Polynomial bound for the nilpotency index
of finitely generated nil algebras

Mátyás Domokos

Polynomial bound for the nilpotency index of finitely generated nil algebras

Mátyás Domokos

Working over an infinite field of positive characteristic, an upper bound is given for the nilpotency index of a finitely generated nil algebra of bounded nil index n in terms of the maximal degree in a minimal homogenous generating system of the ring of simultaneous conjugation invariants of tuples of n-by-n matrices. This is deduced from a result of Zubkov. As a consequence, a recent degree bound due to Derksen and Makam for the generators of the ring of matrix invariants yields an upper bound for the nilpotency index of a finitely generated nil algebra that is polynomial in the number of generators and the nil index. Furthermore, a characteristic free treatment is given to Kuzmin's lower bound for the nilpotency index.

1. Introduction

Throughout this note $\mathbb{F}$ stands for an infinite field of positive characteristic. All vector spaces, tensor products and algebras are taken over $\mathbb{F}$. The results of this paper are valid in arbitrary characteristic, but they are known in characteristic zero (in fact stronger statements hold in characteristic zero, see Formanek [1991], giving in particular an account of relevant works of Razmyslov [1974] and Procesi [1976]).

Write $\mathcal{F}_m := \mathbb{F}\langle x_1, \ldots, x_m \rangle$ for the free associative $\mathbb{F}$-algebra with identity 1 on m generators $x_1, \ldots, x_m$, and let $\mathcal{F}_m^+$ be its ideal generated by $x_1, \ldots, x_m$ (so $\mathcal{F}_m^+$ is the free nonunitary associative algebra of rank m). For a positive integer n denote by $I_{n,m}$ the ideal in $\mathcal{F}_m$ generated by $\{a^n \mid a \in \mathcal{F}_m^+\}$. A theorem of Kaplansky [1946] asserts that if a finitely generated associative algebra satisfies the polynomial identity $x^n = 0$, then it is nilpotent. Equivalently, there exists a positive integer d such that for all $i_1, \ldots, i_d \in \{1, \ldots, m\}$ the monomial $x_{i_1} \cdots x_{i_d}$ belongs to $I_{n,m}$. Denote by $d_{\mathbb{F}}(n, m)$ the minimal such d. In other words, $d_{\mathbb{F}}(n, m)$ is the minimal positive integer d such that all $\mathbb{F}$-algebras that are generated by m elements and satisfy the polynomial identity $x^n = 0$ satisfy also the polynomial identity $y_1 \cdots y_d = 0$. This is a notable quantity of noncommutative ring theory; Jacobson [1945] reduced the Kurosh problem for finitely generated algebraic algebras of bounded degree to the case of nil algebras of bounded degree. We mention also that proving nilpotency of nil rings under various conditions is a natural target for ring theorists, see for example the paper of Guralnick, Small and Zelmanov [2010].

The number $d_{\mathbb{F}}(n, m)$ is tightly connected with a quantity appearing in commutative invariant theory defined as follows. Consider the generic matrices

$$X_r = (x_{ij}(r))_{1 \leq i, j \leq n}, \quad r = 1, \ldots, m.$$

These are elements in the algebra $A^{n \times n}$ of $n \times n$ matrices over the mn^2-variable commutative polynomial algebra $A = \mathbb{F}[x_{ij}(r) \mid 1 \leq i, j \leq n, 1 \leq r \leq m]$. The general linear group $\mathrm{GL}_n(\mathbb{F})$ acts on A via $\mathbb{F}$-algebra automorphisms; for $g \in \mathrm{GL}_n(\mathbb{F})$ we have that $g \cdot x_{ij}(r)$ is the (i, j)-entry of the matrix $g^{-1} X_r g$. Set $R_{n,m} = A^{\mathrm{GL}_n(\mathbb{F})}$, the subalgebra of $\mathrm{GL}_n(\mathbb{F})$-invariants. This is the algebra of polynomial invariants under simultaneous conjugation of m-tuples of $n \times n$ matrices. The polynomial ring A is graded in the standard way, and since the $\mathrm{GL}_n(\mathbb{F})$-action preserves the grading, the subalgebra $R_{n,m}$ is generated by homogeneous elements. Being the algebra of invariants of a reductive group, $R_{n,m}$ is finitely generated by the Hilbert–Nagata theorem (see for example [Newstead 1978]). We write $\beta_{\mathbb{F}}(n, m)$ for the minimal positive integer d such that the $\mathbb{F}$-algebra $R_{n,m}$ is generated by elements of degree at most d. The main result of the present note is the following inequality:

Theorem 1.1. $\qquad\qquad\qquad\qquad d_{\mathbb{F}}(n, m) \leq \beta_{\mathbb{F}}(n, m + 1).$

Remark 1.2. In the reverse direction it was shown in [Domokos 2002, Theorem 3] that for $n \geq 2$ we have

$$\beta_{\mathbb{F}}(n, m) \leq \left\lfloor \frac{n}{2} \right\rfloor d_{\mathbb{F}}(n, m).$$

Theorem 1.1 is derived from a theorem of Zubkov [1996] (for which Lopatin [2013] gave versions and improvements), see Theorem 2.1. Using a result of Ivanyos, Qiao and Subrahmanyam [2017], Derksen and Makam [2017b] found strong bounds on the degrees of invariants defining the null-cone of m-tuples of $n \times n$ matrices under simultaneous conjugation, and derived from this the following upper bound on $\beta_{\mathbb{F}}(n, m)$:

Theorem 1.3 [Derksen and Makam 2017a, Theorem 1.4]. *We have the inequality*

$$\beta_{\mathbb{F}}(n, m) \leq (m + 1)n^4.$$

Given this result Derksen and Makam conjectured [2017a, Conjecture 1.5] that there exists an upper bound on $d_{\mathbb{F}}(n, m)$ that is polynomial in n and m. Combining Theorem 1.1 and Theorem 1.3 we obtain the following affirmative answer to this conjecture:

Corollary 1.4. $\qquad\qquad\qquad\qquad d_{\mathbb{F}}(n, m) \leq (m + 2)n^4.$

Remark 1.5. Corollary 1.4 is a drastic improvement of the earlier known general upper bounds on $d_{\mathbb{F}}(n, m)$:

(1) $d_{\mathbb{F}}(n, m) \leq n^6 m^{n+1}$ by Belov [1992].

(2) $d_{\mathbb{F}}(n, m) \leq \frac{1}{6} n^6 m^n$ by Klein [2000].

(3) $d_{\mathbb{F}}(n, m) \leq 2^{18} m n^{12 \log_3(n) + 28}$ by Belov and Kharitonov [2012].

It is easy to see that $d_{\mathbb{F}}(2, m) \leq m+1$. We note that for the case $n = 3$ exact results on $d_{\mathbb{F}}(3, m)$ were obtained by Lopatin [2005]. Moreover, Lopatin [2012] proved that if $\mathrm{char}(\mathbb{F}) > \frac{n}{2}$ then $d_{\mathbb{F}}(n, m) \leq n^{1+\log_2(3m+2)}$ and $d_{\mathbb{F}}(n, m) \leq 2^{2+n/2}m$.

Remark 1.6. When $\mathrm{char}(\mathbb{F}) > n^2 + 1$, we have $\beta_{\mathbb{F}}(n, m) \leq n^2$. Indeed, the proof presented by Formanek [1986] (following the original arguments of Razmyslov [1974] and Procesi [1976]) for the zero characteristic case of the corresponding inequality goes through without essential changes when $\mathrm{char}(\mathbb{F}) > n^2 + 1$. Thus by Theorem 1.1 we get that $d_{\mathbb{F}}(n, m) \leq n^2$ when $\mathrm{char}(\mathbb{F}) > n^2 + 1$.

In Section 3 we show that the following lower bound for $d_{\mathbb{F}}(n, m)$ due to E. N. Kuzmin [1975] when $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > n$ holds in arbitrary characteristic:

Theorem 1.7. *The monomial $x_2 x_1 x_2 x_1^2 x_2 x_1^3 \cdots x_2 x_1^{n-1}$ is not contained in the ideal $I_{n,2}$. In particular, for $m \geq 2$ we have $d_{\mathbb{F}}(n, m) \geq n(n + 1)/2$.*

Remark 1.8. It is well known that when $0 < \mathrm{char}(\mathbb{F}) \leq n$, the element $x_1 x_2 \cdots x_m$ is not contained in $I_{n,m}$, see for example [Nagata 1952, 5. Remark (I)]. So in this case for $m \geq 2$ we have

$$\max\left\{m + 1, \frac{n(n + 1)}{2}\right\} \leq d_{\mathbb{F}}(n, m) \leq (m + 2)n^4.$$

2. Identities of matrices with forms

The map $x_i \mapsto X_i$ $(i = 1, \ldots, m)$ extends to a unique $\mathbb{F}$-algebra homomorphism $\varphi_1 : \mathcal{F}_m \to A^{n \times n}$. We have $\varphi_1(1) = I$, the $n \times n$ identity matrix. Consider the commutative polynomial algebra

$$\mathcal{P}_{n,m} = \mathbb{F}[s_l(a) \mid a \in \mathcal{F}_m^+, l = 1, \ldots, n]$$

generated by the infinitely many commuting indeterminates $s_l(a)$. Define the $\mathbb{F}$-algebra homomorphism

$$\varphi_2 : \mathcal{P}_{n,m} \to R_{n,m}, \quad \varphi_2(s_l(a)) = \sigma_l(\varphi_1(a)),$$

where for $B \in A^{n \times n}$ we have

$$\det(tI + B) = \sum_{l=0}^{n} t^l \sigma_{n-l}(B),$$

so $\sigma_l(B)$ is the sum of the principal $l \times l$ minors of B. A theorem of Donkin [1992] asserts that φ_2 is surjective onto $R_{n,m}$. Combining φ_1 and φ_2 we get an $\mathbb{F}$-algebra homomorphism

$$\varphi : \mathcal{P}_{n,m} \otimes \mathcal{F}_m \to A^{n \times n}, \quad b \otimes a \mapsto \varphi_2(b)\varphi_1(a).$$

The subalgebra $C_{n,m} = \varphi(\mathcal{P}_{n,m} \otimes \mathcal{F}_m)$ is called the *algebra of matrix concomitants*. It can be interpreted as the algebra of $\mathrm{GL}_n(\mathbb{F})$-equivariant polynomial maps $(\mathbb{F}^{n \times n})^m \to \mathbb{F}^{n \times n}$, where $\mathrm{GL}_n(\mathbb{F})$ acts on $\mathbb{F}^{n \times n}$ by conjugation and on the space $(\mathbb{F}^{n \times n})^m$ of m-tuples of matrices by simultaneous conjugation. For $a \in \mathcal{F}_m^+$

define an element $\chi_n(a)$ in $\mathcal{P}_{n,m} \otimes \mathcal{F}_m$ as follows:

$$\chi_n(a) = \sum_{l=0}^{n} (-1)^l s_l(a) \otimes a^{n-l}$$

(where $s_0(a) = 1$). We need the following result of Zubkov [1996] (see also Lopatin [2013, Theorem 2.4]):

Theorem 2.1 [Zubkov 1996]. *The ideal* $\ker(\varphi)$ *is generated by*

$$\{b \otimes 1, \chi_n(a) \mid b \in \ker(\varphi_2), a \in \mathcal{F}_m^+\}.$$

Remark 2.2. The papers [Zubkov 1996; Lopatin 2013] use different commutative polynomial algebras than our $\mathcal{P}_{n,m}$, however, it is straightforward that Theorem 2.1 is an immediate consequence of the versions stated there. We note that those works give descriptions of the ideal $\ker(\varphi_2)$ as well. A self-contained approach to the theorem of Zubkov can be found in the recent book by De Concini and Procesi [2017].

Denote by $\eta : C_{n,m} \to C_{n,m}/R_{n,m}^+ C_{n,m}$ the natural surjection (ring homomorphism), where $R_{n,m}^+$ is the sum of the positive degree homogeneous components of $R_{n,m}$.

Corollary 2.3. *The kernel of* $\eta \circ \varphi_1$ *is the ideal* $I_{n,m} = (a^n \mid a \in \mathcal{F}_m^+)$ *in* $\mathcal{F}_m$.

Proof. We have $\ker(\eta \circ \varphi_1) = \ker(\eta \circ \varphi) \cap \mathcal{F}_m$ (where we identify $\mathcal{F}_m$ with the subalgebra $1 \otimes \mathcal{F}_m$ in $\mathcal{P}_{n,m} \otimes \mathcal{F}_m$). The ideal $(s_l(a) \otimes 1 \mid a \in \mathcal{F}_m^+, 1 \leq l \leq n)$ is mapped surjectively onto $R_{n,m}^+ C_{n,m}$ by [Donkin 1992]. Therefore we have

$$\ker(\eta \circ \varphi) = \varphi^{-1}(R_{n,m}^+ C_{n,m}) = \ker(\varphi) + (s_l(a) \otimes 1 \mid a \in \mathcal{F}_m^+, 1 \leq l \leq n) = (s_l(a) \otimes 1, 1 \otimes a^n \mid a \in \mathcal{F}_m^+, 1 \leq l \leq n),$$

(the last equality follows from Theorem 2.1 and the fact that $1 \otimes a^n - \chi_n(a)$ belongs to $(s_l(a) \otimes 1 \mid a \in \mathcal{F}_m^+, 1 \leq l \leq n)$). Obviously the ideal $(s_l(a) \otimes 1, 1 \otimes a^n \mid a \in \mathcal{F}_m^+, 1 \leq l \leq n)$ intersects $\mathcal{F}_m$ in $I_{n,m}$. $\square$

Remark 2.4. Corollary 2.3 implies that the relatively free algebra $\mathcal{F}_m/I_{n,m}$ is isomorphic to $C_{n,m}/R_{n,m}^+ C_{n,m}$. When $\operatorname{char}(\mathbb{F}) = 0$, this statement is due to Procesi [1976, Corollary 4.7].

The algebras $R_{n,m}$ and $C_{n,m}$ are $\mathbb{Z}^m$-graded:

$$\deg_m(X_{i_1} \cdots X_{i_d}) = (\alpha_1, \ldots, \alpha_m) \text{ where } \alpha_k = |\{j \mid i_j = k\}|$$

and

$$\deg_m(\sigma_l(X_{i_1} \cdots X_{i_d})) = l \cdot \deg_m(X_{i_1} \cdots X_{i_d}).$$

Proof of Theorem 1.1. Set $d = \beta_{\mathbb{F}}(n, m+1)$. We have to show that $x_{i_1} \cdots x_{i_d} \in I_{n,m}$ for all $i_1, \ldots, i_d \in \{1, \ldots, m\}$. Recall that by [Donkin 1992] the algebra $R_{n,m+1}$ is generated by the elements $\sigma_l(W)$, where W is a word in $X_1, \ldots, X_{m+1}$, and $l \in \{1, \ldots, n\}$. The total degree of the element $\operatorname{Tr}(X_{i_1} \cdots X_{i_d} X_{m+1}) \in R_{n,m+1}$ is strictly greater than $\beta_{\mathbb{F}}(n, m+1)$, whence we have a relation

$$\operatorname{Tr}(X_{i_1} \cdots X_{i_d} X_{m+1}) = \sum_{\lambda \in \Lambda} a_\lambda f_\lambda, \tag{1}$$

where Λ is a finite index set, $a_\lambda \in \mathbb{F}$, and each $f_\lambda \in R_{n,m+1}$ is a product $f_\lambda = \sigma_{l_1}(W_1) \cdots \sigma_{l_r}(W_r)$ with $r \geq 2$ and $W_1, \ldots, W_r$ nonempty words in $X_1, \ldots, X_{m+1}$. The $\mathbb{Z}^{m+1}$-multidegree of $\mathrm{Tr}(X_{i_1} \cdots X_{i_d} X_{m+1})$ is

$$\deg_{m+1}(\mathrm{Tr}(X_{i_1} \cdots X_{i_d} X_{m+1})) = (\deg_m(\mathrm{Tr}(X_{i_1} \cdots X_{i_d})), 1).$$

The terms f_λ are all $\mathbb{Z}^{m+1}$-homogeneous, whence we may assume that each has the above $\mathbb{Z}^{m+1}$-degree (since the other possible terms on the right-hand side of (1) must cancel each other). It follows that for each f_λ exactly one of its factors $\sigma_{l_1}(W_1), \ldots, \sigma_{l_r}(W_r)$ has $\mathbb{Z}^{m+1}$-degree of the form $(\alpha_1, \ldots, \alpha_m, 1)$, say this is $\sigma_{l_1}(W_1)$, and the remaining factors have $\mathbb{Z}^{m+1}$-degree of the form $(\gamma_1, \ldots, \gamma_m, 0)$. Necessarily we have $l_1 = 1$ and so $\sigma_{l_1}(W_1) = \mathrm{Tr}(X_{m+1}Z)$ for some (possibly empty) word Z in $X_1, \ldots, X_m$, and $W_2, \ldots, W_r$ are nonempty words in $X_1, \ldots, X_m$. Set

$$g_\lambda = \sigma_{l_2}(W_2) \cdots \sigma_{l_r}(W_r)Z \in C_{n,m},$$

and note that $f_\lambda = \mathrm{Tr}(g_\lambda X_{m+1})$. Using linearity of $\mathrm{Tr}(-)$ relation (1) can be written as

$$\mathrm{Tr}\left(X_{m+1}\left(X_{i_1} \cdots X_{i_d} - \sum_{\lambda \in \Lambda} a_\lambda g_\lambda \right) \right) = 0 \in R_{n,m+1}. \tag{2}$$

Substituting $X_{m+1} \mapsto E_{ij}$ (the matrix whose (i,j)-entry is 1 and all other entries are 0) we get from (2) that the (j,i)-entry of $X_{i_1} \cdots X_{i_d} - \sum_{\lambda \in \Lambda} a_\lambda g_\lambda$ is 0. This holds for all (i,j), thus we have the equality

$$X_{i_1} \cdots X_{i_d} = \sum_\lambda a_\lambda g_\lambda. \tag{3}$$

The right-hand side of (3) is obviously contained in $R_{n,m}^+ C_{n,m}$, therefore it follows from (3) that the element $x_{i_1} \cdots x_{i_d} \in \mathcal{F}_m$ belongs to the kernel of $\eta \circ \varphi_1$. Thus by Corollary 2.3 we conclude that $x_{i_1} \cdots x_{i_d} \in I_{n,m}$. $\square$

3. Lower bound

Kuzmin's proof of the case $\mathrm{char}(\mathbb{F}) = 0$ or $\mathrm{char}(\mathbb{F}) > n$ of Theorem 1.7 (it is presented also in the survey of Drensky in [Drensky and Formanek 2004]) uses crucially Lemma 3.1 below, relating the *complete linearization of* x^n, namely

$$P_n(x_1, \ldots, x_n) = \sum_{\pi \in \mathrm{Sym}\{1,\ldots,n\}} x_{\pi(1)} x_{\pi(2)} \cdots x_{\pi(n)} \in \mathcal{F}_n.$$

Lemma 3.1. *If* $\mathrm{char}(\mathbb{F}) = 0$ *or* $\mathrm{char}(\mathbb{F}) > n$, *then* $I_{n,m}$ *is spanned as an* $\mathbb{F}$-*vector space by the elements* $P_n(w_1, \ldots, w_n)$, *where* $w_1, \ldots, w_n$ *range over all nonempty monomials in* $x_1, \ldots, x_m$.

Remark 3.2. The assumption on $\mathrm{char}(\mathbb{F})$ in Lemma 3.1 is necessary, its statement obviously fails if $0 < \mathrm{char}(\mathbb{F}) \leq n$ (as it can be easily seen already in the special case $m = 1$). Now we modify the arguments of Kuzmin to obtain Theorem 1.7 in a characteristic free manner. It turns out that although Lemma 3.1 can not be applied, the main combinatorial ideas of Kuzmin's proof do work.

Consider the free $\mathbb{Z}$-algebra $\mathcal{Z} = \mathbb{Z}\langle x, y \rangle^+$ without unity. Write $\mathcal{M}$ for the set of nonempty monomials (words) in x and y. For a positive integer k write $\mathcal{Z}(k)$ for the $\mathbb{Z}$-submodule of $\mathcal{Z}$ generated by the $w \in \mathcal{M}$ whose total degree in y is $k-1$. It will be convenient to use the following notation, for $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$ set

$$[a_1, \ldots, a_k] = x^{a_1} y x^{a_2} y \cdots y x^{a_k} \in \mathcal{M}.$$

The symmetric group $S_k = \mathrm{Sym}\{1, \ldots, k\}$ acts on the right linearly on $\mathcal{Z}(k)$, extending linearly the permutation action on $\mathcal{Z}(k) \cap \mathcal{M}$ given by

$$[a_1, \ldots, a_k]^\pi = [a_{\pi(1)}, \ldots, a_{\pi(k)}] \quad \text{for } \pi \in S_k.$$

Let $\mathcal{B}$ denote the $\mathbb{Z}$-submodule of $\mathcal{Z}$ generated by all the elements $[a_1, \ldots, a_k]$ ($k \in \mathbb{N}$) such that $a_i \geq n$ for some $i \in \{1, \ldots, k\}$ or $a_i = a_j$ for some $1 \leq i < j \leq k$, and by all the elements of the form $[a_1, \ldots, a_k] + [a_1, \ldots, a_k]^{(ij)}$ where (ij) denotes the transposition interchanging i and j for $1 \leq i < j \leq k$. We shall use the following obvious properties of $\mathcal{B}$:

Lemma 3.3. (i) *The $\mathbb{Z}$-submodule $\mathcal{B} \cap \mathcal{Z}(k)$ of $\mathcal{Z}(k)$ is S_k-stable.*

(ii) *We have the inclusions $y\mathcal{B} \subset \mathcal{B}$, $\mathcal{Z}y\mathcal{B} \subset \mathcal{B}$, $\mathcal{B}y \subset \mathcal{B}$, and $\mathcal{B}y\mathcal{Z} \subset \mathcal{B}$.*

(iii) *Let k be a positive integer, $u_1, \ldots, u_{k-1} \in \mathcal{M}$ monomials such that $u_i \in y\mathcal{Z} \cap \mathcal{Z}y$ or $u_i = y$ for $i = 1, \ldots, k-1$. Then $\mathcal{B}$ contains the image of the $\mathbb{Z}$-module map on $\mathcal{B} \cap \mathcal{Z}(k)$ given by*

$$[a_1, \ldots, a_k] \mapsto x^{a_1} u_1 x^{a_2} u_2 x^{a_3} \cdots u_{k-1} x^{a_k}.$$

(iv) *For any positive integer a, the $\mathbb{Z}$-submodule $\mathcal{B}$ of $\mathcal{Z}$ is preserved by the derivation δ_a on $\mathcal{Z}$ defined by $\delta_a(x) = x^a$ and $\delta_a(y) = 0$.*

(v) *The factor $\mathcal{Z}/\mathcal{B}$ is a free $\mathbb{Z}$-module freely generated by the images under the natural surjection $\mathcal{Z} \to \mathcal{Z}/\mathcal{B}$ of the monomials*

$$\widehat{\mathcal{M}} = \{[a_1, \ldots, a_k] \mid k \in \mathbb{N} \text{ and } 0 \leq a_1 < a_2 < \cdots < a_k \leq n-1\}.$$

Proof. Statements (i), (ii), (iii), (iv) are immediate consequences of the construction of $\mathcal{B}$. To prove (v) note that $\mathcal{Z} = \bigoplus \mathcal{Z}(c_1, \ldots, c_k)$ where the direct sum is taken over $k \in \mathbb{N}$ and $0 \leq c_1 \leq \cdots \leq c_k$, and $\mathcal{Z}(c_1, \ldots, c_k)$ stands for the $\mathbb{Z}$-submodule generated by $[c_1, \ldots, c_k]^\pi$ as π ranges over S_k. Moreover, $\mathcal{B} = \bigoplus \mathcal{B}(c_1, \ldots, c_k)$ where $\mathcal{B}(c_1, \ldots, c_k) = \mathcal{B} \cap \mathcal{Z}(c_1, \ldots, c_k)$. Now $\mathcal{Z}(c_1, \ldots, c_k) \subset \mathcal{B}$ if $c_i = c_j$ for some $i \neq j$ or if $c_i \geq n$ for some i. It is also clear that for $0 \leq a_1 < \cdots < a_k$ we have $\mathcal{Z}(a_1, \ldots, a_k) = \mathbb{Z} \cdot [a_1, \ldots, a_k] + \mathcal{B}(a_1, \ldots, a_k)$, so the monomials in $\widehat{\mathcal{M}}$ generate the $\mathbb{Z}$-module $\mathcal{Z}$ modulo $\mathcal{B}$. Suppose that some nontrivial $\mathbb{Z}$-linear combination of the elements in $\widehat{\mathcal{M}}$ belongs to $\mathcal{B}$. The above direct sum decompositions of $\mathcal{Z}$ and $\mathcal{B}$ imply then that there exist $q, k \in \mathbb{N}$, and $0 \leq a_1 < \cdots < a_k \leq n-1$ such that $q[a_1, \ldots, a_k] \in \mathcal{B}(a_1, \ldots, a_k)$. This means that

$$q[a_1, \ldots, a_k] = \sum_{i=1}^s \varepsilon_i (w_i + w_i^{\pi_i}), \tag{4}$$

where $\varepsilon_i = \pm 1$, $w_i \in \mathcal{Z}(a_1, \ldots, a_k) \cap \mathcal{M}$ and $\pi_i \in S_k$ is a transposition for $i = 1, \ldots, s$. Suppose that s in (4) is minimal. Without loss of generality we may assume that $w_1 = [a_1, \ldots, a_k]$ and $\varepsilon_1 = 1$. The word $w_1^{\pi_1}$ must be canceled by some summand $\varepsilon_i(w_i + w_i^{\pi_i})$ with $i \geq 2$ on the right-hand side of (4), so after a possible renumbering we have $\varepsilon_2(w_2 + w_2^{\pi_2}) = -(w_1^{\pi_1} + w_1^{\pi_1 \pi_2})$. Now the term $-w_1^{\pi_1 \pi_2}$ must be canceled by w_1 or by some summand $\varepsilon_i(w_i + w_i^{\pi_i})$ with $i \geq 3$. It means that the right-hand side of (4) has a subsum of the form

$$(w_1 + w_1^{\pi_1}) - (w_1^{\pi_1} + w_1^{\pi_1 \pi_2}) + (w_1^{\pi_1 \pi_2} + w_1^{\pi_1 \pi_2 \pi_3}) - + \cdots + (-1)^{r-1}(w_1^{\pi_1 \cdots \pi_{r-1}} + w_1^{\pi_1 \cdots \pi_r}), \quad (5)$$

where $w_1^{\pi_1 \cdots \pi_r} = w_1$. This latter equality forces that $\pi_1 \cdots \pi_r$ is the identity permutation, so r is even, and then the sum (5) is zero. So all these terms can be omitted from (4). This contradicts the minimality of s. This shows that $q[a_1, \ldots, a_k]$ is not contained in $\mathcal{B}$. $\qquad \square$

Lemma 3.4. *Let k be a positive integer, $a_1 \leq a_2 \leq \cdots \leq a_k \in \mathbb{N}_0$, and $r \in \mathbb{N}_0$ with $a_1 + k + r > n$. Then*

$$\sum_{c_1 + \cdots + c_k = r} \sum_{\pi \in S_k} [a_1 + c_{\pi(1)}, \ldots, a_k + c_{\pi(k)}] \in \mathcal{B}. \quad (6)$$

Proof. Apply induction on k. In the case $k = 1$ the element in question in (6) is $x^{a_1 + r}$, which belongs to $\mathcal{B}$ by the assumption $a_1 + 1 + r > n$. Suppose next that $k > 1$, and the statement of the lemma holds for smaller k. The terms $[a_1 + d_1, \ldots, a_k + d_k]$ in the sum (6) can be grouped into three classes:

(A) $a_1 + d_1 < a_2$.

(B) $a_1 + d_1 = a_2 + d_2$.

(C) $a_1 + d_1 \geq a_2$ and $a_1 + d_1 \neq a_2 + d_2$.

The sum of the terms of type (A) is a sum of expressions of the form

$$x^{a_1 + d_1} y \sum_{c_2 + \cdots + c_k = r - d_1} \sum_{\pi \in \mathrm{Sym}\{2, \ldots, k\}} [a_2 + c_{\pi(2)}, \ldots, a_k + c_{\pi(k)}]. \quad (7)$$

Here $a_2 + (k - 1) + (r - d_1) \geq a_1 + k + r > n$, hence by the induction hypothesis

$$\sum_{c_2 + \cdots + c_k = r - d_1} \sum_{\pi \in \mathrm{Sym}\{2, \ldots, k\}} [a_2 + c_{\pi(2)}, \ldots, a_k + c_{\pi(k)}]$$

belongs to $\mathcal{B}$. Now by Lemma 3.3(ii) we conclude that the element in (7) belongs to $\mathcal{B}$. The terms of type (B) belong to $\mathcal{B}$ by construction of $\mathcal{B}$. Finally, a term $[a_1 + d_1, \ldots, a_k + d_k]$ of type (C) can be paired off with the term $[a_1 + e_1, a_2 + e_2, a_3 + d_3, \ldots, a_k + d_k]$ where $e_1 = a_2 - a_1 + d_2$ and $e_2 = a_1 - a_2 + d_1$ (so this is also of type (C)), and the sum of these two terms belongs to $\mathcal{B}$ by construction of $\mathcal{B}$. $\qquad \square$

Corollary 3.5. *Let k be a positive integer, $(a_1, \ldots, a_k) \in \mathbb{N}_0^k$, and $r \in \mathbb{N}_0$ with $r + k > n$. Then*

$$\sum_{c_1 + \cdots + c_k = r} \sum_{\pi \in S_k} [a_1 + c_{\pi(1)}, \ldots, a_k + c_{\pi(k)}] \in \mathcal{B}.$$

Proof. Take a permutation $\rho \in S_k$ such that $a_{\rho(1)} \leq \cdots \leq a_{\rho(k)}$. Applying ρ to the element in the statement we get

$$\sum_{c_1 + \cdots + c_k = r} \sum_{\pi \in S_k} [a_{\rho(1)} + c_{\pi(1)}, \ldots, a_{\rho(k)} + c_{\pi(k)}],$$

which belongs to $\mathcal{B} \cap \mathcal{Z}(k)$ by Lemma 3.4. Our statement follows by Lemma 3.3(i). $\square$

Lemma 3.6. *Suppose $1 \leq k \leq n+1$, $w_1, \ldots, w_{k-1} \in \mathcal{M}$ are monomials having positive degree in y, and $a, b \in \mathbb{N}_0$. Then*

$$x^a P_n(w_1, \ldots, w_{k-1}, x, \ldots, x) x^b \in \mathcal{B}. \tag{8}$$

Proof. We have $w_i = x^{a_i} u_i x^{b_i}$ where $a_i, b_i \in \mathbb{N}_0$ and $u_i \in y\mathcal{Z} \cap \mathcal{Z}y$ or $u_i = y$ ($i = 1, \ldots, k-1$). Then the element in (8) is

$$\sum_{\rho \in S_{k-1}} \left((n-k+1)! \sum_{c_1 + \cdots + c_k = n-k+1} \sum_{\pi \in S_k} x^{d_1 + c_{\pi(1)}} u_{\rho(1)} x^{d_2 + c_{\pi(2)}} u_{\rho(2)} \cdots x^{d_{k-1} + c_{\pi(k-1)}} u_{\rho(k-1)} x^{d_k + c_{\pi(k)}} \right),$$

where $d_1 = a + a_{\rho(1)}$, $d_2 = a_{\rho(2)} + b_{\rho(1)}$, $d_3 = a_{\rho(3)} + b_{\rho(2)}$, $d_{k-1} = a_{\rho(k-1)} + b_{\rho(k-2)}$ and $d_k = b_{\rho(k-1)} + b$. The summand corresponding to $\rho \in S_{k-1}$ in the outer sum is contained in $\mathcal{B}$ by Corollary 3.5 and Lemma 3.3(iii). $\square$

Lemma 3.7. *For any $w_1, \ldots, w_n \in \mathcal{M}$, $w_0, w_{n+1} \in \mathcal{M} \cup \{1\}$ we have*

$$w_0 P_n(w_1, \ldots, w_n) w_{n+1} \in \mathcal{B}.$$

Proof. By Lemma 3.3(ii) it is sufficient to deal with the case $w_0 = x^a$, $w_{n+1} = x^b$. We may assume that $w_1, \ldots, w_{k-1}$ have positive degree in y and $w_{k-1+j} = x^{c_j}$ for $j = 1, \ldots, n-k+1$. If $n-k+1 = 0$ or all the $c_j = 1$ then we are done by Lemma 3.6. Suppose next that $n-k+1 > 0$, $c_1, \ldots, c_l > 1$ with $l \geq 1$, and $c_{l+1} = \cdots = c_{n-k+1} = 1$. By induction on l we show that $x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_l}, x, \ldots, x) x^b \in \mathcal{B}$. By the induction hypothesis (or by Lemma 3.6 when $l = 1$)

$$f = x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_{l-1}}, x, \ldots, x) x^b \in \mathcal{B},$$

hence by Lemma 3.3(iv) $\delta_{c_l}(f) \in \mathcal{B}$. We have

$$\delta_{c_l}(f) = ax^{a+c_l-1} P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_{l-1}}, x, \ldots, x) x^b$$
$$+ \sum_{i=1}^{k-1} x^a P_n(w_1, \ldots, \delta_{c_l}(w_i), \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_{l-1}}, x, \ldots, x) x^b$$
$$+ \sum_{j=1}^{l-1} c_j x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_j+c_l-1}, \ldots, x^{c_{l-1}}, x, \ldots, x) x^b$$
$$+ (n-k-l+2) x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_l}, x, \ldots, x) x^b$$
$$+ bx^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_{l-1}}, x, \ldots, x) x^{b+c_l-1}.$$

All terms other than $(n - k - l + 2)x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_l}, x, \ldots, x)x^b$ on the right-hand side above belong to $\mathcal{B}$ by the induction hypothesis. Taking into account that $\mathcal{Z}/\mathcal{B}$ is torsion free by Lemma 3.3(v) we conclude the desired inclusion

$$x^a P_n(w_1, \ldots, w_{k-1}, x^{c_1}, \ldots, x^{c_l}, x, \ldots, x)x^b \in \mathcal{B}. \qquad \square$$

For $\lambda = (\lambda_1, \ldots, \lambda_m) \in \mathbb{N}_0^m$ denote by $P_\lambda(x_1, \ldots, x_m) \in \mathbb{Z}\langle x_1, \ldots, x_m \rangle$ the multihomogeneous component of $(x_1 + \cdots + x_m)^n$ having $\mathbb{Z}^m$-degree λ.

Corollary 3.8. *For any $m \in \mathbb{N}$, $w_1, \ldots, w_m \in \mathcal{M}$, $w_0, w_{m+1} \in \mathcal{M} \cup \{1\}$ and for any $\lambda \in \mathbb{N}_0^m$ we have that*

$$w_0 P_\lambda(w_1, \ldots, w_m)w_{m+1} \in \mathcal{B}.$$

Proof. We have the equality

$$P_\lambda(x_1, \ldots, x_m) = \frac{1}{\prod_{i=1}^m (\lambda_i!)} P_n(\underbrace{x_1, \ldots, x_1}_{\lambda_1}, \ldots, \underbrace{x_m, \ldots, x_m}_{\lambda_m}).$$

Therefore the statement follows from Lemma 3.7 by Lemma 3.3(v). $\qquad \square$

Proposition 3.9. *The ideal $I_{n,2}$ is contained in the subspace $\mathbb{F} \otimes_{\mathbb{Z}} \mathcal{B}$ of $\mathbb{F}\langle x, y \rangle$.*

Proof. The ideal $I_{n,2}$ is spanned as an $\mathbb{F}$-vector space by elements of the form

$$w_0(c_1 w_1 + \cdots + c_m w_m)^n w_{m+1},$$

where the w_i are monomials in x and y and they have positive total degree for $i = 1, \ldots, m$, and $c_1, \ldots, c_m \in \mathbb{F}$. Since we have the equality

$$(c_1 w_1 + \cdots + c_m w_m)^n = \sum_{\lambda \in \mathbb{N}_0^m, \lambda_1 + \cdots + \lambda_m = n} c_1^{\lambda_1} \cdots c_m^{\lambda_m} P_\lambda(w_1, \ldots, w_m),$$

our statement follows from Corollary 3.8. $\qquad \square$

Proof of Theorem 1.7. By Lemma 3.3(v) the monomials

$$\{x^{a_1} y x^{a_2} y x^{a_3} \cdots y x^{a_k} \mid 0 \le a_1 < a_2 < \cdots < a_k \le n - 1\}$$

are linearly independent in $\mathcal{F}_2 = \mathbb{F}\langle x, y \rangle$ modulo the subspace $\mathbb{F} \otimes_{\mathbb{Z}} \mathcal{B}$. Since $\mathbb{F} \otimes_{\mathbb{Z}} \mathcal{B}$ contains the ideal $I_{n,2}$ by Proposition 3.9, our statement follows. $\qquad \square$

References

[Belov 1992] A. J. Belov, "Some estimations for nilpotence of nil-algebras over a field of an arbitrary characteristic and height theorem", *Comm. Algebra* **20**:10 (1992), 2919–2922. MR Zbl

[Belov and Kharitonov 2012] A. Y. Belov and M. I. Kharitonov, "Subexponential estimates in Shirshov's height theorem", *Mat. Sb.* **203**:4 (2012), 81–102. In Russian; translation in *Sb. Math.* **203**:3-4 (2012), 534–553. MR Zbl

[De Concini and Procesi 2017] C. De Concini and C. Procesi, *The invariant theory of matrices*, University Lecture Series **69**, Amer. Math. Soc., Providence, RI, 2017. MR Zbl

[Derksen and Makam 2017a] H. Derksen and V. Makam, "Generating invariant rings of quivers in arbitrary characteristic", *J. Algebra* **489** (2017), 435–445. MR Zbl

[Derksen and Makam 2017b] H. Derksen and V. Makam, "Polynomial degree bounds for matrix semi-invariants", *Adv. Math.* **310** (2017), 44–63. MR Zbl

[Domokos 2002] M. Domokos, "Finite generating system of matrix invariants", *Math. Pannon.* **13**:2 (2002), 175–181. MR Zbl

[Donkin 1992] S. Donkin, "Invariants of several matrices", *Invent. Math.* **110**:2 (1992), 389–401. MR Zbl

[Drensky and Formanek 2004] V. Drensky and E. Formanek, *Polynomial identity rings*, Birkhäuser, Basel, 2004. MR Zbl

[Formanek 1986] E. Formanek, "Generating the ring of matrix invariants", pp. 73–82 in *Ring theory* (Antwerp, 1985), edited by F. M. J. Van Oystaeyen, Lecture Notes in Math. **1197**, Springer, 1986. MR Zbl

[Formanek 1991] E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, CBMS Regional Conf. Ser. in Math. **78**, Amer. Math. Soc., Providence, RI, 1991. MR Zbl

[Guralnick et al. 2010] R. M. Guralnick, L. W. Small, and E. Zelmanov, "Nil subrings of endomorphism rings of finitely generated modules over affine PI-rings", *J. Algebra* **324**:11 (2010), 3044–3047. MR Zbl

[Ivanyos et al. 2017] G. Ivanyos, Y. Qiao, and K. V. Subrahmanyam, "Non-commutative Edmonds' problem and matrix semi-invariants", *Comput. Complexity* **26**:3 (2017), 717–763. MR Zbl

[Jacobson 1945] N. Jacobson, "Structure theory for algebraic algebras of bounded degree", *Ann. of Math.* (2) **46** (1945), 695–707. MR Zbl

[Kaplansky 1946] I. Kaplansky, "On a problem of Kurosch and Jacobson", *Bull. Amer. Math. Soc.* **52** (1946), 496–500. MR Zbl

[Klein 2000] A. A. Klein, "Bounds for indices of nilpotency and nility", *Arch. Math.* (*Basel*) **74**:1 (2000), 6–10. MR Zbl

[Kuzmin 1975] E. N. Kuzmin, "О теореме Нагаты–Хигмана", pp. 101–107 in Математические структуры. Вычислительная математика. Математические моделирование, edited by B. Sendov, Bulgarian Acad. Sci., Sofia, 1975.

[Lopatin 2005] A. A. Lopatin, "Relatively free algebras with the identity $x^3 = 0$", *Comm. Algebra* **33**:10 (2005), 3583–3605. MR Zbl

[Lopatin 2012] A. A. Lopatin, "On the nilpotency degree of the algebra with identity $x^n = 0$", *J. Algebra* **371** (2012), 350–366. MR Zbl

[Lopatin 2013] A. A. Lopatin, "Matrix identities with forms", *J. Pure Appl. Algebra* **217**:11 (2013), 2056–2075. MR Zbl

[Nagata 1952] M. Nagata, "On the nilpotency of nil-algebras", *J. Math. Soc. Japan* **4** (1952), 296–301. MR Zbl

[Newstead 1978] P. E. Newstead, *Introduction to moduli problems and orbit spaces*, Tata Inst. Fundamental Res. Lectures on Math. and Phys. **51**, Tata Inst. Fundamental Res., Bombay, 1978. MR Zbl

[Procesi 1976] C. Procesi, "The invariant theory of $n \times n$ matrices", *Advances in Math.* **19**:3 (1976), 306–381. MR Zbl

[Razmyslov 1974] Y. P. Razmyslov, "Trace identities of full matrix algebras over a field of characteristic zero", *Izv. Akad. Nauk SSSR Ser. Mat.* **38**:4 (1974), 723–756. In Russian; translation in *Math. USSR-Izv.* **8**:4 (1974), 727–760. MR Zbl

[Zubkov 1996] A. N. Zubkov, "On a generalization of the Razmyslov–Procesi theorem", *Algebra i Logika* **35**:4 (1996), 433–457. In Russian; translation in *Algebra Logic* **35**:4 (1996), 241–254. MR Zbl

domokos.matyas@renyi.mta.hu   *MTA Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Hungary*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

Algebra & Number Theory

Volume 12   No. 5   2018