

# An application of lattice basis reduction to polynomial identities for algebraic structures

Murray R. Bremner<sup>a,\*</sup>, Luiz A. Peresi<sup>b</sup>

<sup>a</sup>*Department of Mathematics and Statistics, University of Saskatchewan, Canada*

<sup>b</sup>*Departamento de Matemática, Universidade de São Paulo, Brasil*

---

## Abstract

The authors' recent classification of trilinear operations includes, among other cases, a fourth family of operations with parameter  $q \in \mathbb{Q} \cup \{\infty\}$ , and weakly commutative and weakly anticommutative operations. These operations satisfy polynomial identities in degree 3 and further identities in degree 5. For each operation, using the row canonical form of the expansion matrix  $E$  to find the identities in degree 5 gives extremely complicated results. We use lattice basis reduction to simplify these identities: we compute the Hermite normal form  $H$  of  $E^t$ , obtain a basis of the nullspace lattice from the last rows of a matrix  $U$  for which  $UE^t = H$ , and then use the LLL algorithm to reduce the basis.

*Key words:* Nonassociative algebra, LLL algorithm, Hermite normal form.

*2000 MSC:* Primary 17-08; Secondary 11D04, 11H06, 15A21, 17A40, 68W30.

---

## 1. Introduction

Computational studies of polynomial identities for nonassociative algebras often lead to very complicated identities with large numbers of terms and seemingly random coefficients; see for example Bremner and Hentzel [2, Table IV]. The purpose of this paper is to demonstrate how lattice basis reduction can be applied to find much simpler identities which are equivalent to the original identities. We represent the identities as the nullspace of a large matrix  $E$  with entries in  $\mathbb{Z}$  (the expansion matrix). From the row canonical form of  $E$  over  $\mathbb{Q}$  we can extract an integral basis for the nullspace as a vector space over  $\mathbb{Q}$ , but in general these basis vectors do not form a basis for the nullspace lattice (the set of integral nullspace vectors). We can find a basis for the nullspace lattice by computing the Hermite normal form  $H$  of the transpose  $E^t$  and simultaneously computing a matrix  $U$  for which  $UE^t = H$ . If the nullspace of  $E$  has dimension  $d$  over  $\mathbb{Q}$  then the last  $d$  rows of  $U$  are an integral basis for the nullspace lattice.

---

\*Corresponding author

*Email addresses:* [bremner@math.usask.ca](mailto:bremner@math.usask.ca) (Murray R. Bremner), [peresi@ime.usp.br](mailto:peresi@ime.usp.br) (Luiz A. Peresi)

These basis vectors are often still very complicated; to simplify them we use the LLL algorithm with a suitable value of the parameter.

In this paper we apply this approach to the most difficult cases arising from our recent classification of trilinear operations; see Bremner and Peresi [3]. We use standard algorithms for the Hermite normal form, for lattice basis reduction, and for representations of the symmetric group; the application of the LLL algorithm to the study of polynomial identities for algebras seems to be new. The trilinear operations we study first appeared in [3]; at that time we had not discovered simple identities satisfied by these operations. In this paper we present 32 new identities in degree 5 satisfied by these operations; the maximum coefficient (in absolute value) appearing in these identities is 3, which is a great improvement over the results that can be obtained without lattice basis reduction.

## 2. Classification of trilinear operations

In this section we recall the relevant results from Bremner and Peresi [3].

**Definition 1.** A **ternary algebra** is a vector space  $V$  over a field  $\mathbb{F}$  with a trilinear map  $V \times V \times V \rightarrow V$  denoted  $(a, b, c) \mapsto abc$ . If  $(abc)de = a(bcd)e = ab(cde)$  for all  $a, b, c, d, e \in V$  then we say that this ternary algebra is **totally associative**.

**Definition 2.** A **trilinear operation** is a linear combination of permutations of the indeterminates  $a, b, c$ :

$$[a, b, c] = x_1 abc + x_2 acb + x_3 bac + x_4 bca + x_5 cab + x_6 cba \quad (x_i \in \mathbb{F}).$$

If we regard  $[a, b, c]$  as an element of the group algebra  $\mathbb{F}S_3$ , then we say that two trilinear operations are **equivalent** if they generate the same left ideal. If we regard the permutations as products in a totally associative ternary algebra, then  $[a, b, c]$  is a new nonassociative operation on the same underlying vector space.

**Proposition 3.** *There are infinitely many equivalence classes of trilinear operations over  $\mathbb{Q}$ : eight isolated operations and four one-parameter families.*

*Proof.* Bremner and Peresi [3, §3.3]. □

The eight isolated operations are the zero operation, the symmetric sum, the alternating sum, the cyclic sum, the cyclic commutator, the weakly commutative operation, the weakly anticommutative operation, and the original totally associative operation. The four one-parameter families are the Lie, Jordan and anti-Jordan families, and a fourth family. All these operations (except the original totally associative operation) satisfy polynomial identities in degree 3. In some cases, simple polynomial identities in degree 5 can be obtained from the expansion matrix for the operation by computing the row canonical form over  $\mathbb{Q}$  and extracting the canonical integral basis for the nullspace. However, for

the fourth family and for the weakly commutative and weakly anticommutative operations, this gives very complicated results. Our goal in this paper is to show how lattice basis reduction can be used to quickly simplify the polynomial identities for these operations.

**Definition 4.** The **fourth family** of trilinear operations consists of

$$\begin{aligned} [a, b, c]_\infty &= abc + acb - bac + 2 bca, \\ [a, b, c]_q &= 2 abc + q acb + (1-q) bac + q bca + (1-q) cab - cba \quad (q \in \mathbb{Q}). \end{aligned}$$

**Lemma 5.** For each operation in the fourth family, every homogeneous multilinear identity in degree 3 is a consequence of the identity

$$G(a, b, c) = [a, b, c] - [a, c, b] - [b, c, a] + [c, b, a].$$

*Proof.* We first consider  $q \in \mathbb{Q}$ . Let  $E$  be the matrix in which  $E_{ij}$  is the coefficient of the  $i$ -th associative monomial in the expansion of the  $j$ -th nonassociative monomial:

$$E = \begin{bmatrix} 2 & q & 1-q & 1-q & q & -1 \\ q & 2 & q & -1 & 1-q & 1-q \\ 1-q & 1-q & 2 & q & -1 & q \\ q & -1 & q & 2 & 1-q & 1-q \\ 1-q & 1-q & -1 & q & 2 & q \\ -1 & q & 1-q & 1-q & q & 2 \end{bmatrix}.$$

We find the row canonical form over  $\mathbb{Q}[q]$  and extract a basis for the nullspace:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & -1 & 1 & -1 & 1 & 0 \\ 1 & -1 & 0 & -1 & 0 & 1 \end{bmatrix}.$$

The basis vectors represent these identities:

$$-[a, c, b] + [b, a, c] - [b, c, a] + [c, a, b], \quad [a, b, c] - [a, c, b] - [b, c, a] + [c, b, a].$$

The second is  $G(a, b, c)$ , and the first is  $G(b, a, c)$ . Thus  $G(a, b, c)$  is satisfied by  $[a, b, c]_q$  and implies all the identities in degree 3 for  $[a, b, c]_q$ . The proof for  $q = \infty$  is similar.  $\square$

**Lemma 6.** For the homogeneous multilinear subspace of degree 5 in the free ternary algebra satisfying the identity  $G(a, b, c) \equiv 0$ , a basis consists of the 160 monomials obtained by permuting  $[[a, b, c], d, e]$  and  $[a, [b, c, d], e]$  such that the first argument of the inner triple does not lexicographically follow both the second and third arguments.

*Proof.* The polynomial  $G(a, b, c)$  can be “lifted” to degree 5 in six ways: replacing  $a$ ,  $b$  or  $c$  by a triple, or embedding  $G(a, b, c)$  in a triple. This gives six polynomials in degree 5:

$$\begin{aligned} G([a, d, e], b, c), & \quad G(a, [b, d, e], c), & \quad G(a, b, [c, d, e]), \\ [G(a, b, c), d, e], & \quad [d, G(a, b, c), e], & \quad [d, e, G(a, b, c)]. \end{aligned}$$

Every consequence in degree 5 of  $G(a, b, c)$  is a linear combination of the monomials obtained by permutating the 5 arguments in these six “liftings”.

First, we show that the monomials of the Lemma span the subspace. Any homogeneous multilinear polynomial of degree 5 for a trilinear operation is a linear combination of the monomials obtained by permutating the arguments in three basic monomials, one for each association type:  $[[a, b, c], d, e]$ ,  $[a, [b, c, d], e]$ ,  $[a, b, [c, d, e]]$ . From the identity  $G(a, b, [c, d, e]) \equiv 0$  we get

$$[a, b, [c, d, e]] \equiv [a, [c, d, e], b] + [b, [c, d, e], a] - [[c, d, e], b, a].$$

This implies that any monomial of the third type is a linear combination of monomials of the first and second types. From the identities  $[G(b, a, c), d, e] \equiv 0$  and  $[d, G(b, a, c), e] \equiv 0$  we get

$$\begin{aligned} [[c, a, b], d, e] & \equiv [[a, c, b], d, e] - [[b, a, c], d, e] + [[b, c, a], d, e], \\ [d, [c, a, b], e] & \equiv [d, [a, c, b], e] - [d, [b, a, c], e] + [d, [b, c, a], e]. \end{aligned}$$

These imply the condition on the inner triple in the first and second types.

Second, we enumerate the monomials of the Lemma. There are  $5!$  permutations of the arguments in each of the first two types:  $[[a, b, c], d, e]$ ,  $[a, [b, c, d], e]$ . The condition on the inner triple eliminates the last two of the six permutations  $abc$ ,  $acb$ ,  $bac$ ,  $bca$ ,  $cab$ ,  $cba$ . Thus each of the first two types contributes  $\frac{2}{3} \cdot 5! = 80$  monomials.

Third, we show that the monomials of the Lemma are linearly independent. Suppose to the contrary that they satisfy some non-trivial dependence relation. Any such dependence relation must come from the “liftings” of  $G(a, b, c)$  to degree 5. We have already used  $G(a, b, [c, d, e])$ ,  $[G(a, b, c), d, e]$ ,  $[d, G(a, b, c), e]$ . It remains to show that the other three can be expressed as linear combinations of the polynomials obtained by permutating the arguments in these three. It can be easily verified by direct calculation that

$$\begin{aligned} G([a, d, e], b, c) & = -G(b, c, [a, d, e]) + G(c, b, [a, d, e]), \\ G(a, [b, d, e], c) & = -G(a, c, [b, d, e]), \\ [d, e, G(a, b, c)] & = G(d, e, [a, b, c]) - G(d, e, [a, c, b]) - G(d, e, [b, c, a]) \\ & \quad + G(d, e, [c, b, a]) - [G(a, b, c), e, d] + [d, G(a, b, c), e] + [e, G(a, b, c), d]. \end{aligned}$$

This completes the proof.  $\square$

**Lemma 7.** For  $q = \infty$ , the operation  $[a, b, c]_\infty$  satisfies a space of dimension  $54$  of identities in degree 5 which do not follow from  $G(a, b, c)$ . For  $q \in \mathbb{Q}$ ,

the operation  $[a, b, c]_q$  satisfies a space of dimension 40 of identities in degree 5 which do not follow from  $G(a, b, c)$ . For five finite values of  $q$  there are further identities: for  $q \in \{0, 1, -1, 2\}$  the space has dimension 49; for  $q = \frac{1}{2}$  the space has dimension 54.

*Proof.* Bremner and Peresi [3, Theorem 21].  $\square$

**Remark 8.** The automorphism group  $PGL_2(\mathbb{Q})$  of the function field  $\mathbb{Q}(q)$  consists of the transformations  $q \mapsto (aq + b)/(cq + d)$  for  $ad - bc \neq 0$  which can be regarded as acting on the projective line  $\mathbb{Q} \cup \{\infty\}$ . The subgroup which permutes  $\{\infty, 0, 1, -1, 2, \frac{1}{2}\}$  is isomorphic to the dihedral group of order 12.

**Definition 9.** The **weakly commutative** and **weakly anticommutative** operations are

$$\begin{aligned} [a, b, c]_+ &= 5abc + acb + bac - bca - cab + cba, \\ [a, b, c]_- &= 5abc - acb - bac - bca - cab - cba. \end{aligned}$$

**Lemma 10.** *For the weakly commutative and weakly anticommutative operations, every homogeneous multilinear identity in degree 3 is a consequence of the identities*

$$\begin{aligned} H_+(a, b, c) &= [a, b, c]_+ - [a, c, b]_+ - [b, a, c]_+ + [b, c, a]_+ + [c, a, b]_+ - [c, b, a]_+, \\ H_-(a, b, c) &= [a, b, c]_- + [a, c, b]_- + [b, a, c]_- + [b, c, a]_- + [c, a, b]_- + [c, b, a]_-. \end{aligned}$$

*Proof.* Similar to the proof of Lemma 5.  $\square$

**Lemma 11.** *For the multilinear subspace of degree 5 in the free ternary algebra satisfying either of the identities of Lemma 10, a basis consists of the 250 monomials obtained by permuting  $[[a, b, c], d, e]$ ,  $[a, [b, c, d], e]$  and  $[a, b, [c, d, e]]$  such that the arguments of the inner triple are not in decreasing order and (in the third case only) the first argument of the outer triple precedes the second argument.*

*Proof.* Similar to the proof of Lemma 6.  $\square$

**Lemma 12.** *The operation  $[a, b, c]_+$  (respectively  $[a, b, c]_-$ ) satisfies a space of dimension 141 of identities in degree 5 which do not follow from the first (respectively second) identity of Lemma 10.*

*Proof.* Bremner and Peresi [3, Theorems 23 and 24].  $\square$

**Definition 13.** The **ordered basis of nonassociative monomials** in degree 5 for any operation in the fourth family (respectively the weakly commutative and weakly anticommutative operations) consists of the monomials of Lemma 6 (respectively Lemma 11) ordered first by association type and then lexicographically by the permutation of the arguments  $a, b, c, d, e$ . The **ordered basis of associative monomials** consists of the permutations of  $a, b, c, d, e$  in lexicographical order. The **expansion of a nonassociative monomial**

is the linear combination of the associative monomials obtained by applying Definition 4 (respectively Definition 9). The **expansion matrix**  $E$  has 120 rows labeled by the associative monomials and 160 (respectively 250) columns labeled by the nonassociative monomials; entry  $E_{ij}$  is the coefficient of the  $i$ -th associative monomial in the expansion of the  $j$ -th nonassociative monomial.

**Example 14.** The expansion of the fourth family monomial  $[[a, b, c]_\infty, d, e]_\infty$ :

$$\begin{aligned} & abcde + acbde - bacde + 2bcade + abced + acbed - baced + 2bcaed \\ & - dabce - dacbe + dbace - 2dbcae + 2deabc + 2deacb - 2debac + 4debca \end{aligned}$$

**Example 15.** The expansion of the fourth family monomial  $[[a, b, c]_q, d, e]_q$ :

$$\begin{aligned} & 4 abcde + 2q abced + 2q acbde + q^2 acbed \\ +2(1-q) bacde - q(q-1) baced + 2q bcade + q^2 bcaed \\ +2(1-q) cabde - q(q-1) cabed - 2 cbade - q cbaed \\ +2(1-q) dabce - q(q-1) dacbe + (q-1)^2 dbace - q(q-1) dbcae \\ + (q-1)^2 dcabe + (q-1) dcbae + 2q deabc + q^2 deacb \\ - q(q-1) debac + q^2 debca - q(q-1) decab - q decba \\ +2(1-q) eabcd - q(q-1) eacbd + (q-1)^2 ebacd - q(q-1) ebcad \\ + (q-1)^2 ecabd + (q-1) ecbad - 2 edabc - q edacb \\ + (q-1) edbac - q edbca + (q-1) edcab + edcba \end{aligned}$$

### 3. Algorithms for the nullspace lattice of an integer matrix

**Definition 16.** For an  $m \times n$  matrix  $A$  over  $\mathbb{Z}$ , the **nullspace lattice** is

$$\text{Null}_{\mathbb{Z}}(A) = \{ X \in \mathbb{Z}^n \mid AX = O \}.$$

The rank of this lattice equals the dimension  $d$  of the nullspace of  $A$  over  $\mathbb{Q}$ .

**Example 17.** Consider the matrix  $A$  and its row canonical form:

$$A = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 2 & 3 & 5 \end{bmatrix}, \quad \text{RCF}(A) = \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & \frac{3}{2} & \frac{5}{2} \end{bmatrix}.$$

We want to find vectors  $X_1, X_2 \in \text{Null}_{\mathbb{Z}}(A)$  which are linearly independent over  $\mathbb{Q}$  and satisfy  $\text{Null}_{\mathbb{Z}}(A) = \mathbb{Z}X_1 \oplus \mathbb{Z}X_2$ . From  $\text{RCF}(A)$  we obtain the canonical basis for the nullspace of  $A$  as a vector space over  $\mathbb{Q}$  and then clear denominators to obtain integral basis vectors:

$$\left[-1, -\frac{3}{2}, 1, 0\right], \left[-2, -\frac{5}{2}, 0, 1\right] \longrightarrow \left[-2, -3, 2, 0\right], \left[-4, -5, 0, 2\right].$$

However,  $\text{Null}_{\mathbb{Z}}(A)$  also contains the vector  $[-1, -1, -1, 1]$ , which is not an integral linear combination of the integral basis vectors.

- Input: An  $m \times n$  matrix  $A$  over  $\mathbb{Z}$ .
  - Output: The  $m \times n$  matrix  $H$  over  $\mathbb{Z}$  in Hermite normal form, and an  $m \times m$  matrix  $U$  over  $\mathbb{Z}$  with  $\det(U) = \pm 1$  and  $UA = H$ .
1. Set  $H \leftarrow A$ ,  $U \leftarrow I_m$ ,  $i \leftarrow 1$ ,  $j \leftarrow 1$ .
  2. While  $i \leq m$  and  $j \leq n$  do:
    - If  $\text{zerocol}(H, i, m, j)$  then
      - (a) Set  $j \leftarrow j+1$
    - else
      - (b) While not  $[H[i, j] > 0 \text{ and } \text{zerocol}(H, i+1, m, j)]$  do:
        - i. Set  $s \leftarrow \min\{|H_{pj}| : H_{pj} \neq 0, i \leq p \leq m\}$ .
        - ii. Choose  $p$  so that  $|H_{pj}| = s$ .
        - iii. Exchange rows  $i$  and  $p$  of  $H$ , and the same for  $U$ .
        - iv. If  $H_{ij} < 0$  then multiply row  $i$  of  $H$  by  $-1$ , and the same for  $U$ .
        - v. For  $k = i+1$  to  $m$  do:
          - Write  $H_{kj} = qH_{ij} + r$  uniquely with  $0 \leq r < H_{ij}$ .
          - If  $q \neq 0$  then add  $-q$  times row  $i$  of  $H$  to row  $k$ , and the same for  $U$ .
      - (c) For  $k = 1$  to  $i-1$  do:
        - i. Write  $H_{kj} = qH_{ij} + r$  uniquely with  $0 \leq r < H_{ij}$ .
        - ii. If  $q \neq 0$  then add  $-q$  times row  $i$  of  $H$  to row  $k$ , and the same for  $U$ .
      - (d) Set  $i \leftarrow i+1$  and  $j \leftarrow j+1$ .
  - $\text{zerocol}(H, i_1, i_2, j)$ : If  $H_{ij} = 0$  for  $i_1 \leq i \leq i_2$  then **true**, otherwise **false**.

Figure 1: Algorithm for the Hermite normal form

**Definition 18.** The  $m \times n$  matrix  $H$  over  $\mathbb{Z}$  is in **Hermite normal form (HNF)** if there exists an integer  $r$  (the **rank** of  $H$ ) with  $0 \leq r \leq m$  and a sequence  $1 \leq j_1 < j_2 < \dots < j_r \leq n$  of integers such that

1.  $H_{ij} = 0$  for  $1 \leq i \leq r$  and  $1 \leq j < j_i$ ,
2.  $H_{i, j_i} \geq 1$  for  $1 \leq i \leq r$ ,
3.  $0 \leq H_{k, j_i} < H_{i, j_i}$  for  $1 \leq i \leq r$  and  $1 \leq k < i$ ,
4.  $H_{ij} = 0$  for  $r+1 \leq i \leq m$  and  $1 \leq j \leq n$ .

**Lemma 19.** *If  $A$  is an  $m \times n$  matrix over  $\mathbb{Z}$ , then there is a unique  $m \times n$  matrix  $H$  over  $\mathbb{Z}$  in Hermite normal form such that  $UA = H$  for some  $m \times m$  matrix  $U$  over  $\mathbb{Z}$  with  $\det(U) = \pm 1$ . (The matrix  $U$  is in general not unique.)*

*Proof.* Adkins and Weintraub [1, §5.2]. □

**Lemma 20.** *Let  $A$  be an  $m \times n$  matrix over  $\mathbb{Z}$ , let  $H$  be the Hermite normal form of  $A^t$ , and let  $U$  be an  $n \times n$  matrix over  $\mathbb{Z}$  with  $\det(U) = \pm 1$  and  $UA^t = H$ . If  $r$  is the rank of  $H$ , then the last  $n-r$  rows of  $U$  form a lattice basis for  $\text{Null}_{\mathbb{Z}}(A)$ .*

- Input: A basis  $b_1, \dots, b_n$  of  $\mathbb{R}^n$  and a parameter  $\alpha \in \mathbb{R}$  with  $\frac{1}{4} < \alpha \leq 1$ .
- Output: An  $\alpha$ -reduced basis  $c_1, \dots, c_n$  of the lattice  $L = \mathbb{Z}b_1 \oplus \dots \oplus \mathbb{Z}b_n$ .

1. For  $i = 1, \dots, n$  do: Set  $c_i \leftarrow b_i$ .
  2. For  $i = 1, \dots, n$  do:
    - (a) Set  $c_i^* \leftarrow c_i$ .
    - (b) For  $j = 1, \dots, i-1$  do: Set  $\mu_{ij} \leftarrow (c_i \cdot c_j^*)/\gamma_j^*$  and  $c_i^* \leftarrow c_i^* - \mu_{ij}c_j^*$ .
    - (c) Set  $\gamma_i^* \leftarrow c_i^* \cdot c_i^*$ .
  3. Set  $k \leftarrow 2$ .
  4. While  $k \leq n$  do:
    - (a) Call **reduce**( $k, k-1$ ).
    - (b) If  $\gamma_k^* \geq (\alpha - \mu_{k,k-1}^2)\gamma_{k-1}^*$  then
      - i. For  $\ell = k-2, \dots, 1$  do: Call **reduce**( $k, \ell$ ).
      - ii. Set  $k \leftarrow k+1$ .
    - else
      - (iii) Call **exchange**( $k$ ).
      - (iv) If  $k > 2$  then set  $k \leftarrow k-1$ .
- **reduce**( $k, \ell$ ): If  $|\mu_{k\ell}| > \frac{1}{2}$  then
    1. Set  $c_k \leftarrow c_k - \lceil \mu_{k\ell} \rceil c_\ell$ .
    2. For  $j = 1, \dots, \ell-1$  do: Set  $\mu_{kj} \leftarrow \mu_{kj} - \lceil \mu_{k\ell} \rceil \mu_{\ell j}$ .
    3. Set  $\mu_{k\ell} \leftarrow \mu_{k\ell} - \lceil \mu_{k\ell} \rceil$ .
  - **exchange**( $k$ ):
    1. Exchange  $c_{k-1}$  and  $c_k$ .
    2. Set  $\mu \leftarrow \mu_{k,k-1}$  and set  $\beta \leftarrow \gamma_k^* + \mu^2\gamma_{k-1}^*$ .
    3. Set  $\mu_{k,k-1} \leftarrow \mu\gamma_{k-1}^*/\beta$ , set  $\gamma_k^* \leftarrow \gamma_k^*\gamma_{k-1}^*/\beta$ , and set  $\gamma_{k-1}^* \leftarrow \beta$ .
    4. For  $j = 1, \dots, k-2$  do: Exchange  $\mu_{k-1,j}$  and  $\mu_{kj}$ .
    5. For  $i = k+1, \dots, n$  do:
      - (a) Set  $\lambda \leftarrow \mu_{ik}$  and set  $\mu_{ik} \leftarrow \mu_{i,k-1} - \mu\mu_{ik}$ .
      - (b) Set  $\mu_{i,k-1} \leftarrow \mu_{i,k-1}\mu_{ik} + \lambda$ .

Figure 2: The LLL algorithm for lattice basis reduction

*Proof.* Since  $H$  has rank  $r$ , the last  $n-r$  rows of  $H$  are zero, and so  $NA^t = O$  where  $N$  is the  $(n-r) \times n$  matrix consisting of the last  $n-r$  rows of  $U$ . Hence  $AN^t = O$ , and so the rows of  $N$  are in  $\text{Null}_{\mathbb{Z}}(A)$ . It remains to show that any vector  $X \in \text{Null}_{\mathbb{Z}}(A)$  is a linear combination over  $\mathbb{Z}$  of the rows of  $N$ ; for this we follow Cohen [4, Proposition 2.4.9]. Suppose that  $XA^t = O$  for some  $1 \times n$  vector  $X$  over  $\mathbb{Z}$ ; then  $YH = O$  where  $Y = XU^{-1}$ . Solving the linear system  $YH = O$  from top to bottom, we find that the first  $r$  components of  $Y$  are zero, and the last  $n-r$  components of  $Y$  are arbitrary. Hence the last  $n-r$  standard

- Input: A basis  $X_1, \dots, X_m \in \mathbb{Q}^n$  for the subspace of multilinear polynomial identities in degree  $k$ , where  $n$  is the number of monomials in degree  $k$ .
  - Output: A subset of  $X_1, \dots, X_m$  which generates the subspace of polynomial identities as a module over the symmetric group  $S_k$ .
1. Create an  $(n+k!) \times n$  matrix  $M$  with an  $n \times n$  upper block and a  $k! \times n$  lower block. Initialize  $M$  to zero.
  2. Set  $r \leftarrow 0$  (the rank of  $M$ ).
  3. For each  $i = 1, \dots, m$  do:
    - (a) Set  $\ell \leftarrow 0$ .
    - (b) For each  $\sigma \in S_k$  do:
      - i. Increment  $\ell$ .
      - ii. Apply  $\sigma$  to the polynomial identity  $X_i$ , obtaining  $\sigma X_i$ .
      - iii. Store  $\sigma X_i$  in row  $n + \ell$  of  $M$ .
    - (c) Compute the row canonical form of  $M$ . Set  $s \leftarrow \text{rank}(M)$ .
    - (d) If  $s > r$  then record  $X_i$  as a new generator and set  $r \leftarrow s$ .

Figure 3: Algorithm to extract module generators

unit vectors in  $\mathbb{Z}^n$  form a lattice basis for the solutions of  $H^t Y^t = O$  over  $\mathbb{Z}$ , that is for  $\text{Null}_{\mathbb{Z}}(H^t)$ . Since  $X = UY$ , the claim follows.  $\square$

**Example 21.** On the matrix  $A^t$  from Example 17 we perform the following row operations:

$$\begin{aligned} R_3 &\leftarrow R_3 - R_1, & R_4 &\leftarrow R_4 - 2R_1, & R_3 &\leftarrow R_3 - R_2, & R_4 &\leftarrow R_4 - 2R_2, & R_2 &\leftrightarrow R_3, \\ R_3 &\leftarrow R_3 - 2R_2, & R_4 &\leftarrow R_4 - R_2. \end{aligned}$$

We obtain  $UA^t = H$ :

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ 2 & 3 & -2 & 0 \\ -1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \\ 1 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

The last two rows of  $U$  form a basis for  $\text{Null}_{\mathbb{Z}}(A)$ .

**Remark 22.** Our algorithm for the Hermite normal form appears in Figure 1. (For a similar algorithm, which however uses “goto” statements, see Cohen [4, Algorithm 2.4.4].) Our algorithm makes no attempt to control the size of the matrix entries, and so it will not perform well on very large matrices. However, it is useful for our purposes, since it produces a matrix  $U$  which is “top-heavy”:  $U$  has large entries in the first  $r$  rows (which we do not need) and small entries in the last  $n-r$  rows (which give a basis for the nullspace lattice).

**Definition 23.** By the **square-length** of a vector  $X = (x_1, \dots, x_n) \in \mathbb{Z}^n$  we mean the square of its Euclidean length, that is  $x_1^2 + \dots + x_n^2 \in \mathbb{Z}$ .

**Example 24.** Consider this matrix:

$$A = \begin{bmatrix} 0 & 3 & 9 & 4 & 1 & 6 & 6 & 3 & -8 & 6 \\ -5 & -5 & 5 & 6 & 2 & 2 & 4 & 2 & -9 & -5 \\ 3 & -3 & -1 & 5 & 6 & 8 & -8 & 8 & 7 & -1 \\ 1 & -1 & 2 & 8 & 4 & -6 & 6 & 7 & 6 & -7 \\ 2 & 2 & 4 & 2 & -1 & -9 & -2 & -2 & -9 & -4 \end{bmatrix}$$

Our HNF algorithm applied to  $A^t$  produces this matrix  $U = [U_1|U_2]$ :

$$U_1 = \begin{bmatrix} 3133761 & 3269601 & 2999659 & -30494186 & 27570528 \\ -1491117 & -1555753 & -1427308 & 14509849 & -13118704 \\ -25284 & -26380 & -24202 & 246035 & -222446 \\ 44 & 46 & 42 & -428 & 387 \\ -1 & -1 & -1 & 10 & -9 \\ -11 & -7 & -4 & 52 & -13 \\ -2 & -3 & 4 & -14 & 42 \\ -9 & -8 & -15 & 92 & -60 \\ 12 & 13 & 12 & -122 & 114 \\ 2 & 5 & -11 & 10 & 14 \end{bmatrix}$$

$$U_2 = \begin{bmatrix} -71888 & 5979970 & 9185619 & -6267522 & -9257507 \\ 34206 & -2845410 & -4370733 & 2982234 & 4404939 \\ 580 & -48248 & -74112 & 50568 & 74692 \\ -1 & 84 & 129 & -88 & -130 \\ 0 & -2 & -3 & 2 & 3 \\ -7 & -10 & -32 & 12 & 26 \\ -7 & 3 & -11 & -1 & 6 \\ -2 & -15 & -37 & 16 & 32 \\ -1 & 24 & 35 & -25 & -36 \\ 1 & 3 & -12 & -3 & 3 \end{bmatrix}$$

The last five rows of  $U$  form a basis of  $\text{Null}_{\mathbb{Z}}(A)$ . The square-lengths of these vectors are 5052, 2205, 15312, 32060, 618.

**Definition 25.** If  $f_1, \dots, f_n$  is a basis of  $\mathbb{R}^n$ , then its **Gram-Schmidt orthogonalization** is the basis  $f_1^*, \dots, f_n^*$  defined inductively by

$$f_1^* = f_1, \quad f_i^* = f_i - \sum_{j=1}^{i-1} \mu_{ij} f_j^* \text{ where } \mu_{ij} = \frac{f_i \cdot f_j^*}{f_j^* \cdot f_j^*} \text{ for } i \geq 2.$$

**Definition 26.** We fix  $\alpha \in \mathbb{R}$  with  $\frac{1}{4} < \alpha \leq 1$ . A basis  $f_1, \dots, f_n$  of  $\mathbb{R}^n$  is called  **$\alpha$ -reduced** if these two conditions hold:

$$(a) \quad |\mu_{ji}| \leq \frac{1}{2} \text{ for } 1 \leq i < j \leq n,$$

$$(b) \quad \|f_{j+1}^* + \mu_{j+1,j} f_j^*\|^2 \geq \alpha \|f_j^*\|^2 \text{ for } 1 \leq j \leq n-1.$$

Condition (a) says that each  $f_j$  is almost orthogonal to the previous vectors  $f_1^*, \dots, f_{j-1}^*$  in the Gram-Schmidt orthogonalization. Condition (b) says that exchanging  $f_j$  and  $f_{j+1}$ , and recomputing the Gram-Schmidt orthogonalization, can produce a new shorter vector  $\hat{f}_j^* = f_{j+1}^* + \mu_{j+1,j} f_j^*$ , but not too much shorter.

**Lemma 27.** *Let  $f_1, \dots, f_n$  be an  $\alpha$ -reduced basis of  $\mathbb{R}^n$  and let  $L$  be the lattice it generates. Then  $f_1$  is no longer than a multiple depending on  $n$  (and  $\alpha$ ) of the shortest nonzero vector in  $L$ :*

$$\|f_1\|^2 \leq \left(\frac{4}{4\alpha-1}\right)^{n-1} \|g\|^2 \text{ for any } g \in L, g \neq 0.$$

*Proof.* Lenstra, Lenstra and Lovász [6]. □

**Definition 28.** We define the nearest integer to  $x \in \mathbb{R}$  by  $\lceil x \rceil = \lceil x - \frac{1}{2} \rceil$ : the smallest integer  $\geq x - \frac{1}{2}$ . (In  $\lceil x \rceil$  note the top hook on the left and the bottom hook on the right.)

**Remark 29.** The original LLL algorithm for lattice basis reduction (from [6], here rewritten without “goto” statements) appears in Figure 2. Step (2) computes the Gram-Schmidt orthogonalization of the input vectors. Procedure **reduce** makes  $c_k$  almost orthogonal to  $c_\ell$  and then updates the Gram-Schmidt data. Procedure **exchange** transposes  $c_{k-1}$  and  $c_k$  and then updates the Gram-Schmidt data.

**Example 30.** If we apply the LLL algorithm with  $\alpha = 1$  to the last five rows of the matrix  $U$  of Example 24, then (after 31 calls to **reduce** and **exchange**) we obtain the reduced basis formed by the rows of this matrix:

$$\begin{bmatrix} -3 & 1 & 3 & 0 & 7 & -1 & -1 & -5 & 2 & 1 \\ -3 & 4 & -7 & 10 & -3 & 0 & -1 & -2 & -1 & 3 \\ -4 & -2 & -5 & -4 & 8 & -6 & 0 & 7 & -4 & 7 \\ -8 & 0 & 7 & 0 & -10 & -2 & -5 & 5 & 4 & 1 \\ 9 & -13 & 4 & 6 & -6 & -1 & 1 & -7 & 3 & 5 \end{bmatrix}$$

The square-lengths of these vectors are 100, 198, 275, 284, 423: the longest reduced vector is shorter than the shortest original vector.

**Remark 31.** In this paper the nullspace of the matrix  $A$  has the structure of a module over the symmetric group  $S_k$  since the nullspace vectors represent homogeneous multilinear polynomial identities of degree  $k$ . We reduce the number of identities by considering a set of module generators instead of a complete basis. Our algorithm for this process appears in Figure 3.

#### 4. The fourth family of trilinear operations

All computations in the rest of this paper were done with Maple 11 on an IBM ThinkCentre M55 Tower 8811V2D with Intel Core 2 CPU 6700 at 2.66 GHz and 3 GB of memory.

We first consider the case  $q = \infty$ . The expansion matrix  $E$  has size  $120 \times 160$ ; each column contains 16 nonzero entries; the absolute values of these nonzero entries belong to  $\{1, 2, 4\}$ . The row canonical form of  $E$  has  $r = 106$  nonzero rows, so the nullspace lattice has rank 54. We can extract an integral basis for the nullspace in the canonical way: set the free variables equal to the standard basis vectors in  $\mathbb{Q}^{54}$ , solve for the leading variables, clear denominators, and cancel common factors. This gives vectors whose square-lengths are described in the following table:

number of digits	1	2	3	4	5	6	7	8	9	10	11	12	13
number of vectors	—	1	—	1	1	3	4	2	13	14	4	7	4

Recall however that these vectors do not necessarily form a basis of the nullspace lattice.

Using the algorithm of Figure 1 to compute  $H$  and  $U$  for  $E^t$  takes 53 seconds and uses 107 operations of type 1 (negate a row), 248 of type 2 (exchange two rows), and 21810 of type 3 (add a multiple of one row to another row). The largest integer occurring as an entry of  $H$  has 317 digits. For the first 106 rows of  $U$ , the square-lengths have between 28 and 658 digits. For the last 54 rows (giving a basis of the nullspace lattice by Lemma 20), the square-lengths have between 25 and 30 digits; at this point the results are worse than those obtained from the row canonical form of the expansion matrix.

For the Gram-Schmidt orthogonal basis vectors computed during the initialization of the LLL algorithm, the largest integer occurring in the numerators and denominators of the square-lengths has 102 digits.

We now list the square-lengths of the reduced basis vectors produced by the LLL algorithm with the values  $\alpha = 3/4$ ,  $\alpha = 9/10$ ,  $\alpha = 99/100$  and  $\alpha = 1$ . These lists are sorted by increasing square-length: the output of the LLL algorithm is an  $\alpha$ -reduced basis, which in general is not sorted this way. For  $\alpha = 3/4$  (with  $q = \infty$ ), the sorted square-lengths of the reduced vectors are

132	174	202	202	206	210	222	236	242	246	246	252
254	260	262	268	276	280	282	286	290	290	290	290
296	300	300	304	308	310	316	316	324	326	326	328
328	330	332	354	358	358	366	368	382	402	410	416
428	452	498	530	550	584						

For  $\alpha = 9/10$  (with  $q = \infty$ ), the sorted square-lengths are

74	90	90	102	110	112	124	126	128	130	130	130
132	134	138	140	142	148	148	148	148	150	152	152
152	156	158	158	160	160	162	164	166	166	168	170
172	172	174	174	176	180	186	188	188	194	200	202
228	228	262	262	272	290						

For  $\alpha = 99/100$  (with  $q = \infty$ ), the sorted square-lengths are

24	24	24	24	24	30	30	30	30	36	36	36
40	40	40	40	40	42	44	44	44	44	46	48
48	50	50	52	52	52	54	54	54	54	54	54
58	60	60	60	60	60	62	66	70	72	78	82
86	98	162	162	170	192						

For  $\alpha = 1$  (with  $q = \infty$ ), the sorted square-lengths are

24	24	24	24	24	30	30	30	30	30	36	36
36	36	40	40	40	40	40	40	42	42	44	44
48	48	50	50	50	52	52	54	54	58	58	60
60	62	68	68	68	70	72	78	80	80	82	84
90	90	160	160	162	162						

These results are much better than those obtained from the row canonical form of the expansion matrix. All 54 vectors now have square-length with  $\leq 3$  digits. Only one vector obtained from the row canonical form had such a small square-length.

The following table summarizes our results. Columns  $xx$  and  $xxx$  give the number of basis vectors whose square-lengths have 2 and 3 digits respectively. The next four columns give the square-lengths of the shortest and longest vectors, and the number of calls to **reduce** and **exchange**. The last column gives the computation time in minutes and seconds:

$\alpha$	$xx$	$xxx$	min	max	reduce	exchange	time
3/4	—	54	132	584	40657	5556	3:29
9/10	3	51	74	290	58377	10209	6:13
99/100	50	4	24	192	94079	19446	11:40
1	50	4	24	162	96519	20585	12:30

Increasing  $\alpha$  from 3/4 to 1 made the square-length of the shortest (respectively longest) vector decrease to  $\approx 18.18\%$  (respectively  $\approx 27.74\%$ ) of its original value, at the cost of increasing the computation time by a factor of  $\approx 3.57$ .

We next extract a set of module generators from the sorted list of reduced basis vectors for  $\alpha = 1$ . We say that one identity is “simpler” than a second if the square-length of its coefficient vector is less than that of the second.

**Theorem 32.** *For the operation  $[a, b, c]_\infty = abc + acb - bac + 2bca$ , the simplest identity in degree 5 (relative to lattice basis reduction with  $\alpha = 1$ ) is*

$$\begin{aligned}
J_\infty = & [[abc]de] - [[abe]dc] + [[acb]de] - [[aeb]dc] - [[bac]de] + [[bae]dc] \\
& - [[bca]de] + [[bea]dc] - [[cde]ab] + [[cde]ba] - [a[cde]b] + [b[cde]a] \\
& + [c[abd]e] + [c[abe]d] + [c[adb]e] + [c[aeb]d] - [c[bad]e] - [c[bae]d] \\
& - [c[bda]e] - [c[bea]d] + [d[abe]c] + [d[aeb]c] - [d[bae]c] - [d[bea]c].
\end{aligned}$$

The simplest identity which does not follow from  $J_\infty$  is

$$K_\infty = [[abd]ce] - [[abe]cd] + [[acd]be] - [[ace]bd] + [[bad]ce] - [[bae]cd]$$

$$\begin{aligned}
& + [[bcd]ae] - [[bce]ad] + [[cad]be] - [[cae]bd] + [[cbd]ae] - [[cbe]ad] \\
& + [a[bcd]e] - [a[bce]d] + [a[cbd]e] - [a[cbe]d] + [b[acd]e] - [b[ace]d] \\
& + [b[acd]e] - [b[cae]d] + [c[abd]e] - [c[abe]d] + [c[bad]e] - [c[bae]d].
\end{aligned}$$

The simplest identity which does not follow from  $J_\infty, K_\infty$  is

$$\begin{aligned}
L_\infty = & [[acb]ed] + [[adb]ce] + [[adc]eb] + [[aeb]dc] + [[aec]bd] + [[aed]cb] \\
& + [[bac]de] - [[bac]ed] - [[bad]ce] + [[bad]ec] + [[bae]cd] - [[bae]dc] \\
& + [[bca]ed] + [[bda]ce] + [[bea]dc] + [[cad]be] - [[cad]eb] - [[cae]bd] \\
& + [[cae]db] + [[cda]eb] + [[cea]bd] + [[dae]bc] - [[dae]cb] + [[dea]cb] \\
& - [b[acd]e] - [b[ade]c] - [b[aec]d] - [c[abe]d] - [c[adb]e] - [c[aed]b] \\
& - [d[abc]e] - [d[ace]b] - [d[aeb]c] - [e[abd]c] - [e[acb]d] - [e[adc]b].
\end{aligned}$$

The simplest identity which does not follow from  $J_\infty, K_\infty, L_\infty$  is

$$\begin{aligned}
M_\infty = & [[abd]ce] - [[abd]ec] + [[acd]eb] + [[adb]ec] - [[ade]cb] + [[aed]cb] \\
& + [[bad]ce] + [[bce]da] + 2[[bda]ec] - [[bec]da] + [[cad]eb] - [[ceb]ad] \\
& - [[ceb]da] + 2[[dea]cb] - [a[ceb]d] - [c[adb]e] + 2[c[aed]b] - [c[bad]e] \\
& - 2[c[bda]e] - [c[dae]b] + [c[dea]b] + [d[bce]a] - [d[bec]a] - [d[ceb]a] \\
& - [e[acd]b] - [e[adb]c] + [e[adc]b] - [e[bad]c] - 2[e[bda]c] + 2[e[cda]b].
\end{aligned}$$

The simplest identity which does not follow from  $J_\infty, K_\infty, L_\infty, M_\infty$  is

$$\begin{aligned}
N_\infty = & [[abc]ed] - [[abe]cd] - [[acb]de] - [[acb]ed] + [[ace]bd] - [[aeb]dc] \\
& - [[aec]bd] - [[aec]db] - [[bac]ed] + [[bae]cd] - [[bca]de] - [[bce]ad] \\
& - [[bea]cd] - [[bea]dc] - [[bec]da] - [[cae]bd] + [[cbe]ad] - [[cea]db] \\
& - [[ceb]ad] - [[ceb]da] + 2[a[bce]d] - 2[a[cbe]d] + 2[a[ceb]d] - 2[b[ace]d] \\
& + 2[b[aec]d] + 2[b[cae]d] + 2[c[abe]d] - 2[c[bae]d] + 2[c[bea]d] - 3[d[abc]e] \\
& + 3[d[abe]c] + 2[d[acb]e] - 3[d[ace]b] - [d[aeb]c] + 2[d[aec]b] + 3[d[bac]e] \\
& - 3[d[bae]c] - [d[bca]e] + 3[d[bce]a] + 2[d[bea]c] - [d[bec]a] + 3[d[cae]b] \\
& - 3[d[cbe]a] - [d[cea]b] + 2[d[ceb]a] - 2[e[abc]d] + 2[e[acb]d] + 2[e[bac]d]
\end{aligned}$$

These five identities imply all the identities in degree 5 for  $[a, b, c]_\infty$ . Identities  $J_\infty, M_\infty, N_\infty$  are independent (no two imply the other) and imply identities  $K_\infty, L_\infty$ .

*Proof.* The algorithm of Figure 3 produces these five generators. Further computations with the same algorithm establish the final claim.  $\square$

The computational proofs for the remaining special values of  $q$  are very similar to the proof of Theorem 32. The following table summarizes our results; in the LLL algorithm, we use  $\alpha = 1$ :

$q$	$xx$	$xxx$	min	max	reduce	exchange	time
$\infty$	50	4	24	162	96519	20585	12:30
0	48	1	16	114	169928	35960	19:16
1	49	–	16	86	42004	10997	9:18
–1	48	1	16	110	11531	4049	4:51
2	45	4	16	120	111014	26100	16:01
1/2	54	–	12	34	203493	38378	25:01

**Definition 33.** We consider the following polynomial:

$$\begin{aligned}
I = & [[acb]de] + [[adb]ce] + [[adc]be] + [[bca]de] + [[bda]ce] + [[bdc]ae] \\
& + [[cda]be] + [[cdb]ae] - [a[bd]c]e] - [a[cd]b]e] - [b[ad]c]e] - [b[ca]d]e] \\
& - [c[ab]d]e] - [c[ba]d]e] - [d[abc]e] - [d[bca]e].
\end{aligned}$$

**Lemma 34.** *The identity  $I \equiv 0$  is satisfied by the operation  $[a, b, c]_q$  for all  $q \in \mathbb{Q}$ , but is not satisfied by the operation  $[a, b, c]_\infty$ .*

*Proof.* This is a straightforward computation using Examples 14 and 15, and the analogous expansions for the second association type. For  $[a, b, c]_\infty$  the polynomial  $I$  expands to

$$\begin{aligned}
& - abced - abdec - acbed - acdeb - adbec - adceb + aebcd + aebdc \\
& + aecbd + aecdb + aedbc + aedcb - baced - badec - bcaed - bcdea \\
& - bdaec - bdcea + beacd + beadc + becad + becda + bedac + bedca \\
& - cabed - cadeb - cbaed - cbdea - cdaeb - cdbea + ceabd + ceadb \\
& + cebad + cebda + cedab + cedba - dabec - daceb - dbaec - dbcea \\
& - dcaeb - dcbea + deabc + deacb + debac + debca + decab + decba.
\end{aligned}$$

For  $[a, b, c]_q$  the polynomial  $I$  expands to 0. □

**Theorem 35.** *For the operation  $[a, b, c]_0 = 2abc + bac + cab - cba$ , the simplest identity in degree 5 (relative to  $\alpha = 1$ ) is the identity  $I$  of Definition 33. The simplest identity which does not follow from  $I$  is*

$$\begin{aligned}
J_0 = & [[abc]de] - [[abd]ce] - [[acb]de] + [[acd]be] - [[adc]be] - [[bac]de] \\
& + [[bad]ce] - [[bcd]ae] - [[bda]ce] - [[cad]be] + [[cbd]ae] - [[cdb]ae] \\
& - [a[bcd]e] + [a[bdc]e] + [a[cbd]e] + [b[acd]e] - [b[cad]e] + [b[cda]e] \\
& - [c[abd]e] + [c[adb]e] + [c[bad]e] + [d[abc]e] - [d[bac]e] + [d[bca]e].
\end{aligned}$$

*The simplest identity which does not follow from  $I$ ,  $J_0$  is*

$$\begin{aligned}
K_0 = & [[abe]cd] + [[acb]de] + [[adc]be] + [[ade]cb] - [[bae]dc] + [[bca]de] \\
& - [[bce]da] + [[cbe]ad] + [[cda]be] + [[cde]ab] - [[dae]bc] - [[dce]ba] \\
& + [a[bce]d] - [a[bdc]e] - [a[cbe]d] - [a[cd]b]e] - [a[cde]b] + [a[dce]b] \\
& - [b[ade]c] - [b[cde]a] + [b[dae]c] + [b[dce]a] - [c[abe]d] - [c[adb]e]
\end{aligned}$$

$$\begin{aligned}
& - [c[ade]b] + [c[bae]d] - [c[bda]e] + [c[dae]b] - [d[abe]c] + [d[bae]c] \\
& + [d[bce]a] - [d[cbe]a].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_0, K_0$  is

$$\begin{aligned}
L_0 = & [[abc]de] - [[abc]ed] - [[abd]ce] + [[abd]ec] + [[abe]cd] - [[abe]dc] \\
& + [[acb]ed] + [[adb]ce] + [[aeb]dc] + [[bca]ed] + [[bda]ce] + [[bdc]ea] \\
& + [[bea]dc] + [[bec]ad] + [[bed]ca] + [[cbd]ae] - [[cbd]ea] - [[cbe]ad] \\
& + [[cbe]da] + [[cdb]ea] + [[ceb]ad] + [[dbe]ac] - [[dbe]ca] + [[deb]ca] \\
& - [a[bcd]e] - [a[bde]c] - [a[bec]d] - [c[bae]d] - [c[bda]e] - [c[bed]a] \\
& - [d[bac]e] - [d[bce]a] - [d[bea]c] - [e[bad]c] - [e[bca]d] - [e[bd]c]a].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_0, K_0, L_0$  is

$$\begin{aligned}
M_0 = & [[abc]de] + [[abe]cd] - [[abe]dc] + [[acb]de] - [[adb]ce] + 2[[adc]be] \\
& - [[ade]bc] - [[bae]cd] - [[bca]de] - 2[[cad]be] + [[cbd]ae] + [[cbe]ad] \\
& + [[cbe]da] + [[cda]be] + [[cde]ba] - [[dae]bc] + [[dce]ab] - [[dce]ba] \\
& + [a[bdc]e] - 2[a[cbd]e] - 2[a[cbe]d] + [a[cdb]e] - [a[cde]b] + [b[ade]c] \\
& + [b[ca]d]e - [b[cda]e] - [b[cde]a] + [b[dae]c] + [c[ade]b] + [c[bae]d] \\
& - 2[c[bda]e] + [c[dae]b] + [d[abc]e] - [d[acb]e] + [d[bae]c] - 2[d[cbe]a].
\end{aligned}$$

These five identities imply all the identities in degree 5 for  $[a, b, c]_0$ . Identities  $J_0, M_0$  are independent (neither implies the other) and imply identities  $I, K_0, L_0$ .

**Theorem 36.** For the operation  $[a, b, c]_1 = 2abc + acb + bca - cba$ , the simplest identity in degree 5 (relative to  $\alpha = 1$ ) is the identity  $I$  of Definition 33. The simplest identity which does not follow from  $I$  is

$$\begin{aligned}
J_1 = & [[abc]de] + [[abd]ce] - [[acb]ed] - [[ace]bd] - [[adb]ec] - [[ade]bc] \\
& + [[aec]db] + [[aed]cb] + [[bdc]ea] + [[cdb]ea] + [[ced]ba] + [[dec]ba] \\
& - [a[bdc]e] + [a[bec]d] + [a[bed]c] - [a[cdb]e] + [a[ceb]d] - [a[ced]b] \\
& + [a[deb]c] - [a[dec]b] - [b[ced]a] - [b[dec]a] - [e[bd]c]a - [e[cdb]a].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_1$  is

$$\begin{aligned}
K_1 = & [[abc]de] - [[abc]ed] - [[abd]ce] + [[abd]ec] + [[abe]cd] - [[abe]dc] \\
& + [[acb]ed] + [[adb]ce] + [[aeb]dc] + [[bca]ed] + [[bda]ce] + [[bdc]ea] \\
& + [[bea]dc] + [[bec]ad] + [[bed]ca] + [[cbd]ae] - [[cbd]ea] - [[cbe]ad] \\
& + [[cbe]da] + [[cdb]ea] + [[ceb]ad] + [[dbe]ac] - [[dbe]ca] + [[deb]ca] \\
& - [a[bcd]e] - [a[bde]c] - [a[bec]d] - [c[bae]d] - [c[bda]e] - [c[bed]a] \\
& - [d[bac]e] - [d[bce]a] - [d[bea]c] - [e[bad]c] - [e[bca]d] - [e[bd]c]a].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_1, K_1$  is

$$\begin{aligned}
L_1 = & [[acd]eb] + [[ace]db] + [[ade]cb] + [[bac]de] + [[bac]ed] + [[bad]ce] \\
& + [[bad]ec] + [[bae]cd] + [[bae]dc] - [[bcd]ae] - [[bce]ad] - [[bde]ac] \\
& - [[cda]eb] + [[cdb]ae] - [[cea]db] + [[ceb]ad] + [[ced]ab] - [[dea]cb] \\
& + [[deb]ac] + [[dec]ab] - [a[bdc]e] - [a[bec]d] - [a[bed]c] - [a[cdb]e] \\
& - [a[ceb]d] - [a[ced]b] - [a[deb]c] - [a[dec]b] - [b[acd]e] - [b[ace]d] \\
& - [b[ade]c] + [b[cda]e] + [b[cea]d] + [b[dea]c] + [c[abd]e] + [c[abe]d] \\
& - [c[bda]e] - [c[bea]d] + [d[abc]e] + [d[abe]c] - [d[bca]e] - [d[bea]c] \\
& + [e[abc]d] + [e[abd]c] - [e[bca]d] - [e[bda]c].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_1, K_1, L_1$  is

$$\begin{aligned}
M_1 = & 2[[abc]de] - [[acb]de] + [[adb]ec] - [[aeb]dc] - [[bac]de] - [[bad]ec] \\
& - [[bca]de] - [[bda]ec] - [[bed]ac] + [[cad]be] + [[cad]eb] + [[cae]bd] \\
& - [[cbd]ae] - [[cbe]ad] + [[cdb]ea] - [[cde]ab] + 2[[cde]ba] - [[cea]db] \\
& - [[ceb]ad] - [[dae]bc] + 2[[dbe]ac] + [a[bed]c] - 2[a[dbe]c] + [b[dae]c] \\
& - [c[adb]e] + [c[aed]b] + 2[c[bad]e] + [c[bea]d] - [c[dae]b] - [c[dbe]a] \\
& + [c[dea]b] - 2[c[deb]a] + [d[aeb]c] - [e[adb]c] + [e[bad]c] + [e[bda]c].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_1, K_1, L_1, M_1$  is

$$\begin{aligned}
N_1 = & [[abc]de] - [[abd]ce] + [[acd]be] + [[adb]ce] - [[bac]de] + [[bad]ce] \\
& + [[bca]de] - [[bcd]ae] + [[bdc]ae] - [[cad]be] + [[cbd]ae] + [[cda]be] \\
& + [a[bcd]e] - [a[bdc]e] - [a[cbd]e] - [b[acd]e] + [b[cad]e] - [b[cda]e] \\
& + [c[abd]e] - [c[adb]e] - [c[bad]e] - [d[abc]e] + [d[bac]e] - [d[bca]e] \\
& - 2[e[abc]d] + 2[e[abd]c] + [e[acb]d] - 2[e[acd]b] - [e[adb]c] + [e[adc]b] \\
& + 2[e[bac]d] - 2[e[bad]c] - [e[bca]d] + 2[e[bcd]a] + [e[bda]c] - [e[bdc]a] \\
& + 2[e[cad]b] - 2[e[cbd]a] - [e[cda]b] + [e[cdb]a].
\end{aligned}$$

These six identities imply all the identities in degree 5 for  $[a, b, c]_1$ . Identities  $M_1, N_1$  are independent (neither implies the other) and imply identities  $I, J_1, K_1, L_1$ .

**Theorem 37.** For the operation  $[a, b, c]_{-1} = 2abc - acb + 2bac - bca + 2cab - cba$ , the simplest identity in degree 5 (relative to  $\alpha = 1$ ) is the identity  $I$ . The simplest identity which does not follow from  $I$  is

$$\begin{aligned}
J_{-1} = & [[abc]de] - [[abc]ed] - [[acb]de] + [[acb]ed] - [[ade]bc] + [[ade]cb] \\
& + [[aed]bc] - [[aed]cb] - [[bec]da] - [[cdb]ea] - [[ced]ba] - [[dbe]ca] \\
& + [[dce]ba] - [[dec]ba] + [b[ced]a] - [b[dce]a] + [b[dec]a] + [c[dbe]a] \\
& + [d[bec]a] + [e[cdb]a].
\end{aligned}$$

The simplest identity which does not follow from  $I, J_{-1}$  is

$$\begin{aligned} K_{-1} = & [[abc]de] - [[abe]cd] + [[abe]dc] + [[ace]bd] - [[ace]db] + [[adb]ce] \\ & - [[bac]de] + [[bae]cd] - [[bae]dc] + [[bca]de] - [[bce]ad] + [[bce]da] \\ & + [[bdc]ae] - [[cae]bd] + [[cae]db] + [[cbe]ad] - [[cbe]da] + [[cda]be] \\ & - [a[bdc]e] - [b[cda]e] - [c[adb]e] - [d[abc]e] + [d[bac]e] - [d[bca]e]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_{-1}, K_{-1}$  is

$$\begin{aligned} L_{-1} = & [[abc]de] - [[abc]ed] + [[abe]cd] - [[abe]dc] + [[acb]ed] + [[adb]ce] \\ & + [[aeb]dc] + [[bac]ed] - [[bad]ce] + [[bad]ec] - [[bae]cd] + [[bcd]ae] \\ & - [[bcd]ea] + [[bce]ad] + [[bda]ce] + [[bdc]ea] + [[bea]cd] + [[bea]dc] \\ & + [[bed]ca] - [[cbe]ad] + [[cbe]da] + [[cdb]ea] + [[ceb]ad] + [[deb]ac] \\ & - [a[bcd]e] - [a[bce]d] - [a[bde]c] - [c[bda]e] - [c[bea]d] - [c[bed]a] \\ & - [d[bac]e] - [d[bce]a] - [d[bea]c] - [e[bac]d] - [e[bad]c] - [e[bdc]a]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_{-1}, K_{-1}, L_{-1}$  is

$$\begin{aligned} M_{-1} = & [[abc]ed] - [[abd]ec] - [[abe]cd] + [[ade]cb] + [[aeb]cd] - [[aed]cb] \\ & + [[bad]ec] + [[bcd]ae] - [[bde]ac] + [[bde]ca] + [[bea]cd] + [[bec]ad] \\ & - [[cae]bd] + [[cae]db] + [[cbe]ad] - [[cbe]da] + [[cdb]ea] + [[ceb]ad] \\ & + [[ced]ba] + [[dae]bc] - [[dae]cb] - [[dea]cb] + [[deb]ca] + [[dec]ab] \\ & - [a[bce]d] + [a[bde]c] - [a[bec]d] - [a[bed]c] - [a[cdb]e] - [a[ceb]d] \\ & + [a[ced]b] - [a[dbe]c] - [a[deb]c] + [a[dec]b] + [b[acd]e] + [b[ace]d] \\ & - [b[ade]c] - [b[aec]d] - [b[cae]d] - [b[cda]e] - [b[cea]d] + [b[ced]a] \\ & + [b[dec]a] + [c[abd]e] + [c[abe]d] - [c[ade]b] + [c[aeb]d] - [c[bad]e] \\ & + [c[dae]b] - [c[dbe]a] - [c[dea]b] - [c[deb]a] - [d[abc]e] + [d[abe]c] \\ & + [d[acb]e] + [d[ace]b] + [d[aeb]c] - [d[bce]a] + [d[bea]c] - [d[bec]a] \\ & - [d[cae]b] + [d[cbe]a] - [d[cea]b] - [d[ceb]a] + [e[acd]b] + [e[adb]c] \\ & - [e[bac]d] - [e[bad]c] - [e[cda]b] - [e[cdb]a]. \end{aligned}$$

These five identities imply all the identities in degree 5 for  $[a, b, c]_{-1}$ . Identity  $M_{-1}$  implies identities  $I, J_{-1}, K_{-1}, L_{-1}$ .

**Theorem 38.** For the operation  $[a, b, c]_2 = 2abc + 2acb - bac + 2bca - cab - cba$ , the simplest identity in degree 5 (relative to  $\alpha = 1$ ) is the identity  $I$ . The simplest identity which does not follow from  $I$  is

$$\begin{aligned} J_2 = & [[abc]de] - [[abc]ed] - [[aeb]dc] - [[bac]de] + [[bac]ed] - [[bda]ec] \\ & - [[bed]ac] - [[cde]ab] + [[cde]ba] + [[ced]ab] - [[ced]ba] - [[dae]bc] \\ & + [[dbe]ac] - [[deb]ac] + [a[bed]c] - [a[dbe]c] + [a[deb]c] + [b[dae]c] \\ & + [d[aeb]c] + [e[bda]c]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_2$  is

$$\begin{aligned} K_2 = & [[abc]de] - [[abc]ed] - [[bac]de] + [[bac]ed] + [[bad]ec] - [[bae]dc] \\ & - [[bda]ec] + [[bde]ac] + [[bea]dc] - [[bed]ac] + [[cbd]ae] - [[cbd]ea] \\ & - [[cbe]ad] + [[cbe]da] - [[cdb]ae] + [[cdb]ea] + [[ceb]ad] - [[ceb]da] \\ & - [a[bde]c] + [a[bed]c] + [d[bae]c] - [d[bea]c] - [e[bad]c] + [e[bda]c]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_2, K_2$  is

$$\begin{aligned} L_2 = & [[abd]ce] - [[abd]ec] - [[abe]cd] + [[abe]dc] + [[acb]de] + [[adb]ec] \\ & + [[aeb]cd] - [[bac]de] + [[bac]ed] + [[bad]ec] - [[bae]dc] + [[bca]de] \\ & + [[bdc]ae] + [[bde]ac] + [[bea]cd] + [[bea]dc] + [[bec]da] + [[cdb]ea] \\ & + [[ceb]ad] - [[dbe]ac] + [[dbe]ca] + [[deb]ac] - [a[bce]d] - [a[bdc]e] \\ & - [a[bde]c] - [c[bad]e] - [c[bde]a] - [c[bea]d] - [d[bca]e] - [d[bea]c] \\ & - [d[bec]a] - [e[bac]d] - [e[bad]c] - [e[bcd]a]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_2, K_2, L_2$  is

$$\begin{aligned} M_2 = & [[abc]de] - [[abd]ce] - [[abe]cd] + [[abe]dc] - [[acb]de] + [[acd]be] \\ & + [[ace]bd] - [[ace]db] + [[adb]ce] - [[adc]be] - [[ade]bc] + [[ade]cb] \\ & - [[aeb]cd] + [[aeb]dc] + [[aec]bd] - [[aec]db] - [[aed]bc] + [[aed]cb] \\ & + [[bcd]ea] - [[bdc]ea] - [[bea]cd] + [[bea]dc] - [[bec]da] - [[cbd]ea] \\ & + [[cea]bd] - [[cea]db] - [[ced]ba] - [[dea]bc] + [[dea]cb] - [[deb]ca] \\ & + [b[acd]e] - [b[adc]e] + [b[ced]a] - [c[abd]e] + [c[adb]e] + [c[deb]a] \\ & + [d[abc]e] - [d[acb]e] + [d[bec]a] + [e[abc]d] - [e[abd]c] - [e[acb]d] \\ & + [e[acd]b] + [e[adb]c] - [e[adc]b] - [e[bcd]a] + [e[bdc]a] + [e[cbd]a]. \end{aligned}$$

The simplest identity which does not follow from  $I, J_2, K_2, L_2, M_2$  is

$$\begin{aligned} N_2 = & [[abd]ec] - [[acd]eb] - [[ade]cb] - [[aec]bd] - [[bac]ed] - [[bad]ec] \\ & + [[bae]cd] + [[bca]ed] + [[bdc]ea] - [[bea]cd] + [[bec]ad] + [[cae]db] \\ & - [[cbd]ae] + [[cbd]ea] - [[cbe]da] + [[cda]be] - [[cda]eb] - [[cea]bd] \\ & + [[ceb]ad] - [[ced]ba] - [[dea]bc] - [[dec]ab] - [a[bcd]e] - [a[bce]d] \\ & - [a[bdc]e] - [a[bde]c] - [a[bec]d] + [a[cbd]e] - [a[cdb]e] + 2[a[ced]b] \\ & + [a[deb]c] + 2[a[dec]b] - [b[cad]e] - [b[cea]d] + 2[b[ced]a] + [b[dea]c] \\ & + 2[b[dec]a] - [c[bde]a] + [c[dea]b] + [c[deb]a] + [d[abe]c] + 2[d[acb]e] \\ & - [d[bae]c] + [d[bca]e] - [d[bec]a] - [d[cbe]a] - [d[cea]b] + 2[e[acb]d] \\ & + [e[acd]b] - [e[adc]b] + [e[bad]c] + [e[bca]d] - [e[bda]c] - [e[bdc]a] \\ & - [e[cad]b] - [e[cdb]a]. \end{aligned}$$

These six identities imply all the identities in degree 5 for  $[a, b, c]_2$ . Identities  $I$  and  $N_2$  are independent (neither implies the other) and imply identities  $J_2, K_2, L_2, M_2$ .

In the final case, we consider the operation  $2[a, b, c]_{1/2}$  instead of  $[a, b, c]_{1/2}$  to obtain integral entries in the expansion matrix. These two operations clearly satisfy the same polynomial identities.

**Theorem 39.** *For the operation  $2[a, b, c]_{1/2} = 4abc + acb + bac + bca + cab - 2cba$ , the simplest identity in degree 5 (relative  $\alpha = 1$ ) is*

$$J_{1/2} = [[abc]de] + [[adb]ce] - [[bad]ce] + [[bcd]ae] + [[bda]ce] + [[cda]be] \\ - [a[bcd]e] - [b[cda]e] - [c[adb]e] + [c[bad]e] - [c[bda]e] - [d[abc]e].$$

The simplest identity which does not follow from  $J_{1/2}$  is

$$K_{1/2} = [[abe]cd] - [[acd]be] - [[acd]eb] - [[bea]cd] + [[bed]ca] - [[dbe]ca] \\ - [a[bec]d] - [a[bed]c] + [a[cbe]d] + [a[dbe]c] + [b[acd]e] - [c[bed]a] \\ + [c[dbe]a] + [e[acd]b].$$

The simplest identity which does not follow from  $J_{1/2}$ ,  $K_{1/2}$  is

$$L_{1/2} = [[abc]de] - [[abd]ce] + [[acd]be] - [[adc]be] - [[bac]de] + [[bad]ce] \\ - [[bcd]ae] + [[bdc]ae] - [e[abc]d] + [e[abd]c] - [e[acd]b] + [e[adc]b] \\ + [e[bac]d] - [e[bad]c] + [e[bcd]a] - [e[bdc]a].$$

These three identities imply all the identities in degree 5 for  $[a, b, c]_2$ , and are independent (no two imply the other).

**Remark 40.** The identity  $I$  of Definition 33 does not appear in Theorem 39, but we easily check using Lemma 5 that

$$I(a, b, c, d, e) = J_{1/2}(a, b, d, c, e) + J_{1/2}(a, c, d, b, e).$$

## 5. The weakly commutative and anticommutative operations

For these operations, the expansion matrix  $E$  has size  $120 \times 250$ ; each column contains 36 nonzero entries; the absolute values of these nonzero entries belong to  $\{1, 5, 25\}$ . The row canonical form of  $E$  has  $r = 109$  nonzero rows, so the nullspace has dimension 141. The square-lengths of the integral basis vectors for the nullspace obtained from the row canonical form have between 8 and 12 digits.

The following table summarizes our results for the weakly commutative operation. Columns  $x$ ,  $xx$ ,  $xxx$ ,  $xxxx$  give the number of basis vectors whose square-lengths have 1, 2, 3, 4 digits respectively. The next four columns give the square-lengths of the shortest and longest vectors, and the number of calls to **reduce** and **exchange**. The last column gives the computation time in minutes and seconds:

$\alpha$	$x$	$xx$	$xxx$	$xxxx$	min	max	reduce	exchange	time
3/4	4	5	22	110	8	2138	55197	4441	9:19
9/10	17	11	113	—	8	380	123369	10446	22:14
99/100	15	11	115	—	8	320	209612	17535	37:35
1	52	89	—	—	8	68	298998	28679	57:41

We achieved especially significant improvement in basis reduction between  $\alpha = 3/4$  and  $\alpha = 9/10$ , and again between  $\alpha = 99/100$  and  $\alpha = 1$ . Increasing  $\alpha$  from  $3/4$  to  $1$  did not improve the shortest vector, but it made the square-length of the longest vector decrease to  $\approx 3.18\%$  of its original value, at the cost of increasing the computation time by a factor of  $\approx 6.18$ . We obtained the following identities.

**Theorem 41.** *Every polynomial identity of degree  $\leq 5$  for the weakly commutative operation follows from these three identities, no two of which imply the other:*

$$\begin{aligned} & [[abc]de] - [[ade]bc] + [[dea]bc] - [a[bde]c] + [a[deb]c] - [ab[cde]] + [ab[dec]] - [de[abc]], \\ & [[abc]de] - [[bcd]ae] + [[cda]be] - [[dab]ce] - [a[bcd]e] + [b[cda]e] - [c[dab]e] + [d[abc]e], \\ & [[bcd]ea] + [[bdc]ea] - [a[bcd]e] - [a[bdc]e] - [b[cde]a] - [b[dce]a] + [ab[cde]] + [ab[dce]]. \end{aligned}$$

**Theorem 42.** *Every polynomial identity of degree  $\leq 5$  for the weakly anti-commutative operation follows these three identities, no two of which imply the other:*

$$\begin{aligned} & [[abc]de] - [[ade]bc] + [[dea]bc] - [a[bde]c] + [a[deb]c] - [ab[cde]] + [ab[dec]] - [de[abc]], \\ & [[abc]de] + [[bcd]ae] + [[cda]be] + [[dab]ce] - [a[bcd]e] - [b[cda]e] - [c[dab]e] - [d[abc]e], \\ & [[bcd]ea] - [[bdc]ea] - [a[bcd]e] + [a[bdc]e] - [b[cde]a] + [b[dce]a] + [ab[cde]] - [ab[dce]]. \end{aligned}$$

**Remark 43.** The first identities are the same in Theorems 41 and 42. The second identities differ only in the sign of the monomials; likewise for the third identities.

## 6. Conclusion

For the fourth family, only two values of the parameter ( $q = \infty, \frac{1}{2}$ ) have a 54-dimensional space of polynomial identities in degree 5. These are also the only values which require three module generators (Theorems 32 and 39). The other four values ( $q = 0, 1, -1, 2$ ) have a 49-dimensional space of identities, and in these cases the identity  $I$  of Definition 33 occurs as the shortest vector (and hence a module generator) in the reduced lattice basis. For  $q = 0, 1, 2$  we require two generators (Theorems 35, 36 and 38), but for  $q = -1$  we require only one (Theorem 37). The case  $q = \frac{1}{2}$  also satisfies  $I$ , but  $I$  does not occur as one of the generators; this is also the only case in which the module generators are independent.

Using lattice basis reduction to simplify the identities has produced results with very small coefficients. The largest coefficient (in absolute value) occurring in our identities is  $\pm 3$ , and this appears only in the last identity for  $q = \infty$ . Identities with maximum coefficient  $\pm 2$  appear for  $q = \infty, 0, 2$  (one identity in each case) and  $q = 1$  (two identities). In all the other identities for the fourth family, all the coefficients are  $\pm 1$ . All the identities for the weakly commutative and anticommutative operations have coefficients  $\pm 1$ .

We checked our results using C programs based on the ideas of Hentzel [5] for processing identities using the representation theory of the symmetric group. For more information about the application of this method to trilinear operations, see Bremner and Peresi [3].

#### *Acknowledgements*

Murray Bremner thanks NSERC for financial support, the University of Saskatchewan for a sabbatical leave from January to June 2008, and the Department of Mathematics at the University of São Paulo for its hospitality during his visit from January to April 2008.

#### **References**

- [1] W. A. Adkins and S. H. Weintraub. *ALGEBRA: AN APPROACH VIA MODULE THEORY*. Springer, Berlin, 1992.
- [2] M. R. Bremner and I. R. Hentzel. *Identities for generalized Lie and Jordan products on totally associative triple systems*. *J. Algebra* 231 (2000) 387–405.
- [3] M. R. Bremner and L. A. Peresi. *Classification of trilinear operations*. *Comm. Algebra* 35 (2007) 2932–2959.
- [4] H. Cohen. *A COURSE IN COMPUTATIONAL ALGEBRAIC NUMBER THEORY*. Springer, Berlin, 1993.
- [5] I. R. Hentzel. *Processing identities by group representation*. *COMPUTERS IN NONASSOCIATIVE RINGS AND ALGEBRAS* (Special Session, 82nd Annual Meeting of the American Mathematical Society, San Antonio, Texas, 1976), Academic Press, New York, 1977, pages 13–40.
- [6] A. K. Lenstra, H. W. Lenstra Jr. and L. Lovász. *Factoring polynomials with rational coefficients*. *Math. Ann.* 261 (1982) 515–534.