Journal of Statistical Physics, Vol. 118, Nos. 3/4, February 2005 (© 2005)
DOI: 10.1007/s10955-004-8829-x

On the Positivity of the Coefficients of a Certain Polynomial Defined by Two Positive Definite Matrices

Christopher J. Hillar[1] **and Charles R. Johnson**[2]

Received December 24, 2003; accepted September 15, 2004

It is shown that the polynomial

$$p(t) = \mathrm{Tr}[(A + tB)^m]$$

has positive coefficients when $m = 6$ and A and B are any two 3-by-3 complex Hermitian positive definite matrices. This case is the first that is not covered by prior, general results. This problem arises from a conjecture raised by Bessis, Moussa, and Villani in connection with a long-standing problem in theoretical physics. The full conjecture, as shown recently by Lieb and Seiringer, is equivalent to $p(t)$ having positive coefficients for any m and any two n-by-n positive definite matrices. We show that, generally, the question in the real case reduces to that of singular A and B, and this is a key part of our proof.

KEY WORDS: Bessis–Moussa–Villani conjecture; computational minimization; Hurwitz product; positive definite; trace, words in two matrices.

1. INTRODUCTION

In ref. 1, while studying partition functions of quantum mechanical systems, a conjecture was made regarding a positivity property of traces of matrices. If this property holds, explicit error bounds in a sequence of Padé approximants follow. Recently, in ref. 8, and as previously communicated to us,[(7)] the conjecture of[(1)] was reformulated as a question about the traces of certain sums of words in two positive definite matrices.

[1]Department of Mathematics, University of California, Berkeley, CA 94720; chillar@math.berkeley.edu
[2]Department of Mathematics, College of William and Mary, Williamsburg, VA 23187-8795; crjohnso@math.wm.edu

Conjecture 1.1. (BMV). The polynomial $p(t) = \mathrm{Tr}[(A + tB)^m]$ has all positive coefficients whenever A and B are n-by-n positive definite (PD) matrices.

The coefficient of t^k in $p(t)$ is the trace of $S_{m,k}(A, B)$, the sum of all words of length m in A and B, in which k B's appear (sometimes called the k-th Hurwitz product of A and B). In ref. 7, among other things, it was noted that, for $m < 6$, each constituent word in $S_{m,k}(A, B)$ has positive trace. Thus, the above conjecture is valid for $m < 6$ and arbitrary positive integers n. It was also noted in ref. 7 that the conjecture is valid for arbitrary m and $n < 3$. Thus, the first case in which prior methods do not apply and the conjecture is in doubt, is $m = 6$ and $n = 3$. Even in this case, all coefficients, except $\mathrm{Tr}[S_{6,3}(A, B)]$, are known to be positive (also as shown in ref. 7). Our purpose here is to show that the remaining coefficient $\mathrm{Tr}[S_{6,3}(A, B)]$ is nonnegative when A and B are 3-by-3 positive definite matrices, which requires notably different methods (some summands of $S_{6,3}(A, B)$ can have negative trace ref. 7). It follows that the conjecture is valid for $m = 6$, $n = 3$, our new result. A key tool is that it suffices to prove the conjecture for singular (positive semidefinite) matrices.

The coefficients $S_{m,k}(A, B)$ may be generated via the recurrence:

$$S_{m+1,k+1}(A, B) = S_{m,k}(A, B)B + S_{m,k+1}(A, B)A$$

(variants are available). The following lemma will be useful for computing the $S_{m,k}$. We give an algebraic proof although a purely combinatorial proof is also available.

Lemma 1.2. For any two n-by-n matrices A and B, we have

$$\mathrm{Tr}\left[S_{m,k}(A, B)\right] = \frac{m}{m-k}\mathrm{Tr}\left[A S_{m-1,k}(A, B)\right].$$

Proof.

$$\begin{aligned}
0 &= \mathrm{Tr}\left[\sum_{i=1}^{m} (A + tB)^{i-1} (A - A) (A + tB)^{m-i}\right] \\
&= \mathrm{Tr}\left[mA (A + tB)^{m-1}\right] - \mathrm{Tr}\left[\sum_{i=1}^{m} (A + tB)^{i-1} A (A + tB)^{m-i}\right] \\
&= \mathrm{Tr}\left[mA (A + tB)^{m-1}\right] - \mathrm{Tr}\left[\frac{d}{dy} (Ay + tB)^m\right]\Bigg|_{y=1} \\
&= \mathrm{Tr}\left[mA (A + tB)^{m-1}\right] - \frac{d}{dy}\left[\mathrm{Tr}\,(Ay + tB)^m\right]\Bigg|_{y=1}.
\end{aligned}$$

Since $S_{m,k}(Ay, B) = y^{m-k} S_{m,k}(A, B)$, it follows that the coefficient of t^k in the last expression above is just

$$m\mathrm{Tr}[AS_{m-1,k}(A, B)] - (m-k)\mathrm{Tr}[S_{m,k}(A, B)],$$

which proves the lemma. ▮

2. REDUCTION TO THE SINGULAR CASE

Of course, when A and B are Hermitian, $S_{m,k}(A, B)$ is Hermitian, but even when A and B are n-by-n real symmetric PD matrices, $n > 2$, $S_{m,k}(A, B)$ need not be PD. Examples are easily generated, and computational experiments suggest that it is usually not PD. We want to show that $\mathrm{Tr}[S_{6,3}(A, B)]$ is nonnegative for 3-by-3 positive definite A, B. This is subtle as $S_{6,3}(A, B)$ need not have positive eigenvalues, and as some words within the $S_{6,3}(A, B)$ expression can have negative trace.(7) A main component of our argument is based on the following technical observation.

Theorem 2.1. Let B be any real n-by-n matrix, and let $A = \mathrm{diag}(1, x_1, \dots, x_{n-1})$. Suppose that $\mathbf{a} = (a_1, \dots, a_{n-1}) \in [0, 1]^{n-1}$, and let $D = \mathrm{diag}(1, d_1, \dots, d_{n-1})$ be such that $d_i = 0$ if $a_i = 0$, and $d_i = 1$ otherwise. If $\mathbf{a}$ achieves the minimum of the function $f\colon [0, 1]^{n-1} \to \mathbb{R}$ given by $f(x_1, \dots, x_{n-1}) = \mathrm{Tr}[S_{m,k}(A, B)]$, then, with $A' = \mathrm{diag}(1, a_1, \dots, a_{n-1})$, we have

$$f(a_1, \dots, a_{n-1}) = \mathrm{Tr}[S_{m,k}(A', B)] = \frac{m}{m-k}\mathrm{Tr}\left[DS_{m-1,k}(A', B)\right].$$

Proof. Let A', B, D, and $\mathbf{a} = (a_1, \dots, a_{n-1}) \in [0, 1]^{n-1}$ be as in the hypotheses of the theorem. First suppose that $A' = D$. Then, it is clear that the formula in the theorem reduces to the identity in Lemma 1.2. When $A' \neq D$, consider the differentiable function g: $[-1/2, 1] \to \mathbb{R}$ given by

$$g(z) = \mathrm{Tr}\left[S_{m,k}\left(\frac{A' + zD}{1+z}, B\right)\right].$$

By hypothesis, $\mathbf{a} \in [0, 1]^{n-1}$ achieves the minimum for f. Consequently, it follows (from basic variational techniques) that

$$\left.\frac{dg(z)}{dz}\right|_{z=0} = 0. \tag{2.1}$$

Next, notice that,

$$\frac{d}{dz}\left[\mathrm{Tr}\left(\frac{A'+zD}{1+z}+tB\right)^m\right]=\mathrm{Tr}\left[\frac{d}{dz}\left(\frac{A'+zD}{1+z}+tB\right)^m\right]$$

$$=\mathrm{Tr}\left[\sum_{i=1}^{m}\left(\frac{A'+zD}{1+z}+tB\right)^{i-1}\frac{d}{dz}\left(\frac{A'+zD}{1+z}+tB\right)\left(\frac{A'+zD}{1+z}+tB\right)^{m-i}\right].$$

In particular, at $z=0$, the above expression evaluates to

$$\begin{aligned}
&\mathrm{Tr}\left[\sum_{i=1}^{m}\left(A'+tB\right)^{i-1}\left(D-A'\right)\left(A'+tB\right)^{m-i}\right]\\
&=\mathrm{Tr}\left[mD\left(A'+tB\right)^{m-1}\right]-\mathrm{Tr}\left[\sum_{i=1}^{m}\left(A'+tB\right)^{i-1}A'\left(A'+tB\right)^{m-i}\right] \quad (2.2)\\
&=\mathrm{Tr}\left[mD\left(A'+tB\right)^{m-1}\right]-\mathrm{Tr}\left[\tfrac{d}{dy}\left(A'y+tB\right)^{m}\right]\Big|_{y=1}\\
&=\mathrm{Tr}\left[mD\left(A'+tB\right)^{m-1}\right]-\tfrac{d}{dy}\left[\mathrm{Tr}\left(A'y+tB\right)^{m}\right]\Big|_{y=1}.
\end{aligned}$$

Finally, observe that $S_{m,k}(A'y, B)=y^{m-k}S_{m,k}(A', B)$ so that the coefficient of t^k in (2.2) is

$$m\mathrm{Tr}[DS_{m-1,k}(A', B)]-(m-k)\mathrm{Tr}[S_{m,k}(A', B)].$$

It follows, therefore, from (2.1) that

$$\mathrm{Tr}[S_{m,k}(A', B)]=\frac{m}{m-k}\mathrm{Tr}\left[DS_{m-1,k}(A', B)\right].$$

This completes the proof. ∎

Example 2.2. As an example of the theorem, let $m=4$, $n=3$, $k=2$, and

$$B=\begin{bmatrix}-2 & 1 & 0\\ -1 & 2 & 3\\ 1 & -1 & 3\end{bmatrix},\quad A=\begin{bmatrix}1 & 0 & 0\\ 0 & x_1 & 0\\ 0 & 0 & x_2\end{bmatrix}.$$

A straightforward computation gives us that

$$\begin{aligned}\mathrm{Tr}[S_{4,2}(A,B)] &= 20-4x_1+8x_1{}^2-12x_1x_2+42x_2{}^2,\\ \mathrm{Tr}[S_{3,2}(A,B)] &= 9+18x_2.\end{aligned}$$

The minimum of $\mathrm{Tr}[S_{4,2}(A,B)]$ is achieved by $x_1=7/25$, $x_2=1/25$, and one has

$$\mathrm{Tr}[S_{4,2}(A',B)]=2\mathrm{Tr}[S_{3,2}(A',B)]=\frac{486}{25}.$$

Let A, B, and f be as in Theorem 2.1. If we are fortunate enough that f achieves a minimum $f(\mathbf{a})$ with $\mathbf{a}\in(0,1]^{n-1}$, then D is the identity matrix and the theorem statement simplifies to the following.

Corollary 2.3. Suppose that f as in Theorem 2.1 achieves a minimum $f(\mathbf{a})$ with $\mathbf{a}\in(0,1]^{n-1}$. Then, the nonnegativity of $\mathrm{Tr}[S_{m-1,k}(A',B)]$ implies the nonnegativity of $\mathrm{Tr}[S_{m,k}(A',B)]$.

To see the importance of this corollary, we next examine the real version of Conjecture 1.1. Suppose we know that the conjecture is true for the power $m-1$ and also suppose (by way of contradiction) that there exist n-by-n real positive definite matrices A and B such that $\mathrm{Tr}[S_{m,k}(A,B)]$ is negative. Then, in particular, (by homogeneity) there are real positive definite A and B with norm 1 such that $\mathrm{Tr}[S_{m,k}(A,B)]$ is negative (here, we use the spectral norm ref. 5, p. 295 so that for positive semidefinite A, it is just the largest eigenvalue of A). Let M be the (compact) set of real positive semidefinite matrices with norm 1 and choose $(A,B)\in M\times M$ that minimizes $\mathrm{Tr}[S_{m,k}(A,B)]$; our goal is to show that this minimum is 0. By a uniform (real) unitary similarity we may assume that $A=\mathrm{diag}(1,a_1,\ldots,a_{n-1})$ is diagonal with $1\geqslant a_1\geqslant\cdots\geqslant a_{n-1}\geqslant 0$.

Corollary 2.3 then tells us that A must be singular, because by induction, $\mathrm{Tr}[S_{m-1,k}(A,B)]$ will be nonnegative for all positive semidefinite A and B. By symmetry, it also follows that B is singular. We combine these observations into the following theorem.

Theorem 2.4. Suppose that $\mathrm{Tr}\left[(A+tB)^{m-1}\right]$ has all positive coefficients for each pair of n-by-n real positive definite matrices A and B. If $p(t)=\mathrm{Tr}\left[(A+tB)^m\right]$ has all positive coefficients whenever $A,B\neq 0$ are singular n-by-n real positive semidefinite matrices, then $p(t)$ has all positive coefficients whenever A and B are arbitrary n-by-n real positive definite matrices.

3. SYMBOLIC REAL ALGEBRAIC GEOMETRY

In this section, we discuss the symbolic algebra preliminaries necessary for solving the $m=6$, $n=3$ case of Conjecture 1.1. Let $R=\mathbb{Q}[x_1,\ldots,x_n]$, and let I, J be two ideals of R. The *quotient ideal* of I by J is the ideal of R given by ref. 2, p. 23

$$(I:J)=\{f\in R: fg\in I \text{ for all } g\in J\}.$$

We can iterate this process to get the increasing sequence of ideals

$$I\subseteq(I:J)\subseteq(I:J^2)\subseteq(I:J^3)\subseteq\cdots.$$

This sequence stabilizes to an ideal called the *saturation* of I with respect to J (see ref. 9, p. 15):

$$(I, J^{\infty})=\{f\in R: \exists m\in\mathbb{N} \text{ with } f^m\cdot J\subseteq I\}.$$

If I is any ideal in R, let $V(I)$ denote the set,

$$V(I)=\{(a_1,\ldots,a_n)\in\mathbb{C}^n: f(a_1,\ldots,a_n)=0 \text{ for all } f\in I\}.$$

From these definitions, it is easily verified that for any two ideals, $I, J\subseteq R$,

$$V(I)\setminus V(J)\subseteq V(I:J^{\infty}).$$

For our particular application, we will be interested in proving that $V(I)\setminus V(J)$ contains no elements in $(0,1)^n$. Let P denote the saturation ideal $(I:J^{\infty})$. If we are fortunate enough to find that $P=\langle 1\rangle=\mathbb{Q}[x_1,\ldots,x_n]$, then there are no points in $V(I)\setminus V(J)$ (and hence none in $(0,1)^n$). One difficulty with this approach is that these new saturations do not always produce unit ideals. One more idea is needed, which we describe below.

If K is an ideal of R, the *elimination ideal* ref. 2, p. 25 of K with respect to x_i is $K_i=\mathbb{Q}[x_i]\cap R$. The x_i-coordinates of elements in $V(K)$ are elements in $V(K_i)$. For our purposes, we need only verify that for a saturation P, there is an elimination ideal P_i of P such that $V(P_i)$ contains no numbers in $(0,1)$.

Normally, a procedure such as the one outlined above would be relatively intractable (the symbolic algorithms are doubly exponential in nature). Our reductions give us enough efficiency to complete a proof computationally. We performed our computations using the symbolic algebra system Macaulay 2.

4. THE CASE $m = 6, n = 3$

The remainder of this article is devoted to a technical consideration of the case $m=6$, $k=3$, $n=3$ which is the content of the theorem below.

Theorem 4.1. The polynomial $p(t) = \mathrm{Tr}[(A + tB)^m]$ has positive coefficients when $m=6$ and A and B are any two 3-by-3 positive definite matrices.

Proof. Suppose that there exist 3-by-3 (complex Hermitian) positive definite matrices A and B such that $\mathrm{Tr}[S_{6,3}(A, B)]$ is negative; we will derive a contradiction. Performing a uniform unitary similarity and using homogeneity, we may assume that A and B are of the form,

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & s \end{bmatrix}, \quad B = \begin{bmatrix} a & x & z \\ \overline{x} & b & y \\ \overline{z} & \overline{y} & c \end{bmatrix},$$

in which $1 \geqslant r \geqslant s$, $a, b, c \geqslant 0$, and $x, y, z \in \mathbb{C}$. If $x, y, z \geqslant 0$, then we clearly have a contradiction. Otherwise, perform a simultaneous diagonal unitary similarity on A and B (a similarity by a diagonal matrix with entries on the complex unit circle) making $x, y \geqslant 0$. This does not change the trace of $S_{6,3}(A, B)$.

We next show that we may assume $z \in \mathbb{R}$. A computation of $\mathrm{Tr}[S_{6,3}(A, B)]$ reveals that it has the form $w = \alpha z\overline{z} + \beta z + \gamma \overline{z} + \delta$, in which $\alpha, \beta, \gamma, \delta \geqslant 0$. Since w is real, we have

$$\begin{aligned} w = \mathrm{Re}(w) &= \alpha z\overline{z} + \beta \mathrm{Re}(z) + \gamma \mathrm{Re}(\overline{z}) + \delta \\ &\geqslant \alpha \mathrm{Re}(z)^2 + \beta \mathrm{Re}(z) + \gamma \mathrm{Re}(z) + \delta. \end{aligned}$$

Consequently, it follows that we can assume z is real and negative. Theorem 2.4 now applies, so that it is enough to verify the claim with $s=0$ and $\det(B)=0$.

Since B is positive semidefinite, we have $ab - x^2 \geqslant 0$. If $b=0$, then $x=0$, and an easy computation shows that

$$\mathrm{Tr}[S_{6,3}(A, B)] = 6z^2c + 24az^2 + 20a^3 + 6r^3y^2c \geqslant 0,$$

a contradiction. Therefore, we must have $b > 0$. A similar computation also shows that $a, x, y > 0$.

Next, we prove that $c > 0$. Since

$$\det(B) = 2xzy + abc - ay^2 - x^2c - z^2b = 0,$$

it follows that when $c=0$, we have $2xyz=bz^2+ay^2$. From this, it is clear that $z<0$ is impossible, and therefore $z=0$, a contradiction. Finally, if $ab=x^2$, then from $\det(B)=0$, we have that $2xyz=bz^2+x^2y^2/b$. This implies again that $z=0$, another impossibility. Hence, $ab-x^2>0$.

Summarizing these observations, we may assume that

$$B=\begin{bmatrix} \frac{x^2+u^2}{b} & x & -z \\ x & b & y \\ -z & y & \frac{x^2y^2+u^2y^2+2xbzy+z^2b^2}{u^2b} \end{bmatrix}$$

in which $u,b,x,y>0$ and $z>0$. Furthermore, if $r=1$ or $r=0$, then ref. 4, Theorem 4 (along with a straightforward continuity argument) implies that $\mathrm{Tr}[S_{6,3}(A,B)]$ is nonnegative. Therefore, we may assume that $0<r<1$.

A direct computation shows that $b^3u^2\mathrm{Tr}[S_{6,3}(A,B)]$ is a polynomial $p(r,x,y,z,u,b)\in\mathbb{Z}[r,x,y,z,u,b]$. The negative terms in p factor as

$$-12b^3u^2xzy\left(r^2+r+1\right). \tag{4.1}$$

We shall verify that the minimum of $p(r,x,y,z,u,b)$ over $r,x,y,z,u,b\in[0,1]$ is 0, which will prove the claim (by homogeneity of the matrix B in the variables x,y,z,u,b).

If any of $x,y,z,u,$ or b is zero, then we are done by (4.1); therefore, we begin by determining the critical points of p in $(0,\infty)^6$. This amounts to a calculation of

$$D=\left\langle\frac{\partial p}{\partial r},\frac{\partial p}{\partial x},\frac{\partial p}{\partial y},\frac{\partial p}{\partial z},\frac{\partial p}{\partial u},\frac{\partial p}{\partial b}\right\rangle, \tag{4.2}$$

which is an ideal in the ring $\mathbb{Q}[r,x,y,z,u,b]$. We are interested in verifying that the set of points $V(D)\setminus V(rxyzub)$ contains no element in $(0,1)^6$. From the discussion in the previous section, it suffices to verify this claim for $V(D\colon\langle rxyzub\rangle^\infty)$.

Let $P=\left(D\colon\langle rxyzub\rangle^\infty\right)$. Using Macaulay 2, it can be checked that P is the unit ideal $\mathbb{Q}[r,x,y,z,u,b]$. It follows that the minimum of the function p above must occur when one of the x,y,z,u,b is 1 (in other words, on the "boundary").

This process now continues, recursively, by next finding the critical points of the functions $p(r,1,y,z,u,b),\ldots,p(r,x,y,z,u,1)$, and checking that they either do not occur in $(0,1)^5$ or that the function is nonnegative when they do. As noted before, a difficulty is that these new saturations do not always produce unit ideals. Therefore, we finish by showing that for each saturation P, there is an elimination ideal P_i of P such that $V(P_i)$ contains no positive numbers in $(0, 1)$. Since each P_i is generated by a single-variable polynomial, we use Sturm's algorithm to verify such a claim symbolically. These computations were also performed in Macaulay 2. This completes the proof of the theorem. ∎

As a final remark, we should note that there are some good tools for the numerical exploration of such problems. Namely, the program SOSTOOLS written by Prajna, Papachristodoulou, and Parrilo is an excellent resource for investigating real algebraic systems.[3]

REFERENCES

1. D. Bessis, P. Moussa, and M. Villani, Monotonic converging variational approximations to the functional integrals in quantum statistical mechanics, *J. Math. Phys.* **16**:2318–2325 (1975).
2. D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry* (Springer, New York, 1998).
3. C. Hillar, and C. R. Johnson, Symmetric word equations in two positive definite letters, *Proc. Ame. Math. Soc.* **132**:945–953 (2004).
4. C. Hillar, C. R. Johnson, and I. M. Spitkovsky, Positive eigenvalues and two-letter generalized words, *Electron. J. Linear Algebra* **9**:21–26 (2002).
5. R. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, New York, 1985).
6. R. Horn and C. R. Johnson, *Topics in Matrix Analysis* (Cambridge University Press, New York, 1991).
7. C. R. Johnson and C. Hillar, Eigenvalues of Words in Two Positive Definite Letters, *SIAM J. Matrix Anal. Appl.* **23**:916–928 (2002).
8. E. H. Lieb and R. Seiringer, Equivalent forms of the Bessis–Moussa–Villani conjecture, *J. Stat. Phys.*, **115**:185–190 (2004).
9. B. Sturmfels, *Solving Systems of Polynomial Equations, CBMS Regional Conference Series in Mathematics, 97*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, (American Mathematical Society, Providence, RI, 2002).

[3]http://www.cds.caltech.edu/sostools/