A NEW EXISTENCE PROOF OF JANKO'S SIMPLE GROUP J_4

G. D. COOPERMAN, W. LEMPKEN, G. O. MICHLER, AND M. WELLER

Introduction

Janko's large simple sporadic group J_4 was originally constructed by Benson, Conway, Norton, Parker and Thackray as a subgroup of the general linear group $GL_{112}(2)$ of all invertible 112×112-matrices over the field $GF(2)$ with 2 elements, see [1] and [13]. So far the construction of the 112-dimensional 2-modular irreducible representation of J_4 is only described in Benson's thesis [1] at Cambridge University. Furthermore, its proof is very involved.

In his paper [12] Lempken has constructed two matrices $x, y \in GL_{1333}(11)$ of orders $o(x) = 42$, $o(y) = 10$, respectively, which describe a 1333-dimensional 11-modular irreducible representation of J_4. These two matrices are the building blocks for the new existence proof for J_4 given in this article.

In [17] the fourth author has used this linear representation of the finite group $G = \langle x, y\rangle$ to construct a permutation representation of G of degree 173 067 389 with stabilizer $M = \langle x^3, y, (x^{14})^t\rangle$, where $t = (x^{14}y^5)^2$. His main result is described in section 2. It is based on a high performance computation on the supercomputers of the Theory Center of Cornell University and the University of Karlsruhe.

Using Weller's permutation representation we show in Theorem 5.1 of this article that the group $G = \langle x, y\rangle$ is simple and has order

$$|G| = 2^{12} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43.$$

Furthermore, we construct an involution $u_1 \neq 1$ of G and an element a_1 of order 3 as words in x and y such that $H = C_G(u_1)$ has the following properties:

(a) The subgroup $Q = O_2(H)$ is an extra-special group of order $|Q| = 2^{13}$ such that $C_H(Q) = \langle u_1\rangle$.

(b) $P = \langle a_1\rangle$ is a Sylow 3-subgroup of $O_{2,3}(H)$, and $C_Q(P) = \langle u_1\rangle$.

(c) $H/O_{2,3}(H) \cong Aut(M_{22})$, the automorphism group of the Mathieu group $M_{22}, N_H(P) \neq C_H(P) \cong 6M_{22}$, the sixfold cover of M_{22}.

Hence $G \cong J_4$ by Theorem A of Janko's article [11].

In fact we give generators of these subgroups of H in terms of short words in x and y, see Theorem 5.1. Therefore all the assertions of this result can easily be checked by means of the computer algebra systems GAP or MAGMA without using the programs of [17].

In section 1 we determine the group structure of the subgroup $M = \langle x^3, y, (x^{14})^t\rangle$, where $t = (x^{14}y^5)^2$. Proposition 1.3 asserts that M is the split extension of an elementary abelian group E of order 2^{11} by the simple Mathieu group M_{24}. By Proposition 1.4 the restriction of Lempken's 1333-dimensional 11-modular representation V of $G = \langle x, y\rangle$ to M decomposes into two irreducible 11-modular representations W and S of dimensions $\dim_F W = 45$ and $\dim_F S = 1288$. From these data the fourth author has constructed the above mentioned permutation representation of G having degree 173067389 in [17].

Section 3 is devoted to determine the group structure of $H = \langle x^7, y^5, (x^{14})^a, (r_1)^b\rangle$ of G, where a and b are suitably chosen elements of G described in Lemma 3.2. In Lemma 3.1 we construct an involution $u_1 \neq 1$ of G such that $H \leq C_G(u_1)$. In fact, we show in Proposition 3.3 that the group H has all the properties stated in assertions (a), (b) and (c) above.

In section 4 we study the fusion of the involutions of the stabilizer M in G. Proposition 4.1 asserts that G has 2 conjugacy classes of involutions $(u_1)^G$ and $(w_1)^G$. Using this result and another high performance computation determining the number of fixed points of the involution u_1 on the permutation module of degree 173 067 389 we prove in Proposition 4.2 that $H = C_G(u_1)$. In the final section it is shown that G is a simple group. This is done in Theorem 5.1, which completes our existence proof of Janko's simple group J_4.

Concerning our notation and terminology we refer to the Atlas [4] and the books by Butler [3], Gorenstein [7], Gorenstein, Lyons, Solomon [8] and Isaacs [10].

1. Lempken's subgroup $G = \langle x, y\rangle$ of $GL_{1333}(11)$

Throughout this paper F denotes the prime field $GF(11)$ of characteristic 11. Let V be the canonical 1333-dimensional vector space over F. In Theorem 3.16 and Remark 3.21 of [12] Lempken describes the construction of two 1333×1333-matrices $x, y \in GL_{1333}(11)$ of orders $o(x) = 42$ and $o(y) = 10$, which will become the starting data for the construction and new existence proof of Janko's group J_4. Because of their size these matrices cannot be restated here, but they can be received by e-mail from eowmob@@exp-math.uni-essen.de.

Throughout this paper $G = \langle x, y\rangle$ is the subgroup of $GL_{1333}(11)$generated by the matrices x and y of orders 42 and 10, respectively. The following notations are taken from Lempken's article [12]. There he considers the subgroup $M = \langle x^3, y, (x^{14})^t\rangle$ with $t = (x^{14}y^5)^2$ as well. However we cannot quote any result of [12] on the structure of the subgroup M, because Lempken assumes the existence of the simple Janko group J_4.

In this section we show that the subgroup M is a split extension of an elementary abelian normal subgroup E of order $|E| = 2^{11}$ by the simple Mathieu group M_{24}. Furthermore, the module structure of the restriction of the 1333-dimensional representation of G to the subgroup M is determined.

The following notations are kept throughout the remainder of this article.

Notation 1.1. *In $G = \langle x, y\rangle \le GL_{1333}(11)$ define the following elements:*
$r_0 = yx^{21}y^{-1}$
$r_1 = x^{14}yx^{21}y^{-1}x^{-14} = (r_0)^{x^{28}}$
$r_2 = y^3x^{21}y^7$
$r_3 = x^{14}y^3x^{21}y^7x^{-14} = (r_2)^{x^{28}}$
$v_1 = y^6x^{21}y^4$
$v_2 = y^8x^{21}y^2$
$v_3 = y^4x^{21}y^6$
$v_4 = x^{21}$
$w_1 = [x^6, y^5]$
$u_1 = [x^{-6}w_1x^6, r_1] = (v_1r_2)^2 = [x^{-12}(y^5x^6)^2(x^{21})^{y^{-1}x^{28}}]^2$
$u_2 = (v_3r_0)^2$
$u_3 = u_1(v_4r_0)^2$
$u_4 = (v_3r_2)^2$
$u_5 = u_4(v_4r_2)^2$
$u_6 = [x^{21}(x^{21})^y]^2$
$s_1 = y^2r_1y^{-2} = (r_1)^{y^8}$
$s_2 = (x^{21})^{yx^{28}} = x^{14}y^{-1}x^{21}yx^{-14}$
$d_1 = [(r_1)^b, s_1]$, *where* $b = y^{-2}x^{-6}$
$d_2 = (x^{21})^y$

$a_1 = d_1x^6d_1x^{24}d_1$
$t_1 = s_1(r_1)^bs_1$
$t_2 = (x^{21})^{y^5}$
$q_0 = r_1r_3d_1s_1(x^6y^2)^4$
$a_3 = s_1(q_0)^3s_1(q_0)^4s_1s_2$
$a_6 = t_1(x^{14}y^5)^{-2}x^{14}(x^{14}y^5)^2t_1$
$z \ = (x^{14})^t, \textit{where}\ t = (x^{14}y^5)^2$

Observe that the elements $a_1, a_3, a_6, z \in G$ have order 3, and $q_0 \in G$ has order 7. All other elements are involutions of G.

Lemma 1.2. *Let* $L = \langle x^6, y^2, z\rangle \leq G = \langle x, y\rangle$. *Let* $T = \langle x^6, y^2\rangle$, $j = (x^6y^2x^{12})^3$, *and* $s = y^6(y^2x^{18})^4$. *Then the following assertions hold:*

- (a) $T = \langle x^6, y^2\rangle \cong GL_4(2)$.
- (b) $r_1 = (j)^s \in T$.
- (c) $r_0 = (r_1)^{z^2} \in L$.
- (d) $t_2 = (r_0)^{y^6}, r_2 = (r_0)^{y^8}, d_2 = (r_0)^{y^2} \in L$.
- (e) $E_2 = \langle r_0, r_2, d_2, t_2\rangle$ *is an elementary abelian normal subgroup of* $N = \langle T, E_2\rangle$ *with order* $|E_2| = 2^4$.
- (f) $N = E_2T$, $E_2 \cap T = 1$, *and* N *is perfect.*
- (g) $|L : N| = 759$, *and* $|L| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.
- (h) $L \cong M_{24}$, *the simple Mathieu group.*

Proof. (a) By MAGMA the simple group $GL_4(2) \cong A_8$ has the following presentation with respect to the generators a and b of orders 5 and 7, respectively:

$$(*)\quad \begin{array}{l} a^5 = b^7 = (ba^3)^4 = 1\ , \\ (b^2a)^2 \cdot b^{-1}ab^{-1}a^3b^{-1}a^{-1} = 1\ , \\ b^3aba^3b^{-3}ab^{-1}a^2 = 1\ , \\ b^3a^{-1}b^{-1}a^3b^{-2}a^{-1}b^{-1}aba^{-1} = 1\ , \\ b^2aba^{-1}b^{-1}a^3b^{-1}ab^{-1}aba = 1\ , \\ (b^2ab^{-1}a^{-1}b^{-1}a^{-1})^2 = 1. \end{array}$$

Choosing $a = y^2$ and $b = x^6$ it follows by means of MAGMA that all the relations of $(*)$ are satisfied. Hence $T = \langle x^6, y^2\rangle \cong GL_4(2)$.

(b) Certainly $j = (x^6y^2x^{12})^3$, $s = y^6(y^2x^{18})^4 \in T$. Hence $(j)^s \in T$. Using MAGMA one checks that $r_1 = (j)^s$.

(c) From $r_1 \in T \leq L$ we obtain $(r_1)^{z^2} \in L$. Using MAGMA again one gets that $r_0 = (r_1)^{z^2}$.

(d) As y^2 has order 5 it is easily checked that conjugation by y^2 yields the following orbit:

$$y^2 : t_2 \to r_2 \to r_0 \to d_2 \to r_0r_2d_2t_2 \to t_2.$$

Hence all assertions of (d) hold.

(e) Similarily x^6 has the following conjugation action:

$$x^6 : t_2 \to t_2, \text{ and } r_0 \to r_2 \to d_2 \to r_0d_2$$

Thus $E_2 = \langle r_0, r_2, d_2, t_2\rangle$ is a normal elementary abelian subgroup of $N = \langle T, E_2\rangle$ of order $|E_2| = 2^4$.

(f) As T is a simple group by (a) we now get $N = E_2T$, and $E_2 \cap T = 1$. Since E_2 is a simple 2-modular representation of T, it follows that N is perfect.

(g) Using the coset enumeration algorithm of MAGMA we see that $|L : N| = 759$. Hence $|L| = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.

(h) A matrix computation inside $GL_{1333}(11)$ shows that $[z, t_2] = z$. Therefore $L = \langle N, z\rangle$ is perfect by (f). As $|L : N|$ is odd, any Sylow 2-subgroup of L is isomorphic to a Sylow 2-subgroup of N, and therfore to those of $L_5(2)$ or M_{24}. Applying now Theorem 1 of Schoenwaelder [16] we get $L \cong M_{24}$.

□

Proposition 1.3. *Let $M = \langle x^3, y, z\rangle \le G = \langle x, y\rangle$. Then the following assertions hold:*

(a) $E = \langle u_1, u_2, u_3, u_4, u_5, u_6, v_1r_0, v_2r_2, v_3d_2, v_4t_2, y^5\rangle$ *is an elementary abelian normal subgroup of M with order $|E| = 2^{11}$.*

(b) $L = \langle x^6, y^2, z\rangle$ *is a subgroup of M such that $M = EL$, $E \cap L = 1$, and L is isomorphic to the simple Mathieu group M_{24} acting irreducibly on E.*

(c) $|M| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.

(d) *M is perfect.*

(e) *M has six conjugacy classes of involutions with representatives: u_1, r_0, r_1r_2, w_1, u_4r_0 and $u_4r_1r_2$.*

Proof. (a) By Lemma 1.2 (b) the elements t_2, d_2, r_0, r_2 are contained in $L = \langle x^6, y^2, z\rangle \le M = \langle x^3, y, z\rangle$. The following equations are verified by means of MAGMA:

$[y^5, t_2] = v_4t_2, [y^5, d_2] = v_3d_2, [y^5, r_2] = v_2r_2, [y^5, r_0] = v_1r_0, [v_2r_2, r_0] = u_1$, $[v_3d_2, r_0] = u_2, [v_4t_2, r_0] = u_1u_3, [v_2d_2, r_2] = u_4, [v_4t_2, r_2] = u_4u_5$, and $[v_4t_2, d_2] = u_6$. Hence $E = \langle u_1, u_2, u_3, u_4, u_5, u_6, v_1r_0, v_2r_2, v_3d_2, v_4t_2, y^5\rangle \le M$.

Using the computer and MAGMA it is checked that the 11 involutions $u_1, u_2, u_3, u_4, u_5, u_6, v_1r_0, v_2r_2, v_3d_2, v_4t_2$ and y^5 commute pairwise, and that they generate an elementary abelian normal subgroup of M with order $|E| = 2^{11}$.

(b) $L = \langle x^6, y^2, z\rangle$ is a simple subgroup of M by Lemma 1.2. Thus $E \cap L = 1$, and EL is a subgroup of M. We claim that $M = EL$. Certainly, $y = y^5 \cdot (y^2)^3 \in EL$. Lemma 1.2 (d) asserts that $t_2 \in L$. Hence

$$x^3 = (x^6)^4 \cdot x^{21} = (x^6)^4 \cdot v_4 = (x^6)^4 \cdot (v_4t_2) \cdot t_2 \in EL$$

Thus $M = \langle x^3, y, z\rangle = EL$. It is well known that the smallest, non-trivial, irreducible 2-modular representation of $L \cong M_{24}$ is of degree 11. Hence L acts irreducibly on E, because $1 \ne w_1 = [x^6, y^5] \in [L, E]$.

(c) By (a), (b) and Lemma 1.2 (g) we have

$$|M| = |E \cdot L| = 2^{11} \cdot 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23.$$

(d) As L is a simple group, $L = L' \le M'$. Since L acts irreducibly on E by (b), we have $E = [E, L] \le M'$. Therefore $M = EL = M'$.

(e) It is well known that the simple Mathieu group M_{24} has 2 non-isomorphic simple 2-modular representations of degree 11. They are dual to each other. Hence there are 2 non-isomorphic split extensions $2^{11}M_{24}$. By GAP [15] the character tables of these groups are both known. It follows that M has six conjugacy classes. Certainly, u_1^M, w_1^M, r_0^M, $(u_4r_0)^M$ and $(r_1r_2)^M$ are 5 different conjugacy classes of involutions of M, because their lengths $|u_1^M| = 7 \cdot 11 \cdot 23$, $|w_1^M| = 2^2 \cdot 3 \cdot 23$, $|r_0^M| = 2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 23$, $|(u_4r_0)^M| = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$, and $|(r_1r_2)^M| = 2^6 \cdot 3^2 \cdot 7 \cdot 11 \cdot 23$ are all distinct. Furthermore, $|(u_3r_1r_2)^M| = 2^6 \cdot 3^2 \cdot 7 \cdot 11 \cdot 23$, but the matrices r_1r_2 and $u_3r_1r_2$ are not conjugate in M, because they have different traces $tr(r_1r_2) = 9$ and $tr(u_3r_1r_2) = 0$ in $GF(11)$ as is checked by means of MAGMA. □

The following result is due to Lempken [12].

Proposition 1.4. *Let $G = \langle x, y\rangle$, and $M = \langle x^3, y, z\rangle$. Then the following assertions hold:*

(a) $V = F^{1333}$ *is a simple* FG*-module.*
(b) M *is a subgroup of* G *such that the restriction* $V_{|M} = W \bigoplus S$, *where* W *and* S *are simple* FM*-modules with dimensions* $dim_F W = 45$ *and* $dim_F S = 1288$.

Proof. Assertion (a) is a restatement of Theorem 3.20 of [12]. (b) is checked by means of Parker's Meat-Axe algorithm contained in GAP, see [15].

□

2. Transformation of G into a permutation group

In [5] Cooperman, Finkelstein, York and Tselman have described a method for the transformation of a linear representation of a finite group $\kappa : X \to GL_n(K)$ over a finite field K into a permutation representation $\pi : X \to S_m$, where m denotes the index of a given subgroup U of X.

This transformation is an important idea, because most of the efficient algorithms in computational group theory deal with permutation groups, see [3]. In particular, there is a membership test for a permutation $\sigma \in S_m$ to belong to the subgroup $\pi(X)$.

Using Algorithm 2.3.1 of [6] M. Weller [17] strengthened the results of Cooperman et al. [5] as follows:

Theorem 2.1. *Let* K *be a finite field of characteristic* $p > 0$. *Let* U *be a subgroup of a finite group* X, *and let* V *be a simple* KX*- module such that its restriction* $V_{|U}$ *contains a proper non-zero* KU*- submodule* W. *Then there is an algorithm to construct:*
(a) *The stabilizer* $\hat{U} = Stab_G(W) = \{g \in G | Wg = W \le V\}$,
(b) *a full set of double coset representations* $x_i, 1 \le i \le k$, *of* $\hat{U}$ *in* G, *i. e.* $G = \bigcup_{i=1}^{k} \hat{U} x_i \hat{U}$,
(c) *a base* $[\beta_1, \beta_2, \cdots, \beta_j]$ *and strong generating set* $\{g_s | 1 \le s \le q\}$ *of* G *with respect to the action of* G *on the cosets of* $\hat{U}$, *which coincides with the given operation of* G *on the* FU*-submodule* W *of* V.

Using an efficient implementation of this algorithm on the supercomputers of the Theory Center at Cornell University and of the computer center of Karlsruhe University M. Weller [17] has obtained the following result.

Theorem 2.2. *Let* $G = \langle x, y \rangle \le GL_{1333}(11)$ *and* $M = \langle x^3, y, z \rangle$. *Then the following assertions hold:*
(a) $|G : M| = 173067389$
(b) $|G| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$
(c) *If* Ω *denotes the index set of the cosets* Mg_i *of* M *in* G, *then* G *induces on* $\Omega = \{1, 2, \cdots, 173067389\}$ *a faithful permutation action with stabilizer* $stab_G(1) = M$.
(d) $G = \bigcup_{i=1}^{7} M x_i M$, *where the double coset representatives* x_i *of* M *are given by the following words:*

$x_1 = 1$ $(|Mx_1M| = 1)$
$x_2 = x^{14}c^{12}$ $(|Mx_2M| = 15180)$
$x_3 = x_6cyc^{20}yc^{16}yc^{19}yc^{17}yc^{17}yc^{19}yc^{8}xc^{22}$
$= x_6y^2c^{16}yc^{13}yc^{4}yc^{10}yc^{18}xc^{21}$ $(|Mx_3M| = 28336)$
$x_4 = x_3c^3x^{-1}c^{11}$ $(|Mx_4M| = 3400320)$
$x_5 = x_6xc$ $(|Mx_5M| = 54405120)$
$x_6 = xc^{12}xc^3xc^2$ $(|Mx_6M| = 32643072)$
$x_7 = x_5xc^9xc^{16}$ $(|Mx_7M| = 82575360)$

where $c := (x^{14})^ty^4(x^{14})^ty^{-1}(x^{14})^t$ *has order 23, and* $t = (x^{14}y^5)^2$.

3. Group structure of the approximate centralizer H

Lempken [12] determines a suitable involution $u_1 \in G$ and an approximation H of the centralizer $C_G(u_1)$. It is now defined by means of the notation 1.1.

Lemma 3.1. *In* $G = \langle x, y\rangle$ *let* $a = r_1y^{-4}x^6y^4$ *and* $b = y^{-2}x^{-6}$.

The subgroup $H = \langle x^7, y^5, (x^{14})^a, (r_1)^b\rangle$ *of* $G = \langle x, y\rangle$ *contains the involution* $u_1 \neq 1$, *and*

$$H \leq C_G(u_1).$$

Proof. The subgroup H of G is defined in Lemma 2.5 of [12]. Using GAP [15] it can easily be checked that $u_1^2 = 1$, and that u_1 commutes with the given generators of H. □

The remainder of this section is devoted to determine the group structure of H.

Lemma 3.2. *Let* $H = \langle x^7, y^5, (x^{14})^a, (r_1)^b\rangle$, $M = \langle x^3, y, z\rangle$, *where* $a = r_1(x^6)^{y^4}$ *and* $b = y^{-2}x^{-6}$. *Let* $W = H \cap M$. *Then the following assertions hold:*

(*a*) $|H : W| = 77$

(*b*) $Q = \langle u_1, u_2, u_3, u_4, u_5, v_1, v_2, r_0, r_1, r_2, r_3, d_1, s_1\rangle$ *is a normal extra-special* 2*-subgroup of* H *with* $|Q| = 2^{13}$.

(*c*) $K = \langle d_2, s_2, t_2, a_1, a_3, a_6\rangle$ *is a subgroup of* W *with center* $Z(K) = \langle a_1\rangle$ *such that* $K \cong 3A_6$.

(*d*) $A = \langle u_1, u_6, v_3d_2, v_4t_2, y^5\rangle$ *is an elementary abelian subgroup of* W *with order* $|A| = 2^5$ *normalized by* $K\langle t_1\rangle$, *and* $A \cap K\langle t_1\rangle = 1$.

(*e*) $H \cap M = QAK\langle t_1\rangle$, *and* $K\langle t_1\rangle \cong 3S_6$.

(*f*) $|H| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$

Proof. (a) By Theorem 2.2 $G = \langle x, y\rangle$ has a faithful permutation action on the 173067389 cosets Mg of the subgroup $M = \langle x^3, y, z\rangle$. Using the computer we restrict this permutation representation to the subgroup H. It follows that

$$|H : H \cap M| = 77.$$

(b) Let $Q = \langle u_1, u_2, u_3, u_4, u_5, v_1, v_2, r_0, r_1, r_2, r_3, d_1, s_1\rangle$. Using again the computer and the permutation representation of G described in Theorem 2.2 it follows that $Q \leq H \cap M$. Furthermore, we get the following relations:

$(u_2)^{s_1} = u_1u_2, (u_3)^{r_3} = u_1u_3, (u_4)^{d_1} = u_1u_4$

$(u_1u_4u_5)^{r_1} = u_1(u_1u_4u_5) = u_4u_5,\ \ (v_1)^{r_2} = u_1v_2,\ \ (v_2)^{r_0} = u_1r_0.$

Since u_1 commutes with all the generators it follows that $\langle s_1, u_2\rangle$, $\langle r_3, u_3\rangle$, $\langle d_1, u_4\rangle$, $\langle r_1, u_1u_4u_5\rangle$, $\langle r_2, v_1\rangle$ and $\langle r_0, v_2\rangle$ are six dihedral subgroups of order 8 with almagamated subgroup $\langle u_1\rangle$, which commute pairwise as subgroups. Hence Q is their central product. In particular, Q is an extra-special 2-group of order

$|Q| = 2^{13}$. Another matrix computation shows that Q is invariant under conjugation by the 4 given generators of H. Thus Q is normal in H.

(c) Let $K := \langle a_1, d_2, s_2, t_2, a_3, a_6\rangle$. Using the computer again we see that K is a subgroup of $W = H \cap M$. Define $a := t_2a_1^2d_2a_3^2a_6a_3^2a_6^2s_2a_1s_2a_3$, $b := s_2t_2$, $o(a) = 2$, $o(b) = 4$ and $o(ab) = 15$.

Let $x_1 := b^2ab^2abab^2abab$, $x_2 := a$, $x_3 := b^3abab^3ab^2abab^2ab^2ab$,
$x_4 := b^3ab^3ab^3ab^2ab^2abababa$, and $c := x_3^2$. Then the following relations hold in $B = \langle x_1, x_2, x_3, x_4\rangle \le K$:

$c^3 = 1, x_1^3 = 1, x_2^2 = 1, x_3^2 = c, x_4^2 = 1, (x_1x_2)^3 = 1, (x_2x_3)^3 = 1, (x_3x_4)^3 = 1,$
$(x_1x_3)^2 = 1, (x_1x_4)^2 = 1, (x_2x_4)^2 = 1, c^{x_1} = c, c^{x_2} = c, c^{x_3} = c, c^{x_4} = c.$

By Huppert [9], p.138 $B/\langle c\rangle$ is isomorphic to the alternating group A_6.
Thus $|B| = 3|A_6|$.

Now $|\langle a, b\rangle| = 3|A_6|$ by MAGMA. Furthermore we have $a = x_2$, and

$$b = x_1^2x_2x_1^2x_3^4x_1^2x_2x_1^2x_3^4x_2x_4x_1x_4x_3^5x_2x_4x_3^2x_1x_3^5x_2x_3x_4x_1^2x_4x_3^2x_1x_2x_1x_4x_3^2x_4x_1.$$

Hence $B = \langle x_1, x_2, x_3, x_4\rangle = \langle a, b\rangle$.
We claim that $K = \langle a, b\rangle$. This follows immediately from the following equations:

$$\begin{aligned}
a_1 &= (bab^2ab^3abab^3ab^3)^8\\
d_2 &= b^2\\
s_2 &= (bab^2ab^3abab^3ab^3)^6\\
t_2 &= bab^2ab^3(ababab^3)^5abab^3a\\
a_3 &= bab^2ab^3(ababab^3)^2abab^3ab^3ababab^3\\
a_6 &= bab^2ab^3(ababab^3)^2abab^3ab^2\ .
\end{aligned}$$

Let $p_1 = b^2ab^2abab^2ab^3abab^3$. Then p_1 has order 3 and commutes with a_1. Furthermore, $[p_1, a_3] = a_1$. Hence $D = \langle p_1, a_3\rangle$ is a Sylow 3-subgroup of K. It is extra-special. Therefore its center $Z(D) = \langle a_1\rangle = \langle c\rangle$ does not split off. Hence $K = \langle a, b\rangle \cong 3A_6$, the non-split 3-fold cover $3A_6$ of A_6.

(d) Another application of the permutation representation of G described in Theorem 2.2 on the computer shows that $A = \langle u_1, u_6, v_3d_2, v_4t_2, y^5\rangle \le W$, and that $a_1, a_3, a_6 \in W$. Then A is an elementary 2-subgroup of W of order $|A| = 2^5$. Another computation shows that A is normalized by $K\langle t_1\rangle$, and $A \cap K\langle t_1\rangle = 1$.

(e) and (f) As $(a_1)^{t_1} = (a_1)^2, (AK)^{t_1} = AK$ and $K\langle t_1\rangle \cong 3S_6$ by (c).

Certainly $H \cap M \le C_M(u_1)$ by Lemma 3.1. Using MAGMA we see that $|(u_1)^M| = 1771 = 7 \cdot 11 \cdot 23$. Therefore $|C_M(u_1)| = |M| : |(u_1)^M| = 2^{21} \cdot 3^3 \cdot 5$ by Proposition 1.3.

Thus $H \cap M = C_M(u_1)$, because $|H \cap M| \ge |QAK\langle t_1\rangle| = 2^{13} \cdot 2^4 \cdot 2^3 \cdot 3^3 \cdot 5 \cdot 2 = 2^{21} \cdot 3^3 \cdot 5$. Hence $|H| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$ by (a), and $W = QAK\langle t_1\rangle$.

□

Proposition 3.3. *Let $H = \langle x^7, y^5, (x^{14})^a, (r_1)^b\rangle$, where $a = r_1(x^6)^{y^4}$, $b = y^{-2}x^{-6}$. Then the following assertions hold:*

(a) $U_0 = \langle u_6, v_3, v_4, d_2, s_2, t_2, a_1, a_3, a_6, x^{14}, y^5\rangle$ is a subgroup of H with center $Z(U_0) = \langle u_1a_1\rangle$

(b) $U_0/Z(U_0) \cong M_{22}$, and $U_0 \cong 6M_{22}$

(c) $Q \cap Z(U_0) = \langle u_1\rangle$.

(d) The element a_1 of order 3 generates a Sylow 3-subgroup of $O_{2,3}(H)$, and $C_Q(a_1) = Z(Q) = \langle u_1\rangle$.

(e) $U = U_0 : \langle t_1\rangle = N_H(\langle a_1\rangle)$.

(f) $H = QU$, $U \cap Q = U_0 \cap Q = Z(U) = \langle u_1\rangle$, and $U_0 = C_H(a_1)$

(g) *$U/Z(U_0) \cong Aut(M_{22})$, the automorphism group of the simple Mathieu group M_{22}.*

Proof. By Lemma 3.2 we know that u_6, v_3, v_4, s_2, t_2 and $d_2 = (s_2t_2)^2$ belong to $W = H \cap M$. Certainly $x^{14} \in H$.

By Lemma 3.2 (e) we have $a_1, a_3 \in W$. ¿From $[y^5, s_2] = (y^5s_2)^2 = u_1u_6 \in U_0$ follows that $u_1a_1 \in U_0$ and has order 6. By Lemma 3.2

$$U_0 = \langle u_6, v_3, v_4, d_2, s_2, t_2, a_1, a_3, a_6, x^{14}, y^5\rangle$$

is a subgroup of H. Using MAGMA it is checked that the matrix u_1a_1 commutes with the 11 generators of U_0. Thus $\langle u_1a_1\rangle \le Z(U_0)$.

By Lemma 3.2 (d) $A = \langle u_1, u_6, v_3d_2, v_4t_2, y^5\rangle$ is an elementary abelian subgroup of U_0 with $|A| = 2^5$. By Lemma 3.2 (c) and (d) it is normalized by the perfect subgroup $K = \langle d_2, s_2, t_2, a_1, a_3, a_6\rangle$ of U_0. Using MAGMA it can be checked that $A = [A, K]$ is a uniserial $GF(2)K$-module. Hence

$$AK = AK' \le (U_0)'.$$

Lemma 3.2 (a), (e) and (f) assert that $|U_0 : AK| = 77$. Since x^{14} has order 3, and $U_0 = \langle AK, x^{14}\rangle$ we get $x^{14} \in U_0'$. Hence U_0 is perfect.

Let $\bar{U}_0 = U_0/\langle u_1a_1\rangle$. Then $\bar{U}_0$ is perfect. Let $\bar{H} = H/Q\langle a_1\rangle$. From Lemma 3.2 we get $|\bar{H} : \bar{U}_0| = 2$, and $|\bar{U}_0| = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.

Now we claim that $\bar{U}_0$ is simple. Since x^{14} does not normalize A, it follows that $\langle u_1a_1\rangle$ is the largest normal subgroup of U_0 contained in AK. Thus $O_2(\bar{U}_0) = O_3(\bar{U}_0) = O_5(\bar{U}_0) = 1$. Suppose that Y is a minimal normal subgroup of $\bar{U}_0$. If $|Y|$ is odd, then $|Y| \in \{7, 11\}$, and $\bar{U}_0$ splits over Y. Furthermore, $Aut(Y)$ is cyclic. As $\bar{U}_0$ is perfect we get $Y \le Z(\bar{U}_0)$. Hence $\bar{U}_0'$ is a proper subgroup of $\bar{U}_0$, a contradiction.

Therefore $|Y|$ is even, and $Y \cap (\bar{A} : \bar{K}) \ne 1$. As $\bar{A}$ is not normal in $\bar{U}_0$, we get $\bar{A} : \bar{K} \le Y$. Thus $Y = \bar{U}_0$, because $|\bar{U}_0 : Y|$ is odd and $\bar{U}_0$ is perfect. Hence $\bar{U}_0$ is a simple group of order $|\bar{U}_0| = 2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. Now Theorem A of Parrott [14] asserts that $\bar{U}_0 \cong M_{22}$, the simple Mathieu group M_{22}. Therefore (b) holds. Assertions (a) and (c) are immediately clear.

(d) Using MAGMA it can be seen that $(a_1)^{t_1} = (a_1)^2$. By Lemma 3.2 and (b) we have $H = QU_0\langle t_1\rangle, |H : QU_0| = 2$ and $O_{2,3}(QU_0) = Q\langle a_1\rangle$. Hence $O_{2,3}(H) = Q : \langle a_1\rangle$. Another computation with MAGMA yields that $C_Q(a_1) = Z(Q) = \langle u_1\rangle$.

(e) Certainly $U = U_0 : \langle t_1\rangle \le N_H(\langle a_1\rangle)$. In fact, $U = N_H(\langle a_1\rangle)$ by (d) and the Frattini argument applied to the Sylow 3-subgroup $\langle a_1\rangle$ of $O_{2,3}(H)$.

(f) is now obvious.

(g) By Lemma 3.2 and (f) we know that $(H \cap M)/Q \cong 2^4 : \hat{3}S_6$. Therefore $(H \cap M)/O_{2,3}(H) \cong 2^4 : S_6$. Hence $H/O_{2,3}(H) \cong Aut(M_{22})$.

□

4. The order of $C_G(u_1)$

In this section the order of the centralizer $C_G(u_1)$ of the involution $u_1 \in G = \langle x, y\rangle$ is determined. From Proposition 3.3 we then get: $H = C_G(u_1)$.

Proposition 4.1. *The group $G = \langle x, y\rangle$ has two conjugacy classes of involutions with representatives u_1, $w_1 \in GL_{1333}(11)$ having traces $tr(u_1) = 9$, $tr(w_1) = 0 \in F$.*

Proof. Certainly the matrices u_1 and w_1 are not conjugate in G, because they have different traces $tr(u_1) = 9$, $tr(w_1) = 0$ in $F = GF(11)$. By Proposition 3.1 the following elements $u_1, w_1, r_0,\ u_4r_0,\ r_1r_2$, and $u_3r_1r_2$ of M yield a complete set of representatives of all six conjugacy classes of M.

Let $q_0 = r_1r_3d_1s_1(x^6y^2)^4$, and $a_6 = (x^{14})^{y^5x^{14}}$. Then in G the following fusion takes place:

$$u_1 \sim r_0 \sim (r_1r_2) \text{ and } w_1 \sim (u_4r_0) \sim (u_3r_1r_2),$$

because $r_0^{y^5x^{14}r_3(q_0)^6} = u_1 = (r_1r_2)^{y^5x^{14}t_2r_2s_2(q_0)^6(a_6)^2(q_0)^6}$,
$(u_4r_0)^{y^5x^{14}r_3} = w_1 = (u_3r_1r_2)^{y^5x^{14}s_2(q_0)^6y^5x^{14}r_3}$

By Theorem 2.2 (b) the index of M in G is odd. Therefore each involution i of G has a G-conjugate $i^g \in M$. Hence i^g is contained in one of the six conjugacy classes of M. Since they are G-fused to u_1^G or w_1^G it follows that either $i \in u_1^G$ or $i \in w_1^G$.

□

Proposition 4.2. $H = C_G(u_1)$

Proof. Let f be the number of fixed points of the permutation afforded by u_1 on the 173067389 cosets of M in G. As $|G : M| = 173067389$ is odd, each involution i of u_1^G is contained in $f > 0$ different conjugates M^g of M for some $g \in G = \langle x, y\rangle$. By the proof of Proposition 4.1 the group G fuses the conjugacy classes u_1^M, $(r_0)^M$ and $(r_1r_2)^M$. Furthermore, $|u_1^M| = 7 \cdot 11 \cdot 23$, $|r_0^M| = 2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 23$, and $|(r_1r_2)^M| = 2^6 \cdot 3^2 \cdot 7 \cdot 11 \cdot 23$. Hence

$$\begin{aligned} |u_1^G| &= \frac{|G : M|(|u_1^M| + |r_0^M| + |(r_1r_2)^M|)}{f} \\ &= \frac{173067389 \cdot 11 \cdot 23(7 + 2^4 \cdot 3^2 \cdot 5 + 2^6 \cdot 3^2 \cdot 7)}{f} \\ &= \frac{173067389 \cdot 11 \cdot 23 \cdot 4759}{f} \end{aligned}$$

Using now the computer again, we see that u_1 has $f = 52349$ fixed points. Therefore

$$|u_1^G| = |G : C_G(u_1)| = 11^2 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43,$$

and $|C_G(u_1)| = 2^{21} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ by Theorem 2.2. Now Lemma 3.2 and Proposition 3.3 assert that $H = C_G(u_1)$. □

5. The main result

In this section we show that $G = \langle x, y\rangle$ is a simple group. As $C_G(u_1)$ satisfies the hypothesis of Janko's theorem A [11] by Propositions 3.3 and 4.2 our existence proof for Janko's simple group J_4 then is complete.

Theorem 5.1. *Let $G = \langle x, y\rangle$ where $x, y \in GL_{1333}(11)$ are matrices constructed in [12] of orders $o(x) = 42$ and $o(y) = 10$. Then G is a simple group of order*

$$|G| = 2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$$

such that $u_1 = [x^{-12}(y^5x^6)^2(x^{21})^{y^{-1}x^{28}}]^2 \neq 1$ is an involution of G with centralizer $H = C_G(u_1) = \langle x^7, y^5, (x^{14})^a, (r_1)^b\rangle$, where $a = r_1(x^6)^{y^4}$, and $b = y^{-2}x^{-6}$. Furthermore, with the Notation 1.1 the following assertions hold:

(a) $Q = O_2(H) = \langle u_1, u_2, u_3, u_4, u_5, v_1, v_2, r_0, r_1, r_2, r_3, d_1, s_1\rangle$ is an extra-special normal subgroup of H with $|Q| = 2^{13}$.

(b) The element $a_1 = d_1x^6d_1y^{24}d_1$ of order 3 generates a Sylow 3-subgroup of $O_{2,3}(H)$, and $C_Q(a_1) = Z(Q) = \langle u_1\rangle$.

(c) $U_0 = C_H(a_1) = \langle u_6, v_3, v_4, d_2, s_2, t_2, a_1, a_3, a_6, x^{14}, y^5\rangle \cong 6M_{22}$, *the sixfold cover of the Mathieu group* M_{22} *with center* $Z(U_0) = \langle u_1a_1\rangle$.

(d) $U = N_H(a_1) = U_0 : \langle t_1\rangle$ *is a subgroup of* H *with* $U/Z(U_0) \cong Aut(M_{22})$, *and center* $Z(U) = \langle u_1\rangle$.

(e) $H = QU$, *and* $Q \cap U = \langle u_1\rangle = C_Q(a_1)$.

In particular, G *is isomorphic to Janko's simple group* J_4.

Proof. In view of Proposition 4.2, Theorem 2.2, Lemma 3.2 and Proposition 3.3 it remains to show that G is a simple.

Proposition 3.1 asserts that $M = \langle x^3, y, (x^{14})^t\rangle = M'$,where $t = (x^{14}y^5)^2$. Hence $x^3, y \in M' \leq G'$. Furthermore, $(x^{14})^t \in M' \leq G'$. As G' is normal in G we see that $x^{14} \in G'$. But $gcd(3, 14) = 1$ and so $\langle x\rangle = \langle x^3, x^{14}\rangle$. Therefore $G = \langle x, y\rangle = G'$, and G is perfect.

Let N be any normal subgroup of G. If $|N|$ is even, then there is an involution $y \neq 1$ in N. By Proposition 4.1 it is either conjugate to u_1 or to w_1 in G. Using Proposition 1.3 (b) and the fusion of the conjugacy classes u_1^M, r_0^M, $(r_1r_2)^M$ of involutions of M in G it follows that

$$\langle y^G \cap M\rangle = M \leq N.$$

By Theorem 2.2 the index $|G : M|$ is odd. Hence G/N is a solvable group by the Feit-Thompson theorem. As G is perfect, we get $N = G$.

Therefore we may assume that $|N|$ is odd. As u_1 and u_2 are two commuting involutions $W = \langle u_1, u_2\rangle$ is a Klein four-group acting on the normal subgroup N. Using the computer it follows that the matrix $u_1u_2 \in GL_{1333}(11)$ has trace $tr(u_1u_2) = 9$. Since $tr(u_1u_2) = tr(u_1)$ Proposition 4.1 implies that all three involutions of W belong to u_1^G. Now the Brauer-Wielandt formula of [8], p. 198 asserts that

$$|N||C_N(W)|^2 = |C_N(u_1)|^3.$$

By Lemma 3.4 $O_{2'}(H) = 1$, because $H = C_G(u_1)$ by Proposition 4.2. Hence $C_N(u_1) = 1$. Thus $N = 1$. Therefore G is a simple group, and $G \cong J_4$ by Theorem A of Janko [11]. □

ACKNOWLEDGEMENTS

The authors of this paper have been supported by the DFG research project "Algorithmic Number Theory and Algebra".

A substantial part of the high performance computations proving Theorem 2.2 were conducted using the resources of the Cornell Theory Center, which receives major funding from the National Science Foundation and New York State with additional support from the Research Resources at the National Insitutes of Health, IBM Cooperation and members of the Corporate Research Institute. The total computing time on all the involved notes was 28137 CPU-h. We owe special thanks to Professor J. Guckenheimer and Dr. A. Hoisie for their support.

The authors also would like to thank the Computer Center of Karlsruhe University for providing 38785 CPU-h on their supercomputer IBM RS/6000 SP with 256 knots. This help was necessary to complete the above mentioned computations. We are very grateful to Professor W. Schönauer for his assistance.

References

[1] D. J. Benson, *The Simple Group J_4*. PhD. Thesis, Trinity College, Cambridge (1980).
[2] W. Bosma, J. Cannon, *MAGMA Handbook*. Sydney (1993)
[3] G. Butler, *Fundamental algorithms for permutation groups*. Lect. Notes in Computer Science, Springer Verlag, Heidelberg (1991)
[4] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford (1985).
[5] G. Cooperman, L. Finkelstein, M. Tselman, B. York, *Constructing permutation representations for large matrix groups*, J. Symbolic Computation **24** (1997), 471-488.
[6] H. W. Gollan, *A new existence proof for Ly, the sporadic group of R. Lyons.*, Preprint IEM Essen **(1995)**.
[7] D. Gorenstein, *Finite simple groups*, Plenum Press, New York (1982).
[8] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups, Number 2*, Mathematical Surveys and Monographs **40**, No. 2, American Mathematical Society, Providence, Rhode Island (1996).
[9] B. Huppert, *Endliche Gruppen I*, Grundlehren der mathematischen Wissenschaften **134**, Springer Verlag, Heidelberg (1983).
[10] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York (1972).
[11] Z. Janko, *A new finite simple group of order* $86 \cdot 775 \cdot 571 \cdot 046 \cdot 077 \cdot 562 \cdot 880$ *which possesses* M_{24} *and the full covering group of* M_{22} *as subgroups*, J. Algebra **42** (1972), 564–596.
[12] W. Lempken, *Constructing* J_4 *in* $GL(1333, 11)$, Communications in Algebra, **21** (1993), 4311–4351.
[13] S. Norton, *The construction of* J_4, Proceedings of Symposia in Mathematics AMS **37** (1980), 271-277.
[14] D. Parrott, *On the Mathieu groups* M_{22} *and* M_{11}, J. Austr. Math. Soc. **11** (1970), 69-81.
[15] M. Schönert et al., *GAP-Groups, Algorithms, and Programming*, 3rd ed., Lehrstuhl D für Mathematik, RWTH Aachen (1993).
[16] U. Schoenwaelder, *Finite groups with a Sylow 2-subgroup of type* M_{24}, II. J. Algebra **28** (1974), 46-56.
[17] M. Weller, *Construction of large permutation representations for matrix groups*, Preprint IEM Essen (1997).

College of Computer Science, Northeastern University, 161 Cullinane Hall, Boston, MA 02115, USA
E-mail address: `gene@@ccs.neu.edu`

Institut für Experimentelle Mathematik, Universität Essen-GH, Ellernstrasse 29, Essen, Germany
E-mail address: `lempken@@exp-math.uni-essen.de`
E-mail address: `archiv@@exp-math.uni-essen.de`
E-mail address: `eowmob@@exp-math.uni-essen.de`