Journal of Symbolic Computation 44 (2009) 786–800

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

Non-associative Gröbner bases, finitely-presented Lie rings and the Engel condition, II

Serena Cicalò [1], Willem A. de Graaf

Dipartimento di Matematica, Università di Trento, Italy

ARTICLE INFO

Article history:
Received 22 November 2007
Accepted 15 April 2008
Available online 26 September 2008

Keywords:
Non-associative Gröbner bases
Finitely-presented Lie rings
The n-Engel condition

ABSTRACT

We give an algorithm for constructing a basis and a multiplication table of a finite-dimensional finitely-presented Lie ring. Secondly, we give relations that are equivalent to the n-Engel condition, and only have to be checked for the elements of a basis of a Lie ring. We apply this to construct the freest t-generator Lie rings that satisfy the n-Engel condition, for $(t, n) = (2, 3), (3, 3), (4, 3), (2, 4)$.

1. Introduction

A Lie ring L is a $\mathbb{Z}$-module equipped with a multiplication, $[\ ,\ ] : L \times L \to L$, $(x, y) \mapsto [x, y]$, that is anticommutative and satisfies the Jacobi identity. Lie rings appear naturally in several areas of group theory. Examples are the theory of nilpotent groups (Huppert and Blackburn, 1982), the classification of p-groups (Newman et al., 2004; O'Brien and Vaughan-Lee, 2005), and the restricted Burnside problem (see for example Kostrikin (1990) and Vaughan-Lee (1998)). Also Vaughan-Lee (2003) contains an account of some striking Lie ring techniques in group theory. On many occasions these Lie rings are given by a presentation by means of generators and relations (for a precise definition of this concept we refer to Section 3). Therefore it would be of great interest to have an algorithm for constructing a basis and multiplication table for a Lie ring given in this way. It is the objective of this paper to describe such an algorithm.

We say that a Lie ring is finite-dimensional if it is finitely generated as an Abelian group. Of course it is only possible to construct a basis and multiplication table for Lie rings that are finite-dimensional. Our algorithm will terminate whenever the input defines a finite-dimensional Lie ring. Otherwise it will run forever.

E-mail addresses: cicalo@science.unitn.it (S. Cicalò), degraaf@science.unitn.it (W.A. de Graaf).
URL: http://www.science.unitn.it/~degraaf (W.A. de Graaf).
[1] Tel.: +39 0461 882069; fax: +39 0461 881624.

0747-7171/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2008.04.007

Recently Gröbner bases in general non-associative algebras have been studied (see e.g., Gerritzen (2006), de Graaf and Wisliceny (1999) and Rajaee (2006)). In this paper we use these to deal with finitely-presented Lie rings. However, because we are working over $\mathbb{Z}$ rather than over a field, some modifications are necessary. In Section 2 we describe a reduction algorithm analogous to the one presented in Adams and Loustaunau (1994), Chapter 4. In Section 3 we describe how to apply this to finitely-presented Lie rings.

There are a few algorithms known for constructing finitely-presented Lie algebras (e.g., de Graaf and Wisliceny (1999), Havas et al. (1990), Leeuwen and Roelofs (1997) and Gerdt and Kornyak (1996)). These bear some similarity to the algorithms described here. The main difference lies in the fact that we work over $\mathbb{Z}$ and not over a field, which causes a lot of additional problems. In Schneider (1997) an algorithm is described to compute so-called nilpotent quotients of finitely-presented Lie rings. However, the approach via Gröbner bases leads to a more general algorithm, that will work whenever the finitely-presented Lie ring is finite-dimensional.

In the second half of the paper we study Lie rings that satisfy the n-Engel identity, i.e., Lie rings L such that

$$[x, [x, \dots, [x, y] \dots]] = 0$$

for all $x, y \in L$ (n factors x). The study of these Lie rings goes back at least to Higgins (1954). It follows from a result of Zel'manov (see for example Vaughan-Lee (1998)) that a finitely-generated Lie ring that satisfies an n-Engel identity is nilpotent. By $E(t, n)$ we denote the "freest" t-generator Lie ring that satisfies the n-Engel identity. Now a natural question is what the structure of $E(t, n)$ is. For example, in Higgins (1954) and Traustason (1993, 1995) for various t, n upper bounds for the nilpotency class of $E(t, n)$ are given (with the difference that in these references the $E(t, n)$ are defined over fields). One problem when dealing with the n-Engel condition is that it is not a multilinear relation. In Section 4 we describe several sets of relations with the following property: a Lie ring satisfies the n-Engel condition if and only if its basis elements satisfy the relations of the given set. In combination with the algorithms in the first half of the paper, this yields an algorithm to construct a basis and a multiplication table for $E(t, n)$. Using an implementation of the algorithms in the computer algebra systems GAP4 (GAP, 2004), and MAGMA (Bosma et al., 1997) we have constructed $E(2, 3)$, $E(3, 3)$, $E(4, 3)$ and $E(2, 4)$. At the end of the paper we list the terms of the lower central series of these Lie rings.

The GAP4 implementations of the algorithms will be released as a GAP package in the near future. The MAGMA implementations are part of the current release of the system (V2.14).

This paper is a sequel to Cicalò and de Graaf (2007) which appeared in the proceedings of ISSAC'07. We have tried to keep the intersection of both papers as small as possible. In particular, the description of the algorithm for constructing a finitely-presented Lie ring now makes use of general Gröbner bases in $A_{\mathbb{Z}}(X)$, which in our opinion makes its description much more elegant. Also we have investigated the n-Engel condition in far greater depth. In Section 4 we take a theorem from Cicalò and de Graaf (2007) that gives a set of relations equivalent to the n-Engel condition, as the starting point and obtain several sets of equivalent relations. The objective of this is to eliminate redundancy as much as possible. Finally, in the last section we have added one more 3-Engel Lie ring ($E(4, 3)$). We were able to construct it with the MAGMA implementation of the algorithms, which was not available to us at the time of writing Cicalò and de Graaf (2007).

2. Gröbner bases in free algebras

Throughout X will be a finite set of symbols, also called letters. The free magma $M(X)$ on X is defined as follows. Firstly, $X \subset M(X)$, and secondly if $m, n \in M(X)$ then $(m, n) \in M(X)$. So $M(X)$ is the set of all bracketed words in the letters in X. The free magma is equipped with a binary operation: $m \cdot n = (m, n)$. The degree of elements of $M(X)$ is defined in the obvious way: $\deg(x) = 1$ for $x \in X$ and $\deg((m, n)) = \deg(m) + \deg(n)$.

We use a total order $<$ on $M(X)$ that is defined as follows. Firstly, the elements of X are ordered arbitrarily. Secondly, $\deg(m) < \deg(n)$ implies that $m < n$. Finally, if $m = (m', m'')$, $n = (n', n'')$ and $\deg(m) = \deg(n)$ then $m < n$ if and only if $m' < n'$ or $m' = n'$ and $m'' < n''$. We note that this ordering is multiplicative, i.e., $m < n$ implies $(p, m) < (p, n)$ and $(m, p) < (n, p)$ for all $p \in M(X)$. Furthermore, every subset of $M(X)$ has a minimal element.

The free algebra on X over $\mathbb{Z}$ is the $\mathbb{Z}$-span of $M(X)$. We denote it by $A_{\mathbb{Z}}(X)$. The binary operation of $M(X)$ is bilinearly extended to $A_{\mathbb{Z}}(X)$. The elements of $M(X)$ that occur in an $f \in A_{\mathbb{Z}}(X)$ are called the monomials of f. The leading monomial of f, denoted by $\mathrm{LM}(f)$, is the biggest monomial of f. Its coefficient in f is denoted by $\mathrm{LC}(f)$. We say that f is monic if $\mathrm{LC}(f) = 1$. The degree of f will be the degree of $\mathrm{LM}(f)$.

Now let $\sigma = (m_1, \dots, m_k)$ be a sequence of elements of $M(X)$ and $\delta = (d_1, \dots, d_k)$ a sequence of letters $d_i \in \{\mathrm{l}, \mathrm{r}\}$ (for "left" and "right"). Then we call the pair $\alpha = (\sigma, \delta)$ a *product prescription*. Corresponding to α there is a map $P_\alpha : M(X) \to M(X)$ defined inductively. If $k = 0$ then $P_\alpha(m) = m$ for all m. If $k > 0$ then set $\beta = ((m_2, \dots, m_k), (d_2, \dots, d_k))$, and $P_\alpha(m) = P_\beta((m_1, m))$ if $d_1 = \mathrm{l}$, and if $d_1 = \mathrm{r}$ then $P_\alpha(m) = P_\beta((m, m_1))$. We extend P_α linearly to $A_{\mathbb{Z}}(X)$.

An $m \in M(X)$ is said to be a factor of $n \in M(X)$ if there is a product prescription α such that $P_\alpha(m) = n$. Let $G \subset A_{\mathbb{Z}}(X)$ be a finite set, and $f \in A_{\mathbb{Z}}(X)$. Let $g_1, \dots, g_s \in G$ be all elements of G such that $\mathrm{LM}(g_i)$ is a factor of $\mathrm{LM}(f)$. Suppose that $\mathrm{LC}(f)$ is divisible by $d = \gcd(c_1, \dots, c_s)$, where $c_i = \mathrm{LC}(g_i)$. Let e_i be such that $e_1c_1 + \cdots + e_sc_s = d$. Let α_i be a product prescription such that $P_{\alpha_i}(\mathrm{LM}(g_i)) = \mathrm{LM}(f)$. Then we say that f reduces in one step modulo G to $f' = f - c(e_1P_{\alpha_1}(g_1) + \cdots + e_sP_{\alpha_s}(g_s))$, where c is such that $\mathrm{LC}(f) = cd$. More generally we say that f reduces to f' modulo G if there are $f = f_1, \dots, f_k = f'$ such that f_i reduces in one step modulo G to f_{i+1}. From the properties of $<$ it follows that any sequence of reduction steps modulo G terminates with an element that cannot be reduced further.

Here all ideals of $A_{\mathbb{Z}}(X)$ that we consider will be two sided.

Let $J \subset A_{\mathbb{Z}}(X)$ be an ideal. We call a $G \subset J$ a *Gröbner basis* of J if every $f \in J$ reduces to zero modulo G.

A set $G \subset A_{\mathbb{Z}}(X)$ is said to be self-reduced if no reductions between elements of G are possible. It is known that a self-reduced set whose elements are monic automatically is a Gröbner basis (cf. de Graaf (2000), Proposition 7.3.8).

3. Finitely generated Lie rings

Let L be a Lie ring over $\mathbb{Z}$ given by a finite set of generators that satisfy a set R of relations. We assume that L is finite-dimensional, and we want to find a basis and multiplication table of L.

Let X be a set of symbols, in bijection with the generators of L. Then we consider the ideal J of $A_{\mathbb{Z}}(X)$ generated by:

(1) (m, m) and $(m, n) + (n, m)$ for $m, n \in M(X)$,
(2) $\mathrm{Jac}(m, n, p) = (m, (n, p)) + (p, (m, n)) + (n, (p, m))$ for $m, n, p \in M(X)$,
(3) the elements of R.

Then $L \cong A_{\mathbb{Z}}(X)/J$. If R is finite then L is said to be finitely-presented. However, we will also consider infinite sets of relations R.

The main idea for constructing a basis and multiplication table of L, is to construct a Gröbner basis of J. However, in general it is not clear how to do this. Here we show that, if L is finite-dimensional, then we can compute a Gröbner basis of J.

For a set $G \subset A_{\mathbb{Z}}(X)$ we let G^{mon} be the set of all monic $g \in G$. An m in $M(X)$ is called a *normal monomial* modulo G if there is no $g \in G^{\mathrm{mon}}$ such that $\mathrm{LM}(g)$ is a factor of m. Let $f \in A_{\mathbb{Z}}(X)$; then we can compute $f' \in A_{\mathbb{Z}}(X)$ such that f reduces to f' modulo G^{mon}, and such that no $\mathrm{LM}(g)$ for $g \in G^{\mathrm{mon}}$ is a factor of any monomial occurring in f'. We call f' the normal form of f modulo G^{mon} and write $f' = f \bmod G^{\mathrm{mon}}$.

We also need to compute a basis of a space spanned by $b_1, \dots, b_t \in A_{\mathbb{Z}}(X)$. We do this as follows. First, let $m_1, \dots, m_r$ be the totality of monomials that occur in the b_i, with $m_1 > m_2 > \cdots > m_r$. Then we let an element b_i correspond to a vector of length r; the kth coefficient being the coefficient of m_k in b_i. We let the vectors that we get be the rows of a matrix, and compute its Hermite normal form (cf. Sims (1994)). Then we transform the rows of this matrix back to elements of $A_{\mathbb{Z}}(X)$ and obtain a basis of the space spanned by the b_i. We call a basis computed in this way a *normal basis*.

The main idea of the algorithm is to compute sets $G_d \subset J$ (for $d \geq 1$) that will grow into a Gröbner basis of J. The set G_d takes care of the generators of J of degrees $\leq d$. The non-monic elements require special care: we put them into a set $B_d \subset G_d$; and we require that this set be closed under multiplication by monomials, as explained below. This will then imply that at the end the span of B_d is an ideal. More precisely, for $d \geq 1$ we compute sets $G_d, B_d \subset J$, with the following properties:

P1 the generators of J of degree $\leq d$ reduce to 0 modulo G_d,
P2 G_d^{mon} is self-reduced, i.e., no reductions are possible between the elements of G_d^{mon},
P3 B_d is a normal basis of a subspace of the space spanned by the normal monomials of degree $\leq d$ modulo G_d,
P4 all non-monic elements of G_d are contained in the span of B_d,
P5 the elements of B_d reduce to zero modulo G_d,
P6 if $b \in B_d$ and $m \in M(X)$ is a normal monomial modulo G_d with $\deg(b) + \deg(m) \leq d$, then $m \cdot b \bmod G_d^{\text{mon}}$ and $b \cdot m \bmod G_d^{\text{mon}}$ are contained in the span of B_d.

Remark 1. The pair (G_d, B_d) is similar to the reduction pairs considered in Cicalò and de Graaf (2007). But it is not quite the same, as here $B_d \subset G_d$.

Now let M_d be the set of normal monomials modulo G_d of degree d. Let $I_d \subset A_{\mathbb{Z}}(X)$ be the ideal generated by G_d. Then $J = \cup_{d\geq 1} I_d$. So since $A_{\mathbb{Z}}(X)/J$ is finite-dimensional, there is a d_0 with $M_{d_0+1} = \emptyset$. Now let s_0 be such that $s_0 \geq 2d_0 + 1$ and all elements of R reduce to zero modulo I_{s_0}. Set $G = G_{s_0}$.

Let $\widetilde{J}$ be the ideal of $A_{\mathbb{Z}}(X)$ generated by G^{mon}. Since G^{mon} is self-reduced, it is a Gröbner basis of $\widetilde{J}$ ((de Graaf, 2000), Proposition 7.3.8). Set $A = A_{\mathbb{Z}}(X)/\widetilde{J}$. Then A is a finite-dimensional $\mathbb{Z}$-algebra. Let $U \subset A$ be the image of the span of B_{s_0}. Then U is an ideal of A by P6.

Lemma 2. *We have $I_{s_0} = J$ and G is a Gröbner basis of J.*

Proof. Since $G = G_{s_0} \subset J$, also $I_{s_0} \subset J$. For the reverse inclusion we first show that all $\text{Jac}(m, n, p)$ for $m, n, p \in M(X)$ are contained in I_{s_0}. By a well-known fact (cf. de Graaf (2000), Lemma 7.4.3), it is enough to show this when $m = x \in X$. Now $\text{Jac}(x, n, p)$ reduces modulo G^{mon} to a linear combination of elements of the form $\text{Jac}(x, n', p')$, where $\deg(n'), \deg(p') \leq d_0$. But they are all contained in I_{s_0}. In the same way we see that (m, m) and $(m, n) + (n, m)$ lie in I_{s_0}. By the choice of s_0 we also get $R \subset I_{s_0}$. So $I_{s_0} = J$.

We claim that for $d \geq 1$ every element in the span of B_d reduces to zero modulo G_d. Let $b_1, \dots, b_r \in B_d$ and $f = \mu_1 b_1 + \cdots + \mu_r b_r$, where $\mu_i \in \mathbb{Z}$, and $\text{LM}(b_i) > \text{LM}(b_{i+1})$ for $1 \leq i \leq r-1$. Since b_1 reduces to zero modulo G, we have that b_1 reduces in one step to $b_1' = b_1 - \lambda_1 P_{\beta_1}(h_1) - \cdots - \lambda_s P_{\beta_s}(h_s)$, where $h_i \in G$. Since b_1 is in normal form modulo G_d^{mon} the h_i's are non-monic. So the h_i's lie in the span of B_d, and by P6, $P_{\beta_i}(h_i) \bmod G_d^{\text{mon}}$ as well. In particular, $b_1' \bmod G_d^{\text{mon}}$ lies in the span of B_d. But f reduces to $f' = \mu_1 b_1' + \mu_2 b_2 + \cdots + \mu_r b_r \bmod G_d^{\text{mon}}$, which again lies in the space spanned by B_d. Therefore we can reduce again, and eventually reach zero.

Now for $1 \leq i \leq s$ let $g_i \in G$, $c_i \in \mathbb{Z}$, and let α_i be a product prescription. Then since G^{mon} is a Gröbner basis we get that $c_1 P_{\alpha_1}(g_1) + \cdots + c_s P_{\alpha_s}(g_s) \bmod G^{\text{mon}}$ is equal to

$$c_1 P_{\alpha_1}(g_1 \bmod G^{\text{mon}}) + \cdots + c_s P_{\alpha_s}(g_s \bmod G^{\text{mon}}) \bmod G^{\text{mon}}.$$

If $g_i \in G^{\text{mon}}$ then $g_i \bmod G^{\text{mon}} = 0$. On the other hand, if $g_i \notin G^{\text{mon}}$ then g_i lies in the span of B_{s_0}, and hence $g_i \bmod G^{\text{mon}} = g_i$. We conclude that $c_1 P_{\alpha_1}(g_1) + \cdots + c_s P_{\alpha_s}(g_s) \bmod G^{\text{mon}} \in U$. In other words, $c_1 P_{\alpha_1}(g_1) + \cdots + c_s P_{\alpha_s}(g_s) \bmod G^{\text{mon}}$ lies in the span of B_{s_0}. So by the claim above it reduces to zero modulo G. So every element of I_{s_0} reduces to zero modulo G; therefore G is a Gröbner basis of $I_{s_0} = J$. $\square$

Lemma 3. *We have $L \cong A/U$.*

Proof. We define a surjective homomorphism $\varphi : A_{\mathbb{Z}}(X) \to A/U$ by $\varphi(f) = (f \bmod \widetilde{J}) \bmod U$. Then $\varphi(f) = 0$ if and only if $f \bmod \widetilde{J} \in U$. But this happens if and only if $f \bmod G^{\text{mon}}$ lies in the span of B_{s_0}. The latter immediately implies that $f \in J$. On the other hand, if $f \in J$, then f reduces to zero modulo G by Lemma 2. In particular we can write $f = c_1 P_{\alpha_1}(g_1) + \cdots + c_s P_{\alpha_s}(g_s)$, where $g_i \in G$, $c_i \in \mathbb{Z}$ and the α_i are product prescriptions. But in the proof of Lemma 2 we have seen that this means that $f \bmod G^{\text{mon}}$ lies in the span of B_{s_0}. We conclude that $\ker(\varphi) = J$, and hence $A_{\mathbb{Z}}(X)/J \cong A/U$. $\square$

Now the main algorithm works as follows. For $d = 1, 2, \ldots$ we compute the sets G_d, B_d with the properties P1–P6. We also compute the normal monomials modulo G_d of degree $\leq d$. At some point we find d_0 such that $M_{d_0+1} = \emptyset$. Then we let $s_0 \geq 2d_0 + 1$ be such that I_{s_0} contains all elements of R and compute $G = G_{s_0}$ and $B = B_{s_0}$. The set of normal monomials modulo G forms a basis of the algebra $A = A_{\mathbb{Z}}(X)/\widetilde{J}$. Also, using reductions modulo G^{mon} we can compute products in the algebra A. Now using the technique of Smith normal form (cf. Sims (1994)) we can compute a surjective $\mathbb{Z}$-linear map

$$\sigma : A \to \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_t\mathbb{Z}$$

with kernel U (which is the image of the span of B in A). Every direct summand on the right-hand side leads to a basis element v_i of the algebra L. Furthermore, the product $[v_i, v_j]$ is computed by $[v_i, v_j] = \sigma(\sigma^{-1}(v_i) \cdot \sigma^{-1}(v_j))$.

Remark 4. If R is finite then it is straightforward to choose s_0 ($s_0 \geq 2d_0 + 1$ and such that s_0 is at least the maximal degree of the elements of R). If R is infinite, then some care may be needed. For example, we can have R containing all monomials of degree $\geq c + 1$ (where c is some given constant). This amounts to computing a nilpotent quotient of class c. Then it is enough to choose $s_0 \geq 2c + 1$.

4. The *n*-Engel condition

Throughout we let L be a Lie ring generated as an Abelian group by $\mathfrak{B} = \{x_1, \ldots, x_m\}$. We will use the right normed convention for iterated commutators. For example, $[xxxxy]$ will be the element $[x[x[x[xy]]]]$ of L.

Definition 5. The Lie ring L satisfies the *n-Engel condition*, or L is n-Engel, if

$$[\underbrace{x \ldots x}_{n} y] = 0$$

for all $x, y \in L$. With $E(t, n)$ we denote the freest Lie ring with t generators which satisfies the n-Engel condition.

The n-Engel condition $[x \ldots xy] = 0$ is only linear in y. Hence in order to establish whether L is n-Engel it is not sufficient to check this condition for $x \in \mathfrak{B}$ only. In this section we describe several sets of conditions on the elements of $\mathfrak{B}$; only that are necessary and sufficient for L to be n-Engel.

Let $1 \leq j_1, \ldots, j_s \leq m$. Let $k_i \geq 1$ be such that $k_1 + \cdots + k_s = n$. Let $(i_1, \ldots, i_n)$ be the n-tuple with $i_1 = \cdots = i_{k_1} = j_1$, $i_{k_1+1} = \cdots = i_{k_1+k_2} = j_2$, and so on. Then we consider the sum of all elements $[x_{\sigma_1} \cdots x_{\sigma_n} y]$ where $(x_{\sigma_1}, \ldots, x_{\sigma_n})$ is a permutation of $(x_{i_1}, \ldots, x_{i_n})$. We denote this sum by $[(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y]$. A more formal description goes as follows. Let S_n (the symmetric group on n points) act on the n-tuples by $(i_1, \ldots, i_n)\tau = (i_{\tau(1)}, \ldots, i_{\tau(n)})$. Let $H \subset S_n$ be the stabiliser of $(i_1, \ldots, i_n)$, and let $X \subset S_n$ be a set of right coset representatives of H in S_n. Then

$$[(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y] = \sum_{\tau \in X} [x_{i_{\tau(1)}} \ldots x_{i_{\tau(n)}} y].$$

For a proof of the following theorem we refer to Cicalò and de Graaf (2007).

Theorem 6. *The Lie ring L satisfies the n-Engel condition if and only if for all $y \in L$, $1 \leq s \leq n$, $1 \leq j_1 \leq \cdots \leq j_s \leq m$, and choices of signs $p_{j_r} = \pm 1$ $(1 \leq r \leq s)$ the following relations are satisfied*

$$\sum_{\substack{k_1, \ldots, k_s \geq 1 \\ k_1 + \cdots + k_s = n}} p_{j_1}^{k_1} \cdots p_{j_s}^{k_s} [(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y] = 0. \qquad (1)$$

Example 7. For $n = 4$ we get the following relations

$$
\begin{aligned}
&[(x_{j_1}^{(4)})^* y] = 0\\
&[(x_{j_1}^{(3)} x_{j_2}^{(1)})^* y] + [(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(3)})^* y] = 0\\
&[(x_{j_1}^{(3)} x_{j_2}^{(1)})^* y] - [(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(3)})^* y] = 0\\
&[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] - [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] - [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] - [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] - [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&[(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(1)} x_{j_4}^{(1)})^* y] = 0,
\end{aligned}
$$

for $j_1 \leq j_2 \leq j_3 \leq j_4$. In fact, we get more relations; but they are all ± 1 times the ones shown here.

We now derive an equivalent set of conditions that do not involve a choice of signs. For this we need to introduce some notation.

Since the summation in (1) is uniquely determined by s and n we put

$$\sum_n [(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y] := \sum_{\substack{k_1,\ldots,k_s \geq 1\\ k_1+\cdots+k_s=n}} [(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y].$$

In what follows, we will often distinguish between cases where certain k_i are odd respectively even. For example $\sum_n [(x_{j_1}^{(2h_1)} x_{j_2}^{(k_2)} x_{j_3}^{(2h_3-1)} x_{j_4}^{(2h_4)})^* y]$ is the sum

$$\sum_{\substack{h_1,k_2,h_3,h_4 \geq 1\\ 2h_1+k_2+(2h_3-1)+2h_4=n}} [(x_{j_1}^{(2h_1)} x_{j_2}^{(k_2)} x_{j_3}^{(2h_3-1)} x_{j_4}^{(2h_4)})^* y].$$

Remark 8.

$$\sum_n [(x_{j_1}^{(k_1)} \ldots x_{j_s}^{(k_s)})^* y] = \sum_n [(x_{\sigma_1}^{(k_1)} \ldots x_{\sigma_s}^{(k_s)})^* y]$$

for all permutations $(\sigma_1, \ldots, \sigma_s)$ of $(j_1, \ldots, j_s)$.

Let $(\sigma_1, \ldots, \sigma_s)$ be a permutation of $(j_1, \ldots, j_s)$. Then

$$\sum_{\substack{\mathcal{A} \subseteq \{\sigma_1,\ldots,\sigma_r\}\\ |\mathcal{A}|=q}}^{\square} \sum_n [(x_{\sigma_1}^{(k_1)} \ldots x_{\sigma_s}^{(k_s)})^* y]$$

will denote the sum of all $\sum_n [(x_{\sigma_1}^{(k_1)} \ldots x_{\sigma_s}^{(k_s)})^* y]$ such that $k_i = 2h_i$ whenever $\sigma_i \in \mathcal{A}$, where $\mathcal{A}$ runs over the subsets of $\{\sigma_1, \ldots, \sigma_r\}$ of size q.

Example 9. We have

$$
\begin{aligned}
\sum_{\substack{\mathcal{A} \subseteq \{\sigma_1,\sigma_2,\sigma_3\}\\ |\mathcal{A}|=2}}^{\square} \sum_n [(x_{\sigma_1}^{(k_1)} x_{\sigma_2}^{(k_2)} x_{\sigma_3}^{(k_3)} x_{\sigma_4}^{(k_4)})^* y] &= \sum_n [(x_{\sigma_1}^{(2h_1)} x_{\sigma_2}^{(2h_2)} x_{\sigma_3}^{(k_3)} x_{\sigma_4}^{(k_4)})^* y]\\
&\quad + \sum_n [(x_{\sigma_1}^{(2h_1)} x_{\sigma_2}^{(k_2)} x_{\sigma_3}^{(2h_3)} x_{\sigma_4}^{(k_4)})^* y]\\
&\quad + \sum_n [(x_{\sigma_1}^{(k_1)} x_{\sigma_2}^{(2h_2)} x_{\sigma_3}^{(2h_3)} x_{\sigma_4}^{(k_4)})^* y].
\end{aligned}
$$

Similarly

$$\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_r\}\\|\mathcal{A}|=q}}^{\boxtimes}\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y]$$

will denote the sum of all $\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y]$ such that $k_i=2h_i$ whenever $\sigma_i\in\mathcal{A}$ and $k_i=2h_i-1$ whenever $\sigma_i\in\{\sigma_1,\ldots,\sigma_r\}\setminus\mathcal{A}$.

Lemma 10. *For all r with* $1\le r\le s$ *we have*

$$\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_r\}\\|\mathcal{A}|=2l+1\\1\le 2l+1\le r}}^{\boxtimes}\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y]=\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_r\}\\|\mathcal{A}|=q\\1\le q\le r}}^{\square}(-2)^{q-1}\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y].$$

Proof. First we show that

$$\sum_n[(x_{\sigma_1}^{(2h_1-1)}\ldots x_{\sigma_p}^{(2h_p-1)}x_{\sigma_{p+1}}^{(k_{p+1})}\ldots x_{\sigma_s}^{(k_s)})^*y]=\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_p\}\\|\mathcal{A}|=q\\0\le q\le p}}^{\square}(-1)^q\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y].\qquad(2)$$

For this we use induction on p. The case $p=0$ is trivial. Now we suppose it is true for $p-1$. We have

$$\begin{aligned}&\sum_n[(x_{\sigma_1}^{(2h_1-1)}\ldots x_{\sigma_p}^{(2h_p-1)}x_{\sigma_{p+1}}^{(k_{p+1})}\ldots x_{\sigma_s}^{(k_s)})^*y]\\&\quad=\sum_n[(x_{\sigma_1}^{(k_1)}x_{\sigma_2}^{(2h_2-1)}\ldots x_{\sigma_p}^{(2h_p-1)}x_{\sigma_{p+1}}^{(k_{p+1})}\ldots x_{\sigma_s}^{(k_s)})^*y]\\&\qquad-\sum_n[(x_{\sigma_1}^{(2h_1)}x_{\sigma_2}^{(2h_2-1)}\ldots x_{\sigma_p}^{(2h_p-1)}x_{\sigma_{p+1}}^{(k_{p+1})}\ldots x_{\sigma_s}^{(k_s)})^*y].\end{aligned}$$

Hence by the induction hypothesis

$$\begin{aligned}&\sum_n[(x_{\sigma_1}^{(2h_1-1)}\ldots x_{\sigma_p}^{(2h_p-1)}x_{\sigma_{p+1}}^{(k_{p+1})}\ldots x_{\sigma_s}^{(k_s)})^*y]\\&\quad=\sum_{\substack{\mathcal{A}\subseteq\{\sigma_2,\ldots,\sigma_p\}\\|\mathcal{A}|=q\\0\le q\le p-1}}^{\square}(-1)^q\sum_n[(x_{\sigma_1}^{(k_1)}x_{\sigma_2}^{(k_2)}\ldots x_{\sigma_s}^{(k_s)})^*y]-\sum_{\substack{\mathcal{A}\subseteq\{\sigma_2,\ldots,\sigma_p\}\\|\mathcal{A}|=q\\0\le q\le p-1}}^{\square}(-1)^q\sum_n[(x_{\sigma_1}^{(2h_1)}x_{\sigma_2}^{(k_2)}\ldots x_{\sigma_s}^{(k_s)})^*y]\\&\quad=\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_p\}\\|\mathcal{A}|=q\\0\le q\le p}}^{\square}(-1)^q\sum_n[(x_{\sigma_1}^{(k_1)}x_{\sigma_2}^{(k_2)}\ldots x_{\sigma_s}^{(k_s)})^*y].\end{aligned}$$

We note that if some of the k_i for $i\ge p+1$ on the left-hand side are required to be even (odd) (so equal to $2h_i$ or $2h_i-1$) then they are likewise on the right-hand side.

Let $t\in\{0,\ldots,r\}$ be fixed. Then we claim that

$$\sum_{\substack{\mathcal{B}\subseteq\{\sigma_1,\ldots,\sigma_r\}\\|\mathcal{B}|=t}}^{\boxtimes}\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y]=\sum_{\substack{\mathcal{A}\subseteq\{\sigma_1,\ldots,\sigma_r\}\\|\mathcal{A}|=v\\t\le v\le r}}^{\square}(-1)^{v-t}\binom{v}{t}\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^*y].$$

In order to show this, let $\mathcal{B}\subseteq\{\sigma_1,\ldots,\sigma_r\}$ with $|\mathcal{B}|=t$ be given. Let $(\tau_1,\ldots,\tau_s)$ be a permutation of $(\sigma_1,\ldots,\sigma_s)$ such that $\mathcal{B}=\{\tau_{p+1},\ldots,\tau_r\}$ (so $p=r-t$) and $\tau_i=\sigma_i$ for $i>r$. Then the term corresponding to $\mathcal{B}$ on the left-hand side is

$$\sum_n[(x_{\tau_1}^{(2h_1-1)}\cdots x_{\tau_p}^{(2h_p-1)}x_{\tau_{p+1}}^{(2h_{p+1})}\cdots x_{\tau_r}^{(2h_r)}x_{\tau_{r+1}}^{(k_{r+1})}\cdots x_{\tau_s}^{(k_s)})^*y].$$

But by (2) this is equal to

$$\sum^{\square}_{\substack{\mathcal{C}\subseteq\{\tau_1,\dots,\tau_p\}\\ |\mathcal{C}|=q\\ 0\le q\le p}} (-1)^q \sum_n [(x_{\tau_1}^{(k_1)}\cdots x_{\tau_p}^{(k_p)} x_{\tau_{p+1}}^{(2h_{p+1})}\cdots x_{\tau_r}^{(2h_r)} x_{\tau_{r+1}}^{(k_{r+1})}\cdots x_{\tau_s}^{(k_s)})^* y]. \tag{3}$$

So we get terms where some of the exponents are required to be even. More precisely, the exponents of x_τ for $\tau \in \mathcal{C}\cup\{\tau_{p+1},\dots,\tau_r\} = \mathcal{C}\cup\mathcal{B}$ are even, where $\mathcal{C}$ runs through the subsets of $\{\tau_1,\dots,\tau_p\}$.

Now let $\mathcal{A}\subseteq\{\tau_1,\dots,\tau_r\}$ with $|\mathcal{A}| = v \ge t$. Then (3) contains a (unique) term with $\mathcal{C}\cup\mathcal{B} = \mathcal{A}$ if and only if $|\mathcal{B}\cap\mathcal{A}| = t$. The coefficient of this term is $(-1)^{|\mathcal{C}|} = (-1)^{v-t}$. Since there are $\binom{v}{t}$ such $\mathcal{B}$'s, the claim follows.

So we get

$$\begin{aligned}
&\sum^{\boxtimes}_{\substack{\mathcal{A}\subseteq\{\sigma_1,\dots,\sigma_r\}\\ |\mathcal{A}|=2l+1\\ 1\le 2l+1\le r}} \sum_n [(x_{\sigma_1}^{(k_1)}\dots x_{\sigma_s}^{(k_s)})^* y]\\
&\quad = \sum_{1\le 2l+1\le r} \sum^{\square}_{\substack{\mathcal{A}\subseteq\{\sigma_1,\dots,\sigma_r\}\\ |\mathcal{A}|=q\\ 2l+1\le q\le r}} (-1)^{q-1}\binom{q}{2l+1} \sum_n [(x_{\sigma_1}^{(k_1)}\dots x_{\sigma_s}^{(k_s)})^* y],
\end{aligned}$$

which is equal to

$$\sum^{\square}_{\substack{\mathcal{A}\subseteq\{\sigma_1,\dots,\sigma_r\}\\ |\mathcal{A}|=q\\ 1\le q\le r}} (-1)^{q-1} \sum_{1\le 2l+1\le r} \binom{q}{2l+1} \sum_n [(x_{\sigma_1}^{(k_1)}\dots x_{\sigma_s}^{(k_s)})^* y]$$

because for all $1 \le q < 2l+1$ we have that $\binom{q}{2l+1} = 0$. Now

$$\sum_{1\le 2l+1\le r} \binom{q}{2l+1} = \sum_{1\le 2l+1\le r} \left[\binom{q-1}{2l+1} + \binom{q-1}{2l}\right] = \sum_{l=0}^{q-1} \binom{q-1}{l} = 2^{q-1},$$

which concludes the proof. $\square$

Remark 11. We claim that

$$\sum_n p_{j_1}^{k_1}\dots p_{j_s}^{k_s}[(x_{j_1}^{(k_1)}\dots x_{j_s}^{(k_s)})^* y] = 0 \text{ for all } p_{j_r} = \pm 1, \text{ where } 1\le r\le s \tag{4}$$

if and only if

$$\sum_n p_{j_2}^{k_2}\dots p_{j_s}^{k_s}[(x_{j_1}^{(k_1)}\dots x_{j_s}^{(k_s)})^* y] = 0 \text{ for all } p_{j_r} = \pm 1, \text{ where } 2\le r\le s. \tag{5}$$

It is obvious that (4) implies (5). Also (5) implies (4) if $p_{j_1} = 1$. So suppose that $p_{j_1} = -1$. Let $k_1,\dots,k_s \ge 1$ with $k_1+\dots+k_s = n$. Then $(-1)^n(-p_{j_2})^{k_2}\cdots(-p_{j_s})^{k_s} = (-1)^{k_1} p_{j_2}^{k_2}\cdots p_{j_s}^{k_s}$. Hence (5) implies that

$$\begin{aligned}
0 &= (-1)^n \sum_n (-p_{j_2})^{k_2}\cdots(-p_{j_s})^{k_s}[(x_{j_1}^{(k_1)}\dots x_{j_s}^{(k_s)})^* y]\\
&= \sum_n (-1)^{k_1} p_{j_2}^{k_2}\cdots p_{j_s}^{k_s}[(x_{j_1}^{(k_1)}\dots x_{j_s}^{(k_s)})^* y].
\end{aligned}$$

Proposition 12. *Relations* (1) *are equivalent to*

$$\sum_n [(x_{j_1}^{(k_1)}\dots x_{j_s}^{(k_s)})^* y] = 0 \tag{6}$$

$$\sum_{\mathcal{A}=\{\sigma_2,\ldots,\sigma_r\}}^{\square} 2^{r-1}\sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y] = 0 \tag{7}$$

for all r, $2 \le r \le s$ *and for all permutations* $(\sigma_1,\ldots,\sigma_s)$ *of* $(j_1,\ldots,j_s)$ *such that* $\sigma_1 = j_1$.

Proof. By Remark 11 we can put $p_{j_1} = +1$ in (1); moreover we can divide these relations by $p_{j_2}\cdots p_{j_s}$. Then (1) is equivalent to

$$\sum_n p_{j_2}^{k_2-1}\cdots p_{j_s}^{k_s-1}[(x_{j_1}^{(k_1)}\cdots x_{j_s}^{(k_s)})^* y] = 0, \tag{8}$$

for all choices of signs $p_{j_r} = \pm 1$, $2 \le r \le s$.

Let $(\sigma_1,\ldots,\sigma_s)$ be a permutation of $(j_1,\ldots,j_s)$ where $\sigma_1 = j_1$ is fixed. We suppose that $p_{\sigma_2} = \cdots = p_{\sigma_r} = -1$ and $p_{\sigma_{r+1}} = \cdots = p_{\sigma_s} = +1$. Then the left-hand side of (8) becomes

$$\sum_n (-1)^{k_2-1}\cdots(-1)^{k_r-1}[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y]. \tag{9}$$

In this expression if a summand has an even number of odd $k_i - 1$, then it has a positive coefficient, otherwise it has a negative coefficient. Hence if we subtract (9) from $\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y]$, the summands of the first type vanish while those of second type are doubled. So $\sum_n[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y]$ minus (9) is

$$2\sum_{\substack{\mathcal{A}\subseteq\{\sigma_2,\ldots,\sigma_r\}\\ |\mathcal{A}|=2l+1\\ 1\le 2l+1\le r-1}}^{\boxtimes} \sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y]. \tag{10}$$

By Lemma 10 this is equal to

$$2\sum_{\substack{\mathcal{A}\subseteq\{\sigma_2,\ldots,\sigma_r\}\\ |\mathcal{A}|=q\\ 1\le q\le r-1}}^{\square} (-2)^{q-1}\sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y], \tag{11}$$

which is equal to

$$\sum_{\substack{1\le q\le r-1\\ 2\le t_1<\cdots<t_q\le r}} (-1)^{q-1} \sum_{\mathcal{A}=\{\sigma_{t_1},\ldots,\sigma_{t_q}\}}^{\square} 2^q \sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y].$$

Summarizing, we have showed that

$$\sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y] - \sum_n (-1)^{k_2-1}\cdots(-1)^{k_r-1}[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y]$$
$$= \sum_{\substack{1\le q\le r-1\\ 2\le t_1<\cdots<t_q\le r}} (-1)^{q-1} \sum_{\mathcal{A}=\{\sigma_{t_1},\ldots,\sigma_{t_q}\}}^{\square} 2^q \sum_n [(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y].$$

From this we immediately get that, if (6) and (7) are true then

$$\sum_n (-1)^{k_2-1}\cdots(-1)^{k_r-1}[(x_{\sigma_1}^{(k_1)}\ldots x_{\sigma_s}^{(k_s)})^* y] = 0$$

implying (1).

Vice versa, if (1) is true, we get (6) by putting $p_{j_l} = 1$ for all l. In order to show (7) we use induction on r.

If $r = 2$ the left-hand side of (7) becomes

$$\sum_{\mathcal{A}=\{\sigma_2\}}^{\square} 2 \sum_{n} [(x_{\sigma_1}^{(k_1)} \dots x_{\sigma_s}^{(k_s)})^* y]$$

and this is zero because as we have seen (1) implies that (11) is zero. For the induction step we note that (1) implies

$$\begin{aligned} 0 &= \sum_{\substack{1\le q\le r-1 \\ 2\le t_1<\cdots<t_q\le r}} (-1)^{q-1} \sum_{\mathcal{A}=\{\sigma_{t_1},\dots,\sigma_{t_q}\}}^{\square} 2^q \sum_{n} [(x_{\sigma_1}^{(k_1)} \dots x_{\sigma_s}^{(k_s)})^* y] \\ &= \sum_{\substack{1\le q\le r-2 \\ 2\le t_1<\cdots<t_q\le r}} (-1)^{q-1} \sum_{\mathcal{A}=\{\sigma_{t_1},\dots,\sigma_{t_q}\}}^{\square} 2^q \sum_{n} [(x_{\sigma_1}^{(k_1)} \dots x_{\sigma_s}^{(k_s)})^* y] \\ &\quad + (-1)^{r-2} \sum_{\mathcal{A}=\{\sigma_2,\dots,\sigma_r\}}^{\square} 2^{r-1} \sum_{n} [(x_{\sigma_1}^{(k_1)} \dots x_{\sigma_s}^{(k_s)})^* y]. \end{aligned}$$

Now, by the induction hypothesis the first sum on the right-hand side is zero. So we get (7). $\square$

Example 13. For $n = 4$ the relations of Proposition 12 become

$$\begin{aligned} &[(x_{j_1}^{(4)})^* y] = 0 \\ &[(x_{j_1}^{(3)} x_{j_2}^{(1)})^* y] + [(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(3)})^* y] = 0 \\ &2[(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] = 0 \\ &[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0 \\ &2[(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] = 0 \\ &2[(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0 \\ &[(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(1)} x_{j_4}^{(1)})^* y] = 0, \end{aligned}$$

for $1 \le j_1 \le j_2 \le j_3 \le j_4$.

Now we show that we can dispense with relations (7). For that we first need a technical lemma.

Lemma 14.

$$\sum_{m=2}^{n} (-1)^m \sum_{\substack{k_1,\dots,k_m\ge 1 \\ k_1+\cdots+k_m=n}} \frac{n!}{k_1!\cdots k_m!} = \begin{cases} 2, & \textit{if } n \textit{ is even;} \\ 0, & \textit{if } n \textit{ is odd.} \end{cases}$$

Proof. By induction the following can be shown:

$$\sum_{\substack{k_1,\dots,k_m\ge 1 \\ k_1+\cdots+k_m=n}} \frac{n!}{k_1!\cdots k_m!} = \sum_{r=0}^{m-1} (-1)^r \binom{m}{r} (m-r)^n, \tag{12}$$

$$\sum_{i=0}^{n-k} \binom{k+i}{i} = \binom{n+1}{k+1}, \tag{13}$$

$$\sum_{k=0}^{n} (-1)^k (a+k)^n \binom{n}{k} = (-1)^n n! \text{ for } a \in \mathbb{Z}. \tag{14}$$

Using these we get

$$\begin{aligned}
\sum_{m=2}^{n}(-1)^m \sum_{\substack{k_1,\dots,k_m\geq 1\\ k_1+\cdots+k_m=n}} \frac{n!}{k_1!\cdots k_m!} &= \sum_{m=2}^{n}(-1)^m \sum_{r=0}^{m-1}(-1)^r \binom{m}{r}(m-r)^n \\
&= 1+\sum_{m=1}^{n}(-1)^m \sum_{r=0}^{m-1}(-1)^r \binom{m}{r}(m-r)^n \\
&= 1+\sum_{k=1}^{n}\sum_{m=k}^{n}(-1)^{2m-k}\binom{m}{m-k}k^n \\
&= 1+\sum_{k=1}^{n}(-1)^k k^n \sum_{m=k}^{n}\binom{m}{m-k} \\
&= 1+\sum_{k=1}^{n}(-1)^k k^n \binom{n+1}{k+1} \\
&= 1+\sum_{k=1}^{n}(-1)^k k^n \binom{n}{k} + \sum_{k=1}^{n}(-1)^k k^n \binom{n}{k+1} \\
&= 1+\sum_{k=0}^{n}(-1)^k k^n \binom{n}{k} - \sum_{k=0}^{n}(-1)^k (-1+k)^n \binom{n}{k} + (-1)^n \\
&= 1+(-1)^n n! - (-1)^n n! + (-1)^n \\
&= 1+(-1)^n
\end{aligned}$$

and this expression is equal to 2 if n is even and 0 if n is odd. $\square$

Let $h > 0$. We recall that an *ordered partition* of h is a t-tuple $\pi = (n_1, \dots, n_t)$ where the n_i are positive integers with $n_1 + \cdots + n_t = h$. We denote with $l(\pi)$ the length of π, that is $l(\pi) = t$. Also we denote as $\pi!$ the product

$$\pi! := n_1! \cdots n_t!.$$

Now let $n > 0$, and $k_1, \dots, k_s \geq 1$ with $k_1 + \cdots + k_s = n$. We write $\bar{k} = (k_1, \dots, k_s)$. For fixed $0 = m_0 < m_1 < \cdots < m_q = s$ we define the sequence $h_1(\bar{k}), \dots, h_q(\bar{k})$ as

$$h_r(\bar{k}) = \sum_{i=m_{r-1}+1}^{m_r} k_i. \tag{15}$$

It is obvious that $h_1(\bar{k}) + \cdots + h_q(\bar{k}) = n$. Moreover, we set $\pi_r(\bar{k}) = (k_{m_{r-1}+1}, \dots, k_{m_r})$. For the following lemma we recall that $\sum_n$ is short for

$$\sum_{\substack{k_1,\dots,k_s\geq 1\\ k_1+\cdots+k_s=n}}.$$

Lemma 15. *Fix m_i with $0 = m_0 < m_1 < \cdots < m_q = s$. Then* (6) *implies that*

$$\sum_n \frac{h_1(\bar{k})!}{\pi_1(\bar{k})!} \cdots \frac{h_q(\bar{k})!}{\pi_q(\bar{k})!} [(x_{j_{m_1}}^{(h_1(\bar{k}))} \cdots x_{j_{m_q}}^{(h_q(\bar{k}))})^* y] = 0 \tag{16}$$

for all $j_{m_1} \leq \cdots \leq j_{m_q}$.

Proof. We recall that a term $[(x_{j_1}^{(k_1)} \dots x_{j_s}^{(k_s)})^* y]$ from (6) involves a summation over all permutations of

$$(\underbrace{j_1, \dots, j_1}_{k_1}, \dots, \underbrace{j_s, \dots, j_s}_{k_s}),$$

where $k_1 + \cdots + k_s = n$. Now we put

$$j_1 = \cdots = j_{m_1} \le j_{m_1+1} = \cdots = j_{m_2} \le \cdots \le j_{m_{q-1}+1} = \cdots = j_{m_q},$$

then we get

$$[(x_{j_1}^{(k_1)} \dots x_{j_s}^{(k_s)})^* y] = \frac{h_1(\bar{k})!}{\pi_1(\bar{k})!} \cdots \frac{h_q(\bar{k})!}{\pi_q(\bar{k})!} [(x_{j_{m_1}}^{(h_1(\bar{k}))} \cdots x_{j_{m_q}}^{(h_q(\bar{k}))})^* y]. \quad \square$$

Remark 16. For an integer $h \ge 1$, the set of all ordered partitions of h of length t is denoted by $P_t(h)$. Now in Lemma 15 we set $t_i = m_i - m_{i-1}$ for $1 \le i \le q$. Then (16) can be written as

$$\sum_{\substack{h_1,\dots,h_q \ge 1 \\ h_1+\cdots+h_q = n}} \sum_{\substack{\pi_i \in P_{t_i}(h_i) \\ 1 \le i \le q}} \frac{h_1!}{\pi_1!} \cdots \frac{h_q!}{\pi_q!} [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y] = 0, \tag{17}$$

for $i_1 \le \cdots \le i_q$. Now (17) depends only on n, q and on the t_i.

Note that in (17) we can permute the $i_1, \dots, i_q$, cf. Remark 8 (we only lose the condition $i_1 \le \cdots \le i_q$). So we may assume that there is a p with $t_i > 1$ if $i \le p$ and $t_i = 1$ for $i > p$. But if $t_i = 1$, then $P_{t_i}(h_i)$ consists of one element, $\pi_i = (h_i)$, only, and moreover, $\frac{h_i!}{\pi_i!} = 1$. Hence we can rewrite (17) as

$$\sum_{\substack{h_1,\dots,h_q \ge 1 \\ h_1+\cdots+h_q = n}} \sum_{\substack{\pi_i \in P_{t_i}(h_i) \\ 1 \le i \le p}} \frac{h_1!}{\pi_1!} \cdots \frac{h_p!}{\pi_p!} [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y] = 0. \tag{18}$$

Lemma 17. *For all p,*

$$\sum_{t_1 \ge 2} \cdots \sum_{t_p \ge 2} (-1)^{t_1+\cdots+t_p} \sum_{\substack{h_1,\dots,h_q \ge 1 \\ h_1+\cdots+h_q = n}} \sum_{\substack{\pi_i \in P_{t_i}(h_i) \\ 1 \le i \le p}} \frac{h_1!}{\pi_1!} \cdots \frac{h_p!}{\pi_p!} [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y] \tag{19}$$

$$= \sum_{\mathcal{A} = \{i_1,\dots,i_p\}}^{\square} 2^p \sum_{\substack{h_1,\dots,h_q \ge 1 \\ h_1+\cdots+h_q = n}} [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y]. \tag{20}$$

Proof. We can write (19) as

$$\sum_{\substack{h_1,\dots,h_q \ge 1 \\ h_1+\cdots+h_q = n}} \left(\sum_{t_1=2}^{h_1} (-1)^{t_1} \sum_{\pi_1 \in P_{t_1}(h_1)} \frac{h_1!}{\pi_1!} \right) \cdots \left(\sum_{t_p=2}^{h_p} (-1)^{t_p} \sum_{\pi_p \in P_{t_p}(h_p)} \frac{h_p!}{\pi_p!} \right) [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y].$$

But by Lemma 14 we have that

$$\sum_{t_i=2}^{h_i} (-1)^{t_i} \sum_{\pi_i \in P_{t_i}(h_i)} \frac{h_i!}{\pi_i!} = \begin{cases} 2, & \text{if } h_i \text{ is even;} \\ 0, & \text{otherwise.} \end{cases}$$

So we obtain (20). $\square$

This lemma implies that every instance of (7) can be obtained as a sum of elements of the form (18). But these are all zero by (6). So we get the following result.

Theorem 18. *The Lie ring L satisfies the n-Engel condition if and only if relation* (6) *is satisfied for all* $y \in L$, $1 \le j_1 \le \cdots \le j_s \le m$ *and* $1 \le s \le n$.

Remark 19 (*M. Vaughan-Lee*). We claim that it is only necessary to check the relation $[(x_{j_1}^{(1)} \cdots x_{j_n}^{(1)})^* y] = 0$ for y a generator of L. We ease notation a little by omitting the exponents, as they are (1) everywhere. Suppose that we have $[(x_{j_1} \cdots x_{j_n})^* y] = 0$ for all $j_1 \le \cdots \le j_n$ and a certain $y \in L$. Let $z \in L$, and a d$z : u \mapsto [z, u]$. Then

$$\begin{aligned} 0 &= \mathrm{ad}\, z([(x_{j_1} \cdots x_{j_n})^* y]) \\ &= [([z, x_{j_1}] \cdots x_{j_n})^* y] + \cdots + [(x_{j_1} \cdots [z, x_{j_n}])^* y] + [(x_{j_1} \cdots x_{j_n})^* [z, y]]. \end{aligned}$$

Now $[z, x_{j_1}] = \sum_{i=1}^{m} \alpha_i x_i$ for certain $\alpha_i \in \mathbb{Z}$. So

$$[([z, x_{j_1}] \cdots x_{j_n})^* y] = \sum_i \alpha_i [(x_i x_{j_2} \cdots x_{j_n})^* y].$$

But by hypothesis all summands on the right-hand side are zero. So $[([z, x_{j_1}] \cdots x_{j_n})^* y] = 0$. Similarly we get $[(x_{j_1}[z, x_{j_2}] \cdots x_{j_n})^* y] = \cdots = [(x_{j_1} \cdots [z, x_{j_n}])^* y] = 0$. Therefore $[(x_{j_1} \cdots x_{j_n})^* [z, y]] = 0$. We conclude that $[(x_{j_1} \cdots x_{j_n})^* y] = 0$ for all generators y of L implies it for all $y \in L$.

Remark 20. If L is defined over a field in which $n!$ is invertible, then only the relation $[(x_{j_1}^{(1)} \cdots x_{j_n}^{(1)})^* y] = 0$ with $j_1 \le j_2 \le \cdots \le j_n$ is needed. Indeed, this implies that $[(x_{j_1}^{(k_1)} \cdots x_{j_s}^{(k_s)})^* y] = 0$ (cf. the proof of Lemma 15). Hence we get all relations (6). This can also be proved independently. It is used in Havas et al. (1990) to compute several n-Engel Lie rings over finite fields.

Proposition 21. *Relations* (6) *are satisfied for all* $1 \le s \le n$ *and* $j_1 \le \cdots \le j_s$ *if and only if* (17) *is satisfied for all* $q = 1, \ldots, n$, *for all* $t_r \ge 1$, $r = 1, \ldots, q$, $t_1 + \cdots + t_q \le n$ *and for all* $i_1 < \cdots < i_q$.

Proof. This is shown by the same reasoning as used for Lemma 15. This time we set

$$j_1 = \cdots = j_{m_1} < j_{m_1+1} = \cdots = j_{m_2} < \cdots < j_{m_{q-1}+1} = \cdots = j_{m_q}. \quad \square$$

We remark that, in this way, we obtain a system of relations that can be reduced. Next we describe a method for doing this. First we set

$$f_n(m) := \sum_{\substack{k_1, \ldots, k_m \ge 1 \\ k_1 + \cdots + k_m = n}} \frac{n!}{k_1! \cdots k_m!} = \sum_{r=0}^{m-1} (-1)^r \binom{m}{r} (m-r)^n,$$

(cf. (12)). Obviously $f_n(m) = 0$ for all $m > n$ and $f_n(1) = 1$ for all n. So (17) can be written as

$$\sum_{\substack{h_1, \ldots, h_q \ge 1 \\ h_1 + \cdots + h_q = n}} f_{h_1}(t_1) \cdots f_{h_q}(t_q) [(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y] = 0. \tag{21}$$

We denote the left-hand side of (21) as $g(t_1, \ldots, t_q)$.

We define an order "$>$" on the elements $[(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y]$ (where the $i_1, \ldots, i_q$ are fixed) as follows

$$[(x_{i_1}^{(h_1)} \cdots x_{i_q}^{(h_q)})^* y] > [(x_{i_1}^{(\bar{h}_1)} \cdots x_{i_q}^{(\bar{h}_q)})^* y]$$

if and only if $h_{i_0} > \bar{h}_{i_0}$, where i_0 is the minimal index with $h_{i_0} \ne \bar{h}_{i_0}$.

For all q we can consider a matrix M_q where a row consists of the coefficients of $g(t_1, \ldots, t_q)$ ordered with $>$. So the rows of M_q are indexed by q-tuples $(t_1, \ldots, t_q)$ with $t_1 + \cdots + t_q \le n$.

Note that the columns of M_q are indexed by $(h_1, \ldots, h_q)$, which are ordered partitions of n of length q. So we have $\binom{n-1}{q-1}$ columns in M_q, one for every ordered partition of n of length q. We claim that the rank of M_q is exactly $\binom{n-1}{q-1}$. Indeed, let $(h_1^0, \ldots, h_q^0)$ be the index of a column, and set $t_i = h_i^0$. Then in the row indexed by $(t_1, \ldots, t_q)$ we have a non-zero entry only in the column indexed by $(h_1^0, \ldots, h_q^0)$. So if we calculate the Hermite normal form of M_q, we obtain a matrix with $\binom{n-1}{q-1}$ non-zero rows, which

Table 1
Terms of the lower central series of the free n-Engel Lie rings $E(2,3)$, $E(3,3)$, $E(4,3)$, $E(2,4)$. The last line indicates the running time. Here L^k denotes the kth term of the lower central series of L.

	$E(2,3)$	$E(3,3)$	$E(4,3)$	$E(2,4)$
L^1	$2^3 0^5$	$2^{40} 10^3 0^{17}$	$2^{466} 10^{26} 40^4 0^{45}$	$5^{15} 10^8 0^{11}$
L^2	$2^3 0^3$	$2^{40} 10^3 0^{14}$	$2^{466} 10^{26} 40^4 0^{41}$	$5^{15} 10^8 0^9$
L^3	$2^3 0^2$	$2^{40} 10^3 0^{11}$	$2^{466} 10^{26} 40^4 0^{35}$	$5^{15} 10^8 0^8$
L^4	2^3	$2^{40} 10^3 0^3$	$2^{466} 10^{26} 40^4 0^{15}$	$5^{15} 10^8 0^6$
L^5	2^2	$2^{33} 10^3$	$2^{442} 10^{26} 40^4$	$5^{15} 10^8 0^3$
L^6		2^{18}	$2^{378} 10^{10}$	$5^{16} 10^7 0^1$
L^7		2^9	$2^{289} 10^4$	$5^{15} 10^5$
L^8		2^3	2^{173}	$5^{14} 10^2$
L^9			2^{62}	5^{12}
L^{10}			2^{18}	5^6
L^{11}			2^4	5^3
L^{12}				5^1
Time	0.5 (s)	23 (s)	12 (days)	88 (s)

correspond to the relations that remain. Summing, we obtain

$$\sum_{q=1}^{n} \binom{n-1}{q-1} = 2^{n-1}$$

relations.

Example 22. If we apply this to the case $n = 4$ we get the following result: L is 4-Engel if and only if for all $1 \le j_1 < j_2 < j_3 < j_4 \le m$ we have

$$\begin{aligned}
&[(x_{j_1}^{(4)})^* y] = 0\\
&[(x_{j_1}^{(3)} x_{j_2}^{(1)})^* y] + [(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(3)})^* y] = 0\\
&2[(x_{j_1}^{(2)} x_{j_2}^{(2)})^* y] = 0\\
&6[(x_{j_1}^{(1)} x_{j_2}^{(3)})^* y] = 0\\
&[(x_{j_1}^{(2)} x_{j_2}^{(1)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] + [(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&2[(x_{j_1}^{(1)} x_{j_2}^{(2)} x_{j_3}^{(1)})^* y] = 0\\
&2[(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(2)})^* y] = 0\\
&[(x_{j_1}^{(1)} x_{j_2}^{(1)} x_{j_3}^{(1)} x_{j_4}^{(1)})^* y] = 0.
\end{aligned}$$

We would like to emphasize the main difference with Example 13: here the indices j_i satisfy strict inequalities. This leads to a lot fewer relations that have to be checked.

5. Some n-Engel Lie rings

We have used our implementations of the algorithms described in this paper to obtain a basis and multiplication table of the "freest" n-Engel Lie rings with t generators for $(t, n) = (2, 3), (3, 3), (4, 3), (2, 4)$. In Table 1 we list the terms of their lower central series. We give their structure as an Abelian group (i.e., as a $\mathbb{Z}$-module). Now a finitely generated Abelian group can uniquely be written as $(\mathbb{Z}/d_1\mathbb{Z})^{k_1} \oplus \cdots \oplus (\mathbb{Z}/d_r\mathbb{Z})^{k_r} \oplus \mathbb{Z}^m$, where d_i divides d_{i+1}. We denote this group by $d_1^{k_1} \cdots d_r^{k_r} 0^m$.

The table also lists the time needed for the constructions (which were done on a 2 GHz machine with 2 GB of memory). The rather long time needed for the construction of $E(4, 3)$ is explained by the huge number of relations (to enforce the 3-Engel identity) that are generated in this case. We used a basic linear dependence test (based on the Hermite normal form algorithm for matrices over $\mathbb{Z}$) to try and discard relations that are linearly dependent on others. By this method many relations could be discarded immediately, and the program was mainly busy doing that. We are not yet able to construct $E(3, 4)$ and $E(2, 5)$. When dealing with these cases the programs ran out of memory because of the large number of relations and their greater density (i.e., they contain more monomials than in the 3-Engel case).

Acknowledgements

We thank M. Vaughan-Lee for suggesting the topic of n-Engel Lie rings to us, and for very helpful conversations on the subject. Also we would like to thank J. Cannon, and the Magma group at the University of Sydney, for their kind hospitality during May 2007, when part of the work in the paper was done, and the Magma implementation of the algorithms was written. Finally, the comments of S. Mattarei on an earlier version of this paper are gratefully acknowledged.

References

Adams, W.W., Loustaunau, P., 1994. An introduction to Gröbner bases. In: Graduate Studies in Mathematics, vol. 3. American Mathematical Society, Providence, RI.
Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. In: Computational Algebra and Number Theory (London, 1993). J. Symbolic Comput. 24 (3–4), 235–265.
Cicalò, S., de Graaf, W.A., 2007. Non-associative gröbner bases, finitely-presented Lie rings and the engel condition. In: Brown, C.W. (Ed.), Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation. ISSAC'07. ACM, New York, pp. 100–107.
GAP, 2004. GAP – Groups, Algorithms, and Programming, Version 4.4. The GAP Group. http://www.gap-system.org.
Gerdt, V.P., Kornyak, V.V., 1996. Construction of finitely presented Lie algebras and superalgebras. J. Symbolic Comput. 21 (3), 337–349.
Gerritzen, L., 2006. Tree polynomials and non-associative Gröbner bases. J. Symbolic Comput. 41 (3–4), 297–316.
de Graaf, W.A., 2000. Lie Algebras: Theory and Algorithms. In: North-Holland Mathematical Library, vol. 56. Elsevier Science.
de Graaf, W.A., Wisliceny, J., 1999. Constructing bases of finitely presented Lie algebras using Gröbner bases in free algebras. In: Dooley, S. (Ed.), Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation. ISSAC'99. ACM Press, pp. 37–43.
Havas, G., Newman, M.F., Vaughan-Lee, M.R., 1990. A nilpotent quotient algorithm for graded Lie rings. J. Symbolic Comput. 9 (5–6), 653–664.
Higgins, P.J., 1954. Lie rings satisfying the Engel condition. Proc. Cambridge Philos. Soc. 50, 8–15.
Huppert, B., Blackburn, N., 1982. Finite Groups II. Springer Verlag, New York, Heidelberg, Berlin.
Kostrikin, A.I., 1990. Around Burnside. In: Ergebnisse der Mathematik und ihrer Grenzgebiete (3) (Results in Mathematics and Related Areas (3)), vol. 20. Springer-Verlag, Berlin. Translated from the Russian and with a preface by James Wiegold.
Leeuwen, M.A.A.v., Roelofs, M., 1997. Termination for a class of algorithms for constructing algebras given by generators and relations. J. Pure Appl. Algebra 117/118, 431–445.
Newman, M.F., O'Brien, E.A., Vaughan-Lee, M.R., 2004. Groups and nilpotent Lie rings whose order is the sixth power of a prime. J. Algebra 278 (1), 383–401.
O'Brien, E.A., Vaughan-Lee, M.R., 2005. The groups with order p^7 for odd prime p. J. Algebra 292 (1), 243–258.
Rajaee, S., 2006. Non-associative Gröbner bases. J. Symbolic Comput. 41 (8), 887–904.
Schneider, C., 1997. Computing nilpotent quotients in finitely presented Lie rings. Discrete Math. Theoret. Comput. Sci. 1 (1), 1–16 (electronic).
Sims, C.C., 1994. Computation with Finitely Presented Groups. Cambridge University Press, Cambridge.
Traustason, G., 1993. Engel Lie-algebras. Quart. J. Math. Oxford Ser. (2) 44 (175), 355–384.
Traustason, G., 1995. A polynomial upper bound for the nilpotency classes of Engel-3 Lie algebras over a field of characteristic 2. J. London Math. Soc. (2) 51 (3), 453–460.
Vaughan-Lee, M.R., 1998. On Zel'manov's solution of the restricted Burnside problem. J. Group Theory 1 (1), 65–94.
Vaughan-Lee, M.R., 2003. Lie methods in group theory. In: Groups St. Andrews 2001 in Oxford. Vol. II. In: London Math. Soc. Lecture Note Ser., vol. 305. Cambridge Univ. Press, Cambridge, pp. 547–585.