

A characterization of finite soluble groups by laws in two variables*

John N. Bray, John S. Wilson and Robert A. Wilson

Abstract

Define a sequence (s_n) of two-variable words in variables x, y as follows: $s_0(x, y) = x$, $s_{n+1}(x, y) = [s_n(x, y)^{-y}, s_n(x, y)]$ for $n \geq 0$. It is shown that a finite group G is soluble if and only if s_n is a law of G for all but finitely many values of n .

1 Introduction

It is well known that a finite group G is nilpotent if and only if e_n is a law in G for all sufficiently large integers n , where the words e_n in the free group on x, y are defined inductively by

$$e_0(x, y) = x, \quad e_{n+1} = [e_n(x, y), y] \quad \text{for } n \geq 0$$

(see for example [?, 12.3.4 on p. 358]). In [?] a sequence v_n of words in two variables was given with the property that a finite group G is soluble if and only if v_n is a law in G for all sufficiently large integers n . However the sequence (v_n) does not have a simple recursive definition like that of the sequence (e_n) : it depends on an enumeration of the elements of a subgroup of the free group, and there is no easily described relationship between its consecutive terms. It was shown in [?] that this deficiency can be partly remedied at the cost of allowing four variables instead of two. Further progress on sequences of laws in two variables which characterize finite soluble groups was made in [?] and the preprint [?]. Here we prove the following result.

Theorem A *Define the sequence s_n of laws in two variables x, y by*

$$s_0 = x, \quad s_{n+1}(x, y) = [s_n(x, y)^{-y}, s_n(x, y)] \quad \text{for all } n \geq 0.$$

Then a finite group G is soluble if and only if s_n is a law in G for all sufficiently large integers n .

*Mathematics Subject Classification 20D10, 20D06

Our notation for conjugates and commutators is as follows: $x^y = y^{-1}xy$, $x^{-y} = y^{-1}x^{-1}y$, $[x, y] = x^{-1}x^y$.

In [?], a somewhat more complicated recursively defined sequence is given that characterizes finite soluble groups: its properties are established as a consequence of Thompson's classification [?] of the minimal simple groups, together with a fixed-point theorem whose proof depends on deep results in algebraic geometry and a substantial amount of computation. Our proof depends on the classification of the minimal simple groups, but it is otherwise self-contained.

Since the values of s_n in a group G evidently lie in the n th term of the derived series for G , soluble groups of derived length n_0 satisfy the law s_n for all $n \geq n_0$. To prove the converse, one considers a minimal counter-example: such a group is a minimal simple group. For each element u of a group G define the map $\theta_u : G \rightarrow G$ by $\theta_u(w) = [w^{-u}, w]$. Thus the images of an element w of G under the powers of the map θ_u are just the terms of the sequence $(s_n(w, u))_{n \geq 1}$. Hence Theorem A is an immediate consequence of the following result.

Theorem B *Every minimal simple group S has an involution u and a non-empty subset X with $\theta_u(X) \subseteq X$ and $1 \notin X$.*

Thompson's classification of the minimal simple groups implies that the minimal simple groups are to be found among the groups $L_2(q)$ with q a prime power such that $q \geq 5$, the Suzuki groups $Sz(q)$ with $q = 2^{2m+1} \geq 8$, together with the group $L_3(3)$. Sections 2 and 3 are dedicated to groups $SL_2(F)$ and Suzuki groups respectively: they contain results giving immediately the assertion of Theorem B for groups of types $L_2(q)$ and $Sz(q)$. The case of $L_3(3) \cong SL_3(3)$ is easy and we deal with it here. Let u, w be the matrices in $SL_3(3)$ given below:

$$u = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{and} \quad w = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Clearly $u^2 = 1$ and it is routine to verify that $\theta_u^4(w) = w \neq \theta_u^2(w)$; thus the set $X = \{w, \theta_u(w), \theta_u^2(w), \theta_u^3(w)\}$ is permuted as a 4-cycle by θ_u and certainly does not contain the identity matrix.

2 Groups of type $SL_2(F)$

In order to prove Theorem B for groups $S \cong L_2(q)$ it is sufficient to work with groups $SL_2(F)$ with F finite of order at least 5 and to find an element $u \in SL_2(F)$ and a subset

X of $\mathrm{SL}_2(F)$ with $u^2 = \pm 1$, $\theta_u(X) \subseteq X$ and $\pm 1 \notin X$. Let F be an arbitrary field and fix the element

$$u = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

of $\mathrm{SL}_2(F)$. Thus $u^2 = -1$. We recall that $\theta_u : \mathrm{SL}_2(F) \rightarrow \mathrm{SL}_2(F)$ is the map defined by $\theta_u(w) = [w^{-u}, w]$. Let

$$w = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \theta_u(w) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

Easy calculations show that

$$[u, w^{-1}] = \begin{pmatrix} c^2 + d^2 & -ac - bd \\ -ac - bd & a^2 + b^2 \end{pmatrix}, \quad [u, w] = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix},$$

and so since $\theta_u(w) = [u, w^{-1}][u, w]$ we have

$$\begin{aligned} A &= (a^2 + c^2)(c^2 + d^2) - (ab + cd)(ac + bd), \\ B &= (c^2 + d^2)(ab + cd) - (b^2 + d^2)(ac + bd), \\ C &= (a^2 + b^2)(ab + cd) - (a^2 + c^2)(ac + bd), \\ D &= (a^2 + b^2)(b^2 + d^2) - (ab + cd)(ac + bd). \end{aligned}$$

Let $\Delta = (a - d)^2 + (b + c)^2$. From above we have

$$\begin{aligned} A - D &= -(b + c)(b - c)(a^2 + b^2 + c^2 + d^2), \\ B + C &= (a - d)(b - c)(a^2 + b^2 + c^2 + d^2), \\ B - C &= -(a + d)(b - c)\Delta, \end{aligned}$$

and

$$\begin{aligned} A + D &= (b - c)^2\Delta + 2(ad - bc)^2 \\ &= (b - c)^2\Delta + 2. \end{aligned}$$

Now we observe that

$$a^2 + b^2 + c^2 + d^2 = (a - d)^2 + (b + c)^2 + 2(ad - bc) = \Delta + 2,$$

and thus we find that

$$(A - D)^2 + (B + C)^2 = (b - c)^2(\Delta + 2)^2((b + c)^2 + (a - d)^2) = (b - c)^2(\Delta + 2)^2\Delta.$$

THEOREM 2.1. *Let $\mathrm{char} F = 2$. If $|F| > 2$ then $\mathrm{SL}_2(F)$ has a non-empty subset X such that $\theta_u(X) \subseteq X$ and such that $1 \notin X$.*

Proof. Let

$$w = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(F) \quad \text{and} \quad \theta_u(w) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}.$$

From above we have

$$\begin{aligned} A + D &= (b + c)^2(a + b + c + d)^2, \\ B + C &= (a + d)(b + c)(a + b + c + d)^2, \\ A + B + C + D &= (b + c)(a + b + c + d)^3. \end{aligned}$$

Thus $0 \in \{a + d, b + c, a + b + c + d\}$ if and only if $0 \in \{A + D, B + C, A + B + C + D\}$. Define X to be the set of matrices w such that $0 \notin \{a + d, b + c, a + b + c + d\}$. It follows that $\theta_u(X) \subseteq X$ and clearly the identity matrix is not in X . For $\mu \notin \{0, 1\}$ we have

$$t = \begin{pmatrix} 1 & 1 \\ \mu & \mu + 1 \end{pmatrix} \in X.$$

The result follows.

THEOREM 2.2. *Let $\text{char } F \neq 2$. If $|F| > 3$ then $\text{SL}_2(F)$ has a non-empty subset X such that $\theta_u(X) \subseteq X$ and such that $\pm 1 \notin X$.*

Proof. Write F^* for the multiplicative group of F , define $Q = \{\mu^2 \mid \mu \in F^*\}$ and let $N = F^* \setminus Q$. If $F = \mathbb{Q}$ or F is finite then we have $Q \neq F^*$. However if $Q = F^*$ then F clearly contains either \mathbb{Q} or a field of order p^2 for some prime $p > 2$; thus $\text{SL}_2(F)$ contains either $\text{SL}_2(\mathbb{Q})$ or a group $\text{SL}_2(p^2)$. Therefore in the proof below we may assume that $Q \neq F^*$.

We use the same notation as above for the entries of a matrix $w \in \text{SL}_2(F)$ and of its image $\theta_u(w)$, and we write $\Delta = (a - d)^2 + (b + c)^2$. Let X be the set of matrices w such that $a + d \neq 0$, $b - c \neq 0$ and $-2\Delta \in N$. We proceed to show that $\theta_u(X) \subseteq X$.

Suppose that $w \in X$. Since $a + d$, $b - c$ and Δ are all non-zero, $B - C$ is also non-zero. Moreover $(b - c)^2 \cdot (-2\Delta) \in N$ so that $(b - c)^2 \cdot (-2\Delta) \neq 4$ and $A + D$ is non-zero. Now note that if $\Delta + 2 = 0$, then $-2\Delta = 4 \in Q$, a contradiction. So $\Delta + 2 \neq 0$ and hence

$$-2((A - D)^2 + (B + C)^2) = (b - c)^2(\Delta + 2)^2(-2\Delta) \in N.$$

Thus we have now shown that $\theta_u(X) \subseteq X$. Clearly $\pm 1 \notin X$.

To complete the proof, we must show that X is non-empty whenever $|F| > 3$. If $-2 \in N$ then we have

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in X.$$

In particular, if $|F| = 5$ then $-2 \in N$ and $X \neq \emptyset$. Suppose then that $-2 \in Q$, so that $|F| \geq 7$. We shall consider

$$w = \begin{pmatrix} \mu & 0 \\ \lambda(\mu - \mu^{-1}) & \mu^{-1} \end{pmatrix},$$

where $\mu^2 \notin \{0, \pm 1\}$ and $\lambda \neq 0$. Since $|F| \geq 7$ there is an element μ with the required properties. The conditions on μ and λ guarantee that both $a + d = \mu + \mu^{-1}$ and $b - c = -\lambda(\mu - \mu^{-1})$ are non-zero. We then find that

$$-2((a - d)^2 + (b + c)^2) = -2(\lambda^2 + 1)(\mu - \mu^{-1})^2,$$

and so the requirement (for $w \in X$) that this be in N is equivalent to $-2(\lambda^2 + 1) \in N$, or to $\lambda^2 + 1 \in N$, since $-2 \in Q$. Suppose that there is no λ with this property; then for all $\lambda \in F^*$ we have $\lambda^2 + 1 \in Q \cup \{0\}$, and so for all $\lambda_1, \lambda_2 \in F$ we have $\lambda_1^2 + \lambda_2^2 \in Q \cup \{0\}$. This implies that $-1 = (-2) + 1 \in Q$, so that there is an element i with $i^2 = -1$, and that for each $x \in F^*$ we have

$$x = \frac{1}{4}((x + 1)^2 - (x - 1)^2) = \frac{1}{4}((x + 1)^2 + ((x - 1)i)^2) \in Q.$$

This is a contradiction to the assumption that $Q \neq F^*$ and the result follows.

3 The case $G \cong \text{Sz}(q)$

We begin by recalling the definition of the Suzuki groups and explaining our notation for some of its elements. Let m be a positive integer, write $q = 2^{2m+1}$ and $s = \sqrt{2q} = 2^{m+1}$, and let $F = \mathbb{F}_q$. For $\lambda \in F$, the maps $\lambda \mapsto \lambda^s$ and $\lambda \mapsto \lambda^2$ are automorphisms of F . Moreover, we have $\lambda^{s^2} = \lambda^2$ for all $\lambda \in F$. For $a, b \in F$, we define

$$T(a, b) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ a^{1+s} + b & a^s & 1 & 0 \\ a^{2+s} + ab + b^s & b & a & 1 \end{pmatrix}.$$

The set H of elements $T(a, b)$ is a group of order q^2 with multiplication given by

$$T(a, b)T(c, d) = T(a + c, ac^s + b + d).$$

For $k \in F^*$ we define

$$D(k) := \begin{pmatrix} k^{s/2+1} & 0 & 0 & 0 \\ 0 & k^{s/2} & 0 & 0 \\ 0 & 0 & k^{-s/2} & 0 \\ 0 & 0 & 0 & k^{-s/2-1} \end{pmatrix}.$$

The set D of elements $D(k)$ is a group of order $q - 1$ and we have $D(k)^{-1}T(a, b)D(k) = T(a, b)^{D(k)} = T(ak, bk^{1+s})$, so that the group L generated by H, D is the split extension $H \rtimes D$ and has order $q^2(q - 1)$. Finally, we define

$$z := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Clearly $\langle D, z \rangle$ is a dihedral group. Let $G = \langle L, z \rangle$. Then each element of $G \setminus L$ can be written uniquely in the form $h_1 d z h_2$ with $h_1, h_2 \in H, d \in D$, and so $|G| = q^2(q-1)(q^2+1)$. The group G is isomorphic to the Suzuki group $\text{Sz}(q)$: this is the description given by Suzuki [?, p. 133], but with slightly different notation.

THEOREM 3.1. *For all $q \geq 8$ the group $\text{Sz}(q)$ has an involution u and a non-empty subset X with $\theta_u(X) \subseteq X$ and $1 \notin X$.*

Proof. We begin by defining the element u and the set X . Let

$$u = T(0, 1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Then u is an involution in H and $C_G(u) = H$. Now define $Y = Y_1 \cup Y_2 \cup Y_3$ and $X = G \setminus Y$ where

- (i) $Y_1 = L$,
- (ii) Y_2 consists of the matrices in G of trace 0, and
- (iii) Y_3 consists of those $g \in G$ such that $(ug)^2 = 1$.

Clearly $1 \notin X$. We also observe immediately that X is non-empty. Indeed, choose $b \notin \{0, 1\}$, and consider the matrix

$$x := T(0, b)D(1)z = T(0, b)z = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & b \\ 1 & 0 & b & b^s \end{pmatrix}.$$

Thus $x \notin Y_1 = L$, and x has trace b^s , so that $x \notin Y_2$. Finally, we calculate that the $(1, 3)$ -entry of $(ux)^2$ is $b + 1 \neq 0$, so that $x \notin Y_3$. Therefore $x \in X$.

We shall prove that $\theta_u(X) \subseteq X$ by showing that

$$\text{if } \theta_u(w) \in Y \text{ then } w \in Y.$$

We begin by making a reduction, using the fact that each of the sets Y_1, Y_2 and Y_3 is invariant under conjugation by the elements of $H = C_G(u)$. Clearly we may restrict attention to elements w not in $Y_1 = L$; each such element w is in $HDzH$ and so can be written in the form \tilde{w}^h with $\tilde{w} \in HDz$. The invariance of each Y_i under H and the fact that $\theta_u(\tilde{w}^h) = (\theta_u(\tilde{w}))^h$ (since $h \in H = C_G(u)$) show that $w \in Y$ if and only if $\tilde{w} \in Y$ and that $\theta_u(w) \in Y_2 \cup Y_3$ if and only if $\theta_u(\tilde{w}) \in Y_2 \cup Y_3$. Therefore it is sufficient to prove that

$$\text{if } \tilde{w} \in HDz \text{ and } \theta_u(\tilde{w}) \in Y \text{ then } \tilde{w} \in Y_2 \cup Y_3. \quad (*)$$

Let \tilde{w} be an element of HDz such that $\theta_u(\tilde{w}) \in Y$. Write $\tilde{w} = T(a, b)D(k)z$ where $a, b, k \in F$ and $k \neq 0$, and write $\theta_u(\tilde{w}) = M = (M_{ij})$.

LEMMA 3.2. *The entries M_{ij} of the matrix M are as follows:*

$$\begin{aligned}
M_{11} &= 1 + k^{s+1}(b+1) + k^{s+2}\xi \\
M_{12} &= k^{s+1}a^s + k^{s+2}(a^{s+1} + b + 1) \\
M_{13} &= k^{s+2}a + k^{2s+2}(b+1) + k^{2s+3}\xi \\
M_{14} &= k^{2s+2}a^s + k^{2s+3}a^{s+1} + k^{2s+4}\xi \\
M_{21} &= k^{s+1}(a^{s+2} + b^s + 1) + k^{s+2}a\xi \\
M_{22} &= 1 + k^{s+1}(b+1) + k^{s+2}(a^{s+2} + ab + a) \\
M_{23} &= k^{s+2}a^2 + k^{2s+2}(a^{s+2} + b^s + 1) + k^{2s+3}a\xi \\
M_{24} &= k^{s+2}a + k^{2s+2}(b+1) + k^{2s+3}(a^{s+2} + \xi) + k^{2s+4}a\xi \\
M_{31} &= M_{42} = k^{s+1}\mu + k^{s+2}\nu \\
M_{32} &= k^{s+2}(a^{s+1} + b + 1)^2 \\
M_{33} &= 1 + k^{s+1}(b+1) + k^{s+2}(a^{s+2} + ab + a) + k^{2s+2}\mu + k^{2s+3}\nu \\
M_{34} &= k^{s+1}a^s + k^{s+2}(a^{s+1} + b + 1) + k^{2s+3}(a^s b^s + a^s) + k^{2s+4}\nu \\
M_{41} &= k^{s+2}\xi^2 \\
M_{43} &= k^{s+1}(a^{s+2} + b^s + 1) + k^{s+2}a\xi + k^{2s+3}\xi^2 \\
M_{44} &= 1 + k^{s+1}(b+1) + k^{s+2}\xi + k^{2s+2}\mu + k^{2s+3}\nu + k^{2s+4}\xi^2,
\end{aligned}$$

where

$$\begin{aligned}
\mu &= a^{2s+2} + a^s b^s + a^s + b^2 + 1 \\
\nu &= a\mu + (b+1)(b^s + 1) \\
\xi &= a^{s+2} + b^s + ab + a + 1.
\end{aligned}$$

The proof of the lemma is a routine but tedious calculation which can be carried out either by hand or using one of the standard computer algebra packages such as MAGMA [?].

We proceed now to prove the assertion (*).

Case 1. Suppose that $M \in Y_1 = L$.

Here we have $M_{12} = M_{13} = M_{14} = 0$, and hence

$$k^{s+1}M_{12} + kM_{13} + M_{14} = ak^{s+3} = 0.$$

Thus $a = 0$ since $k \neq 0$. The equation $M_{12} = 0$ now becomes $k^{s+2}(b+1) = 0$, so that $b = 1$. Therefore $\tilde{w} = T(0,1)D(k)z$ for some $k \in F^*$; but then $u\tilde{w} = D(k)z$ is an involution in the dihedral group $D\langle z \rangle$, and thus $\tilde{w} \in Y_3$.

Case 2. Suppose that $M \in Y_2$.

Here we have $M_{11} + M_{22} + M_{33} + M_{44} = 0$. This gives the equation $k^{2s+4}\xi^2 = 0$, and so since $k \neq 0$ we have $\xi = 0$. It follows that

$$a^s \xi + \xi^s = a^{s+1}b + a^{s+1} + b^2 + 1 = 0,$$

giving $a^{s+1}(b+1) + (b+1)^2 = 0$, whence $b = 1$ or $a^{s+1} = b+1$. If $a^{s+1} = b+1$ then the equation $\xi = 0$ becomes $b^s + 1 = 0$, and we obtain that $b = 1$.

Therefore $b = 1$. Now the equation $\xi = 0$ becomes $a^{s+2} = 0$ and we have $a = 0$. Thus $\tilde{w} = T(0, 1)D(k)z$, and we have already seen that this element lies in Y_3 .

Case 3. Suppose that $M \in Y_3$.

We need to determine the form of the typical element of $Y_3 \setminus Y_1$. We recall that Y_3, Y_1 are invariant under conjugation by $H = C_G(u)$. Each element g of $G \setminus Y_1$ has the form $\tilde{g}^{T(c,d)}$ where $\tilde{g} \in HDz \subseteq G \setminus Y_1$, and $g \in Y_3$ if and only if $\tilde{g} \in Y_3$. Writing $\tilde{g} = T(\alpha, \beta)D(\lambda)z$, we have $(u\tilde{g})^2 = 1$ if and only if $(T(\alpha, \beta+1)D(\lambda)z)^2 = 1$, or equivalently if and only if

$$T(\alpha, \beta+1)D(\lambda) = zD(\lambda)^{-1}(T(\alpha, \beta+1)^{-1})z$$

Since the right-hand side here is an upper-triangular matrix this equation implies that $\alpha = 0$ and $\beta = 1$. Thus the typical element of $Y_3 \setminus Y_1$ has the form

$$N := (T(0, 1)D(l)z)^{T(c,d)},$$

where $c, d, l \in F$ and $l \neq 0$.

Therefore, we must solve the equation $M = N$. Another calculation gives some of the matrix entries of N :

LEMMA 3.3. *Some entries N_{ij} of the matrix $N = (T(0, 1)D(l)z)^{T(c,d)}$ are as follows:*

$$\begin{aligned} N_{11} &= l^{s/2+1}(c^{s+2} + d^s + cd) \\ N_{12} &= l^{s/2+1}d \\ N_{13} &= N_{24} = l^{s/2+1}c \\ N_{14} &= l^{s/2+1} \\ N_{22} &= l^{s/2}c^s + l^{s/2+1}cd \\ N_{31} &= l^{-s/2}c + l^{s/2}(c^{2s+1} + c^s d) + l^{s/2+1}(c^{s+2} + cd + d^s + c^{s+2}d + cd^2 + d^{s+1}) \\ N_{34} &= l^{s/2+1}(d+1) \\ N_{42} &= l^{-s/2}c + l^{s/2}(c^{2s+1} + c^s d + c^s) + l^{s/2+1}(c^{s+2}d + d^{s+1} + cd^2 + cd + d). \end{aligned}$$

From the information in this lemma we have (for all values of c, d and l)

$$\begin{aligned} N_{11} + N_{12} + N_{22} + N_{31} + N_{42} &= 0, \\ N_{13} + N_{24} &= 0, \\ N_{12} + N_{14} + N_{34} &= 0. \end{aligned}$$

Considering the three corresponding equations for entries of M , and dividing by $k^{s+2}, k^{2s+4}, k^{2s+4}$, we obtain the equations

$$a^{s+1} + b + a^s k^{-1} + b^s = 0, \tag{1}$$

$$a^{s+3} + a^2b + a^{s+2}k^{-1} + a^2 + ab^s + a = 0, \quad (2)$$

$$a^{2s+3} + a^{s+2} + ab^2 + ab + a^{s+1}b^s + a^{s+1} + b^{s+1} + b + (a^{s+1} + a^s b^s + a^s)k^{-1} + a^s k^{-2} = 0. \quad (3)$$

Multiplying Equation (1) by a^2 and adding (2) we obtain

$$a^2b^s + a^2 + ab^s + a = a(a+1)(b^s + 1) = 0,$$

so that either $a \in \{0, 1\}$ or $b = b^{s^2}b^{-1} = b^{-1}$ and hence $b = 1$.

First suppose that $a = 0$. Then (1) becomes $b+b^s = 0$, and so we have $b = b^s = b^{s^2} = b^2$ and hence $b = 0$ or $b = 1$. If $(a, b) = (0, 0)$ then $\tilde{w} = D(k)z$, which has trace 0, and so lies in Y_2 . The case $(a, b) = (0, 1)$ has arisen before: we have $T(0, 1)D(k)z \in Y_3$.

Next suppose that $b = 1$ and $a \neq 0$. Then (1) gives $a^s(a + k^{-1}) = 0$ and so we have $a = k^{-1}$. Equation (3) yields that $a^{s+1} + 1 = 0$ and hence $a = a^{s^2-1} = (a^{s+1})^{s-1} = 1$.

Suppose that $a = 1$. We note that for all $\beta \in F$, $\kappa \in F^*$ the matrix $T(1, \beta)D(\kappa)z$ has diagonal entries $0, 0, \kappa^{s/2}, \kappa^{s/2+1}(\beta + \beta^s + 1)$ and hence trace $\kappa^{s/2}(1 + \kappa(\beta + \beta^s + 1))$. Thus when $a = 1$, Equation (1) yields that $(b + b^s + 1) + k^{-1} = 0$ and that $\tilde{w} = T(1, b)D(k)z$ has trace 0 and lies in Y_2 .

This concludes the proof of Theorem 3.1.

References

- [1] T. Bandman, G.-M. Greuel, F. Grunewald, B. Kunyavskii, G. Pfister and E. Plotkin. Engel-like identities characterizing finite soluble groups. [arXiv:math.GR/0303165](https://arxiv.org/abs/math/0303165) v1, 13 March 2003.
- [2] Rolf Brandl and John S. Wilson. Characterization of finite soluble groups by laws in a small number of variables. *J. Algebra* **116** (1988), 334–341.
- [3] J. J. Cannon *et al.* The MAGMA programming language, version 2.8. School of Mathematics and Statistics, University of Sydney (2001).
- [4] F. Grunewald, B. Kunyavskii, D. Nikolova and E. Plotkin. Two-variable identities in groups and Lie algebras. *Zap. Nauchn. Sem. S.-Peterburg Otdel. Mat. Inst. Steklov. (POMI)* **272** (2000), 161–176.
- [5] D. J. S. Robinson. *A course in the theory of groups* (Springer-Verlag, 1982).
- [6] M. Suzuki. On a class of doubly transitive groups. *Ann. of Math. (2)* **75** (1962), 105–145.
- [7] J. G. Thompson. Nonsolvable groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* **74** (1968), 383–437.

Authors' addresses

John N. Bray, School of Mathematics and Statistics, University of Birmingham, Edgbaston, Birmingham B15 2TT

E-mail: `jnb@maths.bham.ac.uk`

John S. Wilson, Mathematical Institute, 29–29 St Giles', Oxford OX1 3LB

E-mail: `wilsonjs@maths.ox.ac.uk`

Robert A. Wilson, School of Mathematics and Statistics, University of Birmingham, Edgbaston, Birmingham B15 2TT

E-mail: `raw@maths.bham.ac.uk`