A computer-assisted analysis of some matrix groups

Derek F. Holt and E.A. O'Brien

Abstract

We use algorithms developed recently for the study of linear groups to investigate a sequence of matrix groups defined over GF(2); these are representations of finitely-presented groups considered by Soicher in a study of simplicial complexes.

1 Introduction

In [22], Soicher considers a sequence of simplicial complexes known as $\Gamma_n$-complexes, and classifies a more restricted type of complex, known as $\Gamma^*_n$ complexes, for $n \leq 8$. These complexes arise naturally in connection with a sequence $\Gamma_n$ of graphs, the Suzuki sequence graphs. The automorphism groups of these graphs are well-known for $n \leq 6$. For example, $\text{Aut}(\Gamma_6) = \text{Suz}:2$, where Suz is the sporadic simple group of Suzuki. Our notation for the structure of finite groups follows that of [2].

Soicher established that the automorphism group of a $\Gamma_n$-complex is a quotient of the finitely-presented $(n + 2)$-generator group

\[ U_n := \langle a, u_0, u_1, \ldots, u_n \mid a^2, u_i^2 (0 \leq i \leq n), (au_0)^3, (u_0u_1)^3, (u_1u_2)^8, (u_iu_{i+1})^3 (2 \leq i < n), (u_1u_j)^2 (i + 1 < j), a^{-1}(u_1u_2)^4 \rangle. \]

Alternatively, $U_n$ is the group defined by the Coxeter diagram

We thank J.N. Bray, L.G. Kovács, L.H. Soicher and B. Souvignier for valuable discussions and suggestions. This work was supported in part by the Marsden Fund of New Zealand via grant UOA 0412. 2000 Mathematics Subject Classification. Primary 20C20
with the extra relation $a = (u_1 u_2)^4$. He proved that $U_2 \cong L_3(2): 2$ and $U_3 \cong (3 \times U_3(3)): 2$.

The automorphism group of a $\Gamma_n^*$-complex is a quotient of the group $U_n^*$, which is the quotient of $U_n$ obtained by adjoining the additional relator $(u_0 u_1 u_2 u_3)^8$. (This element generates the normal subgroup of order 3 in $U_3$). In [21], Soicher proved that, for $3 \leq n \leq 8$, $U_n^*$ is isomorphic to $U_3(3): 2$, $J_2: 2$, $G_2(4): 2$, $3 \cdot \text{Suz}: 2$, $Co_1 \times 2$, and $2 \cdot (Co_1 \wr 2)$, respectively.

In unpublished work, Richard Parker described a construction for two matrix representations of $U_n$ over GF(2): these are identical for even $n$ but distinct for odd $n > 1$. They are also representations of $U_n^*$ for $n \geq 3$. For $n \geq 2$, the representations have degree $6 \cdot 2^{m-2}$ and $6 \cdot 2^{m-1}$ when $n = 2m - 1$, and degree $6 \cdot 2^{m-1}$ when $n = 2m$. We describe the construction in Section 2. We denote the matrix groups defined by these representations of $U_n^*$ as $G_n$ and, when $n$ is odd, $G_n^l$, respectively. (The superscript $l$ means ‘large’.)

One of the major projects in computational group theory during the past 15 years has been the development of effective algorithms for analysing the structure of linear groups defined by generating matrices over a finite field. For a recent survey of this project, see O’Brien [18]. Implementations of some of the resulting algorithms are available in MAGMA [4] as part of a package developed by Leedham-Green and O’Brien. Although the machinery is not yet complete, it frequently allows us to identify the composition factors of a linear group.

As a case study, we used this machinery to study Parker’s groups $G_n$ and $G_n^l$ for $n \leq 20$, hence for groups of degree at most 3072. This motivated us to develop some additional machinery and to exploit some (reasonably well-known) representation-theoretic results.

The outline of the paper is the following. We first describe the matrix representations of Parker. In Section 3 we consider some basic questions about linear groups. We then discuss a geometric-based approach to the study of linear groups, and introduce the concept of a composition tree whose leaves are the composition factors of a group. In Section 6 we record some module-theoretic results which assist in our structural analysis. In Section 7 we report the structure of the groups, commenting on the individual cases. In Section 8, we show that our results establish the existence of a $\Gamma_n^*$-complex for $n = 10$. Finally we consider briefly the finitely-presented groups.
The representations

We now describe generating sequences $X_n$ and $X^l_n$ for the matrix groups $G_n$ and $G^l_n$ over GF(2) for $n \geq 1$, where $X_n^l$ and $G^l_n$ are defined only for odd $n$.

For $n \geq 2$, if we map the generating sequence $[a, u_0, \ldots, u_n]$ of $U_n$ (or of $U^*_n$ when $n \geq 3$) to $X_n$ or $X^l_n$, then we obtain Parker’s representations of $U_n$ (or of $U^*_n$ when $n \geq 3$).

For $(m \times m)$– and $(n \times n)$–matrices $\alpha$ and $\beta$, the Kronecker product $K(\alpha, \beta)$ of $\alpha$ and $\beta$ is defined to be the $(mn \times mn)$–matrix in which the entry in position $((i-1)n+k, (j-1)n+l)$ is equal to $\alpha_{ij}\beta_{kl}$, for $1 \leq i, j \leq m, 1 \leq k, l \leq n$.

Define

$$\alpha := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \beta := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\gamma := \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad \delta := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \epsilon := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where all matrices are over GF(2), and let $I_k$ denote the $k \times k$ identity matrix over GF(2).

We define $X_1 = X_n^l = [(\beta\gamma)^4, \alpha, \beta]$. For $n > 1$, we define $X_n$ and $X_n^l$ recursively. If $n = 2m$ is even, then we set $X_n[i] := X_{n-1}^l[i]$ for $1 \leq i \leq n + 1$, and $X_n[n+2] := K(\gamma, I_{2m-1})$.

If $n = 2m - 1$ is odd, then we define $X_n$ by $X_n[i] := X_{n-1}^l[i]$ for $1 \leq i \leq n + 1$, $X_n[n + 2] := K(\epsilon, I_{3.2m-2})$, and $X_n^l$ by $X_n^l[i] := K(I_2, X_n[i])$ for $1 \leq i \leq n + 1$, $X_n^l[n + 2] := K(\delta, I_{3.2m-2})$.

That these define representations of $U_n$ and $U^*_n$ is readily verified.
3 Some natural questions

If we are given $G \leq \text{GL}(d, q)$, a natural question is: what is the order of $G$? The Schreier-Sims algorithm, first introduced for permutation groups by Sims [19], can sometimes provide an answer. We review this briefly; for a detailed discussion, see [9, Chapter 4].

Let a group $G$ act faithfully on $\Omega = \{1, \ldots, n\}$. Recall that a base for $G$ is a sequence of points $B = [\beta_1, \beta_2, \ldots, \beta_k]$ such that the sequence stabiliser $G_{\beta_1, \beta_2, \ldots, \beta_k} = 1$. This determines a chain of stabilisers

$$G = G^{(1)} \geq G^{(2)} \geq \cdots \geq G^{(k)} \geq G^{(k+1)} = 1,$$

where $G^{(i)} = G_{\beta_1, \beta_2, \ldots, \beta_{i-1}}$. A strong generating set for $B$ is a subset $S$ of $G$ such that $G^{(i)} = \langle S \cap G^{(i)} \rangle$, for $i = 1, \ldots, k$.

The main task in setting up such a data structure is the construction of basic orbits – the orbit $B_i$ of $\beta_{i+1}$ under $G^{(i)}$. Observe that $|G^{(i)} : G^{(i+1)}| = |B_i|$. Sims used Schreier’s Lemma to obtain a deterministic algorithm to construct the strong generating sets. By contrast, Leon’s random Schreier-Sims [14] uses random elements of $G$. It is usually significantly faster, giving smaller strong generating sets. Its results can be verified; see, for example, [9, Section 6.3].

If we simply exploit the natural faithful action of $G \leq \text{GL}(d, q)$ on the vectors in $V = GF(q)^d$, then the basic orbits are usually very large; if $G$ is simple, the first orbit length is often $|G|$. By choosing base points having shorter basic orbits, we extend significantly the range of application of the Schreier-Sims. Butler [5] developed the algorithm for linear groups, choosing as base points the one-dimensional subspaces of $V$. A general strategy to select good base points was introduced by Murray & O’Brien [15].

Despite various limitations imposed by the basic orbit sizes, the algorithm and its variations underpin most of the long-standing machinery for computing with linear groups. The implementations in MAGMA are very effective for “moderate” degree representations defined over “small” fields.

Celler & Leedham-Green [7] present an algorithm to compute the order of $g \in \text{GL}(d, q)$. In summary, from a consideration of the minimal polynomial of $g$, they first obtain a “good” multiplicative upper bound for $|g|$ and then use a “divide-and-conquer” strategy to obtain the order.

Many of the algorithms developed recently for linear groups rely on random selections, and the analysis of their performance assumes that we select uniformly distributed random elements. MAGMA uses the product replacement algorithm of

In the same paper they introduce the following technique, which can be used to prove that $G$ is perfect. By taking commutators of generators, we construct a normal generating set for $G'$, the derived subgroup of $G$. For each generator $g$ of $G$, we compute the orders $o_i$ of elements $gh_i$ for randomly chosen elements $h_i$ of $G'$. If the greatest common divisor of the $o_i$ is 1 (and we check this after each choice of $h_i$), then we have proved that $g \in G'$.

4 A geometric approach

A classification of the maximal subgroups of the classical groups by Aschbacher [1] underpins the geometric approach to the study of linear groups.

Let $Z$ denote the group of scalar matrices of $G$. Then $G$ is almost simple modulo scalars if there is a non-abelian simple group $T$ such that $T \leq G/Z \leq \text{Aut}(T)$, the automorphism group of $T$. In summary, Aschbacher’s classification implies that a linear group preserves some natural linear structure in its action on the underlying vector space $V$ and has a normal subgroup related to this structure, or it is almost simple modulo scalars.

In more detail, if $G$ is a maximal subgroup of a classical group, then it is in at least one of the following Aschbacher categories.

C1. $G$ acts reducibly.

C2. $G$ acts imprimitively.

C3. $G$ acts on $V$ as a group of semilinear automorphisms of a $(d/e)$-dimensional space over the extension field GF($q^e$), for some $e > 1$, and so $G$ embeds in $\Gamma L(d/e, q^e)$.

C4. $G$ preserves a decomposition of $V$ as a tensor product $U \otimes W$ of spaces of dimensions $d_1, d_2 > 1$ over $F$.

C5. $G$ is definable modulo scalars over a subfield.

C6. For some prime $r$, $d = r^m$ and $G/Z$ is contained in the normaliser of an extraspecial group of order $r^{2m+1}$, or of a group of order $2^{2m+2}$ and symplectic-type.

C7. $G$ is tensor-induced.
C8. $G$ normalises a classical group in its natural representation.

C9. Otherwise $G$ is almost simple modulo scalars.

The first seven categories have a normal subgroup associated with a decomposition. The C9-class consists of absolutely irreducible, tensor-indecomposable, primitive groups which are almost simple modulo scalars, cannot be defined over a proper subfield, and are not classical in their natural representation.

In broad outline, this theorem suggests that a first step in investigating a linear group is to determine (at least one of) its categories in the Aschbacher classification. If a category is recognised, then we investigate the group structure more completely using algorithms designed for this category. Usually, we have reduced the size and nature of the problem. For example, if $G \leq \text{GL}(d, q)$ acts imprimitively, then we obtain a permutation representation of degree dividing $d$ for $G$. If a proper normal subgroup $N$ exists, we recognise $N$ and $G/N$ recursively, ultimately obtaining a composition series for $G$. Many questions about the structure of $G$ can then be answered by consideration of its composition factors.

5 The composition tree

In ongoing work, Leedham-Green and O’Brien have developed the concept of a composition tree, which seeks to realise and exploit the Aschbacher classification. Leedham-Green [8] provides a detailed description of this concept and its practical realisation. Here we summarise it briefly.

A composition series for a group $G$ can be viewed as a labelled rooted binary tree. The nodes correspond to sections of $G$, the root node to $G$. A node that corresponds to a section $K$ of $G$, and is not a leaf, has a left descendant corresponding to a proper normal subgroup $N$ of $K$ and a right descendant corresponding to $K/N$. The right descendant is an image under a homomorphism; usually these arise naturally from an Aschbacher category of the group, but we also exploit additional ones for unipotent and soluble groups. The left descendant of a node is the kernel of the chosen homomorphism.

The tree is constructed in right depth-first order. Namely, we process the node associated with $K$: if $K$ is not a leaf, construct recursively the subtree rooted at its right descendant $I$, then the subtree rooted at its left descendant $N$. Each leaf is a composition factor of the root group $G$.

It is easy to construct $I$, since it is the image of $K$ under a homomorphism $\phi$. We generate a random element of $N$ as follows. Let $K = \langle x_1, \ldots, x_m \rangle$, and let
\(I = \phi(K) = \langle x_1, \ldots, x_m \rangle\). Choose random \(k \in K\), and evaluate \(\phi(k) \in I\). If we establish that \(\phi(k) = w(x_1, \ldots, x_m)\), then the residue \(k \cdot w(x_1, \ldots, x_m)^{-1} \in N\). by selecting sufficient random elements of \(K\), we construct with high probability a generating set for \(N\).

Observe that this strategy assumes that we can write an arbitrary element of \(I\) as a word in its defining generators. A major ongoing goal is to develop constructive recognition algorithms which perform such a task. Currently they are available for certain classes of groups; see [18] for details.

If \(N\) is nontrivial, we can usually find some elements randomly, by computing \(k^r\), where \(k\) is a random element of \(K\) and \(r\) is the order of \(kN\) in \(K/N\).

If we know presentations for \(K/N\) and \(N\), then we can construct one for \(K\); see for example [8] for details. If so, we can decide that we have constructed a generating set for \(N\) – and not just one for a proper subgroup of \(N\).

### 5.1 Identifying the composition factors

A natural question is: identify the non-abelian composition factors of \(G\). A non-constructive recognition algorithm names a simple group \(G\). (More precisely, it may establish that \(G\) contains a particular named group as a subgroup.) If, for example, we identify \(G\) as a member of a particular family of finite simple groups, then we may apply algorithms to \(G\) which are specially designed for this family.

Neumann & Praeger [16] presented a Monte Carlo algorithm to decide whether or not a subgroup of \(\text{GL}(d,q)\) contains \(\text{SL}(d,q)\). Niemeyer & Praeger [17] answer the corresponding question for an arbitrary classical group in the natural representation; their algorithm is available in MAGMA.

Babai et al. [3] present an algorithm to name a black-box group of Lie type in known defining characteristic. In 2001 Malle and O’Brien developed a practical implementation of this algorithm. It also includes identification procedures for the other quasisimple groups. If the non-abelian composition factor is sporadic, then we identify it by considering the (projective) orders of random elements. Similar methods can be used to deduce the degree of an alternating group.

### 6 A module argument

We now consider a situation which arises frequently in our analysis of these groups and exploit module structure to obtain more detailed structural information.
Let $F := GF(q)$, and let $M$ be the $d$-dimensional right module over $F$ on which $G \leq GL(d, q)$ acts. Suppose that $G$ acts reducibly on $M$ with submodule $M_1$ of dimension $d_1$ and quotient $M_2 := M/M_1$ of dimension $d_2$, where $d_1 + d_2 = d$. We make a basis change to bring the elements of $G$ into the block form

$$
\begin{pmatrix}
A & 0 \\
C & B
\end{pmatrix}
$$

(6.1)

where the diagonal blocks $A$ and $B$ are $(d_1 \times d_1)$– and $(d_2 \times d_2)$–matrices, respectively.

Thus $G$ has the structure $N.H$, where $N$ is the subgroup of $G$ consisting of matrices of the form

$$
\begin{pmatrix}
I & 0 \\
C & I
\end{pmatrix}
$$

(6.2)

and $H \cong G/N$ is isomorphic to the group having elements of the form

$$
\begin{pmatrix}
A & 0 \\
0 & B
\end{pmatrix}
$$

induced in the obvious way from the elements of $G$. (We are not of course claiming that the matrices of this form necessarily constitute a subgroup of $G$.)

Since $N$ acts trivially on $M_1$ and $M_2$, we may also regard $M_1$ and $M_2$ as modules over $H$. Let $H_1$ and $H_2$ be the images of the projections of $H$ onto the upper and lower diagonal blocks, respectively (so $H$ is a subdirect product of $H_1$ and $H_2$). The following allows us to obtain readily some structural information about $H$.

**Lemma 6.1.** (i) Let $h \in H$, and let $h_1$ and $h_2$ be the projections of $h$ onto $H_1$ and $H_2$. If $|h| > |h_i|$ for $i = 1$ or $2$, then $|H| > |H_i|$.

(ii) If $M_1$ is isomorphic as $FH$-module to either $M_2$ or to the dual of $M_2$, then $H \cong H_1 \cong H_2$.

**Proof.** (i) is clear. Let $K_1$ and $K_2$ be the kernels of the actions of $H$ on $M_1$ and $M_2$, respectively. Then $K_1$ and $K_2$ consist of those elements of $H$ that induce the identity on the upper and lower diagonal blocks, respectively, and $H/K_i \cong H_i$ for $i = 1, 2$. If $M_1$ is $FH$-isomorphic to $M_2$ or to its dual, then $K_1 = K_2$, and so $K_1 = K_2 = 1$ and the result follows. \[\square\]

Let $L$ be the elementary abelian group of order $q^{d_1d_2}$ consisting of all matrices that have the form 6.2 defined above. Then $H_1 \times H_2$ acts by conjugation on $L$, thereby making it into a module for $H_1 \times H_2$ over $F = GF(q)$. Conjugating an
element of form 6.2 by one of form 6.1 results in the \((d_2 \times d_1)\)–matrix \(C\) being replaced by \(B^{-1}CA\). In particular, if we denote the matrix of form 6.2 in which \(C\) is a matrix with a single one in position \((i,j)\) by \(e_{ij}\), and let \(A = (\alpha_{ij})\) and \((B^{-1})^T = (\beta_{ij})\), then \(e_{ij}\) is conjugated to \(\sum_{k=1}^{d_2} \sum_{l=1}^{d_1} \beta_{ik} \alpha_{jl} e_{kl}\). This demonstrates that, as an \(F(H_1 \times H_2)\)-module, \(L \cong M_2^* \otimes_F M_1\), where \(M_2^*\) denotes the dual of the module \(M_2\). By [12, VII, Lemma 8.8 b]), we also have \(L \cong \text{Hom}_F(M_2, M_1)\).

The subgroup \(N\) of \(L\) can be regarded in the same manner as a module for \(H\) under the conjugation action. However, it is not in general a \(GF(q)\)-submodule of the restriction of \(L\) to \(H\), but only a \(GF(p)\)-submodule, where \(q = p^e\) is a power of the prime \(p\). Then \(N\) has \(GF(p)\)-dimension \(k\) for some \(k\) with \(0 \leq k \leq ed_1d_2\).

In practice, this is not very useful if \(ed_1d_2\) is very large. Since \(N\) has potentially large order (and consequently many generators), constructing its generating set remains a challenging open problem. Recall from Section 5 that we can construct some elements of \(N\). If \(ed_1d_2\) is not too large (the current limit of practicality in MAGMA is about 80000 for \(q = 2\)), then we can compute the \(GF(p)H\)-submodule that they generate, and thereby obtain a lower bound for \(|N|\).

The following theoretical result is sometimes applicable. Since \(q = p = 2\) in the examples of Section 7, we shall avoid complications arising from the fact that, in general, \(N\) is only a \(GF(p)\)-submodule of \(L\), by assuming that \(q = p\).

**Lemma 6.2.** If \(N\) is nontrivial, \(H = H_1 \times H_2\), \(F = GF(p)\), and \(M_1\) and \(M_2\) are absolutely irreducible \(FH\)-modules, then \(N = L\).

**Proof.** Since \(H_2\) acts trivially on \(M_1\) and \(H_1\) acts trivially on \(M_2\), we may regard \(M_1\) and \(M_2\) as absolutely irreducible \(F\)-modules for \(H_1\) and \(H_2\), respectively. By [11, V, Satz 10.3 b]), the tensor product of irreducible modules \(V_1\) and \(V_2\) over an algebraically closed field for finite groups \(A_1\) and \(A_2\) is irreducible as an \((A_1 \times A_2)\)-module. The same result holds for absolutely irreducible modules over an arbitrary field, since such modules remain irreducible when we extend to the algebraic closure of the field. Hence \(N \cong M_2^* \otimes_F M_1\) is an irreducible \(FH\)-module, and the result follows.

**Remark.** More generally, if \(M_1\) and \(M_2\) are irreducible \(FH\)-modules over an arbitrary field \(F\) of non-zero characteristic, and \(E_i = \text{End}_{FG}(M_i)\) for \(i = 1, 2\), then \(M_1 \otimes_G M_2\) is an irreducible \(F(H_1 \times H_2)\)-module if and only if \(|E_1:F|\) and \(|E_2:F|\) are coprime. We are grateful to L.G. Kovács for pointing this out to us.

Knowledge of a presentations for \(H = G/N\) and \(N\) would allow us to verify conclusively that we have constructed \(N\), rather than a proper subgroup. In the absence of a presentation, we know of no general method to obtain an upper
bound for the order of $N$. But, as we shall see in the examples below, we can sometimes use specialised knowledge to deduce such.

7 The groups $G_n$ and $G_n^t$

We summarise the results of our investigations into the structure of the groups $G_n$ and $G_n^t$ in Table 1. The times given are in seconds, and are the totals for all Magma commands executed for the computations involving that group. These can vary considerably from run to run. They were carried out using Magma 2.12 on a 400MHz Ultrasparc with 4GB of memory. By combining the results of our computations and the theoretical results presented in Section 6, we were able to confirm these results in all cases.

For $n \geq 10$, there is evidence of a pattern emerging with period 8: namely $X_n$ and $X_n^t$ have similar structures to $X_{n+8}$ and $X_{n+8}^t$. But the evidence is too limited to justify a conjecture about their structure for arbitrary $n$.

Five of the nine Aschbacher categories arise when analysing the structure of these groups. These are C1, C2, C3, C8 and C9.

The C9-groups that arise are $L(2,7):2$, $U(3,3):2$, $J_2$, $G_2(4):2$, $3: \text{Suz}:2$, and $\text{Co}_1$. They are sufficiently small for us to recognise them constructively using the base and strong generating set method described in Section 3. The simple socles of the two largest examples, $3: \text{Suz}$ and $\text{Co}_1$, arise as subgroups of SL(12,4) and SL(24,2), respectively. By sampling (projective) orders of random elements as discussed in Section 5.1, we were able to identify their isomorphism types with a high probability of correctness. Using the method described in Section 3, we established that both groups were perfect, so it remained only to verify their orders deterministically to complete their identification. In applying the Schreier-Sims, we chose base points appropriate to these representations, and so the remaining computations were efficient. For $3: \text{Suz}$ we completed the verification using the matrix representation; for $\text{Co}_1$ we constructed a permutation representation of degree 98280, and used this to confirm the order of the group.

We now discuss the groups in Table 1 individually. Let $F := \text{GF}(2)$. The groups $G_n$ for $2 \leq n \leq 7$ are C9-groups, whereas $G_{11}$, $G_{15}$ and $G_{19}$ are C8-groups.

For $1 \leq n \leq 5$, we immediately established using the standard Magma functions $\text{Order}$ and $\text{ChiefFactors}$ (both using variations of the Schreier-Sims algorithm), that $G_n$, and also $G_n^t$ when $n$ is odd, are isomorphic to $S_4$, $L(2,7):2$, $U_3(3):2$, $J_2:2$, $G_2(4):2$, respectively. This, together with the identification of $G_6$ as $3: \text{Suz}:2$, confirms the results of [22].
The C8-groups arising are $\text{SL}(48,2)$, $\text{SL}(768,2)$, $\Omega^{+}(96,2)$, $\Omega^{+}(96,4)$, $\Omega^{+}(384,2)$, $\Omega^{+}(1536,2)$, $\Omega^{+}(1536,4)$, and $\text{SU}(192,2)$. As mentioned in Section 5.1, we readily identify these groups non-constructively. We confirmed that the orthogonal groups are of type $\Omega^{+}$ rather than $\text{SO}^{+}$, by proving that they are perfect using the method outlined in Section 3.

The groups $G_6$, $G_{12}$, $G_{13}$, $G_{14}$ and $G_{20}$ are C3-groups. Hence they have a normal subgroup $N$ that acts irreducibly but not absolutely irreducibly, and so $N$ can be rewritten as a group acting absolutely irreducibly in smaller dimension over a larger field. The elements outside of $N$ act as field automorphisms on $N$. In each of these examples, we have $|G_n : N| = 2$, and $N$ can be rewritten as a group of degree half the original dimension over $\text{GF}(4)$. For $G_6$, we identified $N$ as $3 \cdot \text{Suz}$, as discussed above. In the other cases, the rewritten group $N$ is a C8-group, and so can be recognised as described above.

We commented in Section 5 upon the difficulty of obtaining generators of normal subgroups $N$ of $G$ that arise in the composition tree program. However, in these examples $|G/N| = 2$, and we readily calculate Schreier generators for $N$. 

<table>
<thead>
<tr>
<th>$n$</th>
<th>Dim</th>
<th>$X_n$</th>
<th>time</th>
<th>Dim</th>
<th>$Y_n$</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>6</td>
<td>$S_4$</td>
<td>0</td>
<td>12</td>
<td>$U(3,3) : 2$</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>$L(2,7) : 2$</td>
<td>0</td>
<td>24</td>
<td>$G_2(4) : 2$</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>$U(3,3) : 2$</td>
<td>0</td>
<td>48</td>
<td>$\text{Co}_1 \wr 2$</td>
<td>95</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>$J_2 : 2$</td>
<td>1</td>
<td>96</td>
<td>$\Omega^{+}(96,2)$</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>$G_2(4) : 2$</td>
<td>2</td>
<td>192</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>59</td>
</tr>
<tr>
<td>6</td>
<td>24</td>
<td>$3 \cdot \text{Suz} : 2$</td>
<td>14</td>
<td>384</td>
<td>$\text{SU}(384,2)$</td>
<td>274</td>
</tr>
<tr>
<td>7</td>
<td>24</td>
<td>$\text{Co}_1$</td>
<td>129</td>
<td>768</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>993</td>
</tr>
<tr>
<td>8</td>
<td>48</td>
<td>$\text{Co}_1 \wr 2$</td>
<td>208</td>
<td>1536</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>1040</td>
</tr>
<tr>
<td>9</td>
<td>48</td>
<td>$\text{Co}_1 \wr 2$</td>
<td>213</td>
<td>1536</td>
<td>$\Omega^{+}(1536,2)$</td>
<td>12637</td>
</tr>
<tr>
<td>10</td>
<td>96</td>
<td>$\text{SL}(48,2) : 2$</td>
<td>9</td>
<td>192</td>
<td>$\Omega^{+}(96,2)$</td>
<td>43</td>
</tr>
<tr>
<td>11</td>
<td>96</td>
<td>$\Omega^{+}(96,2)$</td>
<td>12</td>
<td>384</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>57</td>
</tr>
<tr>
<td>12</td>
<td>192</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>57</td>
<td>384</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>20239</td>
</tr>
<tr>
<td>13</td>
<td>192</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>57</td>
<td>384</td>
<td>$\Omega^{+}(96,4) : 2$</td>
<td>20239</td>
</tr>
<tr>
<td>14</td>
<td>384</td>
<td>$\text{SU}(192,2) : 2$</td>
<td>69</td>
<td>384</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>274</td>
</tr>
<tr>
<td>15</td>
<td>384</td>
<td>$\Omega^{+}(384,2)$</td>
<td>274</td>
<td>768</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>993</td>
</tr>
<tr>
<td>16</td>
<td>768</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>1040</td>
<td>1536</td>
<td>$\Omega^{+}(1536,2)$</td>
<td>12637</td>
</tr>
<tr>
<td>17</td>
<td>768</td>
<td>$\Omega^{+}(384,2) : 2$</td>
<td>1040</td>
<td>3072</td>
<td>$\Omega^{+}(1536,2)$</td>
<td>589724</td>
</tr>
<tr>
<td>18</td>
<td>1536</td>
<td>$\text{SL}(768,2) : 2$</td>
<td>4560</td>
<td>3072</td>
<td>$\Omega^{+}(1536,2)$</td>
<td>129643</td>
</tr>
</tbody>
</table>

Table 1: The structure of the groups $G_n$ and $G_n^d$
The groups $G_8$, $G_9$, $G_{10}$, $G_{16}$, $G_{17}$ and $G_{18}$ are $C_2$-groups, with two blocks of imprimitivity. Again we have a normal subgroup $N$ of index 2 for which we can find Schreier generators, but here $N$ acts decomposably with two components of degree half of the original. The restricted actions on the components are $C_8$-groups in each case, and they can be recognised as before.

Since these $C_8$-groups $S$ are simple, there are only two possibilities for the structure of $N$: either $N \cong S$ or $N \cong S \times S$. We used Lemma 6.1 to distinguish between the two possibilities. For $G_8$, $G_9$, $G_{10}$ and $G_{17}$, we found elements in $N$ for which the restrictions onto the two components have different orders. Thus $N \cong S \times S$ in these examples and, by [10, Theorem 3] for example, $G$ is isomorphic to the wreath product $S \wr 2$. For $G_{10}$ and $G_{18}$, the $FN$-modules corresponding to the actions on the two components were dual to each other. Hence $N \cong S$, and the groups $G_{10}$, $G_{18}$ are $SL(48,2)$ and $SL(768,2)$, respectively, extended by the duality automorphism.

The remaining examples, $G_{n}^{l}$ for odd $3 \leq n \leq 19$, are $C_1$-groups with two irreducible constituents each having dimension $d/2$, where $d$ is the dimension of $G_{n}^{l}$. From the discussion in Section 6, we learn that $G_{n}^{l} \cong N_{n}, H_{n}$, where $N_{n}$ is an elementary abelian group of order $2^k$ with $0 \leq k \leq d^2/4$, and $H_{n} \leq GL(d/2,2) \times GL(d/2,2)$. In each of these examples, the $FH_{n}$-modules (referred to as $M_1$ and $M_2$ in Section 6) corresponding to the actions on the two components of $H_{n}$ are isomorphic. Hence, by Lemma 6.1, $H_{n} \leq GL(d/2,2)$, and $H_{n}$ acts faithfully on each of the two components. We analysed the structure of $H_{n}$, and found that $H_{n} \cong G_{n}$ in each case.

For $G_{3}^{l}$ and $G_{5}^{l}$ we verified immediately with the MAGMA function ChiefSeries that $G_{n}^{l} \cong H_{n}$, so $N_{n}$ is trivial.

For $G_{7}^{l}$, $G_{11}^{l}$, $G_{15}^{l}$ and $G_{19}^{l}$, the derived group $[G_{n}^{l}, G_{n}^{l}]$ acts decomposably with two components of dimension $d/2$. Since $H_{n}$ is perfect, this implies that $[G_{n}^{l}, G_{n}^{l}] \cong H_{n}$, and $G_{n}^{l} \cong N_{n} \times H_{n}$. By using Schreier generators, as described earlier, we were able to show that $|G_{n}^{l}: H_{n}| = 2$, so $G_{n}^{l} \cong 2 \times H_{n}$. Alternatively, the fact that $N_{n}$ is nontrivial and $G_{n}^{l} \cong N_{n} \times H_{n}$ enables us to deduce theoretically that $|N_{n}| = 2$, as follows. We saw in Section 6 that $L_{n} \cong \text{Hom}_{F}(M_2, M_1)$, where $L_{n}$ is the module for $H_{n}$ consisting of all matrices of the form 6.2. But $M_1$ and $M_2$ are isomorphic absolutely irreducible modules for $H_{n}$, and so the submodule of fixed points of $L_{n}$ under the action of $H_{n}$ corresponds to $\text{Hom}_{FH_{n}}(M_2, M_1)$ which has dimension 1 over $F$. Since $N_{n}$ clearly lies in the fixed point submodule in these examples, we conclude $|N_{n}| \leq 2$.

In the remaining examples, $G_{9}^{l}$, $G_{13}^{l}$ and $G_{17}^{l}$, the subgroup $N_{n}$ is much larger. For $G_{9}^{l}$ and $G_{13}^{l}$, we constructed in MAGMA the $FH_{n}$-module $L_{n}$ defined in Section 6, and then constructed the submodule generated by a few randomly chosen
elements of $N_n$ to prove that $|N_9| \geq 2^{24^2}$ and $|N_{13}| \geq 2^{96^2}$. For $G_{17}^l$, $L_n$ has dimension $384^2 = 147456$; although we could define this module in MAGMA, we were unable to construct submodules of $L_n$.

For $G_9^l$, we used the permutation representation of degree 98280 of Co$_1$ to obtain a presentation of $H_9 \cong$ Co$_1 \langle 2 \rangle$, which we could then use to prove that $|N_9| = 2^{24^2}$. We also applied an alternative approach to $G_9^l$, however, which proved more generally applicable, in particular to the other two examples. We first found generators for the subgroup $N_9.H_9'$ of index 2 in $G_9^l$, where $H_9' =$ Co$_1 \times$ Co$_1$. We then found that the restriction of the natural module $M$ for $G_9^l$ to $N_9.H_9'$ is decomposable with two isomorphic components of dimension $d/2 = 48$. Hence, by Lemma 6.1, $N_9.H_9'$ acts faithfully on each of these components, so we can restrict to the action on one of them. This restricted action is reducible with two irreducible constituents of degree $d/4 = 24$, from which it is clear that $|N_9| \leq 2^{24^2}$.

We were able to find the corresponding decomposition for $G_{17}^l$, and thereby deduce in the same way that $|N_{17}| \leq 2^{384^2}$, but in this case we could not find a lower bound for $|N_{17}|$. However, by the theory described in Section 6, $N_{17}$ is a submodule of the tensor product $M_2^* \otimes M_1$ for the direct product $\Omega^+(384,2) \times \Omega^+(384,2)$, where $M_1$ and $M_2$ are both equal to the natural module for $\Omega^+(384,2)$. Since this natural module is absolutely irreducible, it follows from Lemma 6.2 that $|N_{17}| = 2^{384^2}$. We can apply the same argument to $G_9^l$.

At first sight, it seems not possible to apply a similar argument to find an upper bound for $|N_{13}|$, since $H_{13}$ is semilinear rather than imprimitive. However, if we regard $G_{13}^l$ as a subgroup of GL(384,4) rather than of GL(384,2), then $H_{13}$ is imprimitive. We now find the analogous decomposition to that of $G_9^l$ and $G_{17}^l$, and so deduce that $N_{13}$ has dimension at most $96^2$ as a vector space over GF(4). But the GF(4)-dimension of $N_{13}$ is just the GF(4)-dimension of $N_{13} \otimes_F GF(4)$, which is equal to the dimension of $N_{13}$ over $F = GF(2)$, and so $|N_{13}| \leq 2^{96^2}$.

8 The existence of $\Gamma_n^*$-complexes

Parker constructed the representations of $U_n^*$ to allow further study of the $\Gamma_n^*$-complexes, so it is natural to ask whether our analysis of these representations implies the existence of these complexes for larger values of $n$.

Theorem 4 of [22] provides conditions sufficient for the construction of a $\Gamma_n$-complex from a known $\Gamma_{n-1}$-complex. Suppose that we have an epimorphism $\phi : U_n \to G$ for a finite group $G$ and let $H_i := \phi(\langle a, u_0, \ldots, u_i \rangle)$ for $1 \leq i \leq n$. Then the restriction of $\phi$ to $\langle a, u_0, \ldots, u_{n-1} \rangle$ induces a homomorphism $\psi : U_{n-1} \to H_{n-1}$. We call $\psi$ a $\Gamma_{n-1}$-map if $H_{n-1} \leq \text{Aut}(L)$ for some $\Gamma_{n-1}$-complex $L$, and
if certain other technical conditions are satisfied. Further \( \phi \) is a \( \Gamma_n \)-map if \( H_{n+1} \) is a core-free subgroup of \( G \) and \( H_{n+1} \cap H_{n+1}^{\phi(u_n)} = H_{n+2} \). Observe that \( H_{n+2} \) is always a subgroup of \( H_{n+1} \cap H_{n+1}^{\phi(u_n)} \); if \( H_{n+1} \) is a core-free subgroup of \( G \), then it cannot be normalized by \( \phi(u_n) \), so a sufficient condition for equality is that \( H_{n+2} \) is a maximal subgroup of \( H_{n+1} \). Corresponding assertions apply with \( U_n \) replaced by \( U_n^* \) and \( \Gamma_n \) by \( \Gamma_n^* \).

Let \( \psi_n : U_n \to U_{n+1} \) be the homomorphism induced by mapping each generator of \( U_n \) to the generator of \( U_{n+1} \) with the same name. If we denote Parker’s representations by \( \phi_n : U_n^* \to G_n \) and \( \psi_n^l : U_n^* \to G_n^l \), then it is immediately clear from the definitions of \( \phi_n \) and \( \phi_n^l \) in Section 2 that there are embeddings \( \psi_n^l : G_n \to G_{n+1}^l \) (n even) and \( \psi_n^l : G_n \to G_{n+1} \) (n odd) such that \( \phi_n \psi_n = \psi_n^l \phi_n \) (n even) and \( \phi_n \psi_n = \psi_n^l \phi_n^l \) (n odd).

Consider the case when \( n = 9 \). Theorem 6 of [22] shows that \( \psi = \phi_8 \) is a \( \Gamma_8 \)-map, \( H_8 = \psi(G_8) \) is a core-free subgroup of \( G_9^l \), and \( H_7 = \psi(G_7^l) = H_8 \cap H_8^{\phi(U_9)} \) since \( \psi(G_7^l) \) is a maximal subgroup of \( G_8 \). As Soicher comments at the end of Section 4 of [22], this shows that \( \phi = \phi_9^l \) is a \( \Gamma_9 \)-map, and establishes the existence of a \( \Gamma_9^* \)-complex with automorphism group containing \( G_9^l = 2^{24^2} \). (Co1 \( \cap \) 2).

Since \( \psi(G_8) \) is a maximal subgroup of \( G_9 \) (it is a complement in the extension \( 2^{24^2} \) (Co1 \( \cap \) 2) that acts irreducibly on the subgroup \( 2^{24^2} \)) and \( \psi(G_9^l) \) is clearly a core-free subgroup of the almost simple group \( G_{10} = \text{SL}(48, 2) \). 2, we deduce the existence of a \( \Gamma_{10}^* \)-complex with automorphism group containing \( \text{SL}(48, 2) \). 2.

However, as was pointed out to us by J.N. Bray, any intersection of two conjugates of \( \text{SL}(48, 2) \). 2 in \( G_{11}^{l1} = 2 \times \Omega^+(96, 2) \) that contains a subgroup \( 2^{24^2} \) (Co1 \( \cap \) 2) must necessarily contain the larger group \( 2^{24^2} \) (Sp(24, 2) \( \cap \) 2). Hence the condition \( H_9 = H_{10} \cap H_{10}^{\phi(U_{11})} \) does not hold, and so these methods cannot be applied to construct \( \Gamma_n^* \)-complexes for \( n > 10 \).

9 The presentations

We now briefly consider the finitely-presented groups \( U_n \) and \( U_n^* \). Soicher [22] proved that \( U_2 \cong L_3(2) : 2 \) and \( U_3 \cong (3 \times U_3(3)) : 2 \), and comments that “\( U_4 \) may in fact be infinite”.

We can confirm this. In 2005 Bernd Souvignier (private communication) exhibited a subgroup of \( U_4 \) having a free abelian quotient of dimension 4. He used the low-index subgroup algorithm [20, Section 5.6] to investigate subgroups of index 36 in the subgroup of \( U_4 \) of index 200 that maps onto \( U_3(3) \). The kernel \( K \) of the map of one of these subgroups onto a 2-quotient of order 2 has such
an abelianisation. Note that \( K \) has index 691200 in \( U_4 \); we have also found a subgroup of index 172800 in \( U_4 \) with infinite abelianisation.

It seems plausible that the homomorphism \( \nu_n \) from \( U_n \) to \( U_{n+1} \) defined in Section 8 is an embedding for all \( n \), which would imply that \( U_n \) is infinite for all \( n \geq 4 \). However we were not able to prove this. Neither did investigations of subgroups of low index in \( U_n \) for \( n \geq 5 \) yield a proof that they are infinite.

Of course \( U_n^* \) may also be infinite for sufficiently large \( n \geq 9 \), but again we failed to prove this. For \( n \geq 5 \), \( U_n \) and \( U_n^* \) have perfect derived group of index 2. For \( n > 8 \), the only finite homomorphic images of \( U_n^* \) of order greater than 2 that we could construct are those listed in Table 1; these do not provide subgroups of sufficiently low index to allow us to compute their abelianization. We established that the derived groups of \( U_9^* \), \( U_{10}^* \) and \( U_{11}^* \) have no simple homomorphic images of order up to \( 10^8 \).

References


Addresses:

Mathematics Institute
University of Warwick
Coventry CV4 7AL
Great Britain
e-mail: dfh@maths.warwick.ac.uk

Department of Mathematics
University of Auckland
Private Bag 92019
New Zealand
e-mail: obrien@math.auckland.ac.nz