

Most switching classes with primitive automorphism groups contain graphs with trivial groups

PETER J. CAMERON

*School of Mathematics and Statistics
University of St Andrews
St Andrews, Fife KY16 9SS
Scotland*

PABLO SPIGA

*Dipartimento di Matematica e Applicazioni
University of Milano-Bicocca
Milano, 20125 Via Cozzi 55
Italy*

To the memory of Ákos Seress

Abstract

The operation of *switching* a graph Γ with respect to a subset X of the vertex set interchanges edges and non-edges between X and its complement, leaving the rest of the graph unchanged. This is an equivalence relation on the set of graphs on a given vertex set, so we can talk about the automorphism group of a *switching class* of graphs.

It might be thought that switching classes with many automorphisms would have the property that all their graphs also have many automorphisms. However the main theorem of this paper shows a different picture: with finitely many exceptions, if a non-trivial switching class \mathcal{S} has primitive automorphism group, then it contains a graph whose automorphism group is trivial. We also find all the exceptional switching classes; up to complementation, there are just six.

1 Introduction

The purpose of this paper is to prove the following theorem:

Theorem 1.1 *Let \mathcal{S} be a switching class of graphs on n vertices, whose automorphism group is primitive but not the symmetric group. Then, with just six exceptions (up to complementation), there is a graph $\Gamma \in \mathcal{S}$ with trivial automorphism group.*

The six exceptions are as follows (we give the degree and automorphism group of the switching class in each case): $(5, D_{10})$, $(6, \text{PSL}(2, 5))$, $(9, S_3 \text{ wr } S_2)$, $(10, \text{P}\Sigma\text{L}(2, 9) \cong S_6)$, $(14, \text{PSL}(2, 13))$, and $(16, 2^4.S_6 \cong 2^4.\text{Sp}(4, 2))$.

The next two sections explain the context and give definitions. Then we prove that the list of exceptions is finite, and lastly we find all the exceptions.

Note that the assumption of primitivity is necessary: the switching class containing the complete multipartite graph $K_{r,r,\dots,r}$ with $r \geq 3$ contains no graph with trivial automorphism group. (The switching set X or its complement meets a set of the multipartition in at least two points, and the permutation transposing two such points is an automorphism.)

2 Primitive permutation groups

One of the most useful consequences of the Classification of the Finite Simple Groups (CFSG) is that primitive permutation groups (other than the symmetric and alternating groups) are “small”. In fact, elementary combinatorial arguments due to Babai [1] for uniprimitive groups and Pyber [14] for multiply transitive groups, provide bounds which are good enough for many purposes; but the results can be strengthened by using CFSG. The best result, which we use later, is due to Maróti [12]. (Babai’s bound asserts that if G is primitive but not 2-transitive of degree n , then $|G| \leq n^{4\sqrt{n}\log_2(n)}$. This is best possible apart from the logarithm in the exponent, but Maróti’s result gives a bound of $n^{1+\log_2(n)}$ with known exceptions.) We state Maróti’s theorem later.

A *permutation group* is a subgroup of the symmetric group S_n of degree n , acting on a domain Ω of size n . It is *transitive* if it leaves no subset of Ω invariant except for \emptyset and Ω , and *primitive* if, in addition, it leaves no partition of Ω invariant apart from the partition into singletons and the partition into a single part.

The line of research reported here began with a theorem of Cameron, Neumann and Saxl [6]:

Theorem 2.1 *If G is a primitive group on Ω , other than S_n and A_n and finitely many exceptions, then there is a subset of Ω whose setwise stabiliser in G is the identity.*

This result has been quantified in various ways:

- (a) Seress [16] found all the exceptions: there are 43 of them, the largest degree being 32. (We give a slight strengthening of this result in Section 4.)
- (b) Cameron [5] showed that the proportion of subsets whose stabiliser is the identity tends to 1 as $n \rightarrow \infty$ (in primitive groups of degree n other than S_n and A_n).

- (c) Babai and Cameron [2] showed that we can take the size of the subset to be at most $n^{1/2+o(1)}$.

In his paper, Seress gives the numbers of the primitive groups in the GAP computer algebra system. However, the numbers have changed. For the reader's convenience, we repeat the list, with the numbers in the current version 4.7.4 of GAP. Each entry has the form (n, m, G) , where G is `PrimitiveGroup`(n, m) in GAP.

(5, 2, D_{10}), (5, 3, $\text{AGL}(1, 5)$), (6, 1, $\text{PSL}(2, 5)$), (6, 2, $\text{PGL}(2, 5)$), (7, 4, $\text{AGL}(1, 7)$),
 (7, 5, $\text{PSL}(3, 2)$), (8, 2, $\text{AGL}(1, 8)$), (8, 4, $\text{PSL}(2, 7)$), (8, 5, $\text{PGL}(2, 7)$),
 (8, 3, $\text{AGL}(3, 2)$), (9, 2, $3^2 \cdot D_8 = S_3 \text{ wr } S_2$), (9, 5, $\text{AGL}(1, 9)$), (9, 6, $\text{ASL}(2, 3)$),
 (9, 7, $\text{AGL}(2, 3)$), (9, 8, $\text{PSL}(2, 8)$), (9, 9, $\text{PGL}(2, 8)$), (10, 2, S_5), (10, 3, $\text{PSL}(2, 9)$),
 (10, 5, $\text{P}\Omega\text{L}(2, 9)$), (10, 4, $\text{PGL}(2, 9)$), (10, 6, M_{10}), (10, 7, $\text{P}\Gamma\text{L}(2, 9)$),
 (11, 1, $\text{PSL}(2, 11)$), (11, 2, M_{11}), (12, 4, $\text{PGL}(2, 11)$), (12, 1, M_{11}), (12, 2, M_{12}),
 (13, 7, $\text{PSL}(3, 3)$), (14, 2, $\text{PGL}(2, 13)$), (15, 4, $\text{PSL}(4, 2)$), (16, 12, $\text{AGL}(2, 4)$),
 (16, 17, $2^4 \cdot A_6$), (16, 16, $2^4 \cdot S_6$), (16, 20, $2^4 \cdot A_7$), (16, 11, $\text{AGL}(4, 2)$),
 (17, 7, $\text{PSL}(2, 16) \cdot 2$), (17, 8, $\text{P}\Gamma\text{L}(2, 16)$), (21, 7, $\text{P}\Gamma\text{L}(3, 4)$), (22, 1, M_{22}),
 (22, 2, $M_{22} \cdot 2$), (23, 5, M_{23}), (24, 1, M_{24}), (32, 3, $\text{AGL}(5, 2)$).

3 Switching

This section gives a very brief introduction to graph switching and some of its many applications. See Seidel [15] or Taylor [20] for more details, including connections with equiangular lines, group cohomology, graph spectra, and finite simple groups.

Switching of graphs was introduced by Seidel in connection with equiangular lines in Euclidean space, and later used in his classification of strongly regular graphs with least eigenvalue -2 . At about the same time, Higman introduced an equivalent concept, that of a “two-graph” (which we describe below), to give a direct construction of the Conway group Co_3 .

Let Γ be a graph on the vertex set Ω . For a subset X of Ω , the operation σ_X with respect to X replaces edges between X and $\Omega \setminus X$ by non-edges and non-edges by edges, leaving edges and non-edges within or outside X unchanged. Since $\sigma_X \sigma_Y = \sigma_{X \Delta Y}$, switching is an equivalence relation on the set of all graphs on the vertex set Ω . Since $\sigma_X = \sigma_{\Omega \setminus X}$, there are 2^{n-1} graphs in a switching class, where $n = |\Omega|$.

Example A regular icosahedron has six diagonals, any two making the same angle. Choose one of the two vertices on each diagonal. The corresponding induced subgraph of the skeleton of the icosahedron has one of four possible forms: a pentagon with an isolated vertex; a pentagon with a vertex joined to all others; a triangle with pendant edges at each vertex; and the complement of the preceding. These graphs form a switching class; the numbers of graphs of each type are 6, 6, 10, 10 respectively. (For switching with respect to a subset X of the six diagonals corresponds to changing the choice of vertex on the diagonals in X .) Any switching class can be represented by a set of equiangular lines in this way; see Seidel [15] for a description of this.

Given a graph Γ with vertex set Ω , the 3-uniform hypergraph on Ω whose hyperedges are the 3-subsets of Ω containing an odd number of edges of Γ is unaffected by switching; indeed, two graphs belong to the same switching class if and only if they give the same 3-uniform hypergraph in this way. The hypergraphs which arise are characterised by the property that any 4-subset of Ω contains an even number of hyperedges. Graham Higman, who introduced this notion, called such an object a *two-graph*. He gave a combinatorial construction and uniqueness proof for a two-graph on 276 points whose automorphism group is Conway’s third group Co_3 . (The corresponding set of 276 equiangular lines occurs in the Leech lattice.)

The *automorphism group* of a switching class consists of all permutations of the vertex set which map the graphs of the class among themselves. It suffices to assume that a single graph in the switching class is mapped to a graph in the class. The automorphism group of a switching class coincides with the automorphism group of the associated two-graph (as 3-uniform hypergraph). The automorphism group of a switching class contains the automorphism groups of all the graphs in the class as subgroups. Indeed, there is a Frucht-style *representation theorem* for a group and its subgroups [4]:

Proposition 3.1 *Given any finite group G , there is a switching class \mathcal{S} with the properties:*

- (a) $\text{Aut}(\mathcal{S}) \cong G$;
- (b) *identifying these two groups, for any subgroup $H \leq G$, there is a graph $\Gamma \in \mathcal{S}$ with $\text{Aut}(\Gamma) = H$.*

Switching classes can be divided into two types, which we will call Type I and Type II; the types are distinguished by the vanishing or non-vanishing of a certain cohomology class (see Cameron [3]).

Type I: A Type I switching class \mathcal{S} contains a graph Γ such that $\text{Aut}(\Gamma) = \text{Aut}(\mathcal{S})$. For any subset X of the vertex set V of Γ , $\text{Aut}(\sigma_X(\Gamma))$ is the stabiliser of the partition $\{X, V \setminus X\}$ in $\text{Aut}(\Gamma)$. Every switching class on an odd number of vertices is of Type I: for such a switching class contains a unique graph Γ in which all vertices have even valency, and the partition $\{X, V \setminus X\}$ is the partition of V into vertices of even and odd valency in $\sigma_X(\Gamma)$. The switching classes of the 5-cycle and the 3×3 grid (the line graph of $K_{3,3}$) are of this type, and provide two of the examples in Theorem 1.1; their automorphism groups are D_{10} and $S_3 \text{ wr } S_2$ respectively.

Type II: The automorphism group of a Type II switching class \mathcal{S} properly contains the automorphism group of any graph in \mathcal{S} . It can happen that the automorphism group of a switching class is 2-transitive; such a class, if not trivial (i.e. the switching class of the complete or null graph), is necessarily of Type II. Note, however, that no non-trivial switching class can have a 3-transitive automorphism group, since $\text{Aut}(\mathcal{S})$ is equal to the automorphism group of the corresponding two-graph.

We now briefly describe the other four examples occurring in our theorem. (The examples on 5 and 9 points are of Type I and are described above.)

- Let q be a prime power congruent to 1 (mod 4). The group $\text{P}\Sigma\text{L}(2, q)$, acting on $q + 1$ points, has two orbits on 3-subsets; each orbit forms a two-graph, which is self-complementary (that is, the two-graphs are isomorphic). The examples with 6, 10 and 14 points are of this type. The example on 6 points corresponds to the six diagonals of the icosahedron, as described earlier. The example on 10 points corresponds to the switching class containing the Petersen graph (or its complement, the line graph of K_5).
- The example on 16 points is a *symplectic* two-graph. The points are the vectors of a 4-dimensional vector space over \mathbb{F}_2 , carrying a symplectic form (a non-degenerate alternating bilinear form) B . The triples of the two-graph are those $\{x, y, z\}$ for which

$$B(x, y) + B(y, z) + B(z, x) = 0.$$

It can also be described as the switching class of the Clebsch graph. Its automorphism group is the semidirect product of the translation group of V by the symplectic group $\text{Sp}(4, 2) \cong S_6$.

4 Bounding the exceptions

We begin the proof of Theorem 1.1. In this section we show that exceptions have degree at most 32.

Let Ω be a finite set and let g be a permutation on Ω . We denote by $\text{Fix}_\Omega(g)$ the set $\{\omega \in \Omega \mid \omega^g = \omega\}$, by $\text{fix}_\Omega(g)$ the cardinality $|\text{Fix}_\Omega(g)|$ and by $\text{orb}_\Omega(g)$ the number of cycles of g (in its decomposition in disjoint cycles).

Given a subset X of Ω , we denote by G_X the set-wise stabiliser $\{g \in G \mid X^g = X\}$. We denote by 2^Ω the power-set of Ω , that is, the set of subsets of Ω . Moreover, we define

$$\mathcal{F}(G) = \{X \in 2^\Omega \mid X^g = X \text{ for some } g \in G \setminus \{1\}\}.$$

Lemma 4.1 *Let g be a permutation of Ω and let p the smallest prime dividing the order of g . Then*

$$\text{orb}_\Omega(g) \leq \frac{|\Omega|}{p} + \frac{p-1}{p} \text{fix}_\Omega(g)$$

and

$$2^{\text{orb}_\Omega(g)} = |\{X \in 2^\Omega \mid X^g = X\}|.$$

In particular,

$$|\{X \in 2^\Omega \mid X^g = X\}| \leq 2^{\frac{|\Omega|}{p} + \frac{p-1}{p} \text{fix}_\Omega(g)}$$

and

$$|\mathcal{F}(G)| \leq \sum_{g \in G \setminus \{1\}} 2^{\text{orb}_\Omega(g)} \leq \sum_{g \in G \setminus \{1\}} 2^{\frac{|\Omega|}{p} + \frac{p-1}{p} \text{fix}_\Omega(g)}.$$

Proof The element g has cycles of size 1 on $\text{Fix}_\Omega(g)$ and of size at least p on $\Omega \setminus \text{Fix}_\Omega(g)$. Thus

$$\text{orb}_\Omega(g) \leq |\text{Fix}_\Omega(g)| + \frac{|\Omega \setminus \text{Fix}_\Omega(g)|}{p} = \frac{|\Omega|}{p} + \frac{p-1}{p} \text{fix}_\Omega(g).$$

The rest of the lemma is obvious. □

We require a slight strengthening of the result of Seress [16] on primitive groups with no regular orbit on the power set.

Proposition 4.2 *Let G be a finite primitive group on Ω with $\text{Alt}(\Omega) \not\leq G$. Then either there exists a subset X of Ω with $|X| < n/2$ and $G_X = 1$, or G is one of the groups listed in [16, Theorem 2], or $|\Omega| = 16$ and $G = 2^4.\text{SO}_4^-(2)$.*

Proof Let n be the cardinality of Ω . Observe that if there exists $X \in 2^\Omega$ with $G_X = 1$, then replacing X by $\Omega \setminus X$ if necessary we have $|X| \leq n/2$ and we still have $G_X = 1$.

If n is odd, then the proof follows from [16, Theorem 2]. Suppose then that n is even. Let M be a subgroup of $\text{Sym}(\Omega)$ maximal (with respect to set-inclusion) such that $G \leq M$ and $M \notin \{\text{Alt}(\Omega), \text{Sym}(\Omega)\}$. Observe that if $M_X = 1$ for some $X \in 2^\Omega$, then also $G_X = 1$. Replacing G by M if necessary, we assume that $G = M$. Now, the structure of M is well understood (see for example [10]):

- (a) $n = m^r$ for some positive integers m and r with $m \geq 5$ and $r \geq 2$, and G is permutation isomorphic to S_m wr S_r with its natural product action;
- (b) G is the stabiliser of a diagonal structure, that is, G is a group of “diagonal type”;
- (c) G is the stabiliser of an affine structure, that is, $n = 2^d$ for some positive integer d , and G is permutation isomorphic to $\text{AGL}_d(2)$ endowed of its natural “affine” action;
- (d) G is almost simple.

We deal with each of these cases in turn.

Suppose that Case (a) holds. Then from the proof of [16, Lemma 4] we see that there exists $X \in 2^\Omega$ with $G_X = 1$ and with $|X| = 4m - 5$ when $r = 2$, and $|X| = \sum_{i=0}^{r-1} (m-2)^i m^{r-1-i} + 3m - 5$ when $r \geq 3$. An easy calculation gives $|X| < n/2$ unless $(m, r) = (6, 2)$. When $m = 6$, we have $|X| = 19$, $|\Omega \setminus X| = 11 < n/2$ and $G_{\Omega \setminus X} = 1$.

Suppose that Case (c) holds. Then $G \cong \text{AGL}(d, 2)$ for some positive integer d . Now, a non-identity element of G fixes at most $n/2$ points and hence fixes at most $2^{3n/4}$ elements of 2^Ω by Lemma 4.1. Therefore $|\mathcal{F}(G)| \leq 2^{3n/4}|G|$. Now a computation gives $2^{3n/4}|G| < 2^n - \binom{n}{n/2}$ when $d \geq 9$. In particular, for $d \geq 9$, there exists $X \in 2^\Omega$ with $|X| < n/2$ and $G_X = 1$. When $d \leq 8$, the proof follows by computation.

Suppose that Case (d) holds. Assume that $G = S_m$ in its action on the r -subsets of $\{1, \dots, m\}$, with $2 \leq r < m/2$. Then Seress [16, Lemma 9] shows that there exists $X \in 2^\Omega$ such that $G_X = 1$ and with $|X| = m - r + 1$ when $r \in \{2, 3\}$ and $|X| \leq 2(m - r + 1)$ when $r \geq 4$. In both cases $|X| < \frac{1}{2} \binom{m}{r} = n/2$.

When $G = M_n$ (where M_n is the Mathieu group of degree n) the proof follows from a computation.

Suppose that Case (b) holds, or that Case (d) holds and G is neither S_m in its action on the r -subsets of $\{1, \dots, m\}$ nor the Mathieu group of degree n . Now from [9, Corollary 1] we have $\text{fix}_\Omega(g) \leq 4n/7$ for every $g \in G \setminus \{1\}$, and from [12] we have $|G| \leq n^{1+\log_2(n)}$. Thus Lemma 4.1 gives $|\mathcal{F}(G)| \leq 2^{11n/14} n^{1+\log_2(n)}$. Now a computation gives that $2^{11n/14} n^{1+\log_2(n)} < 2^n - \binom{n}{n/2}$ when $n \geq 386$. In particular, for $n \geq 386$, there exists $X \in 2^\Omega$ with $X \notin \mathcal{F}(G)$ and $|X| \neq n/2$, and the proof follows immediately.

Finally the primitive groups of diagonal type and almost simple of degree less than 386 can be easily checked with a computer. □

Observe that $\text{SO}_4^-(2) \cong S_5$. There are two non-isomorphic primitive groups of degree 16 and with point stabiliser isomorphic to S_5 : one 2-transitive and the other (namely $2^4.\text{SO}_4^-(2)$ in the statement of Proposition 4.2) having rank 3. The latter is `PrimitiveGroup(16,18)` in the current GAP list.

We now begin the proof of the main theorem. We will show that an exception has degree at most 32.

In the following proof, with a slight abuse of terminology, we say that M is a *maximal subgroup* of $\text{Sym}(\Omega)$ if $M \leq \text{Sym}(\Omega)$, $\text{Alt}(\Omega) \not\leq M$ and either $\text{Alt}(\Omega)$ or $\text{Sym}(\Omega)$ is the only subgroup of $\text{Sym}(\Omega)$ containing M .

Proof of Theorem 1.1: the degree is at most 32. Let \mathcal{S} be a switching class of graphs on n vertices, whose automorphism group G is primitive but not the symmetric group. Let Ω be the domain of G , let \mathbb{F}_2 be the finite field of cardinality 2 and let V be the permutation $\mathbb{F}_2 G$ -module for the action of G on Ω . Thus V has basis $(e_\omega \mid \omega \in \Omega)$ indexed by the elements of Ω . Let $e = \sum_{\omega \in \Omega} e_\omega$ and let W be the quotient G -module $V/\langle e \rangle$.

The proof is divided into the two parts we called Type I and Type II earlier; recall that a switching class has Type I if its automorphism group is equal to the automorphism group of some graph in the class.

Type I: Thus $G = \text{Aut}(\mathcal{S}) = \text{Aut}(\Gamma_0)$, for some $\Gamma_0 \in \mathcal{S}$.

If there exists $X \in 2^\Omega$ with $|X| < n/2$ and $G_X = 1$, then the proof follows immediately: the graph $\sigma_X(\Gamma_0)$ lies in \mathcal{S} and has trivial automorphism group. In particular, in view of Proposition 4.2 we may assume that G is one of the groups listed in [16, Theorem 2], or $|\Omega| = 16$ and $G = 2^4.\text{SO}_4^-(2)$.

A quick inspection reveals that the groups in [16, Theorem 2] have degree at most 32.

Type II: Assume that no graph in \mathcal{S} has trivial automorphism group. Thus G has no regular orbit on \mathcal{S} and hence

$$\#G\text{-orbits on } \mathcal{S} \geq 2 \cdot \frac{|\mathcal{S}|}{|G|} = \frac{2^n}{|G|}. \tag{1}$$

A result of Mallows and Sloane [11] asserts that any permutation g which fixes a switching class \mathcal{S} fixes a graph $\Gamma \in \mathcal{S}$. Moreover, another graph, $\Gamma' \in \mathcal{S}$ is fixed by g if and only if the partition $\{X, \Omega \setminus X\}$ which switches Γ to Γ' is fixed by g . It follows that the number of graphs in \mathcal{S} fixed by g is equal to the number of vectors of W fixed by g ; that is,

$$\text{fix}_{\mathcal{S}}(g) = \text{fix}_W(g) \quad \text{for every } g \in G.$$

It follows that the permutation characters of $G = \text{Aut}(\mathcal{S})$ on the switching class \mathcal{S} and on the “switching module” W are equal. Therefore

$$\#G\text{-orbits on } \mathcal{S} = \#G\text{-orbits on } W. \tag{2}$$

The definition of W gives

$$\begin{aligned} \#G\text{-orbits on } W &= \frac{1}{2} \left(\#G\text{-orbits on } 2^\Omega \right. \\ &\quad \left. + \# \text{self-complementary } G\text{-orbits on } 2^\Omega \right), \end{aligned} \tag{3}$$

where a G -orbit is self-complementary if it contains the complement of each of its elements. From the Orbit-Stabiliser lemma and Lemma 4.1, the first summand in Equation (3) is $\sum_{g \in G} 2^{\text{orb}_\Omega(g)} / |G|$.

A subset X of Ω lies in a self-complementary orbit if and only if there is a fixed-point-free element $g \in G$ of 2-power order with $\Omega = X \cup X^g$ and $X \cap X^g = \emptyset$. The number of such sets X arising from a given element g is $2^{\text{orb}_\Omega(g)}$. Denote by G_2 the set

$$\{g \in G \mid |g| = 2^\ell \text{ for some } \ell > 1 \text{ and } \text{fix}_\Omega(g) = 0\}.$$

Thus, the second summand in Equation (3) is at most $\sum_{g \in G_2} 2^{\text{orb}_\Omega(g)}$.

Now from Equations (1), (2) and (3) we obtain

$$\frac{2^n}{|G|} \leq \frac{1}{2} \left(\frac{1}{|G|} \sum_{g \in G} 2^{\text{orb}_\Omega(g)} + \sum_{g \in G_2} 2^{\text{orb}_\Omega(g)} \right). \tag{4}$$

Before dealing with the general case we deal separately with a few special situations. The case division here is dictated by the theorem of Maróti [12] on the orders of primitive groups. For convenience we state Maróti’s result here.

Theorem 4.3 *Let G be a primitive permutation group of degree n . Then one of the following holds:*

- (a) G is a subgroup of S_m wr S_r containing $(A_m)^r$, where the action of S_m is on k -subsets of $\{1, \dots, m\}$ and the wreath product has the product action of degree $n = \binom{m}{k}^r$;
- (b) $G = M_{11}, M_{12}, M_{23}$ or M_{24} with their 4-transitive action;
- (c) $|G| \leq n \cdot \prod_{i=0}^{\lceil \log_2(n) \rceil - 1} (n - 2^i) < n^{1 + \lceil \log_2(n) \rceil}$.

Case (a)(i): the socle of G is A_m in its action on the k -subsets of $\{1, \dots, m\}$ with $2 \leq k < m/2$ and $m \geq 5$.

Suppose first that $k = 2$. Hence $n = \binom{m}{2}$ and we may identify Ω with the set of 2-subsets of $\{1, \dots, m\}$. Let τ be the two-graph induced by the switching class \mathcal{S} . Suppose that $m \geq 9$. Now, G has rank 3 in its action on Ω and G has five orbits on the set of 3-subsets of Ω : namely

$$\begin{aligned} \mathcal{O}_1 &= \{\{a, b\}, \{a, c\}, \{a, d\} \mid a, b, c, d \text{ distinct elements of } \{1, \dots, m\}\}, \\ \mathcal{O}_2 &= \{\{a, b\}, \{b, c\}, \{a, c\} \mid a, b, c \text{ distinct elements of } \{1, \dots, m\}\}, \\ \mathcal{O}_3 &= \{\{a, b\}, \{b, c\}, \{c, d\} \mid a, b, c, d \text{ distinct elements of } \{1, \dots, m\}\}, \\ \mathcal{O}_4 &= \{\{a, b\}, \{a, c\}, \{d, e\} \mid a, b, c, d, e \text{ distinct elements of } \{1, \dots, m\}\}, \\ \mathcal{O}_5 &= \{\{a, b\}, \{c, d\}, \{e, f\} \mid a, b, c, d, e, f \text{ distinct elements of } \{1, \dots, m\}\}. \end{aligned}$$

(These orbits correspond to the non-isomorphic graphs with three edges.) Replacing τ by its complement $\tau' = \{x \subseteq \Omega \mid |x| = 3, x \notin \tau\}$, we may assume that $\mathcal{O}_1 \subseteq \tau$. Now consider the 4-subset $x = \{\{a, b\}, \{a, c\}, \{a, d\}, \{e, f\}\}$ of Ω . Clearly, x has one 3-subset in common with \mathcal{O}_1 , zero with $\mathcal{O}_2, \mathcal{O}_3$ and \mathcal{O}_5 , and three with \mathcal{O}_4 . As τ is a two-graph, x has an even number of 3-subsets in common with τ and hence $\mathcal{O}_4 \subseteq \tau$. An entirely similar argument using $x = \{\{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}\}$ yields $\mathcal{O}_2 \subseteq \tau$. Now an easy inspection gives that $\mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_4$ is a two-graph and (using that τ is a proper two-graph) we have $\tau = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{O}_4$.

Recall that the Kneser graph Γ is the graph with vertex set Ω and where two vertices α and β are declared to be adjacent if they are disjoint, that is, $\alpha \cap \beta = \emptyset$. It is readily seen that the two-graph afforded by Γ is τ and hence $\Gamma \in \mathcal{S}$. Thus $\text{Aut}(\Gamma) \leq \text{Aut}(\tau) = G$ and hence $\text{Aut}(\Gamma) < G$ because we are dealing with Type II. It is well-known (see for example [10, Theorem and Table II–VI]) that, for $m \geq 9$, $\text{Aut}(\Gamma) \cong S_m$ and $\text{Aut}(\Gamma)$ is a maximal subgroup of $\text{Sym}(\Omega)$. Thus $\text{Aut}(\Gamma) = \text{Aut}(\mathcal{S})$, contradicting the assumption of Type II.

When $m \leq 8$ and $k = 2$, we have $n \in \{10, 15, 21, 28\}$ and hence $n \leq 32$.

Suppose now that $k \geq 3$. A careful analysis of the elements of G yields $\text{fix}_\Omega(g) \leq \binom{m-2}{k} + \binom{m-2}{k-2}$ for every $g \in G \setminus \{1\}$; the upper bound is achieved when g is a transposition. Observe also that $\text{orb}_\Omega(g) \leq n/2$ for every $g \in G_2$. Therefore from Equation (4) and Lemma 4.1 we deduce

$$2 \binom{m}{k} \leq 2^{\frac{1}{2} \binom{m}{k} + \frac{1}{2} (\binom{m-2}{k} + \binom{m-2}{k-2})} |\text{Aut}(A_m)| + 2^{\frac{1}{2} \binom{m}{k}} |\text{Aut}(A_m)|^2. \tag{5}$$

Thus

$$2^{\binom{m}{k}} \leq 2^{\frac{1}{2}\binom{m}{k} + \frac{1}{2}(\binom{m-2}{k} + \binom{m-2}{k-2}) + 1} |\text{Aut}(A_m)|^2$$

and

$$2^{\frac{1}{2}\binom{m}{k} - \frac{1}{2}\binom{m-2}{k} - \frac{1}{2}\binom{m-2}{k-2}} \leq 2 |\text{Aut}(A_m)|^2,$$

and hence

$$2^{\binom{m-2}{k-1}} \leq 2 |\text{Aut}(A_m)|^2, \tag{6}$$

where we use Pascal’s recurrence for binomial coefficients twice to obtain

$$\binom{m}{k} = \binom{m-2}{k} + 2\binom{m-2}{k-1} + \binom{m-2}{k-2}.$$

Using $2^{\binom{m-2}{k-1}} \geq 2^{(m-2)(m-3)/2}$ and $m! \leq m^{m-1}$, we find that Equation (6) holds true only for $m \leq 21$. For $m \leq 21$, a careful computation yields that Equation (5) holds true only for $m \leq 8$. Finally, when $m \leq 8$, we may consider in turn all the possibilities for G and check that Equation (4) is never satisfied.

Case (a)(ii) Now suppose that the socle of G is A_m^ℓ in its product action on ℓ direct copies of $\{1, \dots, m\}$ with $\ell \geq 2$ and $m \geq 5$.

Suppose first that $\ell = 2$. Hence $n = m^2$ and we may identify Ω with the set of ordered pairs of elements of $\{1, \dots, m\}$. Let τ be the two-graph induced by the switching class \mathcal{S} . Now, G has rank 3 in its action on Ω and G has four orbits on the set of 3-subsets of Ω : namely

$$\begin{aligned} \mathcal{O}_1 &= \{ \{(a, a), (a, b), (a, c)\} \mid a, b, c \text{ distinct elements of } \{1, \dots, m\} \}, \\ \mathcal{O}_2 &= \{ \{(a, a), (a, b), (c, c)\} \mid a, b, c \text{ distinct elements of } \{1, \dots, m\} \}, \\ \mathcal{O}_3 &= \{ \{(a, a), (a, b), (b, a)\} \mid a, b \text{ distinct elements of } \{1, \dots, m\} \}, \\ \mathcal{O}_4 &= \{ \{(a, a), (b, b), (c, c)\} \mid a, b, c \text{ distinct elements of } \{1, \dots, m\} \}. \end{aligned}$$

(These orbits correspond to the non-equivalent geometric positions of three points in an $m \times m$ grid.) Replacing τ by its complement $\tau' = \{x \subseteq \Omega \mid |x| = 3, x \notin \tau\}$, we may assume that $\mathcal{O}_1 \subseteq \tau$. Now consider the 4-subset $x = \{(a, a), (a, b), (a, c), (b, a)\}$ of Ω . Clearly, x has one 3-subset in common with \mathcal{O}_1 , one with \mathcal{O}_2 , two with \mathcal{O}_3 and zero with \mathcal{O}_4 . As τ is a two-graph, x has an even number of 3-subsets in common with τ and hence $\mathcal{O}_2 \subseteq \tau$. Now an easy inspection gives that $\mathcal{O}_1 \cup \mathcal{O}_2$ is a two-graph and (using that τ is a proper two-graph) we have $\tau = \mathcal{O}_1 \cup \mathcal{O}_2$.

Recall that the grid graph Γ' is the graph with vertex set Ω and where two distinct vertices α and β are declared to be adjacent if α and β are in the same row or in the same column (that is, the first or the second coordinates of α and β are equal). It is readily seen that the two-graph afforded by the complement Γ of Γ' is τ and hence $\Gamma \in \mathcal{S}$. Thus $\text{Aut}(\Gamma) \leq \text{Aut}(\tau) = G$ and hence $\text{Aut}(\Gamma) < G$ because we are dealing with Type II. It is well-known (see for example [10, Theorem and Table I]) that $\text{Aut}(\Gamma) \cong S_m \text{ wr } S_2$ and $\text{Aut}(\Gamma)$ is a maximal subgroup of $\text{Sym}(\Omega)$. Thus $\text{Aut}(\Gamma) = \text{Aut}(\mathcal{S})$, contradicting the assumption of Type II.

Suppose then that $\ell \geq 3$. Now $\text{fix}_\Omega(g) \leq m^{\ell-1}(m-2)$ for every $g \in G \setminus \{1\}$; the upper bound is achieved when g is a transposition (see for example [8, Lemma 6.13] or the proof of [19, Lemma 4.5]). Observe also that $\text{orb}_\Omega(g) \leq n/2$ for every $g \in G_2$. Therefore from Equation (4) and Lemma 4.1 we deduce

$$2^{m^\ell} \leq 2^{\frac{1}{2}m^\ell + \frac{1}{2}(m^{\ell-1}(m-2))} m!^\ell \ell! + 2^{\frac{1}{2}m^\ell} (m!^\ell \ell!)^2. \tag{7}$$

Thus

$$2^{m^\ell} \leq 2^{m^\ell - m^{\ell-1} + 1} (m!^\ell \ell!)^2$$

and hence

$$2^{m^{\ell-1} - 1} \leq (m!^\ell \ell!)^2. \tag{8}$$

Using $\ell \geq 3$, $m! \leq m^{m-1}$ and $\ell! \leq \ell^{\ell-1}$, we find that Equation (8) holds true only when $\ell = 3$. In this case, a careful computation yields that Equation (7) is never satisfied.

Case (a)(iii): the socle of G is A_m^ℓ in its product action on ℓ direct copies of the k -subsets of $\{1, \dots, m\}$ with $\ell \geq 2$, $m \geq 5$ and $2 \leq k < m/2$.

The argument is similar to the previous two cases. Here $n = \binom{m}{k}^\ell$. From [8, Lemma 6.13] (or from an easy computation), we deduce that

$$\text{fix}_\Omega(g) \leq \binom{m}{k}^{\ell-1} \left(\binom{m-2}{k} + \binom{m-2}{k-2} \right),$$

for every $g \in G \setminus \{1\}$. Moreover, as usual, $\text{fix}_\Omega(g) \leq 2^{n/2}$ for every $g \in G_2$. Therefore from Equation (4) and Lemma 4.1 we get

$$2^{\binom{m}{k}^\ell} \leq 2^{\frac{1}{2}\binom{m}{k}^\ell + \frac{1}{2}\left(\binom{m}{k}^{\ell-1} \left(\binom{m-2}{k} + \binom{m-2}{k-2}\right)\right)} m!^\ell \ell! + 2^{\frac{1}{2}\binom{m}{k}^\ell} (m!^\ell \ell!)^2. \tag{9}$$

Observe that

$$\frac{1}{2} \binom{m}{k}^\ell + \frac{1}{2} \left(\binom{m}{k}^{\ell-1} \left(\binom{m-2}{k} + \binom{m-2}{k-2} \right) \right) = \binom{m}{k}^\ell - \binom{m-2}{k-1} \binom{m}{k}^{\ell-1}.$$

Now, using $k \geq 2$, $\ell \geq 2$ and $\binom{m}{k} \geq m(m-1)/2$ and arguing as in the previous two cases, we see that Equation (9) is never satisfied.

Case (b): the group G is the Mathieu group M_n with $n \in \{11, 12, 23, 24\}$ and hence $n \leq 32$.

Case (c): We assume that none of the previous cases occurs.

From [12, Theorem 1.1], we have $|G| \leq n^{1+\log_2(n)}$. Moreover from [9, Corollary 1], for every $g \in G \setminus \{1\}$, we have $\text{fix}_\Omega(g) \leq 4n/7$. In particular, for every $g \in G \setminus \{1\}$,

we get $\text{orb}_\Omega(g) \leq n/2 + 2n/7 = 11n/14$ by Lemma 4.1. Observe also that, for every $g \in G_2$, $\text{orb}_\Omega(g) \leq n/2$. Taking these bounds into account, Equation (4) yields

$$\frac{2^n}{|G|} \leq \frac{1}{2} \left(\frac{2^n}{|G|} + 2^{\frac{11n}{14}} \frac{|G| - 1}{|G|} + |G_2| 2^{\frac{n}{2}} \right) < \frac{1}{2} \left(\frac{2^n}{|G|} + 2^{\frac{11n}{14}} + |G| 2^{\frac{n}{2}} \right).$$

Hence

$$2^n \leq 2^{11n/14} |G| + 2^{n/2} |G|^2 \leq 2^{11n/14} n^{1+\log_2(n)} + 2^{n/2} n^{2+2\log_2(n)}. \tag{10}$$

A computation yields $n \leq 384$.

Observe that G is not 3-homogeneous because it is the automorphism group of a non-trivial two-graph. In particular, we may (and will) assume that G is not 3-homogeneous. Now that the degree n is so small we can afford to compute the exact value of Equation (4). Indeed, a computer calculation using the database of small primitive groups shows that, for $n \leq 384$, Equation (4) holds true only if $n \leq 64$.

For the remaining cases, we first construct the switching module W and we compute (using the Orbit-Stabiliser lemma) the exact value of

$$\#G\text{-orbits on } W = \frac{1}{|G|} \sum_{g \in G} |\mathbf{C}_W(g)|.$$

Using this formula and Equation (2), we check that Equation (1) is satisfied only for primitive groups of degree $n \leq 32$. □

5 Groups of small degree

For groups of small degree, including the examples, we adopted a different strategy. We only need to consider even degrees n : as explained earlier, any possible example for odd n will fall under Type I, and will be on Seress’ list. A simplified version of the algorithm takes a primitive group G of degree n , and does the following.

- (a) Compute the orbits of G on 3-element subsets of $\{1, \dots, n\}$.
- (b) For each union of orbits, check whether G is the full automorphism group of the corresponding 3-uniform hypergraph, and discard it if not. Then check whether the hypergraph is a two-graph, and discard it if not.
- (c) On reaching this point, compute the graphs in the corresponding switching class and their automorphism groups. Stop when either a graph with trivial group is found, or every graph in the switching class has been considered. In the latter case, record that an example has been found.

The computations were done using GAP [7]. We describe each step in more detail.

Step (a) is straightforward; a single line of GAP code does this. In Step (b), we only need one of each complementary pair of two-graphs; this is most easily achieved by omitting the last orbit on triples from the union. Also, we do not have to consider the empty collection of orbits. We compute the automorphism group using nauty [13], interfaced to GAP via the DESIGN package [17].

To check the two-graph property, it would suffice to check orbit representatives for G on 4-subsets, to see whether each contains an even number of 3-subsets from the collection being considered. To avoid a potentially large orbit computation, but use the fact that G is transitive, we simply checked all 4-subsets containing the point n .

Up to degree 32, the only two-graphs on an even number of points with primitive automorphism groups are

- those with 2-transitive groups, classified by Taylor [20]: these are the Paley two-graphs with automorphism group $\text{P}\Sigma\text{L}(2, q)$, where q is a prime power congruent to 1 (mod 4), the symplectic two-graph on 16 points with group $2^4.S_6$, and the orthogonal two-graph on 28 points with group $\text{P}\text{Sp}(6, 2)$;
- two (isomorphic) examples on 10 points with group A_5 , six on 28 points with group $\text{PGL}(2, 7)$, and six on 28 points with group $\text{PSL}(2, 8)$.

Exploration in the range from 32 to 40 suggests that examples become commoner.

The second type above surprised us a little; here is an explanation of the two examples on 10 points. The group is A_5 acting on pairs. The orbits of S_5 on triples of pairs are isomorphism types of graphs with five vertices and three edges, namely K_3 , $K_{1,3}$, $K_2 \cup P_3$, and P_4 , where K_r , $K_{r,s}$ and P_s are complete graphs, complete bipartite graphs, and paths respectively (the subscripts are the number of vertices). Since the automorphism group of P_4 contains only even permutations, this orbit splits into two under the action of A_5 . Now Table 1 gives the inclusions of graphs in these orbits in 4-edge graphs.

	1	1	0	1	1
	1	0	3	0	0
	0	0	0	2	2
	0	1	1	1	1
	0	4	0	0	0
	0	0	2	0 or 2	2 or 0

Table 1: Graphs on 5 vertices

The table shows (up to complementation) one two-graph admitting S_5 , consisting of the P_4 graphs. This is the Paley two-graph with automorphism group $\text{P}\Sigma(2, 9)$, aka S_6 . But we have two further two-graphs admitting A_5 , each consisting of one orbit on P_4 s together with the $K_{1,3}$ s. An element of $S_5 \setminus A_5$ induces an isomorphism between these two-graphs; their symmetric difference is the Paley two-graph.

For step (c), we first construct the graph in the switching class which has vertex n isolated: join x and y if and only if $\{x, y, n\}$ is a triple in the collection. We can then use the fact that switching with respect to a set and its complement are identical, so we need only consider switching sets not containing n . These sets are generated iteratively, the starting graph is switched, and the automorphism group found by calling `nauty` from the `GAP` package `GRAPE` [18].

References

- [1] L. Babai, On the order of uniprimitive permutation groups, *Ann. Math. (2)* **113** (1981), 553–558.
- [2] L. Babai, P. J. Cameron, Most primitive groups are automorphism groups of edge-transitive hypergraphs, *J. Algebra* **421** (2015), 512–523.
- [3] P. J. Cameron, Cohomological aspects of two-graphs, *Math. Z.* **157** (1977), 101–119.
- [4] P. J. Cameron, Automorphism groups of graphs, in *Selected Topics in Graph Theory II* (ed. L. W. Beineke and R. J. Wilson), Academic Press, London, 1983, pp.89–127.
- [5] P. J. Cameron, Regular orbits of permutation groups on the power set, *Discrete Math.* **62** (1986), 307–309.
- [6] P. J. Cameron, P. M. Neumann, J. Saxl, On groups with no regular orbits on the set of subsets, *Arch. Math.* **43** (1984), 295–296.
- [7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.7.5; 2014. (<http://www.gap-system.org>)
- [8] M. Giudici, C. E. Praeger, P. Spiga, Finite primitive permutation groups and regular cycles of their elements, *J. Algebra* **421** (2015), 27–55.
- [9] R. Guralnick, K. Magaard, On the minimal degree of a primitive permutation group, *J. Algebra* **207** (1998), 127–145.
- [10] M. W. Liebeck, C. E. Praeger, J. Saxl, A classification of the maximal subgroups of the finite alternating and symmetric groups, *J. Algebra* **111** (1987), 365–383.
- [11] C. L. Mallows, N. J. A. Sloane, Two-graphs, switching classes, and Euler graphs are equal in number, *SIAM J. Appl. Math.* **28** (1975), 876–880.

- [12] A. Maróti, On the orders of primitive groups, *J. Algebra* **258** (2002), 631–640.
- [13] B.D. McKay, `nauty` user’s guide (version 1.5), Technical report TR-CS-90-02, Australian National University, Computer Science Department, 1990, <http://cs.anu.edu.au/people/bdm/nauty/>.
- [14] L. Pyber, On the orders of doubly transitive permutation groups, elementary estimates, *J. Combinatorial Theory (A)* **62** (1993), 361–366.
- [15] J. J. Seidel, A survey of two-graphs, pp. 481–511 in *Proc. Internat. Coll. Teorie Combinatorie* (Roma 1973), Accad. Naz. Lincei, Roma, 1977.
- [16] Á. Seress, Primitive groups with no regular orbits on the set of subsets, *Bull. London Math. Soc.* **29** (1997), 697–704.
- [17] L.H. Soicher, The DESIGN package for GAP, Version 1.6, 2011, <http://designtheory.org/software/gap-design/>.
- [18] L.H. Soicher, The GRAPE package for GAP, Version 4.6.1, 2012, <http://www.maths.qmul.ac.uk/~leonard/grape/>.
- [19] P. Spiga, Finite primitive groups and edge-transitive hypergraphs, arXiv 1407.0953.
- [20] D. E. Taylor, Regular 2-graphs, *Proc. London Math. Soc. (3)* **35** (1977), 257–274.

(Received 20 July 2014; revised 19 Feb 2015)