Available online at www.sciencedirect.com
SCIENCE DIRECT®
LINEAR ALGEBRA AND ITS APPLICATIONS
ELSEVIER Linear Algebra and its Applications 395 (2005) 175–181
www.elsevier.com/locate/laa

Lengths of finite dimensional representations of PBW algebras ☆

D. Constantine [a,*], M. Darnall [b]

[a] *Eastern Nazarene College, 23 E. Elm Ave., Quincy, MA 02170, USA*
[b] *Humboldt State University, 1 Harpst St., Arcata, CA 95521, USA*

Received 13 October 2003; accepted 3 August 2004

Submitted by R. Guralnick

Abstract

Let Σ be a set of $n \times n$ matrices with entries from a field, for $n > 1$, and let $c(\Sigma)$ be the maximum length of products in Σ necessary to linearly span the algebra it generates. Bounds for $c(\Sigma)$ have been given by Paz and Pappacena, and Paz conjectures a bound of $2n - 2$ for any set of matrices. In this paper we present a proof of Paz's conjecture for sets of matrices obeying a modified Poincaré–Birkhoff–Witt (PBW) property, applicable to finite dimensional representations of Lie algebras and quantum groups. A representation of the quantum plane establishes the sharpness of this bound, and we prove a bound of $2n - 3$ for sets of matrices with this modified PBW property which do not generate the full algebra of all $n \times n$ matrices. This bound of $2n - 3$ also holds for representations of Lie algebras, although we do not know whether it is sharp in this case.

AMS classification: 15A30

Keywords: Representations of Lie Algebras; Representations of quantum groups; PBW sets; Lengths of representations

☆ This research was begun during the 2003 Temple Mathematics Research Experience for Undergraduates, supported by Temple University and NSF REU Site Grant DMS-0138991. The authors were participants in this program.

* Corresponding author. Address: Department of Mathematics, University of Michigan, 2074 East Hall, Ann Arbor, MI 48109, USA.

E-mail addresses: constand@umich.edu (D. Constantine), darnall@math.wisc.edu (M. Darnall).

0024-3795/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.laa.2004.08.006

1. Introduction

For a fixed integer $n > 1$, let $\Sigma = \{X_1, \ldots, X_t\}$ be a set of $n \times n$ matrices over an arbitrary field $\mathbf{k}$, and let Σ^m be the set of products of length m in the X_i, where Σ^0 is defined as the identity. Let L_i be the linear space spanned by $\Sigma^0 \cup \Sigma^1 \cup \ldots \cup \Sigma^i$, and denote the dimension of this space by r_i. Next, let L_* be the linear space spanned by products of any length, and let r_* denote its dimension. Finally, let $c(\Sigma) = \min\{i : r_i = r_*\}$.

In [4], Paz proved that $c(\Sigma) \leqslant \lceil (n^2+2)/3 \rceil$, and Pappacena proved an upper bound which is $O(n^{3/2})$ [3]. Paz conjectured a bound of $2n-2$ and suggested a lemma which, if proved, would prove the conjecture. We prove this lemma (listed as Proposition 2.6 below) for matrices satisfying the following property: every product $u = X_{i_1} X_{i_2} \cdots X_{i_l}$ in the matrices $X_1, \ldots, X_t$ can be written, modulo L_{l-1}, in the form

$$\sum_{j_1+j_2\cdots+j_t=l} c_{(j_1,\ldots,j_t)} X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1},$$

with $c_{(j_1,\ldots,j_t)} = 0$ whenever $X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1} < u$ in the lexicographical ordering.

This modified PBW property allows any l-length matrix product u to be written as a linear combination of ordered products of length l, modulo products (not necessarily ordered) of lesser length; here by *ordered product* we mean a product in which $X_i X_j$ never appears for $i < j$. Our condition is, in fact, looser than what is generally found in homomorphic images of algebras satisfying the PBW property (see, e.g. [1] for further details). Sets of matrices obeying our property include finite dimensional representations of Lie algebras and quantum groups (see, e.g., [2] for further details).

The $2n-2$ bound is in fact sharp for the class of matrices satisfying the above property, as an example using the quantum plane illustrates, but smaller upper bounds for certain other cases can be obtained. In particular, knowledge about r_* allows the constraints of Paz's suggested lemma to be tightened, resulting in such smaller upper bounds on $c(\Sigma)$. As an example we provide a proof of a $2n-3$ bound when the $\mathbf{k}$-algebra generated by Σ is not equal to $M_n(\mathbf{k})$, the full algebra of all $n \times n$ matrices over the field $\mathbf{k}$.

This research was begun during the summer 2003 Research Experience for Undergraduates program supervised by E. S. Letzter at Temple University. The authors are greatly indebted to Dr. Letzter for his guidance during the program and his help in writing this paper.

2. Proof of the main theorem

We begin with a formal definition of the modified PBW property then continue with some notation and preliminaries necessary to our proof. We then prove Lemmas

2.4 and 2.5. Together, these preliminary lemmas establish Paz's suggested lemma, listed below as Proposition 2.6. We then proceed to prove our main theorem.

Definition 2.1. A set of matrices $\Sigma = \{X_1, \ldots, X_t\}$ is said to have the modified PBW property if every product $u = X_{i_1} X_{i_2} \cdots X_{i_l}$ can be written, modulo L_{l-1}, in the form

$$\sum_{j_1+j_2\cdots+j_t=l} c_{(j_1,\ldots,j_t)} X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1},$$

with $c_{(j_1,\ldots,j_t)} = 0$ whenever $X_t^{j_t} X_{t-1}^{j_{t-1}} \cdots X_1^{j_1} < u$ in the lexicographical ordering.

2.2. *Notation*

(i) We first note that the matrix product $X_{i_1} \cdots X_{i_k}$ in Σ^m corresponds naturally to the formal word $i_1 \ldots i_k$. We make here a distinction between a matrix product of length m, which is an element of Σ^m, and a formal word of length m, which is an element of the free monoid on t letters of length m. Any formal word is uniquely associated with a matrix product in Σ^m, but a matrix product may have many different representations by formal words. We will denote matrix products in Σ^m by lower case letters, i.e. u, and corresponding formal words with a bar, i.e. $\bar{u}$. An *l-subword* of a formal word $\bar{u}$ is any set of l consecutive letters in $\bar{u}$.

(ii) We say two formal words are *formally equivalent* if their ith letters match for all i; otherwise we say they are *formally distinct*. We call a subword consisting of one repeated letter, such as $111 \ldots 1$, *formally constant*.

(iii) If $u_1, u_2, u_3, \ldots, u_k$ are m-length matrix products, $u_{i_1} \propto (u_{i_2}, u_{i_3}, \ldots, u_{i_l})$ means u_{i_1} is a linear combination of $u_{i_2}, u_{i_3}, \ldots, u_{i_l}$ modulo L_{m-1}.

(iv) We call a matrix product *reducible* if it can be written as a linear combination of matrix products of lesser length.

2.3. *Preliminaries*

(i) Any matrix product that can be written as a linear combination, modulo products of lesser length, of other products that are all reducible is itself reducible. Thus, we will examine only ordered products, and the modified PBW property guarantees that our results will carry over to all matrix products in sets that satisfy that property.

(ii) If any formal word contains a subword of n or more of the same letter, the corresponding matrix product will be reducible by the Cayley–Hamilton Theorem.

(iii) There is a natural ordering on the formal words which coincides exactly with the lexicographical ordering on matrix products previously mentioned.

Lemma 2.4. *Suppose that $r_k - r_{k-1} \leqslant N$ for some positive integers k and N. If $u \in \Sigma^m$ is such that some representative $\bar{u}$ contains more than N formally distinct k-subwords, then*

$$u \equiv \sum_i \alpha_i u_i \,(\mathrm{mod}\, L_m),$$

with representative $\bar{u}_i$ each having at most N formally distinct k-subwords.

Proof. Given such a formal word $\bar{u}$ of length m, let $\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_s$ for $s > N$ be $\bar{u}$'s formally distinct k-subwords, numbered such that $\bar{u}_1 < \bar{u}_2 < \cdots < \bar{u}_s$. Since there are more subwords than $r_k - r_{k-1}$, these subwords must be linearly dependent, modulo L_{k-1}. Therefore there exists a minimum i such that $u_i \propto (u_{j_1}, u_{j_2}, \ldots, u_{j_p})$ with $j_1, j_2, \ldots, j_p > i$. (Note that if $i = s$ then u_s is equal, modulo L_{k-1}, to zero, and u is trivially reducible.) We form the new formal words $\bar{u}^{(1)}, \bar{u}^{(2)}, \ldots, \bar{u}^{(p)}$ from $\bar{u}$ by replacing $\bar{u}_i$ with $\bar{u}_{j_l}$ to form $\bar{u}^{(l)}$. We see that $u \propto (u^{(1)}, u^{(2)}, \ldots, u^{(p)})$ and that $\bar{u}^{(l)} > \bar{u}$ for all l.

We can apply the above process to each of the formal words $\bar{u}^{(l)}$ as long as they have more than N formally distinct subwords. Since this process continually increases the numerical value of these formal words and there are finitely many formal words of length m, we will eventually write u as a linear combination, modulo L_{m-1}, of matrix products with representative formal words that have at most N formally distinct k-subwords.

In addition, because rewriting matrix products in ordered form via the modified PBW property also continually increases their representative formal words in the natural ordering, we can, at each step in the above process, put all our matrix products in ordered form. Therefore, when working with sets of matrices obeying the modified PBW property we can write any ordered matrix product u as a linear combination, modulo L_{m-1}, of *ordered* matrix products with representative formal words having at most N formally distinct k-subwords. □

Lemma 2.5. *For a positive integer $k \leqslant 2n - 2$, set*

$$N = \begin{cases} k & \text{for } 1 \leqslant k \leqslant n-1, \\ 2n-k-2 & \text{for } n \leqslant k \leqslant 2n-2. \end{cases}$$

Any ordered formal word of length $2n - 1$ not reducible by the Cayley–Hamilton Theorem contains at least $N + 2$ formally distinct k-subwords.

Proof. Let $\bar{u}$ be an ordered formal word of length $2n - 1$ that is not reducible by the Cayley–Hamilton Theorem.

Case I. Suppose $1 \leqslant k \leqslant n - 1$. Recall $N = k$.

Subcase i. The longest formally constant subword in $\bar{u}$ has length greater than or equal to k.

Specifically, call the longest formally constant subword $\bar{w}$ and say it has length $j \geqslant k$. Since our formal word is not reducible by Cayley–Hamilton, $j < n$. Since

$k \leqslant j < n$ and $\hat{u}$ has length $2n-1$ there will be at least $k+1 = N+1$ k-subwords overlapping but not contained in $\bar{w}$. Examining these k-subwords, we see that they will be formally distinct since each features the transition between $\bar{w}$ and the surrounding letters in a different spot. Thus, including one of the formally constant k-subwords found within $\bar{w}$, we conclude that $\bar{u}$ contains at least $N+2$ formally distinct k-subwords.

Subcase ii. The longest formally constant subword in $\bar{u}$ has length less than k.

In this case no two k-subwords will be formally equivalent since none will be constant. Since $k < n$, $\bar{u}$ has at least $n+1k$-subwords. Since $N = k < n$, $\bar{u}$ contains at least $N+2$ formally distinct k-subwords.

Case II. Now suppose $n \leqslant k \leqslant 2n-2$. Recall $N = 2n-2-k$. Since $k \geqslant n$, no two k-subwords can be formally equivalent or else $\bar{u}$ will be reducible by Cayley–Hamilton since $\bar{u}$ will contain a formally constant subword of length greater than n. There are $2n-kk$-subwords in total, so $\bar{u}$ contains $N+2$ formally distinct k-subwords. □

We now prove the lemma suggested by Paz.

Proposition 2.6. *Let Σ have the modified PBW property. Suppose that for some positive integer $k \leqslant 2n-2$ the following condition holds*:

$$r_k - r_{k-1} \leqslant k, \quad \textit{if } 1 \leqslant k \leqslant n-1,$$

$$r_k - r_{k-1} \leqslant 2n-k-2, \quad \textit{if } n \leqslant k \leqslant 2n-2.$$

Then $c(\Sigma) \leqslant 2n-2$.

Proof. Lemmas 2.4 and 2.5 establish this proposition in the following manner. Suppose the above condition holds for a certain k and let N correspond to k as described in the statement of Lemma 2.5. Consider a matrix product u of length $2n-1$. We will show that u is reducible, giving us that $c(\Sigma) \leqslant 2n-2$.

If u is reducible by Cayley–Hamilton, we are done. If u is not reducible by Cayley–Hamilton then Lemma 2.5 implies that a representative $\bar{u}$ has more than N formally distinct k-subwords. Lemma 2.4 then implies that u is congruent (modulo L_{m-1}) to a linear combination of matrix products with representative formal words which do not have more than N distinct k-subwords. Finally, the contrapositive of Lemma 2.4 implies that these products are reducible by Cayley–Hamilton. Thus u is reducible, and $c(\Sigma) \leqslant 2n-2$. □

We now prove our main theorem.

Theorem 2.7. *Let Σ be a set of $n \times n$ matrices satisfying the modified PBW property. Then $c(\Sigma) \leqslant 2n-2$.*

Proof (following [4]). If $c(\Sigma) > 2n-2$, none of the conditions of Proposition 2.6 can hold. Thus, if $c(\Sigma) \geqslant 2n-1$, then $r_0 = 1, r_1 - r_0 \geqslant 2, r_2 - r_1 \geqslant 3, \ldots, r_{n-1} - r_{n-2} \geqslant n, r_n - r_{n-1} \geqslant n-1, \ldots, r_{2n-2} - r_{2n-3} \geqslant 1$. Then we have $r_{2n-2} \geqslant 1 + 2 + \cdots + n - 1 + n + n - 1 + \cdots + 1 = 2(n(n-1))/2 + n = n^2 \geqslant r_*$. This, however, contradicts $c(\Sigma) > 2n-1$, for if r_{2n-2} is already greater than or equal to the dimension of all of L_*, r_{2n-1} can be no larger than r_{2n-2}. $\square$

3. Sharpness of the bound

The bound of $2n-2$ is sharp for the general set of matrices described above as the following example from the quantum plane shows.

Consider complex $n \times n$ matrices X and Y satisfying $XY = qYX$, where $q = \mathrm{e}^{2\pi \mathrm{i}/n}$, such that the algebra generated by X and Y is all of $M_n(\mathbb{C})$. Because X^n and Y^n are reducible by the Cayley–Hamilton Theorem, the set $P = \{X^i Y^j | 0 \leqslant i, j \leqslant n-1\}$ must span all of L_*. Since $M_n(\mathbb{C})$ has dimension n^2 and P contains n^2 matrices, P is in fact a basis. Thus the $(2n-2)$-length product $X^{n-1}Y^{n-1}$ is linearly independent from any products of lesser length, giving us that $c(\Sigma) = 2n-2$ for such a set of matrices.

It remains only to show that such matrices do indeed exist. We leave it to the reader to verify that the following matrices satisfy the above conditions.

$$X = \begin{bmatrix} 1 & & & \\ & q & & \\ & & \ddots & \\ & & & q^{n-1} \end{bmatrix}, \quad Y = \begin{bmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix}.$$

Lower bounds for certain sets of matrices can be obtained. Paz's suggested lemma is set up to deal with sets of matrices for which r_* could be as great as n^2. With more information about the dimension of L_* for a given set of matrices, the conditions of the lemma can be tightened, resulting in lower bounds for $c(\Sigma)$, as the following shows.

We prove a slightly more restrictive form of Proposition 2.6, which we then use to prove Theorem 3.2.

Proposition 3.1. *Suppose that for some $k \leqslant 2n-3$ the following condition holds*:

$$r_k - r_{k-1} \leqslant k, \quad \text{if } 1 \leqslant k \leqslant n-1,$$

$$r_k - r_{k-1} \leqslant 2n-k-2, \quad \text{if } n \leqslant k \leqslant 2n-3.$$

Then $c(\Sigma) \leqslant 2n-3$.

Proof. Lemma 2.5 tells us that in an ordered word of length $2n-1$ there are at least $N+2$ formally distinct k-subwords. Since decreasing to length $2n-2$ eliminates at most one of these k-subwords, there will still be at least $N+1$. Since we only need more than N, the proof of Proposition 3.1 then follows directly from the proof of Proposition 2.6. $\square$

Theorem 3.2. *Let Σ have the modified PBW property, and suppose that it does not generate all of $M_n(\mathbf{k})$. Then $c(\Sigma) \leqslant 2n-3$.*

Proof. Now we proceed as before. If $c(\Sigma) > 2n-3$, then none of the conditions in Proposition 3.1 can hold. This implies $r_0 = 1, r_1 - r_0 \geqslant 2, r_2 - r_1 \geqslant 3, \ldots, r_{n-1} - r_{n-2} \geqslant n, r_n - r_{n-1} \geqslant n-1, \ldots, r_{2n-3} - r_{2n-4} \geqslant 2$. Then we have $r_{2n-3} \geqslant 1 + 2 + \cdots + n - 1 + n + n - 1 + \cdots + 2 = 2(n(n-1))/2 + n - 1 = n^2 - 1$. Because of the restriction placed on the algebra generated by Σ, $n^2 - 1 \geqslant r_*$. As before, this contradicts $c(\Sigma) > 2n-3$. $\square$

For representations of Lie algebras $c(\Sigma)$ is bounded by $2n-3$ as well. No Lie algebra consisting of two matrices generates all of $M_n(\mathbf{k})$, and for a Lie algebra of three or more matrices to do so those three matrices, together with the identity, must be linearly independent, implying that $r_1 - r_0 \geqslant 3$. This allows a proof similar to that given for Theorem 3.2 since now the sum of the $r_{i+1} - r_i$ terms will be greater than or equal to n^2 by the time we get to a length of $2n-3$. We leave as an open question whether the bound of $2n-3$ is sharp for representations of Lie algebras. We have looked for an example achieving this bound but have been unable to find one.

References

[1] J. Dixmier, Enveloping Algebras, Graduate Studies in Mathematics, vol. 11, AMS, Providence, 1996.

[2] A. Joseph, Quantum Groups and Their Primitive Ideals, Ergebnisse der Mathematik und ihrer Grenzgebiete 3, vol. 29, Springer-Verlag, Berlin, 1995.

[3] C.J. Pappacena, An upper bound for the length of a finite-dimensional algebra, J. Algebra 197 (1997) 535–545.

[4] A. Paz, An application of the Cayley–Hamilton theorem to matrix polynomials in several variables, J. Linear Multilinear Algebra 15 (1984) 161–170.