Symmetric generation and existence of $J_3:2$, the automorphism group of the third Janko group

J.D. Bradley, R.T. Curtis *

School of Mathematics, University of Birmingham, Edgbaston, Birmingham B15 2TT, UK

Received 27 June 2005
Available online 28 February 2006
Communicated by Jan Saxl

Abstract

We make use of the primitive permutation action of degree 120 of the automorphism group of $L_2(16)$, the special linear group of degree 2 over the field of order 16, to give an elementary definition of the automorphism group of the third Janko group $J_3$ and to prove its existence. This definition enables us to construct the 6156-point graph which is preserved by $J_3:2$, to obtain the order of $J_3$ and to prove its simplicity. A presentation for $J_3:2$ follows from our definition, which also provides a concise notation for the elements of the group. We use this notation to give a representative of each of the conjugacy classes of $J_3:2$.

© 2006 Elsevier Inc. All rights reserved.

1. Introduction

The group $J_3$ was predicted by Janko in a paper in 1968 [10]. He considered a finite simple group with a single class of involutions in which the centraliser of an involution was isomorphic to $2^{1+4}:A_5$. The following year Higman and McKay, using an observation of Thompson that $J_3$ must contain a subgroup isomorphic to $L_2(16):2$, constructed the group on a computer [9]. Weiss constructed $J_3$ as the automorphism group of a graph with 17442 vertices [12]. This graph has diameter 10 and has a rather complicated structure.

* Corresponding author.
E-mail address: rtc@for.mat.bham.ac.uk (R.T. Curtis).
Kleidman and Wilson realised an embedding of $J_3$ into $E_6(4)$ [11], which was later proved without computers by Aschbacher [1]. More recently Baumeister has constructed $3J_3$ in terms of an amalgam [2].

In this paper we give a concise definition of $\text{Aut}(J_3) \cong J_3:2$. The minimum degree permutation representation for $J_3$ is 6156, and as complex matrices the minimum degree is 85 (170 for $J_3:2$). Our construction gives a much more concise way of recording elements of $J_3$.

Now $J_3$ possesses a triple cover $3J_3$ which has a 9-dimensional irreducible representation over $\mathbb{F}_4$, the field of order 4, see the ATLAS [6]. Our definition of $\text{Aut}(J_3)$ is shown to define either a group of order 100465920 containing a simple subgroup to index 2, or the cyclic group of order 2. The 9-dimensional representation is used to show that the former, in fact, holds.

We consider the (primitive) action of $\text{Aut}(L_2(16)) \cong L_2(16):4$ on 120 letters. We take $2^{*120} = \langle t_1, \ldots, t_{120} \mid t_i^2 = 1 \rangle$, the free product of 120 copies of the cyclic group of order 2, and construct a semi-direct product of the form $P = 2^{*120} \rtimes (L_2(16):4)$; as in Curtis [7,8], we refer to such an infinite group as a progenitor. The second author argued that $J_3:2$ is a homomorphic image of $P$ as follows. The normaliser of a Sylow 17-subgroup of $J_3:2$ is of the form $17 \times 8 \times 16 \times 15 \times 4$; the subgroup $N \cong L_2(16):4$ of $J_3:2$ contains a maximal subgroup isomorphic to $17 \times 8$ which must be contained in this normaliser, and so centralises an involution. Under conjugation by $N$ this involution thus has $\frac{17 \times 16 \times 15 \times 4}{17 \times 8} = 120$ images which, together with the maximal subgroup $N$, generate $J_3:2$. Indeed, the set of 120 involutions generates a subgroup of $J_3:2$ which is normalised by the whole group and which is not contained in $J_3$; thus it forms a generating set for $J_3:2$. Now elements of $P$ can be written, essentially uniquely, in the form $\pi w$ where $\pi$ is a permutation in $N$ and $w$ is a word in the 120 symmetric generators; thus any relator by which we might factor $P$ has this form. We produce below an easily described relator, found by John Bray, such that

$$G = \frac{P}{\langle \pi w \rangle^P} \cong J_3:2,$$

where $\langle \pi w \rangle^P$ denotes the normal closure of the subgroup $\langle \pi w \rangle$.

The subgroup $N \cong L_2(16):4$ has index 6156 in $J_3:2$. We are able to construct a graph of rank 7 on 6156 vertices by joining a coset $Nw$ of $N$ to the 120 cosets $Nw_i$, assuming the above relator holds (and, of course, all of its conjugates by permutations of $N$). This shows that $G$ has order at most $6156 \times |L_2(16):4|$. It is shown that this graph has diameter 3, so we can represent elements of $J_3:2$ by an element of $L_2(16):4$ followed by a word in the 120 symmetric generators of length at most 3.

2. $L_2(16):4$ and its action on 120 letters

In what follows we shall be defining and constructing a group which contains a set $T$ of 120 involutions whose set normaliser $N$ is isomorphic to $\text{Aut}(L_2(16)) \cong L_2(16):4$ acting primitively on $T$ by conjugation. We shall need to understand this 120 point action in some detail.
Table 1
The permutation character of degree 120

<table>
<thead>
<tr>
<th>Centraliser</th>
<th>16320</th>
<th>64</th>
<th>60</th>
<th>30</th>
<th>15</th>
<th>17</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>A</td>
<td>2A</td>
<td>3A</td>
<td>5AB</td>
<td>15ABCD</td>
<td>17ABCD</td>
<td>17EFGH</td>
</tr>
<tr>
<td>Fixed points</td>
<td>120</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Shape</td>
<td>1^{120}</td>
<td>18.2^{56}</td>
<td>3^{40}</td>
<td>5^{24}</td>
<td>15^{8}</td>
<td>1.177</td>
<td>1.177</td>
</tr>
</tbody>
</table>


To obtain a copy of the field of order 16 we extend the prime field \( \mathbb{Z}_2 \) by a root, \( \nu \) say, of the irreducible quartic \( x^4 + x + 1 \). Thus we let \( F = \mathbb{Z}_2(\nu) \cong \mathbb{Z}_2[x]/(x^4 + x + 1) \). We let \( \sigma \) be the field automorphism of order 4 which maps each element of \( F \) to its square. We represent each element of \( N \cong L_2(16) : 4 \) by a \( 2 \times 2 \) matrix of determinant 1 with entries from \( F \), followed by a power of \( \sigma \). Let the set of Sylow 17-subgroups of \( N \) be denoted by \( S \). Then \( |S| = 120 \) and \( N \) acts primitively, by conjugation, on \( S \). In order to obtain a convenient notation for the members of \( S \) we proceed as follows. For each \( H \in S \) we choose the unique element \( \pi_H \in H \) which, when it acts on the projective line \( P^1(16) \), maps \( \infty \) to 0. We label \( H \) by the ordered pair \((0^{\pi_H},0^{\pi_2})\). The group \( N \) is sharply 3-transitive on \( P^1(16) \), so this pair defines the subgroup uniquely.

The normaliser of one such Sylow 17-subgroup has shape 17:8. Inducing the trivial character of this subgroup up to \( N \) (or equivalently, writing down for an element of each conjugacy class of \( N \) the number of Sylow 17-subgroups it normalises) we obtain the permutation character shown in the Table 1, where the classes are labelled as in the ATLAS [6].

This permutation character has norm 4 and using it we may readily write down the cycle shapes of elements in the 120-point action. In particular we see from Table 1 that elements of order 8 have cycle shape \( 1^2.2.4.8^{14} \) and that all fixed point free elements are semi-regular, i.e. their cycles all have the same length.

Since elements of order 8 have two fixed points we see that one of the nontrivial orbits of the point stabiliser has length 17, and since the other two have lengths of the form \( 2^a.17 \) they must contain 34 and 68 points. We say that 2 points are \( \alpha \)-joined, \( \beta \)-joined or \( \gamma \)-joined according to whether they lie in the 17-, 34- or 68-orbits of one another’s stabiliser. In Fig. 1 we give a diagram of the resulting \( \alpha \)-graph, indicating the orbit lengths of the stabiliser of a point in each of the four suborbits. Thus, for instance the stabiliser of two points \( x \) and \( y \) which are \( \beta \)-joined to one another has an orbit of length 4 on points \( \alpha \)-joined to both \( x \) and \( y \), three orbits of length 4 on points \( \gamma \)-joined to \( x \) and \( \alpha \)-joined to \( y \), and a unique point \( \beta \)-joined to \( x \) and \( \alpha \)-joined to \( y \). Now an element of order 8 lying in our point stabiliser must, by simple arithmetic, act on these suborbits as

\[
1 + (1 + 8^2) + (2 + 8^4) + (4 + 8^8)
\]

and so points in its 2-orbit must be \( \beta \)-joined to its fixed points and points in its 4-orbit must be \( \gamma \)-joined to its fixed points. This shows us that the subgraph on \{a, b, c, d, e, f, g, h\},

...
Fig. 1. The graph on 120 letters.

Fig. 2. The fix of an involution.

the fixed point set of an involution, has form consisting of 4 $\alpha$-edges $ab, cd, ef$ and $gh$ and otherwise points in the same half are $\beta$-joined whilst those in opposite halves are $\gamma$-joined, see Fig. 2. An element of order 8 whose 4th power has this fixed point set acts as $(a)(b)(c d)(e g f h)$. By considering the number of involutions and the number of pairs of points each fixes, we can see that every pair of points is fixed by a unique involution. Let us consider how the centraliser of an involution acts on its fixed point set. The normaliser of a Sylow 17-subgroup contains no Klein fourgroup and so commuting involutions cannot fix the same point. Thus the fixed point sets of commuting involutions are disjoint, and the fixed point sets of the 15 involutions in a Sylow 2-subgroup of $N \cong L_2(16)$ cover the 120 points. In particular every element of the elementary abelian subgroup of order 16 must act trivially or with cycle shape $2^4$ on our fixed point set. So without loss of generality the action of the centraliser of an involution in $N'$ on its fixed point set is given by:

$$\{(a b)(c d)(e f)(g h), (a c)(b d)(e g)(f h), (a e)(b f)(c g)(d h), (c d)(e g f h)\}.$$  

We now prove a lemma which we shall use in the next section.

**Lemma 1.** The group $N$ is transitive on ordered triples of the form $(a, b, c)$ where $b$ is $\alpha$-joined to $a$ and $c$, and $a$ is $\gamma$-joined to $c$. In particular there is an element which fixes $b$ and interchanges $a$ and $c$. This element must be an involution.

**Proof.** The group $N$ is transitive on $\gamma$-joined edges. A pair of $\gamma$-joined points, $(a, c)$ say, is fixed by a unique involution, $\pi$ say. From Fig. 1 we can see that there are two points, $b$ and $b'$ say, $\alpha$-joined to both $a$ and $c$. From Fig. 2 and Table 1 we see that no nontrivial element of $N$ fixes such a configuration, and so the involution fixing $a$ and $c$ must interchange $b$
and \( b' \). Hence \( N \) is transitive on triples such as \( a, b, c \). Similarly, the element, \( \rho \) say, which fixes \( b \) and interchanges \( a \) and \( c \) must be an involution since \( \rho^2 \) fixes \( a, b \) and \( c \).

3. The progenitor and relation

As in Curtis [7,8] we let \( m^n \) denote a free product of \( n \) copies of the cyclic group \( C_m \); that is, a group generated by \( n \) elements of order \( m \) with no other relation holding between them. In this paper we are only concerned with the case \( m = 2 \) and so have

\[
2^n \cong \langle t_1, t_2, \ldots, t_n \mid t_i^2 = 1 \rangle.
\]

A permutation of the \( n \) symmetric generators will clearly induce an automorphism on this free product. (In more generality, if \( m > 2 \) we would consider monomial automorphisms which permute the symmetric generators while raising them to powers co-prime to their order.) If \( N \) is a group of permutations of the set \( \{1, 2, \ldots, n\} \) then we may form a group

\[
2^n : N,
\]
a split extension of \( 2^n \) by \( N \) in which \( t_i^\pi = t_i^\pi \) for \( \pi \in N \). We call the infinite group \( P \) a progenitor. We note that every element of \( P \) can be written, essentially uniquely, in the form \( \pi w \), where \( \pi \in N \) and \( w \) is a word in the symmetric generators. Thus any homomorphic image of \( P \) can be written in the form

\[
\frac{P = 2^n : N}{\pi_1 w_1, \pi_2 w_2, \ldots}.
\]

From our observations in Section 1 we see that \( J_3:2 \) is an image of \( P = 2^{120}: (L_2(16):4) \). We factor this group by a single relation found by John Bray to obtain the group \( G \). We then find an upper bound on the size of \( G \) by enumerating the cosets of \( N \cong L_2(16):4 \) in \( G \). In Section 5 we argue that \( G \) must either have that order or be a cyclic group of order 2. In Section 6 we exhibit a group of order greater than 2 with \( G \) as an image. Section 4 involves a great deal of calculation involving the group \( L_2(16):4 \) as a permutation group on 120 letters. Whilst these calculations, if one had the requisite patience, could be done by hand, we use the computer package MAGMA, see [5], to operate within \( L_2(16):4 \).

The relation by which we factor \( P \) involves an element of order 12 in \( L_2(16):4 \). As in Table 1, any element of order 12, \( \mu \) say, has cycle shape \( 12^{10} \) when acting on 120 points; it turns out that one of the cycles is unique in having the property that if \( i \) is a point in the cycle, \( i \) is \( \alpha \)-joined to \( i^\mu \) and \( \gamma \)-joined to \( i^{\mu^2} \). The relation says that an element, \( \mu \), of order 12 in \( L_2(16):4 \) multiplied by a symmetric generator, \( t_i \), in the unique cycle described above has order 5, i.e. \( (\mu t_i)^{5} = 1 \). We note that although elements of order 12 in \( L_2(16):4 \) are not conjugate to their inverses, using \( \sim \) to mean ‘has the same order as,’ we have \( \mu t_i \sim (\mu t_i)^{-1} = t_i \mu^{-1} \sim \mu^{-1} t_i \); so we may choose \( \mu \) from either of the conjugacy classes of elements of order 12.
The element
\[
\begin{pmatrix}
1 & 1 \\
1 & 0
\end{pmatrix}
\]
of \(L_2(16)\) has order 3 and clearly commutes with the field automorphism \(\sigma\), so
\[
\begin{pmatrix}
1 & 1 \\
1 & 0
\end{pmatrix} \sigma
\]
has order 12. It can be checked that the Sylow 17-subgroup we denote by \((\nu, \nu^7)\) lies in the appropriate cycle. Therefore the theorem we seek to prove is:

**Theorem 1.**

\[
G \cong \frac{2^{*120} \cdot (L_2(16) : 4)}{\left(\frac{11}{16}\right)^5 \sigma t_{(\nu, \nu^7)}} \cong J_3; 2.
\]

The first step of the proof is to find an upper bound for the number of cosets of \(N \cong L_2(16) : 4\) in \(G\).

### 4. Coset enumeration and the graph

A full manual enumeration of the cosets of \(N \cong L_2(16) : 4\) in \(G\) can be found in Bradley [3] but, since it is a fairly long and involved calculation, it would not be illuminating to reproduce it in full here. Instead we describe the general method, prove two lemmas which illustrate this method and list some of the properties of the graph we obtain as a result of the enumeration. In Section 9 we describe how the enumeration was done separately by machine.

We note, as in the previous section, that an element of \(G\) can be written in the form \(\pi w\) where \(\pi \in N\) and \(w\) is a word in the symmetric generators, although when we are dealing with an image of \(P\) this notation is no longer unique. Hence a coset of \(N\) can be written as \(N\pi w = Nw\). In the enumeration we consider all double cosets of the form \(NgN\) for \(g \in N\); by the above these take the simple form \(NwN\). For each double coset \(NwN\), we find how many single cosets of \(N\) it contains and show that for any symmetric generator \(t_i\) the coset \(N\nu t_i\) is in a double coset we have already considered. We obtain a Cayley graph by joining the coset \(Nw\) to the 120 cosets \(N\nu t_i\) for \(t_i\) a symmetric generator. When the graph is closed we have shown that \(G\) is finite and have an upper bound for its order.

**Lemma 2.** Let \(t_a\) and \(t_b\) be two \(\alpha\)-joined symmetric generators, and let \(t_c, t_d, t_e, t_f, t_g\) and \(t_h\) be the other 6 symmetric generators fixed by the unique involution in \(N\) which fixes \(t_a\) and \(t_b\) in the notation of Fig. 2. Then the double coset \(Nt_a t_b N\) contains at most 510 single
cosets of \( N \) and the coset \( Nt_\alpha t_\beta \) is fixed under right multiplication by a subgroup of \( N \) of order 32. Furthermore

\[
Nt_\alpha t_\beta = Nt_\beta t_\alpha = Nt_c t_d = Nt_d t_c.
\]

**Proof.** We start with the relation \((\mu t_j)^5 = 1\) which we described above. We multiply this out to get \( t_i t_j t_k t_l t_m = \mu^5 \), where \( t_j = t_i^\mu \), \( t_k = t_j^\mu \), etc. We can rearrange this to find \( t_i^{\mu^7} t_m^{\mu^7} t_i t_j t_k = \mu^5 \). As described above, \( t_i \) and \( t_j \) are \( \alpha \)-joined, as are \( t_j \) and \( t_k \), whereas \( t_i \) and \( t_k \) are \( \gamma \)-joined. By Lemma 1 we can find an involution \( \rho \) which fixes \( t_j \) and interchanges \( t_i \) and \( t_k \). If we conjugate by this we find that \( t_k t_j t_i t_l t_m = (\mu \rho)^5 \in N \). If we multiply this by the rearrangement of our original relation we find \( t_i^{\mu^7} t_m^{\mu^7} t_i^{\rho} t_l^{\rho} t_m = (\mu \rho)^5 \in N \).

By construction the first two of these are \( \alpha \)-joined, as are the latter two. If we let \( t_a \) and \( t_b \) denote \( t_i^{\mu^7} \) and \( t_m^{\mu^7} \), respectively, then \( t_a \) and \( t_b \) lie in the fixed point set of a unique involution, \( \pi \) say. When we calculate \( t_i^{\rho} \) and \( t_m^{\rho} \) it turns out that they are \( t_c \) and \( t_d \). We have the relation \( t_a t_b t_c t_d = (a b)(c d) \), by which we mean an element of order 4 acting as \( (a b)(c d) \) on the fixed point set. If we consider an element of order 8 which fixes \( t_a \) and \( t_b \) and has 4th power equal to \( \pi \), then it must preserve the fixed points of \( \pi \). Then since it fixes no other points than \( t_a \) and \( t_b \), by consideration of the joins in the fixed point set of \( \pi \) it must interchange \( t_c \) and \( t_d \). Thus we have \( Nt_\alpha t_\beta = Nt_\beta t_\alpha = Nt_c t_d = Nt_d t_c \). The involution \( \pi \) is centralised by a subgroup of \( N \) of order 64. All these elements will preserve the fixed point set of \( \pi \) and half will preserve the set \{a, b, c, d\}. Hence \( Nt_\alpha t_\beta \) will be stabilised by a subgroup of \( N \) of order 32. This means that the double coset \( Nt_\alpha t_\beta N \) will contain at most \( \frac{16,320}{32} = 510 \) single cosets of \( N \). \( \square \)

**Lemma 3.** Let \( t_b \) and \( t_c \) be two \( \beta \)-joined symmetric generators, and let \( t_a, t_d, t_e, t_f, t_g \) and \( t_h \) be the other 6 symmetric generators fixed by the unique involution in \( N \) which fixes \( t_a \) and \( t_b \) in the notation of Fig. 2. Then the double coset \( Nt_b t_c N \) contains at most 2040 single cosets of \( N \) and the coset \( Nt_b t_c \) is fixed under right multiplication by a subgroup of \( N \) of order 8. Furthermore \( Nt_b t_c = Nt_b t_d \).

**Proof.** From above we have \( t_a t_b t_c t_d = (a b)(c d) \). Multiplication by \( t_a \) gives \( t_b t_c t_d = t_a (a b)(c d) = (a b)(c d) t_b \) and so we have \( t_b t_c t_d t_b = (a b)(c d) t_b \) and we so have \( t_b t_c t_d t_b = (a b)(c d) \in N \) or

\[
Nt_b t_c = Nt_b t_d.
\]

This coset is fixed under right multiplication by the subgroup of the centraliser of \( \pi \) which commutes with \( t_b \), a group of order 8. Hence the double coset \( Nt_b t_c N \) will contain \( \frac{16,320}{8} = 2040 \) single cosets of \( N \).

Continuing in this manner we obtain the collapsed Cayley diagram of the graph as shown in Fig. 3. The graph indicates that there are at most 6156 cosets of \( N \) inside \( G \) and so

\[
|G| \leq 16320 \times 6156 = 100,465,920 = |J_3:2|.
\]
The numbers around each double coset represent the orbits of a stabiliser of a single coset on the 120 symmetric generators. We now list some of the properties of the graph which emerge from the enumeration.

The cosets in the orbit of length 2720 are of the form \( Nt_a t_e \) where \( t_a \) and \( t_e \) are \( \gamma \)-joined symmetric generators. In this case the coset is stabilised by a subgroup of \( N \) isomorphic to \( S_3 \) and there are 3 names for the coset. These names and the \( S_3 \) which stabilises the coset are not as easy to describe as in the previous two cases, but a description can be found in Bradley [3].

The cosets in the 680 orbit are fixed by one of the 680 subgroups of \( N \) of the form 12:2, the normaliser of an element of order 12.

The cosets in the orbit of length 85 are of the form \( Nt_a t_c \) where \( t_a \) and \( t_c \) are \( \beta \)-joined symmetric generators. If we take the unique involution \( \pi \) which stabilises \( a \) and \( c \) then \( C_N(\pi) \) contains a normal subgroup isomorphic to the Klein fourgroup \( V_4 \) containing \( \pi \). The normaliser of this \( V_4 \) in \( N \) is of order 192 and is the stabiliser of the coset \( Nt_a t_c t_a \).

Referring again to Fig. 2, if we take any of the 3 involutions in this \( V_4 \) fixing \( x \) and \( y \) say with \( x \) and \( y \) \( \beta \)-joined we have \( Nt_a t_c t_a = Nt_x t_y t_x \), giving us 48 names for the coset. \( \square \)

5. Existence of \( J_3 \)

Lemma 4. Either \( G \) is a group of order 100,465,920 containing a simple subgroup of index 2, or \( G \) is the cyclic group of order 2.

Proof. We consider the possibility that a relation which we have not yet discovered holds in \( G \). If any relation holds we can put it in the form \( \pi w = 1 \), where \( \pi \in N \) and \( w \) is a word in the symmetric generators. From Fig. 3 we know that the length of \( w \) is at most 3.
The progenitor \( P \) has a normal subgroup consisting of elements of \( L_2(16):2 \) multiplied by a word of even length in the symmetric generators and elements of \( L_2(16):4 \) \( \setminus \) \( L_2(16):2 \) multiplied by a word of odd length in the symmetric generators. The element \( \mu t_i \) whose fifth power we factor by lies in this normal subgroup, and so any relator \( \pi w \) which is implied must also lie in this subgroup.

Firstly we consider the case that a nontrivial element \( \pi \in L_2(16):2 \) is set equal to the identity. Then the simple group \( L_2(16) \) must collapse to the identity, and since this group is transitive on the symmetric generators these must all be equal to each other. Then our relation \((\mu t_i)^5 = 1\) says that \( t_i^5 = t_i = \mu^5 \in L_2(16):4 \setminus L_2(16):2 \), so we have \( G \cong C_2 \).

The next case to consider is if \( \pi t_a = 1 \) for some \( \pi \in L_2(16):4 \setminus L_2(16):2 \). Then \( \pi \in C_N(C_N(t_a)) \) which is trivial, so some collapse must occur in \( N \) and we are in the above case with \( G \cong C_2 \).

Thirdly, if \( \pi t_a t_b = 1 \) for some \( \pi \in L_2(16):2 \) then we have \( Nt_a = Nt_b \) and since the subgroups of \( N \) stabilising these cosets are distinct and maximal we have \( t_x t_y \in N \forall x, y \). The relation now tells us that \( t_1 t_i \mu t_i \mu^2 t_i \mu^3 t_i \mu^4 \in N \) and hence \( t_i \in N \) so we are in the second case and \( G \cong C_2 \).

Lastly, there is the case that \( \pi t_a t_b t_c = 1 \) for some \( \pi \in L_2(16):4 \setminus L_2(16):2 \). From Fig. 3 we see that the coset \( Nt_a t_b t_c = Nt_{a'} t_{b'} t_{c'} \) where \( a' \) and \( b' \) are \( y \)-joined, so without loss of generality we may assume that \( a = y \)-joined to \( b \). We have \( Nt_a t_b = Nt_c \), now the stabiliser of \( Nt_a t_b \) is of order 6 and the stabiliser of \( Nt_c \) is maximal and 3 does not divide its order. So \( Nt_c \) is stabilised by the whole of \( N \) and we are in the above case with \( G \cong C_2 \).

We have now proved the lemma since we have shown that either we found all the relations which hold in \( G \) in our enumeration of the cosets and \( |G| = 100,465,920 \), or other relations hold and \( G \cong C_2 \). The subgroup of index 2 we described must be simple since if any further relation is imposed on it, it collapses to the trivial group.

So if we can find a group, not isomorphic to \( C_2 \), which is an image of \( G \) we have proved the existence of a simple group of order 50,232,960. By the classification of finite simple groups this must be the group \( J_3 \).

6. A presentation for \( J_3:2 \)

John Bray (unpublished) obtained the following presentation for the automorphism group of the special linear group \( SL_2(16) \):

\[
\langle x, y, z \mid x^{17} = y^8 = 1, \ x^y = x^2, \ z^2 = (xyz)^4 = (xz)^{17} = 1, \ y^5 = y^6 \rangle.
\]

We can check that the following elements of \( L_2(16):4 \) satisfy the presentation:

\[
x = \begin{pmatrix} 0 & \nu^{10} \\ \nu^5 & \nu^4 \end{pmatrix}, \quad y = \begin{pmatrix} \nu^9 & 0 \\ \nu^4 & \nu^6 \end{pmatrix}, \quad z = \begin{pmatrix} 1 & 0 \\ \nu^4 & 0 \end{pmatrix},
\]

where \( \nu \) is the primitive element of \( F \cong GF(16) \) defined in Section 2, and \( \sigma \) is the field automorphism which squares every element of \( F \). It is readily verified that the subgroup \( \langle x, y \rangle \), which is visibly isomorphic to the Frobenius group of order 17 \( \times \) 8, has index 120; so the presentation does indeed define \( L_2(16):4 \). In fact \( x \) and \( y \) generate the normaliser...
of the Sylow 17-subgroup which we denote by \((\nu, \nu^7)\) and \(z y x^{-3} = (1 1 0) \sigma\), the desired element of order 12. This leads to the following presentation for \(G\):

\[
G \cong \langle x, y, z, t \mid x^{17} = y^8 = 1, \ x^z = x^2, \ z^2 = (xyz)^4 = (xz)^{17} = 1, \ y^z = y^5, \ t^2 = [t, x] = [t, y] = (z y x^{-3} t)^5 = 1 \rangle.
\]

By Lemma 4, if we can find elements which satisfy this presentation and generate a group bigger than \(C_2\), then we have proved that \(G \cong J_3:2\). We use the construction of \(3 \cdot J_3:2\) given in the ATLAS [6, p. 82]. The group \(3 \cdot J_3\) is given as a group of 9-dimensional matrices over the field \(\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}\). We denote the basis of the 9-dimensional vector space by \(\{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8, e_9\}\). The subspace spanned by \(\langle \bar{\omega} e_i + \omega e_i + 1 \mid i \in 0, 1, 4, 5 \rangle\) is preserved by a subgroup isomorphic to \(L_2(16):2\). We let \(\tau\) denote the element \(F_1\) from the construction. Then \(\tau\) is an involution in the outer half of \(3 \cdot J_3:2\). Conjugation by \(\tau\) corresponds to conjugation by the permutation matrix corresponding to the permutation \((e_1 e_3)(e_2 e_6)(e_5 e_7)\) followed by the field automorphism of \(\mathbb{F}_4\). Consider the following elements:

\[
X = \begin{pmatrix}
\omega & \omega & 0 & \bar{\omega} & \bar{\omega} & 0 & 0 & \bar{\omega} & 0 \\
\omega & \omega & 0 & 1 & 0 & \bar{\omega} & \bar{\omega} & 0 & 0 \\
\bar{\omega} & 0 & 0 & 0 & \bar{\omega} & 0 & 0 & \bar{\omega} & 0 \\
\omega & 0 & 0 & 0 & \omega & 0 & 0 & \bar{\omega} & 0 \\
\omega & 1 & \bar{\omega} & \omega & \bar{\omega} & 0 & 0 & \bar{\omega} & 0 \\
0 & \bar{\omega} & \omega & \omega & \omega & 1 & 1 & 1 & 1 \\
\bar{\omega} & 0 & 1 & \bar{\omega} & 1 & 1 & 0 & \bar{\omega} & 1 \\
\omega & 1 & \bar{\omega} & 0 & \bar{\omega} & 0 & 0 & \omega & 0 \\
0 & \omega & 0 & 0 & 0 & 0 & 0 & \bar{\omega} & 1 \\
\end{pmatrix},
\]

\[
Y = \begin{pmatrix}
0 & \bar{\omega} & \omega & 0 & 1 & \bar{\omega} & 0 & \bar{\omega} & 0 \\
0 & 0 & 0 & 1 & \omega & 1 & 1 & \omega & 0 \\
1 & 1 & 0 & \bar{\omega} & 1 & \bar{\omega} & 0 & 1 \\
1 & 1 & \bar{\omega} & \omega & \bar{\omega} & \omega & 0 & 0 \\
\omega & 1 & \bar{\omega} & \bar{\omega} & \bar{\omega} & 0 & 1 & 0 \\
0 & \bar{\omega} & 0 & 0 & 1 & 0 & \bar{\omega} & 0 \\
\bar{\omega} & \omega & 0 & \omega & 1 & 0 & \bar{\omega} & 0 \\
0 & 1 & 0 & 0 & 0 & \bar{\omega} & 0 & 1 & 0 \\
\end{pmatrix},
\]

\[
Z = \begin{pmatrix}
1 & 1 & 0 & 0 & 0 & \bar{\omega} & 0 & 0 & 0 \\
1 & 1 & \bar{\omega} & 0 & 0 & 0 & 0 & \omega & 0 \\
0 & \omega & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \bar{\omega} & \omega & \omega & 0 \\
\omega & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \omega & 0 & 0 & \bar{\omega} & \bar{\omega} \\
0 & 0 & 0 & \bar{\omega} & 0 & \omega & 1 & 0 & 1 \\
0 & 0 & 0 & \bar{\omega} & 0 & \omega & 0 & 1 \\
\end{pmatrix}.
\]
These satisfy the presentation, apart from the final relation. We find $(Z Y X^{-3} T)^5 = \omega I$, where $I$ is the identity matrix. So if we factor by the group of scalar matrices, which has order 3, we have an image of $G$ bigger than $C_2$ and so we have proved Theorem 1. In fact, as in Lemma 4, we have proved—essentially by hand—that the group generated by the displayed matrices (or more properly semi-linear maps) has order $3 \times 100,465,920$ and contains to index 2 a perfect subgroup with centre of order 3, whose quotient by that centre is simple.

7. Elements of $J_3:2$

The construction of $J_3:2$ given in this paper gives us a very concise way of denoting elements of the group. An element of $J_3:2$ can be written as an element of $L_2(16):4$ followed by a word of length at most 3 in the symmetric generators. Since elements of $L_2(16):4$ can be written as $2 \times 2$ matrices followed by a power of the field automorphism our notation for elements is considerably shorter than the minimum degree permutation representation of degree 6156, the minimum degree complex matrix representation of degree 170 and even more concise than as $36 \times 36$ matrices over $GF(3)$. In Bradley [3] a MAGMA [5] program is given for multiplying symmetrically presented elements of $J_3:2$ together. The program also provides a way of switching between symmetrically presented elements of $J_3:2$ and permutations on 6156 letters, so all MAGMA functions relating to permutation groups can be used.

In Table 2 we give an element of each conjugacy class of $J_3:2$, demonstrating the conciseness of our new notation for elements of the group.

8. Centralisers of involutions

The group $J_3$ was originally defined in terms of the centraliser of an involution. In this section we give generators for the subgroups of $G \cong J_3:2$ which centralise involutions occurring naturally in our symmetric presentation. During the enumeration of cosets in Bradley [3, p. 52] we find that, in the notation of Fig. 2, $t_a^c = t_d^b$. We use this fact twice in this section.

If we take an involution, $\pi$ say, in $N' \cong L_2(16)$ then it is in the simple group $G' \cong J_3$. This means the centraliser in $J_3$ is of the form $2^{1+4}:A_5$ and the centraliser in $J_3:2$ has form
Table 2
The conjugacy classes of $J_3$:

<table>
<thead>
<tr>
<th>Class</th>
<th>Representative</th>
<th>Class</th>
<th>Representative</th>
<th>Class</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>1A</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})$</td>
<td>10A</td>
<td>$(\begin{pmatrix} 5 \ 1 \ 1 \ 0 \end{pmatrix})\sigma^2$</td>
<td>8B</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})\sigma^2t(\nu, v, v^5)$</td>
</tr>
<tr>
<td>2A</td>
<td>$(\begin{pmatrix} 0 \ 1 \ 0 \ 0 \end{pmatrix})$</td>
<td>10B</td>
<td>$(\begin{pmatrix} 5 \ 1 \ 5 \ 1 \ 0 \end{pmatrix})\sigma^2$</td>
<td>8C</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})\sigma$</td>
</tr>
<tr>
<td>3A</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})$</td>
<td>12A</td>
<td>$t_{(1,0)}t_{(1,0,2)}$</td>
<td>12B</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})\sigma$</td>
</tr>
<tr>
<td>3B</td>
<td>$(\begin{pmatrix} 0 \ 1 \ 0 \ 0 \end{pmatrix})t_{(1,0)}t_{(1,0,2)}$</td>
<td>15A</td>
<td>$(\begin{pmatrix} 7 \ 1 \ 1 \end{pmatrix})$</td>
<td>18A</td>
<td>$(\begin{pmatrix} 3 \ 1 \ 0 \end{pmatrix})_{1,0}v$</td>
</tr>
<tr>
<td>4A</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma^2$</td>
<td>15B</td>
<td>$(\begin{pmatrix} 14 \ 1 \ 0 \end{pmatrix})$</td>
<td>18B</td>
<td>$(\begin{pmatrix} 3 \ 1 \ 0 \end{pmatrix})_{1,0}v^4$</td>
</tr>
<tr>
<td>5A</td>
<td>$(\begin{pmatrix} 0 \ 1 \ 0 \end{pmatrix})\sigma^2$</td>
<td>17A</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})$</td>
<td>18C</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})t_{(1,0)}$(v)</td>
</tr>
<tr>
<td>5B</td>
<td>$(\begin{pmatrix} 0 \ 1 \ 0 \end{pmatrix})\sigma^2$</td>
<td>19A</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma t_{(1,0,8)}$</td>
<td>24B</td>
<td>$(\begin{pmatrix} 1 \ 0 \ 0 \end{pmatrix})t_{(1,0,3)}$</td>
</tr>
<tr>
<td>6A</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})$</td>
<td>19B</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma t_{(1,0,9)}$</td>
<td>34A</td>
<td>$(\begin{pmatrix} 3 \ 1 \ 0 \end{pmatrix})_{1,0,2,0,5}$</td>
</tr>
<tr>
<td>8A</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma t_{(1,0,5)}$</td>
<td>2B</td>
<td>$t_{(1,0)}$</td>
<td>34B</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})t_{(1,0,14,0,8)}$</td>
</tr>
<tr>
<td>9A</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma t_{(1,0,9)}$</td>
<td>4B</td>
<td>$\sigma$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9B</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma t_{(1,0,9)}$</td>
<td>6B</td>
<td>$(\begin{pmatrix} 1 \ 0 \end{pmatrix})\sigma^2t_{(1,0)}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$2^{1+4}:S_5$. As in Section 2, $\pi$ will commute with 8 symmetric generators; these elements generate the whole centraliser of $\pi$, i.e.

$$C_G(\pi) = \langle t_a, t_b, \ldots, t_h \rangle.$$

Consider the involution $\sigma^2$ in $G'$. Since all involutions in $J_3$ are conjugate we know $C_G(\sigma^2) \cong C_G(\pi) \cong 2^{1+4}:S_5$. The element $\sigma^2$ fixes the subfield of $F$ of order 4 so commutes with $L \cong L_2(4)$, a subgroup of $N$. Now $\sigma^2$ acts fixed point free on the symmetric generators and conjugates each symmetric generator into a symmetric generator to which it is $\beta$-joined. Then if $t_a^{\sigma^2} = t_c$, in the notation of Fig. 2, $t_a$ and $t_c$ must lie in the fixed point set of a unique involution, which must therefore commute with $\sigma^2$; hence its fixed point set is preserved by $\sigma^2$ and so $t_b^{\sigma^2} = t_d$. Then $(t_At_Bt_A)^{\sigma^2} = t_Bt_Bt_C = t_at_Bt_A$ by the first paragraph of this section. Hence $t_at_Bt_A \in C_G(\sigma^2)$, and we have

$$C_G(\sigma^2) = \langle L, t_a^{\sigma} \rangle.$$

We also consider the centraliser of a symmetric generator $t_a$, once more using the notation of Fig. 2. This commutes with a subgroup of $G'$ isomorphic to $L_2(17)$, so $C_G(t_a) \cong L_2(17) \times 2$. Let $\rho \in N$ conjugate $t_a$ into a symmetric generator $\beta$-joined to $t_a$, so $t_a^\rho = t_d$ say. Now $t_a$ and $t_d$ lie in the fixed point set of a unique involution so, as in Fig. 2, $t_b$ and $t_c$ are well defined. Consider $t_a^{\rho}t_Bt_C = t_Ct_Dt_Bt_C = t_Et_At_Et_C$, since $t_a^c = t_d^b$, hence $t_a^{\rho}t_Bt_C = t_a$. Now $C_N(t_a) \cong 17:8$ is maximal in $C_G(t_a) \cong L_2(17) \times 2$, and so we have

$$C_G(t_a) = \langle C_N(t_a), \rho t_Bt_C \rangle.$$
9. Mechanical enumeration of the double cosets of $N$ in $G$

In order to illustrate the manner in which the above enumeration of double cosets can be performed using the double coset enumerator described in Bray and Curtis, see [4], we include the required input and relevant parts of the output. Thus

```plaintext
> n<x,y,z>:=Group<x,y,z|x^17=y^8=z^2=1,x^y=x^2,y^z=y^5,
> (x*y*z)^4=(x*z)^17=1>;
> h:=sub<n|x,y>;
> Index(n,h);
120

As in Section 6 the group $\text{Aut}(\text{L}_2(16)) \cong \text{L}_2(16):4$ is defined in terms of three generators $x$, $y$ and $z$, such that $h = \langle x, y \rangle$ is a Frobenius group of order $17 \times 8$. The index of 120 is confirmed by the coset enumerator in MAGMA [5].

```plaintext
> f,n120,k:=CosetAction(n,h);
> xp:=f(x);yp:=f(y);zp:=f(z);
> N:=n120;
> zp*yp*xp^-3;
(1, 21, 63, 36, 50, 44, 30, 114, 102, 40, 39, 2)
(3, 66, 53, 24, 77, 92, 67, 9, 41, 104, 97, 13)
(4, 15, 18, 98, 84, 26, 11, 86, 91, 82, 101, 6)
(5, 100, 28, 27, 79, 19, 8, 16, 58, 106, 64, 51)
(7, 55, 69, 90, 42, 10, 72, 112, 119, 80, 85, 49)
(12, 33, 88, 96, 99, 62, 120, 93, 113, 110, 32, 76)
(14, 95, 68, 23, 71, 108, 37, 35, 47, 46, 34, 59)
(17, 20, 45, 89, 115, 73, 78, 116, 70, 29, 25, 31)
(22, 94, 87, 65, 43, 118, 52, 57, 54, 61, 56, 81)
(38, 117, 74, 111, 109, 60, 103, 105, 75, 107, 83, 48)
> RR:=<[1,21,63,36,50],(zp*yp*xp^-3)^5>];
> HH:=[N];
```

The action of the group $n$ on the cosets of $h$ is returned as $n120$; the images of $x$, $y$ and $z$ are defined as $xp$, $yp$, and $zp$; and the control subgroup $N$ is defined to be the group $n120$, of degree 120.

As is shown above, the element $u = zyx^{-3}$ belongs to the class of elements of order 12 referred to in the text. The special 12-cycle is the first cycle displayed; it contains $t_1$. So the relator by which we wish to factor is $(ut_1)^5$. Note that this relator is equivalent to the relation

$$t_1t_{21}t_{63}t_{36}t_{50} = u^5,$$

which is the manner in which we input it in the Double Coset Enumerator as $RR$. The input $HH$ simply gives the subgroup over which we wish to perform the enumeration, in this case the control subgroup $N$. 

The computer is now instructed to perform an enumeration of the double cosets of \( N \) in the group \( G = \langle N, t_1 \rangle \), which by the transitivity of \( N \) contains all 120 symmetric generators, subject to the additional relation given in \( RR \). The output CT contains: in CT[1], the index of \( N \) in \( G \); in CT[2], the number of suborbits, which is to say the rank of the permutation action of \( G \) on the cosets of \( N \) in \( G \); in CT[7], lengths of those suborbits; and in CT[4], canonical representatives (CDCRs, see [4]) for these 7 double cosets. Thus, for example, the third double coset contains 510 single cosets and is, in fact, \( N t_1 N t_2 N \). Detailed information about the edges of the graph is also returned, but is not included here.

It must be stressed that the CDCR is not necessarily the shortest possible, but is essentially the first word in the symmetric generators which does not lie in a previously discovered double coset. In this case we see from Fig. 3 that the graph has diameter 3 and that the shortest CDCRs would have lengths 0, 1, 2 (three times) and 3 (twice). So the CDCRs recorded here are indeed the shortest possible.

The conventional presentation for the group \( J_3:2 \) given in Section 6 may be verified by single coset enumeration using MAGMA [5]. We must adjoin an involution \( t \) which commutes with \( x \) and \( y \), and then factor by the additional relation. Thus

```plaintext
> j3a<x,y,z,t>:={Group<x,y,z,t|x^17=y^8=z^2=1,x^y=x^2,y^z=y^5,(x*y*z)^4=(x*z)^17=t^2=(x,t)=(y,t)=(z*y*x^-3*t)^5=1>;
> nn:=sub<g|x,y,z>;
> Index(j3a,nn);
6156
```
References