $s \in S$ with $s^{g_u} \in S_j$. Then $s^{g_u} \in \mathcal{O}_j = v_0^{\gamma_j N} = v_0^{N\gamma_j}$ and $s^{g_u\gamma_j^{-1}} \in v_0^N = \mathcal{O}_1$. Since g_u maps the element v_0 of $\mathcal{O}_1$ to the element u of $\mathcal{O}_i$, we see that $g_u \in \gamma_i N$ and $s \in \mathcal{O}_1^{\gamma_j g_u^{-1}} = v_0^{\gamma_j\gamma_i^{-1}N} = \mathcal{O}_{ji^{-1}}$. This shows that

$$\sigma(S,u,j) = S_j \cap S_{ji^{-1}}^{g_u}. \tag{1}$$

For two distinct vertices $u, v \in \mathcal{O}_i$, let

$$\Psi_i(u,v,j) := \{S \subseteq R \mid |\sigma(S,u,j)| \equiv |\sigma(S,v,j)| \mod 2\}.$$

We claim that

$$|\Psi_i(u,v,j)| \leq \frac{3}{4}\cdot 2^r. \tag{2}$$

Since $u, v \in \mathcal{O}_i$, we have $u = v_0^{\gamma_i n_u}$ and $v = v_0^{\gamma_i n_v}$, for some $n_u, n_v \in N$. Let $S \in \Psi_i(u,v,j)$. From (1), we obtain

$$|\sigma(S,u,j)| = |S_{ji^{-1}} \cap S_j^{n_u^{-1}\gamma_i^{-1}}| \quad \text{and} \quad |\sigma(S,v,j)| = |S_{ji^{-1}} \cap S_j^{n_v^{-1}\gamma_i^{-1}}|. \tag{3}$$

From this we see that the condition $|\sigma(S,u,j)| \equiv |\sigma(S,v,j)| \mod 2$ does not impose any constraints on S_k, for $k \notin \{j, ji^{-1}\}$. Therefore

$$|\Psi_i(u,v,j)| = A \cdot 2^{r-2n},$$

where A is the number of pairs of subsets $S_{ji^{-1}} \subseteq \mathcal{O}_{ji^{-1}}$ and $S_j \subseteq \mathcal{O}_j$ with

$$|S_{ji^{-1}} \cap S_j^{n_u^{-1}\gamma_i^{-1}}| \equiv |S_{ji^{-1}} \cap S_j^{n_v^{-1}\gamma_i^{-1}}| \mod 2. \tag{4}$$

Let x be the number of subsets S_j of $\mathcal{O}_j$ with $S_j^{n_u^{-1}} = S_j^{n_v^{-1}}$, and let $y = 2^n - x$.

Observe that for every subset $S \subseteq R$ with $S_j^{n_u^{-1}} = S_j^{n_v^{-1}}$, we have $S \in \Psi_i(u,v,j)$ because (4) is automatically satisfied in this case. Now $n_v^{-1}n_u \in N \setminus \{1\}$ and, if $S_j = S_j^{n_v^{-1}n_u}$, then S_j is a union of $\langle n_v^{-1}n_u\rangle$-cosets. As $o(n_v^{-1}n_u) \geq 2$ and as N acts regularly on $\mathcal{O}_j$, we have $x \leq 2^{n/2}$.

Next let $S \in \Psi_i(u,v,j)$ and suppose that S_j is a subset of $\mathcal{O}_j$ with $S_j^{n_u^{-1}} \neq S_j^{n_v^{-1}}$. Now $S_j^{n_u^{-1}\gamma_i^{-1}}$ and $S_j^{n_v^{-1}\gamma_i^{-1}}$ are two distinct subsets of $\mathcal{O}_{ji^{-1}}$ of the same size a, say. Let b be the size of $S_j^{n_u^{-1}\gamma_i^{-1}} \cap S_j^{n_v^{-1}\gamma_i^{-1}}$. Observe that $a-b>0$. Moreover, a subset $S_{ji^{-1}}$ of $\mathcal{O}_{ji^{-1}}$ with $|S_{ji^{-1}} \cap S_j^{n_u^{-1}\gamma_i^{-1}}| \equiv |S_{ji^{-1}} \cap S_j^{n_v^{-1}\gamma_i^{-1}}| \mod 2$ can be written as $X \cup Y$, where X is as an arbitrary subset of $\mathcal{O}_{ji^{-1}} \setminus (S_j^{n_v^{-1}\gamma_i^{-1}} \setminus S_j^{n_u^{-1}\gamma_i^{-1}})$ and Y is a subset of $S_j^{n_v^{-1}\gamma_i^{-1}} \setminus S_j^{n_u^{-1}\gamma_i^{-1}}$ of size having parity uniquely determined by the parity of $|X|$. Therefore we have $2^{n-(a-b)}2^{(a-b)-1} = 2^{n-1}$ choices for $S_{ji^{-1}}$. Altogether we have

$$\begin{aligned} A &= x\cdot 2^n + y\cdot 2^{n-1} = x2^n + 2^{2n-1} - x2^{n-1} = 2^{2n-1} + x2^{n-1}\\ &\leq 2^{2n-1} + 2^{n/2}2^{n-1} = \left(\frac{1}{2} + \frac{1}{2^{n/2+1}}\right)2^{2n} \leq \frac{3}{4}\cdot 2^{2n} \end{aligned}$$

and (2) is proved.

Choose a subset $J \subseteq \{2,\dots,b\}\setminus\{i\}$ of maximal size with $J \cap Ji^{-1} = \emptyset$. We claim that $|J| \geq (b-2)/3$. We argue by contradiction and we suppose that $|J| < (b-2)/3$. Clearly $|J \cup Ji \cup Ji^{-1}| \leq |J| + |Ji| + |Ji^{-1}| = 3|J| < b-2$ and hence there exists $x \in \{1,\dots,b\}\setminus(J\cup Ji\cup Ji^{-1}\cup\{1,i\})$. Set $J' = J\cup\{x\}$ and observe that $|J'| = |J|+1$ and $J' \subseteq \{2,\dots,b\}\setminus\{i\}$. Since $J\cap Ji^{-1} = \emptyset$ and $i \neq 1$, we have $J'\cap J'i^{-1} = (\{x\}\cap Ji^{-1}) \cup (J\cap\{xi^{-1}\}) = \emptyset$.

Given two distinct elements u, v in $\mathcal{O}_i$, define $\Psi_i(u,v,J) := \bigcap_{j\in J}\Psi_i(u,v,j)$. Observe that from (3) and from the definition of J (requiring that $J\cap Ji^{-1} = \emptyset$) the events $\{\Psi_i(u,v,j)\}_{j\in J}$ are pairwise independent. Therefore it follows from (2) that

$$|\Psi_i(u,v,J)| \leq \left(\frac{3}{4}\right)^{|J|} 2^r.$$

We are now ready to conclude the proof of this lemma. Let $S \in \Phi_i$ and let $f \in (F_S)_{v_0}$ with $f|_{\mathcal{O}_i} \neq 1$. Let u and v be distinct vertices of $\Gamma(R,S)$ in $\mathcal{O}_i$ with $u^f = v$. Since f fixes v_0 and fixes every N-orbit setwise, we get $(\sigma(S,u,j))^f = \sigma(S,u^f,j) = \sigma(S,v,j)$, for every $j\in\{2,\dots,b\}$ and hence (in particular) $S \in \Psi_i(u,v,J)$. Therefore, given u and v, we have at most $|\Psi_i(u,v,J)| \leq (3/4)^{(b-2)/3}2^r$ choices for S. As we have $\binom{n}{2}$ choices for $\{u,v\}$, we have

$$|\Phi_i| \quad\leq\quad \binom{n}{2}\left(\frac{3}{4}\right)^{\frac{b-2}{3}} 2^r$$

and the lemma follows. □

We are now ready to state the first reduction.

Theorem 2.4. *Let R be a finite group of order r and let n be a positive integer with $n \geq 71$. The number of subsets S of R such that there exists*

- *a non-identity proper normal subgroup N of R with $|N| \geq n$ and*
- *an automorphism $f \in \mathrm{Aut}(\Gamma(R,S))$ normalising N, with $f \notin R$ and with f fixing setwise every N-orbit*

is at most $2^{r-\frac{n}{4}+(\log_2(n))^2+(\log_2(r))^2+\log_2(r)}$.

Proof. Every subgroup of R has at most $\log_2(r)$ generators and hence R has at most $r^{\log_2(r)} = 2^{(\log_2(r))^2}$ subgroups. In particular, we have at most $2^{(\log_2(r))^2}$ choices for a non-identity proper normal subgroup N of R. Now, fix such a normal subgroup N, and let $S \subseteq R$ such that there exists $g \in \mathrm{Aut}(\Gamma(R,S))\setminus R$ normalising N and fixing setwise every N-orbit. Thus $g \in F_S \setminus N$. Moreover, replacing g by gx^{-1}, for a suitable $x\in N$ if necessary, we may assume that g fixes the vertex $v_0 \in \mathcal{O}_1$, that is, $g \in (F_S)_{v_0}\setminus\{1\}$.

Since our original g was not in R, we certainly have $g \neq 1$, so there exists $i \in \{2,\dots,b\}$ such that $g|_{\mathcal{O}_i} \neq 1$, where $g \in (F_S)_{v_0}$. By Lemma 2.2, we have at most $(|R:N|-1)M'$ choices for S, where

$$M' = 2^{r-\frac{|N|}{4}+(\log_2(|N|))^2+\log_2(|N|)}$$

(observe that the factor $|R:N|-1$ counts the number of choices of i). Since $|R:N| = 2^{\log_2(r)-\log_2(|N|)}$, this proves that the number of choices for S is at most

$$2^{(\log_2(r))^2}\cdot 2^{\log_2(r)-\log_2(|N|)}\cdot M'.$$

Finally, observe that the mapping $x \mapsto -x/4 + (\log_2(x))^2$ is decreasing for $x \geq 71$. Therefore, the lemma follows observing that $|N| \geq n \geq 71$. □

Theorem 2.5. *Let R be a finite group of order r and let n be a positive integer. The number of subsets S of R such that there exists*

- *a non-identity proper normal subgroup N of R with $|N| \leq n$ and*
- *an automorphism $f \in \mathrm{Aut}(\Gamma(R,S))$ with $f \notin R$ and with f fixing setwise every N-orbit*

is at most $2^{r-\frac{r/n-2}{3}\log_2(4/3)+(\log_2(r))^2+\log_2(r)+\log_2(n)-1}$.

Proof. The proof follows verbatim the proof of Theorem 2.4 replacing Lemma 2.2 with Lemma 2.3 and noticing that $|N| \leq n$ in this case. □

It is important to observe that in Theorem 2.4 we require N to be normalised by f and not too small, whereas in Theorem 2.5 we do not require N to be normalised by f however we do require N to be small.

3. Preliminary lemmas and second reduction

In this section, as usual, we let R be a finite group of order r and we represent R as a regular subgroup of $\mathrm{Sym}(r)$. We show that the problem of enumerating Cayley digraphs over R is strictly related (but possibly not equivalent) to the problem of enumerating the subgroups G of $\mathrm{Sym}(r)$ with $R < G$ and with R maximal in G. Next, we show that the number of such groups G with $|G|$ "small" is negligible and we will deduce yet another useful reduction for the problem of asymptotically enumerating Cayley digraphs.

Lemma 3.1. *Let G be a transitive subgroup of $\mathrm{Sym}(\Omega)$, let $\omega \in \Omega$ and let κ be the number of orbits of G_ω on Ω. Then there exist 2^κ digraphs Γ with $\Omega = V\Gamma$ and $G \le \mathrm{Aut}(\Gamma)$. Moreover, if G is not regular, then $\kappa \le \frac{3}{4}|\Omega|$.*

Proof. Since G is acting transitively on Ω, a digraph Γ with vertex set Ω and with $G \le \mathrm{Aut}(\Gamma)$ is uniquely determined by the out-neighbourhood $\Gamma^+(\omega)$ of the given vertex ω. As $\Gamma^+(\omega)$ is a union of G_ω-orbits, we have 2^κ choices for $\Gamma^+(\omega)$ and hence 2^κ choices for Γ.

Suppose now that G is not regular on Ω. Set $\Delta := \{\delta \in \Omega \mid G_\omega \text{ fixes } \delta\}$. Since Δ is a block for a system of imprimitivity for G, $|\Delta|$ divides $|\Omega|$. Since G is not regular, we have $G_\omega \neq 1$ and hence $|\Delta| < |\Omega|$, so $|\Delta| \le |\Omega|/2$. Clearly, G_ω has at most $(|\Omega| - |\Delta|)/2$ orbits on $\Omega \setminus \Delta$. Thus G_ω has at most

$$|\Delta| + \frac{|\Omega| - |\Delta|}{2} = \frac{1}{2}|\Delta| + \frac{|\Omega|}{2} \le \frac{|\Omega|}{4} + \frac{|\Omega|}{2} = \frac{3|\Omega|}{4}$$

orbits on Ω. (We note that this is the same argument used in Remark 1.6(3).) □

Lemma 3.2. *For every $\varepsilon \in (0, 1/2)$, there exists $r_\varepsilon \in \mathbb{N}$ such that, for every $r > r_\varepsilon$ and for every regular subgroup R of $\mathrm{Sym}(r)$, the number of subgroups G of $\mathrm{Sym}(r)$ with*

- *$R < G$,*
- *G having at most $\log_2(r) + 1$ generators and*
- *$|G_1| \le 2^{r^{1/2-\varepsilon}}$,*

is at most $2^{r^{1-\varepsilon}}$.

Proof. Fix $\varepsilon \in (0, 1/2)$. We let $r_\varepsilon \in \mathbb{N}$ be the smallest positive integer such that

$$(2\log_2(r) + 5)r^{1-2\varepsilon} + (\log_2(r) + 1)r^{1/2-\varepsilon} + 2(\log_2(r))^2 \le r^{1-\varepsilon}, \tag{5}$$

for every $r \ge r_\varepsilon$. Comparing the asymptotics of the right-hand side and the left-hand side of (5), we see that r_ε is well-defined.

Given G and G' two abstract groups and $H \le G$, $H' \le G'$, we write $(G, H) \sim (G', H')$ if there exists a group isomorphism $\varphi : G \to G'$ with $H^\varphi = H'$. Clearly, $\sim$ defines an equivalence relation. We denote by $[G, H]$ the $\sim$-equivalence class containing (G, H). Now consider

$$\begin{aligned}\mathcal{M} = \{[G, H] \quad \mid \quad & G \text{ is a group}, H \le G, |G| \le 2^{r^{1/2-\varepsilon}} \\ & \text{and } G \text{ is } (\log_2(r) + 1)\text{-generated}\}.\end{aligned}$$

Claim 1: We have

$$|\mathcal{M}| \le 2^{(2\log_2(r)+5)r^{1-2\varepsilon} + r^{1/2-\varepsilon}}. \tag{6}$$

From [25, Theorem 1] together with [25, Remark 3(1)] we get that the number of isomorphism classes of groups of order N that are d-generated is at most $N^{2(d+1)\log_2(N)} = 2^{2(d+1)(\log_2(|N|))^2}$. In particular, applying this theorem with $d := \log_2(r) + 1$ and with $N \le 2^{r^{1/2-\varepsilon}}$, we get that the number of groups G that are $(\log_2(r) + 1)$-generated and of order at most $2^{r^{1/2-\varepsilon}}$ is at most $2^{2(\log_2(r)+2)r^{1-2\varepsilon}} \cdot 2^{r^{1/2-\varepsilon}}$ (observe that the second factor counts the number of choices for N: the cardinality of G). Now, let G be a group of order at most $2^{r^{1/2-\varepsilon}}$. Since every subgroup of G is at most $\log_2(|G|)$-generated, the number of subgroups H of G is at most $|G|^{\log_2(|G|)} \le 2^{r^{1-2\varepsilon}}$, and hence our claim is proved. ■

Now, let R be a regular subgroup of $\mathrm{Sym}(r)$ and let $\mathcal{S}_R$ be the set of subgroups of $\mathrm{Sym}(r)$ with $R < G$, with G having at most $(\log_2(r) + 1)$ generators and with $|G| \le 2^{r^{1/2-\varepsilon}+\log_2(r)}$.

Claim 2: We have

$$|\mathcal{S}_R| \le 2^{\log_2(r)r^{1/2-\varepsilon} + 2(\log_2(r))^2}|\mathcal{M}|. \tag{7}$$

Observe that every element G of $\mathcal{S}_R$ determines an element of $\mathcal{M}$ via the mapping $\varphi : G \mapsto [G, G_1]$ where G_1 is the stabiliser of 1 in G. We show that there are at most $2^{\log_2(r)r^{1/2-\varepsilon}+2(\log_2(r))^2}$ elements of $\mathcal{S}_R$ having the same image via φ, from which (7) immediately follows. We argue by contradiction and we let $G^1, \ldots, G^\ell \in \mathcal{S}_R$ with $\varphi(G^i) = \varphi(G^1)$, for every $i \in \{1, \ldots, \ell\}$, where $\ell > 2^{\log_2(r)r^{1/2-\varepsilon}+2(\log_2(r))^2}$. Thus there exists a group isomorphism $\phi_i : G^1 \to G^i$ with $(G^i)_1 = ((G^1)_1)^{\phi_i}$. Therefore the permutation representation of G^1 on the coset space $G^1/(G^1)_1$ is permutation isomorphic to the permutation representation of G^i on the coset space $G^i/(G^i)_1$. Thus G^1 and G^i are conjugate via an element of

$\mathrm{Sym}(r)$, that is, $G^1 = (G^i)^{\sigma_i}$ for some $\sigma_i \in \mathrm{Sym}(r)$. Now, as G^1 acts transitively on $\{1,\dots,r\}$, replacing σ_i by an element of the form $g_i\sigma_i$ (for some $g_i \in G^1$), we may assume that σ_i fixes 1, that is, $1^{\sigma_i} = 1$.

As $R \le G^i$ for every i, we get that $R^{\sigma_1},\dots,R^{\sigma_\ell}$ are ℓ regular subgroups of G^1. Since R is $\log_2(r)$-generated, we see that G^1 contains at most $|G^1|^{\log_2(r)} \le 2^{\log_2(r)r^{1/2-\varepsilon}+(\log_2(r))^2}$ distinct subgroups of order r. In particular, since $\ell > 2^{\log_2(r)r^{1/2-\varepsilon}+2(\log_2(r))^2}$, we see that $R^{\sigma_{i_1}} = \cdots = R^{\sigma_{i_t}}$ for some $t > 2^{(\log_2(r))^2}$ and some subset $\{i_1,\dots,i_t\}$ of size t of $\{1,\dots,\ell\}$. Therefore $\sigma_{i_1}\sigma_{i_j}^{-1}$ normalises R. As $1^{\sigma_{i_1}\sigma_{i_j}^{-1}} = 1$, $\sigma_{i_1}\sigma_{i_j}^{-1}$ is an automorphism of R, for every $j \in \{1,\dots,t\}$. Since R has at most $|R|^{\log_2(r)} = 2^{(\log_2(r))^2}$ automorphisms, we get $\sigma_{i_1}\sigma_{i_j}^{-1} = \sigma_{i_1}\sigma_{i_{j'}}^{-1}$ for two distinct indices j and j'. Thus $\sigma_{i_j} = \sigma_{i_{j'}}$ and $G^{i_j} = (G^1)^{\sigma_{i_j}^{-1}} = (G^1)^{\sigma_{i_{j'}}^{-1}} = G^{i_{j'}}$, which is a contradiction. ■

From (5), (6) and (7), we have

$$|\mathcal{S}_R| \le 2^{r^{1-\varepsilon}},$$

that is, the number of subgroups G of $\mathrm{Sym}(r)$ with $R < G$, with G having at most $\log_2(r)+1$ generators and with $|G| \le 2^{r^{1/2-\varepsilon}+\log_2(r)}$ is at most $2^{r^{1-\varepsilon}}$. Now, whenever $G \le \mathrm{Sym}(r)$ with $R < G$, G has at most $\log_2(r)+1$ generators, and $|G_1| \le 2^{r^{1/2-\varepsilon}}$, we must have

$$|G| = r|G|_1 \le r2^{r^{1/2-\varepsilon}} = 2^{r^{1/2-\varepsilon}+\log_2(r)},$$

so that $G \in \mathcal{S}_R$. The proof of this lemma immediately follows. □

We are now ready to give two more reductions.

Theorem 3.3. *Let R be a finite group of order r. For every $\varepsilon \in (0,1/2)$, there exists r_ε such that if $r \ge r_\varepsilon$, then the number of subsets S of R such that $\mathrm{Aut}(\Gamma(R,S))$ contains a subgroup G with*

- *$R < G$ and*
- *$|G_1| \le 2^{r^{1/2-\varepsilon}}$,*

is at most $2^{3r/4+r^{1-\varepsilon}}$.

Proof. Given $\varepsilon \in (0,1/2)$, using Lemma 3.2 choose r_ε such that, for $r \ge r_\varepsilon$, the number of subgroups G of $\mathrm{Sym}(r)$ with $R < G$, with G having at most $\log_2(r)+1$ generators and with $|G_1| \le 2^{r^{1/2-\varepsilon}}$ is at most $2^{r^{1-\varepsilon}}$.

Let $S_1,\dots,S_\ell$ be the subsets of R such that $\mathrm{Aut}(\Gamma(R,S_i))$ contains a subgroup G'^i with $R < G'^i$ and with $|G_1'^i| \le 2^{r^{1/2-\varepsilon}}$. We show that $\ell \le 2^{3r/4+r^{1-\varepsilon}}$. We argue by contradiction and we assume that $\ell > 2^{3r/4+r^{1-\varepsilon}}$. For each i, fix a subgroup $R < G^i \le G'^i$ with R maximal in G^i. Observe that, since R is at most $\log_2(r)$-generated, G^i is at most $(\log_2(r)+1)$-generated. In particular, by Lemma 3.2, the set $\{G^1,\dots,G^\ell\}$ contains at most $2^{r^{1-\varepsilon}}$ distinct elements. By the pigeonhole principle, there exists a group G^{i_0} such that $R < G^{i_0} \le \mathrm{Aut}(\Gamma(R,S))$ for more than $2^{3r/4}$ subsets S of R. However this contradicts Lemmas 3.1. □

Theorem 3.4. *Let R be a finite group of order r. For every $\varepsilon \in (0,1/2)$, there exists r_ε such that if $r \ge r_\varepsilon$, then the number of subsets S of R such that $\mathrm{Aut}(\Gamma(R,S))$ contains a subgroup G with*

- *$R < G$,*
- *R maximal in G,*
- *$|G_1| > 2^{r^{1/2-\varepsilon}}$ and*
- *the core $G_R := \bigcap_{g\in G} R^g$ of R in G has size greater than $4\log_2(r)$,*

is at most $2^{r-\frac{r}{4\log_2(r)}\log_2(e)-\log_2(4\log_2(r))+(\log_2(r))^2+\log_2(r)}$.

Proof. As usual, we identify R with its image under the right regular representation in $\mathrm{Sym}(r)$ and, given $G \le \mathrm{Sym}(r)$ with $R < G$, we denote by $G_R := \cap_{g\in G}R^g$ the core of R in G. For each $\varepsilon \in (0,1/2)$, we consider

$$\mathcal{S}_{\varepsilon,r} = \{G \le \mathrm{Sym}(r) \mid R < G, |G_1| > 2^{r^{1/2-\varepsilon}}, R \text{ is maximal in } G, |G_R| > 4\log_2(r)\}.$$

Let $r_\varepsilon \in \mathbb{N}$ such that

$$r^{1/2-\varepsilon} > (\log_2(r))^2, \tag{8}$$

for every $r \ge r_\varepsilon$.

Let $G \in \mathcal{S}_{\varepsilon,r}$. Since $G_R \lhd G$, we get $G_1 \le \mathbf{N}_G(G_R)$ and hence G_1 acts by conjugation as a group of automorphisms on G_R. Since $|\mathrm{Aut}(G_R)| \le |G_R|^{\log_2(|G_R|)} \le 2^{(\log_2(r))^2}$ and since $r^{1/2-\varepsilon} > (\log_2(r))^2$, there exists $g \in \mathbf{C}_{G_1}(G_R)$ with $g \ne 1$. Since R is maximal in G, we get $G = \langle R, g\rangle$ and hence the group G is uniquely determined by a non-identity element g of $\mathbf{C}_{\mathrm{Sym}(r)}(G_R)$. Observe that $\mathbf{C}_{\mathrm{Sym}(r)}(G_R)$ is uniquely determined by the normal subgroup G_R of R.

The group G_R is a subgroup of R and since $|R| = r$, we see that we have at most $r^{\log_2(r)} = 2^{(\log_2(r))^2}$ choices for G_R. Now $\mathbf{C}_{\mathrm{Sym}(r)}(G_R) \cong G_R \,\mathrm{wr}\, \mathrm{Sym}(|R|/|G_R|)$. Hence we have

$$|\mathcal{S}_{\varepsilon,r}| \le 2^{(\log_2(r))^2} \cdot |G_R|^{|R|/|G_R|}(|R|/|G_R|)! \tag{9}$$

(the first term counts the number of choices of G_R and the second term counts the number of choices of g). Using (8) and (9), the inequality $n! \leq n(n/e)^n$ and $|G_R| > 4\log_2(r)$, we get

$$\begin{aligned}
\log_2(|\mathcal{S}_{\varepsilon,r}|) &\leq (\log_2(r))^2 + \frac{|R|\log_2(|G_R|)}{|G_R|} + \log_2\left(\frac{|R|}{|G_R|}\right) + \frac{|R|}{|G_R|}\log_2\left(\frac{|R|}{e|G_R|}\right)\\
&= (\log_2(r))^2 + \log_2\left(\frac{|R|}{|G_R|}\right) + \frac{|R|}{|G_R|}\log_2\left(\frac{|R|}{e}\right)\\
&\leq (\log_2(r))^2 + \log_2\left(\frac{r}{4\log_2(r)}\right) + \frac{r}{4\log_2(r)}\left(\log_2(r) - \log_2(e)\right)\\
&= \frac{r}{4} - \frac{r}{4\log_2(r)}\log_2(e) - \log_2(4\log_2(r)) + (\log_2(r))^2 + \log_2(r).
\end{aligned}$$

Now the proof follows by using the last part of the argument in Theorem 3.3. In fact from Lemma 3.1, for each $G \in \mathcal{S}_{\varepsilon,r}$, there exist at most $2^{3r/4}$ subsets S of R with $G \leq \mathrm{Aut}(\Gamma(R,S))$. □

4. Some notation

Let R be a finite regular subgroup of $\mathrm{Sym}(r) = \mathrm{Sym}(\{1,\ldots,r\})$. In the rest of this paper,

- we take $\varepsilon := 0.001$,
- we choose $r_\varepsilon \in \mathbb{N}$ satisfying both Theorems 3.3 and 3.4 for this choice of ε and,
- we assume that our regular subgroup R satisfies $r/(4\log_2(r)) \geq r_\varepsilon$, where $r = |R|$.

Since we are interested in the asymptotic number of DRRs, the actual value of r_ε is not relevant in our arguments. However, with some rough estimates one might show that $r_\varepsilon \leq 2^{15\,000}$.

In the light of Theorems 3.3 and 3.4, since the number of subsets of R satisfying the hypothesis of either Theorem 3.3 or 3.4 are negligible compared to 2^r when r tends to infinity, we are left with estimating the number of subsets S of R with the property that

(H1) $\mathrm{Aut}(\Gamma(R,S)) > R$,

(H2strong) for every subgroup G of $\mathrm{Aut}(\Gamma(R,S))$ with $R < G$, the stabiliser G_1 has cardinality greater than $2^{r^{0.499}}$,

(H3strong) for every subgroup G as above, the core $G_R := \bigcap_{g\in G} R^g$ of R in G has cardinality at most $4\log_2(r)$.

First of all, we remark that G_RG_1 is the setwise stabiliser of G_R in G, where G_R is viewed as the subset $1^{G_R} = \{1^x \mid x \in G_R\} = G_R$ of the vertex set of $\Gamma(R,S)$.

Suppose now that $S \subseteq R$ satisfies (H1), (H2strong), and (H3strong) and, for some $G \leq \mathrm{Aut}(\Gamma(R,S))$ with $R < G$, the subgroup G_1 fixes every G_R-orbit setwise. In particular, since $|G_R|$ is "small", that is, $|G_R| \leq 4\log_2(r)$, Theorem 2.5 applied to the normal subgroup G_R of R gives an upper bound on the number of these subsets S of R; namely we have at most

$$2^{r-\frac{\frac{r}{4\log_2(r)}-2}{3}\log_2(4/3)+(\log_2(r))^2+\log_2(r)+\log_2(4\log_2(r))-1}. \tag{10}$$

choices for S. Therefore, since (10) is negligible compared to 2^r when r tends to infinity, we only need to estimate the number of subsets S of R which also satisfy the additional property that

(H4strong) for every subgroup G and G_R as above, some G_R-orbit is not fixed (setwise) by G_1. In particular, the group G_RG_1 is not normal in G.

In particular, we need to show that the number of subsets S of R satisfying (H1), (H2strong), (H3strong), and (H4strong) is negligible compared to 2^r.

At some point, our proof relies on previous cases of our proof, and to make that argument easier it is much more convenient to work under weaker hypotheses. Therefore, we are interested in the subsets S of R with the property that

(H1) $\mathrm{Aut}(\Gamma(R,S)) > R$, and ***for some*** subgroup G of $\mathrm{Aut}(\Gamma(R,S))$, we have

(H2) R is maximal in G and the stabiliser G_1 has cardinality greater than $2^{r^{0.499}}$,

(H3) the core $G_R := \bigcap_{g\in G} R^g$ of R in G has cardinality at most $4\log_2(r)$,

(H4) some G_R-orbit is not fixed (setwise) by G_1. In particular, the group G_RG_1 is not normal.

Observe that if a subset S of R satisfies (H1), (H2strong), (H3strong), (H4strong), then S satisfies also (H1), (H2), (H3) and (H4), so if we can show that the number of sets satisfying the weaker hypotheses is negligible compared to 2^r, this will be sufficient for our purposes.

In what follows, we also need the reduction given by Theorem 2.4, but since its role will appear only later in our work we do not include it here in our notation.

Definition 4.1. We denote by $\mathcal{T}$ the subsets of R satisfying (H1)–(H4). The set $\mathcal{T}$ depends upon the group R and hence, in principal, we need a notation depending on R, however we find that this would make our notation too cumbersome to use.

Moreover, we denote by $\mathcal{T}'$ the elements $S \in \mathcal{T}$ such that there exists $G \leq \mathrm{Aut}(\Gamma(R,S))$ satisfying (H2), (H3) and (H4) and with

(H5) $G_R = \bigcap_{g \in G} R^g = 1$.

For each $S \in \mathcal{T}'$, choose once and for all $G_S \leq \mathrm{Aut}(\Gamma(R,S))$ witnessing that S does belong to $\mathcal{T}'$. In particular, G_S depends upon the set S.

Lemma 4.2. *For each $S \in \mathcal{T}'$, the group G_S acts primitively and faithfully on the set of right cosets of R in G_S and $(G_S)_1$ is a non-normal regular subgroup of G_S.*

Proof. Write $G := G_S$. The fact that G acts primitively and faithfully on the set of right cosets of R in G follows from the maximality of R in G and from $1 = G_R = \bigcap_{g \in G} R^g$. From (H4), $G_1 G_R = G_1$ is not normal in G. Finally, as $G = G_1 R$ and $G_1 \cap R = 1$, we deduce that G_1 acts regularly in this primitive action. □

Definition 4.1 and Lemma 4.2 set up a natural link between our original problem of enumerating Cayley digraphs and the powerful theory of finite primitive groups.

From now on, for each $S \in \mathcal{T}'$, the group G_S is endowed with two faithful actions: the primitive action on the set of right cosets of R in G_S and the transitive action on the vertices of the Cayley digraph $\Gamma(R,S)$. We try henceforth to emphasise which action of G_S we are considering; this hopefully avoids possible confusion.

The modern key for analysing a finite primitive permutation group L is to study the *socle* N of L, that is, the subgroup generated by the minimal normal subgroups of L. The socle of an arbitrary finite group is isomorphic to the non-trivial direct product of simple groups; moreover, for finite primitive groups these simple groups are pairwise isomorphic. The O'Nan-Scott theorem describes in details the embedding of N in L and collects some useful information about the action of N. In [20, Theorem] five types of primitive groups are defined (depending on the group- and action-structure of the socle), namely HA (*Affine*), AS (*Almost Simple*), SD (*Simple Diagonal*), PA (*Product Action*) and TW (*Twisted Wreath*), and it is shown that every primitive group belongs to exactly one of these types. We remark that in [37] this subdivision into types is refined, namely the PA type in [20] is partitioned in four parts, which are called HS (*Holomorphic simple*), HC (*Holomorphic compound*), CD (*Compound Diagonal*) and PA. For what follows it is convenient to use this subdivision into eight types of the finite primitive primitive groups.

Definition 4.3. For each $\mathcal{C} \in \{HA, HS, HC, SD, CD, TW, AS, PA\}$, we let $\mathcal{T}'^{\mathcal{C}}$ be the elements $S \in \mathcal{T}'$ with G_S having O'Nan-Scott type $\mathcal{C}$ in its action on the set $\Omega_S := R\backslash G_S$ of right cosets of R in G_S. Moreover, we let P_S be the socle of G_S. Thus, we have the following partition of $\mathcal{T}'$:

$$\mathcal{T}' = \mathcal{T}'^{HA} \cup \mathcal{T}'^{HS} \cup \mathcal{T}'^{HC} \cup \mathcal{T}'^{SD} \cup \mathcal{T}'^{CD} \cup \mathcal{T}'^{TW} \cup \mathcal{T}'^{AS} \cup \mathcal{T}'^{PA}.$$

In the next section we aim to prove a strong upper bound for the cardinality of $\mathcal{T}'$. Then we use this strong upper bound on $|\mathcal{T}'|$ to obtain a weaker upper bound (but still adequate for our purposes) for $|\mathcal{T}|$.

5. Estimating the cardinality of $\mathcal{T}'$

Recall, from Definition 4.1 in Section 4, for each $S \in \mathcal{T}'$, we have chosen a certain subgroup G_S of $\mathrm{Aut}(\Gamma(R,S))$ and we have denoted by P_S the socle of G_S in its primitive action on $\Omega_S = R\backslash G_S$.

In this section, we estimate the cardinality of $\mathcal{T}'$ by estimating separately the cardinality of $\mathcal{T}'^{\mathcal{C}}$, for each $\mathcal{C} \in \{HA, HS, HC, SD, CD, TW, AS, PA\}$. In most of our analysis we use detailed information on the factorisations of the almost simple groups, see [23].

5.1. **Estimating the cardinality of $\mathcal{T}'^{AS}$.**

Lemma 5.1. *Let $S \in \mathcal{T}'^{AS}$. If $|R| > (3 \cdot 29!)!$, then one of the following happens for some prime p:*

- **(i):** $G_S = \mathrm{Sym}(\{1,\ldots,p\})$ *and* $(G_S)_1 = \mathrm{Sym}(\{1,\ldots,p-2\})$*;*
- **(ii):** $G_S = \mathrm{Alt}(\{1,\ldots,p\})$ *and* $(G_S)_1 = (\mathrm{Sym}(\{1,\ldots,p-2\}) \times \mathrm{Sym}(\{p-1,p\})) \cap \mathrm{Alt}(p)$*;*
- **(iii):** $G_S = \mathrm{Sym}(\{1,\ldots,p\})$ *and* $(G_S)_1 = (\mathrm{Sym}(\{1,\ldots,p-2\}) \times \mathrm{Sym}(\{p-1,p\})) \cap \mathrm{Alt}(p)$*;*
- **(iv):** $G_S = \mathrm{Sym}(\{1,\ldots,p\})$ *and* $(G_S)_1 = \mathrm{Alt}(\{1,\ldots,p-2\}) \times \mathrm{Sym}(\{p-1,p\})$*.*

Proof. We consider the actions of G_S on Ω_S and on the vertices R of $\Gamma(R,S)$. Suppose that $r = |R| > (3 \cdot 29!)!$. Let $n = |(G_S)_1| = |\Omega_S|$ be the degree of G_S in its action on Ω_S.

Suppose that G_S, seen as a primitive subgroup of $\mathrm{Sym}(\Omega_S)$, contains $\mathrm{Alt}(\Omega_S)$. Then $r = |R| \geq (n-1)!/2$ because R is the stabiliser in G_S of a point of Ω_S. Hence (from (H2)) $|(G_S)_1| \geq 2^{((n-1)!/2)^{0.499}}$. Since $G_S = R(G_S)_1$and $R \cap (G_S)_1 = 1$, we have $n! \geq |G_S| = |R||(G_S)_1| \geq |(G_S)_1|(n-1)!/2$, so $|(G_S)_1| \leq 2n$. With an easy computation, from

$$2n \geq 2^{((n-1)!/2)^{0.499}},$$

we get $n \leq 4$. In particular, $|R| \leq |G_S| \leq 4! = 24 < (3 \cdot 29!)!$, which is a contradiction. Thus G_S, seen as a primitive subgroup of $\mathrm{Sym}(\Omega_S)$, does not contain $\mathrm{Alt}(\Omega_S)$.

Since $R < \mathrm{Sym}(n)$ and $r = |R| > (3 \cdot 29!)!$, we have

$$(3 \cdot 29!)! < r < n! \tag{11}$$

and

$$n > 3 \cdot 29!.$$

Since G_S is an almost simple group, we have $P_S \trianglelefteq G_S \leq \mathrm{Aut}(P_S)$ and P_S is a non-abelian simple group. Recall that from Lemma 4.2, $(G_S)_1$ acts regularly on Ω_S.

Now, the almost simple primitive permutation groups admitting a regular subgroup are classified in [21]. From [21, Corollary 1.2 and Tables 16.1, 16.2, 16.3], we see that (as $\mathrm{Alt}(n) \not\leq G_S$ and $n > 3 \cdot 29!$) one of the following occurs (this is where we really use the very large lower bound on $|R|$, to avoid all exceptional cases):

(1) $P_S = \mathrm{PSL}_m(q)$, $|(G_S)_1| = (q^m - 1)/(q-1)$ and $P_S \cap R$ is the stabiliser of a projective point or of a projective line;
(2) $P_S = \mathrm{PSL}_2(q)$, $|(G_S)_1| = q(q-1)/2$ and $P_S \cap R \cong D_{q+1}$;
(3) $P_S = \mathrm{Alt}(q)$, $|(G_S)_1| = q(q-1)/2$ and $P_S \cap R \cong \mathrm{Sym}(q-2)$;
(4) $P_S = \mathrm{Alt}(p)$, $(G_S)_1$ is isomorphic to $\mathrm{Sym}(p-2)$ or $\mathrm{Alt}(p-2) \times C_2$, and $|P_S \cap R| = p(p-1)/2$, for some prime p;
(5) $P_S = \mathrm{Alt}(p+1)$, $(G_S)_1 \cong \mathrm{Sym}(p-2)$ or $\mathrm{Alt}(p-2) \times 2$, and $|P_S \cap R| = p(p^2-1)/2$, for some prime p;
(6) $P_S = \mathrm{Alt}(p^2+1)$, $(G_S)_1 \cong \mathrm{Alt}(p^2-2)$ and $P_S \cap R \cong \mathrm{PSL}_2(p^2).2$, for some prime $p \equiv 3 \mod 4$.

For each of the first three cases, a direct computation using the order of the non-abelian simple group P_S shows that

$$|G_S| \leq |\,\mathrm{Aut}(P_S)| \leq |P_S \cap R|^4 \leq |R|^4 = r^4.$$

Now $r^4 > |(G_S)_1| > 2^{r^{0.499}}$ only if $r \leq 1936$, contradicting (11).

In the fifth case, we have $|G_S| \leq (p+1)!$ and $|R| \geq |R \cap P_S| \geq p(p^2-1)/2$. Now with a computation we see that $(p+1)! > |G_S| > |(G_S)_1| \geq 2^{r^{0.499}} \geq 2^{(p(p^2-1)/2)^{0.499}}$ only if $p \leq 26$. Therefore, $|R| < |G_S| \leq 27!$, which is a contradiction to (11). Similarly, in the sixth case we have $|G_S| \leq (p^2+1)!$ and $|R| \geq |R \cap P_S| = p^2(p^4-1)$, and the inequality $(p^2+1)! > 2^{(p^2(p^4-1))^{0.499}}$ is never satisfied.

We now consider the fourth case, that is, $P_S = \mathrm{Alt}(p)$, for some prime p, $|P_S \cap R| = p(p-1)/2$ and $(G_S)_1 \cong \mathrm{Sym}(p-2)$ or $(G_S)_1 \cong \mathrm{Alt}(p-2) \times C_2$. A direct case-by-case analysis yields that the only possibilities for G_S, $(G_S)_1$ and R are listed in the statement of this lemma (in cases (ii) and (iii) $(G_S)_1 \cong \mathrm{Sym}(p-2)$). □

Theorem 5.2. *We have $|\mathcal{T}'^{AS}| \leq a$, where $a := 2^{(3 \cdot 29!)!}$.*

Proof. If $r = |R| \leq (3 \cdot 29!)!$, then $|\mathcal{T}'^{AS}| \leq 2^r \leq a$. Suppose then $r > (3 \cdot 29!)!$. Let $S \in \mathcal{T}'^{AS}$. From Lemma 5.1, there are only four possibilities for G_S and $(G_S)_1$: we have only four possibilities for the permutation group G_S in its action on the set of right cosets of $(G_S)_1$, that is, we have only four possibilities for G_S as a permutation group on the vertices of $\Gamma(R,S)$. Now, it is an easy computation to see that for each of these four cases G_S in its action on the right cosets of $(G_S)_1$, that is, on the vertices of $\Gamma(R,S)$, has rank at most 7. Therefore, arguing as in Lemma 3.1, there are at most 2^7 choices for S. Since we have at most four choices for G_S and $(G_S)_1 \backslash G_S$, we have $|\mathcal{T}'^{AS}| \leq 4 \cdot 2^7 < a$. □

5.2. **Estimating the cardinality of $\mathcal{T}'^{PA}$.** The upper bound in Theorem 5.3 (as well as the upper bound in Theorem 5.2) should not be taken too seriously, it simply shows that the set $|\mathcal{T}'^{PA}|$ is bounded above by a constant independent on the cardinality of R, which in our opinion is an interesting remark on its own.

Theorem 5.3. *We have $|\mathcal{T}'^{PA}| \leq 2^b$, where $b := (442^2)!^6 \cdot 6!$.*

Proof. Given $S \in \mathcal{T}'^{PA}$, we have $G_S \leq H \,\mathrm{wr}\, \mathrm{Sym}(\kappa)$ endowed of its natural wreath product action on $\Omega = \Delta^\kappa$, where H is a primitive group of AS type on Δ and $\kappa \geq 2$. The socle $P_S \cong T^\kappa$, where T is the socle of H. Replacing R by a suitable conjugate, we may assume that $R = (G_S)_\omega$ where $\omega = (\delta, \ldots, \delta) \in \Delta^\kappa = \Omega$ with $\delta \in \Delta$. We have

$$R = (G_S)_\omega \geq P_S \cap (G_S)_\omega = (P_S)_\omega = T_\delta^\kappa,$$

with $T_\delta \neq 1$: this last fact is immediate because in a primitive group of PA type, the socle P_S does not act regularly.

As $(G_S)_1$ acts regularly on Ω_S and $T_\delta \neq 1$, we see that $(G_S)_1$ contains no simple direct factor of P_S. Therefore we are in the position to apply Theorem 1 (i) in [22] to the primitive group G_S of PA type and to its regular subgroup $(G_S)_1$. From [22, Theorem 1 (i)], we deduce that there exists a transitive core-free subgroup K of H in its action on Δ. Unfortunately, there is not enough information in [22] to guarantee that K acts regularly on Δ, this will make the rest of this proof longer, but in spirit similar to the proof of the AS case done above.

Since $|R \cap P_S| = |T_\delta|^\kappa$ and since R acts transitively by conjugation on the κ simple direct summands of P_S, we have $|R| \geq \kappa |T_\delta|^\kappa$. As $|(G_S)_1| = |\Omega_S| = |\Delta^\kappa| = |T/T_\delta|^\kappa$ and $|(G_S)_1| \geq 2^{|R|^{0.499}}$, we deduce the inequality

$$|T/T_\delta|^\kappa \geq 2^{(\kappa |T_\delta|^\kappa)^{0.499}}. \tag{12}$$

Since K acts transitively on Δ, from the Frattini argument we obtain the factorisation

$$H = K H_\delta.$$

As H acts primitively on Δ, H_δ is a maximal subgroup of H. Among all core-free subgroups of H containing K choose one, K' say, as large as possible. We now consider two cases depending on whether K' is a maximal subgroup of H, or K' is not a maximal subgroup of H. Observe that in the second case every maximal subgroup of H containing K must contain also the socle T of H.

From (12) and the transitivity of K on Δ, we deduce

$$|K'|\geq |K|\geq |\Delta| = |T/T_\delta|\geq 2^{\frac{1}{\kappa}(\kappa|T_\delta|^{\kappa})^{0.499}}. \tag{13}$$

Case 1: Suppose K' is maximal in H.

In this case, the action of H on the coset space $K'\backslash H$ is faithful and primitive. Write $n := |H : K'|$. For the reader's convenience we report a very useful result of Maróti [28, Theorem 1.1] phrased in terms of our current notation: Consider the primitive action of H on $K' \setminus H$ of degree n. Then, one of the following holds:

- **(i):** there exist three natural numbers m, k, y with $m \geq 5$, $m/2 > k \geq 1$, $y \geq 1$, such that H is a subgroup of the wreath product $\mathrm{Sym}(m) \operatorname{wr} \mathrm{Sym}(y)$ containing $(\mathrm{Alt}(m))^y$, where the action of $\mathrm{Sym}(m)$ is on k-subsets of $\{1,\ldots,m\}$ and the wreath product has the product action of degree $n = \binom{m}{k}^y$;
- **(ii):** H equals M_{11}, M_{12}, M_{23} or M_{24} in their 4-transitive actions;
- **(iii):** $|H| \leq n\cdot\prod_{i=0}^{\lfloor\log_2(n)\rfloor-1}(n-2^i) < n^{1+\lfloor\log_2(n)\rfloor}$.

We now combine this detailed information on H and its maximal subgroup K' with (13). However, first we make two preliminary observations. First, since H is almost simple, in case **(i)** we have $y = 1$. Second, $H = K'H_\delta$ and hence

$$n = |H : K'| \leq |H_\delta| = |T_\delta||H_\delta : T_\delta| \leq |T_\delta|^2, \tag{14}$$

where in the last inequality we used some basic information on the cardinality of the outer-automorphism group of a non-abelian simple group (here we are using the fact that $|\operatorname{Out}(T)| \leq |T_\delta|$, which can be obtained with a case-by-case analysis using the CFSG).

We are now ready to consider the three possibilities: **(i)**, **(ii)** and **(iii)**. We start with **(iii)**. From (14), we deduce

$$|K'| = |H|/n < n^{\lfloor\log_2(n)\rfloor} \leq (|T_\delta|^2)^{\log_2(|T_\delta|^2)}. \tag{15}$$

From (13) and (15), we get

$$(|T_\delta|^2)^{\log_2(|T_\delta|^2)} \geq 2^{\frac{1}{\kappa}(\kappa|T_\delta|^{\kappa})^{0.499}}.$$

Now a computation shows that this inequality is satisfied only when

- $\kappa = 2$ and $|T_\delta| \leq 442$, or
- $\kappa = 3$ and $|T_\delta| \leq 30$, or
- $\kappa = 4$ and $|T_\delta| \leq 9$, or
- $\kappa = 5$ and $|T_\delta| \leq 4$, or
- $\kappa = 6$ and $|T_\delta| = 2$.

In particular, $|T_\delta| \leq 422$ and hence $n \leq 422^2$ by (14). Since H acts faithfully on the cosets of K' (since K' is core-free in H), we have $|H| \leq |\mathrm{Sym}(n)| = n! \leq (442^2)!$. As $\kappa \leq 6$, we have $r = |R| \leq |G_S| \leq |H|^\kappa\cdot\kappa! \leq ((442^2)!)^6\cdot 6!$ and hence the cardinality of $\mathcal{T}'^{PA}$ is bounded above by 2^b, where $b := ((442^2)!)^6\cdot 6!$.

The proof for Case **(ii)** is entirely similar and actually easier. In fact, $H = T$ because H is a non-abelian simple group; therefore $T_\delta = H_\delta$. Moreover,

$$|K'| = \begin{cases} 720 & \text{when } H = M_{11},\\ 7920 & \text{when } H = M_{12},\\ 443520 & \text{when } H = M_{23},\\ 10200960 & \text{when } H = M_{24},\end{cases} \quad\text{and}\quad |T_\delta| \geq \begin{cases} 660 & \text{when } H = M_{11},\\ 72 & \text{when } H = M_{12},\\ 253 & \text{when } H = M_{23},\\ 168 & \text{when } H = M_{24}.\end{cases} \tag{16}$$

(The bound on $|T_\delta|$ follows with a case by case analysis determining the minimal size of a maximal subgroup X of H with $H = K'X$.) With a computation we see that there is no solution with $\kappa \geq 2$ of (13) and (16). Therefore, $\mathcal{T}'^{PA} = \emptyset$ in this case.

Summing up, we have proved that $\mathrm{Alt}(m) \leq H \leq \mathrm{Sym}(m)$ and K' is the setwise stabilizer of a k-subset of $\{1,\ldots,m\}$ with $1 \leq k < m/2$. Since $H = K'H_\delta$, we deduce that H_δ is a k-homogeneous group, that is, H_δ acts transitively on the k-subsets of $\{1,\ldots,m\}$. In this concrete action, we have

$$|T_\delta| \geq \binom{m}{k} \quad\text{and}\quad |K'| \leq k!(m-k)!$$

and hence (13) gives

$$k!(m-k)! \geq 2^{\frac{1}{\kappa}(\binom{m}{k}^{\kappa}\kappa)^{0.499}}. \tag{17}$$

Observe that the left hand side is at most $m! \leq m^m = 2^{m\log_2(m)}$ and that $\binom{m}{k} \geq m$. Recall also that $\kappa \geq 2$. From this and a computation, we obtain that (17) holds true only when

- $\kappa = 2$ and $k = 1$, or
- $\kappa = 2$, $k = 2$ and $m \leq 10$, or
- $\kappa = 3$, $k = 1$, and $m \leq 170$.

In the last two possibilities, we have $|R| < |G_S| \leq |\operatorname{Sym}(m) \operatorname{wr} \operatorname{Sym}(3)| \leq 170!^3 \cdot 6$ and hence $|\mathcal{T'}^{PA}| \leq 2^{(170!)^3 \cdot 6} < 2^b$.

Assume then $k = 1$ and $\kappa = 2$, that is, $\operatorname{Alt}(m) \operatorname{wr} \operatorname{Sym}(2) \leq G_S \leq \operatorname{Sym}(m) \operatorname{wr} \operatorname{Sym}(2)$, and K' equals $\operatorname{Alt}(\{1, \ldots, m-1\})$ when $H = \operatorname{Alt}(m)$ or $\operatorname{Sym}(\{1, \ldots, m-1\})$ when $H = \operatorname{Sym}(m)$. Since $H = K'H_\delta$, we deduce that H_δ is a transitive subgroup of $\operatorname{Sym}(m)$ in its natural action on $\{1, \ldots, m\}$. From this and from the maximality of H_δ in H, it is not difficult to deduce that T_δ is a transitive subgroup of $\operatorname{Alt}(m)$ in its natural action on $\{1, \ldots, m\}$.

Without loss of generality, we may assume that $m \geq 442^2$, because otherwise we again have $|\mathcal{T'}^{PA}| \leq 2^b$ (since $|\mathcal{T'}^{PA}| \leq 2^{|R|}$, and $|R| \leq |G_S|$).

With a computation we see that, if $|R| > m^2(m-1)/2 - 1$, then the inequality

$$2(m!)^2 \geq |G_S| = |R||(G_S)_1| \geq |R| 2^{|R|^{0.499}}$$

is not satisfied when $m \geq 450$. Thus

$$|R| \leq m^2(m-1)/2 - 1$$

and hence

$$|G_S : (G_S)_1| = |R| \leq m^2(m-1)/2 - 1. \tag{18}$$

For $i \in \{1, 2\}$, we let $\pi_i : P_S \cap (G_S)_1 \to \operatorname{Alt}(m)$ be the projection of $P_S \cap (G_S)_1$ in the i^{th} coordinate. Moreover, we let C_1 and C_2 be the image of π_1 and π_2, respectively. Suppose that, for some $i \in \{1, 2\}$, π_i is surjective. To simplify the notation we assume that $i = 1$. Now, $\operatorname{Ker}(\pi_2)$ is normal in $P_S \cap (G_S)_1$ and hence it is normalized by $\pi_1(P_S \cap (G_S)_1) = \operatorname{Alt}(m)$. Therefore, either $\operatorname{Ker}(\pi_2) = \operatorname{Alt}(m)$ or π_2 is injective. In the first case, we have $P_S \cap (G_S)_1 = \operatorname{Alt}(m) \times \operatorname{Alt}(m)$, but this contradicts the fact that $(G_S)_1 \cap R = 1$. Thus π_2 is injective and, since π_1 is surjective, we deduce that $P_S \cap (G_S)_1$ is a diagonal sugroup of $\operatorname{Alt}(m) \times \operatorname{Alt}(m)$. Again this contradicts $(G_S)_1 \cap R = 1$. So far we have shown that π_1 and π_2 are not surjective, that is, C_1 and C_2 are proper sugroups of $\operatorname{Alt}(m)$.

Thus $(G_S)_1 \leq C_1 \times C_2$ and hence

$$|P_S : C_1 \times C_2| \leq |P_S : P_S \cap (G_S)_1| = |P_S(G_S)_1 : (G_S)_1| \leq |G_S : (G_S)_1| \leq m^2(m-1)/2 - 1 \text{ (by (18))}. \tag{19}$$

Clearly, $|\operatorname{Alt}(m) : C_1|, |\operatorname{Alt}(m) : C_2| \geq m$. If $|\operatorname{Alt}(m) : C_i| \geq m(m-1)/2$ for some $i \in \{1, 2\}$, then

$$|P_S : C_1 \times C_2| = |\operatorname{Alt}(m) : C_1||\operatorname{Alt}(m) : C_2| \geq m^2(m-1)/2$$

contradicting (19). Therefore $|\operatorname{Alt}(m) : C_i| < m(m-1)/2$ for every $i \in \{1, 2\}$. Now the only proper subgroup of $\operatorname{Alt}(m)$ having index less then $m(m-1)/2$ is $\operatorname{Alt}(m-1)$, see [8, Theorem 5.2A] for instance. Therefore $C_1 = C_2 = \operatorname{Alt}(m-1)$. Since $P_S \cap (G_S)_1$ projects to $\operatorname{Alt}(m-1)$ on both coordinates with a simple argument (using the fact that $\operatorname{Alt}(m-1)$ is simple and (19)), we deduce

$$P_S \cap (G_S)_1 = \operatorname{Alt}(\{1, \ldots, m-1\}) \times \operatorname{Alt}(\{1, \ldots, m-1\}). \tag{20}$$

We now show that this contradicts the maximality of R. Indeed, recall that T_δ is a transitive subgroup of $\operatorname{Alt}(m)$ in its natural action on $\{1, \ldots, m\}$. Since $R \cap (G_S)_1 = 1$, from (20) we deduce $T_\delta \cap \operatorname{Alt}(\{1, \ldots, m-1\}) = 1$, that is, T_δ acts regularly on $\{1, \ldots, m\}$. In particular, T_δ is not a maximal subgroup of $\operatorname{Alt}(m)$ (recall $m > 3$). This immediately implies $H = \operatorname{Sym}(m)$, because H_δ is maximal in H. Now, $T_\delta \trianglelefteq H_\delta$ and hence the maximality of H_δ yields $H_\delta = \mathbf{N}_H(T_\delta)$. Since T_δ is a regular subgroup of $\operatorname{Sym}(m) = H$, we get that $\mathbf{N}_H(T_\delta)$ is the holomorph of T_δ and hence $|H_\delta| = |T_\delta||\operatorname{Aut}(T_\delta)|$. On the other hand, $|H_\delta| = |H_\delta : T_\delta||T_\delta| = 2|T_\delta|$ and hence $|\operatorname{Aut}(T_\delta)| = 2$. However, this implies that T_δ is cyclic of order 3, which is a contradiction.

Case 2: Suppose K' is not maximal in H, that is, every maximal subgroup of H containing K must contain also the socle T of H.

Using the terminology in [24], we have $K' \max^- H$, $H_\delta \max^+ H$ and $H = K'H_\delta$. Applying [24, Theorem] to this factorization, we see that either $K'T = K'(H_\delta \cap K'T)$ is a factorization of the almost simple group $K'T$ with K' and $H_\delta \cap K'T$ both maximal and core-free in $K'T$, or $(T, K' \cap T, T_\delta)$ is in [24, Table 1]. In the former case, we argue exactly as in the argument above with the group H replaced by $K'T$ and we obtain $|\mathcal{T'}^{PA}| \leq 2^b$. Therefore, we have to investigate the possibilities in [24, Table 1]. In all of the cases listed in [24, Table 1], the set Δ and the action of T on Δ are explicitly described. Therefore, with another case-by-case analysis and with routine computations we check (12) and we see that, there exists a constant a with $|G_S| \leq a$. Moreover, one might take $a < b$ and hence $|\mathcal{T'}^{PA}| \leq 2^b$ also in this case. □

5.3. Estimating the cardinality of $\mathcal{T}'^{HS} \cup \mathcal{T}'^{HC}$.

Theorem 5.4. *We have $\mathcal{T}'^{HS} \cup \mathcal{T}'^{HC} = \emptyset$.*

Proof. Let $S \in \mathcal{T}'^{HS} \cup \mathcal{T}'^{HC}$. In both of these cases, $P_S = H \times K$ where H and K are isomorphic normal regular subgroups of G_S. Since $(G_S)_1$ also acts regularly on Ω_S, we deduce $|(G_S)_1| = |H|$. From the structure of primitive groups of HS and HC type [37], the stabiliser of a point of Ω_S in G_S is isomorphic, as an abstract group, to a subgroup of $\mathrm{Aut}(H)$ containing the inner automorphisms of H. Therefore $|H| \leq |R| \leq |\mathrm{Aut}(H)|$. We deduce

$$r = |R| \geq |H| = |(G_S)_1| \geq 2^{r^{0.499}}.$$

A simple calculation gives $|R| = r \leq 16$. Thus $|H| \leq 16$, but this is a contradiction because H has size at least $|\mathrm{Alt}(5)| = 60$. Therefore $|\mathcal{T}'^{HS} \cup \mathcal{T}'^{HC}| = \emptyset$. □

5.4. **Estimating the cardinality of $\mathcal{T}'^{HA} \cup \mathcal{T}'^{SD} \cup \mathcal{T}'^{TW}$.** Before continuing our discussion on Cayley digraphs and using the theory of finite primitive groups for estimating the cardinality of $\mathcal{T}'$, we need an auxiliary result which is a refinement of a result of Liebeck and Praeger. We believe that this refinement is of considerable interest in its own.

In [22], Liebeck and Praeger investigate the transitive subgroups of the finite primitive groups. This pioneer work highlights for the first time that, if G is primitive and M is a transitive subgroup of G containing no non-identity normal subgroup of the socle of G, then M is rather limited in its structure. We generalise, for regular subgroups only, the main result of Liebeck and Prager [22, Theorem 1], when G is of type SD or TW. We do believe that a similar generalisation holds for other classes of transitive subgroups, but we do not take this detour here. First we need some notation.

Suppose that G is primitive on Ω of type SD. By the description of the O'Nan-Scott types in [37], there exists a non-abelian simple group T such that the socle N of G is isomorphic to $T_1 \times \cdots \times T_\ell$ with $T_i \cong T$ for each $i \in \{1, \ldots, \ell\}$. The set Ω can be identified with $T_1 \times \cdots \times T_{\ell-1}$ and, for the point $\omega \in \Omega$ that is identified with $(1, \ldots, 1)$, the stabilizer N_ω is the diagonal subgroup $\{(t, \ldots, t) \mid t \in T\}$ of N. That is to say, the action of N_ω on Ω is permutation isomorphic to the action of T on $T^{\ell-1}$ by "diagonal" component-wise conjugation: the image of the point $(x_1, \ldots, x_{\ell-1})$ under the permutation corresponding to $t \in T$ is

$$(x_1^t, \ldots, x_{\ell-1}^t).$$

The group G_ω is isomorphic to a subgroup of $\mathrm{Aut}(T) \times \mathrm{Sym}(\ell)$ and G is isomorphic to a subgroup of $T^\ell \cdot (\mathrm{Out}(T) \times \mathrm{Sym}(\ell))$.

Proposition 5.5. *Let G and N be as above and let B be a regular subgroup of G. Then $B \leq N \cdot \mathrm{Out}(T)$ and B contains at least $\ell - 3$ simple direct factors of N.*

Proof. Using the notation that we have established above, $N \trianglelefteq G \leq W := T^\ell \cdot (\mathrm{Out}(T) \times \mathrm{Sym}(\ell))$. Without loss of generality, for simplicity we may assume that $G = W$.

We argue by induction on ℓ and we suppose first that $\ell = 2$. In this case, $\ell - 3 = -1$ and hence the condition "B contains at least $\ell - 3$ simple direct factors of N" is satisfied vacuously. If $\ell = 2$ and B contains a simple direct factor of $N = T_1 \times T_2$, then $T_1 \leq B$ or $T_2 \leq B$ and hence, since B is regular, B equals either T_1 or T_2. In particular, $B \leq N \leq N \cdot \mathrm{Out}(T)$. If $\ell = 2$ and B contains no simple direct factor of N, then G and B satisfy the hypothesis of [22, Theorem 1]. Now, we see that $B \leq N \cdot \mathrm{Out}(T)$ from Remark (2) on page 295 and Example 1.2 in [22].

Suppose now that $\ell > 2$. Assume first that B contains no simple direct factor of $N = T_1 \times \cdots \times T_\ell$. Again, as above, G and B satisfy the hypothesis of [22, Theorem 1]. From [22, Theorem 1 (ii)], we deduce $\ell = 3$ and $B \leq N \cdot \mathrm{Out}(T)$ from Remark (2) on page 295 and Example 1.3 in [22]. Therefore, we are done in this case.

Assume that B contains some simple direct factor of N. Replacing B by a suitable G-conjugate, we may assume that $T_1 \leq B$. Set $V := \langle T_1^b \mid b \in B \rangle$. Clearly, $V \cong T^\kappa$, for some $1 \leq \kappa \leq \ell - 1$. If $\kappa = \ell - 1$, then $B = V$ because B and $T^{\ell-1}$ act regularly on Ω; thus $B \leq N$ and B contains $\ell - 1$ simple direct factors of N. Assume then $\kappa \leq \ell - 2$. We have

$$\frac{B}{V} \leq \frac{\mathbf{N}_W(V)}{V} \cong T^{\ell-\kappa} \cdot (\mathrm{Out}(T) \times \mathrm{Sym}(\ell - \kappa))$$

and the action of $\mathbf{N}_W(V)$ on the set of V-orbits on Ω is primitive with kernel V and having O'Nan-Scott type SD. Moreover, in this action, B/V is a regular subgroup of $\mathbf{N}_W(V)/V$. Thus our result follows immediately applying the inductive hypothesis to B/V and $\mathbf{N}_W(V)/V$. □

A similar, but somehow weaker, proposition can be proved for finite primitive groups of TW type.

Proposition 5.6. *Let G be a finite primitive group of TW type with socle $N = T^\ell$, where T is a non-abelian simple group, and let B be a regular subgroup of G. Then $|B : B \cap N| \leq |\mathrm{Aut}(T)|$ and B contains at least $\ell - 3$ simple direct factors of N.*

Proof. From the embeddings among the finite primitive groups, as G is a primitive group of TW type, there exists a finite primitive group of SD type $W \cong T^{\ell+1} \cdot (\mathrm{Out}(T) \times \mathrm{Sym}(\ell))$ with $G \leq W$. Applying Proposition 5.5 to W and B we deduce that B contains at least $(\ell + 1) - 3 = \ell - 2$ simple direct factors of the socle of W and hence B contains at least $\ell - 3$ simple direct factors of the socle of G. Moreover, $B \leq T^{\ell+1} \cdot \mathrm{Out}(T)$ and hence $|B : B \cap N| = |BN : N| \leq |T^{\ell+1} \cdot \mathrm{Out}(T) : T^\ell| = |\mathrm{Aut}(T)|$. □

We do not believe that Proposition 5.6 is best possible. It is enough for our purpose and our proof actually follows immediately from the analogous result for primitive groups of SD type.

After this short detour of Propositions 5.5 and 5.6, we go back to estimating $|\mathcal{T}'|$.

Proposition 5.7. *For each $S\in\mathcal{T}'^{HA}\cup\mathcal{T}'^{SD}\cup\mathcal{T}'^{TW}$, $|1^{P_S}|\le r^{0.501}(\log_2(r))^2$ where 1^{P_S} is the P_S-orbit containg 1 in the action of P_S on the vertices of $\Gamma(R,S)$.*

Proof. We consider a case-by-case analysis depending on the O'Nan-Scott type of G_S in its action on Ω_S.

Case $S\in\mathcal{T}'^{HA}$.

Here, P_S is an elementary abelian p-group of cardinality p^ℓ, for some prime number p and for some positive integer ℓ, acting regularly on Ω_S. Moreover, $G_S=P_S\rtimes R$, with R acting irreducibly by conjugation as a linear group on P_S. Since $(G_S)_1$ is also regular on Ω_S and $(G_S)_1$ is not normal in G_S, we have $(G_S)_1\ne P_S$ and $(G_S)_1P_S>P_S$. As $G_S=P_S\rtimes R$, there exists a non-identity p-sugroup Q of R with

$$P_S(G_S)_1=P_S\rtimes Q.$$

In particular, $p\le|Q|\le|R|=r$.

Since Q is a p-group, the group action of Q on P_S fixes a non-identity element $x\in P_S\setminus\{1\}$. Therefore $Q\le\mathbf{C}_R(x)$. Since R acts irreducibly on P_S, the set $x^R=\{x^t\mid t\in R\}$ spans P_S and so $\ell\le|x^R|=|R:\mathbf{C}_R(x)|\le|R:Q|$.

We have $p^\ell=|P_S|=|(G_S)_1|\ge 2^{r^{0.499}}$ and hence $\ell\log_2(p)\ge r^{0.499}$. Since $|R:Q|\ge\ell$ and $p\le r$, we deduce

$$\frac{r}{|Q|}\log_2(r)\ge r^{0.499}$$

and $|Q|\le r^{0.501}\log_2(r)$.

Since $|(G_S)_1|=|P_S|$, we have $|(G_S)_1P_S|=|(G_S)_1||P_S|/|(G_S)_1\cap P_S|=|P_S|^2/|(P_S)_1|$ from which it follows

$$|P_S:(P_S)_1|=|(G_S)_1P_S:P_S|=|P_S\rtimes Q:P_S|=|Q|.$$

Thus $|1^{P_S}|=|P_S:(P_S)_1|=|Q|\le r^{0.501}\log_2(r)\le r^{0.501}(\log_2(r))^2$.

Case $S\in\mathcal{T}'^{SD}$.

We use the notation that we have established above for primitive groups of diagonal type. Thus $P_S=T^\ell$ for some non-abelian simple group T and for some positive integer ℓ with $\ell\ge 2$. Since $(G_S)_1$ acts regularly on Ω_S, we have $|(G_S)_1|=|T|^{\ell-1}$. From Proposition 5.5 applied to the regular subgroup $(G_S)_1$, we infer $(G_S)_1\le T^\ell\cdot\mathrm{Out}(T)$. Thus $(G_S)_1P_S\le T^\ell\cdot\mathrm{Out}(T)$ and hence $|(G_S)_1P_S|\le|T|^\ell|\mathrm{Out}(T)|$. Since $|(G_S)_1P_S:(G_S)_1|=|P_S:(G_S)_1\cap P_S|$, we deduce

$$|P_S:(P_S)_1|=\frac{|(G_S)_1P_S|}{|(G_S)_1|}\le\frac{|T|^\ell|\mathrm{Out}(T)|}{|T|^{\ell-1}}=|T||\mathrm{Out}(T)|. \tag{21}$$

Now, $|T|^{\ell-1}=|(G_S)_1|\ge 2^{r^{0.499}}$ and hence

$$\ell\log_2(|T|)>(\ell-1)\log_2(|T|)\ge r^{0.499}. \tag{22}$$

Recall that the stabiliser of a point in a primitive group of SD type contains the diagonal of P_S and projects to a subgroup of $\mathrm{Sym}(\ell)$ acting transitively on the ℓ simple direct summands of the socle $P_S=T^\ell$. Thus, we obtain the bound

$$r=|R|\ge|T|\ell. \tag{23}$$

From (21), (22) and (23), we deduce

$$\begin{aligned}|1^{P_S}|=|P_S:(P_S)_1|\le|T|\log_2(|T|)\le\frac{r}{\ell}\log_2(|T|)\le\frac{r}{\frac{r^{0.499}}{\log_2(|T|)}}\log_2(|T|)\\=r^{0.501}(\log_2(|T|))^2\le r^{0.501}(\log_2(r))^2.\end{aligned}$$

Case $S\in\mathcal{T}'^{TW}$.

We use the notation that we have established above for primitive groups of TW type. Thus $P_S=T^\ell$ for some non-abelian simple group T and for some positive integer ℓ with $\ell\ge 6$, see [37]. Since P_S and $(G_S)_1$ act regularly on Ω_S, we have $|P_S|=|(G_S)_1|=|T|^\ell$ and hence

$$|1^{P_S}|=|P_S:(P_S)_1|=|G_S:(G_S)_1\cap P_S|. \tag{24}$$

From Proposition 5.6 applied to the regular subgroup $(G_S)_1$, we infer $(G_S)_1\le T^\ell\cdot\mathrm{Out}(T)$ and hence

$$|(G_S)_1:(G_S)_1\cap P_S|\le|\mathrm{Aut}(T)|. \tag{25}$$

Now, $|T|^\ell=|(G_S)_1|\ge 2^{r^{0.499}}$ and hence $1\le\ell\log_2(|T|)/r^{0.499}$, that is,

$$|\mathrm{Aut}(T)|\le|\mathrm{Aut}(T)|\frac{\ell\log_2(|T|)}{r^{0.499}}. \tag{26}$$

Recall that the stabiliser of a point in a primitive group of TW type acts transitively on the ℓ simple direct summands of the socle $P_S = T^\ell$ and contains a subgroup isomorphic to T normalizing one of the simple direct summands of P_S, see [20]. Thus, the inequality in (23) holds true also in this case. Hence, from (24), (25) and (26), we obtain

$$|1^{P_S}| \le \frac{|\operatorname{Aut}(T)|\ell\log_2(|T|)}{r^{0.499}} \le \frac{|T|\ell(\log_2(|T|))^2}{(\ell|T|)^{0.499}} = (\ell|T|)^{0.501}(\log_2(|T|))^2 \le r^{0.501}(\log_2(r))^2.$$

Observe that in the second inequality we have used the crude upper bound $|\operatorname{Out}(T)| \le \log_2(|T|)$, which follows easily from the CFSG. □

For our next result we need the notion of *normal quotient* for digraphs.

Definition 5.8. Let Γ be a digraph, let G be a group of automorphisms of Γ transitive on the vertices of Γ and let N be a normal subgroup of G. Let α^N denote the N-orbit containing the vertex α of Γ. Then the *normal quotient* Γ/N is the digraph whose vertices are the N-orbits on the vertices of Γ, with a directed edge from α^N to β^N if and only if there is a directed edge of Γ from α' to β', for some $\alpha' \in \alpha^N$ and some $\beta' \in \beta^N$. The normal quotient is non-trivial if $N \neq 1$ and N is not transitive.

Note that the group G acts as a group of automorphisms on Γ/N and induces a transitive action on the vertices of the normal quotient Γ/N. Also, for adjacent α^N, β^N of Γ/N, each vertex of α^N is adjacent to the same number of vertices in β^N (because N is transitive on both sets). Moreover, the stabiliser in G of the vertex α^N in Γ/N is $G_\alpha N$.

Theorem 5.9. *We have* $|\mathcal{T}'^{HA} \cup \mathcal{T}'^{SD} \cup \mathcal{T}'^{TW}| \le 2^{r-\frac{r^{0.499}}{8(\log_2(r))^2}+2(\log_2(r))^2+1}$.

Proof. For simplicity, write $\mathcal{T}'' := \mathcal{T}'^{HA} \cup \mathcal{T}'^{SD} \cup \mathcal{T}'^{TW}$ and we let $S \in \mathcal{T}''$. We have $P_S \trianglelefteq G_S \le \operatorname{Aut}(\Gamma(R,S))$ and hence $\Gamma(R,S)$ admits a normal quotient by the normal subgroup P_S of G_S; let us denote by $\Gamma(R,S)/P_S$ this normal quotient. Since R acts regularly on the vertices of $\Gamma(R,S)$, the system of imprimitivity given by the P_S-orbits on the vertices of $\Gamma(R,S)$ coincides with the set of cosets of R via a suitable subgroup Q_S of R with

$$(G_S)_1 P_S = (G_S)_1 Q_S,$$

indeed $Q_S := 1^{P_S}$, that is, the P_S-orbit containing the identity element of R. Now, the group R acts as a group of automorphisms on the graph $\Gamma(R,S)/P_S$ with vertex stabilizer $R_1 Q_S = Q_S$.

Now define

$$\mathcal{T}''_{\trianglelefteq} := \{S \in \mathcal{T}'' \mid Q_S \trianglelefteq R\}, \qquad \mathcal{T}''_{\ntrianglelefteq} := \{S \in \mathcal{T}'' \mid Q_S \ntrianglelefteq R\}.$$

From Proposition 5.7, for each $S \in \mathcal{T}''$, we have

$$|Q_S| = |1^{P_S}| \le r^{0.501}(\log_2(r))^2.$$

Claim 1: $|\mathcal{T}''_{\ntrianglelefteq}| \le 2^{r-\frac{r^{0.499}}{4(\log_2(r))^2}+(\log_2(r))^2}$.

We start our argument by estimating, given a non-normal subgroup Q of R, the number of subsets S of R such that the cosets of the subgroup Q partition the vertices of $\Gamma(R,S)$ into Q-cosets forming a *normal* system of imprimitivity, that is, a system of imprimitivity arising also from the orbits of a normal subgroup of $\operatorname{Aut}(\Gamma(R,S))$. Then, the proof of this claim immediately follows because R has at most $2^{(\log_2(r))^2}$ subgroups.

Let S be a subset of R and let Q be a non-normal subgroup of R with the property that the Q-cosets form a normal system of imprimitivity for the graph $\Gamma(R,S)$. Let $\Delta := Q\backslash R$ and $S_\delta := S \cap \delta$, for each $\delta \in \Delta$. Fix $q \in Q$. Since the outneighbourhood of 1 in δ is $S \cap \delta = S_\delta$, the outneighbourhood of q in δq is $(S \cap \delta)q = S_q \cap \delta q$. However, since $\Gamma(R,S)/P_S$ is a normal quotient graph (see Definition 5.8), 1 and q have the same number of outneighbours in δq and hence

$$|S \cap \delta q| = |Sq \cap \delta q|.$$

Clearly this yields

$$|S \cap \delta q| = |S \cap \delta|, \text{ for each } \delta \in \Delta \text{ and for each } q \in Q.$$

In other words, the cardinality of $S \cap \delta$ depends only on the orbits of Q on Δ, that is,

$$\text{if } \delta_1, \delta_2 \in \Delta \text{ are in the same } Q\text{-orbit, then } |S_{\delta_1}| = |S_{\delta_2}|.$$

Let us denote by $d_1, \ldots, d_o$ the cardinality of the orbits of Q on Δ; observe that $d_1, \ldots, d_o$ are not all equal to 1 because Q is not acting trivially on Δ for $Q \ntrianglelefteq R$. Clearly, $|\Delta| = |R : Q| = \sum_{i=1}^{o} d_i$.

Let $\delta_1, \ldots, \delta_o$ be a set of representatives for the orbits of Q on Δ. From the previous paragraph, for each $q \in Q$, S_{δ_i} and $S_{\delta_i q}$ have the same cardinality and hence, in particular, they have the same parity modulo 2. Therefore, to obtain an upper bound on the number of subsets S of R with $\Gamma(R,S)$ admitting a normal quotient arising from the Q-cosets, we may choose an arbitrary subset S_i of δ_i, for each $i \in \{1, \ldots, o\}$, and for each $\delta \in \delta_i^Q$, we may choose a subset of δ having the same parity of S_i. In this manner, we obtain the following over-estimate on the number of possibilities for S:

$$\begin{aligned}2^{o|Q|+\sum_{i=1}^{o}(|Q|-1)(d_i-1)} &= 2^{o|Q|+(|Q|-1)(|R:Q|-o)} = 2^{|R|-|R:Q|+o}\\ &\le 2^{|R|-|R:Q|+\frac{3}{4}|R:Q|} = 2^{|R|-\frac{1}{4}|R:Q|} \le 2^{r-\frac{r^{0.499}}{4(\log_2(r))^2}}.\end{aligned}$$

In the first inequality above, we are using Lemma 3.1. ■

Claim 2: $|\mathcal{T}''_{\trianglelefteq}| \le 2^{r-\frac{r^{0.499}}{8(\log_2(r))^2}+2(\log_2(r))^2}$.

Let $S \in \mathcal{T}''_{\trianglelefteq}$. Clearly, $P_S \nleq R$, otherwise $G_S = RP_S = R$. Let $f \in P_S \setminus R$ and observe that f fixes each P_S-orbit setwise and hence it fixes each Q_S-coset setwise. Since $Q_S \trianglelefteq R$, we are in the position to apply Theorem 2.5 with the normal subgroup Q_S of R and with the automorphism f. We obtain that

$$\begin{aligned}|\mathcal{T}''_{\trianglelefteq}| &\le 2^{r-\frac{r/n-2}{3}\log_2(4/3)+(\log_2(r))^2+\log_2(r)+\log_2(n)-1}\\ &\le 2^{r-\frac{r^{0.499}}{3(\log_2(r))^2}\log_2(4/3)+(\log_2(r))^2+\log_2(r)+(\log_2(r^{0.501}(\log_2(r))^2))}\\ &\le 2^{r-\frac{r^{0.499}}{8(\log_2(r))^2}+2(\log_2(r))^2},\end{aligned}$$

where the second inequality follows because $\frac{2}{3}\log_2(4/3) - 1 < 0$, and the last inequality follows from the facts that $\frac{1}{3}\log_2(4/3) > 1/8$. ■

The proof now follows by adding the bounds given in the previous two claims. □

5.5. **Estimating the cardinality of $\mathcal{T}'^{CD}$.** We start by reviewing the structure of primitive groups of CD type. Let $S \in \mathcal{T}'^{CD}$. Here, G_S is contained in a wreath product $H \,\mathrm{wr}\, \mathrm{Sym}(\kappa)$ endowed of its natural product action on Δ^κ, where $\kappa \ge 2$ and H is a primitive group of SD type on Δ. Thus, using the notation for primitive groups of SD type that we established above, there exists a positive integer ℓ and a non-abelian simple group T with

$$T^\ell \le H \le T^\ell \cdot (\mathrm{Out}(T) \times \mathrm{Sym}(\ell)).$$

Now, we denote by Q the projection of H to $\mathrm{Sym}(\ell)$. The group Q can be described more formally. The socle $P_S \cong T^{\kappa\ell}$ of G_S is

$$(T_{1,1} \times \cdots \times T_{1,\ell}) \times (T_{2,1} \times \cdots \times T_{2,\ell}) \times \cdots \times (T_{\kappa,1} \times \cdots \times T_{\kappa,\ell}).$$

Take $V := T_{1,1} \times \cdots \times T_{1,\ell}$ and $W := T_{1,1}$. Now, from the structure of primitive groups of CD type, $\mathbf{N}_{G_S}(V)$ has index κ in G_S. Moreover, replacing H by a suitable subgroup, we may assume that

$$\mathbf{N}_{G_S}(V) \le H \times (H \,\mathrm{wr}\, \mathrm{Sym}(\kappa - 1))$$

projects surjectively to H. Similarly, $\mathbf{N}_{G_S}(W)$ has index $\kappa\ell$ in G_S and $\mathbf{N}_{G_S}(V)/\mathbf{N}_{G_S}(W)$ projects to a primitive subgroup of $\mathrm{Sym}(\ell)$, which we denote by Q. Clearly, all the subgroups of G_S we have defined so far (for instance, H, V, W and Q) depend on S because so does G_S, but to avoid making the notation too cumbersome to use, we do not stress this.

Recall that $(G_S)_1$ is transitive on Ω_S and hence

$$|(G_S)_1| = |\Omega_S| = |T|^{\kappa(\ell-1)}.$$

Moreover, as $G_S = RP_S$ and $P_S \le \mathbf{N}_{G_S}(W) \le \mathbf{N}_{G_S}(V)$, we deduce that $|R : \mathbf{N}_R(V)| = \kappa$ and that $\mathbf{N}_R(V)/\mathbf{N}_R(W)$ projects to Q. Since $\mathbf{N}_R(W) \ge R \cap P_S \cong T^\kappa$, we get

$$|R| = |R : \mathbf{N}_R(V)||\mathbf{N}_R(V) : \mathbf{N}_R(W)||\mathbf{N}_R(W)| \ge \kappa|Q||R \cap P_S| \ge \kappa|Q||T|^\kappa$$

and hence we obtain the inequality

$$|T|^{\kappa(\ell-1)} = |(G_S)_1| \ge 2^{|R|^{0.499}} \ge 2^{(\kappa|Q||T|^\kappa)^{0.499}}.$$

Rearranging the terms, we get

$$\frac{\ell-1}{|Q|^{0.499}} \ge \frac{|T|^{0.499\cdot\kappa}\kappa^{-0.501}}{\log_2(|T|)}. \tag{27}$$

Moreover, since Q is a transitive subgroup of $\mathrm{Sym}(\ell)$, we have $|Q| \ge \ell$ and hence, from the inequality $|R| \ge \kappa|Q||T|^\kappa \ge \kappa\ell|T|^\kappa$, we obtain

$$\kappa \le \frac{\log_2(r/4)}{\log_2(60)}, \quad \ell \le \frac{r}{7200}, \quad |T| \le \frac{\sqrt{r}}{2}. \tag{28}$$

The inequalities in (28) are all easy to obtain: for instance, since $r \ge \kappa\ell|T|^\kappa$, $\ell, \kappa \ge 2$ and $|T| \ge 60$, we have $r \ge 4 \cdot 60^\kappa$ and hence $\kappa \le \log_2(r/4)/\log_2(60)$.

We claim that

$$|Q| < \ell^{2.01}. \tag{29}$$

Suppose, arguing by contradiction, that $|Q| \geq \ell^{2.01}$. From (27), we deduce

$$1 \geq \frac{\ell - 1}{\ell^{1.00299}} \geq \frac{\ell - 1}{|Q|^{0.499}} \geq \frac{|T|^{0.499 \cdot \kappa}\kappa^{-0.501}}{\log_2(|T|)};$$

however, with a simple calculation we see that this inequality is never satisfied.

We are now ready to conclude our analysis on the cardinality of $\mathcal{T}'^{CD}$.

Theorem 5.10. *There exists an absolute constant c such that*

$$|\mathcal{T}'^{CD}| \leq 2^{\frac{3}{4}r + (\log_2(r))^4 + (\log_2(r))^3/5 + (c+1)(\log_2(r))^2 + \log_2(r)}.$$

Moreover, one might take the costant c to be equal to the constant in Theorem I in [41].

Proof. We use the notation we have established above and, in particular, (28) and (29). For each $S \in \mathcal{T}'^{CD}$, G_S is of CD type and hence there exist

- a non-abelian simple group T with $|T| \leq \sqrt{r}/2$, and
- some positive integers $\ell, \kappa \geq 2$ with $\ell \leq r/7200$ and $\kappa \leq \log_2(r/4)/\log_2(60)$, and
- a primitive subgroup Q of $\mathrm{Sym}(\ell)$ with $|Q| < \ell^{2.01}$,

such that

$$G_S \leq W := (T^\ell \cdot (\mathrm{Out}(T) \times Q)) \mathrm{wr}\, \mathrm{Sym}(\kappa)$$

endowed of its natural compound diagonal action on Ω_S.

A fundamental result of Pyber and Shalev [41, Theorem I] shows that there exists an absolute constant c such that the number of conjugacy classes of primitive subgroups of $\mathrm{Sym}(\ell)$ is at most $2^{c(\log_2(\ell))^2}$. We deduce the following:

Fact 1: The number of possibilities for the group W, up to isomorphism, is at most

$$2|T|\ell\kappa 2^{c(\log_2(r))^2} \leq \kappa\ell|T|^\kappa \cdot 2^{c(\log_2(r))^2} \leq 2^{c(\log_2(r))^2 + \log_2(r)}.$$

Observe that the factor 2 in front of $\sqrt{r}/2$ accounts for the fact that for each natural number x, there exist at most two non-abelian simple groups having order x. In the last inequality we are using the inequality $r \geq \kappa\ell|T|^\kappa$.

Observe that $W/P_S \cong (\mathrm{Out}(T) \times Q)\mathrm{wr}\,\mathrm{Sym}(\kappa)$. Checking the order of the outer-automorphism group of a non-abelian simple group, we have $|\,\mathrm{Out}(T)| \leq \log_2(|T|)$ and, since $\kappa! \leq \kappa^\kappa$, we obtain

$$\begin{aligned} |W : P_S| &= (|\,\mathrm{Out}(T)||Q|)^\kappa \kappa! \leq (\log_2(|T|)\ell^{2.01})^\kappa \kappa! \leq (\log_2(|T|)\ell^{2.01}\kappa)^\kappa \\ &\leq 2^{\frac{\log_2(r/4)}{\log_2(60)}[\log_2(\log_2(\sqrt{r}/2)) + 2.01 \cdot \log_2(r/7200) + \log_2(\log_2(r/4)/\log_2(60))]} \\ &\leq 2^{(\log_2(r))^2/5}. \end{aligned}$$

Observe that P_S is the socle of W and hence it is uniquely determined by W. Now, $P_S \leq G_S = P_S R \leq W$ and the group R has at most $\lfloor \log_2(r) \rfloor$ generators, therefore the number of choices for G_S is at most $|W/P_S|^{\log_2(r)} = 2^{(\log_2(r))^3/5}$. Combining this with Fact 1, we obtain

Fact 2: The number of possibilities for the abstract group G_S, up to isomorphism, is at most $2^{(\log_2(r))^3/5 + c(\log_2(r))^2 + \log_2(r)}$.

Observe that P_S is the socle of G_S and hence it is uniquely determined by G_S. Let C be the core of $(G_S)_1 \cap P_S = (P_S)_1$ in P_S, see Figure 1. As $C \trianglelefteq P_S = T^{\kappa\ell}$, we have $P_S/C \cong T^s$, for some positive integer s. Therefore, we have

$$\binom{\kappa\ell}{s} \leq (\kappa\ell)^s$$

choices for C. As $|G_S : (G_S)_1| = r$, we deduce $|P_S : (P_S)_1| \leq r$ and hence $P_S/C \cong T^s$ has a faithful permutation representation on the set of right cosets of $(P_S)_1$ in P_S of degree at most r. From [11, Theorem 3.1], the minimal degree of a faithful permutation representation of T^s is $(m(T))^s$, where $m(T)$ is the minimal degree of a faithful permutation representation of the simple group T. Clearly, $m(T) \geq 5$. Therefore, we have

$$5^s \leq m(T)^s \leq r$$

and hence $5^s \leq r$. From this we deduce

$$s \leq \log_2(r)/\log_2(5).$$

Therefore, the number of choices for C is at most

$$\frac{\log_2(r)}{\log_2(5)} \cdot (\kappa\ell)^{\frac{\log_2(r)}{\log_2(5)}} \leq \frac{\log_2(r)}{\log_2(5)} \cdot 2^{\frac{\log_2(r)}{\log_2(5)}[\log_2(\log_2(r/4)/\log_2(60)) + \log_2(r/7200)]} \leq 2^{(\log_2(r))^2}.$$

Moreover,

$$|G_S : C| = |G_S : (G_S)_1||(G_S)_1 : C| = r|T|^{s-\kappa} \leq r(\sqrt{r}/2)^{\frac{\log_2(r)}{\log_2(5)}} \leq 2^{(\log_2(r))^2}.$$

The group $(G_S)_1$ is contained between G_S and C and hence we have at most $|G_S : C|^{\log_2(|G_S:C|)} = 2^{(\log_2(|G_S:C|))^2} \leq 2^{(\log_2(r))^4}$ choices for the subgroup $(G_S)_1$, when the subgroup C is given. Summing up, we have proved the following:

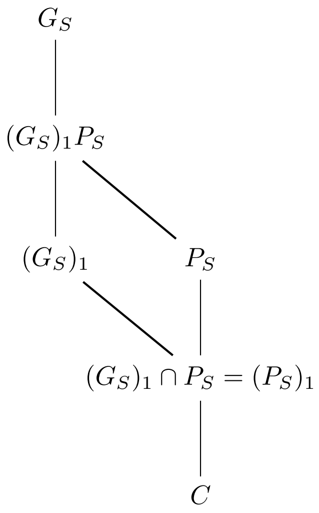

Figure 1. Subgroup lattice for G_S

Fact 3: Given the group G_S as an abstract group, the number of choices for $(G_S)_1$ is at most

$$2^{(\log_2(r))^4+(\log_2(r))^2}.$$

Combining Facts 2 and 3, we have that

$$|\{G_S \mid S \in \mathcal{T}'^{CD}\}| \leq 2^{(\log_2(r))^4+(\log_2(r))^3/5+(c+1)(\log_2(r))^2+\log_2(r)}.$$

Now, the proof follows immediately from Lemma 3.1: each permutation group in $\{G_S \mid S \in \mathcal{T}'^{CD}\}$ is acting as a group of automorphisms on at most $2^{3r/4}$ graphs. □

5.6. **Pulling the threads together.** Summing up, in this section we have proved the following result.

Theorem 5.11. *There exist two positive constants a' and b' with $|\mathcal{T}'| \leq 2^{r-a'r^{0.499}/(\log_2(r))^2} + b'$, whenever $r \geq r_\varepsilon$.*

Corollary 5.12. *There exist two positive constants b and r'_ε with $|\mathcal{T}'| \leq 2^{r-br^{0.499}/(\log_2(r))^2}$, whenever $r \geq r'_\varepsilon$.*

Proof. This follows from Theorem 5.11 by choosing a value for b that is smaller than a', with the result that the resulting increase to the power of 2 compensates for not adding the constant b'. □

6. The remaining sets in $\mathcal{T}$

In the previous section, we dealt with the sets in $\mathcal{T}'$; that is, the subsets $S \subseteq R$ that satisfy (H1) and admit a subgroup $G \leq \mathrm{Aut}(\Gamma(R,S))$ satisfying (H2), (H3), (H4) and (H5). We showed that the number of such sets is negligible compared to $2^{|R|}$. It remains to be shown that the total number of sets in $\mathcal{T}$, that is, those that satisfy (H1) and admit a subgroup $G \leq \mathrm{Aut}(\Gamma(R,S))$ satisfying (H2), (H3) and (H4) but not necessarily (H5), is also negligible. This is the goal of this section.

We begin by observing that since we have already counted the sets in $\mathcal{T}'$, we need only count the subsets in $\mathcal{T} \setminus \mathcal{T}'$; that is, subsets S that satisfy (H1) and admit a subgroup $G \leq \mathrm{Aut}(\Gamma(R,S))$ satisfying (H2), (H3) and (H4) with the additional property that the core G_R (of R in G) is non-trivial. (Note that some of these subsets S might also satisfy (H5) with a different choice of the subgroup $G \leq \mathrm{Aut}(\Gamma(G,S))$, but this only means that we might be counting some sets twice; the upper bound we arrive at will still be valid.)

In this section, we will rely on applying the results achieved in Section 5 to particular quotients of the group R. Therefore, to avoid possible misunderstandings, we use the notation $\mathcal{T}(R)$ and $\mathcal{T}'(R)$ for emphasising the ambient group R.

As mentioned above, if $S \in \mathcal{T}(R) \setminus \mathcal{T}'(R)$, then there exists a subgroup $G \leq \mathrm{Aut}(\Gamma(R,S))$ with

- **(H2):** R maximal in G and $|G_1| \geq 2^{|R|^{0.499}}$,
- **(H3):** $|G_R| \leq 4\log_2(|R|)$,
- **(H4):** some G_R-orbit is not fixed (setwise) by G_1,
- **($\neg$H5):** the core G_R of R in G is non-trivial.

Fix any such G. By (H4) with this G, we see that $G_R \neq R$ (since $RG_1 = G \trianglelefteq G$), so we have $1 < G_R < R$. Thus, the orbits of G_R form a non-trivial system of imprimitivity for G. There is a traditional definition of a quotient graph that can be formed in such a case; indeed, we have introduced this normal quotient in Definition 5.8 and we already used some of its properties in Theorem 5.9. However, to make our argument work, we define a different quotient graph.

Definition 6.1. Let Γ be a digraph whose vertex set V has been partitioned into a collection of sets, $\mathcal{B}$, with the additional property that given any two sets $B, B' \in \mathcal{B}$, and any vertex $v \in B$, the number of arcs from v to B' does not depend on the choice of $v \in B$. Define the *odd quotient digraph* of Γ with respect to the partition $\mathcal{B}$ to be the digraph whose vertices are the sets $B \in \mathcal{B}$, with an arc from B to B' if and only if the number of arcs from each $v \in B$ to B' is odd.

Clearly since G_R acts transitively on its orbits while fixing each of them setwise, the number of arcs from any vertex in one orbit to any other orbit does not depend on the choice of the vertex, so we can form the odd quotient digraph of $\Gamma := \Gamma(R, S)$ with respect to the orbits of G_R. We denote this odd quotient by $\Gamma_{G_R}^{\mathrm{odd}}$. Notice that any automorphism of Γ induces an automorphism of $\Gamma_{G_R}^{\mathrm{odd}}$.

As R/G_R acts regularly on the vertices of $\Gamma_{G_R}^{\mathrm{odd}}$, we observe that $\Gamma_{G_R}^{\mathrm{odd}}$ is a Cayley digraph on R/G_R, say $\Gamma_{G_R}^{\mathrm{odd}} = \Gamma(R/G_R, S')$. Moreover, G/G_R acts as a group of automorphisms of $\Gamma_{G_R}^{\mathrm{odd}}$. Let K be the kernel of the action of G/G_R on the vertices of $\Gamma_{G_R}^{\mathrm{odd}}$. Then

$$K = \bigcap_{g \in G} (G_1 G_R)^g.$$

Now, K is a normal subgroup of G fixing each G_R-orbit setwise. Therefore, by (H4), $K_1 = 1$, that is, $K = G_R$ and G/G_R acts faithfully on the vertices of $\Gamma_{G_R}^{\mathrm{odd}}$. So, in what follows, we may regard G/G_R as a subgroup of $\mathrm{Aut}(\Gamma_N^{\mathrm{odd}})$.

Since R is maximal in G, R/G_R is maximal in G/G_R. Moreover, $|G_1 G_R : G_R| = |G_1| \geq 2^{|R|^{0.499}} \geq 2^{|R/G_R|^{0.499}}$. Therefore,

$$G/G_R \text{ satisfies (H2).}$$

Since G_R is the core of R in G, we obtain that $G_R/G_R = 1$ is the core of R/G_R in G/G_R, that is, R/G_R is core-free in G/G_R and hence

$$G/G_R \text{ satisfies (H3), (H4) and (H5).}$$

In particular, $S' \in \mathcal{T}'(R/G_R)$ (recall that S' is the connection set for the odd quotient graph) and we are in a position to apply the main results of Section 5 to the quotient group R/G_R.

Theorem 6.2. *With the choice of ε from the start of Section 4, there is a value r''_ε and a positive constant b such that for every $r \geq r''_\varepsilon$ and for every regular subgroup R of* $\mathrm{Sym}(r)$*, the number of subsets S in $\mathcal{T}(R) \setminus \mathcal{T}'(R)$ is at most $2^{r - br^{0.499}/(4(\log_2(r))^3)+1}$.*

Proof. We use the notation laid out in this section, and for any $S \in \mathcal{T}(R) \setminus \mathcal{T}'(R)$ form the Cayley graph $\Gamma := \Gamma(R, S)$, and choose some fixed $G \leq \mathrm{Aut}(\Gamma)$ that satisfies (H2), (H3), (H4) and ($\neg$H5). Set $n := |G_R|$, and form the odd quotient graph $\Gamma_{G_R}^{\mathrm{odd}}$. Since $S \notin \mathcal{T}'(R)$, G_R is non-trivial. Define S' to be the connection set for $\Gamma_{G_R}^{\mathrm{odd}}$ viewed as a Cayley digraph over R/G_R, so $\Gamma_{G_R}^{\mathrm{odd}} = \Gamma(R/G_R, S')$.

From the discussion preceding the statement of this theorem, $S' \in \mathcal{T}'(R/G_R)$. Therefore, by Corollary 5.12, when $r/n \geq r'_\varepsilon$, the number of choices for S' is at most

$$2^{r/n - b(r/n)^{0.499}/(\log_2(r/n))^2},$$

for some positive constant b.

The cardinality of $\mathcal{T}(R) \setminus \mathcal{T}'(R)$ (which we are trying to count) is the number of choices for S. By this reduction, this value is the number of choices for S', times the product over all distinct cosets gG_R of G_R in R, of the number of choices for $S \cap gG_R$ that lead to gG_R being in or not in S', as appropriate. We have bounded the number of choices for S'; now we consider the number of choices for $S \cap gG_R$ that lead to gG_R being in or not in S', as appropriate.

By our construction of $\Gamma_{G_R}^{\mathrm{odd}}$, any connection set S' for $\Gamma_{G_R}^{\mathrm{odd}} = \Gamma(R/G_R, S')$ comes from any connection set S for Γ that satisfies the following conditions: $S \cap G_R$ can be any subset of G_R; and for any $g \in R \setminus G_R$, $S \cap gG_R$ must have odd cardinality if $gG_R \in S'$, and must have even cardinality if $gG_R \notin S'$.

Recall that given a finite set X, the number of subsets of X whose cardinality is even is equal to the number of subsets of X whose cardinality is odd, and both are equal to $2^{|X|-1}$.

Thus, the product over all distinct cosets gG_R of G_R in R, of the number of choices for $S \cap gG_R$ that lead to gG_R being in or not in S', as appropriate, is simply

$$2^n (2^{n-1})^{r/n-1} = 2^{r - r/n + 1}.$$

We therefore conclude that, when $r/n \geq r'_\varepsilon$, the cardinality of $\mathcal{T}(R) \setminus \mathcal{T}'(R)$ is at most

$$2^{r - r/n + 1} 2^{r/n - b(r/n)^{.499}/(\log_2(r/n))^2} = 2^{r - b(r/n)^{.499}/(\log_2(r/n))^2 + 1}.$$

Since $n \geq 2$, this is no bigger than

$$2^{r - b(r/n)^{.499}/(\log_2(r))^2 + 1} = 2^{r - br^{.499}/(n^{.499}(\log_2(r))^2) + 1} \leq 2^{r - b' r^{.499}/(n(\log_2(r))^2) + 1}.$$

Since $n \leq 4 \log_2(r)$, this is bounded above by

$$2^{r - br^{.499}/(4(\log_2(r))^3) + 1},$$

as claimed.

To ensure that $r/n > r'_\varepsilon$, since $n \leq 4\log_2(r)$ it is sufficient to require $r/\log_2(r) > 4r'_\varepsilon$. Since $r/\log_2(r)$ is an increasing function when $r > 2$, we take r''_ε large enough that $r''_\varepsilon/\log_2(r''_\varepsilon) = 4r'_\varepsilon$. □

Proof of Theorems 1.2 *and* 1.3. The proof follows immediately from Corollary 5.12 and Theorem 6.2, observing that these bounds should be added and the bound from Corollary 5.12 is the smaller of the two, so that doubling the bound from Theorem 6.2 gives an overall bound. □

7. Unlabeled digraphs

An *unlabeled* (di)graph is simply an equivalence class of (di)graphs under the relation "being isomorphic to". We will often identify a representative with its class. Using this terminology, we have the following unlabeled version of Theorem 1.2.

Theorem 1.5. *Let R be a group of order r. Then the ratio of the number of unlabeled* DRR*s on R over the number of unlabeled Cayley digraphs on R tends to* 1 *as $r \to \infty$.*

Proof. For this proof, we let $\mathrm{CD}(R)$ denote the set of unlabeled Cayley digraphs on R, we let $\mathrm{DRR}(R)$ denote the set of unlabeled DRRs on R, we let $\mathrm{NDG}(R)$ denote the set of unlabelled Cayley digraphs on R which are not DRRs, we let 2^R_{DRR} denote the collection of the subsets S of R with $\Gamma(R,S)$ a DRR and we let 2^R_{NDG} denote the collection of the subsets S of R with $\Gamma(R,S)$ not a DRR. In particular, $\mathrm{CD}(R) = \mathrm{DRR}(R) \cup \mathrm{NDG}(R)$ and $2^R = 2^R_{\mathrm{DRR}} \cup 2^R_{\mathrm{NDG}}$, where 2^R denotes the collection of the subsets of R. We aim to prove that $|\mathrm{DRR}(R)|/|\mathrm{CD}| \to 1$ as $|R| \to \infty$, or equivalently $|\mathrm{DRR}(R)|/|\mathrm{NDG}(R)| \to \infty$ as $|R| \to \infty$.

Let S_1 and S_2 be in 2^R_{DRR} and let $\Gamma_1 := \Gamma(R,S_1)$ and $\Gamma_2 := \Gamma(R,S_2)$. Suppose that $\Gamma_1 \cong \Gamma_2$ and let φ be a digraph isomorphism from Γ_1 to Γ_2. Without loss of generality, we may assume that $1^\varphi = 1$. Note that φ induces a group automorphism from $\mathrm{Aut}(\Gamma_1) = R$ to $\mathrm{Aut}(\Gamma_2) = R$. In particular, $\varphi \in \mathrm{Aut}(R)$ and S_1 and S_2 are conjugate via an element of $\mathrm{Aut}(R)$. This shows that

$$|\mathrm{DRR}(R)| \geq \frac{|2^R_{\mathrm{DRR}}|}{|\mathrm{Aut}(R)|}.$$

Since $|\mathrm{Aut}(R)| \leq 2^{(\log_2(r))^2}$, it follows that

$$|\mathrm{DRR}(R)| \geq \frac{|2^R_{\mathrm{DRR}}|}{2^{(\log_2(r))^2}}.$$

Clearly, $|\mathrm{NDG}(R)| \leq |2^R_{\mathrm{NDG}}|$. By Theorem 1.3, we have

$$\frac{|\mathrm{DRR}(R)|}{|\mathrm{NDG}(R)|} \geq \frac{(|2^R_{\mathrm{DRR}}|/2^{(\log_2(r))^2})}{|2^R_{\mathrm{NDG}}|} \to \infty,$$

as $|R| \to \infty$. This completes the proof. □

8. Remarks and comments

8.1. **Classification of finite simple groups.** The work in this paper is very much in line with the philosophy expressed in the pioneer paper [5] of Peter Cameron: many interesting problems on finite permutation groups can be reduced to problems on finite simple groups, and thus can often be completely solved. For a more recent survey, by Robert Guralnick, one of the leading experts in the applications of the CFSGs, see [16]. Clearly, with the CFSG the depth of our understanding of finite simple groups is a function of time, and hence with time deeper and deeper results can be obtained on finite permutation groups and on the symmetries of finite combinatorial structures, provided that one can obtain some sort of reduction to the realm of finite simple groups. When the classification of the finite simple groups was finally announced in 1979 at the Santa Cruz symposium on finite simple groups, many interesting problems on permutation groups were (broadly speaking) immediately trivialized: examples include the classification of the finite 2-transitive groups [5] or Sims' conjecture [6].

For this reason, a major theme in current research on finite permutation groups and on group actions on combinatorial structures involves reducing challenging problems in finite permutation groups to questions regarding simple groups. The heart of our approach for enumerating DRRs and Cayley digraphs are our reductions to questions concerning primitive groups and hence, using the O'Nan-Scott theorem, to questions on simple groups.

There are a number of very interesting questions still widely open where such a reduction might be the key for answering long-standing conjectures. A few of these that are particularly dear to our own hearts are: the enumeration of vertex-transitive graphs, the Polycirculant Conjecture on vertex-transitive graphs [29], or the Isbell Conjecture on homogeneous games [7, 19].

To avoid misunderstandings, we stress that we are far from saying that *all* interesting problems in finite permutation groups require a reduction to questions about simple groups in order to find a solution or an answer, or that such a reduction is always the most productive or advisable way to work on these problems. Recent work on finite semigroups and synchronizing primitive groups is an example in our opinion where exciting new mathematics is obtained without the CFSG, see [1].

8.2. **Asymptotic enumeration of vertex primitive Cayley digraphs.** Our proof of Theorem 1.2 heavily depends upon the Classification of Finite Simple Groups. However, using the exciting new results of Sun and Wilmes [44, 45], generalizing some influential results of paramount importance of Babai [2, 3] and Pyber [38], one can prove the following theorem without invoking the CFSG.

Theorem 8.1. *Let R be a group of order r. The proportion of subsets S of R such that $\mathrm{Aut}(\Gamma(R,S))$ acts primitively and not regularly on the vertices of $\Gamma(R,S)$ tends to 0 as r tends to ∞.*

In other words, without the CFSG one might prove (if so minded) that, when R is not a cyclic group of prime order, the automorphism group of a Cayley graph $\Gamma(R,S)$ over R admits a non-trivial system of imprimitivity with probility approaching 1 as $|R|$ tends to ∞.

Proof of Theorem 8.1. Observe that the results in Sections 2 and 3 do not depend upon the CFSG. Therefore, using Section 4 and Definition 4.1, we are left to prove that

$$\lim_{|R|\to\infty}\frac{|\{S\subseteq R \text{ satisfying (H1)–(H4) in Section 4} \mid \mathrm{Aut}(\Gamma(R,S)) \text{ primitive}\}|}{2^{|R|}}=0.$$

Let $S\subseteq R$, with S satisfying (H1)–(H4) in Section 4 and with $\mathrm{Aut}(\Gamma(R,S))$ primitive. A classical result of Babai [2, 3] shows that, if G is a primitive not 2-transitive group of degree n, then $|G|\le 2^{4\sqrt{n}(\log_2 n)^2}$. Pyber [38] has shown that, if G is a 2-transitive group of degree n with $\mathrm{Alt}(n)\not\le G$, then $|G|\le 2^{72(\log_2 n)^3}$. Although Pyber's result is not relevant to our situation since a 2-transitive group of automorphisms for a digraph arises only when the full automorphism group is $\mathrm{Sym}(n)$, the work was highly influential and stimulated further investigation. These results have been generalized by Sun and Wilmes [44, 45] motivated by some work in the context of coherent configurations and with a CFSG-free proof. In [44, Corollary 1.6], it is proven that, if G is a primitive permutation group of degree n, then either

(1) $|G|\le\exp(O(n^{1/3}\log^{7/3}n))$, or
(2) G is $\mathrm{Sym}(n)$ or $\mathrm{Alt}(n)$, or
(3) G is $\mathrm{Sym}(m)$ or $\mathrm{Alt}(m)$ where $n=\binom{m}{2}$ and G is endowed of its primitive action on the 2-subsets of $\{1,\ldots,m\}$, or
(4) G is a subgroup of $\mathrm{Sym}(m)\mathrm{wr}\,\mathrm{Sym}(2)$ containing $\mathrm{Alt}(m)^2$ where $n=m^2$ and $\mathrm{Sym}(m)\mathrm{wr}\,\mathrm{Sym}(2)$ is endowed of its natural primitive product action.

The first case does not arise in our context because $|G_1|\ge\exp(O(r^{0.499}))$. In the remaining cases G has rank at most 3 and hence the proof follows from Lemma 3.1. Since each of the three cases (2)–(4) above contributes at most 8 groups, and Lemma 3.1 tells us that each group comes from at most 8 connection sets, the numerator (counting the connection sets that aren't accounted for in Sections 2 and 3) is actually bounded by a constant. In fact, a careful examination of the groups and connection sets in these cases reveals that there are at most 8 connection sets that arise, since some of these connection sets arise in multiple cases, and even multiple times within a case. □

Following the estimates in Sections 2 and 3 one can give a quantitative version of Theorem 8.1. To obtain a slightly better estimate one has to refine Lemma 3.1 in the context of primitive groups. To do so, (using the notation in Lemma 3.1) observe that, if $G\le\mathrm{Sym}(\Omega)$ is primitive and not regular on Ω, then ω is the only element of Ω fixed by each permutation in G_ω and hence G acts on at most $2^{\frac{|\Omega|+1}{2}}$ digraphs with vertex set Ω.

8.3. **Undirected Cayley graphs.** Our proof of Theorem 1.2 does not extend to undirected Cayley graphs. Recall that $\Gamma(R,S)$ is undirected if and only if S is inverse-closed, that is, $S^{-1}:=\{s^{-1}\mid s\in S\}=S$. While the number of Cayley digraphs on R is $2^{|R|}$, which is a number that depends on the cardinality of R only, the number of undirected Cayley graphs on R is $2^{\frac{|R|+|I(R)|}{2}}$, where $I(R):=\{\iota\in R\mid \iota^2=1\}$, and hence depends on the algebraic structure of R.

It turns out that there are only two infinite families of groups that do no admit GRRs. The first family consists of abelian groups of exponent greater than two. If A is such a group and ι is the automorphism of A mapping every element to its inverse, then every Cayley graph on A admits $A\rtimes\langle\iota\rangle$ as a group of automorphisms. Since A has exponent greater than 2, $\iota\ne 1$ and hence no Cayley graph on A is a GRR. The other groups that do not admit GRRs are the generalised dicyclic groups, see [32, Definition 1.1] for a definition.

It was proved by Godsil that abelian groups of exponent greater than 2 and generalised dicyclic groups are the only two infinite families of groups that do not admit GRRs. The stronger Conjecture 8.2 was made (at various times) by Babai, Godsil, Imrich and Lovász.

Conjecture 8.2 (see [4], Conjecture 2.1 and [14], Conjecture 3.13)**.** *Let R be a group of order r which is neither generalised dicyclic nor abelian. The proportion of inverse-closed subsets S of R such that $\Gamma(R,S)$ is a* GRR *goes to 1 as $r\to\infty$.*

There are two places where our proofs do not immediately (or with some work) extend to undirected graphs, namely Lemmas 2.3 and 3.1. In these two lemmas, which are pivotal for our reductions, the fact that we are dealing with arbitrary Cayley digraphs seems to be essential. To be more precise, the proof of each of these lemmas generalises perfectly to the undirected case, but the resulting bounds do not produce a negligible fraction of all undirected Cayley graphs except for groups where $I(R)$ is very large; that is, groups that have many involutions. Currently we have no idea in how to fix this problem, that on the surface seems to be purely technical: the undirected case is much much harder on a technical level, but conceptually not very different. Here we simply mention two papers [42, 43], which inspired the work in this paper. In turn, [42, 43] owe a lot to the work of Imrich, Nowitz and Watkins in [18, 33, 34, 35]. The first paper [42] deals with the enumeration of digraphical Frobenius representations and the second [43] deals with graphical (and hence undirected) Frobenius representations. Thus [42] could be compared with the work in this paper and [43] could be compared to the asymptotic enumeration of undirected Cayley graphs (though the analogy does not run very deep). The key strategy in [43] for generalizing [42] to undirected Cayley graphs is to use a dichotomy argument: subdivide arbitrary groups R in two classes, the first class formed by the groups that do not admit any automorphisms inverting many elements and the second class formed by the groups that do admit such an automorphism. (We are deliberately vague about the precise meaning of "many" here, because in our new context we have no clear idea of what "many" might mean.) The groups falling into the first class are dealt with "probabilistic" arguments, whereas the groups in the second class have a highly restricted structure and hence can be analysed with ad-hoc arguments. We hope that in the future a similar approach could also be used for asymptotically enumerating undirected Cayley graphs and hence resolving Conjecture 8.2.

8.4. **Vertex-transitive digraphs.** Some of the arguments in this paper generalize, again with no work or with only little work, to the problem of asymptotic enumeration of vertex-transitive digraphs on n vertices (up to isomorphism). Using the same approach as in this paper and in particular Lemma 3.1, in order to enumerate vertex-transitive digraphs it seems natural and important to asymptotically estimate (up to conjugation in $\mathrm{Sym}(n)$) one of the following classes of transitive permutation groups:

- *minimally transitive groups*, that is, transitive subgroups G of $\mathrm{Sym}(n)$ with the property that each proper subgroup of G is intransitive;
- *transitive* 2*-closed groups.*

Indeed, suppose as a running conjecture that one of the previous two classes of permutation groups has at most $2^{o(n)}$ elements. Just to make these ideas clear, let us assume that the number of 2-closed subgroups of $\mathrm{Sym}(n)$ up to conjugation is at most $2^{o(n)}$. This seems a reasonable conjecture to make: the regular subgroups of $\mathrm{Sym}(n)$ are 2-closed and, up to conjugation, they are in one-to-one correspondence with the groups of order n up to isomorphism. Pyber [40] has shown that there are at most $n^{\left(\frac{2}{27}+o(1)\right)\mu(n)^2}$ groups of order n, where $\mu(n) = \max_{i=1}^{k} g_i$, $n = \prod_{i=1}^{k} p_i^{g_i}$ and $p_1, \ldots, p_k$ are distinct primes. Therefore, we have only at most $n^{\log_2(n)^2} \leq 2^{(\log_2 n)^3}$ regular subgroups up to conjugation. Our wishful thinking requires that there are also at most $2^{o(n)}$ transitive subgroups of $\mathrm{Sym}(n)$ which are 2-closed and not regular. If this happens to be true, applying Lemma 3.1 allows us to conclude that there are at most $2^{3n/4+o(n)}$ vertex-transitive digraphs on n vertices that are not Cayley digraphs. Since Theorem 1.2 shows that we have at least $2^{n+o(n)}$ Cayley digraphs on n vertices, we deduce that most vertex-transitive graphs are Cayley digraphs (actually DRRs), thus answering a question of McKay and Praeger [30, page 54]. A little bit of evidence that this approach has potential is given by Pyber [39, Theorem 4.4].

8.5. **Normal Cayley graphs.** A Cayley (di)graph Γ of G is said to be a *normal* Cayley (di)graph of R if the regular representation of R is normal in $\mathrm{Aut}(\Gamma)$. Xu conjectured that almost all Cayley (di)graphs of R are normal Cayley (di)graphs of R; we have given his formulation more precisely in Theorem 1.4. As noted, we have proven the directed version of this conjecture as any DRR on R has automorphism group R and hence it is a normal Cayley digraph of R. Similar results for undirected graphs, supporting the conjectures of Xu are proved in [9, 32], when R is an abelian group and when R is a dicyclic group.

We find that, in principle and very likely in practise, Conjecture 8.2 and the undirected conjecture of Xu are very similar. Indeed, requiring that $\Gamma(R, S)$ is a normal Cayley graph means requiring that $\mathrm{Aut}(\Gamma(R, S)) \leq R \rtimes \mathrm{Aut}(R)$. Now, since $|\mathrm{Aut}(R)| \leq 2^{(\log_2(|R|))^2}$ is small compared to the number of Cayley graphs, it is reasonable to expect that most Cayley graphs on R are GRRs if and only if most Cayley graphs on R are normal. The forward implication is clear, because each GRR is a normal Cayley graph.

8.6. **Asymtotic enumeration of vertex-transitive graphs and Cayley graphs of bounded valency.** There is another problem we would like to mention. Let d be a positive number. The asymptotic enumeration of vertex-transitive graphs and of Cayley graphs of valency d is a widely open question that has hardly been touched so far. In this context, in our opinion it is more interesting and natural to consider only connected graphs; this also avoids degeneracies. The case $d = 2$ is trivial. Thus the first interesting case is $d = 3$ and this already offers intricate questions in group generation. The best result for $d = 3$ is Theorem 1.2 in [36] where (roughly speaking) it is proved that the functions counting the number of GRRs, Cayley graphs, and vertex-transitive graphs of valency 3 and up to n vertices are asymptotically very similar. Surprisingly, the same result holds if "vertex-transitive" is replaced with the much stronger requirement of the graphs being "5-arc-transitive".

To prove analogous results for arbitrary valencies following the arguments in [36], it seems important to have a strong understanding of certain transitive subgroups of $\mathrm{Sym}(n)$. In this context, we pose a conjecture. First, however, we need to establish the setting. Let G be a transitive subgroup of $\mathrm{Sym}(n)$ and let $\omega \in \{1,\dots,n\}$. Let $O_1,\dots,O_\kappa$ be the orbits of G_ω on $\{1,\dots,n\}$. For each $i \in \{1,\dots,\kappa\}$, there is a digraph Γ_i associated to O_i called the *orbital* digraph for G: the vertex set of Γ_i is $\{1,\dots,n\}$ and the arc set of Γ_i is $\{(\omega,\delta)^g \mid g \in G, \delta \in O_i\}$. For each subset $I \subseteq \{1,\dots,\kappa\}$, we may associate a *merged orbital* digraph Γ_I where the vertex set is again $\{1,\dots,n\}$ and the arc set is $\{(\omega,\delta)^g \mid g \in G, \delta \in O_i, i \in I\}$. It is clear that the merged orbital digraphs of G are exactly the digraphs Γ with vertex set $\{1,\dots,n\}$ and with $G \leq \mathrm{Aut}(\Gamma)$.

Conjecture 8.3. There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that the number of transitive groups of degree n (up to conjugation in $\mathrm{Sym}(n)$) admitting a connected merged digraph of valency d is at most $n^{f(d)\log n}$.

This conjecture is trivially true using Sims' conjecture, if the group G is primitive. It is also true when $d \leq 3$ by the work in [36]. Much is known about the generation of the transitive subgroups of $\mathrm{Sym}(n)$, see for instance [26, 27, 31]. However, there seems to have been no investigation into the number of generators that are necessary for a transitive subgroup G of $\mathrm{Sym}(n)$ where some information on the merged orbitals of G is given.

8.7. **Bipartite regular representations.** Now that we have established that most Cayley digraphs are DRRs, there are other natural questions that arise. For instance, suppose that R has subgroups having index 2, is it true that most bipartite Cayley digraphs on R are DRRs? A partial answer to this question (only in the case of abelian groups) is given in [10].

References

[1] J. Araújo, P. J. Cameron, B. Steinberg, Between primitive and 2-transitive: Synchronization and its frineds, *EMS Surv. Math. Sci.* **4** (2017), 101–184.

[2] L. Babai, On the order of uniprimitive permutation groups, *Annals of Math.* **113** (1981), 553–568.

[3] L. Babai, On the order of doubly transitive permutation groups, *Invent. Math.* **65** (1982), 473–484.

[4] L. Babai, C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15.

[5] P. J. Cameron, Finite permutation groups and finite simple groups, *Bull. London Math. Soc.* **13** (1981), 1–22.

[6] P. J. Cameron, C. E. Praeger, J. Saxl, G. M. Seitz, On the Sims Conjecture and Distance Transitive Graphs, *Bull. London Math. Soc.* **15** (1983), 499–506.

[7] E. Crestani, P. Spiga, Fixed-point-free elements in p-groups, *Israel Jour. Mathematics* **180** (2010), 413–425.

[8] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996.

[9] E. Dobson, P. Spiga, G. Verret, Cayley graphs on abelian groups, *Combinatorica* **36** (2016), 371–393.

[10] J.-L. Du, Y.-Q. Feng, P. Spiga, On the existence and the enumeration of bipartite regular representations of Cayley graphs over abelian groups, in preparation.

[11] D. Easdown, C. E. Praeger, On minimal faithful permutation representations of finite groups, *Bull. Australian Math. Soc.* **38** (1988), 207–220.

[12] P. Erdös, A. Rényi, Asymmetric graphs, *Acta Math. Acad. Sci. Hungar.* **14** (1963), 295–315.

[13] G. W. Ford, G. E. Uhlenbeck. Combinatorial problems in the theory of graphs, IV, *Proc. Natl. Acad. Sci. USA* **43** (1957), 163–167.

[14] C. D. Godsil, On the full automorphism group of a graph, *Combinatorica* **1** (1981), 243–256.

[15] C. Godsil, G. Royle. Algebraic graph theory. Graduate Texts in Mathematics, 207. Springer-Verlag, New York, 2001.

[16] R. Guralnick, Applications of the classification of finite simple groups. Proceedings of the International Congress of Mathematicians – Seoul 2014. Vol. II, 163–177, Kyung Moon Sa, Seoul, 2014.

[17] F. Harary, *Graphical Enumeration*, Academic Press, New York, 1973.

[18] W. Imrich, M. Watkins, On graphical regular representations of cyclic extensions of groups, *Pacific J. Math.* **54** (1974), 1–17.

[19] J. R. Isbell, Homogeneous games II, *Proc. Amer. Mathematical Soc.* **11** (1960), 159–161.

[20] M. W. Liebeck, C. E. Praeger, J. Saxl, On the O'Nan-Scott theorem for finite primitive permutation groups, *J. Australian Math. Soc. (A)* **44** (1988), 389–396

[21] M. W. Liebeck, C. E. Praeger, J. Saxl, Regular subgroups of primitive permutation groups, Memoirs of the Americal Mathematical Society 952, Providence, Rhode Island.

[22] M. W. Liebeck, C. E. Praeger, J. Saxl, Transitive subgroups of Primitive Permutation Groups, *J. Algebra* **234** (2000), 291–361.

[23] M. W. Liebeck, C. E. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups, *Memoirs of the American Mathematical Society*, Volume **86**, Number **432**, 1990.

[24] M. W. Liebeck, C. E. Praeger, J. Saxl, On factorizations of almost simple groups, *J. Algebra* **185** (1996), no. 2, 409–419.

[25] A. Lubotzky, Enumerating boundedly Generated Finite Groups, *J. Algebra* **238** (2001), 194–199.

[26] A. Lucchini, F. Menegazzo, M. Morigi, Asymptotic results for transitive permutation groups, *Bull. London Math. Soc.* **32** (2000), 191–195.

[27] A. Lucchini, F. Menegazzo, M. Morigi, Asymptotic results for primitive permutation groups and irreducile linear groups, *J. Algera* **223** (2000), 154–170.

[28] A. Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.

[29] D. Marušič, On vertex symmetric digraphs, *Discrete Math.* **36** (1981), 69–81.

[30] B. D. McKay, C. E. Praeger, Vertex-transitive graphs which are not Cayley graphs, I, *J. Austral. Math. Soc. (Series A)* **56** (1994), 53–63.

[31] F. Menegazzo, The number of generators of a finite group, *Irish Math. Soc. Bulletin* **50** (2003), 117–128.

[32] J. Morris, P. Spiga, G. Verret, Automorphisms of Cayley graphs on generalised dicyclic groups, *European J. Combin.* **43** (2015), 68–81.

[33] L. A. Nowitz, M. Watkins, Graphical regular representations of direct product of groups, *Monatsh. Math.* **76** (1972), 168–171.

[34] L. A. Nowitz, M. Watkins, Graphical regular represntations of non-abelian groups, II, *Canad. J. Math.* **24** (1972), 1009–1018.

[35] L. A. Notwitz, M. Watkins, Graphical regular representations of non-abelian groups, I, *Canad. J. Math.* **24** (1972), 993–1008.

[36] P. Potočnik, P. Spiga, G. Verret, Asymptotic enumeration of vertex-transitive graphs of fixed valency, *J. Comb. Theory Ser.* **122** (2017), 221–240.

[37] C. E. Praeger, Finite quasiprimitive graphs, in *Surveys in combinatorics*, London Mathematical Society Lecture Note Series, vol. 24 (1997), 65–85.

[38] L. Pyber, The orders of doubly transitive permutation groups, elementary estimates, *J. Comb. Theory Sec. A* **62** (1993), 361–366.

[39] L. Pyber, Asymptotic results for permutation grousp, *Groups and Computation*, L. Finkelstein and W. M. Kantor, eds., DIMACS Series in Discrete Math. and Theoretical Comp. Sci. no. 11, Providence, RI: Amer. Math. Soc. 197–219.

[40] L. Pyber, Enumerating finite groups of a given order, *Ann. Math.* **137** (1993), 203–220.

[41] L. Pyber, A. Shalev, Asymtotic results for primitive permutation groups, *J. Algebra* **188** (1997), 103–124.

[42] P. Spiga, On the existence of Frobenius digraphical representations, *The Electronic Journal of Combinatorics* **25** (2018), paper #P2.6.

[43] P. Spiga, On the existence of graphical Frobenius representations and their asymptotic enumeration: an answer to the GFR conjecture, *Submitted*.

[44] X. Sun, J. Wilmes, Structure and automorphisms of primitive coherent configurations, `arXiv:1510.02195 [math.CO]`

[45] J. Wilmes, *Structure, automorphisms, and isomorphisms of regular combinatorial objects*, Thesis (Ph.D.)–The University of Chicago, 2016, 169 pages.

[46] M.Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319.

Department of Mathematics and Computer Science, University of Lethbridge,
Lethbridge, AB. T1K 3M4. Canada.
E-mail address: `joy.morris@uleth.ca`

Pablo Spiga, Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca,
Via Cozzi 55, 20125 Milano, Italy
E-mail address: `pablo.spiga@unimib.it`