Non-negative hereditary polynomials in a free $*-$algebra

J.William Helton * Scott A. McCullough † Mihai Putinar ‡

April 5, 2004

Abstract

We prove a non-negative-stellensatz and a null-stellensatz for a class of polynomials called hereditary polynomials in a free $*$-algebra over the real field.

1 Introduction and main result

This note is concerned with sums of squares decompositions in a free $*$-algebra. Already quite a few facts about such decompositions are known, see [3, 4, 5] and the references cited there. In particular, the article [4] contains a simple example showing that no analogue of the real nullstellensatz, as known in real algebraic geometry, exists. Another divergence between the commutative and the free $*$ theories was singled out in [5], where a stronger than expected non-negative-stellensatz with prescribed supports was proved. We consider below another fortunate free $*$-algebra case, when both a simple non-negative-stellensatz and a nullstellensatz hold. The proofs are based on the same principles as before ([4, 5]) : Carathéodory's theorem about convex hulls, Minkowski's separation theorem and a general Gelfand-Naimark-Segal construction.

The notation of the article [5] will be used throughout the note. Specifically, $\mathcal{P}$ is the ring of polynomials over the real field, in the non-commuting

*Partially supported by NSF, DARPA and Ford Motor Co.
†Partially supported by NSF grant DMS-0140112
‡Partially supported by NSF grant DMS-0100367

variables $(x, x^T) = \{x_1, x_2, \ldots, x_n, x_1^T, \ldots, x_n^T\}$. The involution on the algebra $\mathcal{P}$ works as expected:

$$(x_k)^T = x_k^T, \quad (x_k^T)^T = x_k, \quad 1 \leq k \leq n,$$

and

$$(uv)^T = v^T u^T,$$

for any words u, v in the free variables.

We call a polynomial belonging to $\mathcal{P}$ **analytic** provided it contains no transposes. The corresponding space is denoted by $\mathcal{A}$. Similarly, we call a polynomial **hereditary** provided all transposes x_k^T appear to the left of x_j's in any monomial. The corresponding space will be denoted by $\mathcal{H}$. The notion of hereditary polynomial has appeared in Agler's work on the dilation theory of linear operators, [1].

By definition, $\mathcal{P}_d$ is the finite dimensional subspace of $\mathcal{P}$ consisting of all polynomials of degree less than or equal to d. We also introduce notation for various classes of polynomials of degree less than or equal to d:

$$\mathcal{A}_d = \mathcal{A} \cap \mathcal{P}_d$$

and similarly for a subset $B \subset A$ we put:

$$B_d = B \cap \mathcal{P}_d.$$

We denote by $\mathcal{H}_{2d}$ the vector space, over the reals, generated by $\mathcal{A}_d^T \mathcal{A}_d$. Thus, $\mathcal{H}_{2d}$ is the vector space of polynomials of the form

$$q = \sum_{u,w} q_{u,w} u^T w, \quad q_{u,w} \in \mathbf{R},$$

where the sum is over words u, w of length at most d is the variables x.

In the following $p_1, ..., p_m \in \mathcal{A}$ will always denote analytic polynomials. The **left ideal** in the algebra $\mathcal{A}$ generated by them is

$$(p) := \{\sum r_j p_j : r_j \in \mathcal{A}\};$$

we consider the associated **symmetrized space**:

$$sym(p) := \{\sum r_j^T f_j + f_j^T r_j : r_j \in \mathcal{A},\ f_j \in (p)\}.$$

The point evaluations in commutative algebraic geometry are replaced in this framework by evaluations on n-tuples of finite matrices. Specifically, consider an arbitrary positive integer N, and let $X = (X_1, X_2, \dots, X_n)$ be $N \times N$ square matrices with real entries, regarded as linear transformations acting on the vector space $\mathbf{R}^N$. Then X^T is the tuple of transposes of these matrices. Thus, for an element $h \in \mathcal{P}$, the **evaluation** $h(X)$ makes sense, and produces a real $N \times N$ matrix. One step further, the **zero set** V_h of an m-tuple $h = (h_1, h_2, \dots, h_m)$ of elements of $\mathcal{P}$ is the collection of all pairs (X, v) with X an n-tuple of real $N \times N$ matrices, and a vector $v \in \mathbf{R}^N$, satisfying $h_k(X)v = 0,\ 1 \le k \le m$, with N an arbitrary integer. The same definition applies to any left ideal I of $\mathcal{P}$ or $\mathcal{A}$, and produces a zero set V_I. As a matter of fact, $V_h = V_{\mathcal{A}h_1+\dots+\mathcal{A}h_m} = V_{\mathcal{P}h_1+\dots+\mathcal{P}h_m}$.

The main result of this note is the following theorem. A few extensions are given in Section 3.

Theorem 1.1 *Let $p = (p_1, \dots, p_m) \in \mathcal{A}^m$ be an m-tuple of analytic polynomials. If a symmmetric hereditary polynomial $q \in \mathcal{H}$ has*

$$\langle q(X)v, v\rangle \ge 0$$

on all pairs (X, v) satisfying $p_\ell(X)v = 0$ $(1 \le \ell \le m)$, then:

$$(a) \qquad q = \sum_{j=1}^{k} f_j^T f_j + g, \tag{1}$$

where $g \in sym(p)$ and $f_j \in \mathcal{A},\ 1 \le j \le k$.

(b) If instead, $\langle q(X)v, v\rangle = 0$, for every (X, v) satisfying $p_\ell(X)v = 0, 1 \le \ell \le m$, then $q \in sym(p)$.

Acknowledgement. We are grateful to the anonymous referee for his critical and constructive comments.

2 Proofs

2.1 Zeroes and Ideals

Throughout this section p is an m-tuple of analytic polynomails. As before, V_p represents its associated zero set of pairs (X, v), where X is an n-tuple of real $N \times N$ matrices, $v \in \mathbf{R}^N$, and $N \in \mathbf{N}$. The next result is a nullstellensatz proved by G. Bergman, see [4] for details.

Lemma 2.1 *If $a \in \mathcal{A}$ and $V_p \subset V_a$, then $a = \sum r_j p_j$ for some analytic polynomials $r_j \in \mathcal{A}$.*

If a and the components p_j of p have degree no greater than d, then the inclusion $V_p \subset V_a$ in the hypothesis need only to be verified on n-tuples of $N \times N$ matrices with $N = (d+1)^2$.

Based on the above lemma we immediately derive part (b) of Theorem 1.1, as follows.

2.2 Proof of Theorem 1.1.(b)

Lemma 2.2 *If $f_j \in \mathcal{A}$, $1 \leq j \leq k$, are analytic polynomials and*

$$\sum_{j=1}^{k} f_j^T f_j + g = 0 \quad on\ V_p,$$

with $g \in sym(p)$, then $f_j \in (p)$, $1 \leq j \leq k$.

Proof: Write $g = \sum (r_j^T g_j + g_j^T r_j)$, where $r_j \in \mathcal{A}$ and $g_j \in (p)$. The conditions $p_j(X)v = 0, 1 \leq j \leq k$, imply $g_j(X)v = 0$, $1 \leq j \leq k$, thus

$$\sum \langle r_j^T(X) g_j(X)v, v\rangle = 0 \quad \text{and} \quad \sum \langle g_j(X)^T r_j(X)v, v\rangle = 0.$$

Therefore $\sum_{j=1}^{k} \langle f_j(X)^T f_j(X)v, v\rangle = 0$ and consequently $f_j(X)v = 0$ for all j's. Now Lemma 2.1 yields the conclusion. ∎

Assume now that part (a) of Theorem 1.1 is true. By Lemma 2.2 we find $f_j \in (p)$, so that

$$q \in \sum_{j=1}^{k} f_j^T f_j + sym(p).$$

Hence $q \in sym(p)$. ∎

The next result asserts that the evaluations at pairs $(X, v) \in V_p$ separate the points of the quotient algebra $\mathcal{A}/(p)$.

Lemma 2.3 *There exist finitely many pairs* $(X_k, v_k) \in V_p,\ 1 \le k \le m$, *such that the function* $S : \mathcal{H}_{2d} \to \mathbf{R}$ *defined by*

$$S(h) = \sum_{j=1}^{n} \sum_{k=1}^{m} \langle r_j(X_k)v_k, q_j(X_k)v_k \rangle, \tag{2}$$

where

$$h = \sum q_j^T r_j \quad (r_j, q_j \in \mathcal{A}),$$

has the property:

$$S(f^T f) = 0 \text{ implies } f \in (p)$$

for any $f \in \mathcal{A}_d$.

Proof: Let W_1 denote the closed unit sphere in the finite dimensional space $W = \mathcal{A}_d/(p)_d$, endowed with an Euclidean norm. Given a non-zero class $[h] \in W_1$, since its representative h is not in (p), we can pick by Lemma 2.1 a pair $(X_h, v_h) \in V_p$, such that

$$\langle r(X_h)^T r(X_h) v_h, v_h \rangle_{\mathcal{R}_{2d}} > 0$$

for all r in an open neighborhood $\mathcal{O}$ of $[h]$ in W_1. By the compactness of W_1 there exists a finite cover consisting of such open sets $\mathcal{O}_k$, each associated with a pair $(X_k, v_k) \in V_p,\ \ 1 \le k \le m$. Use these points to produce the definition (2) of S.

Let h be an analytic polynomial in $\mathcal{A}_d$. If the element h is not in (p), then $[h] \neq 0$ and hence a positive multiple of $[h]$ lies on the unit sphere W_1, hence in some open set $\mathcal{O}_k$. Therefore $S(h^T h) \ge \langle h(X_k)v_k, h(X_k)v_k \rangle_{\mathcal{R}_{2d}} > 0$. ■

2.3 Proof of Theorem 1.1.(a)

Let q be a hereditary polynomial satisfying the hypothesis in Theorem 1.1.

Let d be a fixed degree. Denote by $\mathcal{R}_{2d}$ the subset of $\mathcal{P}_{2d}$ consisting of sums of the form

$$\sum_{j=1}^{k} f_j^T f_j + g, \tag{3}$$

with $f_j \in \mathcal{A}_d,\ g \in sym(p)_{2d}$ and the integer k is arbitrary.

The proof will be divided into a few natural steps. The first one is stated as an independent lemma.

Lemma 2.4 *For every* $d \ge 0$ *the cone* $\mathcal{R}_{2d}$ *is closed in* $\mathcal{P}_{2d}$.

Proof: This is an application of Carathéodory's theorem on convex hulls in finite dimensional vector spaces. A similar application of Carathéodory's theorem appears in [9].

Specifically, if $k-1$ denotes the dimension of $\mathcal{H}_{2d}$, then Carathéodory's theorem asserts that every function h in the convex cone $\mathcal{R}_{2d}$ can be written as a combination of at most k elements from the set $\{f^T f + g : f \in \mathcal{A}_d,\ g \in sym(p)\}$ which generates it. Thus, there exist $f_1, \ldots, f_k \in \mathcal{A}_d$ such that

$$h = f_1^T f_1 + f_2^T f_2 + \ldots + f_k^T f_k + w.$$

with $w \in sym(p)$.

Suppose $h^\nu \in \mathcal{R}_{2d}$ is a Cauchy sequence in the topology of $\mathcal{P}_{2d}$. For each (positive integer) ν pick any $f_1^\nu, \ldots, f_k^\nu$ (some of them possibly equal to zero) in $\mathcal{A}_d$ and w^ν in $sym(p)$ such that

$$h^\nu = \sum_{j=1}^{k} f_j^{\nu T} f_j^\nu + w^\nu. \tag{4}$$

Now h^ν is bounded, and if the f_j^ν would also be bounded, we could pass to convergent subsequences and the proof would finish. Here we use the fact that $\mathcal{A}_d$ is finite dimensional so that the bilinear mapping $\mathcal{A}_d \times \mathcal{A}_d \to \mathcal{H}_{2d}$ given by $(f, g) \mapsto g^T f$ is continuous.

In order to prove that the sequences f_j^ν and w^ν can be chosen to be bounded, recall first the linear functional $S : \mathcal{H}_{2d} \to \mathbb{R}$ from Lemma 2.3. Since S is a linear map on the finite dimensional vector space $\mathcal{H}_{2d}$ and since the sequence $\{h^\nu\}$ is bounded, it follows that

$$S(h^\nu) = \sum_{j=1}^{k} \sum_{\ell} \|f_j^\nu(X_\ell) v_\ell\|^2 \tag{5}$$

is bounded. Note also that

$$\|[f]\|^2 = \sum_{\ell} \|f(X_\ell) v_\ell\|^2$$

defines a norm on the quotient $W_d = \mathcal{A}_d/(p)_d$. Thus, equation (5) implies that each of the sequences $[f_j^\nu]$, $j = 1, 2, \ldots, k$, is bounded in W_d (with respect to any norm) and therefore we may assume, by passing to a subsequence if necessary, that each of these sequences is Cauchy. Since W_d is finite dimensional, it is complete, and thus each of the sequences $\{[f_j^\nu]\}$ converges.

The mapping $\mathcal{A}_d \to W_d$ given by $f \mapsto [f]$ is linear and onto. Therefore it has a right inverse ρ. Consequently, the sequences $\{g_j^\nu = \rho[f_j^\nu]\}_\nu$ are bounded for each $j = 1, \ldots, k$. Since $f_j^\nu = g_j^\nu + r_j^\nu$ for $r_j^\nu \in (p)$,

$$h^\nu = \sum (g_j^\nu)^T g_j^\nu + u^\nu$$

for some u^ν in $sym(p)$, and all terms in this decomposition are uniformly bounded in ν. ■

Separation. If the hereditary polynomial q in the statement of Theorem 1.1 admits the decomposition (1), then $q \in \mathcal{R}_{2d}$ for some large d.

Henceforth we contradict this statement and assume that $q \notin \mathcal{R}_{2d}$, for any large d. For instance the assumption

$$d > 4\max(\deg(p_1), ..., \deg(p_n), \deg(q))$$

is sufficient for the rest of the proof.

In view of Lemma 2.4 and by Minkowski's separation theorem there exists a linear functional L_1 on $\mathcal{P}_{2d}$ satisfying:

$$L_1(q) < 0 \leq L_1(c), \quad c \in \mathcal{R}_{2d}. \tag{6}$$

Note that $L_1(sym(p)) = 0$, since $L_1(sym(p)) \geq 0$ and $sym(p)$ is a real vector space. We modify L_1 to $L := L_1 + \epsilon S$ where S is the function defined in Lemma 2.3 and with $\epsilon > 0$, chosen small enough to make

$$L(q) < 0 \leq L(c), \quad c \in \mathcal{R}_{2d}, \tag{7}$$

still hold true. Then L has the additional critical property: if $h \in \mathcal{A}_d$, then

$$L(h^T h) = 0 \text{ implies } h \in (p).$$

The Hilbert space. We consider again the vector space

$$W = W_d = \mathcal{A}_d/(p)_d$$

and denote by $[f]$ or simply f the class of $f \in \mathcal{A}_d$ in W.

Next we define a symmetric positive semi-definite form on W by

$$\langle [a], [b] \rangle = \frac{1}{2} L(a^T b + b^T a).$$

We must check that the definition is independent of the choice of representatives a, b:

$$L((a+rf)^T(b+sf)+(b+sf)^T(a+rf)) =$$

$$L(a^Tb+b^Ta)+L(a^Tsf+(sf)^Ta)+L((rf)^Tb+b^Trf)+L((rf)^Tsf+(sf)^Trf),$$

for an arbitrary element $f \in (p)_d$. The last three terms have the form $L(g)$ with $g \in sym(p)$, so they vanish; thus we obtain a well defined inner product on W which is strictly positive definite by the choice of L. Thus $(W, \langle \cdot, \cdot \rangle)$ is a real Hilbert space.

Construction of matrices. Let W' be the image in W of $\mathcal{A}_{d-1}$ under the projection map and let $X_j : W' \longrightarrow W$ denote the left multiplication by the variable x_j. This is well defined due to the degree assumption and the fact that $m \in (p)$ implies $x_j m \in (p)$. Extend arbitrarily X_j to a linear transformation from W into W, and denote the extension by the same letter. Then the adjoint X_j^T with respect to the real inner product of W is unambiguously defined.

Suppose that our symmetric hereditary polynomial has the form $q = \sum_k (g_k^T h_k + h_k^T g_k)/2$ with $g_k, h_k \in \mathcal{A}_{d-2}$ for all k. Then

$$L(q) = \sum_k \langle g_k, h_k \rangle = \sum_k \langle g_k(X)1, h_k(X)1 \rangle =$$

$$1/2 \sum_k \langle (h_k(X)^T g_k(X) + g_k(X)^T h_k(X))1, 1 \rangle = \langle q(X^T, X)1, 1 \rangle.$$

Thus $\langle q(X^T, X)1, 1 \rangle = L(q) < 0$ by the construction of the functional L. At the same time

$$\langle p_k(X)1, p_k(X)1 \rangle = \langle [p_k], [p_k] \rangle = 0,$$

whence $p_k(X)1 = 0$ for all k.

In conclusion the pair $(X, 1)$ contradicts the hypothesis of Theorem 1.1 and the proof is complete.■

3 Ramifications of the main result

This last part of the note contains a couple of generalizations of Theorem 1.1.

3.1 Analytic modules

The main result above can easily be adapted to more general polynomial sets. For instance consider a left $\mathcal{A}$-module $\mathcal{M} \subset \mathcal{P}$ which contains 1, hence contains $\mathcal{A}$.

Let $\mathcal{N}$ be an $\mathcal{A}$-submodule of $\mathcal{M}$ and consider its symmetrized vector space:

$$sym(\mathcal{N}) = \{\sum_j (r_j^T f_j + f_j^T r_j; \quad r_j \in \mathcal{A},\ f_j \in \mathcal{N}\}.$$

Let h be a $\mathcal{M}$-hereditary element, that is:

$$h = \sum_j f_j^T g_j, \quad f_j, g_j \in \mathcal{M}.$$

Instead of Lemma 2.2 we assume that the following condition is fulfilled.

A. *If a sum of squares*

$$f = \sum_{k=1}^{m} f_k^T f_k, \quad f_k \in \mathcal{M},$$

vanishes on all pairs $(X, v) \in V_{\mathcal{N}}$*, then* $f_k \in \mathcal{N},\ 1 \leq k \leq m$.

With these notations and assumptions the following variant of Theorem 1.1 is valid.

Proposition 3.1 *Let* $\mathcal{M} \subset \mathcal{P}$ *be an* $\mathcal{A}$ *submodule containing* 1 *and let* $\mathcal{N}$ *be a left* $\mathcal{A}$*-submodule of* $\mathcal{M}$*. Suppose that* $\mathcal{N}, \mathcal{M}$ *are subject to condition A.*

If a symmetric $\mathcal{M}$*-hereditary element* h *satisfies*

$$\langle h(X)v, v\rangle \geq 0, \text{ whenever } \ (X, v) \in V_{\mathcal{N}},$$

then there are $f_k \in \mathcal{M},\ 1 \leq k \leq m$*, such that*

$$h = \sum_{k=1}^{m} f_k^T f_k + g, \ ,$$

where $g \in sym(\mathcal{N})$*.*

Note that assumption A is parallel to the notion of a real ideal in the commutative case, see [2].

3.2 Complex coefficients

The case of a free complex $*$-algebra with antilinear involution is similar, with one little improvement in the second part of Theorem 1.1 which, to be precise, removes the symmetry assumption on q.

Namely we consider the $*$-algebra $\mathcal{P} \otimes_{\mathbf{R}} \mathbf{C}$ with the extended antilinear involution $f \mapsto f^*$. The definitions of an analytic, respectively hereditary element are the same.

For a left ideal I of $\mathcal{A} \otimes_{\mathbf{R}} \mathbf{C}$ the zero set V_I consists of all m-tuples X of complex $N \times N$-matrices and a vector $v \in \mathbf{C}^N$, $N \in \mathbf{N}$, satisfying $f(X)v = 0$, for all $f \in I$.

Proposition 3.2 *Let I be a left ideal of $\mathcal{A} \otimes_{\mathbf{R}} \mathbf{C}$. If a hereditary element $q \in \mathcal{P} \otimes_{\mathbf{R}} \mathbf{C}$ satisfies*

$$\langle q(X)v, v \rangle = 0, \quad (X, v) \in V_I,$$

then $q \in sym(I) + \mathrm{i}\ sym(I)$.

The decomposition $2q = (q + q^*) + i[(q - q^*)/i]$ reduces the proof to the self-adjoint case $q = q^*$, and this can be treated by a direct analogue of Theorem 1.1. Note that all terms in the decomposition remain hereditary.

Indeed, by definition $q^*(X) = q(X)^*$, and

$$\langle q(X)v, v \rangle =< v, q(X)^* v >= \overline{\langle q^*(X)v, v \rangle}$$

for any m-tuple of complex $N \times N$ matrices X and vector $v \in \mathbf{C}^N$. Thus, if q vanishes on V_I (in the sense of the statement), then the same is true of q^*, and hence the real and imaginary parts of q also vanish on V_I.

References

[1] J. Agler, *An abstract approach to model theory*, Surveys of some recent results in operator theory, Vol. II, 1–23, Pitman Res. Notes Math. Ser., **192**, Longman Sci. Tech., Harlow, 1988.

[2] J. Bochnack, M. Coste and J.-F. Roy, *Géométrie Algébrique Réele*, Springer, New York, 1987.

[3] J.W. Helton, *Positive non commutative polynomials are sums of squares* Ann. Math **56**(2002), 675-694.

[4] J.W. Helton and S. McCullough, *A Positivstellensatz for Noncommutative Polynomials*, Trans. Amer. Math. Soc., to appear.

[5] J.W. Helton, S. McCullough, M.Putinar, *A noncommutative Positivstellensatz on isometries*, J. reine angew. Math., to appear.

[6] A.Prestel and C.N.Delzell, *Positive Polynomials*, Springer, Berlin, 2001.

[7] C. Procesi and M. Schacher, *A noncommutative real Nullstellensatz and Hilbert's 17th problem*, Ann. of Math. (2) **104** (1976), no. 3, 395–406.

[8] M. Reed and B. Simon, *Methods of Modern Mathematical Physics Vol. 1: Functional Analysis*, Academic Press, San Diego, 1980.

[9] B. Reznick, *Sums of even powers of real linear forms*, Mem. Amer. Math. Soc. **96** (1992) No. **463**, Amer. Math. Soc., Providence, R.I.

[10] C. Scheiderer, *Positivity and sums of squares: a guide to some recent results*, preprint 2003.

[11] G. Stengle, *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*, Math. Ann. **289**(1991), 203-206.

J. W. Helton, Department of Mathematics, University of California at San Diego, La Jolla CA 92093
helton@osiris.ucsd.edu

S.A. McCullough, Department of Mathematics, University of Florida, Gainesville, FL 32611-8105
sam@mail.math.ufl.edu

M. Putinar, Department of Mathematics, University of California, Santa Barbara, CA 93106
mputinar@math.ucsb.edu