

EXTREMAL PROPERTIES OF OUTER POLYNOMIAL FACTORS

SCOTT MCCULLOUGH

(Communicated by Joseph A. Ball)

ABSTRACT. If $p(s)$ is a positive polynomial of degree $2d$, then its outer factor $q(s)$ has the property that the magnitude of each of its coefficients is larger than the magnitude of the corresponding coefficient of any other factor. In fact, this extremal property holds over vector-valued factorizations $r(s)^*r(s) = p(s)$. Corollaries include a result for symmetric functions and complex conjugate pairs.

0. INTRODUCTION

Let $p(z) = \sum_0^{2d} p_j z^j$ denote a monic polynomial of degree $2d$ in the complex variable z , $d \geq 2$. The polynomial p is positive if $p(s) \geq 0$ for all real s . In this case it is well known and easily seen that there exists a polynomial $r(s)$ of degree d with complex coefficients such that $\overline{r(s)}r(s) = p(s)$. Since p is real-valued, its zeros come in complex conjugate pairs, say $z_j^\pm = \alpha_j \pm i\beta_j$, $j = 1, 2, \dots, d$, where β_j are chosen to be nonnegative and the zeros are counted with multiplicity. The polynomial

$$(0.1) \quad q(z) = (z - z_1^-)(z - z_2^-) \cdots (z - z_d^-)$$

has all its zeros in the lower half-plane, and $q_*(z) = \overline{q(\bar{z})}$ has all of its zeros in the upper half-plane. The polynomials q and q_* are called the outer and *-outer factors of p respectively.

The outer and *-outer factors give rise to the factorization $q_*(z)q(z) = p(z)$ by noting that both sides are monic polynomials of degree $2d$ with the same zeros. Substituting real s for z gives

$$(0.2) \quad \overline{q(s)}q(s) = p(s).$$

A vector-valued polynomial $r(z) = \sum_0^d r_j z^j$ with $r_j \in \mathbb{C}^\ell$ (we may assume, without loss of generality, that $\ell \leq d+1$ since we may choose ℓ to be the dimension of the span of $\{r_j\}$) is a factor of p if

$$(0.3) \quad r(s)^*r(s) = \langle r(s), r(s) \rangle = p(s),$$

for s real. When $r_j \in \mathbb{C}$, r is called a scalar factor and it is easily seen that monic scalar factors are in one-to-one correspondence with choices of w_j , one from each

Received by the editors February 26, 2002 and, in revised form, November 1, 2002.

2000 *Mathematics Subject Classification*. Primary 47A68; Secondary 47A57.

Key words and phrases. Spectral factorization, outer factor, Hankel matrix, symmetric functions.

This research was supported by NSF grant DMS-9970347.

pair z_j^\pm , in much the same way that the outer and $*$ -outer factors are constructed. In particular, if $r(z) = \sum r_j z^j$ is a scalar factor of p and $q = \sum q_j z^j$ is the outer factor, then $|r_1| \leq |q_1|$ and $|r_{d-1}| \leq |q_{d-1}|$ with equality if and only if r is either q or q_* .

0.4 Theorem. *If $r = \sum r_j z^j$ is a factor of p , then, for each $1 \leq m \leq d-1$,*

$$r_m^* r_m \leq |q_m|^2.$$

Moreover, if r is a scalar factor and equality holds, then r is either q or q_ .*

Let M_d denote the $(d+1) \times (d+1)$ matrices with complex entries. We index M_d using $0 \leq j, k \leq d$ and $x \in \mathbb{C}^{d+1}$ by $0 \leq j \leq d$. Let \mathcal{H}_d denote the Hankel matrices in M_d . The proof of (0.4) depends upon the observation that p defines a positive linear functional ϕ_p on \mathcal{H}_d , that factors of p correspond to positive extensions of ϕ_p to all of M_d [5], and the representation theorem of Curto and Fialkow [2] for positive semi-definite Hankel matrices. While far from new [4], this point of view, admitting vector-valued (non-square) factors and identifying factors with positive semi-definite matrices, makes it possible to think of the factors as closed with respect to convex combinations.

Several classical results also point to the extremal nature of outer factors and provide contrast with (0.4). The book of Rosenblum and Rovnyak [7] contains elegant treatments of these topics. First, if r is a scalar factor and z is in the upper half-plane, then $|r(z)| \leq |q(z)|$. The inequality remains true for vector-valued factors r and can be proved with an easier version of the proof of (0.4). In the case of spectral factorization on the unit circle, the discrete time case, a result of Carathéodory (Theorem A of section 5.9 in [7]) says, for each k , that the sum of the squares of the first k terms of the outer factor dominates the sum of the squares for the first k terms of any other factor. The analogue of this result for the real line, continuous time case (Theorem C of section 5.10 in [7]), says that the integral of the norm squared up to time t of an output of the outer factor dominates the corresponding integral for the output of any other factor with the same input. The result of this paper may thus be viewed as giving a discrete time condition for the continuous time case.

Restricting (0.4) to scalar factors yields a corollary stated in terms of symmetric functions and complex conjugate pairs.

0.5 Corollary. *Let f_1, \dots, f_d denote the symmetric functions on d variables and suppose z_j^\pm , $j = 1, 2, \dots, d$, are complex conjugate pairs of points where z_j^+ has non-negative imaginary part. For each $1 \leq k \leq d$ and each choice of points $w_j \in \{z_j^\pm\}$,*

$$|f_k(w_1, \dots, w_d)| \leq |f_k(z_1^+, \dots, z_d^+)|.$$

The body of the paper is organized into five sections. The first contains some preliminary results about extensions of positive maps, positive maps on matrix spaces, and the representation theorem of Curto and Fialkow [2] for positive semi-definite Hankel matrices. This representation has the familiar look of a systems theory realization formula. If H is an $n \times n$ Hankel matrix, then there exists a self-adjoint $n \times n$ matrix S and vector γ such that $H_{j,\ell} = \gamma^* S^{j+\ell} \gamma$. Analogues in the case of several noncommuting variables of this realization formula play an important role in [3] and [5]. The connection between factorizations and positive completions is detailed in section two. That extremal positive extensions of ϕ_p

correspond to low-rank matrices is the topic of section three. Section four contains a proof of (0.4) obtained by combining results from the previous sections. Further results are briefly discussed in section five.

1. PRELIMINARIES

This section collects some mostly known facts formulated as needed for the proof of (0.4). The first subsection treats extensions of positive maps on selfadjoint subspaces of matrix spaces. A representation theorem for positive semi-definite Hankel matrices and a representation theorem for positive mappings on matrix spaces are the subjects of the second and third subsections respectively.

1.1. Extensions of positive maps. There are numerous results extending positive (linear) functionals on subspaces of linear spaces with a positive cone to positive functionals on the whole space. A version attributed to Krein suffices here. A subspace \mathcal{M} of M_m is selfadjoint if $\mathcal{M} = \mathcal{M}^* = \{M^* : M \in \mathcal{M}\}$. In this case let \mathcal{M}^+ denote the cone of positive semi-definite elements of \mathcal{M} . A linear map $\rho : \mathcal{M} \mapsto \mathbb{C}$ is positive, denoted $\rho \geq 0$, if $\rho(M) \geq 0$ whenever $M \geq 0$, where, for a matrix T , the notation $T \geq 0$ means that T is positive semi-definite.

1.1.1 Proposition. *If \mathcal{M} is a selfadjoint subspace of M_m , if \mathcal{M} contains a positive invertible matrix, and if $\rho : \mathcal{M} \mapsto \mathbb{C}$ is positive, then there exists a positive map $\rho' : M_m \mapsto \mathbb{C}$ such that $\rho'|_{\mathcal{M}} = \rho$.*

Sketch of proof. When \mathcal{M} contains the identity, the result can be found in [6]. Otherwise, let X^*X denote a positive invertible element of \mathcal{M} . Let $\mathcal{N} = X^{*-1}\mathcal{M}X^{-1}$. Then \mathcal{N} is selfadjoint and contains the identity and $\sigma : \mathcal{N} \mapsto \mathbb{C}$ defined by $\sigma(T) = \rho(X^*TX)$ is positive. Therefore, σ has a positive extension σ' to all of M_m and $\rho' : M_m \mapsto \mathbb{C}$ defined by $\rho'(T) = \sigma'(X^{*-1}TX^{-1})$ is a positive extension of ρ . □

Compare the following Proposition with the proof of Theorem 9.8 from [1].

1.1.2 Proposition. *Let \mathcal{M} denote a selfadjoint subspace of M_m containing a positive invertible element. If $\rho : \mathcal{M} \mapsto \mathbb{C}$ is linear, if $\rho(T) > 0$ for each nonzero $T \in \mathcal{M}^+$, and if $u \in M_m^+$, but $u \notin \mathcal{M}$, then there exists an S and a positive extension ρ' of ρ to all of M_m such that*

- (1) $S \in \mathcal{M}$ and $S - u \geq 0$;
- (2) $\rho(S) = \inf\{\rho(T) : T - u \geq 0, T \in \mathcal{M}^+\}$;
- (3) $\rho'(u) = \rho(S)$;
- (4) $\rho'(u) = \sup\{\tau(u) : \tau \text{ is a positive extension of } \rho\}$.

Moreover, if S satisfies (1) and (2) and if ρ' is a positive extension of ρ , then ρ' satisfies (3) if and only if ρ' satisfies (4).

Proof. The set \mathcal{S} over which the infimum in (2) is taken is nonempty since \mathcal{M}^+ contains an invertible element. It is also bounded below by 0. To see that the infimum is attained, choose a sequence $S_n \in \mathcal{M}^+$ such that $S_n - u \geq 0$ and $\rho(S_n)$ converges to the infimum. If $\{\|S_n\|\}$, where $\|S_n\|$ is the (any) norm of S_n , is not a bounded sequence, then it may be assumed that $\{\|S_n\|\}$ converges to infinity and $\frac{S_n}{\|S_n\|}$ converges to some $S_0 \in \mathcal{M}^+$ with $\|S_0\| = 1$. But then $\rho(\frac{S_n}{\|S_n\|})$ converges to both 0 and $\rho(S_0)$, contradicting the hypothesis that $\rho(T) > 0$ for nonzero $T \in \mathcal{M}^+$. This contradiction implies that the sequence $\{\|S_n\|\}$ is bounded and thus it may

be assumed that S_n converges to some $S \in \mathcal{M}^+$ so that $\rho(S_n)$ converges to both the infimum and $\rho(S)$.

Now that the existence of S is established, let $\mathcal{N} = \{T + \beta u : T \in \mathcal{M}, \beta \in \mathbb{C}\}$. It is readily verified that \mathcal{N} is selfadjoint and contains a positive invertible element. Define $\sigma : \mathcal{N} \mapsto \mathbb{C}$ by

$$\sigma(T + \beta u) = \rho(T) + \beta\rho(S).$$

Evidently σ is well defined and linear. To verify that σ is positive, suppose $T \in \mathcal{M}$, $\beta \in \mathbb{C} \setminus \{0\}$, and $T - \beta u \geq 0$. Since $T - \beta u$, u , and \mathcal{M} are selfadjoint and $u \notin \mathcal{M}$, it follows that β is real, since otherwise, $u = \frac{T^* - T}{\beta - \beta}$. By scaling, it may be assumed that β is either 1 or -1 . If $\beta = 1$, then, by (2), $\rho(T) \geq \rho(S)$ and $\sigma(T - u) = \rho(T) - \rho(S) \geq 0$. Now suppose $\beta = -1$. Adding $S - u \geq 0$ to $T + u \geq 0$ shows that $T + S \geq 0$. Thus, $\sigma(T + u) = \sigma(T + S) + \sigma(u - S) = \rho(T + S) \geq 0$, since $\sigma(S - u) = 0$ and ρ is positive.

An application of (1.1.1) to σ produces a positive extension ρ' of ρ defined on all of M_m with $\rho'(u) = \sigma(u) = \rho(S)$.

To finish the proof, suppose S satisfies (1) and (2) and $\hat{\rho}$ is a positive extension of ρ . If $\hat{\rho}(u) = \rho(S)$ and if τ is a positive extension of ρ , then

$$0 \leq \tau(S - u) = \rho(S) - \tau(u) = \hat{\rho}(u) - \tau(u).$$

On the other hand, if $\hat{\rho}(u) \geq \tau(u)$ for all positive extensions τ of ρ , then choosing $\tau = \rho'$, so that $\rho'(u) = \rho(S)$, gives

$$0 \leq \hat{\rho}(S - u) = \rho(S) - \hat{\rho}(u) \leq \rho'(u) - \rho'(u) = 0.$$

□

1.2. Positive Hankel matrices. Let \mathcal{H}_d denote the Hankel matrices in M_d . That is, $T \in \mathcal{H}_d$ if $T_{j,k}$ depends only on $j + k$. In particular, a Hankel matrix $T \in \mathcal{H}_d$ is determined by $2d + 1$ complex numbers t_0, \dots, t_{2d} by specifying $T_{j,k} = t_{j+k}$.

Each real number s determines a rank-one matrix $H_s = (s^{j+k})_{j,k=0}^d \in \mathcal{H}_d^+$. Let $H_\infty \in \mathcal{H}_d^+$ denote the rank-one matrix with a 1 in the (d, d) entry and zeros elsewhere.

1.2.1 Theorem. *If $T \in \mathcal{H}_d^+$, then there exists $s_0, \dots, s_d \in (-\infty, \infty]$ and nonnegative numbers $\alpha_0, \dots, \alpha_d$ such that*

$$S = \sum_0^d \alpha_j H_{s_j}.$$

Theorem (1.2.1) is essentially proven in [2]. Proofs of versions of (1.2.1) in several noncommuting variables can be found in [3] and [5].

Proof. Assume, without loss of generality, that $T_{0,0} > 0$. Let r denote the rank of the matrix $(T_{j,k})_{j,k=0}^{d-1}$. There is a nonnegative α_d such that $T - \alpha_d H_\infty$ is still in \mathcal{H}_d^+ and also has rank r . The results of [2] imply the existence of nonnegative numbers α_j and distinct real numbers s_j such that

$$T - \alpha_d H_\infty = \sum_0^{d-1} \alpha_j H_{s_j}.$$

□

1.2.2 Lemma. *If $k \leq d$, $s_0, \dots, s_k \in (-\infty, \infty]$ are distinct, and $\alpha_0, \dots, \alpha_k$ are strictly positive, then*

$$T = \sum_0^k \alpha_j H_{s_j}$$

has rank $k + 1$.

1.2.3 Corollary. *There exists a positive invertible $T \in \mathcal{H}_d$.*

1.3. Positive functionals on M_m . Using the trace, the dual of M_m is identified with M_m . Indeed, an $M \in M_m$ may be identified with the linear map $\rho_M : M_m \mapsto \mathbb{C}$ given by

$$(1.3.1) \quad \rho_M(T) = \text{tr}(MT).$$

Conversely, if $\rho : M_m \mapsto \mathbb{C}$ is linear, then $\rho = \rho_{M_\rho}$, where $M_\rho = (\rho(E_{j,k}))_{j,k}$. Here, and throughout, $E_{j,k}$ is the matrix unit with a 1 in the (j, k) entry and 0 elsewhere.

1.3.2 Proposition. *A linear map $\rho : M_m \mapsto \mathbb{C}$ is positive if and only if M_ρ is positive semi-definite.*

2. FACTORIZATIONS AND POSITIVE EXTENSIONS

The polynomial $p(s) = \sum p_j s^j$ determines a functional $\phi_p : \mathcal{H}_d \mapsto \mathbb{C}$ by

$$(2.1) \quad \phi_p(T) = \sum p_m t_m,$$

where $t_{j+k} = T_{j,k}$.

Given a polynomial $r = \sum_{j=0}^d r_j z^j$ with coefficients r_j in \mathbb{C}^ℓ , identify r with the $\ell \times (d + 1)$ matrix

$$(2.2) \quad r = \begin{pmatrix} r_0 & r_1 & \dots & r_d \end{pmatrix}.$$

2.3 Theorem. *If $r = \sum r_j z^j$ is a factor of p , then ρ_{r^*r} is a positive extension of ϕ_p . Conversely, if $\varphi : M_d \mapsto \mathbb{C}$ is a positive extension of ϕ_p , if P is the unique positive matrix such that $\varphi = \rho_P$, and if $r^*r = P$ is a factorization of P , then $r = \sum r_j z^j$ is a factor of p .*

Proof. For $0 \leq \mu \leq 2d$, let $F_\mu = \sum_{j+k=\mu} E_{j,k}$. The set $\{F_0, F_1, \dots, F_{2d}\}$ is a basis for \mathcal{H}_d . Observe that r is a factor of p if and only if for each μ , $\sum_{j+k=\mu} r_j^* r_k = p_\mu = \phi_p(F_\mu)$ and $P = r^*r$ extends ϕ_p if and only if for each μ ,

$$(2.3.1) \quad \begin{aligned} \phi_p(F_\mu) &= \rho_{r^*r}(F_\mu) \\ &= \text{tr}(r^*r \sum_{j+k=\mu} E_{j,k}) \\ &= \sum_{j+k=\mu} (r^*r)_{j,k} \\ &= \sum_{j+k=\mu} r_j^* r_k. \end{aligned}$$

□

There is some nonuniqueness in the correspondence between positive matrices P such that ρ_P extends ϕ_p and factors of p , since P may have many factorizations as $r^*r = P$. Theorem (0.4) is really a statement about the diagonal entries of P .

3. THE EXISTENCE OF LOW-RANK EXTENSIONS

Throughout this section we add to the hypotheses of (0.4) the technical hypothesis $p(s) > 0$ for all real s . The following is the main result of this section.

3.1 Proposition. *Fix $0 \leq \beta \leq 1$ and $1 \leq m < d - 1$ and let*

$$u = \beta E_{m,m} + (1 - \beta) E_{m+1,m+1}.$$

There exists a unique positive matrix P with real entries such that ρ_P extends ϕ_p and

$$\rho_P(u) = \sup\{\tau(u) : \tau \text{ is a positive extension of } \phi_p\}.$$

Moreover, the rank of P is at most two.

The proof of (3.1) occupies the remainder of this section and requires several preliminary lemmas.

Let \mathcal{P}_p denote the positive semi-definite matrices P such that ρ_P extends ϕ_p . When $P \in \mathcal{P}_p$ has rank one or two there are canonical choices for a corresponding factorization as in (2.3). If P has rank one, then simply factor $P = r^* r$ where r is a $(d + 1)$ (row) vector and, so that $r(z) = \sum r_j z^j$ is monic, choose $r_d = 1$. Of course the normalization $r_d = 1$ is possible since $P_{d,d} = p_{2d} = 1$. In this case there is just one such factor. If P has rank two and real entries, then the Cholesky algorithm applied from the bottom up, rather than the top down, uniquely determines vectors v and w with real entries, such that $v_d = 1$ (since $P_{d,d} = p_{2d} = 1$), $w_d = 0$, the last nonzero entry of w is positive, and

$$(3.2) \quad P = vv^* + ww^*.$$

Writing $v(z) = \sum v_j z^j$ and $w(z) = \sum w_j z^j$ generates two distinct scalar monic factors of p , namely $v(z) \mp iw(z)$.

Of course, if $r = w - iv$ is a scalar monic factor, then P as in (3.2) is in \mathcal{P}_p and has real entries and rank at most two. Furthermore, if r is the outer or $*$ -outer factor, then either $w_{d-1} \neq 0$ or p has only real roots.

3.3 Lemma. *The set of elements of \mathcal{P}_p with rank at most two and real entries is finite.*

Proof. In view of the preceding discussion, the mapping that sends the scalar monic factor $v - iw$ to $P = vv^* + ww^*$ as in (3.2) is onto the collection of $P \in \mathcal{P}_p$ with rank at most two and real entries. The result now follows from the fact that p has only finitely many scalar monic factors. \square

3.4 Lemma. *If $P_1, P_2 \in \mathcal{P}_p$, if P_1 has rank two, P_2 has rank at most two, and if both have real entries, then either for each $0 < \gamma < 1$, $Q_\gamma = \gamma P_1 + (1 - \gamma) P_2$ has rank exceeding two or $P_1 = P_2$.*

Proof. If, for some $0 < \gamma' < 1$, $Q_{\gamma'}$ has rank two, then the range of P_2 is a subset of the range of P_1 . It follows that for every $0 < \gamma < 1$, Q_γ has rank two and real entries. If $P_1 \neq P_2$, then $Q_\gamma \neq Q_\delta$ for $\gamma \neq \delta$ in which case the set of $P \in \mathcal{P}_p$ with rank two and real entries is infinite, a contradiction of (3.3). \square

3.5 Lemma. *There is at most one $P \in \mathcal{P}_p$ with rank one and real entries.*

Proof. Such a P corresponds to a scalar monic factor r of p with real coefficients. Thus, $r(s)^2 = p(s)$ for real s and $P = r^*r$. If $Q \in \mathcal{P}_p$ also has rank one and real entries, then, letting a denote the corresponding factor, $a(s)^2 = p(s)$ for real s . Thus $(a - r)(a + r) = 0$, from which it follows that $r = \pm a$. Since both a and r are monic, $a = r$ and thus $P = r^*r = a^*a = Q$. \square

3.6 Lemma. *If $f(s) = \sum_0^d f_j s^j$ is real-valued, if f has at least d distinct real roots, and if there is an $0 \leq m < d$ such that $f_m = f_{m+1} = 0$, then f is identically zero.*

Proof. The polynomial $f^{(m)}$, the m -th derivative of f , has at least $d - m$ distinct real roots, a double root at 0, and degree at most $d - m$. Hence $f^{(m)}$ is identically zero. It follows that f is a polynomial of degree $m < d$ with d zeros and is thus identically zero. \square

3.7 Lemma. *If $f(s) = \sum_0^d f_j s^j$ is real-valued, has at least $d - 1$ distinct real roots, and if there exists an $0 < m < d$ such that $f_m = f_{m+1} = 0$, then f is identically zero.*

Proof. Note that f has d real roots counting multiplicity, either all distinct, or $d - 1$ distinct of which $d - 2$ have multiplicity one and of which one has multiplicity two. In either case, f' is a real-valued polynomial of degree $d - 1$ with $d - 1$ distinct real roots and, since $m > 0$, consecutive zero coefficients. Hence, by (3.6), f' is identically zero. It follows that f is identically zero. \square

The hypotheses of (3.1) are in force for the remainder of this section. Observe that (1.2.1) and the hypothesis $p(s) > 0$ for all real s (and p actually has degree $2d$) implies that $\phi_p(T) > 0$ for all nonzero T in \mathcal{H}_d^+ . Thus, since $u \notin \mathcal{H}_d$ and $u \geq 0$, (1.1.2) implies that there exists an $S \in \mathcal{H}_d^+$ such that $S - u \geq 0$ and

$$(3.8) \quad \phi_p(S) = \inf\{\phi_p(T) : T \in \mathcal{H}_d^+, T - u \geq 0\}.$$

The argument that the rank of $S - u$ is at least $d - 1$ splits into the cases $\beta = 1$ (same as $\beta = 0$) and $0 < \beta < 1$.

3.9 Lemma. *If $u = E_{m,m}$ ($\beta = 1$) and $1 \leq m < d$, then the rank of S is at least d .*

Proof. Let k denote the rank of S and suppose $k < d$. By (1.2.1) and (1.2.2), there exist distinct s_1, \dots, s_k in $(-\infty, \infty]$ and strictly positive numbers $\alpha_1, \dots, \alpha_k$ such that

$$(3.9.1) \quad S = \sum_1^k \alpha_j H_{s_j}.$$

Since S has rank k , $\ker(S)$, the kernel of S , has dimension $d + 1 - k$. Furthermore, since S has real entries, this kernel is closed under entry-wise conjugation: If x is in the kernel, then \bar{x} is also in the kernel. Finally, since $S - u \geq 0$, $ux = 0$ for x in $\ker(S)$; equivalently, $x_m = 0$.

For now, assume that each s_j is finite. There are two cases. First, suppose $k \geq m$. If $k = d - 1$, let $\mathcal{N} = \{h \in \mathbb{C}^{d+1} : h_{m+1} = 0\}$; otherwise, let $\mathcal{N} = \{h \in \mathbb{C}^{d+1} : h_d = h_{d-1} = \dots = h_{k+2} = h_{m+1} = 0\}$. Since the dimension of \mathcal{N} is $k + 1$ and the dimension of $\ker(S)$ is $d - k + 1$, and these are subspaces of a $(d + 1)$ -dimensional space, there exists a nonzero x in the intersection $\ker(S) \cap \mathcal{N}$. Thus, $x_m = x_{m+1} = 0$ and $x_j = 0$ for $j \geq k + 2$. Since $\ker(S)$ and \mathcal{N} are closed under

entry-wise conjugation, so is the intersection, and thus it may be assumed that x has real entries. The condition $Sx = 0$ implies, in view of (3.9.1) and the nature of the H_s , that

$$(3.9.2) \quad \sum_{\nu=0}^{k+1} x_{\nu} s_j^{\nu} = 0, \quad j = 1, \dots, k.$$

Hence the polynomial $\sum_0^{k+1} x_{\nu} s^{\nu}$ is real-valued, has k distinct real zeros, and consecutive zero coefficients. Therefore, by (3.7), x is identically zero, a contradiction.

Next, suppose $k < m$. In this case let $\mathcal{N} = \{h : h_d = \dots = h_{m+1} = h_{m-1} = \dots = h_k = 0\}$. Since the dimension of \mathcal{N} is $k + 1$, it follows that there is a nonzero $x \in \ker(S) \cap \mathcal{N}$. In particular, $x_j = 0$ for $j \geq k$. This time, from (3.9.1) and the nature of the H_s , the condition $Sx = 0$ implies that the real-valued polynomial $\sum_0^{k-1} x_{\nu} s^{\nu}$ has k distinct real zeros so that we again obtain the contradiction $x = 0$.

Finally, suppose $s_k = \infty$. It then follows, if x is in the kernel of S , then $x_d = 0$ in addition to $x_m = 0$.

If $k = d - 1 = m$, then there exists an $0 \neq x \in \ker(S)$ such that $x_{m-1} = 0$. Thus the polynomial $\sum_{\nu=0}^{k-2} x_{\nu} s^{\nu}$ has the $k - 1$ real zeros s_1, \dots, s_{k-1} and therefore $x = 0$. If $k = d - 1 > m$, then there is an $0 \neq x \in \ker(S)$ with real entries such that $x_{m+1} = 0$. Thus the real-valued polynomial $\sum_{\nu=0}^k x_{\nu} s^{\nu}$ has $k - 1$ distinct real zeros and consecutive zero coefficients ($0 < m < k$) and thus $x = 0$. If $d - 1 > k > m$, then there exists an x in the kernel of S with real entries such that $x_{d-1} = \dots = x_{k+1} = x_{m+1} = 0$. The real-valued polynomial $\sum_{\nu=0}^k x_{\nu} s^{\nu}$ has the $k - 1$ distinct real zeros s_1, s_2, \dots, s_{k-1} and consecutive zero coefficients ($0 < m < k$). Thus, by (3.7), $x = 0$. If $k \leq m$, then there exists an x in the kernel of S such that $x_{d-1} = \dots = x_{m+1} = x_{m-1} = \dots = x_{k-1} = 0$. The polynomial $\sum_{\nu=0}^{k-2} x_{\nu} s^{\nu}$ has $k - 1$ zeros and is thus identically zero, a contradiction. \square

3.10 Lemma. *Suppose $0 < \beta < 1$ and $0 < m < d - 1$. If $u = \beta E_{m,m} + (1 - \beta)E_{m+1,m+1}$, then the rank of S is $d + 1$.*

Proof. Let k denote the rank of S and suppose $k \leq d$. Represent S just as in (3.9). Since S is $(d + 1) \times (d + 1)$ and has rank k , $\ker(S)$ has dimension $d - k + 1$. Since $S - u \geq 0$, $ux = 0$ for x in $\ker(S)$; equivalently, $x_m = x_{m+1} = 0$. For now, assume that each s_j is finite. There are some cases. If $k = d$, then there exists $x \neq 0$ with real entries in the kernel of S such that $x_m = x_{m+1} = 0$. It follows that the real-valued polynomial $\sum_0^d x_{\nu} s^{\nu}$ has d distinct real zeros and consecutive zero coefficients and is therefore, by (3.6), identically zero. If $m < k < d$, then there is an $x \neq 0$ in the kernel of S with real entries such that $x_d = \dots = x_{k+1} = 0$. Thus, since $Sx = 0$, the real-valued polynomial $x(s) = \sum_0^k x_{\nu} s^{\nu}$ has k distinct real zeros and consecutive zero coefficients and consequently, by (3.6), $x = 0$. If $k \leq m < d$, then there exists $x \neq 0$ in the kernel of S such that $x_d = \dots = x_{m+2} = x_{m-1} = \dots = x_{k-1} = 0$. In this case, the real-valued polynomial $\sum_0^{k-2} x_{\nu} s^{\nu}$ has k real zeros. Thus x is identically zero.

The argument for the case that $s_k = \infty$ is similar to that above and omitted. \square

3.11 Lemma. *If $P \in \mathcal{P}_p$ and if $\rho_P(u) = \phi_p(S)$, then the rank of P is at most two.*

Proof. If u is as in (3.9), then, since the rank of S is at least d and the rank of u is one, the rank of $S - u$ is at least $d - 1$. If u is as in (3.10), then, since the rank of

S is $d + 1$ and the rank of u is two, the rank of $S - u$ is at least $d - 1$. If $P \in \mathcal{P}_p$ and $\rho_P(u) = \phi_p(S)$, then

$$(3.11.1) \quad 0 = \rho_P(S - u) = \text{tr}(P(S - u)).$$

Since $S - u$ and P are positive semi-definite and the rank of $S - u$ is at least $d - 1$, (3.11.1) implies that the rank of P is at most two. \square

Proof of (3.1). By (1.3.1) and (1.1.2), there exists a $Q \in \mathcal{P}_p$ such that $\rho_Q(u) = \phi_p(S)$. Furthermore, since ρ_Q extends ϕ_p , for each $0 \leq m \leq 2d$,

$$(3.1.1) \quad p_m = \sum_{j+k=m} Q_{j,k}.$$

Consequently, since each p_m is real, if we let \overline{Q} denote the entry-wise complex conjugate of Q , then $\rho_{\overline{Q}}$ is also a positive extension of ϕ_p . Furthermore, since $\rho_Q(u) = \beta Q_{m,m} + (1 - \beta)Q_{m+1,m+1}$ and the diagonal entries of Q are real, $\rho_{\overline{Q}}(u) = \rho_Q(u) = \phi_p(S)$. It follows that $P = \frac{1}{2}(Q + \overline{Q}) \in \mathcal{P}_p$ has real entries, and $\rho_P(u) = \phi_p(S)$. By the moreover part of (1.1.2), $\rho_P(u)$ is equal to the supremum in (3.1). This establishes the existence part of (3.1). Furthermore, by Lemma (3.11), the rank of P is at most two, which establishes the moreover part of (3.1) once the uniqueness has been proved.

To see that P is unique, suppose $R \in \mathcal{P}_p$ has real entries and $\rho_R(u)$ is the supremum in (3.1). From the moreover part of (1.1.2), $\rho_R(u) = \phi_p(S)$. For each $0 \leq \gamma \leq 1$, $Q_\gamma = \gamma P + (1 - \gamma)R \in \mathcal{P}_p$ has real entries, and $\rho_{Q_\gamma}(u) = \phi_p(S)$. Hence, by (3.11), the rank of Q_γ is at most two. In view of (3.4), either $P = R$ or both Q and R must have rank one. However, if both Q and R have rank one, then (3.5) implies that $P = R$. \square

4. THE EXTREMAL PROPERTY

This section contains the proof of (0.4). The theorem is first proved under the added hypothesis $p(s) > 0$ for all real s .

Write the outer factor q of p in terms of its real and imaginary parts as $q = a - ib$ and let $Q = aa^* + bb^*$ as in (3.2). Given $P \in \mathcal{P}_p$ with real entries and rank at most two, let $r = v - iw$ denote the corresponding scalar factor of p as in (3.2). It follows that $P_{d-1,d-1} \leq Q_{d-1,d-1}$ with equality if and only if r is either q or q_* . An application of (3.1) now proves (0.4) for the case $m = d - 1$.

Arguing by induction, suppose that the result has been proven for $m + 1 \leq d - 1$. For $0 \leq \beta \leq 1$, let $u_\beta = \beta E_{m,m} + (1 - \beta)E_{m+1,m+1}$ and let P_β denote the unique element of \mathcal{P}_p with real entries such that

$$(4.1) \quad \rho_{P_\beta}(u_\beta) = \sup\{\tau(u_\beta) : \tau \text{ is a positive extension of } \phi_p\}.$$

In particular, the induction hypothesis is $Q = P_0 = aa^* + bb^*$ and we are to show $P_1 = Q$.

For $\delta \in [0, 1]$, let $C_\delta = \{\beta : P_\beta = P_\delta\}$. Note, either $C_\gamma = C_\delta$ or the sets are disjoint. Furthermore, the sets C_δ are closed: If $\beta_n \in C_\delta$ and converges to β_0 , then

$$(4.2) \quad \rho_{P_\delta}(u_{\beta_n}) (= \rho_{P_{\beta_n}}(u_{\beta_n})) \geq \rho_{P_{\beta_0}}(u_{\beta_n}).$$

By the continuity ρ_{P_δ} and ρ_{P_β} the inequality holds with n replaced by 0 and thus $\rho_{P_\delta} = \rho_{P_{\beta_0}}$, which means $P_\delta = P_{\beta_0}$ so that $\beta_0 \in C_\delta$.

Since, according to (3.3), there are only finitely many $P \in \mathcal{P}_p$ with rank at most two and real entries, the union $[0, 1] = \bigcup_{\delta} C_{\delta}$ is actually a finite union of disjoint closed sets. Since $[0, 1]$ is connected and each C_{δ} is nonempty, all the C_{δ} are the same. Thus, $C_0 = C_1$, which now proves $P_1 = P_0 = Q$ and establishes (0.4) under the added hypothesis $p(s) > 0$ for all real s .

To finish the proof, given p with $p(s) \geq 0$ for all s and $\delta > 0$, let q_{δ} denote the outer factor of $(p + \delta)(s) = p(s) + \delta$ and, as always, let q denote the outer factor of p . Using Hurwitz's Theorem, $|(q_{\delta})_m|$ converges to $|q_m|$. If $P \in \mathcal{P}_p$, then $P + \delta E_{0,0} \in \mathcal{P}_{p+\delta}$ so that by what has already been proved, for $1 \leq m \leq d - 1$,

$$(4.4) \quad P_{m,m} = (P + \delta E_{0,0})_{m,m} \leq |(q_{\delta})_m|^2.$$

Letting δ tend to 0 finishes the proof.

5. REMARKS

A variant of the proof of (0.4) proves the following version of the well-known fact that if $p(s) \geq 0$ for all s , if q is the outer factor of p , and if r is another scalar factor of p , then $|r(z)| \leq |q(z)|$ for all z in the upper half-plane.

5.1 Proposition. *If r is any factor of p and z is in the upper half-plane, then*

$$r(z)^*r(z) \leq |q(z)|^2.$$

To see that the supremum of $\{r(z)^*r(z) : r \text{ is a factor of } p\}$ is attained at a scalar factor, assume $p(s) > 0$ for all real s and let $z \in \mathbb{C} \setminus \mathbb{R}$ be given. With the notation $u = (z^j \bar{z}^k)_{j,k=0}^d$, There exists an $S \in \mathcal{P}_p$ such $S - u$ is positive semi-definite and

$$(5.1.1) \quad \phi_p(S) = \sup\{\tau(u) : \tau \text{ is a positive extension of } \phi_p\}.$$

Verify that the rank of S is $d + 1$. For instance, if the rank of S is d , then $S = \sum_1^d \alpha_j H_{s_j}$ for some strictly positive α_j and distinct s_j in $(-\infty, \infty]$. Furthermore, there is a nonzero vector x in the kernel of S . Since u and $S - u$ are positive semi-definite, $ux = 0$ also. Thus the polynomial $\sum_0^d x_j s^j$ has the $d + 2$ distinct zeros $s_1, \dots, s_d, z, \bar{z}$. Thus $x = 0$, a contradiction. Since the rank of S is at least d , if ρ_P is any positive extension of ϕ_p with $\rho_P(u) = \phi_p(S)$, then P has rank one. Note this argument does not require the overhead of section three.

A conjecture which would immediately imply (0.4) is: if $\phi : \mathcal{H}_d \mapsto \mathbb{C}$ is positive, and if ρ_P extends ϕ , then $P = \sum \alpha_j P_j$ where each P_j is rank one, $\alpha_j \geq 0$, $\sum \alpha_j = 1$, and ρ_{P_j} extends ϕ .

For the case of the unit circle there is an analogue of (5.1) that generalizes the classical result found in [7].

REFERENCES

1. J. B. Conway, *A course in functional analysis*, Graduate Texts in Mathematics, No. 96, Springer-Verlag, New York, 1990. MR **91e**:46001
2. R. E. Curto and L. A. Fialkow, *Recursiveness, positivity, and truncated moment problems*, Houston J. Math **17** (1991), 603–635. MR **93a**:47016
3. J. W. Helton, *Positive non-commutative polynomials are sums of squares*, Ann. of Math. (2) **156** (2002), 675–694.
4. A. Lindquist, G. Michaletzky and G. Picci, *Zeros of spectral factors, the geometry of splitting subspaces, and the algebraic Riccati inequality*, SIAM J. Control Optim. **33** (1995), 365–401. MR **95m**:93073

5. S. McCullough, *Factorization of operator-valued polynomials in several non-commuting variables*, *Linear Algebra Appl.* **326** (2001), 193–203. MR **2002f**:47035
6. V. I. Paulsen, *Completely bounded maps and dilations*, Pitman Research Notes in Mathematics Series, vol. 146, Longman Scientific and Technical, Harlow; John Wiley and Sons, Inc., New York, 1986. MR **88h**:46111
7. M. Rosenblum and J. Rovnyak, *Hardy classes and operator theory*, Oxford University Press, 1985. MR **87e**:47001

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF FLORIDA, GAINESVILLE, FLORIDA 32611-8105
E-mail address: sam@math.ufl.edu