

Verbal width in the Nottingham group and related Lie algebras

Jorge Martínez Carracedo¹

School of Computing. Ulster University.

Consuelo Martínez López²

Departamento de Matemáticas. Universidad de Oviedo.

Abstract

In [1], B. Klopsch proved that the Nottingham group over a finite field is verbally elliptic. We prove a similar result for fields of zero characteristic. We also prove that the Virasoro Lie algebra and some of its subalgebras are polynomially elliptic.

Keywords: Group; Lower central series; Graded Lie algebra; Nottingham group; Virasoro algebra; Witt algebra; Verbal width; Ellipticity.

1. Introduction

Let $\omega(x_1, \dots, x_k)$ be an element of the free group on k free generators x_1, \dots, x_k . We will refer to elements of free groups as words.

Let G be a group. The verbal subgroup $\omega(G)$ is the subgroup of G generated by the verbal set

$$\omega[G] = \{\omega(g_1, \dots, g_k) \mid g_i \in G, 1 \leq i \leq k\}.$$

The word ω is said to have finite width in the group G if there exists $d \geq 1$ such that every element g in the verbal subgroup $\omega(G)$ can be expressed as $g = g_1^{\pm 1} \dots g_d^{\pm 1}$, where $g_i \in \omega[G]$.

Email addresses: j.martinez-carracedo@ulster.ac.uk (Jorge Martínez Carracedo), cmartinez@uniovi.es (Consuelo Martínez López)

¹Shore Rd, Newtownabbey, BT37 0QB, Northern Ireland (U.K.)

²C/Federico García Lorca, 18, 33007, Oviedo, Spain

If a word ω has finite width in a group G , we say that the group G is ω -elliptic. If all words have finite width in the group G , then the group G is called verbally elliptic.

10 It is clear that every word ω has finite length in a finite group G and the verbal width of ω over G is upper bounded by $|G|$ (see [2]).

Martínez and Zelmanov [3] and, independently, Saxl and Wilson [4] proved that for any natural number n , there is a function $N = N(n)$ such that the width of the word $\tau = x^n$ in any finite simple group is bounded by N .

15 An important result related to verbally elliptic groups was proved by P. Stroud [5]: Every finitely generated abelian-by-nilpotent group is verbally elliptic.

Rhemtulla [6] poses the question of the existence of nontrivial words having finite verbal width in every group G . He proved that a word ω in the free group
20 \mathcal{F}_k has finite width in every group G if and only if there exist relatively prime integers i_1, \dots, i_k such that $\omega \in x_1^{i_1} \dots x_k^{i_k} \mathcal{F}_k'$.

Romankov [7] proved that every finitely generated virtually nilpotent group is verbally elliptic. Segal proved in [2] a more general result using the Prüfer rank of a group defined as

$$rk(G) := \sup\{d(K) \mid K \text{ is a finitely generated subgroup of } G\}.$$

25 Here, $d(G)$ denotes the minimum possible number of generators of the group G . So in [2] it is proved that every virtually nilpotent group with finite Prüfer rank is verbally elliptic.

J.P. Serre [8] considered the same question for profinite groups and Brian Hartley [9] proved that a word ω has finite width in a profinite group G if and
30 only if the verbal subgroup $\omega(G)$ is closed in G .

Andrei Jaikin-Zapirain ([10]) proved that p -adic analytic pro- p -groups are verbally elliptic.

In [11] C. Martínez proved that if Γ is a finitely generated residually- p -torsion group and G is its pro- p -completion, then the group G is verbally elliptic

35 (understanding that a word ω is an arbitrary element in the free pro- p -group on countably many variables).

For a good survey of what is known about verbal subgroups we refer to the book [2]. In this paper we will prove that the Nottingham group in zero characteristic is verbally elliptic. The same result was proved by B. Klopsch in
 40 [12] for the Nottingham group over a finite field. In the paper we will consider a similar question for Lie algebras, proving that the Virasoro algebra and some of its subalgebras, that are related to the Nottingham group, are polynomially elliptic.

2. Lie algebras

45 Let ϕ be an associative commutative ring. Consider an absolutely free algebra $\phi\langle X \rangle$ on the set of free generators $X = \{x_1, x_2, \dots\}$. Let $f(x_1, \dots, x_k) \in \phi\langle X \rangle$. For a ϕ -algebra \mathcal{A} consider the set $f[\mathcal{A}] = \{f(a_1, \dots, a_k) \mid a_1, \dots, a_k \in \mathcal{A}\}$ and the ϕ -linear span $\text{Span}_\phi f[\mathcal{A}]$.

Definition 2.1. (see [11]) *A polynomial f has finite width in the algebra \mathcal{A} if there exists $d \geq 1$ such that*

$$\text{Span}_\phi f[\mathcal{A}] = \underbrace{f[\mathcal{A}] + \dots + f[\mathcal{A}]}_d.$$

In other words, every element $a \in \text{Span}_\phi f[\mathcal{A}]$ can be written as

$$a = f(a_1^{(1)}, \dots, a_k^{(1)}) + \dots + f(a_1^{(d)}, \dots, a_k^{(d)}),$$

where $a_i^{(j)} \in \mathcal{A}$, $1 \leq i \leq k$, $1 \leq j \leq d$.

50 We will define now a stronger notion for multilinear polynomials.

Definition 2.2. *A multilinear polynomial $f(x_1, \dots, x_k)$ is **strongly elliptic** in \mathcal{A} if there exists a finite set of $(k-1)$ -tuples, $M \subset \underbrace{\mathcal{A} \times \dots \times \mathcal{A}}_{k-1}$ such that*

$$f[\mathcal{A}] \subset \sum_{(a_1, \dots, a_{k-1}) \in M} f(\mathcal{A}, a_1, \dots, a_{k-1}).$$

Lemma 2.1. *If a multilinear polynomial $f(x_1, \dots, x_k)$ is strongly elliptic in \mathcal{A} then f has finite width in \mathcal{A} .*

Proof. It is enough to consider the expression

$$\text{Span}_{\mathbb{F}} f[\mathcal{A}] = \sum_{(a_1, \dots, a_{n-1}) \in M} f(\mathcal{A}, a_1, \dots, a_{n-1}),$$

and note that the number of terms to the right is always less than or equal to $|M|$. □

55 Fix a field \mathbb{F} of zero characteristic.

The *centerless Virasoro algebra*, Vir , is the algebra over \mathbb{F} having a basis $\{e_i \mid i \in \mathbb{Z}\}$ with the multiplication $[e_i, e_j] = (i - j)e_{i+j}$.

Theorem 2.2. *An arbitrary multilinear polynomial is strongly elliptic in Vir .*

Proof. Consider $f(x_0, x_1, \dots, x_{n-1})$ a multilinear element of the free Lie algebra. We have that

$$f = \sum_{\pi \in S_{n-1}} \alpha_{\pi} [x_0, x_{\pi(1)}, \dots, x_{\pi(n-1)}], \quad \alpha_{\pi} \in \mathbb{F},$$

where $[x_0, x_1.x_2] = [[x_0, x_1], x_2]$ and inductively,

$$[x_0, x_1, \dots, x_{t+1}] = [[x_0, x_1, \dots, x_t], x_{t+1}].$$

Let M be the finite set given by

$$M = \{(e_{i_1}, \dots, e_{i_{n-1}}) \mid 0 \leq i_1, \dots, i_{n-1} \leq n\}.$$

We want to prove that

$$Vir = \sum_{(e_{i_1}, \dots, e_{i_{n-1}}) \in M} f(Vir, e_{i_1}, \dots, e_{i_{n-1}}).$$

Notice that for an arbitrary $s \in \mathbb{Z}$, we have that

$$f(e_{s-i_1-\dots-i_{n-1}}, e_{i_1}, \dots, e_{i_{n-1}}) = h(s, i_1, \dots, i_{n-1})e_s,$$

where

$$\begin{aligned}
& h(s, i_1, \dots, i_{n-1}) = \\
& = \sum \alpha_\pi (s - i_1 - \dots - i_{n-1} - i_{\pi(1)}) (s - i_1 - \dots - i_{n-1} + i_{\pi(1)} - i_{\pi(2)}) \dots \\
& \dots (s - i_1 - \dots - i_{n-1} + i_{\pi(1)} + i_{\pi(2)} + \dots + i_{\pi(n-2)} - i_{\pi(n-1)}),
\end{aligned}$$

is a homogeneous polynomial in s, i_1, \dots, i_{n-1} of degree $n - 1$.

60 If $f = 0$ is an identity in Vir , then there is nothing to prove. So we will assume that $f(Vir) \neq (0)$. Then $Span_{\mathbb{F}} f[Vir]$ is a non-zero ideal of Vir and Vir is simple, what implies that $Vir = Span_{\mathbb{F}} f[Vir]$.

If there is an integer s such that

$$e_s \notin \sum_{(e_{i_1}, \dots, e_{i_{n-1}}) \in M} f(e_{s-i_1-\dots-i_{n-1}}, e_{i_1}, \dots, e_{i_{n-1}}),$$

then $h(s, i_1, \dots, i_{n-1}) = 0$ for every $(n - 1)$ -tuple $(i_1, \dots, i_{n-1}) \in [0, n]^{n-1}$.

65 But this implies that the polynomial $g(x_1, \dots, x_{n-1}) = h(s, x_1, \dots, x_{n-1})$ (non homogeneous) has degree at most $n - 1$ and it is 0 over $[0, n]^{n-1}$. Consequently g is the zero polynomial, or equivalently, $h(s, x_1, \dots, x_{n-1})$ is the zero polynomial.

But $e_s \in Span_{\mathbb{F}} f[Vir]$, so there are integers j_1, \dots, j_{n-1} such that

$$f(e_{s-j_1-\dots-j_{n-1}}, e_{j_1}, \dots, e_{j_{n-1}}) = \lambda e_s,$$

with $\lambda = h(s, j_1, \dots, j_{n-1}) \neq 0$. This contradiction proves the theorem. □

Let $k \geq -1$. Then $Vir^{(k)} = \sum_{i=k}^{\infty} Fe_i$ is a subalgebra of Vir .

70 **Theorem 2.3.** *An arbitrary multilinear polynomial is strongly elliptic in $Vir^{(k)}$.*

Proof. Let

$$f(x_0, x_1, \dots, x_{n-1}) = \sum_{\pi \in S_{n-1}} \alpha_\pi [x_0, x_{\pi(1)}, \dots, x_{\pi(n-1)}], \quad \alpha_\pi \in F,$$

be a multilinear element of the free Lie algebra that is not identical on $Vir^{(k)}$.

As above,

$$f(e_{s-i_1-\dots-i_{n-1}}, e_{i_1}, \dots, e_{i_{n-1}}) = h(s, i_1, \dots, i_{n-1})e_s,$$

for arbitrary integers $i_1, \dots, i_{n-1}, s \in \mathbb{Z}$.

Consider the finite set $M_1 = \{(e_{i_1}, \dots, e_{i_{n-1}}) \mid k \leq i_1, \dots, i_{n-1} \leq k+n\}$.

We will show that

$$Vir^{((k+n)(n-1)+k)} \subseteq \sum_{(e_{i_1}, \dots, e_{i_{n-1}}) \in M_1} f(Vir^{(k)}, e_{i_1}, \dots, e_{i_{n-1}}).$$

Indeed, if $s \geq (k+n)(n-1) + k$ and $(e_{i_1}, \dots, e_{i_{n-1}}) \in M_1$ then

$$s - i_1 - \dots - i_{n-1} \geq k.$$

If for all $(e_{i_1}, \dots, e_{i_{n-1}}) \in M_1$ we have

$$f(e_{s-i_1-\dots-i_{n-1}}, e_{i_1}, \dots, e_{i_{n-1}}) = h(s, i_1, \dots, i_{n-1})e_s = 0,$$

then arguing as above we conclude that $h(s, i_1, \dots, i_{n-1})$ is the zero polynomial.

75 For every $k \leq j < (k+n)(n-1) + k$ such that $e_j \in \text{Span}_F f[Vir^{(k)}]$ choose elements $a_0^j, \dots, a_{n-1}^j \in \{e_i \mid i \geq k\}$ such that $e_j = f(a_0^j, \dots, a_{n-1}^j)$.

Let $M_2 = M_1 \cup \{(a_1^j, \dots, a_{n-1}^j)\}$. Then

$$\text{Span}_F f[Vir^{(k)}] = \sum_{(a_1, \dots, a_{n-1}) \in M_2} f(Vir^{(k)}, a_1, \dots, a_{n-1}).$$

This completes the proof of the theorem. □

80 The following theorem concerns ideals I of a Lie ring $Vir^{(k)}$, $k \geq -1$. It means that we do not assume, a priori, that I is an F -vector subspace.

Theorem 2.4. *An arbitrary nonzero ideal of a Lie ring $Vir^{(k)}$, $k \geq -1$, contains $Vir^{(l)}$ for some $l \geq k$.*

Proof. Let $I \neq (0)$ be an ideal of the Lie ring $Vir^{(k)}$. Let $0 \neq a = \alpha_1 e_{i_1} + \alpha_2 e_{i_2} + \dots + \alpha_m e_{i_m} \in I$; $0 \neq \alpha_i \in F$, $1 \leq i \leq m$; $k \leq i_1 < \dots < i_m$ and m a
85 minimal integer with this property.

If $m \geq 2$ then

$$0 \neq [a, e_{i_1}] = \alpha_2(i_2 - i_1)e_{i_1+i_2} + \alpha_3(i_3 - i_1)e_{i_1+i_3} + \cdots + \alpha_m(i_m - i_1)e_{i_1+i_m} \in I,$$

which contradicts minimality of m . Hence $m = 1$, the ideal I contains an element αe_i , $0 \neq \alpha \in F$, $i \geq k$. It is easy to see that in this case $Vir^{(i+k)} = [\alpha e_i, Vir^{(k)}] \subseteq I$. This completes the proof of the theorem. \square

3. Nottingham Group in Characteristic 0

90 Given a field \mathbb{F} , consider the set of infinite series

$$N_{\mathbb{F}}(t) := \{t + \sum_{k \geq 1} \alpha_k t^{k+1} \mid \alpha_k \in \mathbb{F} \quad k \in \mathbb{N}\}.$$

with the group multiplication

$$fg := g(f); f, g \in N_{\mathbb{F}}(t)$$

For a finite field $\mathbb{F} = GF(p^k)$, the group $N_{\mathbb{F}}(t)$ is a finitely generated pro- p -group that has been widely studied in the literature.

As always $O(t^n)$ stands for a formal series lying in $t^n F[[t]]$.

Lemma 3.1. [13]

- 95
1. If $f = t + \alpha t^n + O(t^{n+1})$, $g = t + \beta t^n + O(t^{n+1})$, where $\alpha, \beta \in \mathbb{F}$, $n \geq 2$, then $fg = t + (\alpha + \beta)t^n + O(t^{n+1})$.
 2. If $f = t + \alpha t^n + O(t^{n+1})$, $0 \neq \alpha \in \mathbb{F}$, then $f^{-1} = t - \alpha t^n + O(t^{n+1})$.
 3. If $f = t + \alpha t^n + O(t^{n+1})$, $g = t + \beta t^m + O(t^{m+1})$, where $\alpha, \beta \in \mathbb{F}$, $n, m \geq 2$, then $[f, g] = t + \alpha\beta(n - m)t^{n+m-1} + O(t^{n+m})$.

100 Notice that the Nottingham group over a field of characteristic 0 is torsion free.

Lemma 3.2. Let $\text{char}\mathbb{F} = 0$. Then for an arbitrary integer $n \geq 1$ and an arbitrary element $g \in N_{\mathbb{F}}(t)$ there exists a unique element $h \in N_{\mathbb{F}}(t)$ such that $h^n = g$.

105 *Proof.* It is easy to see that for any $n \geq 2$ there exist polynomials $P_k(x_1, \dots, x_{k-2})$, $k \geq 3$, such that the n -th power of an element $t + \sum_{i=2}^{\infty} \alpha_i t^i \in N_{\mathbb{F}}(t)$ is equal to $t + n\alpha_2 t^2 + \sum_{k=3}^{\infty} (n\alpha_k + P_k(\alpha_2, \dots, \alpha_{k-1})) t^k$.

Let $g = t + \sum_{i=2}^{\infty} \beta_i t^i$. Define a sequence

$$\alpha_2 = \frac{1}{n} \beta_2, \dots, \alpha_k = \frac{1}{n} (\beta_k - P_k(\alpha_2, \dots, \alpha_{k-1})), \quad k \geq 3.$$

Let $h = t + \sum_{i=2}^{\infty} \alpha_i t^i$. Then $h^n = g$. It is easy to see that the element h is the unique element with this property. This completes the proof of the

110 lemma. □

For $n \geq 1$ consider

$$K_n := \{t + O(t^{n+1})\}$$

In particular, $K_1 = N_{\mathbb{F}}(t)$. Lemma 3.1 implies that K_n is a normal subgroup of $N_{\mathbb{F}}(t)$ and the mapping

$$\theta : K_n \rightarrow \mathbb{F}, \quad \theta(t + \alpha t^{n+1} + O(t^{n+2})) = \alpha$$

is a homomorphism into the additive group of the field \mathbb{F} , $\text{Ker}\theta = K_{n+1}$. Hence $K_n/K_{n+1} \simeq \mathbb{F}$.

For a group G let $\gamma_n(G)$ denote the n -th term of the lower central series:

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \dots,$$

$$\gamma_n(G) = [\gamma_{n-1}(G), G], \quad n \geq 2.$$

Lemma 3.3. ([13]) *For every $n \geq 1$, we have that $\gamma_n = \gamma_n(N_{\mathbb{F}}(t)) = K_n$.*

Recall that the Lie ring associated with the lower central series of a group G is the \mathbb{N} -graded abelian group

$$L(G) = \bigoplus_{n \geq 1} \gamma_n(G)/\gamma_{n+1}(G)$$

with multiplication

$$[a\gamma_{n+1}(G), b\gamma_{m+1}(G)] = [a, b]\gamma_{n+m+1}(G),$$

115 for $a \in \gamma_n(G)$, $b \in \gamma_m(G)$.

The isomorphisms $K_n/K_{n+1} \simeq \mathbb{F}$ define a structure of \mathbb{F} -vector space on $L(N_{\mathbb{F}}(t))$. Lemma 3.1(3) implies that multiplication on $L(N_{\mathbb{F}}(t))$ is \mathbb{F} -bilinear, hence $L(N_{\mathbb{F}}(t))$ is a Lie algebra over the field \mathbb{F} .

Again from Lemma 3.1(3) it follows that $L(N_{\mathbb{F}}(t)) \simeq \text{Vir}^{(1)}$

Definition 3.1. A group G is said to be residually nilpotent if

$$\bigcap_{n \geq 1} \gamma_n(G) = (1).$$

120 Taking the system of subgroups $\gamma_n(G)$, $n \geq 1$, for the basis of neighbourhoods of 1 we define a topology on the group G .

If this topology is complete then we say that the group G is pronilpotent.

By Lemma 3.3 the pronilpotent topology on the group $N_{\mathbb{F}}(t)$ coincides with the degree topology. Hence $N_{\mathbb{F}}(t)$ is a pronilpotent group.

125 **Lemma 3.4.** Let $g \in K_n \setminus K_{n+1}$, $g = t + \alpha t^{n+1} + O(t^{n+2})$, $0 \neq \alpha \in \mathbb{F}$. Then

1. $K_{2n+1} = [g, K_{n+1}]$.
2. For any s , $n < s < 2n$, we have $K_s = [g, K_{s-n}]K_{2n}$.

Proof. Denote $f_i(\beta) = t + \beta t^{i+1}$, $i \geq 1$, $\beta \in \mathbb{F}$.

We claim that for an arbitrary $s > n$, $s \neq 2n$,

$$K_s = [g, K_{s-n}]K_{s+1} \tag{C}$$

Indeed, choose an arbitrary element $h = t + \gamma t^{s+1} + O(t^{s+2}) \in K_s$. Let

130 $\beta = \frac{\gamma}{(2n-s)\alpha}$.

By Lemma 3.1(3)

$$[g, f_{s-n}(\beta)] = t + (2n-s)\alpha\beta t^{s+1} + O(t^{s+2}) = t + \gamma t^{s+1} + O(t^{s+2}).$$

By Lemma 3.1, $[g, f_{s-n}(\beta)]^{-1}h \in K_{s+1}$, which implies the claim.

Now choose an arbitrary element $h \in K_{2n+1}$. We will construct a sequence of elements $a_i \in K_{n+i}$, $i \geq 1$, such that

$$h \in [g, a_1 \cdots a_i] K_{2n+1+i} \quad \text{for any } i \geq 1.$$

For $i = 1$, by (C), there exists an element $a_1 = f_{n+1}(\beta) \in K_{n+1}$ such that $h \in [g, a_1] K_{2n+2}$.

Suppose that elements a_1, \dots, a_i satisfying that $h \in [g, a_1 \cdots a_i] K_{2n+1+i}$ have been found. Then $[g, a_1 \cdots a_i]^{-1} h \in K_{2n+1+i}$.

By (C) there exists an element $a_{i+1} \in K_{n+i+1}$ such that

$$[g, a_1 \cdots a_i]^{-1} h = [g, a_{i+1}] \text{ mod } K_{2n+i+2}.$$

Hence, $h = [g, a_1 \cdots a_i][g, a_{i+1}] \text{ mod } K_{2n+i+2}$.

Using Hall identity:

$$[x, zy] = [x, y][x, z][[x, z], y]$$

we get $[g, a_1 \cdots a_i][g, a_{i+1}] = [g, a_1 \cdots a_i a_{i+1}] \text{ mod } K_{2n+i+2}$.

We have completed the construction of a sequence $a_1, a_2, \dots, a_m, \dots$ with the required properties.

Let $a = \lim_{i \rightarrow \infty} a_1 \cdots a_i \in K_{n+1}$. Then $h = [g, a]$.

Let's prove the second assertion. Consider s any number satisfying $n < s < 2n$ and $h' \in K_s$. Arguing as above and using (C) we find elements $a_i \in K_i$, $1 \leq i \leq n-1$, such that

$$h' = [g, a_1 \cdots a_i] \text{ mod } K_{n+i+1}.$$

For the element $a = a_1 \cdots a_{n-1}$ we have $h' = [g, a] \text{ mod } K_{2n}$. This completes the proof of the lemma. \square

Corollary 3.5. *An arbitrary non-identical normal subgroup of $N_{\mathbb{F}}(t)$ contains a subgroup K_m for some $m \geq 1$.*

Proof. Let H be a non-identical normal subgroup of $N_{\mathbb{F}}(t)$. Let $1 \neq g \in H$, then there is an n such that $g \in K_n \setminus K_{n+1}$.

Then, by Lemma 3.4(1) $K_{2n+1} = [g, K_{n+1}] \subseteq H$. This completes the proof, taking $m = 2n + 1$. \square

Let $p(x_1, \dots, x_m)$ be a non-zero polynomial over \mathbb{F} . Suppose that

$$p = p_0(x_2, \dots, x_m) + x_1 p_1(x_2, \dots, x_m) + x_1^d p_d(x_2, \dots, x_m),$$

where $p_d(x_2, \dots, x_m) \neq 0$. Let $\mathcal{P} = \{p(\alpha_1, \dots, \alpha_m) \mid \alpha_1, \dots, \alpha_m \in \mathbb{F}\}$.

150 Lemma 3.6. $\mathbb{F} = \underbrace{\pm \mathcal{P} \pm \mathcal{P} \pm \dots \pm \mathcal{P}}_{2^d}$. That is, every element in \mathbb{F} is the sum of 2^d elements, each of them lying in \mathcal{P} or $-\mathcal{P}$.

Proof. Introduce d new variables, y_1, \dots, y_d and consider the polynomial

$$\begin{aligned} \tilde{p}(y_1, \dots, y_d, x_2, \dots, x_m) &= p(y_1 + \dots + y_d, x_2, \dots, x_m) - \\ &\sum_{i=1}^d p(y_1 + \dots + \hat{y}_i + \dots + y_d, x_2, \dots, x_m) + \sum_{1 \leq i < j \leq d} p(y_1 + \dots + \hat{y}_i + \dots + \hat{y}_j + \dots + y_d, x_2, \dots, x_m) + \\ &\dots + (-1)^{d-1} \sum_{i=1}^d p(y_i, x_2, \dots, x_m) + (-1)^d p(0, x_2, \dots, x_m) = d! y_1 \dots y_d p_d(x_2, \dots, x_m). \end{aligned}$$

Every element from the field \mathbb{F} is a value of the polynomial

$$d! y_1 \dots y_d p_d(x_2, \dots, x_m)$$

which implies the assertion of the lemma. \square

Theorem 3.7. Let \mathbb{F} be a field of characteristic zero. Then, the Nottingham group $N_{\mathbb{F}}(t)$ is verbally elliptic.

155 Proof. Let $\omega(x_1, \dots, x_m)$ be an element of the free group \mathcal{F}_m on m free generators x_1, \dots, x_m .

Let $G = N_{\mathbb{F}}(t)$. Suppose that $\omega[G] \subseteq K_n$ and n is maximal with this property.

If $\omega \notin [\mathcal{F}_m, \mathcal{F}_m]$ then $\omega(G) = G$. Indeed, if $\omega \notin [\mathcal{F}_m, \mathcal{F}_m]$ then

$$\omega = x_1^{n_1} x_2^{n_2} \dots x_m^{n_m} \omega',$$

where $\omega' \in [\mathcal{F}_m, \mathcal{F}_m]$ and some $n_i \neq 0$. Suppose that $n_1 \neq 0$. Choose $x_2 = 1, \dots,$

160 $x_m = 1$. Then $\omega(x_1, 1, \dots, 1) = x_1^{n_1}$.

Using Lemma 3.2 we can extract roots in $N_{\mathbb{F}}(t)$ so for every $f \in N_{\mathbb{F}}(t)$, $f = g^{n_1} = \omega(g, 1, \dots, 1) \in \omega[G]$.

Hence, without loss of generality, we assume that $\omega \in [\mathcal{F}_m, \mathcal{F}_m]$, hence $n \geq 2$.

Choose an element $g \in \omega[G]$, $g \in K_n \setminus K_{n+1}$.

There exists a polynomial $p(x_{ij}, 1 \leq i \leq m, 1 \leq j \leq n)$ such that

$$\omega(t + \sum_{j=1}^n \alpha_{1j} t^{j+1}, t + \sum_{j=1}^n \alpha_{2j} t^{j+1}, \dots, t + \sum_{j=1}^n \alpha_{mj} t^{j+1}) = t + p(\alpha_{ij}) t^{n+1} + O(t^{n+2}).$$

165 Let d be the maximum of (total) degrees of monomials from $p(x_{ij})$. By Lemmas 3.1(1) and 3.6, an arbitrary element u from $\omega(G)$ is a product of not more than $r = 2^d$ elements from $\omega[G]^{\pm 1}$ modulo K_{n+1} . Hence there exist elements $g_1, \dots, g_r \in \omega[G]^{\pm 1}$ such that $u = g_1 \dots g_r$ modulo K_{n+1} .

By Lemma 3.4(2) there exists an element $b \in G$ such that

$$(g_1 \dots g_r)^{-1} u = [g, b] \pmod{K_{2n}}.$$

On the other side, since the element $[g, f_1(1)]$ lies in $K_{n+1} \setminus K_{n+2}$, we can
170 use again Lemma 3.4(2) to get an element $b_1 \in K_n$ such that

$$[g, b]^{-1} (g_1 \dots g_r)^{-1} u = [[g, f_1(1)], b_1] \pmod{K_{2(n+1)}}.$$

By Lemma 3.4(1) there exists an element $b_2 \in K_{n+1}$ such that

$$[[g, f_1(1)], b_1]^{-1} [g, b]^{-1} (g_1 \dots g_r)^{-1} u = [g, b_2].$$

Now, $u = g_1 \dots g_r [g, b] [[g, f_1(1)], b_1] [g, b_2]$.

A commutator $[g, b_i]$ is a product of two elements (g^{-1} and $g^{b_i} = b_i^{-1} g b_i$) of $\omega[G]^{\pm 1}$. The commutator $[[g, f_1(1)], b_1]$ is a product of four elements from $\omega[G]^{\pm 1}$. Hence the verbal width in the group $G = N_{\mathbb{F}}(t)$ is at most $r + 8$.

175 This completes the proof of the Theorem. □

Authors are grateful to the referee who provided useful comments.

Acknowledgements

This work has been partially supported by the Government of Spain through the project *MTM2017 – 83506 – C2 – 2 – P* and by the Principado de Asturias
180 through the project *FC – GRUPIN – IDI/2018/000193*.

References

- [1] B. Klopsch, Automorphisms of the nottingham group, *Journal of Algebra* 223 (2000) 37–56.
- [2] D. Segal, Words: Notes on verbal width in groups, *London Mathematical Society Lecture Notes Series* 361 (2009).
185
- [3] C. Martinez, E. I. Zelmanov, Product of powers in finite simple groups, *Israel J. Math.* 96 (1997) 469–479.
- [4] Saxl, J. S. Wilson, A note on powers in simple groups, *Math. Proc. Camb. Phil. Soc.* 122 (1997) 91–94.
- [5] P. Stroud, Topics in the theory of verbal subgroups, PhD Thesis. University of Cambridge (1966).
190
- [6] A. H. Rhemtulla, A problem of bounded expressibility in free products, *Academic Press, New York*, 64 (1994) 573–584.
- [7] V. Romankov, Width of verbal subgroups in solvable groups, *Algebra i logika* 21 (1982) 60–72.
195
- [8] J. Serre, *Cohomologie galoisienne*, Springer Verlag (1964).
- [9] B. Hartley, Subgroups of finite index in profinite groups, *Math. Z.* 168 (1979) 71–76.
- [10] A. Jaikin-Zapirain, On the verbal width of finitely generated pro- p -groups, *Rev. Mat. Iberoam.* 24 (2008) 617–630.
200
- [11] C. Martinez, Ellipticity of words, *Journal of Algebra* 500 (2018) 242–252.
- [12] B. Klopsch, Normal subgroups in substitution groups of formal power series, *Journal of Algebra* 228 (2000) 91–106.
- [13] D. L. Johnson, The group of formal power series under substitution, *Journal of Australian Math. Soc.* 45(3) (1988) 296–302.
205