On the lengths of some generating sets of matrix algebras

Thomas Laffey (University College Dublin)

This work is based on a collaboration with Helena Šmigoc (University College Dublin) and Alexander Guterman and Olga Markova (Lomonosov Moscow State University)

Ljubljana 2017

Let S be a set of generators of a finite dimensional algebra A over the field of complex numbers. So A is spanned by the monomials in elements of S.
Let $\mathcal{L}^i(S)$ be the span of the monomials of degree at most i.
[We write $\mathcal{L}^0(S) = \{I\}$, if A contains an identity element I.]
We have

$$\mathcal{L}^0(S) \sqsubseteq \mathcal{L}^1(S) \sqsubseteq ... \sqsubseteq \mathcal{L}^k(S) \sqsubseteq ... \tag{1}$$

Since dim(A) is finite, we find that dim ($\mathcal{L}^k(S)) = \dim(\mathcal{L}^{k+1}(S))$ $= \dim(A)$, for some nonnegative integer $k \leq \dim(A)$, and the least such k is called the *length* of S.
The maximum of the lengths of all generating sets of A is called the *length* of A.

The problem of determining the length of the full matrix algebra M_n appears to have been first posed by Paz (LAMA **15 (**1984) 161-170), though the problem of the lengths of generating sets for M_n consisting of nilpotent matrices is alluded to in Procesi's book on polynomial identities.
The inclusion argument outlined above shows that the length of M_n is, at most, $n^2 - 1$, and Paz improved this bound to $\frac{n^2+2}{3}$.

Paz conjectured that the length of M_n is at most $2n-2$.
If proved, this bound would be best possible. It is well-known that for every prime p, a nonabelian group of order p^3 has a faithful irreducible representation of degree p, and has generators X, Y satisfying $XY = \omega YX$, where ω is a primitive p^{th} root of unity, and it is easy to check that $\{X, Y\}$ has length $2p-2$. Olga Markova's talk contained a detailed analysis of extensions of this to general n.
Pappacena (J.Algebra **197** (1997) 535-545) has made a strong contribution to bounding the lengths of generating sets S for M_n and proves in particular that the length of S is at most $2n-2$ if S contains a matrix with n distinct eigenvalues. Also, using a complicated refinement of Paz's argument, he obtains an upper bound of $O(n^{3/2})$ for the length of M_n.

One expects that generating sets S of M_n of large length are hard to find and that if one randomly chooses a generating set S, one expects that monomials in the elements of S of small degree will satisfy few linear dependence relations, thus leading to the length of S being small. This expectation has been quantified and formally established by Klep and Špenko (J. Combin. Theory A **143** (2016) 56-65).

For an odd prime p and positive integer n, let P be a (Hall) extraspecial $p-$group of order p^{2n+1} and exponent p.
So the centre $Z(P)$ and commutator subgroup P' of P coincide and have order p. Every non-linear irreducible complex representation Γ of P is faithful and has degree p^n.(Huppert Endliche Gruppen I,Kap. III,V).
Also, P contains elements $x_1, \ldots, x_{2n}$ such that

$$P = \{x_1^{a_1} \quad \ldots \quad x_{2n}^{a_{2n}} z^b : 0 \leq a_i \leq p-1, (1 \leq i \leq 2n),\ 0 \leq b \leq p-1\},$$

where $Z(P) =< z >$. The set $S = \{\Gamma(x_1), \quad \ldots \quad , \Gamma(x_{2n})\}$ generates the full matrix algebra M_{p^n}, and its length is at most $2n(p-1)$.

A key argument used by Paz and later Pappacena in obtaining their upper bounds for the length of M_n is to consider a monomial m in elements of a generating set S of M_n of degree k greater than n and examine whether m can be expressed as a linear combination of monomials in the elements of S of degree less than k. For example, if m contains a subword of the form v^n for some monomial v in the elements of S of degree at least one, then one can apply the Cayley-Hamilton theorem to express v^n as a linear combination of powers of v of lower degree and thus m can be expressed as a linear combination of monomials of degree less than k.

More generally, if for some $s \geq 1$, the quotient space $\mathcal{L}^{s+1}(S)/\mathcal{L}^{s}(S)$ has dimension t, say, and there are $t+1$ distinct subwords of m of degree $s+1$, one can use the linear dependence of these subwords mod $\mathcal{L}^{s}(S)$ to replace one of them by a linear combination of the others and monomials of degree less than $s+1$. This can be carried out in conjunction with an ordering, usually lexicographic, on monomials on the elements of S, and this leads to m being a linear combination of monomials of length k lower in the ordering and monomials of degree less than k. These processes are repeated and eventually shown to imply that for sufficiently large and explicit k, m can be expressed as a linear combination of monomials of degree less than k. This argument is in the spirit of Shirshov's theorem and is a key ingredient of related work of Friedman, Gupta and Guralnick (Pacific J. Math.**181** (1997) 159-176). However, the technique requires k to be large and, as Pappacena points out, it is difficult to get a bound significantly below $O(n^{3/2})$ using only this technique.

Guterman and Markova have developed a powerful variant of this method.
Instead of considering the inclusion

$$\mathcal{L}^0(S) \sqsubseteq \mathcal{L}^1(S) \sqsubseteq ... \sqsubseteq \mathcal{L}^k(S) \sqsubseteq ... \tag{1}$$

for a generating set S of M_n, they choose a particular nonzero matrix B in M_n, whose expression in terms of monomials in S is known, and they consider the left ideal M_nB (and right ideal BM_n).

If B has rank r, then M_nB has dimension rn and the chain of subspaces of M_nB

$$\mathcal{L}^0(S)B \sqsubseteq \mathcal{L}^1(S)B \sqsubseteq ... \sqsubseteq \mathcal{L}^k(S)B \sqsubseteq ... \tag{1}$$

stabilizes ; in fact

$$\mathcal{L}^k(S)B = \mathcal{L}^{k+1}(S)B = M_nB,$$

for some $k \leq rn - 1$.
In particular, if B has rank one, then $\mathcal{L}^{n-1}(S)B = M_nB$.

If S contains an $n \times n$ matrix with n distinct eigenvalues, then using a similarity, we may assume that S contains a diagonal matrix D with distinct diagonal entries. But then, for each integer j with $1 \leq j \leq n$, there is a polynomial $f_j(x)$ of degree at most $n-1$ such that the matrix unit $E_{jj} = f_j(D)$, and taking $B = E_{jj}$ in (2) for $j = 1, \ \ldots \ n$, we immediately deduce that the length of S is at most $2n-2$, as first proved by Pappacena.

Similarly, if S contains a nonderogatory nilpotent matrix, one can assume that S contains the full nilpotent upper triangular Jordan block $J = J_n$, then $\mathcal{L}^{n-1}(S)J^{n-1} = M_n J^{n-1}$, $\mathcal{L}^{n-1}(S)J^{n-2}$ restricted to column $n-1$ is surjective, so that $\mathcal{L}^{n-1}(S)J^{n-2} + \mathcal{L}^{n-1}(S)J^{n-1} = M_n J^{n-2}$, similarly, $\mathcal{L}^{n-1}(S)J^{n-3}$ restricted to column $n-2$ is surjective and $\mathcal{L}^{n-1}(S)J^{n-3} + \mathcal{L}^{n-1}(S)J^{n-2} + \mathcal{L}^{n-1}(S)J^{n-1} = M_n J^{n-1}$, and continuing in this way, one concludes that $\mathcal{L}^{2n-2}(S) = M_n$. Using the Jordan canonical form, one can extend this argument to conclude that if S contains a nonderogatory matrix, then $\mathcal{L}^{2n-2}(S) = M_n$.

If $S = \{P, Q\}$ is a generating set for M_n with Q of rank one, then P is nonderogatory since otherwise the nullspace of Q would contain an eigenvector of P. Hence S has length at most $2n - 2$. This can also be seen from the fact that any monomial in P and Q involving two Qs is equal to one involving at most one Q, since Q has rank one.

Suppose that $S = \{A_1, A_2, \ \ldots \ , A_q\}$ is a generating set for M_n. Let $x_1, x_2, \ \ldots \ , x_q$ be distinct commuting indeterminates and consider the matrix $R = x_1A_1 + x_2A_2 + \ \ldots \ + x_qA_q$ over the rational function field $\mathbb{C}(x_1, x_2, , \ldots \ , x_q)$.

If R is nonderogatory, then there are specializations of the x_i for which the corresponding complex matrix is nonderogatory, and hence S has length at most $2n - 2$.

More generally, one can choose an integer $s \geq 1$ and a set of $s^{\frac{q((q^s-1)}{q-1}}$ distinct commuting indeterminates y_w, w running through the list of all words of positive degree at most s in q indeterminates and consider the matrix $R = \sum y_w w(A_1, \ \ ... \ , A_q)$, where $w(A_1, \ ... \ \ , A_q)$ is obtained from w by replacing corresponding indeterminates by $A_1, \ \ ... \ \ , A_q$. If R is nonderogatory over the rational function field $\mathbb{C}(\{y_w\})$,then a specialization R_0, say, of R is nonderogatory over the complex numbers. Then $S_0 = \{A_1, A_2, \ \ ... \ \ , A_q, R_0\}$ is a generating set for M_n containg the nonderogatory matrix R_0, so M_n is spanned by the monomials in S_0 of degree at most $2n-2$. Since R_0 can be expressed as a linear combination of monomials of degree at most s in the matrices $A_1, A_2, \ \ ... \ \ , A_q$, it follows that S has length at most $(2n-2)s$.

This leads to the following **problem**: Given a generating set $S = \{A_1, A_2, \quad \ldots \quad, A_q\}$ of M_n, determine the least integer s for which a linear combination of the monomials in $A_1, \quad \ldots \quad, A_q$ of degree at most s is nonderogatory.

Though the problem seems a natural one, I could not find it addressed in the literature. One would suspect that the answer should be $O(\ln n)$ and if so, one could deduce that the length of M_n is $O(n \ln n)$.

It appears to be difficult to find generating sets S of M_n for which the generic linear combination of the elements is derogatory. This occurs even in some sets S where the generators have low degree minimal polynomials.

The following example appears in my paper (LAMA **6** (1978) 269-305):
Let

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 4 & 0 & -2 & 0 & 0 \\ 1 & 1 & 0 & -1 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then $S = \{A, B\}$ generates M_6. Here $A^2 = B^3 = 0$ and all monomials $A^i B^j$ $(i \geq 1, j \geq 1)$ are nilpotent. Also $\det(xA + yB - zI) = z^6$. Despite this, $A + B$ is nonderogatory. The monomial $ABAB^2$is not nilpotent.

We now consider another special type of generating set for M_n. We know that if $S = \{P, Q\}$ generates M_n and P and Q are idempotents (or more generally have quadratic minimal polynomials), then $n = 2$. However, for every positive integer n, M_n can be generated by three idempotents. We now show that this can be done under the further restriction that some pair commutes.

Let J_n be the full nilpotent $n \times n$ upper triangular Jordan block and let P be the $n \times n$ matrix with odd numbered rows $1, 3, \ldots$ the same as the corresponding rows of $I_n + J_n$ and all other rows zero.

Let $Q = J_n + I_n - P$ and let $R = E_{n-11} + E_{n-1n-1} + E_{n2} + E_{nn}$, if $n \geq 4$ is even and $R = E_{n-11} + E_{n-1n-1} - E_{n1} + E_{nn}$ if $n \geq 3$ is odd.

Then P, Q, R are idempotents which generate M_n for $n \geq 3$ and $RP = PR$ if n is even, while $QR = RQ$, if n is odd. In this example, $P + Q$ is nonderogatory, so $S = \{P, Q, R\}$ has length at most $2n - 2$.

For example, for $n = 6$,

$$P = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$R = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

To see that $\{P, Q, R\}$ generates M_6, observe that if U is a nonzero invariant subspace of $\mathbb{C}^6$, then U must contain an eigenvector of $P + Q$, so U must contain the standard unit vector e_1 and therefore also $\mathrm{Re}_1 = e_5$ and applying powers of $P + Q$, we see that U must contain e_4,e_3, e_2 and $\mathrm{Re}_2 = e_6$, so $U = \mathbb{C}^6$.

One can also show that the full matrix algebra M_n ($n \geq 3$) can be generated by three idempotents by using

group representation theory as follows:
The symmetric group S_{n+1} of degree $n+1$ is generated by $\alpha = (1\ 2)$ and $\beta = (1\ 2\ \ \ldots\ \ n+1)$, and conjugation of β by

$$\begin{aligned}\gamma &= (2\ \ n+1)(3\ n)(4\ n-1)\ \ \ldots (\frac{n}{2}+1\ \frac{n}{2}+2),\ (n \text{ even})\\ &= (2\ \ n+1)(3\ n)(4\ n-1)\ \ \ldots\ (\frac{n+1}{2}\ \frac{n+5}{2}),\ (n \text{ odd}).\end{aligned}$$

yields β^{-1}. Now $\beta = \gamma\delta$, where γ and also $\delta = \beta^{-1}\gamma$ are involutions (that is, their squares equal the identity element).

Let P, Q, R be the permutation matrices corresponding to α, γ, δ, respectively. Then P, Q, R generate the group of all $(n+1) \times (n+1)$ permutation matrices. Each permutation matrix fixes the 'all ones' vector and its orthogonal (unitary) complement U, say, is $\{P, Q, R\}-$invariant. The space U is irreducible under the induced action and thus the restrictions of P, Q, R to U generate the full matrix algebra M_n. Since $(P+I)/2, (Q+I)/2$ and $(R+I)/2$ are idempotents, it follows that M_n is generated by three idempotents.

Note also that S_{n+1} is generated by $\beta = (1\ 2\ \ \ldots\ \ n)$ and $\epsilon = (1\ n+1)$.
Now, β can be written as the product $\gamma\delta$ of two involutions as above and, in the construction, γ and ϵ act on disjoint sets, so $\gamma\epsilon = \epsilon\gamma$. This yields another proof of the fact that M_n can be generated by three idempotents, some pair of which commute. In this and in the previous example, the generic linear combination of the generating set is nonderogatory.

We now consider a special situation.
Suppose that $n = 2t$ is even and that S is a generating set for M_n which contains a diagonalizable matrix with characteristic polynomial the square of its minimal polynomial. Using a similarity, we may assume that S contains the direct sum $N = \begin{pmatrix} D & 0 \\ 0 & D \end{pmatrix}$, where D is a $t \times t$ real diagonal matrix with distinct nonzero diagonal entries.

Then, for each integer j with $1 \leq j \leq t$, $E_{jj} + E_{t+jt+j}$ is a polynomial in N of degree at most t and $\mathcal{L}^{2n-1}(S)(E_{jj} + E_{t+jt+j}) = M_n(E_{jj} + E_{t+jt+j})$.
This implies that S has length less than $5n/2$ in this case.

A conjecture of Kippenhahn (1951) stated that if H and K are $n \times n$ Hermitian matrices for which $\{H, K\}$ generates M_n, then the matrix $xH + yK$ is nonderogatory over the function field $\mathbb{C}(x, y)$.
In 1983, counterexamples were constructed independently by Waterhouse and the speaker. Waterhouse's counterexamples have a higher power of z dividing $\det(zI - xH - yK)$ than divides the minimal polynomnial of $xH + yK$, while the speaker exhibited such a generating set $\{H, K\}$ in M_8 for which $\det(zI - xH - yK)$ is the square of the minimal polynomial of $xH + yK$.

Notice that had Kippenhahn's conjecture been correct, it would have implied that the length of a generating set $\{H, K\}$ of M_n with H and K Hermitian must have length at most $2n - 2$, but whether this bound holds is still not known.

We now show that counterexamples to Kippenhahn's conjecture with the characteristic polynomial of $xH + yK$ the square of its minimal polynomial are easy to construct for each even $m \geq 8$.

Let $m = 2n \geq 8$ be even and let D be a real diagonal $n \times n$ matrix with distinct nonzero diagonal entries.
Let S be a real symmetric $n \times n$ and $V = (I - iS)(I + iS)^{-1}$, where $i = \sqrt{-1}$.
So $V = V^T$ is unitary.
Let $\overline{V}$ be the complex conjugate of V, so $V^{-1} = \overline{V}$.
Let $\overline{V}DV = 2X + iQ$, where X and Q are real matrices. Then X is real symmetric and Q is real orthogonal.

Let $A = \begin{pmatrix} 0_n & X \\ -X & Q \end{pmatrix}$. Then A is real skewsymmetric.

Let $B = \begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}$ and $H = A^2$ and $K = AB + BA$. So

$$H = \begin{pmatrix} -X^2 & XQ \\ -QX & Q^2 - X^2 \end{pmatrix}, K = \begin{pmatrix} -2X & Q \\ -Q & -2X \end{pmatrix}.$$

Let $J = \begin{pmatrix} I_n & iI_n \\ iI_n & I_n \end{pmatrix}$. Then $J\overline{J} = 2I_n$ and

$$JK\overline{J} = \begin{pmatrix} -(2X + iQ) & 0 \\ 0 & -(2X - iQ) \end{pmatrix}.$$

Let $W = \begin{pmatrix} V & 0 \\ 0 & \overline{V} \end{pmatrix}$. Then $W^{-1} = \overline{W}$ and

$$K_1 = (WJ)K(WJ)^{-1} = \begin{pmatrix} -D & 0 \\ 0 & -D \end{pmatrix}.$$

Now for distinct commuting indeterminates u, v, consider the pencil $uA + vB$. For real specializations of u, v, $uA + vB$ is a real skewsymmetric matrix so it is diagonalizable with (since B is nonsingular) paired eigenvalies $\pm i\lambda$, for various real numbers λ. Hence the characteristic polynomial $\det(zI - (uA + vB)^2)$ is a perfect square in $\mathbb{R}[u, v, z]$. Since $(uA + vB)^2 = u^2H + uvK - v^2I$, it follows that $\det(zI - xH - yK)$ is a perfect square in $\mathbb{R}[x, y, z]$. Since K has n distinct eigenvalues, each with multiplicity two, it follows that $\det(zI - xH - yK) = f(x, y, z)^2$, where $f(x, y, z)$ is the minimal polynomial of $xH + yK$.

Since H and K are Hermitian, the algebra G generated by $\{H, K\}$ is semi-simple.
Hence if G is not M_{2n}, the centralizer of G contains a non-scalar matrix.
To determine whether G is M_{2n}, it suffices to do this for $(WJ)G(WJ)^{-1}$, the algebra generated by K_1 and

$$
\begin{aligned}
H_1 &= (WJ)G(WJ)^{-1} \\
&= (1/4)W \begin{pmatrix} Q^2 - (2X + iQ)^2 & (2X + iQ)Q - Q(2X - iQ) \\ ((2X - iQ)Q - Q(2X + iQ) & Q^2 - (2X - iQ)^2 \end{pmatrix} \\
&= (1/4) \begin{pmatrix} VQ^2\overline{V} - D^2 & DM - MD \\ D\overline{M} - \overline{M}D & \overline{V}Q^2V \end{pmatrix} \\
&= (1/4) \begin{pmatrix} VQ^2\overline{V} - D^2 & [D, M] \\ [D, \overline{M}] & \overline{V}Q^2V \end{pmatrix},
\end{aligned}
$$

where $M = VQV$, and $[D, M] = DM - MD$.

Now, since D has distinct diagonal entries, the centralizer of K_1 is the algebra of all $2n \times 2n$ matrices of the form

$$C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix},$$

where C_1, C_2, C_3, C_4 are $n \times n$ diagonal matrices.
So $\{H_1, K_1\}$ generates M_{2n} if and only if the only such matrices C which commute with H_1 are the scalar matrices.

We can choose D and S randomly and test whether the corresponding $\{H, K\}$ generates M_{2n} by solving the linear system $H_1 C = C H_1$ for C as above, where H, K transform to H_1, K_1, as above.
For example, taking $n = 4$ and

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}. \quad S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix},$$

one finds that the corresponding $\{H, K\}$ do generate M_8, while for the same D and

$$S = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

they do not.

For $n = 6$,

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 \end{pmatrix}, S = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$

the corresponding $\{H, K\}$ generates M_{12}.
By an earlier result, since H and K are Hermitian and the characteristic polynomial of the pencil $xH + yK$ is the square of its minimal polynomial, if $S = \{H, K\}$ generates M_{2n}, then S has length less than $5n/2$.