Manuscript version: Author’s Accepted Manuscript
The version presented in WRAP is the author’s accepted manuscript and may differ from the published version or Version of Record.

Persistent WRAP URL:
http://wrap.warwick.ac.uk/154812

How to cite:
Please refer to published version for the most recent bibliographic citation information. If a published version is known of, the repository item page linked to above, will contain details on accessing it.

Copyright and reuse:
The Warwick Research Archive Portal (WRAP) makes this work by researchers of the University of Warwick available open access under the following conditions.

© 2021 Elsevier. Licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International http://creativecommons.org/licenses/by-nc-nd/4.0/.

Publisher’s statement:
Please refer to the repository item page, publisher’s statement section, for further information.

For more information, please contact the WRAP Team at: wrap@warwick.ac.uk.
THE TRANSITIVE GROUPS OF DEGREE 48 AND SOME APPLICATIONS

DEREK HOLT, GORDON ROYLE, AND GARETH TRACEY

Abstract. The primary purpose of this paper is to report on the successful enumeration in Magma of representatives of the 195,826,352 conjugacy classes of transitive subgroups of the symmetric group $S_{48}$ of degree 48. In addition, we have determined that 25707 of these groups are minimal transitive and that 713 of them are elusive. The minimal transitive examples have been used to enumerate the vertex-transitive groups of degree 48, of which there are 1,538,868,366, all but 0.1625% of which arise as Cayley graphs. We have also found that the largest number of elements required to generate any of these groups is 10, and we have used this fact to improve previous general bounds of the third author on the number of elements required to generate an arbitrary transitive permutation group of a given degree. The details of the proof of this improved bound will be published as a separate paper.

1. Introduction

Since late in the 19th century, significant effort has been devoted to compiling catalogues and databases of various types of groups, including complete lists of (representatives of the conjugacy classes of) the transitive and primitive subgroups of the symmetric groups of small degree. For the transitive groups, earlier references include [27, 26] (with corrections in [30]) for degrees up to 12, [13] for degrees up to 31, [3] for the significantly more difficult case of degree 32, and [12] for degrees 33–47. (There are 2,801,324 groups of degree 32, and 501,045 groups of all other degrees up to 47.) Apart from the early work of Miller, these lists have been compiled by computer, using GAP [8] and Magma [2].

Degree 48 is once again significantly more difficult than earlier degrees, because there are many more groups and the computations involved need more time and computer memory. The main purpose of this paper is to report on the successful enumeration of conjugacy class representatives of the transitive subgroups of degree 48, which is the topic of Section 2. The result is summarised in the following theorem.

**Theorem 1.1.** There are 195,826,352 conjugacy classes of transitive subgroups of the symmetric group $S_{48}$.

The complete list of these subgroups is available in Magma from an optional database that can be downloaded by users from the Magma website.

The computations were carried out in Magma and the final successful runs required about one year of cpu-time (this does not include unsuccessful attempts that had to be aborted for various reasons). The methods used are theoretically essentially the same as those described in [3] and [12] for degrees 32 – 48, but completing the calculations in degree 48 proved to be significantly more challenging, and parts of the Magma code needed to be optimised or sometimes re-designed to cope with the larger amounts of data. For this reason they took more than two years of real time to complete.
Table 1. Transitive, minimal transitive, and elusive groups of degree 48

| MinBlockSize | TransGps | MinTrans | Elusive |
|--------------|----------|----------|---------|
| 2            | 192327620| 15046    | 108     |
| 3            | 3397563  | 10625    | 590     |
| 4            | 94121    | 36       | 3       |
| 6            | 5011     | 0        | 12      |
| 8            | 1275     | 0        | 0       |
| 12           | 103      | 0        | 0       |
| 16           | 646      | 0        | 0       |
| 24           | 9        | 0        | 0       |
| Primitive    | 4        | 0        | 0       |
| Total        | 195826352| 25707    | 713     |

Although the computations were carried out serially on a single processor, they are intrinsically extremely parallelisable: about 98% of the cpu-time was for imprimitive groups with blocks of size 2 and, as we shall explain shortly, that case splits into 25000 independent calculations.

We anticipate that it would be feasible to extend the catalogues up to degree 63, but that degree 64 will remain out of range for the foreseeable future.

We subsequently used our catalogue to identify those groups of degree 48 that are minimal transitive (that is, they have no proper transitive subgroups) and those that are elusive (that is, they contain no fixed-point-free elements of prime order). We shall report on this in Section 3. The various counts of groups involved are summarised in Table 1 where the imprimitive groups have been counted according to the smallest size of a block of imprimitivity.

In Section 4 we describe the computation of the vertex-transitive graphs of order 48, along with some associated data.

We denote the smallest size of a generating set of a group $G$ by $d(G)$. We have established that $d(G) \leq 10$ for all transitive groups of degree 48. In fact, the only examples with $d(G) = 10$ have minimal block size 3 and have 10-generator transitive groups of degree 32 as quotients. The groups with block size 2 all satisfy $d(G) \leq 9$.

We shall discuss how we computed this information at the beginning of Section 5. There we shall explain how these bounds on $d(G)$ have enabled the third author to remove the exceptional cases of the general bound on $d(G)$ for transitive permutation groups of degree $n$ that he established in [33], and thereby to complete the proof of the following result, where logarithms are to the base 2.

**Theorem 1.2.** Let $G$ be a transitive permutation group of degree $n$. Then

$$d(G) \leq \left\lfloor \frac{cn}{\sqrt{\log n}} \right\rfloor$$

where $c := \frac{\sqrt{3}}{2}$.

(It was proved by Lucchini, Menegazzo and Morigi in [22] that this result holds for some unspecified constant $c$.) Since the proof of this result involves some lengthy case-by-case analyses,
we shall just summarise it in Section 5 of this paper, and the details will be published separately (see [34]).

In a related application, the third author is now able to bound the constant \( d \) in the result proved in [23] that
\[
d(G) \leq d \log n / \sqrt{\log \log n}
\]
for primitive subgroups \( G \) of \( S_n \).

The computations described in this paper were carried out on a number of different machines; the most time consuming were done using a model of type “Intel(R) Xeon(R) 3.10GHz” with about 400GBytes of RAM.

**Notation:** For a finite group \( G \), we will write \( \Phi(G) \), \( R(G) \), \([G,G]\) for the Frattini subgroup, soluble radical, and derived subgroup of \( G \), respectively. We will mostly use the notation from [36] for group names, although we simply write \( n \) for the cyclic group of order \( n \) when there is no danger of confusion.

### 2. Computing the transitive groups of degree 48

The primitive permutation groups are known up to degree 40951 (see [5]) and are incorporated into the databases of both **Magma** and **GAP**, and so we need only consider the imprimitive groups. By definition, if a group \( G \) acting transitively on the set \( \Omega \) of size \( n \) is not primitive, then there is at least one partition of \( \Omega \) into a block system \( B \) such that \( G \) permutes the blocks of \( B \). If we let \( G^B \) denote the action of \( G \) on the blocks (“the top group”) and if \( B \) has \( n/k \) blocks of size \( k \), then \( G^B \) is a transitive permutation group of degree \( n/k \). We say that the block system \( B \) is *minimal* if \( k \) is minimal among block systems with \( k > 1 \). Then we can associate to each group \( G \) a set of pairs of the form
\[
\{(k, G^B) : B \text{ is a minimal block system for } G \text{ with blocks of size } k\}.
\]

If this set contains more than one pair (imprimitive groups may of course have more than one minimal block system), then we wish to distinguish just one of them. Thus we define the *signature* of an imprimitive permutation group to be the lexicographically least pair \( (k, G^B) \) associated with \( G \), where the second component is indexed according to its order in the list of transitive groups of degree \( n/k \) already in **Magma** (which is the same as the ordering in **GAP**). But note that it can happen that two different minimal block systems of \( G \) define the same signature.

We separate the computation into parts, with each part constructing only the groups with a particular signature. Given an integer \( k \) such that \( 1 < k < n \), and a transitive group \( H \) of degree \( n/k \), the wreath product \( S_k \wr H \) contains (a conjugate of) every transitive group of degree \( n \) with signature \( (k, H) \). So these groups can all be found by exploring the subgroup lattice of \( S_k \wr H \) (although there are complications arising from the fact that we want representatives of subgroups up to conjugacy in \( S_n \)).

A naive approach to the problem for a fixed \( k \) is to deal with all candidates \( H \) simultaneously, by starting with \( S_k \wr S_{n/k} \), and repeatedly using the **MaximalSubgroups** command of **Magma**, thereby traversing the subgroup lattice downwards and in a breadth-first fashion, pruning each branch of the search as soon as it produces groups with signature differing from \( H \), while using

---

1 This has recently been extended to degree 8191 by Ben Stratford, a student of the first author.
conjugacy tests to avoid duplication. (We also have to eliminate duplicates arising from a group preserving more than one minimal block system with blocks of size $k$.) This was successfully applied in all cases to the transitive groups of degrees $33 - 47$, and we refer the reader to [12, Section 2] for further details. In degree 48, we successfully applied this method to groups with signatures $(k, H)$ with $k \geq 6$; that is for $k = 6, 8, 12, 16$ and 24. The cpu-times in these cases were of order 10 hours, 30 minutes, 3 minutes, 70 minutes, and a few seconds, respectively.

For $k = 2, 3$ and 4, we used the methods described in [12, Section 3] (and also in [3, Section 2.2] for $k = 2$).

The methods for $k = 3$ were essentially the same as in degree 36, but considerably more time-consuming. We have $G \leq S_3 \wr S_{16} \cong C_3^{16} : (C_2 \wr S_{16})$. Let $\rho$ be the induced projection of $G$ onto $C_2 \wr S_{16}$. Then, since we are assuming that $G$ is transitive, $\rho(G)$ must project onto a transitive subgroup of $S_{16}$, and the existing catalogues contain the 1954 possibilities for this projection. Furthermore, either

(i) $\rho(G)$ is a transitive subgroup of $S_{32}$ arising from the imprimitive action of $C_2 \wr S_{16}$, in which case we use the 2801 324 transitive groups of degree 32 as a list of candidates for $\rho(G)$; or

(ii) $\rho(G)$ is an intransitive group of degree 32 that projects onto a transitive subgroup of $S_{16}$. In that case, it is not hard to show that $\rho(G)$ must be conjugate to the natural complement of the base group of $C_2 \wr H$, where $H$ is one of the 1954 transitive groups of degree 16. (We also checked this computationally.)

We enumerated the groups with $k = 3$ by considering each of the $2801324 + 1954$ possibilities for $\rho(G)$ in turn. This involves a cohomology computation, which is analogous to that for the case $k = 2$, which we shall discuss below. The computation for $k = 3$ took a total of about 104 hours of cpu-time. Of the $3397563$ resulting groups, $\rho(G)$ is transitive for all except 55715. Similarly, for $k = 4$, we used the same techniques as in degrees 36 and 40, and the total cpu-time was about 9 hours.

The vast majority of the computational work was for the case $k = 2$, and we shall briefly recall from [3, 12] how we proceed in this case. We have $G \leq W := C_2 \wr H$, where $H := G^B$ is one of the groups in the known list of 25000 transitive groups of degree 24. Again we calculate those groups with signature $(2, H)$ for each individual group $H$, and the 25000 calculations involved are independent and could in principle be done in parallel.

Let $K \cong C_2^{24}$ be the kernel of the action of $W$ on $B$. Then we can regard $K$ as a module for $H$ over the field $\mathbb{F}_2$ of order 2, and $M := G \cap K$ is an $\mathbb{F}_2 H$-submodule. We can use the Magma commands GModule and Submodules to find all such submodules. In fact, since we are looking for representatives of the conjugacy classes of transitive subgroups of $W$, we only want one representative of the conjugation action of $L := C_2 \wr N_{S_{24}}(H)$ on the set all $\mathbb{F}_2 H$-submodules $M$ of $K$, and we use the Magma command IsConjugate to find such representatives.

Now, for each such pair $(H, M)$, the transitive groups $G$ with $H = G^B$ and $M = G \cap K$ correspond to complements of $K/M$ in $W/M$, and the $W$-conjugacy classes of such complements correspond to elements of the cohomology group $H^1(H, K/M)$, which can be computed in Magma.
We also need to test these groups $G$ for conjugacy under the action of $N_L(M)$. In some cases when $H^1(H, K/M)$ is reasonably small, this can be done in straightforward fashion using Magma’s `IsConjugate` function. But in many cases this was not feasible, and we used the induced action on the cohomology group method that is described in detail in [3, Section 2.2]. Finally, for each $G$ that we find, we need to find all block systems with block size 2 preserved by $G$, so that we can eliminate occurrences of groups that are conjugate in $S_n$ but arise either for distinct pairs $(H, M)$ or more than once for the same pair. Again we refer the reader to [3, Section 2.2] for further details.

Here are some statistics concerning some of these calculations.

- The numbers of groups arising from the 25000 candidates for the top group $H$ ranges from 3 to 3 642 186, with average 7693 and median 778. This number is less than 10000 for more than 90% of the top groups. For the majority of these groups $H$, the computations were fast. For example, for the groups $H = \text{TransitiveGroup}(24, k)$ with $20000 < k \leq 25000$, (20% of the groups $H$) the total cpu-time was about 92.4 hours (just over 1% of the total) and the total number of groups $G$ that arise is 2 963 853 (about 1.5% of the total).
- The highest dimension of a cohomology group $H^1(H, K/M)$ was 26. In that case, $|H^1(H, K/M)| = 2^{26} = 67108864$. This occurred with $H = \text{TransitiveGroup}(25, 4010)$ and $|M| = 2^{12}$. The computation of the orbits of the induced action of $N_L(M)$ on the elements of $H^1(H, K/M)$ is one of the most memory intensive parts of the process, and in this example there were 201 792 such orbits. If an example of much higher dimension than this had been encountered (which we might expect to be the case for a corresponding attempt to find the transitive groups of degree 64), then this orbit computation might not have been feasible.
- The case $H = \text{TransitiveGroup}(25, 11363)$ resulted in the largest number of groups $G$, namely 3 642 186. There were 240 possibilities for $M$. This case took about 34 hours of cpu-time, using about 73GBytes RAM.
- The pair $(H, M)$ that resulted in the most groups $G$, namely 1 054 720, arose with $H = \text{TransitiveGroup}(25, 13329)$ and $|M| = 2^7$. Although $H^1(H, K/M)$ had dimension only 22 in this case, there were many more orbits of the action than in the case with dimension 26 discussed above.

3. Minimal transitive and elusive groups

3.1. Minimal transitive groups. For many applications that involve considering all possible transitive actions of a certain degree, it is sufficient to consider only the minimal transitive groups i.e., transitive groups with no proper transitive subgroups. (One example of this was discussed in [12, Section 5], where all vertex-transitive graphs of degrees 33–47 are constructed.) Testing if a transitive group is minimal can be done by finding all of its maximal subgroups and verifying that none is transitive. As most of the groups are not minimal transitive, it proves useful in practice to first construct some random subgroups in an attempt to find a transitive proper subgroup, only undertaking the more expensive step of finding all maximal subgroups if
this fails. Even with 195 million groups to check, this computation is relatively straightforward, and results in a list of 25707 minimal transitive groups, all of which have minimal blocks of sizes 2, 3 or 4 — this data is summarised in Table 1.

3.2. Elusive groups. A transitive permutation group $G$ is called elusive if it contains no fixed-point-free elements (i.e., derangements) of prime order. Elusive groups are interesting because of their connection to Marušić’s Polycirculant Conjecture [25] which asserts that the automorphism group of a vertex-transitive digraph is never elusive. In principle, a positive resolution of the Polycirculant Conjecture may simplify the construction and analysis of vertex-transitive graphs and digraphs, as it would then always be possible to assume the presence of an automorphism with $n/p$ cycles of length $p$ for some prime $p$.

It is relatively easy to test the groups for the property of being elusive by checking to see if any of the conjugacy class representatives are derangements of prime order. For the larger groups, it is often faster to first generate some randomly selected elements inside each of the Sylow subgroups in the hope of stumbling on a suitable derangement without the cost of computing all the conjugacy classes.

The results of this computation reveal that there are 713 elusive groups of degree 48, with orders ranging from 5184 to 806,215,680,000. The numbers of elusive groups of degree 48 with each minimal blocksize are given in Table 1. If an elusive group has minimal blocks of different sizes (say 2 and 3), then it is grouped and counted according to the smallest. In contrast, note that there are only 30 elusive groups of degree less than 48: see [12, Proposition 6.1].

Of these 713 groups, 700 have a unique minimal normal subgroup, and while each of the remaining 13 groups has multiple minimal normal subgroups, these minimal normal subgroups are conjugate in $S_{48}$. Therefore we can partition the elusive groups according to the unique conjugacy class of their minimal normal subgroup(s). Collectively, the 713 elusive groups share just 7 pairwise non-conjugate minimal normal subgroups. Table 2 shows the different minimal normal subgroups that occur and the number of elusive groups with that particular minimal normal subgroup. In addition, it gives the order of the normalizer (in $S_{48}$) of that subgroup, while the final column shows the possible minimal block sizes that occur for that minimal normal subgroup. All but one of the possible minimal normal subgroups are elementary abelian, but two non-conjugate (but obviously isomorphic) groups of orders $2^8$ and $3^8$ occur. For example, the first row shows that an elusive group with minimal normal subgroup $C_3^4$ either has minimal blocks of size 2 (only) or minimal blocks of sizes both 2 and 3.

With this many elusive groups, and no obvious way to get a compact description, it seems unlikely that the Polycirculant Conjecture can be proved by first classifying elusive groups.

4. Vertex-transitive graphs of order 48

The class of vertex-transitive graphs plays a central role in algebraic graph theory, often providing extremal cases or illuminating examples in the study of many graphical properties. Given a list of all the transitive groups of some fixed degree $d$, it is conceptually simple to compute all of the vertex-transitive graphs of order $d$, by computing the $G$-transitive graphs for each group $G$ in turn, and then removing all but one isomorphic copy of each graph. We
Table 2. Minimal normal subgroups of elusive groups of degree 48

| Group | Normalizer | Frequency | Min. Blocks |
|-------|------------|-----------|-------------|
| $C_3^4$ | $2^{17} \cdot 3^{18}$ | 22 | \{2\} or \{2,3\} |
| $C_2^8$ | $2^{28} \cdot 3^3$ | 3 | \{4\} |
| $C_2^8$ | $2^{43} \cdot 3^5$ | 75 | \{2\} |
| $C_3^8$ | $2^{19} \cdot 3^{21}$ | 575 | \{3\} |
| $C_3^8$ | $2^{11} \cdot 3^{17} \cdot 7$ | 2 | \{3\} |
| $C_2^{16}$ | $2^{39} \cdot 3^{10} \cdot 5 \cdot 7$ | 24 | \{2\} |
| $A_6^4$ | $2^{23} \cdot 3^9 \cdot 5^4$ | 12 | \{6\} |

can reduce the number of groups to be considered by observing that if $H \leq G$, then every $G$-transitive graph is $H$-transitive, and so only the minimal transitive groups need be considered.

It proves convenient to separate out the regular minimal transitive groups (those of order 48) from the remainder, as vertex-transitive graphs with a regular subgroup of automorphisms are Cayley graphs. There are a number of interesting questions and conjectures where the distinction between Cayley graphs and non-Cayley graphs appears to be subtle but significant, so keeping them separate is relevant for applications.

4.1. Cayley graphs. Given a group $G$, and a set of group elements $C \subseteq G$ such that $1_G \notin C$ and $C^{-1} = C$, the Cayley graph Cay($G, C$) with connection set $C$ is defined as follows:

$$V(\text{Cay}(G, C)) = G,$$

$$E(\text{Cay}(G, C)) = \{(g, cg) \mid g \in G, c \in C\}.$$ 

The group $G$ acts regularly on Cay($G, C$) and conversely, every graph with a regular group of automorphisms is a Cayley graph for that group.

If we define $\Omega = \{(g, g^{-1}) \mid g \in G, g \neq 1_G\}$ then each subset of $\Omega$ determines the connection sets for some Cayley graph of $G$, and conversely. Therefore, if $G$ has $a$ involutions and $b$ non-identity element-inverse pairs, then $|\Omega| = a + b$, and there are exactly $2^{a+b}$ Cayley graphs for $G$. This list of graphs will usually contain many isomorphic pairs of graphs. Some of these isomorphs arise from automorphisms of $G$, because if $\sigma \in \text{Aut}(G)$, then Cay($G, C$) is isomorphic to Cay($G, C^\sigma$). If we define a Cayley set to be an orbit of Aut($G$) acting on the set of subsets of $\Omega$, then it suffices to consider just one representative connection set from each Cayley set.

In practice, we fix an arbitrary order on $\Omega$, use GAP to compute the action of Aut($G$) on $\Omega$, and then use a straightforward backtrack algorithm using Steve Linton’s SmallestImageSet function to compute the lexicographically least representative of each Cayley set. The exact number of Cayley sets for $G$ can be determined with Redfield-Pólya counting ([28, 29]) by using Magma’s undocumented CycleIndexPolynomial function for Aut($G$) acting on $\Omega$. (The cycle index polynomial of a group can be calculated directly from its conjugacy classes, and so although the function is not documented, it is easy to verify that its output is correct.)
There are 52 transitive groups with order and degree both equal to 48, and for each of these groups, the actual number of Cayley sets constructed by the backtrack algorithm matched the theoretical number, giving us a high degree of confidence in this stage of the computation.

The list of Cayley graphs for a group $G$ constructed from the Cayley sets does not have any isomorphisms between graphs induced by the action of $\text{Aut}(G)$, but can still contain isomorphic graphs, and so each list must be filtered to remove unwanted isomorphs. Sometimes the final filtering step does not remove any graphs, because every isomorphism arises from $\text{Aut}(G)$. Groups with this property are called CI-groups and there is a substantial literature on the still-open question of characterizing CI-groups [19].

Table 3 gives the results of this computation, where the groups are numbered from 1 to 52 according to their order in the Small Groups Libraries of MAGMA and GAP [1] (the groups are in the same order in each library). The group structure is the description returned by the GAP command `StructureDescription`, the values $a$ and $b$ are the number of involutions and the number of non-identity element-inverse pairs respectively. The column labelled $|\text{Aut}|$ lists the order of the automorphism group of the group. In most cases, the value $2^{a+b}/|\text{Aut}|$ is an approximation (an underestimate) for the number of Cayley sets for that group. Where an entry in the $|\text{Aut}|$ column is marked with an asterisk (such as *192 for group number 8), this indicates a group where $\text{Aut}(G)$ does not act faithfully on $\Omega$. These groups are characterized by the existence of a group automorphism $\sigma \in \text{Aut}(G)$ such that $g^\sigma \in \{g, g^{-1}\}$ for each element $g$. It is known that such a group is either an abelian group (where the inverse map is a group automorphism) or a generalised dicyclic group (Watkins [35]). In each of the cases indicated in Table 3 the kernel of the action of $\text{Aut}(G)$ on $\Omega$ has order 2, and so these groups yield approximately $2^{a+b+1}/|\text{Aut}|$ Cayley sets. The column “Cayley Sets” gives the exact number of Cayley sets obtained from Redfield-Pólya counting, while the final column “Cayley Graphs” gives the actual number of pairwise non-isomorphic Cayley graphs. This last step is computationally non-trivial because of the sheer size of some of the lists. For example, there are more than 360 million Cayley graphs for the most prolific group ($C_2 \times D_{24}$).

The only group for which the number of Cayley graphs equals the number of Cayley sets is the abelian group $C_6 \times C_2 \times C_2 \times C_2$, so this is the only CI-group of order 48.

### Table 3. Cayley graphs on 48 vertices

| No. | Structure | $a$ | $b$ | $|\text{Aut}|$ | Cayley Sets | Cayley Graphs |
|-----|-----------|-----|-----|-------------|-------------|--------------|
| 1   | $C_3 : C_{16}$ | 1   | 23  | 48          | 496512      | 493856       |
| 2   | $C_{48}$   | 1   | 23  | 16          | 2151936     | 2122944      |
| 3   | $(C_4 \times C_4) : C_3$ | 3   | 22  | 384         | 104224      | 103726       |
| 4   | $C_8 \times S_3$ | 7   | 20  | 48          | 3752448     | 3516448      |
| 5   | $C_{24} : C_2$ | 7   | 20  | 48          | 3561216     | 337360       |
| 6   | $C_{24} : C_2$ | 13  | 17  | 96          | 13641984    | 11880240     |
| 7   | $D_{48}$   | 25  | 11  | 192         | 364086016   | 360716112    |
| 8   | $C_3 : Q_{16}$ | 1   | 23  | 192         | 275712      | 255696       |
| 9   | $C_2 \times (C_3 : C_8)$ | 3   | 22  | 96          | 647168      | 597648       |
| 10  | $(C_3 : C_8) : C_2$ | 3   | 22  | 96          | 586752      | 553168       |
| 11  | $(C_4 : C_3) : C_4$ | 3   | 22  | 192         | 454176      | 370704       |
| 12  | $(C_3 : C_4) : C_4$ | 3   | 22  | 96          | 893952      | 611760       |
graphs for each minimal transitive group $G$, its edge set is the union of elements of $\Omega$, so therefore it is also $G$-transitive if and only if its edge set is the union of elements of $\Omega$. A graph is $G$-transitive if and only if its edge set is the union of elements of $\Omega$, so therefore it is also $G'$-transitive.

4.2. **Non-Cayley graphs.** To find the non-Cayley graphs we need to construct the $G$-transitive graphs for each minimal transitive group $G$ of order more than 48. If $\Omega$ denotes the orbits of $G$ on unordered pairs of distinct points, then a graph is $G$-transitive if and only if its edge set is the union of elements of $\Omega$. Given a group $G$, its strong 2-closure $G'$ is the group consisting of all the permutations that fix (setwise) each element of $\Omega$. A graph is $G$-transitive if and only if its edge set is the union of elements of $\Omega$, so therefore it is also $G'$-transitive.
Hence it suffices to consider only the strong 2-closures of the minimal transitive groups of
degree 48. Although there are 25707 minimal transitive groups, they give rise to only 840
pairwise non-conjugate strong 2-closures. Even if \( G \) does not have a regular subgroup, it is
possible that \( G' \) does, in which case every \( G' \)-transitive graph is a Cayley graph. Similarly,
even if \( G' \) does not contain a regular subgroup, a \( G' \)-transitive graph may still be a Cayley
graph. These unwanted Cayley graphs must be filtered out, essentially by searching for (an
isomorph of) each graph in the list of Cayley graphs. Due to the sheer size of the files and
the numbers of graphs involved, this is a rather lengthy and somewhat intricate process, but
on completion we end up with 2 501 750 non-Cayley graphs, of which 2 501 630 are connected.
Hence the total number of vertex-transitive graphs on 48 vertices is 1 538 868 366, of which just
0.1625% are not Cayley graphs. By comparison, 2.682% of the vertex-transitive graphs of order
32 are non-Cayley graphs, and less than 1% for every order in the range 33–47. (For smaller
orders, the numbers of graphs are so small that even a single non-Cayley graph is a fairly high
percentage.)

4.3. Edge-transitive and half-arc-transitive graphs. A graph is called edge-transitive if
its automorphism group is transitive on edges (i.e., unordered pairs of adjacent vertices) and
arc-transitive if it is transitive on its arcs (i.e., ordered pairs of adjacent vertices). An edge-
transitive graph might also be vertex-transitive, but there are edge-transitive graphs that are
not vertex transitive, in fact some that are not even regular. Conder & Verret [4] have computed
all of the edge-transitive graphs on up to 47 vertices, separately finding those that are vertex
transitive, and those that are not.

As a result of the computations reported above, we can go one step further and find the
dge-transitive graphs of order 48 that are also vertex transitive. Thus from the 1.54 billion
vertex-transitive graphs of order 48, we extracted 189 edge-transitive graphs, of which 115 are
connected, 115 are twin-free (twins are vertices with the same neighbourhood) and just 71 are
both connected and twin-free.

We can also extract a few more interesting graphs from our lists. A graph is called half-
arc transitive (or just half-transitive) if it is vertex transitive and edge transitive, but not arc
transitive. The most famous, and smallest, such graph is the 4-regular graph on 27 vertices
known as the Doyle-Holt graph after its independent discoverers Doyle [6] (originally in an
unpublished Masters Thesis at Harvard in 1976) and Holt [11] in 1981.

The data tabulated in Conder & Verret [4] indicate that there is a single half-arc-transitive
graph on 27 vertices (degree 4), 2 on 36 vertices (of degrees 8 and 12), 2 on 39 vertices (degrees
4 and 8) and 3 on 40 vertices (all of degree 8). To these we can add another 4 half-arc-
transitive graphs on 48 vertices (all of degree 8). All four of these 8-regular half-arc-transitive
graphs are Cayley graphs for at least one group of order 48, with the groups occurring being
\((C_4 \times C_4) : C_3\) (Group 3 from the list above), \(A_4 : C_4\) (Group 30), \(C_2 \times C_2 \times A_4\) (Group 49)
and \((C_2 \times C_2 \times C_2 \times C_2) : C_3\) (Group 50).
5. Maximal generating number of transitive groups of degree 48

For an arbitrary group \( G \), let \( d(G) \) be the minimal size of a generating set of \( G \). We know of no practically efficient algorithm for computing \( d(G) \) for finite \( G \) that succeeds in reasonable time for all \( G \). But for some groups, including nilpotent groups, this is straightforward. Otherwise we can use the fact that \( d(G/N) \leq d(G) \) for all quotients \( G/N \) of \( G \) and hope to find generating sets of minimal size by random choice of group elements. (In general it is not possible to achieve this with reasonably high probability, but we can expect to find generating sets that are not much larger than \( d(G) \); see [21].)

Fortunately, we found by examining each of the groups in the list, that the transitive groups of degree 48 with \( d(G) \geq 9 \) all satisfy \( d(G) = d(G/\langle G, G \rangle) \), so we were able to identify them definitively. As we saw earlier, for most of these groups that are imprimitive with a block \( \Delta \) of size 3, the quotient group \( \bar{G} := G/O_3(G) \) of \( G \) is naturally isomorphic to a transitive group of degree 32. Indeed, if the block stabilizer \( Stab_G(\Delta) \) in such a group \( G \leq S_3 \wr S_{16} \) induces \( S_3 \) on \( \Delta \), then \( O_3(G) \) is a subgroup of the natural \( A_3^{16} \) subgroup of the base group of \( S_3 \wr S_{16} \). It follows that \( \bar{G} = G/O_3(G) \) is a subgroup of \( (S_3/A_3) \wr S_{16} \cong C_2 \wr S_{16} \leq S_{32} \) (and it is an easy exercise to check that \( \bar{G} \) is transitive as a subgroup of \( S_{32} \)). There are five such groups \( \bar{G} \) with \( d(\bar{G}) = 10 \), namely \( \text{TransitiveGroup}(32, i) \) for \( i \in \{1422821, 1422822, 1514676, 2224558, 2424619\} \), and it turned out that there are also five corresponding groups \( G \), also with \( d(G) = 10 \), namely \( \text{TransitiveGroup}(48, i) \) for \( i \in \{193577238, 193615132, 193616962, 194981057, 195193054\} \).

A lengthy computation showed that these are the only transitive groups of degree 48 with \( d(G) > 9 \).

Among the groups \( G \) with minimal block size 2, there are 11 groups with \( d(G) = 9 \), and these have signatures \( (2, H) \), where \( H = \text{TransitiveGroup}(24, i) \) with \( i \in \{9169, 21182, 23560\} \). The maximum value of \( d(G) \) among primitive groups and groups with minimal block size at least 4 is 6, which arises with block sizes 4 and 6 only.

In [33], the problem of finding numerical upper bounds for \( d(G) \) for an arbitrary transitive permutation group \( G \) of degree \( n \) is considered. It was proved in [22] that \( d(G) \) is at most \( \frac{cn}{\sqrt{\log n}} \) in this case, where \( c \) is an unspecified absolute constant. This bound is shown to be asymptotically best possible in [18] (that is, there exists constants \( c_1 \), \( c_2 \), and an infinite family \( (G_{ni})_{i=1}^\infty \) of transitive groups of degree \( ni \), with \( c_1 \leq \frac{n_i}{d(G_{ni})\sqrt{\log n_i}} \leq c_2 \) for all \( i \)).

In [33] it is proved that, apart from a finite list of possible exceptions, the bound \( d(G) \leq \left\lfloor \frac{cn}{\sqrt{\log n}} \right\rfloor \) holds, where \( c := \sqrt{\frac{3n}{2}} \) (and logarithms are to the base 2). This bound is best possible in the sense that \( d(G) = \frac{\sqrt{3n}}{2\sqrt{\log n}} = 4 \) when \( G = D_8 \circ D_8 < S_8 \) and \( n = 8 \), although it seems likely that there are better bounds that hold for sufficiently large \( n \).

The information in the first paragraph above concerning generator numbers in transitive groups of degree 48 has helped the third author to complete the proof of Theorem [1.2] thereby dispensing with the finite list of exceptions. There are, however, a number of other steps in this proof, some of which involve lengthy case-by-case analyses. For this reason, we will just outline the general strategy of the proof in this paper, and the details will be published separately (see [24]).
First, by [33, Theorem 5.3], one only needs to prove Theorem 1.2 when $G$ is imprimitive with minimal block size 2, and $n$ has the form $n = 2^x 3^y 5$ with either $y = 0$ and $17 \leq x \leq 26$; or $y = 1$ and $15 \leq x \leq 35$. Thus, in particular, $G$ may be viewed as a subgroup in a wreath product $2 \wr G^\Sigma$, where $\Sigma$ is a set of blocks for $G$ of size 2. It follows that $d(G) \leq d_{G^\Sigma}(M) + d(G^\Sigma)$, where $M$ is the intersection of $G$ with the base group of the wreath product, and $d_{G^\Sigma}(M)$ is the minimal number of elements required to generate $M$ as a $G^\Sigma$-module. With this reduction in mind, the proof of Theorem 1.2 has two main ingredients: upper bounds on $d_{G^\Sigma}(M)$, and upper bounds on $d(G^\Sigma)$. We summarise the approach to these two sub-problems from [33] in the next few paragraphs.

We note first that the bulk of the proof is taken up with finding upper bounds on $d_{G^\Sigma}(M)$. Since $d_{G^\Sigma}(M) \leq d_H(M)$ for every subgroup $H$ of $G^\Sigma$, the strategy in [33] in this case involved replacing $G^\Sigma$ by a convenient subgroup $H$ of $G^\Sigma$, and then deriving upper bounds on $d_H(M)$, usually in terms of the lengths of the $H$-orbits in $\Sigma$. This approach turns out to be particularly fruitful when $H$ is chosen to be a soluble transitive subgroup of $G^\Sigma$, whenever such a subgroup exists. When $G^\Sigma$ does not contain a soluble transitive subgroup, however, the analysis becomes much more complicated. This led to less sharp bounds, and ultimately, the omitted cases in [33, Theorem 1.1].

The new approach to bounding $d_{G^\Sigma}(M)$ involves a careful analysis of the orbit lengths of soluble subgroups in a minimal transitive insoluble subgroup of $G^\Sigma$, building on the work in [33] in the case $n = 2^x 3$. This analysis, together with upper bounds on $d_H(M)$ (for soluble $H \leq G^\Sigma$) in terms of the lengths of the $H$-orbits in $\Sigma$, is then used to derive an upper bound for $d_H(M)$. An upper bound for $d_{G^\Sigma}(M)$ follows.

The second sub-problem is to find an upper bound for $d(G^\Sigma)$. The group $G^\Sigma$ is a transitive permutation group of degree $n/2 = 2^{x-1} 3^y 5$, where $n$, $x$, and $y$ are as above. The upper bound $d(G^\Sigma) \leq \frac{n^2}{\sqrt{\log n}}$ can be derived by using induction on $n$. However, combining this with the upper bounds on $d(G^\Sigma)$ detailed in the previous two paragraphs is not enough to prove Theorem 1.2 in all of the required cases. Therefore, a more careful approach is required. This approach was used in the proof of [33, Lemma 5.12]. Informally, the idea is as follows. There exists a factorisation $\frac{n}{2} = r_1 \ldots r_t$ of $\frac{n}{2}$ such that either

1. $d(G^\Sigma) \leq \sum_{i=1}^{t-1} d(r_i, r_{i+1} \ldots r_t) + \log r_t$; or
2. Either $r_t \leq 32$, or $r_t = 48$, and $d(G^\Sigma) \leq \sum_{i=1}^{t-1} d(r_i, r_{i+1} \ldots r_t) + d_{\text{trans}}(r_t)$.

Here, $d_{\text{trans}}(m) := \max\{d(X) : X \text{ transitive of degree } m\}$. If $2 \leq m \leq 32$, or if $m = 48$, then we know $d_{\text{trans}}(m)$ precisely, by [3], and this paper, respectively.

The function $d(r, s)$ is defined as the maximum of $d_X(K_X(\Delta))$, where

1. $X$ runs over the transitive permutation groups of degree $rs$ with minimal block size $r$;
2. $\Delta$ runs over the blocks for $X$ of size $r$;
3. $K_X(\Delta)$ is the kernel of the action of $X$ on $\Delta$; and
4. $d_X(K_X(\Delta))$ is the minimal number of elements required to generate $K_X(\Delta)$ as a normal subgroup of $X$. 


Upper bounds on $d(r,s)$ are available from [33]. Thus, we can find upper bounds on $d(G^Σ)$ by going through all factorisations of $\frac{n^2}{2}$, and taking the maximum of the bounds coming from (1) and (2) above. These maximums almost always come from (2). Thus, the new result $d_{\text{trans}}(48) = 10$ from this paper plays a vital role in deriving upper bounds on $d(G^Σ)$, whence solving the second sub-problem in the proof of Theorem 1.2.

Acknowledgements. We would like to thank Michael Giudici for a number of helpful discussions on transitive permutation groups.

References

[1] Hans Ulrich Besche, Bettine Eick, and E. A. O’Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.* 12(5):623–644, 2002.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] John J. Cannon and Derek F. Holt. The transitive permutation groups of degree 32. *Experiment. Math.*, 17(3):307–314, 2008.

[4] Marston D. E. Conder and Gabriel Verret. Edge-transitive graphs of small order and the answer to a 1967 question by Folkman. *Algebraic Combinatorics*, 2(6):1275–1284, 2019.

[5] Hannah J. Coutts, Martyn Quick, and Colva M. Roney-Dougal. The primitive permutation groups of degree less than 4096. *Comm. Algebra*, 39(10):3526–3546, 2011.

[6] Peter G. Doyle. A 27-vertex graph that is vertex-transitive and edge-transitive but not 1-transitive. https://arxiv.org/abs/math/0703861.

[7] Paul Erdős. On a Theorem of Sylvester and Schur. *J. London Math. Soc.* 9(4):282–288, 1934.

[8] The GAP Group. GAP – Groups, Algorithms, and Programming, Version 4.11.1; 2021. https://www.gap-system.org.

[9] Michael Giudici. New constructions of groups without semiregular subgroups. *Comm. Algebra*, 35(9):2719–2730, 2007.

[10] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[11] Derek F. Holt. A graph which is edge transitive but not arc transitive. *Journal of Graph Theory*, 5(2):201–204, 1981.

[12] Derek Holt and Gordon Royle, A census of small transitive groups and vertex-transitive graphs. *J. Symbolic Comput.*, 101:51–60, 2020.

[13] Alexander Hulpke. Constructing transitive permutation groups. *J. Symbolic Comput.*, 39(1):1–30, 2005.

[14] Peter B. Kleidman. The maximal subgroups of the Steinberg triality groups $^3D_4(q)$ and of their automorphism groups. *J. Algebra*, 115(1):182–199, 1988.

[15] Peter B. Kleidman. The maximal subgroups of the Chevalley groups $G_2(q)$ with $q$ odd, the Ree groups $^2G_2(q)$, and their automorphism groups. *J. Algebra*, 117(1):30–71, 1988.

[16] Peter Kleidman and Martin Liebeck. The subgroup structure of the finite classical groups. London Math. Soc. Lecture Note Ser. 129, Cambridge University Press, 1990.

[17] Mikhail Klin and Dragan Marušič. Problem BCC15.12, Research Problems from the Fifteenth British Combinatorial Conference. *Discrete Math.*, 167–168:605–615, 1997.

[18] L. G. Kovács and M. F. Newman. Generating transitive permutation groups. *Quart. J. Math. Oxford Ser. (2)* 39(155):361–372, 1988.

[19] Li, Cai Heng and Lu, Zai Ping and Pálfy, P. P. *J. Algebraic Combin.*, 26(2):161–181, 2007.

[20] Steve Linton. Finding the smallest image of a set. ISSAC 2004, 229–234, ACM, New York, 2004.

[21] Alexander Lubotzky. The expected number of random elements to generate a finite group. *J. Algebra* 257:452–459, 2002.
[22] A. Lucchini, F. Menegazzo and M. Morigi. Asymptotic results for transitive permutation groups. *Bull. London Math. Soc.* 32(2):191–195, 2000.

[23] A. Lucchini, F. Menegazzo, and M. Morigi. Asymptotic results for primitive permutation groups and irreducible linear groups. *J. Algebra* 223(1):154–170, 2000.

[24] Gunter Malle. The maximal subgroups of $^2F_4(q^2)$. *J. Algebra* 139(1):52–69, 1991.

[25] Dragan Marušič. On vertex-symmetric digraphs. *Discrete Math* 36(1):69–81, 1981.

[26] G. A. Miller. List of transitive substitution groups of degree twelve. *Quart. Jour. Math.*, 28:193–231, 1896.

[27] G. A. Miller. The collected works of George Abram Miller, 5 volumes. University of Illinois, 1935–1959.

[28] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta Math.*, 68(1):145–254, 1937.

[29] Howard J. Redfield. The Theory of Group-Reduced Distributions. *Amer. J. Math.*, 49(3):433–455, 1927.

[30] Gordon F. Royle. The transitive groups of degree twelve. *J. Symbolic Comput.*, 4(2):255–268, 1987.

[31] Gordon F. Royle. An orderly algorithm and some applications in finite geometry. *Discrete Math.*, 185(1-3):105–115, 1998.

[32] Michio Suzuki. On a class of doubly transitive groups. *Ann. of Math.* 75(2):105–145, 1962.

[33] Gareth M. Tracey. Minimal generation of transitive permutation groups. *J. Algebra* 509:40–100, 2018.

[34] Gareth M. Tracey. Upper bounds on the minimal number of elements required to generate a transitive permutation group. Submitted to *J. Algebra*.

[35] Mark E. Watkins, On the Action of Non-Abelian Groups on Graphs. *J. Comb. Theory Ser. B* 11:95–104, 1971.

[36] Robert Wilson et al. Atlas of Finite Group Representations, [http://brauer.maths.qmul.ac.uk/Atlas/v3/](http://brauer.maths.qmul.ac.uk/Atlas/v3/)

**Mathematics Institute, University of Warwick**

*Email address:* D.F.Holt@warwick.ac.uk

**Mathematics and Statistics, University of Western Australia**

*Email address:* gordon.royle@uwa.edu.au

**Mathematical Institute, University of Oxford**

*Email address:* garethtracey1@gmail.com