

## Free subalgebras of Lie algebras close to nilpotent

Alexey Belov and Roman Mikhailov

**Abstract.** We prove that for every automata algebra of exponential growth the associated Lie algebra contains a free subalgebra. For  $n \geq 1$ , let  $L_{n+2}$  be a Lie algebra with generators  $x_1, \dots, x_{n+2}$  and the following relations: for  $k \leq n$ , any commutator (with any arrangement of brackets) of length  $k$  which consists of fewer than  $k$  different symbols from  $\{x_1, \dots, x_{n+2}\}$  is zero. As an application of this result about automata algebras, we prove that  $L_{n+2}$  contains a free subalgebra for every  $n \geq 1$ . We also prove the similar result about groups defined by commutator relations. Let  $G_{n+2}$  be a group with  $n + 2$  generators  $y_1, \dots, y_{n+2}$  and the following relations: for  $k \leq n$ , any left-normalized commutator of length  $k$  which consists of fewer than  $k$  different symbols from  $\{y_1, \dots, y_{n+2}\}$  is trivial. Then the group  $G_{n+2}$  contains a 2-generated free subgroup.

The main technical tool is combinatorics of words, namely combinatorics of periodical sequences and period switching.

**Mathematics Subject Classification (2010).** Primary 17B01; Secondary 20E07, 20E05.

**Keywords.** Lie algebra, automata algebra, free group, nilpotency.

### 1. Introduction

Let  $A$  be an associative algebra over a commutative ring with identity, generated by a set  $S$ . Denote by  $A^\sim$  the Lie algebra with the same set of generators  $S$  and operation  $[u, v] = uv - vu$ ,  $u, v \in A$ . In other words  $A^\sim$  is the Lie subalgebra of  $A^\sim$  generated by the given set  $S$ . The algebra  $A^\sim$  clearly depends on the choice of the set of generators of  $A$ .

For  $n \geq 1$ , let  $L_{n+2}$  be a Lie algebra with generator set  $x_1, \dots, x_{n+2}$  and following relations: for  $k \leq n$ , any commutator of length  $k$  which consists of fewer than  $k$  different symbols from  $\{x_1, \dots, x_{n+2}\}$  is zero. For example, the trivial commutators in  $L_n$  which correspond to the case  $k = 3$  are:

$$[[x_i, x_j], x_i], \quad i \neq j.$$

One of the main results of this paper is following:

**Theorem 1.** *For every  $n \geq 1$ ,  $L_{n+2}$  contains a free Lie subalgebra.*

The algebras with few relations were extensively studied [3], [4], [10], [12]. E. I. Zelmanov [15] proved that a free pro- $p$  group with a set of relations satisfying the Golod–Shafarevich condition contains a free pro- $p$  group. This result is in spirit of the present work.

The proof of Theorem 1 is based on the theory of monomial algebras. An algebra with a basis  $X$  is called *monomial* if all its defining relations are of the form  $u = 0$ , where  $u$  is a word written in  $X$ . Let  $A$  be a finitely generated algebra with generators  $x_1, \dots, x_s$ . The *growth function*  $V_A(n)$  is equal to the dimension of the space generated by words of length  $\leq n$ . If  $V_A(n)$  grows exponentially, then  $A$  has *exponential growth*; if polynomially, then  $A$  has *polynomial growth*. *Intermediate growth* is also possible. The polynomial or exponential growth property does not depend on the choice of the set of generators.

For  $n \geq 1$ , let  $A_{n+2}$  be the monomial algebra with generators  $x_1, \dots, x_{n+2}$  and the following relations:  $u(x_1, \dots, x_{n+2}) = 0$  if  $|u| = k$  ( $k \leq n$ ) and  $u$  consists of fewer than  $k$  symbols from  $\{x_1, \dots, x_{n+2}\}$ . Clearly, the Lie algebra  $A_{n+2}^\sim$  is a quotient of  $L_{n+2}$ :  $A_{n+2}^\sim \simeq L_{n+2}/I$ . Hence, if we will be able to prove that  $A_{n+2}^\sim$  contains a 2-generated free subalgebra, then  $L_{n+2}$  also contains a 2-generated free subalgebra, and Theorem 1 follows. The algebra  $A_{n+2}$  has an alternative description based on the following property:  $u(x_1, \dots, x_{n+2}) = 0$  in the algebra  $A_{n+2}$  if the distance between two occurrences of the same letter in  $u(x_1, \dots, x_{n+2})$  is less than  $n + 1$ .

Consider a super-word  $w = (x_1 \dots x_{n+1})^\infty$  (the notion of *super-word* is defined in the Section 2). It is clear that  $w \neq 0$  and any series of changes  $x_{n+1} \mapsto x_{n+2}$  will not yield zero, since the distance between two occurrences of the same letter is still  $\leq n$ .

With the help of above changes it is possible to get  $2^M$  different non-zero words from the word of length  $(n + 1) \cdot M$ ,  $M \geq 1$ . It follows that the number of different non-zero words of length  $k$  in the monomial algebra  $A$  is not less than  $2^{\lfloor \frac{k}{n+1} \rfloor}$ , and the algebra  $A$  has exponential growth. The algebra  $A_{n+2}$  is finitely presented and hence is an automata algebra ([6], e.g., Proposition 5.4). Hence  $A_{n+2}^\sim$  contains a 2-generated (and countably generated) free subalgebra by Theorem 2 below.

**Theorem 2.** *Let  $A = \langle a_1, \dots, a_n \rangle$  be an automata algebra of exponential growth. Then the Lie algebra  $A^\sim$  contains a free 2-generator subalgebra.*

The proof of this Theorem is contained in Section 4.1.

**Remark.** A more complicated proof is needed to show that a Lie algebra with generators  $x_1, \dots, x_{n+1}$  and the relations: for  $k \leq n$ , any commutator of length  $k$  which consists of fewer than  $k$  different symbols from  $\{x_1, \dots, x_{n+1}\}$  is zero, also contains a free subalgebra for every  $n \geq 3$ .

A similar situation takes place in the case of groups. As a natural group-theoretical analog of Theorem 1 we have the following:

**Theorem 3.** For  $n \geq 1$ , let  $G_{n+2}$  be a group with  $n + 2$  generators  $y_1, \dots, y_{n+2}$  and the following relations: for  $k = 3, \dots, n$ , any commutator of length  $k$  which consists of fewer than  $k$  different symbols from  $\{y_1, \dots, y_{n+2}\}$  is trivial. Then the group  $G_{n+2}$  contains a 2-generated free subgroup.

Note that the groups  $G_{n+2}$  are related to the construction of amenable groups with fast Følner function from [8].

It is a pleasure for us to thank Mikhail Gromov for posing the problem and his helpful comments, and Louis Rowen for useful discussions and suggestions. We also thank the referee for constructive comments and corrections. The authors were supported by the Israel Science Foundation grant No. 1178/06, Russian Fundamental Foundation Grant 08-01-91300-IND\_a. The research of the second author was partially supported by Russian Science Support Foundation and Presidential Grant MK-3644.2009.1.

## 2. Periodicity

The order  $a_1 < a_2 < \dots < a_n$  induces a lexicographical order on the set of all words. Two words are incomparable with respect to this order if one of them is the initial of the other. By  $|v|$  will be denoted the length of a word  $v$ . By  $u \subset v$  will be denoted the occurrence of a word  $u$  in a word  $v$ . A word  $u$  is called *cyclic* if  $u = v^k$  for some  $k > 1$ ; otherwise it is called *noncyclic* or *nonperiodic*. If  $W = u^k r$ , where  $r$  is an initial segment in  $u$ , then  $W$  is called *quasi-periodic of order  $|u|$* . In this case  $W$  is a subword of  $u^\infty$  (see next section). The words  $u$  and  $v$  are called *cyclically conjugate* if  $u = cd$  and  $v = dc$  for some words  $c$  and  $d$ . The *cyclic conjugacy* relation is an equivalence relation.

A *super-word* is a word which is infinite in both directions. A word that is infinite to the left is called a *left super-word*; a word that is infinite to the right is called a *right super-word*. By  $u^\infty$  will be denoted a super-word with the period  $u$ , by  $u^{\infty/2}$  a right (left) super-word which begins (terminates) with the word  $u$ .

Since it is clear from the context which super-word is under consideration, left or right, we do not introduce special notation. The notation  $u^{\infty/2} \cdot s \cdot v^{\infty/2}$  means, for example, that  $u^{\infty/2}$  is a left super-word and  $v^{\infty/2}$  is a right one.

Right super-words (unlike finite words, for which incomparable elements exist) constitute a linearly ordered set with respect to the left lexicographic ordering; the same is true for left super-words with respect to the right lexicographic ordering.

**2.1. Periodic super-words.** By  $u$  will be denoted a non-cyclic word. We recall some propositions from [6] (Section 2.1). By  $A_{u^\infty}$  we denote an algebra whose defining relations have the following form:  $s = 0$  where  $s$  is a word which is not a subword of  $u^\infty$ .

**Proposition 1.** *Every two subwords in  $u^\infty$  of length  $N|u|$  are cyclically conjugate; they coincide only when the distance between their first letters is divisible by the period.*

**Proposition 2.** a) *The beginning subword of length  $|u| - 1$  uniquely defines the word from  $A_{u^\infty}$ . If the initial subwords of length  $|u| - 1$  in two subwords  $v$  and  $v'$  coincide ( $v$  and  $v'$  are subwords in the super-word  $u^\infty$ ), then one of them is a subword of the other one. If  $|c| \geq |u|$  and  $d_1$  and  $d_2$  are lexicographically comparable, then at least one of the words  $cd_1, cd_2$  is not a subword in  $u^\infty$ .*

b) *The positions of the occurrences of a word  $v$  of length  $\geq |u|$  in  $u^\infty$  differ by a multiple of a period.*

c) *If  $|v| \geq |u|$  and  $v^2 \subset u^\infty$ , then  $v$  is cyclically conjugate to a power of  $u$ . Therefore, non-nilpotent words in  $A_{u^\infty}$  are exactly those words that are cyclically conjugate to words of the form  $u^k$ .*

**Lemma 1** (on overlapping). *If a subword of length  $m + n - 1$  occurs simultaneously in two periodic words of periods  $m$  and  $n$ , then they are the same up to a shift.*

**2.2. Periodicity and Burnside-type problems.** The periodicity of an infinite word means its invariance with respect to a shift. In the one-sided infinite case a pre-period appears; in the finite case effects related to the truncation appear. This, in conjunction with super-word techniques, provides the essence of many combinatorial arguments (see Proposition 3), especially Burnside-type problems.

**Proposition 3** ([6], Section 2.1). *If  $uW = Wr$ , then  $uW$  is a subword of  $u^\infty$  and  $W = u^n r$ , where  $r$  is an initial segment in  $u$ .*

This proposition implies the following two lemmas.

**Lemma 2** ([6], Section 2.1). *Let  $W = u_l v_l$ ,  $|u_l| = l$ ,  $l = 0, \dots, n$ . Then either all  $v_l$  are lexicographically comparable, or  $u_l$  is quasi-periodic of order  $\leq n$  for some  $l$ .*

From Lemma 2 one can deduce the nilpotency of the subalgebra of  $n \times n$  matrix algebra such that all the words of length  $\leq n$  over generators are nilpotent. (Sketch of the proof [6] (Section 2.1.4): Consider a lexicographically minimal right super-word  $W$ . Let  $W = u_k W_k$ ,  $|u_k| = k$ ,  $k = 0, \dots, n$ ,  $W_0 = W$ . Consider an action of beginners  $u_k$  on the  $n$ -dimensional space  $V$  and note that  $\vec{e}u_0, \dots, \vec{e}u_n$  must be linearly dependent.) This fact is called the *Shestakov–Lvov hypothesis*.

The authors present a sketch of proof of the *Shirshov height theorem*, which says that *a normal basis of an associative affine PI-algebra  $A$  contains only piecewise periodic words whose number of periodic parts is less than  $h(A)$ , and the length of each period is  $\leq m$ , where  $m$  is the minimal degree of a polynomial identity*. More details can be found in [6] (Section 2.2), [1], [5].

**Lemma 3** ([6], Section 2.1). *If  $W$  has no  $n$  pairwise lexicographically comparable subwords, then  $W$  contains the  $k$ -th power of a word  $v$  of order  $\leq n$  and  $k \geq (|W| - 2n)/|v|$ .*

The proof also uses the following facts.

- Any polynomial identity implies a multilinear identity of the same degree.
- If  $V = v_1 \dots v_m$  and  $v_1 \succ \dots \succ v_s$  then for any  $\sigma \in S_m \setminus \text{Id}$ ,

$$V_\sigma = v_{\sigma(1)} \dots v_{\sigma(s)} \prec V = V_{\text{Id}}$$

and  $V$  is a linear combination of smaller words.

- If  $W = s_1 w s_2 \dots w s_{m+1}$  and  $w$  has  $m$  pairwise lexicographically comparable subwords, then  $W = W_0 v_1 \dots v_m$  and  $v_1 \succ \dots \succ v_s$  for some  $v_1, \dots, v_s$ .
- If  $W$  is long enough, then some subword  $w$  such that  $|w| \geq m^2$ , repeats  $m$  times and if  $w$  has not  $m$  pairwise incomparable subwords, we can use Lemma 3.

The general fact is the following: *a normal basis of an associative affine PI-algebra  $A$  contains only piecewise periodic words, the number of periodic parts is less than  $h(A)$ , and the length of each period is at most the maximal dimension of a matrix algebra satisfying all identities of  $A$  (Amitsur–Shestakov hypothesis).*

The proof of the theorem about the coincidence of the nilradical and the Jacobson radical in a monomial algebra is also based on the arguments of the same type applied to super-words.

In this paper we focus on the investigation of places when one period switches to another.

**2.3. Period switching.** Lemma 1 implies the following two technical statements that are needed in sequel.

**Lemma 4.** *Let  $u$  and  $v$  be two different non-cyclic words, let  $k$  and  $l$  be such that  $k|u| > |v| + |u|$ ,  $l|v| > |u| + |v|$ ,  $r = u^n v^m$ ,  $n > k$ ,  $m > l$ . Then  $r$  has no common subwords with  $u^\infty$  of length  $\geq n|u| + |u| + |v| - 1 = (n+1)|u| + |v| - 1$  and no common subwords with  $v^\infty$  of length  $\geq (m+1)|v| + |u| - 1$ .*

**Proposition 4.** *Suppose that  $u, v$  are not powers of the same word,  $l|v| > 2|u|$  and  $s|u| > 2|v|$ . Then  $v^l u^s$  is not a subword of  $u^\infty$  or  $v^\infty$ .*

Now we are going to prove an important fact on the non-cyclicity of period switching.

**Proposition 5.** *Suppose that  $u, v$  are not powers of the same word,  $l|v| \geq 2|u|$  and  $s|u| \geq 2|v|$ . Then  $v^l u^s$  is not a proper power (i.e., it is not cyclical).*

*Proof.* Without loss of generality we may suppose that both  $u$  and  $v$  are non-cyclic. Suppose that  $k > 1$  and  $z^k = v^l u^s$  for some non-cyclic word  $z$ . Without loss of generality we can assume that  $|v^l| \geq |u^s|$ . Since  $s|u| \geq 2|v|$ , we have  $l \geq 3$  or  $l = 2$  and  $|v^l| = |u^s|$ .

If  $k \geq 4$ , then  $v^l$  contains  $z^2$ , hence  $|v^l| \geq |z^2|$ . On the other hand,  $v^l$  is subword of  $z^\infty$ . If  $|v| \leq |z|$  then  $|z^2| \geq |v| + |z|$ . Due to Lemma 1,  $v$  is a power of  $z$  and hence  $v = z$  (both  $z, v$  are non-cyclic). If  $|v| > |z|$  then  $|v^l| \geq |v^2| > |v| + |z|$  and we are also done.

If  $k = 2$  then  $z$  is a subword of  $v^l$ ;  $u^s$  is a subword of  $z$  and hence  $u^s$  is a subword of  $v^l$ . We also have  $z = z_1 u^s$  for some  $z_1$ . Since  $|u^s| \geq 2|v|$ , we have  $|z^2| > |z| + |v|$  and due to Lemma 1 we have  $u^\infty = z^\infty$  and hence  $u = z$  because  $u$  is the end of  $z$  and both words are non-cyclic. We are also done in this case.

If  $k = 3$  and  $l \geq 3$  we have  $|v| \leq |z|/2$ . If  $k = 3$  and  $l = 2$  then  $|v^l| = |u^s|$ . So we also have  $|v| \leq |z|/2$ . In any case  $|v^l| \geq |v| + |z|$ . By Lemma 1 we have that  $v^\infty = z^\infty$  and hence  $v = z$  since both words are non-cyclic. In this case the proposition follows easily.  $\square$

**Remark.** It would be interesting to obtain exact conditions for Proposition 5.

**Lemma 5.** *Let  $k$  and  $l$  be such that  $k|u| > |v| + |u|$ ,  $l|v| > |u| + |v|$ ,  $r = u^n v^m$ ,  $n > k$ ,  $m > l$ . Then  $r$  is not a subword of  $W' = v^{\infty/2} u^{\infty/2}$  and hence of  $v^p u^q$  for all  $p, q$ .*

*Proof.* If  $r$  is a subword of  $W'$  then either  $u^n$  (i.e., the left part of  $r$ ) is a subword of  $v^\infty$  or  $v^m$  (i.e., the right part of  $r$ ) is a subword of  $u^\infty$ . Both cases are excluded by Proposition 4.  $\square$

**Proposition 6** (Period switching). *Consider a super-word  $W = u^{\infty/2} v^{\infty/2}$ , where  $u \neq v$  are different noncyclic words. Let  $S = u^k v^l$  and suppose that  $|u^{k-1}| > 2|v|$ ,  $|v^{k-1}| > 2|u|$ ,  $k, l \geq 2$ . Then  $S$  has just one occurrence in  $W$ , which is the obvious one (which we call the “standard occurrence”).*

*Proof.* Suppose the contrary. Then the extra occurrence of  $S$  is either to the left of the standard occurrence, or to the right. Without loss of generality it is enough to consider the former case.

Then, by Proposition 2,  $W$  is shifted with respect to the standard occurrence by a distance divisible by  $|u|$ . Hence we have:  $u^s W = WR$ , i.e.,  $u^s W$  starts with  $W$ . We can apply Proposition 3 and so we get that  $u^{\infty/2}$  starts with  $W$ . Then from combining Lemma 1 and Proposition 2 we get that  $v$  is cyclically conjugate to  $u$ , and  $|u| = |v|$ .

However in that case  $W = u^k v^l$  is a subword of  $u^\infty$ . This implies that the relative shifts of  $u$  and  $v$  are divisible by  $|u| = |v|$ , and hence  $u = v$ . The statement is proved.  $\square$

This result together with Lemmas 4 and 5 implies:

**Corollary 1.** *Let  $R = r^\infty = (u^n v^m)^\infty$ ,  $n > k$ ,  $m > l$ . All the occurrences of  $S$  in  $R$  are separated by distances divisible by  $|r| = n|u| + m|v|$ .*

*Proof.* First of all, as in Proposition 6, one can define the notion of a *standard occurrence* of  $S$  in  $R$ . Consider an occurrence  $\bar{S}$  of  $S$  in  $R$ . Then only the following cases are logically possible:

- (1)  $\bar{S}$  naturally corresponds to an occurrence of  $S$  in  $W$  (i.e., a power of  $v$  in  $\bar{S}$  starts with a power of  $v$  in  $W$  and, similarly, a power of  $u$  in  $\bar{S}$  ends with a power of  $u$  in  $W$ ).
- (2)  $\bar{S}$  contains completely either  $u^n$  or  $v^m$ .
- (3)  $\bar{S}$  lies on the position of period switching from  $v^m$  to  $u^m$ .

The second possibility is excluded by Lemma 4, and the third one by Lemma 5. By Proposition 6 the first possibility corresponds only to standard occurrences, and they are separated by distances divisible by  $|r| = |u^n v^m| = n|u| + m|v|$ .  $\square$

Note that  $r$  and  $t$  are cyclically conjugate if and only if  $r^\infty = t^\infty$ . Using this observation and the previous corollary we get a proposition needed in the sequel.

**Proposition 7.** *Let  $u, v$  be different non-cyclic words such that  $|u^n| > 2|v|$  and  $|v^n| > 2|u|$ . For all  $k_i, l_i \geq n$ , if  $(k_1, l_1) \neq (k_2, l_2)$ , then  $u^{k_1} v^{l_1}$  and  $u^{k_2} v^{l_2}$  are not cyclically conjugate. (In particular, all of them are different).*

*Proof.* Suppose that  $r = u^{k_1} v^{l_1}$  and  $t = u^{k_2} v^{l_2}$  are cyclically conjugate. Then  $r^\infty = t^\infty$  and  $|r| = |t| = \mu = k_1|u| + l_1|v| = k_2|u| + l_2|v|$  since  $r, t$  are not cyclical. Let us denote  $R = (u^{k_2} v^{l_2})^\infty$ . Put  $S = u^k v^l$  and suppose that  $|u^{k-1}| > 2|v|$ ,  $|v^{k-1}| > 2|u|$ ,  $k, l \geq 2$  and also  $k \leq \min k_1, k_2$ ,  $l \leq \min(l_1, l_2)$ . It is clear that such  $S$  exists and is a subword of both  $r$  and  $t$ .

Next, by Corollary 1, all occurrences of  $S$  in  $W$  are shifted by a distance divisible by  $\mu$ , the period of  $R$ . This means that any occurrence of  $S$  can be extended to an occurrence of  $r$  as well as to an occurrence of  $t$ . Hence there exist the occurrences of  $r = u^{n_1} S v^{m_1}$  and  $t = u^{n_2} S v^{m_2}$  in  $W$  with common part  $S$ , intersection  $\delta = u^{\min(n_1, n_2)} S v^{\min(m_1, m_2)}$  and union  $\omega = u^{\max(n_1, n_2)} S v^{\max(m_1, m_2)}$ .

If  $r \neq t$ , then  $n_1 \neq n_2$  since  $|s| = |t|$ . Without loss of generality we can assume that  $n_1 < n_2$ . In this case  $m_1 > m_2$  and the word  $t$  is shifted to the left from the word  $r$  by the distance  $d = |u^{n_1}| - |u^{n_2}| = |v^{n_2}| - |v^{m_1}|$ .

Consider a union  $\omega$  of  $r$  and  $t$ . Then  $\omega = er = ft$ ,  $|e| = |f| = d$ . Observe that  $r^2$  is a subword of  $t^\infty = W$  and that an occurrence of  $v^{m_1}$  (which is the end of  $r$ ) precedes an occurrence of  $r$ . Since  $|v^{m_2}| > d$  one has  $e = v^{m_2 - m_1}$ . Similarly,  $f = u^{n_1 - n_2}$ .

On the other hand  $\omega$  can be also obtained by extending the subword  $S$  of  $W$  to the left by the distance  $|v^{\max(m_1, m_2)}|$  and to the right by the distance  $|u^{\max(n_1, n_2)}|$ , and  $\omega = u^{\max(n_1, n_2)} v^{\max(m_1, m_2)} = u^{n_1 - n_2} r = t v^{m_2 - m_1}$ .

Hence  $u^{n_1-n_2} = v^{m_2-m_1}$ ,  $n_1 \neq n_2$ ,  $m_1 \neq m_2$ . It follows that  $u, v$  are powers of the same word  $s$ . Therefore  $u \neq v$ , one of these powers is greater than 1 and both  $u$  and  $v$  cannot be non-cyclic words. But this contradicts their initial choice.  $\square$

### 3. Regular words and Lie brackets

We shall extend the partial order  $<$  by defining the following  $\triangleright$ -relation (“Ufnarovsky order”):  $f \triangleright g$  if for any two right super-words  $W_1, W_2$ , such that  $W_2(a, b) \succ W_1(a, b)$  whenever  $b \succ a$ , the inequality  $W_2(g, f) \succ W_1(g, f)$  holds. This condition is well defined and equivalent to the following:  $f \triangleright g$  iff  $f^{\infty/2} \succ g^{\infty/2}$  (i.e.,  $f^m \succ g^n$  for some  $m$  and  $n$ ). It is clear that if  $f \succ g$ , then  $f \triangleright g$ .

The relation  $\triangleright$  is a linear ordering on the following set of equivalence classes:  $f \sim g$  if  $f = s^l, g = s^k$  for some  $s$ .

Observe that every finite word  $u$  yields the right super-word  $u^\infty$ . Two equivalent words correspond to the same super-words. The relation  $\triangleright$  corresponds to the relation  $\succ$  on the set of super-words.

A word  $u$  is called *regular* if one of the following equivalent conditions (see [6] (Section 2.3), [14]) are satisfied:

- a)  $u$  is greater than all its cyclic conjugates: if  $u_1u_2 = u$ , then  $u \succ u_2u_1$ .
- b) If  $u_1u_2 = u$ , then  $u \triangleright u_2$ .
- c) If  $u_1u_2 = u$ , then  $u_1 \triangleright u$ .

A word  $u$  is called *semi-regular* in the following case: If  $u = u_1u_2$ , then either  $u \succ u_2$  or  $u_2$  is a beginning of  $u$ . (An equivalent definition can be obtained if the relation  $\triangleleft$  is replaced by the relation  $\trianglelefteq$  in the definition of a regular word ([6], Section 2.3). Every semi-regular word is a power of a regular one.

**Remark.** Let  $U(a, b) \trianglelefteq V(a, b), u \trianglelefteq v$  be some words in the alphabet  $a < b$ . Then  $U(u, v) \trianglelefteq V(u, v)$  and  $U(v, u) \trianglerighteq V(v, u)$  ([14], p. 106). Let  $u_1 \trianglelefteq u_2$  be regular words, then the word  $u_1u_2$  is also regular; see [14], p. 106.

Let  $u$  be a regular word. Then  $u = u_1u_2$  for some regular word  $u_2 \neq u$  of maximum length. This fact, together with the previous remark, implies the following statement.

**Proposition 8.** *Let  $u \triangleright v$  be regular words. Let  $a \succ b$  and let  $w$  be a regular word. Then  $w(u, v)$  is also a regular word.*

It is well known that every regular word  $u$  defines the unique bracket arrangement  $[u]$  such that after lifting of all Lie brackets  $u$  will be the highest term in this expression and  $[u] = [[u_1], [u_2]]$ . Moreover, the monomials of such type form a basis in the free Lie algebra (so-called *Lyndon–Shirshov basis*) (see [2], [14]).



An arbitrary word  $W$  can be uniquely presented in the form  $W = W_1 \dots W_s$ , where the words  $W_i$  are regular and  $W_1 \trianglelefteq \dots \trianglelefteq W_s$ . This fact corresponds to the Poincaré–Birkhof–Witt theorem.

The fact that any sufficiently large word written in a finite alphabet has a subword of form  $uvu$  with regular  $u, v$  implies that a Lie algebra generated by sandwiches is locally nilpotent. (A non-zero element  $u \in L$  is called a *sandwich* in the Lie algebra  $L$  if  $\text{ad}(u)\text{ad}(v)\text{ad}(u) = 0$  for any  $v \in L$ .)

The positive solution of the restricted Burnside problem in the case of Lie algebras has the following two stages: first to show the existence of a sandwich and then to prove the local nilpotency of the sandwich algebra [14], [6] (Section 2.3.3). This is the result of A. I. Kostrikin and E. I. Zelmanov [9]. Another proof via super-words pointed out here was obtained by J. Backelintje and independently by A. D. Chanyshv [7]. The positive solution of the so-called weak Burnside problem (existence of a universal  $k$ -generated finite group with identity  $x^n = e$  for every  $n$  and  $k$ ) was obtained by E. I. Zelmanov, based on the solution of the restricted Burnside problem for Lie algebras and the classification of finite simple groups.

We shall need some technical statements in sequel.

**Lemma 6** ([6], Section 2.1). *Suppose that  $|u^k| \geq |v^2|$  and  $u^k$  is a subword of  $v^\infty$ . Then there exists a word  $S'$  which is cyclically conjugate to  $S$  such that  $u = (S')^m$  and  $v = (S^2)^n$ . If, moreover, the initial symbols of  $u$  and  $v$  are at a distance divisible by  $|S|$  in  $v^\infty$ , then  $S = S'$ .*

**Corollary 2.** *Let  $u \triangleright v$  be semi-regular words. Then, for sufficiently large  $k$  and  $l$ , the words  $u^k v^l$  are regular and*

$$u^{k_1} v^{l_1} \triangleright u^{k_2} v^{l_2}$$

for  $k_1 > k_2$ .

*Proof.* Let  $\delta$  be a cyclic conjugate of  $u^k v^l$ . It is clear that  $\delta \triangleright u^k v^l$ . We only need to prove that  $\delta \neq u^k v^l$ . In order to do this, we need only to show that  $u^k v^l$  is not a cyclic word, but this follows from Proposition 5.  $\square$

The next lemma follows from Lemma 6 and Corollary 2.

**Lemma 7.** *Let  $k_i > |d|$ ,  $l_i > |u|$  for  $i = 1, 2$ . Then  $u^{k_1} d^{l_1}$  and  $u^{k_2} d^{l_2}$  are not cyclically conjugate, provided that  $u \triangleright d$  and  $u, d$  are not conjugate to proper powers of the same word.*

#### 4. Regular words in automata algebras

Let  $\Phi\langle x_1, \dots, x_s \rangle$  denote a free associative  $\Phi$ -algebra with generators  $x_1, \dots, x_s$ . Let  $A\langle a_1, \dots, a_s \rangle$  be an arbitrary  $\Phi$ -algebra with a fixed set of generators  $a_1, \dots, a_s$ .

A *word* or a *monomial* in the set of generators  $\mathcal{M}$  is an arbitrary product of elements in  $\mathcal{M}$ . The set of all words constitutes a semigroup, which will be denoted by  $\text{Wd}(\mathcal{M})$ . The order  $a_1 < \dots < a_s$  generates the lexicographic order on the set of words: the greater of two words is the one whose first letter is greater; if the first symbols coincide, then the second letters are compared, next the third letters and so on. Two words are incomparable if one of them is an initial of the other.

By a *word* in an algebra we understand a non-zero word in its generators  $\{a_i\}$ . We cannot speak about the *value* of a super-word in an algebra, but we can speak about its *equality* or *nonequality to zero* (and, in some cases, about *linear dependence*). A super-word  $W$  is called a *zero super-word* if it has a finite zero subword, and it is called a *non-zero super-word* if it has no finite zero subwords.

An algebra  $A$  is called *monomial* if it has defining relations of type  $c = 0$ , where  $c$  is a word in  $a_1, \dots, a_s$ . Obviously, a monomial algebra is a semigroup algebra (it coincides with the semigroup algebra over the semigroup of its words).

**4.1. Automata algebras.** The notion of *automata algebra* was introduced by Ufnarovsky [13]. First we recall some well-known definitions from [6], Chapter 5. Suppose we have an alphabet (i.e., a finite set)  $X$ . By a *finite automaton* (FA) with the alphabet  $X$  of input symbols we shall understand an oriented graph  $G$  whose edges are marked by the letters from  $X$ . One of the vertices of this graph is marked as initial, and some vertices are marked as final. A word  $w$  in the alphabet  $X$  is called *accepted* by a finite automaton if there exists a path in the graph, which begins at the initial vertex and finishes in some final vertex such that marks on the path edges in the order of passage constitute the word  $w$ .

By a *language* in the alphabet  $X$  we understand some subset in the set of all words in  $X$ . A language  $L$  is called *regular* or *automata* if there exists a finite automaton that accepts all words from  $L$  and only them.

An automaton is called *deterministic* if all edges which start from one vertex are marked by different letters. If we reject such restriction, then we shall come to the notion of a *non-deterministic* finite automaton. Also we can allow an automaton to have several initial vertices. The following result from the theory of finite automata is well known ([6] (chapter 5), [14]): *For each non-deterministic FA there exists a deterministic FA, which accepts the same set of words (i.e., the same language).*

**Remark.** The standard definition of a *deterministic finite automaton* [11] requires that for each pair of state and input symbol there is one and only one transition to a next state. Our notion is designed for combinatorial ring theory and slightly differs from the standard one.

It will be convenient for us to consider the class of FA such that all vertices are initial and final simultaneously. The reason is that the language of non-zero words in a monomial algebra has the following property: every subword of a word belonging to the language belongs to it as well.

**Remark.** Note that the pair of two different words in a deterministic FA generating a monomial algebra  $A$  corresponding to two circles with common initial vertex generates a free associative subalgebra of  $A$ .

Suppose throughout that  $G$  is the graph of a deterministic FA,  $v$  is a vertex of  $G$ , and  $w$  is a word. If the corresponding path  $C$  starting from  $v$  exists in  $G$ , then one can define the vertex  $vw$  which will be a terminal vertex for  $C$ .

Let  $A$  be a monomial algebra (not necessary finitely defined).  $A$  is called an *automata algebra* if the set of all of its non-zero words in generators of  $A$  is a regular language. It is more convenient to use equivalent definition: a monomial algebra is an *automata algebra* if the set of its non-zero words is the set of all subwords of words of some regular language.

It is known that every automata algebra can be given by a certain deterministic graph, and that every finitely defined monomial algebra is automata ([6], Proposition 5.4, [14]).

The Hilbert series for an automata algebra is rational ([6], Proposition 5.9). An automata algebra has exponential growth if and only if  $G$  has two cycles  $C_1$  and  $C_2$  with common vertex  $v$  such that the corresponding words  $w_1, w_2$  (we read them starting from  $v$ ) are not powers of the same word. In this case the words  $w_1$  and  $w_2$  generate a free 2-generated associative algebra [13]. If there are no such cycles,  $A$  has a polynomial growth. No intermediate growth is possible.

We recall the Theorem 2 which is the aim of this section:

**Theorem 2.** *Let  $A = \langle a_1, \dots, a_n \rangle$  be an automata algebra of exponential growth. Then the Lie algebra  $A^\sim$  contains a free 2-generator subalgebra.*

**Definition 1.** We continue to assume that  $G$  is the graph of a deterministic FA. Call a semiregular word  $u$  *well-based* if it is written on a certain cycle  $C$  with an initial vertex  $v$ , i.e.,  $vu = v$ . Two semi-regular words  $u_1$  and  $u_2$  are *pairwise well-based* if  $u_1$  and  $u_2$  are written on cycles  $C_1$  and  $C_2$  with a common initial vertex  $v$  and  $vC_1 = vC_2 = v$ . In this case, for any word  $W(a, b)$  the word  $W(u_1, u_2) \neq 0$  in  $A$ ; in particular  $u_1^{k_1}u_2^{k_2} \neq 0$ .

**Main Lemma.** *The graph  $G$  contains two regular pairwise well-based words  $u \neq v$ .*

*Deduction of Theorem 2 from the Main Lemma.* We may always assume that the regular pairwise well-based words  $u$  and  $v$  satisfy the condition  $u \triangleright v$ . Let  $a \succ b$  and let  $w$  be a regular word. Then, by the Proposition 8,  $w(u, v)$  also is a regular word.

For every regular word  $u$  we can choose a unique presentation  $u = u_1u_2$  with regular  $u_1$  and regular  $u_2$  of maximal length. In this case  $[u] = [[u_1], [u_2]]$  (see [14]). Therefore, by iterating this process,  $w(u, v)$  can be obtained by setting  $[u] \mapsto a$ ,  $[v] \mapsto b$  to the word with brackets  $[w]$ .

Since  $u$  and  $v$  are well-based, for every word  $R(a, b)$ , one has  $R(u, v) \neq 0$ . Let  $[u]$ ,  $[v]$  be the results of the regular arrangement of the brackets for  $u$  and  $v$ , respectively. Then  $[u] \neq 0$ ,  $[v] \neq 0$ .

Thus we have constructed a one-to-one correspondence between the Lyndon–Shirshov basis of a Lie algebra generated by  $[u]$ ,  $[v]$  and the Lyndon–Shirshov basis of a free 2-generated Lie algebra with generators  $a, b$ . The theorem follows.  $\square$

**4.2. Proof of the Main Lemma.** Corollary 2 implies the following:

**Proposition 9.** *Suppose that the graph  $G$  contains two ordered (in the sense of the operation  $\triangleright$ ) semi-regular pairwise well-based words. Then  $G$  contains also two regular pairwise well-based words.*

It is sufficient to find two ordered semi-regular pairwise well-based words, i.e., with common final and initial vertices. For that it is enough to prove the existence of a sufficiently large number of well-based ordered semi-regular words. In this case, infinitely many of them will have a common initial vertex, hence pairwise well-based, and the main Lemma follows.

**Lemma 8.** *Let  $u_1$  be a well-based word and let  $u_2$  be a cyclically conjugate word. Then  $u_2$  is also well-based.*

*Proof.* Suppose that  $u_1 = w_1w_2$ ,  $u_2 = w_2w_1$  and  $v$  is a base vertex of  $u_1$ . Then  $v' = vw_1$  is a base vertex of  $u_2$ . Indeed,  $v'u_2 = vw_1(w_2w_1) = v(w_1w_2)w_1 = vw_1 = v'$ .  $\square$

**Corollary 3.** *If  $u$  is well-based, then semi-regular word conjugate to  $u$  is also well-based.*

Now we shall finish the proof of the Main Lemma. Let  $u$  and  $d$  be ordered pairwise well-based words (necessarily not semi-regular). Then, for every  $w(a, b)$ , the word  $w(u, d)$  is non-zero. In particular,  $u^k d^l$  are non-zero for all  $k, l$ . It is non-cyclic if  $u$  and  $v$  are not powers of the same word due to Proposition 5 and  $u^k d^l \neq u^{k'} d^{l'}$  for  $(k, l) \neq (k', l')$  due to Proposition 7, provided that  $k$  and  $l$  are sufficiently large.

Now Lemma 7, together with the fact that every non-cyclic word uniquely corresponds to a cyclically conjugated regular word, implies that there are infinitely many well-based words. Infinitely many of them will have the same initial vertex and so will be pairwise well-based; hence the Main Lemma follows.

## 5. Group-theoretical applications

This section is devoted to the proof of the Theorem 3. Let  $\text{id}(S)$  denote the ideal generated by the set  $S$ .

**Lemma 9.** *Suppose that  $a$  and  $b$  are homogeneous elements of a graded associative algebra  $A$  such that the subalgebra generated by  $a, b$  is a free associative algebra with free generators  $a, b$ . Let  $a'$  (resp.  $b'$ ) be a linear combination of elements in  $A$  with degrees strictly greater than the degree of  $a$  (resp.  $b$ ). Let  $\tilde{a} = a + a', \tilde{b} = b + b'$ . Then the algebra generated by  $\tilde{a}, \tilde{b}$  is a free associative with generators  $\tilde{a}, \tilde{b}$ .*

The Lemma follows from the fact that for every polynomial  $h(u, v)$  with non-zero minimal component  $h'(u, v)$ , the minimal component of  $h(\tilde{a}, \tilde{b})$  is  $h'(a, b) \neq 0$ .

We call an algebra *homogeneous* if all its defining relations are homogeneous with respect to the set of generators. Let  $A$  be a homogeneous algebra, and  $J$  be an ideal of  $A$  generated by elements of degree  $\geq 1$ . We call such algebra *good* if  $A/J \cong k$  and  $\bigcap_n J^n = 0$ . Every monomial algebra is good. For any  $x \in A$ , the image of  $x$  in  $A/J^n$  is not zero for some  $n$ , so  $A$  can be embedded into the projective limit  $\varprojlim A/J^n$ .

**Lemma 10.** *Let  $B$  be a good homogeneous algebra with unit such that  $1 + a$  and  $1 + b$  are invertible,  $a, b \in J$ , and the elements  $a$  and  $b$  are free generators of a free associative subalgebra  $C$  of  $B$ . Then the group generated by  $1 + a$  and  $1 + b$  is free.*

**Remark.** Note that the pair of two different pairwise well-based words in a monomial algebra generates a free associative subalgebra (see Remark on p. 25).

*Proof.* Consider subalgebra  $C$  of algebra  $B$  generated by  $a, b$  and isomorphism  $\phi: C \rightarrow k\langle x, y \rangle$  such that  $\phi(a) = x, \phi(b) = y$ .

Suppose that  $W(1 + a, 1 + b) = 1$  for some non-trivial word  $W(x, y) \neq 1$  in a free group. Consider free algebra  $k\langle x, y \rangle$  and its localization by  $1 + x, 1 + y$ . Then  $W(1 + x, 1 + y) \neq 1$ , and, for some  $n_0 = n_0(W)$ ,  $W(1 + \bar{x}, 1 + \bar{y}) \neq 1$  in  $\pi_n(k\langle x, y \rangle) = k\langle x, y \rangle / \text{id}(x, y)^n$  for all  $n \geq n_0$ . In each such image, the elements  $1 + x$  and  $1 + y$  are invertible, so there is no need for localization.

On the other hand, since  $B$  is good homogeneous, the image of  $J^m \cap C$  under isomorphism  $\phi$  lies in  $\text{id}(x, y)^{n_0}$ , and

$$1 = \pi_{n_0}(\phi(W(1 + a, 1 + b))) = W(1 + \bar{x}, 1 + \bar{y}) \neq 1.$$

We get a contradiction. □

Let  $u$  and  $v$  be two pairwise well based regular words. They have canonical Lie bracket arrangement. Let  $[u]$  and  $[v]$  be corresponding Lie elements (obtained via lifting of Lie brackets). Notice that

$$\begin{aligned} [u] &= u + \text{lexicographically smaller terms,} \\ [v] &= v + \text{lexicographically smaller terms.} \end{aligned}$$

We have following result.

**Corollary 4.** *Let  $u$  and  $v$  be two pairwise well based regular words, and let  $[u]$  and  $[v]$  be the corresponding Lie elements (obtained via opening Lie brackets). Then  $[u]$ ,  $[v]$  generate as free generators a 2-generated free associative algebra (and also a free Lie algebra via commutator operation).*

For  $n \geq 1$ , consider the monomial algebra  $A_{n+2}$  with generators  $x_1, \dots, x_{n+2}$  (see Introduction). We adjoin the unit  $A'_{n+2} = A_{n+2} \cup \{1\}$ . Recall that  $x_i^2 = 0$ , so the elements  $\bar{x}_i := 1 + x_i$  have inverses  $\bar{x}_i^{-1} := 1 - x_i$ . Consider the group  $A_{n+2}^\#$  generated by elements  $1 + x_i$ . Consider generators of a free subalgebra in the Lie algebra  $\tilde{A}_{n+2}$  which correspond to regular words and configuration of brackets on these words.

Consider the commutator of group elements

$$\begin{aligned} [\bar{x}_i, \bar{x}_j] &= \bar{x}_i \bar{x}_j \bar{x}_i^{-1} \bar{x}_j^{-1} \\ &= (1 + x_i)(1 + x_j)(1 + x_i)^{-1}(1 + x_j)^{-1} \\ &= 1 + [x_i, x_j] + \text{higher terms.} \end{aligned}$$

Similarly, the longer commutators in group elements are expressed via the Lie commutators

$$[\bar{x}_{i_1}, \dots, \bar{x}_{i_m}] = 1 + [x_{i_1}, \dots, x_{i_m}] + \text{higher terms.}$$

Let  $u, v$  be the two regular words as above. By the process above we construct the corresponding group elements from  $A^\#$ :  $\bar{u} = 1 + [u] + \text{higher terms}$ ,  $\bar{v} = 1 + [v] + \text{higher terms}$ . Then, by Lemmas 9, 10 and Corollary 4,  $\bar{v}$  and  $\bar{u}$  generate a free subgroup in  $A^\#$ .

Consider a commutator of length  $k$  in the generators of  $A^\#$ ,

$$[\bar{x}_{i_1}, \dots, \bar{x}_{i_k}] = 1 + [x_{i_1}, \dots, x_{i_k}] + \text{higher terms,}$$

such that among  $\bar{x}_{i_1}, \dots, \bar{x}_{i_k}$  less than  $k$  are different. Then all monomials on the right-hand side are of length at least  $k$  and contain less than  $k$  letters, thus they are trivial in our monomial algebra and  $[\bar{x}_{i_1}, \dots, \bar{x}_{i_k}] = 1$ . This means that all commutators of length  $k$  in  $A_{n+2}^\#$  which consist of fewer than  $k$  different symbols from  $\{\bar{x}_1, \dots, \bar{x}_{n+2}\}$  are trivial.

The group with the relations as in Theorem 3 can only be mapped onto our group, hence it contains a free subgroup as well, and Theorem 3 follows.

## References

- [1] S. A. Amitsur and L. W. Small, Affine algebras with polynomial identities. *Rend. Circ. Mat. Palermo (2) Suppl.* (1993), 9–43. [Zbl 0807.16001](#) [MR 1244613](#)
- [2] Yu. A. Bahturin, *Identical relations in Lie algebras*. VNU Science Press, Utrecht 1987. [Zbl 0571.17001](#) [MR 0886063](#)

- [3] Y. Bahturin and A. Olshanskii, Large restricted Lie algebras. *J. Algebra* **310** (2007), 413–427. [Zbl 05144400](#) [MR 2307801](#)
- [4] B. Baumslag and S. J. Pride, Groups with one more generator than relators. *Math. Z.* **167** (1979), 279–281. [Zbl 0388.20025](#) [MR 539110](#)
- [5] A. J. Belov, About height theorem. *Comm. Algebra* **23** (1995), 3551–3553. [Zbl 0841.16026](#) [MR 1335316](#)
- [6] A. Y. Belov, V. V. Borisenko, and V. N. Latyshev, Monomial algebras. *J. Math. Sci.* **87** (1997), 3463–3575. [Zbl 0927.16018](#) [MR 1604202](#)
- [7] A. D. Chanyshv, Regular words and the sandwich-algebra theorem. *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* **1990** (1990), no. 5, 84–85; English transl. *Moscow Univ. Math. Bull.* **45** (1990), no. 5, 68–69; [Zbl 0718.17005](#) [MR 1085234](#)
- [8] M. Gromov, Entropy and isoperimetry for linear and non-linear group actions. *Groups Geom. Dyn.* **2** (2008), 499–593. [Zbl 05368764](#) [MR 2442946](#)
- [9] A. I. Kostrikin, Around Burnside. *Ergeb. Math. Grenzgeb.* (3) **20**, Springer-Verlag, Berlin 1990. [Zbl 0702.17001](#) [MR 1075416](#)
- [10] J. P. Labute, Free ideals of one-relator graded Lie algebras. *Trans. Amer. Math. Soc.* **347** (1995), 175–188. [Zbl 0824.17007](#) [MR 1282891](#)
- [11] A. Salomaa, *Jewels of formal language theory*. Computer Science Press, Rockville, Md., 1981. [Zbl 0487.68064](#) [MR 0618124](#)
- [12] R. Stöhr, Groups with one more generator than relators. *Math. Z.* **182** (1983), 45–47. [Zbl 0509.20021](#) [MR 686885](#)
- [13] V. A. Ufnarovskii, On the use of graphs for calculating the basis, growth and Hilbert series of associative algebras. *Mat. Sb.* **180** (1989), 1548–1560; English transl. *Math.-USSR Sb.* **68** (1990), 417–428. [Zbl 0685.16007](#) [MR 1034428](#)
- [14] V. A. Ufnarovskij, Combinatorial and asymptotic methods in algebra. In *Algebra VI*, Encyclopaedia Math. Sci. 57, Springer, Berlin 1995, 1–196. [Zbl 0826.16001](#) [MR 1060321](#)
- [15] E. Zelmanov, On groups satisfying the Golod-Shafarevich condition. In *New horizons in pro-p groups*, Progr. Math. 184, Birkhäuser Boston, Boston, MA, 2000, 223–232. [Zbl 0974.20022](#) [MR 1765122](#)

Received May 19, 2008; revised November 5, 2008

A. Belov, Department of Mathematics, Bar Ilan University, Ramat Gan 52900, Israel

E-mail: [kanel@mccme.ru](mailto:kanel@mccme.ru)

R. Mikhailov, Steklov Mathematical Institute, Gubkina 8, Moscow 119991, Russia

E-mail: [romanvm@mi.ras.ru](mailto:romanvm@mi.ras.ru)