Cherlin's conjecture on finite primitive binary permutation groups

Nick Gill
Department of Mathematics,
University of South Wales,
Treforest CF37 1DL, U.K.
nick.gill@southwales.ac.uk

Martin W. Liebeck
Department of Mathematics,
Imperial College London,
London SW7 2AZ, UK
m.liebeck@imperial.ac.uk

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

In memory of Jan Saxl.

Contents

Chapter 1

Introduction

In this monograph, we are concerned with the problem of classifying the finite primitive binary permutation groups. Let G be a permutation group on the set Ω. Given a positive integer n, given $I := (\omega_1, \omega_2, \ldots, \omega_n)$ in the Cartesian product Ω^n and given $g \in G$, we write

$$I^g := (\omega_1^g, \omega_2^g, \ldots, \omega_n^g).$$

Moreover, for every $1 \leq i < j \leq n$, we let $I_{ij} := (\omega_i, \omega_j)$ be the 2-subtuple of I corresponding to the i^{th} and to the j^{th} coordinate. Now, the permutation group G on Ω is called *binary* if, for all positive integers n, and for all I and J in Ω^n, there exists $g \in G$ such that $I^g = J$ if and only if for all 2-subtuples, I_{ij}, of I, there exists an element g_{ij} such that $I_{ij}^{g_{ij}} = J_{ij}$.

Cherlin has proposed a conjecture listing the finite primitive binary permutation groups [20]. The conjecture is as follows, and our task is to complete the proof of this conjecture.

Conjecture 1.1. *A finite primitive binary permutation group must be one of the following:*

1. *a symmetric group* $\mathrm{Sym}(n)$ *acting naturally on* n *elements;*
2. *a cyclic group of prime order acting regularly on itself;*
3. *an affine orthogonal group* $V \rtimes \mathrm{O}(V)$ *with* V *a vector space over a finite field equipped with a non-degenerate anisotropic quadratic form, acting on itself by translation, with complement the full orthogonal group* $\mathrm{O}(V)$.

The terminology of Conjecture 1.1 is fully explained in subsequent sections. In particular, we give two equivalent definitions of the adjective "binary" in §1.1, and all three families listed in Conjecture 1.1 are fully discussed in §1.2.

The O'Nan–Scott theorem describes the structure of finite primitive permutation groups: there are five families of these. Thus, to prove Conjecture 1.1, it is sufficient to prove it for each of these families.

Cherlin himself gave a proof of the conjecture for the family of affine permutation groups, i.e. when G has an abelian socle [21]. Wiscons then studied the remaining cases and showed that Conjecture 1.1 reduces to the following statement concerning almost simple groups [108].

Conjecture 1.2. *If* G *is a finite binary almost simple primitive group on* Ω*, then* $G = \mathrm{Sym}(\Omega)$.

We recall that an *almost simple group* G is a finite group that has a unique minimal normal subgroup S and, moreover, the group S is non-abelian and simple. Note that S is the socle of G.

We now invoke the Classification of Finite Simple Groups which says that a non-abelian simple group is either an alternating group, $\mathrm{Alt}(n)$ with $n \geq 5$; a simple group of Lie type; or one of 26 sporadic groups.

In [46], Conjecture 1.2 was proved for groups with socle a simple alternating group; in [34], Conjecture 1.2 was proved for groups with socle a sporadic simple group. In this monograph we deal with the remaining family.

Theorem 1.3. *Let G be an almost simple group with socle a finite group of Lie type and assume that G has a primitive and binary action on a set Ω. Then $|\Omega| \in \{5, 6, 8\}$ and $G \cong \mathrm{Sym}(\Omega)$.*

The examples in Theorem 1.3 arise via the isomorphisms

1. $G \cong \mathrm{SL}_2(4).2 \cong \mathrm{PGL}_2(5) \cong \mathrm{Sym}(5)$ and $|\Omega| = 5$;
2. $G \cong \mathrm{Sp}_4(2) \cong \mathrm{PSL}_2(9).2 \cong \mathrm{Sym}(6)$ and $|\Omega| = 6$;
3. $G \cong \mathrm{SL}_4(2).2 \cong \mathrm{Sym}(8)$ and $|\Omega| = 8$.

Note that, here, we have not tried to list all isomorphisms between classical groups and the symmetric groups listed in Theorem 1.3. The listed isomorphisms are the ones that crop up in the proof that follows; there are many further isomorphisms with classical groups not listed in the theorem (for example $\mathrm{SO}_4^-(2) \cong \Gamma\mathrm{O}_3(4) \cong \mathrm{Sym}(5)$).

A special case of Theorem 1.3 has already appeared in the literature; in [34], the theorem is proved for the case where G is almost simple with socle a finite group of Lie type of rank 1.

Theorem 1.3 is the final piece in the jigsaw. We can now assert that Cherlin's conjecture is true:[1]

Corollary 1.4. *Conjecture* 1.1 *is true.*

As will become clear, once the various equivalent definitions of the word "binary" have been introduced, a proof of Conjecture 1.1 is equivalent to a classification of the finite primitive binary relational structures. In particular we have the following (the definition of homogeneous relational structure can be found in Definitions 1.1.1 and 1.1.5):

[1]Wiscons informed us of a small gap in his proof of [108, Proposition 4.1]. After discussion with Wiscons we are able to patch this gap; the rest of this footnote does this. For notation and terminology, we refer to the rest of this chapter.

Proposition 4.1 of [108] is devoted to showing that primitive groups of diagonal type are not binary. The gap in the proof stems from an implicit assumption in the first sentence of the proof of [108, Lemma 4.2] that the socle is a product of at least *three* isomorphic nonabelian simple groups. This leaves open the case of two factors, for which it suffices to consider the following setting: let G be a group with socle $T \times T$ where T is a nonabelian simple group; suppose that G acts on a copy of T in such a way that the stabilizer of $1 \in T$ satisfies $\mathrm{Inn}(T) \le G_1 \le \mathrm{Aut}(T) \times \langle i \rangle$ for $i : T \to T$ the inversion map. In this context, we show the action of G on T is not binary.

To see this, we consider two cases. Suppose first that, there exist $a, b \in T$ with $T = \langle a, b \rangle$ and with the property that there exists no $\varphi \in \mathrm{Aut}(T)$ such that $a^\varphi = a^{-1}$ and $b^\varphi = b^{-1}$. Observe that $(1, a, b, ab)$ and $(1, a, b, ba)$ are 2-subtuple complete (witnessed by conjugating by 1, a, or b^{-1}). However, $(1, a, b, ab)$ and $(1, a, b, ba)$ are not 4-subtuple complete. Indeed, if $\varphi \in G \cap \mathrm{Aut}(T)$ and $(1, a, b, ab)^\varphi = (1, a, b, ba)$, then φ is the identity automorphism of T because a and b generate T; however $ab = (ab)^\varphi \neq ba$, because T is non-abelian. Similarly, if $\varphi i \in G \setminus \mathrm{Aut}(T)$ (for some $\varphi \in \mathrm{Aut}(T)$) and $(1, a, b, ab)^{\varphi i} = (1, a, b, ba)$, then $a^\varphi = a^{-1}$ and $b^\varphi = b^{-1}$, contrary to our assumption on a and b.

Suppose now that, for every $a, b \in T$ with $T = \langle a, b \rangle$, there exists $\varphi \in \mathrm{Aut}(T)$ such that $a^\varphi = a^{-1}$ and $b^\varphi = b^{-1}$. The finite groups T satisfying this property are called strongly symmetric and have been classified in [84]. In particular, $T \cong \mathrm{PSL}_2(q)$, for some prime power q. At this point we argue by contradiction and we suppose that the action of G on T is binary.

Assume q odd. When $q \in \{5, 7, 9\}$, we have verified that the group G is not binary with the help of a computer; therefore, we may suppose that $q \ge 11$. Let a be an involution of T, let $\Lambda := a^{G_1}$ the G_1-orbit containing a and let X be the permutation group induced by G_1 on Λ. As G is binary on T, Lemma 1.7.1 implies that X is binary on Λ. Notice that X is almost simple with socle $X_0 \cong \mathrm{PSL}_2(q)$ and, by definition, X acts transitively on Λ. The stabilizer of the point a is $C_X(a)$ and, since q is odd, we know that $C_{X_0}(a)$ is dihedral of order $q \pm 1$. Referring to [10] we see that, since $q \ge 11$, $C_X(a)$ is maximal in X. We deduce that X is an almost simple primitive group with socle $T \cong \mathrm{PSL}_2(q)$ in its action on Λ. Now, by [45], we reach a contradiction.

Assume q even. When $q \in \{4, 8\}$, we have verified that the group G is not binary with the help of a computer; therefore, we may suppose that $q \ge 16$. Let $x, y \in \mathbb{F}_q$ such that the additive subgroup of $\mathbb{F}_q$ generated by $1, x$ and y has order 8 and with x, y and 1 in distinct orbits under the Galois group $\mathrm{Gal}(\mathbb{F}_q)$. Observe that, as $q \ge 16$, there are some choices for x and y. Now, consider

$$a := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, b := \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, c := \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}.$$

It is not hard to verify that, for the action of G, the triples $(1, a, b)$ and $(1, a, c)$ are 2-subtuple complete, but not 3-subtuple complete.

Corollary 1.5. *Let $\mathcal{R}$ be a homogeneous binary relational structure with vertex set Ω, such that $G = \mathrm{Aut}(\mathcal{R})$ acts primitively on Ω. Then the action of G on Ω is one of the actions listed in Conjecture* 1.1.

We have not completely described the relational structure $\mathcal{R}$ in our statement of Corollary 1.5 – to do this, we would need to specify the relations in $\mathcal{R}$ all of which must be unions of orbits of G on Ω^2. We will not do this here.

It is worth remarking that, although we can assert that Conjecture 1.1 is true, considerable mystery lingers as to "why". Our proof relies on the Classification of Finite Simple Groups, on the O'Nan–Scott theorem and on a lot of algebra. On the other hand, looking at Corollary 1.5 for instance, one might hope to somehow see why the conjecture is true by thinking directly about the geometry of homogeneous binary relational structures. Thus far, this direction of thought has been a frustrating *cul de sac*.

For the remainder of this chapter we have three basic aims: first we seek to give the basic theory of relational complexity for permutation groups including, in particular, the definition of a binary action, and of a binary permutation group. We will also describe some of the key examples.

Second, we will give some motivation for interest in our result – thus we will survey some related results in the study of relational structures, and in group theory. We will also briefly discuss Cherlin's original motivation for studying binary permutation groups, which arises from model theoretic considerations.

In neither of these first two aspects do we make any claim for originality – instead we seek to draw the key definitions and examples together into one place. Much of the material of this kind that we present below was worked out by Cherlin in his papers [20, 21, 26].

Our third aim in this chapter is to present some of the results and methods concerning binary permutation groups that we consider to be most essential. These will be used in subsequent chapters when we commence our proof of Theorem 1.3.

The remainder of this monograph is occupied with a proof of Theorem 1.3. In Chapter **??** we give a number of general background results concerning groups of Lie type; in Chapter **??** we prove the theorem for the exceptional groups of Lie type; in Chapter **??** we prove the theorem for the classical groups of Lie type.

Acknowledgements

All three authors were supported in this work by the Engineering and Physical Sciences Research Council grant number EP/R028702/1.

All three of us wish to express our thanks to Gregory Cherlin for his help and encouragement of our work, and for his creation of the beautiful mathematics that inspired our research in the first place. Thanks are also due to Joshua Wiscons for a number of helpful discussions.

NG and PS would like to thank their PhD students, Scott Hudson and Bianca Lodà; their research into the relational complexity of permutation groups has shed a great deal of light.

1.1 Basics: The definition of relational complexity

The notion of relational complexity can be defined in two different ways. Our job in this section is to present these definitions, and to show that they are equivalent. Throughout this section G is a permutation group on a set Ω of size $t < \infty$. Note that when we write "permutation group" we are assuming that the associated action of G on Ω is faithful – in other words we can think of G as a subgroup of $\mathrm{Sym}(\Omega)$.

1.1.1 Relational structures

The first approach towards relational complexity is via the concept of a relational structure [21]. Recall that, for a positive integer ℓ, Ω^ℓ denotes the set of ℓ-tuples with entries in Ω.

Definition 1.1.1. A *relational structure* $\mathcal{R}$ is a tuple $(\Omega, R_1, \dots, R_k)$, where Ω is a set, k is a non-negative integer and, for each $i \in \{1, \dots, k\}$, there exists an integer $\ell_i \geq 2$ such that $R_i \subseteq \Omega^{\ell_i}$.

The set Ω is called the *vertex set* of the structure, while the sets $R_1, \dots, R_k$ are referred to as *relations*; in addition, for each i, the integer ℓ_i is the *arity* of relation R_i. We say that the relational structure $\mathcal{R}$ *is of arity* ℓ, where $\ell = \max\{\ell_1, \dots, \ell_k\}$.

Example 1.1.2. If a relation, or a relational structure is of arity 2 (resp. 3), then it is commonly called *binary* (resp. *ternary*). Binary relational structures which contain a single relation are nothing more nor less than directed graphs: if $\mathcal{R} = (\Omega, R_1)$ is one such, then the elements of the vertex set Ω are of course the vertices, and each pair in R_1 can be thought of as a directed edge between two elements of Ω. (Note that by "graph" here we implicitly mean a graph with no multiple edges.)

When considering a binary relational structure with more than one relation, it is sometimes helpful to think of it as a directed graph in which there are several different "edge colours" – each relation corresponding to a different "colour".

The notions of isomorphism and automorphism are generalizations of the corresponding definitions for graphs.

Definition 1.1.3. Let $\mathcal{R} = (\Omega, R_1, \dots, R_k)$ and $\mathcal{S} = (\Lambda, S_1, \dots, S_k)$ be relational structures. An isomorphism $h : \mathcal{R} \to \mathcal{S}$ is a bijection $h : \Omega \to \Lambda$ such that

$$(\omega_1, \dots, \omega_{\ell_i}) \in R_i \iff (\omega_1^h, \dots, \omega_{\ell_i}^h) \in S_i.$$

An *automorphism* g of $\mathcal{R}$ is an element of $\mathrm{Sym}(\Omega)$ that is also an isomorphism $g : \mathcal{R} \to \mathcal{R}$. It is clear that the set of all automorphisms of $\mathcal{R}$ forms a group under composition of bijections; we denote this group by $\mathrm{Aut}(\mathcal{R})$, and note that it is a subgroup of $\mathrm{Sym}(\Omega)$.

Note that we have only defined isomorphisms between relational structures that have the same number of relations; the definition also implies that the (ordered) list of relation-arities must be the same for isomorphic relational structures.[2]

Our focus will be on those relational structures that exhibit the maximum possible level of symmetry – this requires the notion of *homogeneity*. To state this definition we must first explain what is meant by "an induced substructure" – once again this notion is a direct analogue of the same idea for graphs.

Definition 1.1.4. Let $\mathcal{R} = (\Omega, R_1, \dots, R_k)$ be a relational structure, with R_i a relation of arity ℓ_i for each $i = 1, \dots, k$. Let Γ be a subset of Ω. The *induced substructure on* Γ is the relational structure $\mathcal{R}_\Gamma = (\Gamma, R_1', \dots, R_k')$ where $R_i' = \Gamma^{\ell_i} \cap R_i$.

So, to clarify what we said above: if $\mathcal{R} = (\Omega, R_1)$ is a binary structure with a single relation (i.e. a directed graph), and Γ is a subset of the vertex set Ω, then $\mathcal{R}_\Gamma$ is precisely the induced subgraph on Γ.

Definition 1.1.5. A relational structure $\mathcal{R} = (\Omega, R_1, \dots, R_k)$ is called *homogeneous* if, for all $\Gamma, \Gamma' \subset \Omega$ and for all isomorphisms $h : \mathcal{R}_\Gamma \to \mathcal{R}_{\Gamma'}$, there exists $g \in \mathrm{Aut}(\mathcal{R})$ such that $g|_\Gamma = h$.

The following example will be important shortly.

Example 1.1.6. Given a permutation group G on a set Ω of size t, we define a relational structure $\mathcal{R}_G = (\Omega, R_1, \dots, R_k)$, where the relations $R_1, \dots, R_k$ are precisely the orbits of the group G on the sets $\Omega, \Omega^2, \dots, \Omega^{t-1}$.

Observe, first, that by definition any element of G maps an element of relation R_i to an element of relation R_i, for all $i \in \{1, \dots, k\}$; we conclude that $G \leq \mathrm{Aut}(\mathcal{R}_G)$.

On the other hand, suppose that $h \in \mathrm{Aut}(\mathcal{R}_G)$, and let $r = (\omega_1, \dots, \omega_{t-1})$ be a tuple of distinct elements in Ω lying in relation R_j, for some j. The image of this tuple under h also lies in R_j; since R_j is an orbit

[2] One can imagine a slight weakening of Definition 1.1.3 where one allows an automorphism of $\mathcal{R}$ to map a set of tuples corresponding to one relation to the set of tuples corresponding to a different relation – for certain relational structures, this would yield a larger automorphism group (which would contain $\mathrm{Aut}(\mathcal{R})$ as defined above, as a normal subgroup). We will not need this extension in what follows.

of G, this implies that there exists $g \in G$ such that for all $i \in \{1, \ldots, t-1\}$, $\omega_i^h = \omega_i^g$. It follows that $\omega_t^h = \omega_t^g$, where ω_t is the only element of Ω not represented in the tuple r. We conclude that $h = g$ and so, in particular, $G = \mathrm{Aut}(\mathcal{R}_G)$.

Finally, suppose that Γ and Δ are proper subsets of Ω of size s such that the associated induced relational structures are isomorphic, i.e. there exists an isomorphism $h : (\mathcal{R}_G)_\Gamma \to (\mathcal{R}_G)_\Delta$. Let $r_\gamma = (\gamma_1, \ldots, \gamma_s)$ be a tuple containing all of the distinct elements of Γ, and observe that r_γ lies in a relation R_j of $\mathcal{R}_G$, for some j. Indeed, by construction, r_γ lies in the corresponding relation R_j of $(\mathcal{R}_G)_\Gamma$, and so $(r_\gamma)^h$ lies in the corresponding relation R_j of $(\mathcal{R}_G)_\Delta$, and hence also lies in the relation R_j of $\mathcal{R}_G$. In particular, since R_j is an orbit of G, we conclude that there exists $g \in G$ such that for all $i \in \{1, \ldots, s\}$, $\gamma_i^h = \gamma_i^g$. Since $G = \mathrm{Aut}(\mathcal{R}_G)$, we conclude that $\mathcal{R}_G$ is homogeneous.

We are ready to give our first definition of relational complexity. Before stating it, we remind the reader that we are assuming that G is a permutation group on a set Ω, and we recall that if $\mathcal{R}$ is any relational structure with vertex set Ω, then $\mathrm{Aut}(\mathcal{R})$ is also a permutation group on Ω.

Definition 1.1.7. The *structural relational complexity* of a permutation group G is equal to the smallest integer $s \geq 2$ for which there exists a homogeneous relational structure $\mathcal{R} = (\Omega, R_1, \ldots, R_k)$ of arity s such that $\mathrm{Aut}(\mathcal{R})$ is permutation isomorphic to G.

Note that Example 1.1.6 implies, in particular, that if $|\Omega| \geq 3$, then the structural relational complexity of G is well-defined, and is bounded above by $|\Omega| - 1$ (and is at least 2). In what follows, we will write $\mathrm{SRC}(G, \Omega)$ for the structural relational complexity of the permutation group G.

One might wonder why we have required that $\mathrm{SRC}(G, \Omega) \geq 2$. The reason is that, in the next section we will define a different statistic $\mathrm{TRC}(G, \Omega)$ using a completely different approach, and we will also require that $\mathrm{TRC}(G, \Omega) \geq 2$. We will then show that $\mathrm{SRC}(G, \Omega) = \mathrm{TRC}(G, \Omega)$ for all permutation groups G on a set Ω. Were we to omit the requirement that $\mathrm{SRC}(G, \Omega) \geq 2$ and $\mathrm{TRC}(G, \Omega) \geq 2$, there would be a number of actions for which $\mathrm{SRC}(G, \Omega) \neq \mathrm{TRC}(G, \Omega)$, for instance the natural action of $\mathrm{Sym}(\Omega)$.

1.1.2 Tuples

In this section we give an alternative approach to the notion of relational complexity based on [26]. We then show that it coincides with the approach of the previous section. As before G is a permutation group on a finite set Ω.

Definition 1.1.8. Let $2 \leq r \leq n$ be positive integers, and let $I = (I_1, \ldots, I_n)$ and $J = (J_1, \ldots, J_n)$ be elements of Ω^n. We say that I and J are *r-subtuple complete with respect to G* if, for all $k_1, k_2, \ldots, k_r$ integers with $1 \leq k_1, k_2, \ldots, k_r \leq n$, there exists $g \in G$ with $I_{k_i}^g = J_{k_i}$ for $i \in \{1, \ldots, r\}$. In this case we write $I \underset{r}{\sim} J$.

Note that if $I \underset{r}{\sim} J$ and $u \leq r$, then $I \underset{u}{\sim} J$.

Definition 1.1.9. The permutation group G has *tuple relational complexity* equal to s if the following two conditions hold:

1. if $n \geq s$ is any integer and I, J are elements of Ω^n such that $I \underset{s}{\sim} J$, then there exists $g \in G$ such that $I^g = J$.
2. $s \geq 2$ is the smallest integer for which (1) holds.

We write $\mathrm{TRC}(G, \Omega)$ for the tuple relational complexity of the permutation group G.

Put another way, the tuple relational complexity of G is the smallest integer $s \geq 2$ such that

$$I \underset{s}{\sim} J \implies I \underset{n}{\sim} J,$$

for any integer $n \geq s$, and any pair of n-tuples I and J.

It is not immediately clear, *a priori*, that $\mathrm{TRC}(G, \Omega)$ exists for every permutation group G on the set Ω. The next lemma deals with this concern.

Lemma 1.1.10. *If* $\mathrm{SRC}(G,\Omega)=s$, *then* $\mathrm{TRC}(G,\Omega)$ *exists and is bounded above by* s.

Proof. Let $n\geq 2$ be some integer, and let I and J be subsets of Ω^n such that $I \underset{s}{\sim} J$. We must prove that there exists $g\in G$ such that $I^g=J$.

Let $\mathcal{R}$ be a homogeneous relational structure of arity s for which $G=\mathrm{Aut}(\mathcal{R})$. Write $\{I\}$ (resp. $\{J\}$) for the underlying set associated with the n-tuple I (resp. J); as $s\geq 2$, these sets must be of equal cardinality bounded above by n. Now consider the induced substructures $\mathcal{R}_{\{I\}}$ and $\mathcal{R}_{\{J\}}$ and consider the map $h:\mathcal{R}_{\{I\}}\to\mathcal{R}_{\{J\}}$ for which $h(I_i)=J_i$ for all $i\in\{1,\dots,n\}$.

We claim that h is an isomorphism of relational structures. Let $(I_{i_1},\dots,I_{i_u})$ be an element of some relation R_j in $\mathcal{R}_{\{I\}}$. Note that $u\leq s$ and recall that $I \underset{u}{\sim} J$ with respect to the action of G. Thus there exists $g\in G$ such that

$$(J_{i_1},\dots,J_{i_u})=(I_{i_1},\dots,I_{i_u})^g.$$

Then, since $g\in\mathrm{Aut}(\mathcal{R})$, we conclude that $(J_{i_1},\dots,J_{i_u})$ is an element of relation R_j in $\mathcal{R}_{\{J\}}$. We conclude that h is an isomorphism as required.

Now, since $\mathcal{R}$ is homogeneous, there exists $g\in G=\mathrm{Aut}(\mathcal{R})$ such that $g_{|\{I\}}=h$; in particular $I^g=J$, as required. □

Lemma 1.1.11. $\mathrm{SRC}(G,\Omega)\leq\mathrm{TRC}(G,\Omega)$.

Proof. Let $r=\mathrm{TRC}(G,\Omega)$. Define $\mathcal{R}=(\Omega,R_1,\dots,R_k)$, where $R_1,\dots,R_k$ are the orbits of G on Ω^i for all $i\in\{1,\dots,r\}$.

Clearly $G\leq\mathrm{Aut}(\mathcal{R})$. Suppose that $\sigma\in\mathrm{Aut}(\mathcal{R})$, and let $I=(\omega_1,\dots,\omega_t)$ be a t-tuple of distinct elements of Ω, where $t=|\Omega|$ (so every entry of Ω occurs as an entry in I). Then $I \underset{r}{\sim} I^\sigma$, and so there exists $g\in G$ such that $I^g=I^\sigma$. This implies that $\sigma=g$, and so $\mathrm{Aut}(\mathcal{R})\leq G$. We conclude that $G=\mathrm{Aut}(\mathcal{R})$.

We must show that $\mathcal{R}$ is homogeneous. Let Γ and Δ be subsets of Ω of size s such that there exists an isomorphism $\varphi:\mathcal{R}_\Gamma\to\mathcal{R}_\Delta$. Furthermore, let $I=(\gamma_1,\dots,\gamma_s)$ be an s-tuple of distinct elements of Γ. Suppose first $s\leq r$. Since $\mathcal{R}$ contains all the orbits of G on Ω^s and since $\mathcal{R}_\Gamma\cong\mathcal{R}_\Delta$, we deduce that I and $\varphi(I)$ are in the same G-orbit, that is, there exists $g\in G$ such that $I^g=\varphi(I)$. Thus $\varphi=g|_\Gamma$, as required. Suppose next $s>r$. Since all r-subtuples of I occur as relations in $\mathcal{R}$ and since $\mathcal{R}_\Gamma\cong\mathcal{R}_\Delta$, we conclude that $I \underset{r}{\sim} \varphi(I)$. Since $r=\mathrm{TRC}(G,\Omega)$, we deduce $I \underset{s}{\sim} \varphi(I)$. As before, this implies that there exists $g\in G=\mathrm{Aut}(\mathcal{R})$ such that $I^g=\varphi(I)$; in other words $\varphi=g|_\Gamma$, as required. □

Corollary 1.1.12. $\mathrm{SRC}(G,\Omega)=\mathrm{TRC}(G,\Omega)$.

In light of this corollary, we now drop the distinction between the two types of relational complexity:

Definition 1.1.13. The *relational complexity* of G is equal to the tuple relational complexity of G (and hence also equal to the structural relational complexity of G), and is denoted $\mathrm{RC}(G,\Omega)$.

In particular, a permutation group $G\leq\mathrm{Sym}(\Omega)$ is called *binary* if $\mathrm{RC}(G,\Omega)=2$.

Our definition of relational complexity has, to this point, pertained only to permutation groups, i.e. to *faithful* group actions. It is convenient to extend this definition now to any group action:

Definition 1.1.14. Suppose that a group G acts on a set Ω. The *relational complexity* of the action, denoted $\mathrm{RC}(G,\Omega)$, is the relational complexity of the permutation group induced by the action of G on Ω.

Note, finally, that in [26] the word *arity* is used as a synonym for relational complexity.

1.2 Basics: Some key examples

Our focus in this monograph is on actions with small relational complexity, thus the examples we present below are skewed in this direction. In particular, all of the actions listed in Conjecture 1.1 are discussed.

As we shall see, there are times when the structural definition of relational complexity is easiest to work with, and times when we prefer the tuple definition.

Before we outline the primary examples, we need to say a few words about the third family in Conjecture 1.1. This family consists of all groups isomorphic to an affine orthogonal group $V \rtimes \mathrm{O}(V)$ with V a vector space over a finite field equipped with a non-degenerate anisotropic quadratic form, acting on itself by translation, with complement the full orthogonal group $\mathrm{O}(V)$. It is a straightforward consequence of the classification of non-degenerate quadratic forms that if V admits an anisotropic quadratic form Q (i.e. one for which $Q(\mathbf{v}) \neq 0$ for all $\mathbf{v} \in V \setminus \{\mathbf{0}\}$)[3], then $\dim(V) \leq 2$. We will split this family into two smaller families according to whether $\dim(V)$ is 1 or 2;

3a. $\dim(V) = 1$: the associated group G is isomorphic to $\mathbb{F}_q \rtimes C_2$, where C_2 acts as -1 on the finite field $\mathbb{F}_q$ with q elements, and the action is on $\Omega = \mathbb{F}_q$. For G to be primitive we require that q is prime, and we obtain that G is isomorphic to the dihedral group of order $2q$, with the action being on the q-gon, as usual.

3b. $\dim(V) = 2$ and the associated quadratic form is of minus type: the associated group G is isomorphic to $\mathbb{F}_q^2 \rtimes \mathrm{O}_2^-(q) \cong \mathbb{F}_q^2 \rtimes D_{2(q+1)}$, where $D_{2(q+1)}$ is a dihedral group of order $2(q+1)$.

It is interesting to observe that, if we consider the relational complexity for infinite permutation groups, then this family gives rise to examples of infinite binary permutation groups. In Example 1.2.5, regardless of the dimension of V and regardless of the field of definition of V, we show that if Q is any anisotropic quadratic form over the vector space V, then the affine permutation group $V \rtimes \mathrm{O}(V)$ is binary in its action on V. The fact that $\dim V \leq 2$ for vector spaces over finite fields is therefore only accidental and due to the classification of quadratic forms. For instance, if the vector space V is over the real numbers $\mathbb{R}$ or over the rational numbers $\mathbb{Q}$, then $\dim V$ can be arbitrarily large. Indeed, for every $\ell \geq 1$, $x_1^2 + \cdots + x_\ell^2$ is an anisotropic quadratic form for $\mathbb{R}^\ell$ or $\mathbb{Q}^\ell$.

First, let us observe that the relational complexity of the natural action of the symmetric group is as small as it can possibly be.

Example 1.2.1. Consider the natural action of $G = \mathrm{Sym}(t)$ on the set $\Omega = \{1, \ldots, t\}$. Define

$$R = \{(i, j) \mid 1 \leq i, j \leq t \text{ and } i \neq j\}.$$

Then $\mathcal{R} = (\Omega, R)$ is the complete directed graph, $\mathcal{R}$ is homogeneous and $G = \mathrm{Aut}(\mathcal{R})$. We conclude immediately that $\mathrm{RC}(G, \Omega) = 2$.

Note that the first family of permutation groups listed in Conjecture 1.1 is precisely the family of finite symmetric groups in their natural action.

In many group-theoretic respects, the alternating group is very like the symmetric group. The next example shows that relational complexity does not conform to this rule-of-thumb: while, as we have just seen, the natural action of the symmetric group has relational complexity as small as it can possibly be, the natural action of the alternating group has relational complexity as large as it can possibly be.

Example 1.2.2. Consider the natural action of $G = \mathrm{Alt}(t)$ on the set $\Omega = \{1, \ldots, t\}$. Consider the tuples

$$I = (1, 2, 3, \ldots, t) \text{ and } J = (2, 1, 3, \ldots, t).$$

It is straightforward to check that $I \underset{t-2}{\sim} J$; it is equally clear that the only permutation h for which $I^h = J$ is $h = (1, 2) \notin G$. We conclude that $\mathrm{RC}(G, \Omega) \geq t - 1$. Now Example 1.1.6 implies that $\mathrm{RC}(G, \Omega) = t - 1$.

[3] It may be perhaps better to call such a Q a *non-singular form* rather than an anisotropic form – a vector $\mathbf{v}$ is generally called *singular* if $Q(\mathbf{v}) = 0$, and *isotropic* if $\beta(\mathbf{v}, \mathbf{v}) = 0$ where β is the polar form of Q. If the characteristic of the field is odd, these two definitions coincide, however in characteristic 2 this is not the case. Our definition of an anisotropic form requires that the only singular vector for Q is the zero vector, but note that all vectors are isotropic in the characteristic 2 case. In any case, we will stick to calling such a Q anisotropic as it is consistent with what has come before in the literature.

The previous two examples are a salutary warning that, in general, relational complexity behaves badly with respect to subgroups. All is not lost however: Lemma 1.7.2 shows that the relational complexity of a group is related to that of some of its subgroups.

Our first aim is to understand the actions listed in Conjecture 1.1. Note that the Families 2 and 3a (using the notation at the start of this section) consist of primitive actions with very small point-stabilizers (size 1 and 2, respectively). In the next couple of examples we consider this situation.

Example 1.2.3. If G acts regularly on Ω, then $\mathrm{RC}(G,\Omega)$ is binary.

Proof: Suppose that $I=(I_1,\dots,I_n)$ and $J=(J_1,\dots,J_n)$ satisfy $I \underset{2}{\sim} J$. For $i\in\{1,\dots,n-1\}$, let g_i be an element of G that satisfies $I_i^{g_i}=J_i$ and $I_{i+1}^{g_i}=J_{i+1}$. The regularity of G implies that, for $j\in\{1,\dots,n\}$, there is a unique element of G satisfying $I_j^g=J_j$. This fact, applied with $j=2$, implies that $g_1=g_2$; then applied with $j=3$, implies that $g_2=g_3$, and so on. Thus $g_1=\dots=g_{n-1}$; calling this element g, we see that $I^g=J$ and we conclude that $I \underset{n}{\sim} J$, as required. □

Recall that the only regular primitive actions are associated with cyclic groups of prime order; we see, then, that the second family of groups in Conjecture 1.1 are precisely the regular primitive groups.

Example 1.2.4. Suppose that G is transitive and a point-stabilizer H has size 2, and suppose that x is the non-trivial element in H. Let $C=x^G$ be the conjugacy class of x in G. Then

$$\mathrm{RC}(G)=\begin{cases}2, & \text{if } C\not\subseteq C^2;\\ 3, & \text{otherwise.}\end{cases}$$

Proof: It is an easy exercise to verify that, under these assumptions, $\mathrm{RC}(G)\le 3$. One can use, for instance, Lemma 1.5.1 below.

Since $\mathrm{RC}(G)\le 3$, it is clear that a pair of n-tuples will be n-subtuple complete if and only if they are 3-subtuple complete. Thus, if there exists an n-tuple that is 2-subtuple complete but not n-subtuple complete, then there must exist a 3-tuple that is 2-subtuple complete but not 3-subtuple complete.

Suppose that G is not binary, and let $(P,Q)=((P_1,P_2,P_3),(Q_1,Q_2,Q_3))$ be a pair of 3-tuples that is 2-subtuple complete but not 3-subtuple complete. Then there is, by assumption, an element g of G that maps (P_1,P_2) to (Q_1,Q_2). Replacing Q by $Q^{g^{-1}}$ and relabelling, we conclude that there exists a pair

$$((P_1,P_2,P_3),(P_1,P_2,P_4))$$

that is 2-subtuple complete but not 3-subtuple complete, in particular $P_3\neq P_4$. Write H_i for the stabilizer of P_i, and let x_i be the non-trivial element of H_i. Then we must have

$$P_3^{x_1}=P_3^{x_2}=P_4.$$

Since (P,Q) is not 3-subtuple complete, $x_1\neq x_2$, otherwise $P^{x_1}=Q$. Moreover, since $P_3^{x_1x_2}=P_3$, we conclude that x_1x_2 is the non-trivial element in H_3. Thus $C\subseteq C^2$, as required.

Suppose now that $C\subseteq C^2$. Let $x_1,x_2,x_3\in C$ with $x_3=x_1x_2$. In particular, there exist three points P_1,P_2 and P_3 with $G_{P_1}=\langle x_1\rangle$, $G_{P_2}=\langle x_2\rangle$ and $G_{P_3}=\langle x_3\rangle$. Set $P_4:=P_3^{x_1}$. We claim that $((P_1,P_2,P_3),(P_1,P_2,P_4))$ is a pair of 3-tuples that is 2-subtuple complete. In fact,

$$\begin{aligned}
&(P_1,P_2)^{1_G}=(P_1,P_2),\\
&(P_1,P_3)^{x_1}=(P_1^{x_1},P_3^{x_1})=(P_1,P_4),\\
&(P_2,P_3)^{x_2}=(P_2^{x_2},P_3^{x_2})=(P_2,P_3^{x_3x_2})=(P_2,P_3^{x_1})=(P_2,P_4).
\end{aligned}$$

If this pair is 3-subtuple complete, then there exists $g\in G$ with $P_1^g=P_1$, $P_2^g=P_2$ and $P_3^g=P_4$. In particular, $g\in\langle x_1\rangle\cap\langle x_2\rangle$. If $g=1$, then $P_3=P_4=P_3^{x_1}$ and hence $x_1\in\langle x_3\rangle$. This gives $x_1=x_3$ and hence $x_2=1$ because $x_1x_2=x_3$. However, this is a contradiction. Thus $g=x_1=x_2$ and hence $x_3=x_1x_2=1$, again a contradiction. Therefore, $((P_1,P_2,P_3),(P_1,P_2,P_4))$ is a pair of 3-tuples that are 2-subtuple complete but that are not 3-subtuple complete; hence G is not binary. □

There is an important special case which occurs when point-stabilizers are of size 2, and G has a regular normal subgroup N. In this case it follows immediately that $C \not\subseteq C^2$ (where C is as in Example 1.2.4), and thus $\mathrm{RC}(G, \Omega) = 2$. Such an action is primitive if and only if N is of prime order, and we now see that Family 3a pertaining to Conjecture 1.1 is precisely this.[4]

Our next example addresses Family 3b in Conjecture 1.1.

Example 1.2.5. This example is Lemma 1.1 of [21]. We identify Ω with a vector space V over a field F, such that V is endowed with a quadratic form Q such that Q is anisotropic, i.e. $Q(v) \neq 0$ for all $v \in V \setminus \{0\}$. We set $G = V \rtimes \mathrm{O}(V)$, where $\mathrm{O}(V)$ is the isometry group of the form Q, and the semidirect product is the natural one, as is the action of G on $\Omega = V$.

Let us see that this action is binary. Let n be a positive integer, and assume that $\mathbf{u} = (u_0, \dots, u_n)$ and $\mathbf{u}' = (u_0', \dots, u_n')$ satisfy $\mathbf{u} \underset{2}{\sim} \mathbf{u}'$. Let us show that $\mathbf{u} \underset{n+1}{\sim} \mathbf{u}'$. We may suppose, without loss of generality that $u_0 = u_0' = 0$.

Note that $\mathbf{u} \underset{2}{\sim} \mathbf{u}'$ implies that $Q(u_i) = Q(u_i')$ for all $i \in \{1, \dots, n\}$. What is more, since the isometry group also preserves the polar form β of Q, $\mathbf{u} \underset{2}{\sim} \mathbf{u}'$ also implies that

$$\beta(u_i, u_j) = \beta(u_i', u_j'),$$

for any $1 \leq i, j \leq n$. This, in turn, implies that

$$Q\left(\sum_{j=1}^{n} c_j u_j\right) = Q\left(\sum_{j=1}^{n} c_j u_j'\right), \tag{1.2.1}$$

for any choice of scalars $c_1, \dots, c_n \in F$.

Let $W = \mathrm{span}(\mathbf{u})$, and let $W' = \mathrm{span}(\mathbf{u}')$ and suppose, without loss of generality, that $u_1, \dots, u_m$ is a basis for W (for $m = \dim(W)$). We claim that then $u_1', \dots, u_m'$ is a basis for W'. To see this, it is enough to show that if $u_1, \dots, u_k$ are linearly independent, then so too are $u_1', \dots, u_k'$. Suppose that $c_1, \dots, c_k \in F$ such that $c_1 u_1' + \cdots + c_k u_k' = 0$. Then, clearly,

$$Q(c_1 u_1' + \cdots + c_k u_k') = Q(0) = 0.$$

But, by the observation above, this implies that $Q(c_1 u_1 + \cdots + c_k u_k) = 0$, which implies that $c_1 u_1 + \cdots + c_k u_k = 0$, which in turn implies that $c_1 = \cdots = c_k = 0$. The claim follows.

Now we can define an isometry $f : W \to W'$ by setting $f(u_i) = u_i'$ for $i \in \{1, \dots, m\}$, and extending linearly. Then Witt's Lemma implies that there exists $g \in \mathrm{O}(V)$ such that $u_i^g = u_i'$ for all $i \in \{1, \dots, m\}$.

[4] The problem of specifying relational complexity when point-stabilizers have size 2 is now reduced to the problem of studying when C, a certain conjugacy class of involutions, satisfies $C \subseteq C^2$. This problem is, in general, difficult, however one potential avenue of investigation is via the *class constants* of the finite group G, denoted a_{ijv}. For any conjugacy class C_i in a group G, we define $\hat{C}_i = \sum_{c \in C_i} c_i$ to be the class sum of C_i in the group algebra $\mathbb{C}G$. Now write

$$\hat{C}_i \hat{C}_j = \sum_{v=1}^{k} a_{ijv} \hat{C}_v,$$

where k is the number of conjugacy classes in G. The non-negative integers a_{ijv} for $1 \leq i, j, v \leq k$ are the *class constants* of G. Now a well-known formula asserts that

$$a_{ijv} = \frac{|C_i||C_j|}{|G|} \sum_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \frac{\chi(g_i)\chi(g_j)\chi(g_v^{-1})}{\chi(1)}.$$

We conclude, therefore, that if a point-stabilizer $H = \langle x \rangle$ has size 2, then $\mathrm{RC}(G) = 2$ if and only if

$$\sum_{\chi \in \mathrm{Irr}_{\mathbb{C}}(G)} \frac{\chi(x)^3}{\chi(1)} = 0.$$

Let us now consider $m < i \leq n$. Write $u_i = \sum_{j=1}^{m} c_j u_j$ and now, observe that (1.2.1) yields that

$$Q\left(u_i' - \sum_{j=1}^{m} c_j u_j'\right) = Q\left(u_i - \sum_{j=1}^{n} c_j u_j\right) = Q(0) = 0.$$

Now the fact that Q is anisotropic implies that $u_i' - \sum_{j=1}^{m} c_j u_j' = 0$, and we conclude that $u_i^g = u_i'$, as required.

All of the examples considered so far have been transitive. Let us briefly consider what can happen with intransitive actions.

Example 1.2.6. Suppose that the action of G on Ω is intransitive with orbits $\Delta_1, \ldots, \Delta_v$. It is immediate from the definition that

$$\mathrm{RC}(G, \Omega) \geq \max\{\mathrm{RC}(G, \Delta_1), \mathrm{RC}(G, \Delta_2), \ldots, \mathrm{RC}(G, \Delta_v)\}.$$

On the other hand, let $n \geq 3$ and consider the intransitive action of $G = \mathrm{Sym}(n)$ with two orbits, where the action on the first orbit is the natural one of degree n, and the second orbit is of size 2. Clearly the action of G on each orbit is binary; on the other hand, one can check directly that $\mathrm{RC}(G, \Omega) = n = t - 2$.

This example suggests that the problem of calculating the relational complexity of intransitive actions may be rather difficult.

1.2.1 Existing results on relational complexity

Results on relational complexity above and beyond the basic examples discussed above are hard to obtain. Nearly all of the important results are due to Cherlin, and his co-authors, and we briefly mention some of these here. The first result is stated in [20], with a small correction in [21].

Theorem 1.2.7. *Let Ω be the set of all k-subsets of the set $\{1, \ldots, n\}$ with $2k \leq n$. If $G = \mathrm{Sym}(n)$, then $\mathrm{RC}(G, \Omega) = 2 + \lfloor \log_2 k \rfloor$. If $G = \mathrm{Alt}(n)$, then*

$$\mathrm{RC}(G, \Omega) = \begin{cases} n-1, & \text{if } k = 1; \\ \max(n-2, 3), & \text{if } k = 2; \\ n-2, & \text{if } k \geq 3 \text{ and } n = 2k+2; \\ n-3, & \text{otherwise.} \end{cases}$$

The actions of the symmetric and alternating groups on partitions, rather than k-sets, are currently being studied by Cherlin and Wiscons [24]. The only general result to date is for $\mathrm{Sym}(2n)$ and $\mathrm{Alt}(2n)$ acting on Ω, the set of partitions of $2n$ into n blocks of size 2 (so, for $G = \mathrm{Sym}(2n)$, this is the action on cosets of a maximal imprimitive subgroup of form $\mathrm{Sym}(2) \operatorname{wr} \mathrm{Sym}(n)$). The result they have obtained for $n \geq 2$ is as follows:

$$\mathrm{RC}(\mathrm{Sym}(2n), \Omega) = n;$$

$$\mathrm{RC}(\mathrm{Alt}(2n), \Omega) = \begin{cases} 2, & n = 2; \\ 4, & n \in \{3, 4\}; \\ n, & n > 3 \text{ and } n \equiv 0, 1, 3, 5 \pmod 6; \\ n-1, & n > 4 \text{ and } n \equiv 2, 4 \pmod 6. \end{cases}$$

As we shall see below (Theorem 1.5.2), when considering large relational complexity, an important family of actions involves groups G which are subgroups of $\mathrm{Sym}(m) \operatorname{wr} \mathrm{Sym}(r)$ containing $(\mathrm{Alt}(m))^r$, 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 $t = \binom{m}{k}^r$. The particular situation where $G = \mathrm{Sym}(m) \operatorname{wr} \mathrm{Sym}(r)$ is studied in [26]. We summarise some of the results there, using the notation just established.

Theorem 1.2.8. *Let $G = \mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$ acting on a set Ω of size $t = \binom{m}{k}^r$, as described.*

1. *If $m = 2$, then $k = 1$ and $\mathrm{RC}(G, \Omega) = 2 + \lfloor \log_2 r \rfloor$.*
2. *If $k = 1$, then $\mathrm{RC}(G, \Omega) \leq m + \lfloor \log_2 r \rfloor$.*
3. *$\mathrm{RC}(G, \Omega) \leq \lfloor 2 + \log_2 k \rfloor \lfloor 1 + \log_2 r \rfloor$ with equality if $m \geq 2k \lfloor 1 + \log_2 r \rfloor$.*

The particular situation where $k = 1$ and $G = \mathrm{Sym}(m) \,\mathrm{wr}\, \mathrm{Sym}(r)$ (so we are considering the natural product action of degree m^r) has been taken much further in a series of papers by Saracino [89, 90, 91]. Saracino's results effectively yield an exact value for the relational complexity of this family of actions. We do not write this value here as the precise formulation of the results is slightly involved; instead we refer to [26, §6] and to the papers of Saracino, particularly the first.

1.3 Motivation: On homogeneity

In his paper [20], Cherlin chooses a quote from Aschbacher as an epigraph. This quote, plus some more, goes as follows:

> Define an object X in a category $\mathfrak{C}$ to possess the *Witt property* if, whenever Y and Z are subobjects of X and $\alpha : Y \to Z$ is an isomorphism, then α extends to an automorphism of X. Witt's Lemma says that orthogonal spaces, symplectic spaces, and unitary spaces have the Witt property in the category of spaces with forms and isometries. All objects in the category of sets and functions have the Witt property. But in most categories few objects have the Witt property; those that do are very well behaved indeed. If X is an object with the Witt property and G is its group of automorphisms, then the representation of G on X is usually an excellent tool for studying G. [3, pp. 81, 82]

One should think of "the Witt property" as a generalization of the notion of homogeneity which we have introduced in the specific setting of relational structures. The study of homogeneous objects in different categories has a long and interesting history.[5]

Before discussing this history, let us delve a little deeper into why such objects have received attention: Aschbacher's answer is given above. This approach has its roots in the *Erlangen Programme* of Klein, in which the key features of a particular "geometry" define, and are defined by, the group of automorphisms of said geometry. The idea here is that one studies the geometry in question, one deduces information about the geometry, which one then reinterprets as information about the associated group; one can use this information about the group to deduce further information about the geometry and so on. Thus the process of mathematical inquiry moves back-and-forth between geometrical study and algebraic (group theoretic).

The efficacy of this approach varies considerably – if an object has a very small automorphism group for instance, then group theory may provide very little insight. On the other hand, as Aschbacher suggests, this approach is most spectacularly successful when the object in question is homogeneous. Indeed the two examples which Aschbacher mentions clearly illustrate the success of this approach.

First, we note that the category of sets and functions have the Witt property. If we restrict ourselves to finite objects in this category, then the associated automorphism groups are the finite symmetric groups, $\mathrm{Sym}(n)$. Of course, all of the basic group-theoretical information about these groups is most naturally expressed in the language of their natural (homogeneous) action on a set of size n. This includes their conjugacy class structure (via cycle type), and their subgroup structure (via the O'Nan–Scott Theorem [2, 93]; see also [72]).

[5] There is some inconsistency in terminology across the literature – homogeneity as we have defined it here is sometimes called "ultra-homogeneity" while homogeneity refers to a strictly weaker property.

Second, in the category of spaces with forms, basic linear algebra asserts that objects associated with a zero form (i.e. naked vector spaces) have the Witt property; Witt's Lemma extends this to cover objects associated with either a non-degenerate quadratic or non-degenerate sesquilinear form. Again, restricting ourselves to finite such objects, we obtain the finite classical groups as the associated automorphism groups. As before, the basic group-theoretical properties of these groups are most naturally expressed in the language of their natural homogeneous action on the associated vector space. This includes their conjugacy class structure (via rational canonical form for $\mathrm{GL}_n(q)$, and the variants due to Wall for the other classical groups [103]), and their subgroup structure (via Aschbacher's Theorem [1]).

In light of all this, a natural question when studying some (permutation) group G is whether we can find an object in some category on which G acts homogeneously. Example 1.1.6 gives an easy answer to this: it turns out that there is always such an object in the category of relational structures. The bad news is that the object provided by Example 1.1.6 is little more than an encoding of the complete structure of the permutation group in terms of a relational structure – studying the structure $\mathcal{R}_G$ will hardly be easier than studying the original group and its associated action.

The investigation of relational complexity seeks to remedy this disappointing state of affairs: given a group G and an associated action, $\mathrm{RC}(G,\Omega)$ gives us an indication of the efficiency with which we can build a relational structure on which G can act homogeneously. From this point of view, an "efficient" representation of G acting homogeneously on a relational structure is one for which the arity of the structure is as small as possible.

There is an alternative way of viewing efficiency in this context where one is, instead, interested in using relational structures with as few relations as possible (but not necessarily worrying about the arity of the relations used). We will not pursue this point of view here, but we refer to [53] (for the primitive case) and to [22] (for the general case), for results that pertain to this approach.

1.3.1 Existing results on homogeneity

We briefly review some important results on homogeneity for particular finite relational structures.

The classification of homogeneous graphs was partially completed by Sheehan [96], and then completely by Gardiner [42]. Indeed, Gardiner's result applies to a wider class of graphs than those we would call homogeneous. This classification was then extended by Lachlan to homogeneous digraphs [61].

In order to state these results we need some terminology: a *digraph*, Γ, is an ordered pair $(V(\Gamma), E(\Gamma))$, where $V(\Gamma)$ is a non-empty set, and $E(\Gamma)$ is an irreflexive binary relation on that set. The digraph is *symmetric* (resp. *anti-symmetric*) if, whenever $(x,y)\in E(\Gamma)$, we have (y,x) in (resp. not in) $E(\Gamma)$. So a symmetric digraph is the object commonly called a *graph* in the literature.

If Γ and Δ are two digraphs, then we can construct two new digraphs with vertex set $V(\Gamma)\times V(\Delta)$:

1. in the *composition of* Γ *and* Δ, $\Gamma[\Delta]$, vertices (u_1,v_1) and (u_2,v_2) are connected if and only if $(u_1,u_2)\in E(\Gamma)$, or $u_1=u_2$ and $(v_1,v_2)\in E(\Delta)$;

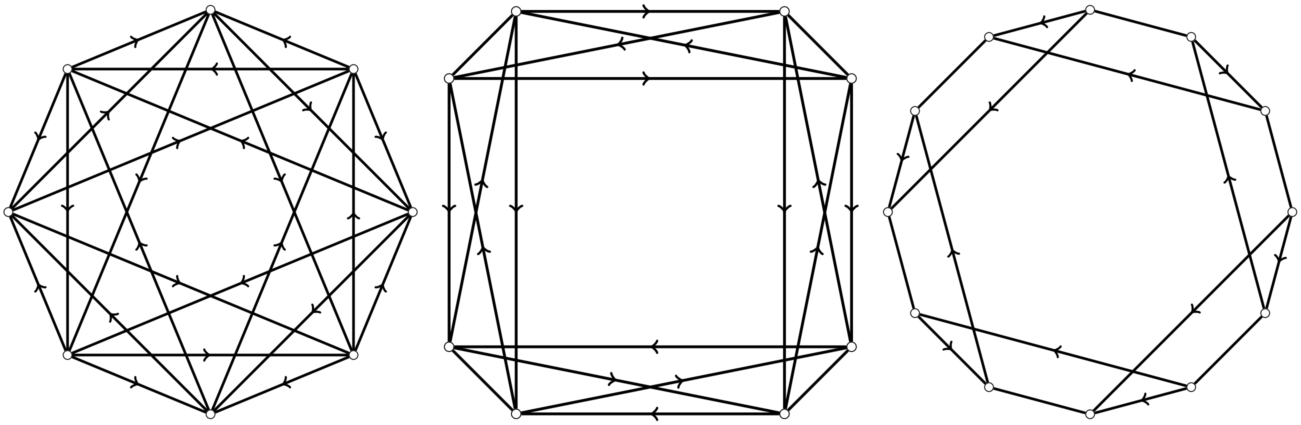
2. in the *direct product of* Γ *and* Δ, $\Gamma\times\Delta$ vertices (u_1,v_1) and (u_2,v_2) are connected if and only if $(u_1,u_2)\in E(\Gamma)$ and $(v_1,v_2)\in E(\Delta)$.

We write K_n for the complete (symmetric di)graph on n vertices. We also define two infinite families of graphs, both indexed by a parameter $n\in\mathbb{Z}$ with $n\geq 3$:

1. Λ_n is the digraph with vertex set $\{0,1,\dots,n-1\}$ and $(x,y)\in E(\Gamma_n)$ if and only if $x-y\equiv 1 \pmod n$;

2. Δ_n is the symmetric digraph with vertex set $\{0,1,\dots,n-1\}$ and $(x,y)\in E(\Delta_n)$ if and only if $x-y\equiv \pm 1 \pmod n$.

Thus Λ_n is the directed cycle on n vertices, and Δ_n is the undirected cycle on n vertices. Let $\mathcal{S}$ (resp. $\mathcal{A}$) denote the set of homogeneous symmetric (resp. antisymmetric) digraphs. We write $\overline{\Gamma}$ for the complement of Γ. Then Gardiner's result is the following:



(a) H_0 (b) H_1 (c) H_2

Figure 1.1: Three homogeneous digraphs. The presence of an undirected edge $\{v, w\}$ in the diagrams for H_0 and H_1 indicates that both directed edges between v and w are present. In the diagram for H_2 we have omitted most of the directed edges. To obtain the remaining edges, note first that each vertex in H_2 has a unique *mate*, to which it is connected by an undirected edge (indicated in the diagram). Next, let v and w be vertices, and let w' be the mate of w. Finally, if (v, w) is a directed edge, then (w', v) is a directed edge, and if (w, v) is a directed edge, then (v, w') is a directed edge. This leads to the insertion of another 36 directed edges.

Theorem 1.3.1. *A digraph Γ is in $\mathcal{S}$ if and only if Γ or $\overline{\Gamma}$ is isomorphic to one of*

$$\Delta_5,\ K_3 \times K_3,\ K_m[\overline{K_n}],$$

where $m, n \in \mathbb{Z}^+$.

Now we will state Lachlan's result in three stages. First we need to define three "sporadic homogeneous digraphs"; this is done in Figure 1.1.

Second we classify the homogeneous antisymmetric digraphs.

Theorem 1.3.2. *A digraph Γ is in $\mathcal{A}$ if and only if Γ is isomorphic to one of*

$$\Lambda_4,\ \overline{K_n},\ \overline{K_n}[\Lambda_3],\ \Lambda_3[\overline{K_n}],\ H_0,$$

where $n \in \mathbb{Z}^+$.

Finally we can state Lachlan's classification of homogeneous digraphs.

Theorem 1.3.3. *A digraph Γ is homogeneous if and only if Γ or $\overline{\Gamma}$ is isomorphic to a digraph with one of the following forms:*

$$K_n[A],\ A[K_n],\ S,\ \Lambda_3[S],\ S[\Lambda_3],\ H_1,\ H_2,$$

where $n \in \mathbb{Z}^+$, $A \in \mathcal{A}$ and $S \in \mathcal{S}$.

Lachlan's result, expressed in our terms, is *almost* a classification of those homogeneous relational structures $\mathcal{R} = (\Omega, R_1)$ such that R_1 is binary. We write "almost" because Lachlan imposes the condition that R_1 is irreflexive whereas we make no such restriction in our definition of a relational struture. Nonetheless, given that in this monograph we are focusing on transitive actions, Lachlan's result does yield the classification of homogeneous relational structures as we have defined them: any relational structure $\mathcal{R} = (\Omega, R_1)$ for which R_1 is binary and $\mathrm{Aut}(\mathcal{R})$ is transitive on Ω, will either be precisely of the form listed in Theorem 1.3.3, or else will be of the form listed in Theorem 1.3.3 with the addition of a loop at every vertex. We have made no attempt to extend this classification to the situation where $\mathrm{Aut}(\mathcal{R})$ is not transitive on Ω although we note that in this situation, $\mathrm{Aut}(\mathcal{R})$ would have exactly two orbits on Ω – one corresponding to vertices with loops, one corresponding to vertices without.

The groups $\mathrm{Aut}(\Gamma)$ for Γ appearing in Theorem 1.3.3 have not been explicitly listed to our knowledge. Notice that Theorem 1.3.3 refers to the set $\mathcal{S}$, which contains Δ_5, and $\mathcal{A}$, which contains Λ_4. It is easy to check that $\mathrm{Aut}(\Lambda_n)$ is the cyclic group of order n, $\mathrm{Aut}(\Delta_n)$ is the dihedral group of order $2n$ and $\mathrm{Aut}(K_n)$ is the symmetric group of degree n. It is slightly more involved to check the larger sporadic examples; the automorphism group and the action on points (which is necessarily binary) are as follows:

1. $\mathrm{Aut}(K_3 \times K_3) = \mathrm{Sym}(3) \,\mathrm{wr}\, \mathrm{Sym}(2)$ in the product action on 9 points;
2. $\mathrm{Aut}(H_0) \cong \mathrm{SL}_2(3)$ acting on the 8 cosets of a Sylow 3-subgroup;
3. $\mathrm{Aut}(H_1)$ is the semidihedral group of order 16 – it has presentation $\langle x, y | x^8 = y^2, x^y = x^3 \rangle$ – in an action of degree 8;
4. $\mathrm{Aut}(H_2) \cong \mathrm{Alt}(4) \rtimes C_4$ where $C_4 = \langle x \rangle$ acts by conjugation on $\mathrm{Alt}(4)$ via $g^x = g^{(1,2,3,4)}$ for all $g \in \mathrm{Alt}(4)$; as an abstract group $\mathrm{Aut}(H_2) \cong (\mathrm{Alt}(4) \times 2).2$, and the action is of degree 12.

In view of Theorem 1.3.3, to complete the list of the automorphism groups of homogeneous digraphs, we need to study the automorphisms of the various graphs arising from the composition of two others. (For instance, $\mathrm{Aut}(A[K_n])$ and $\mathrm{Aut}(K_n[A])$ for each $A \in \mathcal{A}$.) In all of these cases, the automorphism group is the wreath product of the automorphism groups of the two structures we are composing; this is because the languages of the structures being composed are taken to be disjoint.

There are a multitude of results that extend Gardiner, Sheehan and Lachlan's results to finite (di)graphs with automorphism groups that satisfy weaker properties than homogeneity. We particularly mention [48] which considers so-called *set-homogeneous* digraphs. In a different direction Cherlin has classified the homogeneous countable digraphs [25] extending work of Lachlan and Woodrow classifying the homogeneous countable graphs [64], and of Lachlan classifying the homogeneous countable tournaments [62].

Analogues for some of the given results exist for relational structures containing a single relation which may not be binary. Lachlan and Tripp have classified the homogeneous 3-hypergraphs [65] and Cameron has done the same for homogeneous k-hypergraphs with $k \geq 3$ [17, Theorem 5.1]; these results are analogues of Gardiner's result for relational structures with a single relation. Devillers has studied a rather similar problem in her work on homogeneous Steiner systems [37].

1.4 Motivation: On model theory

Cherlin's conjecture arises from model theory considerations rooted in Lachlan's theory of finite homogeneous relational structures (see, for instance, [60, 63]). We give a brief summary of some of the main ideas; the origin of nearly everything we consider here is [20].

Let us consider a family of theorems indexed by parameters k and ℓ, with $k, \ell \in \mathbb{Z}^+$ and $\ell \geq 2$. Theorem (k, ℓ) is a full classification of the homogeneous relational structures with at most ℓ relations, and with arity at most k. So, for instance, the first theorem we are likely to consider is Theorem $(2, 1)$ which (modulo the transitivity assumption we discussed above) is just Theorem 1.3.3, a result of Lachlan himself that classifies finite binary relational structures with one relation; in other words finite simple homogeneous directed graphs.

Lachlan's theory of finite homogeneous relational structures asserted a number of facts about the form of these theorems, and about the relationships between them. With regard to the form of the theorem, Lachlan's theory asserts that each theorem can be written as follows:

> "*A finite homogeneous relational structure of arity at most k with at most ℓ relations lies in one of a number of infinite families, or else is one of a finite number of sporadic individuals.*"

The power of this assertion is in the restrictions which Lachlan placed upon the definition of the word "family": a family of finite homogeneous relational structures in Lachlan's sense is an infinite collection of structures that can be constructed from a single infinite relational structure via a set of explicitly described operations.

With regard to the relationships between these theorems, Lachlan's theory gives us information about what the word "sporadic" means in these theorems. Specifically he asserts that any sporadic individual cropping up in Theorem (k, ℓ), say, will appear later as part of an infinite family in Theorem (k', ℓ') for some $k' \geq k$ and $\ell' \geq \ell$. Thus the "sporadic-ness" of a particular homogeneous relational structure is, in some sense, not genuine – rather, it is an artefact of restricting our investigations to particular values of k and ℓ.

The significance of all of this from a group-theoretic point of view lies in Cherlin's observation that every finite permutation group can be viewed as the automorphism group of a homogeneous relational structure – we demonstrated one way of seeing this in Example 1.1.6. This observation allows us to shift our point of view on the family of theorems studied by Lachlan: we can think of them as being about finite permutation groups.

In this setting the parameters k and ℓ can be seen as providing some kind of stratification on the universe of finite permutations groups, and Lachlan's results concerning "families" and "sporadic-ness" can be seen as statements about groups as well as structures. Finally, we can rewrite the theorems themselves from a group-theoretic point of view; they take the following form:

> "*Let G be the automorphism group of a homogeneous relational structure $\mathcal{R}$ on a set Ω of arity at most k with at most ℓ relations. Then, viewed as a permutation group on Ω, G lies in one of a number of infinite families, or else is one of a finite number of sporadic individuals.*"

With this set-up, any given permutation group G will occur in an infinite number of Theorems (k, ℓ). Typically, though, we are interested in the *first* such occurrence: we are interested in the pair (k, ℓ) for which k is minimal, and having fixed k as this minimal value, we then seek the minimum possible value of ℓ. The resulting pair (k, ℓ) is a measure of the *complexity* of G from the model-theoretic point of view or, using the point of view espoused in §1.3, gives a measure of the efficiency with which G can be represented as the automorphism group of a homogeneous relational structure.

Of course, plenty remains: we know that these theorems about finite permutation groups exist; we know their form, and we know something about the relationships that exist between them. We would like to know the statements of these theorems, and we would like to prove them!

As described in the previous section, this last task has only been completed for Theorem $(2, 1)$ (and, even then, with a small caveat). The main theorem of this monograph completes the task of ascertaining which groups appear as *primitive* permutation groups in any Theorem $(2, \ell)$.

1.5 Motivation: Other important statistics

It turns out that relational complexity is closely connected to a number of other permutation group statistics, some of which have received a great deal of attention in the literature. Our reference for the following definitions is [5].

For $\Lambda = \{\omega_1, \ldots, \omega_k\} \subseteq \Omega$ and for $G \leq \mathrm{Sym}(\Omega)$, we write $G_{(\Lambda)}$ or $G_{\omega_1, \omega_2, \ldots, \omega_k}$ for the point-wise stabilizer. If $G_{(\Lambda)} = \{1\}$, then we say that Λ is a *base*. The size of the smallest possible base is known as the *base size* of G and is denoted $\mathrm{b}(G)$.

We say that a base is a *minimal base* if no proper subset of it is a base. We denote the maximum size of a minimal base by $\mathrm{B}(G)$.

Given an ordered sequence of elements of Ω, $[\omega_1, \omega_2, \ldots, \omega_k]$, we can study the associated *stabilizer chain*:

$$G \geq G_{\omega_1} \geq G_{\omega_1, \omega_2} \geq G_{\omega_1, \omega_2, \omega_3} \geq \cdots \geq G_{\omega_1, \omega_2, \ldots, \omega_k}.$$

If all the inclusions given above are strict, then the stabilizer chain is called *irredundant*. If, furthermore, the group $G_{\omega_1,\omega_2,\dots,\omega_k}$ is trivial, then the sequence $[\omega_1,\omega_2,\dots,\omega_k]$ is called an *irredundant base*. The size of the longest possible irredundant base is denoted $\mathrm{I}(G)$.

Finally, let Λ be any subset of Ω. We say that Λ is an *independent set* if its point-wise stabilizer is not equal to the point-wise stabilizer of any proper subset of Λ. We define the *height* of G to be the maximum size of an independent set, and we denote this quantity by $\mathrm{H}(G)$.

Note that if G is a transitive permutation group on a set Ω, then $\mathrm{H}(G)=1$ if and only if G is regular; similarly, $\mathrm{H}(G)=2$ if and only if the stabilizer of a point is a non-trivial TI-subgroup of G. (Recall that X is said to be a non-trivial TI-subgroup of a group G if X is a proper subgroup of G and $X\cap X^g=1$, for every $g\in G\setminus N_G(X)$.)

There is a basic connection between the four statistics we have defined so far:

$$\mathrm{b}(G)\le \mathrm{B}(G)\le \mathrm{H}(G)\le \mathrm{I}(G)\le \mathrm{b}(G)\log t. \tag{1.5.1}$$

Recall that in this document, if the base is not specified, then "log" always means "log to the base 2"; recall, also, that $t=|\Omega|$. Let us see why (1.5.1) is true:

The first inequality is obvious. For the second, suppose that Λ is a minimal base; then Λ is an independent set. For the third, suppose that $\Lambda := \{\omega_1,\omega_2,\dots,\omega_k\}$ is an independent set and observe that

$$G > G_{\omega_1} > G_{\omega_1,\omega_2} > G_{\omega_1,\omega_2,\omega_3} > \cdots > G_{\omega_1,\omega_2,\dots,\omega_k}$$

is a strictly decreasing sequence of stabilizers. In particular, $[\omega_1,\omega_2,\dots,\omega_k]$ is irredundant and we may extend this irredundant sequence to an irredundant base. Hence $\mathrm{H}(G)\le\mathrm{I}(G)$.

The fourth inequality has been attributed to Blaha [7] who, in turn, describes it as an "observation of Babai" [4]. Suppose that G has a base of size $b=\mathrm{b}(G)$. Then, in particular $|G|\le t^b$. On the other hand, any irredundant base and any independent set have size at most $\log|G|$. We conclude that $\mathrm{I}(G)\le\log(t^b)$, and the result follows.

We are ready to connect relational complexity to the four statistics we have just defined. The key result is the following.

Lemma 1.5.1. $\mathrm{RC}(G)\le \mathrm{H}(G)+1$.

Proof. Let $h=H(G)$ and consider a pair $(I,J)\in\Omega^n$ such that $I \underset{h+1}{\sim} J$. We must show that $I \underset{n}{\sim} J$.

Observe that we can reorder the tuples without affecting their subtuple completeness. Hence, without loss of generality, we can assume that

$$G_{I_1} > G_{I_1,I_2} > \cdots > G_{I_1,I_2,\dots,I_\ell},$$

for some $\ell\le h$ and then this chain stabilizers, i.e.

$$G_{I_1,\dots,I_\ell} = G_{I_1,\dots,I_{\ell+j}},$$

for all $1\le j\le n-\ell$. From the assumption of h-subtuple completeness it follows that there exists an element $g\in G$ such that $I_i^g=J_i$ for all $1\le i\le \ell$ and observe that the set of all such elements g forms a coset of $G_{I_1,\dots,I_\ell}$.

The assumption of $(h+1)$-subtuple completeness implies, moreover, that for all $1\le j\le n-\ell$ there exists $g_j\in G$ such that

$$\begin{cases} I_i^{g_j} = J_i, & \text{for} \quad 1\le i\le \ell,\\ I_{\ell+j}^{g_j} = J_{\ell+j}. \end{cases}$$

The set of all such elements g_j forms a coset of $G_{I_1,\dots,I_\ell,I_{\ell+j}}$, which is, again, a coset of $G_{I_1,\dots,I_\ell}$. Since any coset of $G_{I_1,\dots,I_\ell}$ is defined by the image of the points $I_1,\dots,I_\ell$ under an element of the coset, we conclude that elements of the same coset of $G_{I_1,\dots,I_\ell}$ map $I_{\ell+j}$ to $J_{\ell+j}$ for all $1\le j\le n-\ell$. In particular, $I \underset{n}{\sim} J$, as required. ∎

Lemma 1.5.1 has been exploited in [44], where an upper bound on the height of a primitive permutation group is proved, from which the obvious upper bound on relational complexity is deduced. The main result on height is the following:

Theorem 1.5.2. *Let G be a finite primitive group of degree t. Then one of the following holds:*

1. *G is a subgroup of $\mathrm{Sym}(m)\mathrm{wr}\,\mathrm{Sym}(r)$ containing $(\mathrm{Alt}(m))^r$, 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 $t = \binom{m}{k}^r$;*

2. *$\mathrm{H}(G) < 9\log t$.*

Note that various members of the family listed at item (1) of Theorem 1.5.2 genuinely violate the bound at item (2): for example, when $r = k = 1$, we obtain the groups $\mathrm{Sym}(t)$ and $\mathrm{Alt}(t)$ in their natural action, for which the height is $t-1$ and $t-2$, respectively. In fact, though, we do not know the exact height of the groups listed at item (1) for all possible values of k, m and r.

The proof of Theorem 1.5.2 exploits the rich array of results in the literature giving bounds on $\mathrm{b}(G)$ for various families of permutation groups. In particular, use is made of the proof of the Cameron-Kantor conjecture [19] by Liebeck and Shalev [81], and of Cameron's follow-up conjecture giving a value for the associated constant [18] by many authors [11, 13, 14, 15]. These results mean that, in the almost simple case, work is only required for the so-called "standard actions".

Theorem 1.5.2 is an analogue of an existing result for $\mathrm{b}(G)$ [71]; now (1.5.1) and Lemma 1.5.1 yield analogues for $\mathrm{B}(G)$ and $\mathrm{RC}(G)$. With this result for $\mathrm{RC}(G)$, and with the proof of Conjecture 1.1, we now have a good handle on those permutation groups G for which $\mathrm{RC}(G)$ is either very large, or as small as possible. In the case where $\mathrm{RC}(G)$ is large, work remains to be done to ascertain the relational complexity of the groups listed at item (1) of the theorem; the most important results in this direction can be found in [26], and we summarised some of these above in Theorem 1.2.8.

The relationship between the various statistics occurring in (1.5.1), and between these statistics and $\mathrm{RC}(G)$ is an intriguing area of investigation, although not one that has hitherto received much attention. Cherlin and Wiscons have started to study some of these questions, and we mention two of their remarks [23]:

1. From computational evidence, it appears that $\mathrm{RC}(G)$ and $H(G)$ are "close" (say, $\mathrm{RC}(G) \geq \mathrm{H}(G)-3$). The obvious exceptions to this rule of thumb are the symmetric groups in their natural action; more generally, among primitive groups of degree at most 100, the only groups for which $\mathrm{RC}(G) < \mathrm{H}(G)-3$ are various members of the family listed at item (1) of Theorem 1.5.2.

2. Again, from computational evidence, more often than not, it appears that $\mathrm{B}(G)$ and $\mathrm{H}(G)$ coincide for primitive groups. Moreover, for all primitive groups of degree at most 100, $\mathrm{H}(G) - \mathrm{B}(G) \leq 3$.

We shy away from making conjectures about the general pattern for larger n but, still, these lines of inquiry seem promising.

1.6 Beyond the binary conjecture

In addition to the discussion above about possible future work, we briefly discuss two questions that naturally arise as follow-ups to the proof of Conjecture 1.1.

First, is it possible to generalize our classification of the finite binary primitive permutation groups to a classification of the finite binary transitive permutation groups?

The first thing to observe is that this extended classification will necessarily include all finite groups in their regular action (see Example 1.2.3). Perhaps, then, we should look first for some kind of intermediate extension that is not quite so general.

One interesting line of inquiry was suggested to us by Cherlin: Suppose that a finite group G acts on the set of cosets of a subgroup M and that this action is binary. We say that this action is *minimal binary* if, for every subgroup K with $M < K < G$, the action of G on the set of cosets of K is not binary. Since, as we have just observed, the regular action of G is binary, we know that every finite group G has a minimal binary action (and maybe more than one). Ideally we would like to be able to describe the minimal binary actions of an arbitrary finite group G but even this seems very challenging.

In the first instance one could ask about the minimal binary actions of the (non-abelian) simple groups. In this context Corollary 1.4 tells us that these actions will not be primitive. Is it possible that the regular action may be minimal binary in many cases? To prove this one would need to show that all of the non-regular transitive actions of a given simple group G are non-binary. Many of the techniques in this manuscript would be of potential aid in constructing such a proof.

We should emphasise however that, even were one able to completely describe the minimal binary actions of a large class of finite groups, it may be far from straightforward to extend this description to all binary actions of that class.

Our second question is this: can one prove a statement analogous to Conjecture 1.4 for groups with larger relational complexity? For now let us briefly discuss the case where G is a primitive permutation group on a set Ω with $\mathrm{RC}(G,\Omega) = 3$.

In this case it is not yet clear what to conjecture as there seem to be many more examples than in the binary case: for instance, Scott Hudson has proved in his thesis that if G is a simple group and M is a maximal subgroup of G that is dihedral, then $\mathrm{RC}(G,(G:M)) \leq 3$ [50]. This result implies the existence of infinite families of primitive ternary permutation groups with $G = \mathrm{PSL}_2(q)$ or $G = {}^2B_2(q)$.

A second setting where primitive ternary permutation groups turn up is for the group $\mathrm{A\Gamma L}_1(q)$ in the usual action on $q+1$ points; in this setting relational complexity is either 3 or 4, depending on q. The problem of proving exactly when $\mathrm{RC}(G,\Omega) = 3$, even for this specific family, is already difficult.

1.7 Methods: basic lemmas

Most of the results in this section were first written down in [34, 45, 46]. All of these papers were focused on showing that certain group actions are not binary, hence the lemmas we present here tend to yield lower bounds for relational complexity.

As always G is a group acting on a set Ω. In what follows, we will write $I, J \in \Omega^n$ to mean that $n \geq 2$ is a positive integer and I, J are elements of Ω^n; we will always assume that $I = (I_1, \ldots, I_n)$ and $J = (J_1, \ldots, J_n)$. As above, for an integer $k \leq n$, we will write $I \underset{k}{\sim} J$ to mean that the pair (I, J) is k-subtuple complete.

Note finally that, in addition to the methods described in this section and the two that follow, there is an extra methods section in Chapter **??**: it turns out that when we come to dealing with Aschbacher's $\mathcal{S}$-family of maximal subgroups of classical groups, some extra techniques are needed. These extra techniques, which may have application in a wider setting, are collected in §**??**.

1.7.1 Relational complexity and subgroups

Examples 1.2.1 and 1.2.2 serve as a warning that relational complexity can behave badly with respect to arbitrary subgroups of the group G. Nonetheless, something can still be said.

Lemma 1.7.1. *Let G be a transitive permutation group on Ω and let M be a point-stabilizer in this action. Let Λ be a non-trivial orbit of M. Then*

$$\mathrm{RC}(G,\Omega) \geq \mathrm{RC}(M,\Lambda).$$

Note, in particular, that if G is binary, then the action of M on all non-trivial suborbits must be binary. This will be useful later, particularly when we consider actions in which G is very large and M relatively small (for instance, $G = E_8(2)$, and $M = \mathrm{Aut}(\mathrm{PSU}_3(8))$), in which case it is sometimes possible to use `magma` to list all of the transitive binary actions of M.

Proof. Write α for an element of Ω stabilized by M. Let $r = \mathrm{RC}(M, \Lambda)$; then there exist $I, J \in \Lambda^n$ such that $I \underset{r-1}{\sim} J$ and $I \underset{n}{\not\sim} J$ with respect to the action of M on Λ. But now observe that if we define

$$I^* = (\alpha, I_1, \dots, I_n) \text{ and } J^* = (\alpha, J_1, \dots, J_n),$$

then $I^* \underset{r-1}{\sim} J$ and $I \underset{n+1}{\not\sim} J^*$, and the result follows. □

We write $(G : M)$ here, and below, to mean the set of right cosets of M in G.

Lemma 1.7.2. *Let $M < H < G$. Then* $\mathrm{RC}(G, (G : M)) \geq \mathrm{RC}(H, (H : M))$.

Proof. Write $r = \mathrm{RC}(H, (H : M))$, and observe that $\Lambda = (H : M)$ is a subset of $\Omega = (G : M)$. Then there exist $I, J \in \Lambda^n$ such that $I \underset{r-1}{\sim} J$ and $I \underset{n}{\not\sim} J$ with respect to the action of H.

We must show that $I \underset{r-1}{\sim} J$ and $I \underset{n}{\not\sim} J$ with respect to the action of G. That $I \underset{r-1}{\sim} J$ with respect to the action of G is immediate. Suppose that $I \underset{n}{\sim} J$ with respect to the action of G. Then there exists $g \in G$ such that $I_i^g = J_i$ for all $i \in \{1, \dots, n\}$. Since $I_i, J_i \in (H : M)$ for all $i \in \{1, \dots, n\}$, we must have $g \in H$. But then $I \underset{n}{\sim} J$ with respect to the action of H, which is a contradiction. □

The proofs of Lemmas 1.7.1 and 1.7.2 can be interpreted structurally: Both concern a group G that acts homogeneously on a relational structure $\mathcal{R}$ and transitively on its vertex set, with M the stabilizer of a vertex ω. Now in proving Lemma 1.7.1 we effectively show that, if Λ is a non-trivial orbit of M, then M acts homogeneously on a slight variant of the induced substructure on Λ. Similarly, in proving Lemma 1.7.2 we effectively show that, if $M < H < G$ and Γ is the block of imprimitivity ω^H, then H acts homogeneously on the induced substructure on Γ.

1.7.2 Relational complexity and subsets

For Λ a subset of Ω we write G_Λ for the *set-wise* stabilizer of Λ, and $G_{(\Lambda)}$ for the *point-wise* stabilizer of Λ. We write G^Λ for the permutation group induced on Λ by G_Λ; note that $G^\Lambda \cong G_\Lambda / G_{(\Lambda)}$.

In this section we present some results connecting $\mathrm{RC}(G, \Omega)$ with $\mathrm{RC}(G^\Lambda, \Lambda)$.

Definition 1.7.3. Let $t := |\Omega|$. For $k \in \mathbb{Z}^+$ with $k \geq 2$, we say that the action of G on Ω is *strongly non-k-ary* if there exist $I, J \in \Omega^t$ such that $I \underset{k}{\sim} J$, $I \underset{t}{\not\sim} J$, and all elements of I (resp. J) are distinct.

Note that this definition requires the existence of $I, J \in \Omega^t$ with $I \underset{k}{\sim} J$, $I \underset{t}{\not\sim} J$ and with every element of Ω occurring as an entry of I (and, therefore, also of J). If $k = 2$, then we tend to write *strongly non-binary* as a synonym for strongly non-k-ary.

The notion of a strongly non-k-ary set is connected to a classical notion in permutation group theory which was introduced by Wielandt [105].

Definition 1.7.4. Let $G \leq \mathrm{Sym}(\Omega)$ and let $k \in \mathbb{Z}^+$. The k-closure of G is the set

$$G^{(k)} = \{\sigma \in \mathrm{Sym}(\Omega) \mid \forall I \in \Omega^k, \text{ there exists } g \in G, I^g = I^\sigma\}.$$

We say that G is *k-closed* if $G = G^{(k)}$.

Observe that $G^{(k)}$ is the largest subgroup of $\mathrm{Sym}(\Omega)$ that has the same orbits on the set of k-tuples of Ω as G. Now the connection with strongly non-k-ary sets is as follows.

Lemma 1.7.5. *The group G is strongly non-k-ary if and only if G is not k-closed.*

Proof. Write $\Omega := \{\omega_1, \dots, \omega_t\}$. If G is not k-closed, then there exists $\sigma \in G^{(k)} \setminus G$. Now, it is easy to verify that $I := (\omega_1, \dots, \omega_t)$ and $J := I^\sigma = (\omega_1^\sigma, \dots, \omega_t^\sigma)$ are k-subtuple complete (because $\sigma \in G^{(k)}$) and are not t-subtuple complete (because $\sigma \notin G$). Thus $I \underset{k}{\sim} J$ and $I \underset{t}{\not\sim} J$, and we conclude that the action of G on Ω is strongly non-k-ary. The converse is similar. □

The most important example, for us, of a permutation group that is not k-closed is as follows.

Example 1.7.6. Let G be a k-transitive permutation group on Ω, for some integer $k \geq 2$. The definition implies that $G^{(k)} = \mathrm{Sym}(\Omega)$.

We immediately conclude that $\mathrm{Alt}(\Omega)$ is not $(t-2)$-closed, and we obtain (again) that $\mathrm{RC}(\mathrm{Alt}(\Omega), \Omega) \geq t-1$.

Recall that the Classification of Finite Simple Groups implies that examples of k-transitive permutation groups that do not contain $\mathrm{Alt}(\Omega)$ only exist for $k \leq 5$. What is more, all such groups are classified for $k \geq 2$ (see, for instance [38, §7.7]).

The next lemma shows how we will use the notion of a strongly non-k-ary permutation group in what follows.

Lemma 1.7.7. *Let $\Lambda \subseteq \Omega$. If G^Λ is strongly non-k-ary, then* $\mathrm{RC}(G, \Omega) > k$.

Proof. Suppose that $|\Lambda| = \ell$, and let I, J be ℓ-tuples of distinct elements of Λ such that $I \underset{k}{\sim} J$ and $I \underset{\ell}{\not\sim} J$ with respect to the action of G^Λ. It is enough to show that $I \underset{k}{\sim} J$ and $I \underset{\ell}{\not\sim} J$ with respect to the action of G. It is immediate that $I \underset{k}{\sim} J$ with respect to the action of G. On the other hand, if $I \underset{\ell}{\sim} J$, then there exists $g \in G$ such that $I^g = J$. Since I contains all elements of Λ, we conclude that $g \in G_\Lambda$ which contradicts the fact that $I \underset{\ell}{\not\sim} J$ with respect to the action of G^Λ. □

1.7.3 Strongly non-binary subsets

Our final few results apply specifically to the study of binary actions. As usual G acts on a set Ω, and we refer to a subset $\Lambda \subseteq \Omega$ as *strongly non-binary* if G^Λ is strongly non-binary.

The next lemma details our first example of such a subset. This example was first described in [46]; its key properties are a consequence of Example 1.7.6 and Lemma 1.7.7.

Lemma 1.7.8. Suppose that there exists a subset $\Lambda \subseteq \Omega$ such that $|\Lambda| \geq 2$ and G^Λ is a 2-transitive proper subgroup of $\mathrm{Sym}(\Lambda)$. Then G^Λ is strongly non-binary and the action of G on Ω is not binary.

In subsequent chapters, our focus is on proving that certain actions are not binary. Lemma 1.7.8 means that we will be interested in finding subsets which have 2-transitive set-wise stabilizers. The next lemma requires no proof, but we include it as it clarifies when such subsets exist.

Lemma 1.7.9. *Let K be some 2-transitive group, and let K_0 be a point-stabilizer in K. Let H be a subgroup of G and suppose that $\varphi : H \to K$ is a surjective homomorphism. Let M be the stabilizer in G of a point $\omega \in \Omega$ and let C be the core of $H \cap M$ in H. If $\mathrm{Ker}(\varphi) = C$ and $\varphi(H \cap M) = K_0$, then H acts 2-transitively on the orbit ω^H.*

The next lemma is a useful tool in finding subsets on which a set-stabilizer acts 2-transitively (recall that, when $r \geq 2$, the affine special linear group $\mathrm{ASL}_r(q)$ is 2-transitive in its natural action on q^r points).

Lemma 1.7.10. *Let G be a finite group acting transitively on a set Ω with point-stabilizer M, and suppose that the following two conditions hold:*

(i) *M has a subgroup $A \cong \mathrm{SL}_r(q)$, where $r \geq 2$, and*

(ii) *G has a subgroup S that is a central quotient of $\mathrm{SL}_{r+1}(q)$, such that $A \leq S$ (the natural completely reducible embedding) and $S \not\leq M$.*

Then there is a subset Δ of Ω such that $|\Delta| = q^r$ and $G^\Delta \geq \mathrm{ASL}_r(q)$.

Proof. We have $A \leq S \cap M < S$. Since A is embedded in S via the natural completely reducible embedding, we have $S \cap M \leq P_i(S)$ with $i \in \{1, r\}$, where $P_i(S)$ is a maximal parabolic subgroup of S stabilizing a 1-dimensional or an r-dimensional subspace. Say $i = 1$ (the case $i = r$ is entirely similar). Then writing matrices with respect to a suitable basis,

$$S \cap M \leq P_1(S) = \left\{ \begin{pmatrix} Y & v \\ 0 & \lambda \end{pmatrix} \mid Y \in \mathrm{GL}_r(q), v \in \mathbb{F}_q^r, \det(Y)\lambda = 1 \right\},$$

where A is the subgroup obtained by setting $\lambda = 1$, $\det(Y) = 1$ and $v = 0$. Define

$$U = \left\{ \begin{pmatrix} I & 0 \\ a & 1 \end{pmatrix} \mid a \in \mathbb{F}_q^r \right\},$$

and set $\Delta = \{Mu : u \in U\} \subseteq \Omega$ (where we identify Ω with the set $(G : M)$ of right cosets of M in G).

Since $M \cap U = 1$, the cosets $Mu\,(u \in U)$ are all distinct, and so $|\Delta| = q^r$. Since A normalizes U and $A \leq M$, the subgroup $UA \cong q^r.\mathrm{SL}_r(q)$ stabilizes Δ, and since $UA \cap M = A$, we have $(UA)^\Delta = \mathrm{ASL}_r(q) \leq G^\Delta$. □

It turns out that in the context of almost simple groups, it is convenient to use a variant of Lemma 1.7.8 where we don't just seek proper 2-transitive subgroups of $\mathrm{Sym}(\Omega)$, but also exclude $\mathrm{Alt}(\Omega)$ from our consideration. To that end we include the following definition which first appeared in [46].

Definition 1.7.11. A subset $\Lambda \subseteq \Omega$ is a *G-beautiful subset* if G^Λ is a 2-transitive subgroup of $\mathrm{Sym}(\Lambda)$ that is isomorphic to neither $\mathrm{Alt}(\Lambda)$ nor $\mathrm{Sym}(\Lambda)$.

Observe that a beautiful subset of Ω is a strongly non-binary subset. The reason for the stronger definition (that is, the reason why $\mathrm{Alt}(\Lambda)$ is excluded in the definition) is explained by the following result.

Lemma 1.7.12. *Suppose that G is almost simple with socle S. If Ω contains an S-beautiful subset, then G is not binary.*

Proof. Let Λ be an S-beautiful subset and observe that Λ has cardinality at least 5. Then, since S is normal in G, the group $(S_\Lambda G_{(\Lambda)})/G_{(\Lambda)}$ is a normal subgroup of $G_\Lambda/G_{(\Lambda)}$. This implies that $G_\Lambda/G_{(\Lambda)}$ is (isomorphic to) a 2-transitive proper subgroup of $\mathrm{Sym}(\Lambda)$. Then Lemma 1.7.8 implies that G is not binary. □

In what follows, if the group G is clear from the context, we will speak of a beautiful subset rather than a G-beautiful subset of Ω.

Although in this paper we do not need to deal with $\mathcal{C}_1$-actions for classical groups since they were dealt with in [46], we include the next lemma because it clearly illustrates the beautiful subsets method. The lemma has the added advantage of giving the reader an idea of how to deal with $\mathcal{C}_1$-actions in general. (These actions all yield to the method of beautiful subsets provided n and q are not too small.)

Lemma 1.7.13. *Let $S = \mathrm{PSL}_n(q)$ and for $n = 2$ assume $q > 5$. Let M be a maximal parabolic subgroup of S, and let Ω be the set of right cosets of M. Then Ω contains an S-beautiful subset.*

Proof. Here M is the stabilizer of a subspace W of V, where V is the natural n-dimensional module for $\mathrm{SL}_n(q)$. Since the action of S on the k-dimensional subspaces of V is permutation isomorphic to the action on the $(n-k)$-subspaces of V, we may assume that $\dim(W) \leq n/2$.

If $\dim(W) = 1$, then the action of S on Ω is 2-transitive. Now Ω itself is an S-beautiful subset, because we are assuming $q > 5$ when $n = 2$.

Suppose next that $\dim(W) > 1$. Observe that this implies that $n \geq 4$. Let W' be a subspace of W with $\dim(W') = \dim(W) - 1$ and consider $\Lambda = \{W'' \leq V \mid W' \subset W'', \dim(W'') = \dim(W)\}$. Clearly, $S_\Lambda = \mathrm{Stab}_S(W')$ and the action of S^Λ on Λ is permutation isomorphic to the natural 2-transitive action of $\mathrm{GL}(V/W')$ on the 1-dimensional subspaces of V/W'. Since $\dim(V/W') \geq 3$, the action of $\mathrm{GL}(V/W')$ induces neither the alternating nor the symmetric group on the set $P_1(V/W')$ of 1-dimensional subspaces of V/W'; therefore Λ is a beautiful subset. □

Our second example of a strongly non-binary subset is taken from [45, Example 2.2]. Here and below we use the phrase "non-binary witness" for a group G acting on a set Ω to refer to a pair (I, J) where $I, J \in \Omega^\ell$, for some $\ell \geq 3$, and $I \underset{2}{\sim} J$ but $I \underset{\ell}{\not\sim} J$.

Example 1.7.14. Let G be a subgroup of $\mathrm{Sym}(\Omega)$, let $g_1, g_2, \ldots, g_r$ be elements of G, and let $\tau, \eta_1, \ldots, \eta_r$ be elements of $\mathrm{Sym}(\Omega)$ with

$$g_1 = \tau\eta_1, \; g_2 = \tau\eta_2, \; \ldots, \; g_r = \tau\eta_r.$$

Suppose that, for every $i \in \{1, \ldots, r\}$, the support of τ is disjoint from the support of η_i; moreover, suppose that, for each $\omega \in \Omega$, there exists $i \in \{1, \ldots, r\}$ (which may depend upon ω) with $\omega^{\eta_i} = \omega$. Suppose, in addition, $\tau \notin G$. Now, writing $\Omega = \{\omega_1, \ldots, \omega_t\}$, observe that

$$((\omega_1, \omega_2, \ldots, \omega_t), (\omega_1^\tau, \omega_2^\tau, \ldots, \omega_t^\tau))$$

is a non-binary witness. Thus the action of G on Ω is strongly non-binary.

The next two lemmas which are taken from [34] are based on Example 1.7.14. In both cases, the given assumptions on the permutation group G are enough to conclude that a strongly non-binary subset of the type described in Example 1.7.14 must exist. In both lemmas, given a permutation or a permutation group X on Ω, we let $\mathrm{Fix}_\Omega(X)$ define the subset of Ω fixed point-wise by X; if Ω is clear from the context, we drop the label Ω.

Lemma 1.7.15 ([34, Lemma 2.5])**.** *Let G be a transitive permutation group on Ω, let $\alpha \in \Omega$ and let p be a prime with p dividing both $|\Omega|$ and $|G_\alpha|$ and with p^2 not dividing $|G_\alpha|$. Suppose that G contains an elementary abelian p-subgroup $V = \langle g, h\rangle$ with $g \in G_\alpha$, with $\langle h\rangle$ and $\langle gh\rangle$ conjugate to $\langle g\rangle$ via G. Then G is not binary.*

In [34, Lemma 2.5], the hypothesis actually requires that h and gh are conjugate to g via G; however the same proof yields the conclusion that G is not binary under the weaker assumption that $\langle h\rangle$ and $\langle gh\rangle$ are conjugate to $\langle g\rangle$ in G, as stated in the lemma. We will need this strengthening in what follows.

Lemma 1.7.16 ([34, Lemma 2.6])**.** *Let G be a permutation group on Ω and suppose that g and h are G-conjugate elements of prime order p, and gh^{-1} is conjugate to g (and so to h). Suppose that $V = \langle g, h\rangle$ is elementary abelian of order p^2. Suppose, finally, that G does not contain any elements of order p that fix more points of Ω than g. If $|\mathrm{Fix}(V)| < |\mathrm{Fix}(g)|$, then G is not binary.*

1.8 Methods: Frobenius groups

It turns out that the presence of Frobenius groups can be a powerful tool in proving that certain actions are not binary. We give three lemmas in this direction; the first was proved independently by Wiscons and, as it is notably short and elegant, we give his proof here.

Lemma 1.8.1. *Let G be a Frobenius permutation group on Ω (that is, G acts transitively on Ω, $G_\omega \neq 1$ for every $\omega \in \Omega$ and $G_{\omega\omega'} = 1$ for every $\omega, \omega' \in \Omega$ with $\omega \neq \omega'$). If G is binary, then a Frobenius complement has order equal to 2.*

Proof. For distinct $a, b, c \in \Omega$, the fact that G is binary implies that the intersection of the suborbits cG_a and cG_b is equal to $cG_{a,b}$, so as the action is Frobenius, $(cG_a) \cap (cG_b) = \{c\}$. Also, using again that the action is Frobenius, $|cG_a| = |G_a| = |G_b| = |cG_b|$. This shows that $\bigcup_{a\neq c}(cG_a \setminus \{c\})$ is a disjoint union of sets of constant size $|G_a| - 1$. So, letting $N = |\Omega|$, we find that $N - 1 = |\Omega \setminus \{c\}| \geq (N-1)(|G_a| - 1)$, implying that $|G_a| = 2$. □

Lemma 1.8.2. *Let $F \lhd G \leq \mathrm{Sym}(\Omega)$ with F having an orbit $\Lambda \subseteq \Omega$ on which it acts as a Frobenius group. (As usual, F^Λ is the permutation group induced by the action of F on Λ.) Write $F^\Lambda = T \rtimes C$, where T is the Frobenius kernel, and C is a Frobenius complement. If T is cyclic, and C contains an element x of order strictly greater than 2, then G is not binary.*

Proof. Let $\alpha \in \Lambda$. Since Λ is a block of imprimitivity for G, the group G_α must preserve Λ set-wise. Observe that G_Λ normalizes F, because $F \trianglelefteq G$. In particular, $F^\Lambda \trianglelefteq G^\Lambda$. Since the non-identity elements of T are precisely those elements of F^Λ that are fixed-point-free, G^Λ also normalizes T. Thus T is a regular normal subgroup of G^Λ. As T acts regularly on Λ, from the Frattini argument we obtain $G^\Lambda = T \rtimes G_\alpha^\Lambda$.

We can, therefore, identify T with Λ in such a way that the action of G_α^Λ on Λ is permutation isomorphic to the conjugation-action of G_α^Λ on T. To see this, define

$$\begin{aligned}\theta :& T \to \Lambda\\ & y \mapsto \alpha^y,\end{aligned}$$

and observe that, for $y \in T$ and $g \in G_\alpha$,

$$\theta(y^g) = \alpha^{(y^g)} = \alpha^{g^{-1}yg} = \alpha^{yg} = (\alpha^y)^g = (\theta(y))^g.$$

With this set-up, we write $n = |T|$ and we let y be a generator of T. We will construct (for the action of G) a 2-subtuple complete pair of the form

$$\Big((1, y, y^a),\ (1, y, y^b)\Big). \tag{1.8.1}$$

We must choose a and b appropriately. Let $x \in C$ having order strictly greater than 2. First, let $k \in \mathbb{Z}^+$ be such that $y^x = y^k$; note that $\gcd(k, n) = 1$, and so k is invertible modulo n. Then we set $a = \frac{1+k}{k} \in \mathbb{Z}_n$ and set $b = 1 + k$. Now observe that

$$\begin{aligned}(1, y)^{\mathrm{id}} &= (1, y);\\ (1, y^a)^x &= (1, y^{(k+1)/k})^x = (1, y^{k+1}) = (1, y^b);\\ (y, y^a)^{y^{-1}x^2y} &= (y, y^{(k+1)/k})^{y^{-1}x^2y} = (1, y^{1/k})^{x^2t} = (1, y^k)^y = (y, y^{k+1}) = (y, y^b).\end{aligned}$$

We see immediately that the pair (1.8.1) is 2-subtuple complete.

Note on the other hand that, provided $a \neq b$, this pair cannot be 3-subtuple complete: suppose that an element $g \in G$ sends the first triple in (1.8.1) to the second. Then g fixes 1 and, as we saw above, this means that the action of g on Λ is isomorphic to the action of g by conjugation on T. Since $y^g = y$, we conclude that, if $(y^a)^g = y^b$, then we must have $a = b$ modulo n. But now observe that

$$a = b \iff \frac{1+k}{k} = 1 + k \iff k^2 = 1.$$

Since we chose x to have order strictly greater than 2, we see that $k^2 \neq 1$, and we conclude that (1.8.1) is a pair which is 2-subtuple complete but not 3-subtuple complete. The result follows. ☐

Lemma 1.8.3. *Let $F = T \rtimes C \leq G \leq \mathrm{Sym}(\Omega)$ with C acting by conjugation fixed-point-freely on T. Suppose there exists $\alpha \in \Omega$ such that $F_\alpha = C$, and let Λ be the orbit of α under F. Define*

$$m := \min\{|G_{\gamma_1,\gamma_2}| \mid \gamma_1, \gamma_2 \text{ distinct elements of } \Lambda\}.$$

If $\left\lceil \frac{(|C|-1)(|C|-2)}{|\Lambda|-2} \right\rceil \geq m$, then G is not binary. In particular, if $|G : F| \leq \left\lceil \frac{(|C|-1)(|C|-2)}{|\Lambda|-2} \right\rceil$, then G is not binary.

Proof. Observe that F acts as a Frobenius group on Λ, where T is the Frobenius kernel, and C is a Frobenius complement. It is useful to observe that the regularity of T on Λ implies that, for every $c \in C$ and for every $\beta \in \Lambda$, there exists a unique $x \in T$ such that $\beta^{xc} = \beta$.

We study triples of the form

$$\Big((\alpha, \beta, \gamma),\ (\alpha, \beta, \delta)\Big), \tag{1.8.2}$$

for $\alpha,\beta,\gamma,\delta\in\Lambda$. We make the following claim:

Claim: for any distinct pair of elements (α,β), there are at least $(|C|-1)(|C|-2)$ choices for (γ,δ) such that the set $\{\alpha,\beta,\gamma,\delta\}$ has size 4, and the pair (1.8.2) is 2-subtuple complete.

Proof of claim: First we consider the set of pairs of distinct non-trivial elements in C, i.e.

$$C^{(2)} := \{(c_1,c_2)\mid c_1,c_2\in C\backslash\{1\}, c_1\neq c_2\}.$$

Now we construct a function $\phi: C^{(2)}\to\Omega^2$ as follows. For $(c_1,c_2)\in C^{(2)}$, we let t_1 be the unique non-trivial element of T such that $t_1c_1\in G_\beta$. Now, since $c_1\neq c_2$, we can define γ to be the unique point in Λ fixed by $t_1c_1c_2^{-1}$. Observe that γ is distinct from both α and β.

Next, we see that

$$\gamma^{t_1c_1c_2^{-1}}=\gamma\Longleftrightarrow\gamma^{t_1c_1}=\gamma^{c_2}.$$

We define $\delta:=\gamma^{c_2}$, and we set $\phi(c_1,c_2)=(\gamma,\delta)$. An easy argument shows that δ is distinct from all of α,β and γ. Furthermore we claim that, with these definitions the pair (1.8.2) is 2-subtuple complete. Indeed, observe that

$$(\alpha,\beta)^1=(\alpha,\beta),\ (\alpha,\gamma)^{c_2}=(\alpha,\delta)\text{ and }(\beta,\gamma)^{t_1c_1}=(\beta,\delta).$$

Thus every element (γ,δ) in the image of ϕ gives rise to a 2-subtuple complete pair as in (1.8.2). Since the domain of ϕ, $C^{(2)}$ has order $(|C|-1)(|C|-2)$, the claim will follow if we prove that ϕ is one-to-one.

Suppose, then, that $\phi(c_1,c_2)=(\gamma,\delta)=\phi(c_1',c_2')$. Let t_1 (resp. t_1') be the unique element of T such that t_1c_1 (resp. $t_1'c_1'$) is in G_β. Then $t_1c_1c_2^{-1}$ and $t_1'c_1'(c_2')^{-1}$ fix γ. What is more $\gamma^{c_2}=\gamma^{c_2'}=\delta$ and so $c_2'c_2^{-1}$ fixes γ. However $c_2,c_2'\in C=F_\alpha$ and so $c_2'c_2^{-1}$ fixes two points of Λ. We conclude that $c_2=c_2'$. But now, write $h_1:=t_1c_1$ and $h_1':=t_1'c_1'$; observe that $h_1,h_1'\in G_\beta$ and $\gamma^{h_1}=\gamma^{h_1'}$. As before we conclude that $h_1'h_1^{-1}$ fixes β and γ, and so $h_1=h_1'$. Then $t_1c_1=t_1'c_1'$ and so $t_1^{-1}t_1'=c_1'c_1^{-1}$; since $T\cap C=\{1\}$, this gives $c_1=c_1'$, as required.

The claim and the pigeon-hole principle imply that there exists some $\gamma\in\Lambda\setminus\{\alpha,\beta\}$ for which there are $k:=\left\lceil\frac{(|C|-1)(|C|-2)}{|\Lambda|-2}\right\rceil$ choices for δ such that all pairs of the form (1.8.2) are 2-subtuple complete; call these elements $\delta_1,\dots,\delta_k$. If G is binary, then all of these pairs are 3-subtuple complete and we conclude that the set $\{\gamma,\delta_1,\dots,\delta_k\}$ is a subset of an orbit of $G_{\alpha,\beta}$. But this is only possible if $k+1\leq m$, and the result follows. □

1.9 Methods: On computation

We will use `magma` very frequently in what follows to verify that certain actions are not binary. The methods we use to do this are largely drawn from [34]. We give a brief summary of some of the key methods here. In what follows G acts transitively on the set Ω, and M is the stabilizer of a point.

Test 1: Using the permutation character. Given $\ell\in\mathbb{N}\setminus\{0\}$, we denote by $\Omega^{(\ell)}$ the subset of the Cartesian product Ω^ℓ consisting of the ℓ-tuples $(\omega_1,\dots,\omega_\ell)$ with $\omega_i\neq\omega_j$, for every two distinct elements $i,j\in\{1,\dots,\ell\}$. We denote by $r_\ell(G)$ the number of orbits of G on $\Omega^{(\ell)}$. The next result is Lemma 2.7 of [34].

Lemma 1.9.1. *If G is transitive and binary, then $r_\ell(G)\leq r_2(G)^{\ell(\ell-1)/2}$ for each $\ell\in\mathbb{N}$.*

Let $\pi: G\to\mathbb{N}$ be the permutation character of G, that is, $\pi(g)=\mathrm{fix}_\Omega(g)$ where $\mathrm{fix}_\Omega(g)$ is the cardinality of the fixed point set $\mathrm{Fix}_\Omega(g):=\{\omega\in\Omega\mid\omega^g=\omega\}$ of g. From the Orbit Counting Lemma, we have

$$\begin{aligned} r_\ell(G) &= \frac{1}{|G|}\sum_{g\in G}\mathrm{fix}_\Omega(g)(\mathrm{fix}_\Omega(g)-1)\cdots(\mathrm{fix}_\Omega-(\ell-1))\\ &= \langle\pi(\pi-1)\cdots(\pi-(\ell-1)),1\rangle_G,\end{aligned}$$

where 1 is the principal character of G and $\langle\cdot,\cdot\rangle_G$ is the natural Hermitian product on the space of $\mathbb{C}$-class functions of G.

Clearly whenever the permutation character of G is available in `magma`, we can directly check the inequality in Lemma 1.9.1, and this is often enough to confirm that a particular action is not binary.

Test 2: using Lemma 1.7.5. By connecting the notion of strong-non-binariness to 2-closure, Lemma 1.7.5 yields an immediate computational dividend: there are built-in routines in `magma` to compute the 2-closure of a permutation group.

Thus if Ω is small enough, say $|\Omega| \leq 10^7$, then we can easily check whether or not the group G is 2-closed. Thus we can ascertain whether or not G is strongly non-binary.

Test 3: a direct analysis. The next test we discuss is feasible once again provided $|\Omega| \leq 10^7$. It simply tests whether or not 2-subtuple-completeness implies 3-subtuple completeness, and the procedure is as follows:

We fix $\alpha \in \Omega$, we compute the orbits of G_α on $\Omega \setminus \{\alpha\}$ and we select a set of representatives $\mathcal{O}$ for these orbits. Then, for each $\beta \in \mathcal{O}$, we compute the orbits of $G_\alpha \cap G_\beta$ on $\Omega \setminus \{\alpha, \beta\}$ and we select a set of representatives $\mathcal{O}_\beta$. Then, for each $\gamma \in \mathcal{O}_\beta$, we compute $\gamma^{G_\alpha} \cap \gamma^{G_\beta}$. Finally, for each $\gamma' \in \gamma^{G_\alpha} \cap \gamma^{G_\beta}$, we test whether the two triples (α, β, γ) and (α, β, γ') are G-conjugate. If the answer is "no", then G is not binary because by construction (α, β, γ) and (α, β, γ') are 2-subtuple complete. In particular, in this circumstance, we can break all the "for loops" and deduce that G is not binary.

If the answer is "yes", for every β, γ, γ', then we cannot deduce that G is binary, but we can keep track of these cases for a deeper analysis. We observe that, if the answer is "yes", for every β, γ, γ', then 2-subtuple completeness implies 3-subtuple completeness. At this point, we may either use a different method for checking whether the permutation group is genuinely binary or, with a similar method, we can check whether 3-subtuple completeness implies 4-subtuple completeness. This test is very expensive in terms of time, therefore before starting this whole procedure, we do a preliminary check: for 10^6 times, we select β, γ, γ' as above at random and we check this random triple. This test is actually rather robust because we are checking triples (α, β, γ) and (α, β, γ'), with a common initial segment.

Test 4: studying suborbits. Lemma 1.7.1 implies that if G is binary, then the action of a point-stabilizer M on any nontrivial suborbit is also binary. This fact is particularly useful for computation in situations where the group G is very large compared to the group M.

In general, our approach is to demonstrate that there must be some suborbit on which the action of M is not binary. For instance, this would follow in the case where $|\Omega| = |G : M|$ is divisible by some integer d, and all non-trivial transitive binary actions of M are also of degree divisible by d.

This last approach sometimes fails for just a few possible actions of M; in this situation, provided the action of G on Ω is primitive, the following lemma is often useful.

Lemma 1.9.2 ([105, Theorem 18.2])**.** *Suppose that G is a finite primitive subgroup of* $\mathrm{Sym}(\Omega)$*. Let Γ be a non-trivial orbit of a point-stabilizer M. Then, every simple section of M is isomorphic to a section of the group M^Γ which M induces on Γ. In particular, each composition factor of M is isomorphic to a section of M^Γ.*

This lemma means that when studying possible suborbits of our action we may disregard the actions of M (on a set Γ say) where M has a simple section not isomorphic to a section of the group M^Γ. If the resulting set of actions are all not binary, then we can conclude that the action of G on Ω is also not binary. The method is summarised in Lemma 3.1 of [34]:

Lemma 1.9.3. *Let G be a primitive group on a set Ω, let α be a point of Ω, let M be the stabilizer of α in G and let d be an integer with $d \geq 2$. Suppose $M \neq 1$ and, for each transitive action of M on a set Λ satisfying:*

1. *$|\Lambda| > 1$, and*

2. *every composition factor of M is isomorphic to some section of M^Λ, and*

3. *either $M_{(\Lambda)} = 1$ or, given $\lambda \in \Lambda$, the stabilizer M_λ has a normal subgroup N with $N \neq M_{(\Lambda)}$ and $N \cong M_{(\Lambda)}$, and*

4. M is binary in its action on Λ,

we have that d divides $|\Lambda|$. Then either d divides $|\Omega| - 1$ or G is not binary.

Often, we do require an indirect method for determining whether the action of G on the right cosets of a certain maximal subgroup M is binary. This indirect method is offered by our Test 4, together with Lemmas 1.9.2 and 1.9.3. There are various reasons for requiring indirect methods. First, there will be circumstances where the index of M in G is so large that it is computationally impractical to search for a useful suborbit (indeed, in these cases, most suborbits are expected to be regular). Second, there will be circumstances where the group G and its subgroup M are available in some library in `magma` as abstract groups, but the embedding of M in G is missing. Therefore, for these cases, one needs indirect methods (mainly studying transitive actions of M) for establishing whether the action of G on $(G : M)$ is binary.

Test 5: special primes. We have turned Lemmas 1.7.15 and 1.7.16 into a routine in `magma`. Both of these lemmas are rather convenient from a computational point of view because they do not require us to construct the permutation representation of G on $(G : M)$. For example, the only critical step in the routine for Lemmas 1.7.15 and Lemma 1.7.16 is the construction of the centraliser in G of an element g in M of prime order p. There is a standard built-in command in `magma` for constructing centralizers. Most often than not, this command is sufficient for our computations. However, for very large groups, where it is computationally out of reach to use a general command for computing centralizers, we have constructed $C_G(g)$ with *ad hoc* methods exploiting the subgroup structure of the group G under consideration.

Test 6: M very small. This method draws on the following lemma.

Lemma 1.9.4 ([46, Lemma 2.5]). *Let $\omega_0, \omega_1, \omega_2 \in \Omega$ with $G_{\omega_0} \cap G_{\omega_1} = 1$. Suppose there exists $g \in G_{\omega_0} \cap G_{\omega_2} G_{\omega_1}$ with $g \notin G_{\omega_2}$. Then the two triples $(\omega_0, \omega_1, \omega_2)$ and $(\omega_0, \omega_1, \omega_2^g)$ are 2-subtuple complete but are not 3-subtuple complete. In particular, G is not binary.*

This method is particularly useful when M (G_{ω_0} in Lemma 1.9.4) is small compared to G because in this case it is more likely that $G_{\omega_0} \cap G_{\omega_1} = 1$, for some ω_1. This method also has the benefit that it does not require us to construct the permutation representation of G on $(G : M)$, and that all the computations are performed locally. Since this method is designed to deal with the case that $(G : M)$ is large compared to M, we do not exhaustively check all triples $\omega_0, \omega_1, \omega_2 \in (G : M)$. In practice, we let $\omega_0 := M$, we generate at random $g_1, g_2 \in G$, we let $G_{\omega_1} := M^{g_1}$ and $G_{\omega_2} := M^{g_2}$ and we check whether Lemma 1.9.4 applies to $\omega_0, \omega_1, \omega_2$. We repeat this routine 10^5 times and if at some point we find a triple satisfying Lemma 1.9.4, then G acting on $(G : M)$ is not binary and we stop the routine. If, after the 10^5 trials, we have not found any triple satisfying Lemma 1.9.4, then we turn to a different method.

We give an explicit and typical example where this test does play a role. In Chapter **??**, among other things, we prove that the primitive faithful actions of the exceptional groups $G_2(q)$ are not binary. We use general arguments for dealing with these actions but, for this particular family of Lie groups, our arguments fail when $q \leq 5$. At this point, to keep our arguments uniform, we have decided not to take detours for dealing with the remaining groups with ad hoc theoretical methods but have instead turned to computational methods. Thus, in Proposition **??**, using mainly Test 6, we prove that the faithful primitive actions of the groups $G_2(q)$, with $q \leq 5$, are not binary.

Bibliography

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Invent. Math.*, 76(3):469–514, 1984.

[2] M. Aschbacher and L. Scott. Maximal subgroups of finite groups. *J. Algebra*, 92:44–80, 1985.

[3] Michael Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986.

[4] Laszlo Babai. On the order of doubly transitive permutation groups. *Invent. Math.*, 65:473–484, 1982.

[5] Robert F. Bailey and Peter J. Cameron. Base size, metric dimension and other invariants of groups and graphs. *Bull. London Math. Soc.*, 43(2):209–242, 2011.

[6] John Ballantyne, Chris Bates, and Peter Rowley. The maximal subgroups of $E_7(2)$. *LMS J. Comput. Math.*, 18:323–371, 2015.

[7] Kenneth D. Blaha. Minimum bases for permutation groups: the greedy approximation. *J. Algorithms*, 13(2):297–306, 1992.

[8] Armand Borel and Jacques Tits. Éléments unipotents et sous-groupes paraboliques de groupes réductifs. I. *Invent. Math.*, 12:95–104, 1971.

[9] Nicolas Bourbaki. *Elements of mathematics. Lie groups and Lie algebras. Chapters 4–6. Transl. from the French by Andrew Pressley.* Springer, Berlin, 2002.

[10] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal. *The maximal subgroups of the low-dimensional finite classical groups*, volume 407 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2013.

[11] Timothy C. Burness. On base sizes for actions of finite classical groups. *J. Lond. Math. Soc.*, 75(3):545–562, 2007.

[12] Timothy C. Burness and Michael Giudici. *Classical groups, derangements and primes*, volume 25 of *Australian Mathematical Society Lecture Series*. Cambridge University Press, Cambridge, 2016.

[13] Timothy C. Burness, Robert M. Guralnick, and Jan Saxl. On base sizes for symmetric groups. *Bull. Lond. Math. Soc.*, 43(2):386–391, 2011.

[14] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev. Base sizes for simple groups and a conjecture of Cameron. *Proc. Lond. Math. Soc.*, 98(1):116–162, 2009.

[15] Timothy C. Burness, E. A. O'Brien, and Robert A. Wilson. Base sizes for sporadic simple groups. *Israel J. Math.*, 177:307–333, 2010.

[16] Timothy C. Burness and Adam R. Thomas. On the involution fixity of exceptional groups of Lie type. *Int. J. Algebra Comput.*, 28(3):411–466, 2018.

[17] Peter J. Cameron. 6-transitive graphs. *J. Comb. Theory, Ser. B*, 28:168–179, 1980.

[18] Peter J. Cameron. Some open problems on permutation groups. In *Groups, combinatorics and geometry. Proceedings of the L.M.S. Durham symposium, 1990*, volume 165, pages 340–350. Cambridge University Press, 1992.

[19] Peter J. Cameron and William M. Kantor. Random permutations: Some group-theoretic aspects. volume 2, pages 257–262. Cambridge University Press, Cambridge, 1993.

[20] Gregory Cherlin. Sporadic homogeneous structures. In *The Gelfand Mathematical Seminars, 1996–1999. Dedicated to the memory of Chih-Han Sah*, pages 15–48. Boston, MA: Birkhäuser, 2000.

[21] Gregory Cherlin. On the relational complexity of a finite permutation group. *J. Alg. Combin.*, 43(2):339–374, 2016.

[22] Gregory Cherlin and Ehud Hrushovski. *Finite structures with few types*, volume 152 of *Annals of Mathematics Studies*. Princeton University Press, 2003.

[23] Gregory Cherlin and Joshua Wiscons. Personal communication.

[24] Gregory Cherlin and Joshua Wiscons. The relational complexity of partitions of shape $n \times 2$ under Sym_{2n} and Alt_{2n}. In preparation.

[25] Gregory L. Cherlin. The classification of countable homogeneous directed graphs and countable homogeneous n-tournaments. *Mem. Am. Math. Soc.*, 621, 1998.

[26] Gregory L. Cherlin, Gary A. Martin, and Daniel H. Saracino. Arities of permutation groups: Wreath products and k-sets. *J. Comb. Theory, Ser. A*, 74(2):249–286, 1996.

[27] Arjeh M. Cohen and Gary M. Seitz. The r-rank of the groups of exceptional Lie type. *Indag. Math.*, 49:251–259, 1987.

[28] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson. *Atlas of finite groups*. Oxford University Press, 1985.

[29] Bruce N. Cooperstein. Maximal subgroups of $G_2(2^n)$. *J. Algebra*, 70:23–36, 1981.

[30] David Craven, David Stewart, and Adam Thomas. A new maximal subgroup of E_8 in characteristic 3. 2014, Preprint available on the Math arXiv: `https://arxiv.org/pdf/2103.12148.pdf`.

[31] David A. Craven. Maximal PSL_2 subgroups of exceptional groups of lie type. To appear in *Mem. Amer. Math. Soc.*

[32] David A. Craven. On medium-rank lie primitive and maximal subgroups of exceptional groups of lie type. To appear in *Mem. Amer. Math. Soc.*

[33] David A. Craven. Alternating subgroups of exceptional groups of Lie type. *Proc. Lond. Math. Soc.*, 115(3):449–501, 2017.

[34] Francesca Dalla Volta, Nick Gill, and Pablo Spiga. Cherlin's conjecture for sporadic simple groups. *Pac. J. Math.*, 297(1):47–66, 2018.

[35] D. I. Deriziotis. The centralizers of semisimple elements of the Chevalley groups E_7 and E_8. *Tokyo J. Math.*, 6:191–216, 1983.

[36] D. I. Deriziotis and Martin W. Liebeck. Centralizers of semisimple elements in finite twisted groups of Lie type. *J. Lond. Math. Soc.*, 31:48–54, 1985.

[37] Alice Devillers. Homogeneous and ultrahomogeneous steiner systems. *J. Comb. Designs*, 11:153–161, 2003.

[38] John D. Dixon and Brian Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[39] Hikoe Enomoto. The characters of the finite Chevalley group $G_2(q)$, $q = 3^f$. *Japan. J. Math.*, 2:191–248, 1976.

[40] Walter Feit and Jacques Tits. Projective representations of minimum degree of group extensions. *Canad. J. Math.*, 30:1092–1102, 1978.

[41] Jason Fulman and Robert Guralnick. Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements. *Trans. Am. Math. Soc.*, 364(6):3023–3070, 2012.

[42] A. Gardiner. Homogeneous graphs. *J. Comb. Theory, Ser. B*, 20:94–102, 1976.

[43] Meinolf Geck. Generalized Gelfand-Graev characters for Steinberg's triality groups and their applications. *Commun. Algebra*, 19(12):3249–3269, 1991.

[44] N. Gill, B. Lodà, and P. Spiga. On the height and relational complexity of finite primitive permutation groups. To appear in *Nagoya Math. J.*

[45] Nick Gill, Francis Hunt, and Pablo Spiga. Cherlin's conjecture for almost simple groups of Lie rank 1. *Math. Proc. Camb. Philos. Soc.*, 167(3):417–435, 2019.

[46] Nick Gill and Pablo Spiga. Binary permutation groups: alternating and classical groups. *Am. J. Math.*, 142(1):1–43, 2020.

[47] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups. Number 3. Part I. Chapter A*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1998.

[48] Robert Gray, Dugald Macpherson, Cheryl E. Praeger, and Gordon F. Royle. Set-homogeneous directed graphs. *J. Comb. Theory, Ser. B*, 102(2):474–520, 2012.

[49] Frank Himstedt. Character tables of parabolic subgroups of Steinberg's triality groups ${}^3D_4(2^n)$. *J. Algebra*, 316(1):254–283, 2007.

[50] Scott Hudson. *The relational complexity of the primitive actions of* $\mathrm{PSL}_2(q)$ *and* $\mathrm{PGL}_2(q)$. PhD thesis, University of South Wales. In preparation.

[51] Christoph Jansen, Klaus Lux, Richard Parker, and Robert Wilson. *An atlas of Brauer characters*, volume 11. Oxford: Clarendon Press, 1995.

[52] W. M. Kantor. Linear groups containing a Singer cycle. *J. Algebra*, 62:232–234, 1980.

[53] W. M. Kantor, Martin W. Liebeck, and H. D. Macpherson. $\aleph_0$-categorical structures smoothly approximated by finite substructures. *Proc. Lond. Math. Soc. (3)*, 59(3):439–463, 1989.

[54] William M. Kantor and Ákos Seress. Prime power graphs for groups of Lie type. *J. Algebra*, 247(2):370–434, 2002.

[55] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1990.

[56] Peter B. Kleidman. The maximal subgroups of the finite 8-dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. *J. Algebra*, 110:173–242, 1987.

[57] 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.

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

[59] Peter B. Kleidman and Robert A. Wilson. The maximal subgroups of $E_6(2)$ and $\mathrm{Aut}(E_6(2))$. *Proc. London Math. Soc. (3)*, 60(2):266–294, 1990.

[60] Julia F. Knight and Alistair H. Lachlan. Shrinking, stretching and codes for homogeneous structures. Classification theory, Proc. U.S.-Israel Workshop on Model Theory in Math. Logic, Chicago 1985, Lect. Notes Math. 1292, 192–229, Springer, Berlin, 1987.

[61] A. H. Lachlan. Finite homogeneous simple digraphs. Logic colloquium '81, Proc. Herbrand Symp., Marseille 1981, Stud. Logic Found. Math. 107, 189–208, 1982.

[62] A. H. Lachlan. Countable homogeneous tournaments. *Trans. Am. Math. Soc.*, 284:431–461, 1984.

[63] A. H. Lachlan. Homogeneous structures. Proc. Int. Congr. Math., Berkeley 1986, Vol. 1, 314–321, Amer. Math. Soc., Providence, RI, 1987.

[64] A. H. Lachlan and Robert E. Woodrow. Countable ultrahomogeneous undirected graphs. *Trans. Am. Math. Soc.*, 262:51–94, 1980.

[65] Alistair H. Lachlan and Allyson Tripp. Finite homogeneous 3-graphs. *Math. Log. Q.*, 41(3):287–306, 1995.

[66] V. Landazuri and G. M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.

[67] R. Lawther. Unipotent classes in maximal subgroups of exceptional algebraic groups. *J. Algebra*, 322(1):270–293, 2009.

[68] R. Lawther. Sublattices generated by root differences. *J. Algebra*, 412:255–263, 2014.

[69] Ross Lawther, Martin W. Liebeck, and Gary M. Seitz. Fixed point ratios in actions of finite exceptional groups of Lie type. *Pacific J. Math.*, 205(2):393–464, 2002.

[70] M. W. Liebeck, C. E. Praeger, and J. Saxl. The maximal factorizations of the finite simple groups and their automorphism groups. *Mem. Am. Math. Soc.*, 432, 1990.

[71] Martin W. Liebeck. On minimal degrees and base sizes of primitive permutation groups. *Arch. Math.*, 43:11–15, 1984.

[72] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *J. Aust. Math. Soc., Ser. A*, 44(3):389–396, 1988.

[73] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. On factorizations of almost simple groups. *J. Algebra*, 185(2):409–419, 1996.

[74] Martin W. Liebeck and Jan Saxl. The primitive permutation groups of odd degree. *J. Lond. Math. Soc.*, 31:250–264, 1985.

[75] Martin W. Liebeck, Jan Saxl, and Gary M. Seitz. Subgroups of maximal rank in finite exceptional groups of Lie type. *Proc. Lond. Math. Soc.*, 65(2):297–325, 1992.

[76] Martin W. Liebeck and Gary M. Seitz. Subgroups generated by root elements in groups of Lie type. *Ann. Math. (2)*, 139(2):293–361, 1994.

[77] Martin W. Liebeck and Gary M. Seitz. Reductive subgroups of exceptional algebraic groups. *Mem. Am. Math. Soc.*, 580, 1996.

[78] Martin W. Liebeck and Gary M. Seitz. On finite subgroups of exceptional algebraic groups. *J. Reine Angew. Math.*, 515:25–72, 1999.

[79] Martin W. Liebeck and Gary M. Seitz. A survey of maximal subgroups of exceptional groups of Lie type. In *Groups, combinatorics and geometry. Proceedings of the L. M. S. Durham symposium, Durham, 2001*, pages 139–146. World Scientific, River Edge, NJ, 2003.

[80] Martin W. Liebeck and Gary M. Seitz. The maximal subgroups of positive dimension in exceptional algebraic groups. *Mem. Am. Math. Soc.*, 802, 2004.

[81] Martin W. Liebeck and Aner Shalev. Simple groups, permutation groups, and probability. *J. Am. Math. Soc.*, 12(2):497–520, 1999.

[82] Frank Lübeck. Conjugacy classes and character degrees of $E_7(2)$. `http://www.math.rwth-aachen.de/~Frank.Luebeck/chev/E72.html?LANG=en`. Accessed: 2019-03-13.

[83] Frank Lübeck. Small degree representations of finite Chevalley groups in defining characteristic. *LMS J. Comput. Math.*, 4:135–169, 2001.

[84] Andrea Lucchini and Pablo Spiga. Hypermaps over non-abelian simple groups and strongly symmetric generating sets, arXiv:2103.03777.

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

[86] Joy Morris, Cheryl E. Praeger, and Pablo Spiga. Strongly regular edge-transitive graphs. *Ars Math. Contemp.*, 2(2):137–155, 2009.

[87] S. P. Norton and R. A. Wilson. The maximal subgroups of $F_4(2)$ and its automorphism group. *Comm. Algebra*, 17(11):2809–2824, 1989.

[88] Rimhak Ree. A family of simple groups associated with the simple Lie algebra of type (G_2). *Amer. J. Math.*, 83:432–462, 1961.

[89] Dan Saracino. On a combinatorial problem from the model theory of wreath products. I. *J. Comb. Theory, Ser. A*, 86(2):281–305, 1999.

[90] Dan Saracino. On a combinatorial problem from the model theory of wreath products. II. *J. Comb. Theory, Ser. A*, 86(2):306–322, 1999.

[91] Dan Saracino. On a combinatorial problem from the model theory of wreath products. III. *J. Comb. Theory, Ser. A*, 89(2):231–269, 2000.

[92] Mark Schaffer. Twisted tensor product subgroups of finite classical groups. *Commun. Algebra*, 27(10):5097–5166, 1999.

[93] Leonard L. Scott. Representations in characteristic p. Finite groups, Santa Cruz Conf. 1979, *Proc. Symp. Pure Math.* 37, 319–331, 1980.

[94] Gary M. Seitz. Representations and maximal subgroups of finite groups of Lie type. *Geom. Dedicata*, 25:391–406, 1988.

[95] Gary M. Seitz. Maximal subgroups of exceptional algebraic groups. *Mem. Am. Math. Soc.*, 441, 1991.

[96] J. Sheehan. Smoothly embeddable subgraphs. *J. Lond. Math. Soc.*, 9:212–218, 1974.

[97] Kenichi Shinoda. The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic 2. *J. Fac. Sci., Univ. Tokyo, Sect. I A*, 21:133–159, 1974.

[98] Kenichi Shinoda. The conjugacy classes of the finite Ree groups of type (F_4). *J. Fac. Sci., Univ. Tokyo, Sect. I A*, 22:1–15, 1975.

[99] Charles C. Sims. Graphs and finite permutation groups. *Math. Z.*, 95:76–86, 1967.

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

[101] Adam R. Thomas. Simple irreducible subgroups of exceptional algebraic groups. *J. Algebra*, 423:190–238, 2015.

[102] Pham Huu Tiep. Low dimensional representations of finite quasisimple groups. In *Groups, combinatorics and geometry. Proceedings of the L. M. S. Durham symposium, Durham, 2001*, pages 277–294. World Scientific, River Edge, NJ, 2003.

[103] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Aust. Math. Soc.*, 3:1–62, 1963.

[104] H. N. Ward. On Ree's series of simple groups. *Bull. Am. Math. Soc.*, 69:113–114, 1963.

[105] Helmut Wielandt. *Finite permutation groups.* Academic Press, New York and London, 1964.

[106] Robert A. Wilson. Maximal subgroups of sporadic groups. In *Finite simple groups: thirty years of the atlas and beyond*, volume 694 of *Contemp. Math.*, pages 57–72, Providence, RI, 2017. Amer. Math. Soc.

[107] Robert A. Wilson. Maximal subgroups of ${}^2E_6(2)$ and its automorphism groups. Preprint available: `https://arxiv.org/abs/1801.08374`, 2018.

[108] Joshua Wiscons. A reduction theorem for primitive binary permutation groups. *Bull. Lond. Math. Soc.*, 48(2):291–299, 2016.